Veiklos nuostatai ir politika, teikiant kvalifikuotas paslaugas

Dokumento versija: v1.3

Unikalus dokumento numeris ID (OID): 3.6.1.4.1.60536.1.1

Galioja nuo 2024-03-01

Turinys

1. ĮVADAS

UAB „iSense Technologies“ pagrindinė veikla – informacinių sistemų kūrimas, diegimas ir priežiūra viešojo sektoriaus organizacijoms ir verslo bendrovėms.

1.1. Dokumento apžvalga

Šis dokumentas detaliai apibrėžia UAB „iSense Technologies“ veiklą, teikiant Kvalifikuotas patikimumo užtikinimo paslaugas.

Kvalifikuotų patikimumo užtikrinimo paslaugų sąrašas:

- (QVal for QESig) Kvalifikuotų elektroninių parašų kvalifikuotos galiojimo patvirtinimo paslaugos (Qualified validation service for qualified electronic signature).
- (QVal for QESeal) Kvalifikuotų elektroninių spaudų kvalifikuotos galiojimo patvirtinimo paslaugos (Qualified validation service for qualified electronic seal).

1.2. Dokumento keitimai

Versija	Data	Aprašymas
1.1	2023 06 25	Pradinė dokumento versija
1.2.2	2023 06 29	Darbinė dokumento versija
1.3	2023 12 01	Versija derinimui su RRT

1.3. Naudojamos sąvokos ir trumpiniai

Trumpiniai	Aprašymas
QVal for QESig	Kvalifikuotų elektroninių parašų kvalifikuotos galiojimo patvirtinimo paslaugos
QVal for QESeal	Kvalifikuotų elektroninių spaudų kvalifikuotos galiojimo patvirtinimo paslaugos
Kvalifikuotos paslaugos	QVal for QESig ir QVal for QESeal paslaugos
ISENSE	UAB „iSense Technologies“

VERIFFY IS	ISENSE valdoma informacinė sistema, skirta teikti kvalifikuotas paslaugas
Dokumentacijos saugykla	www.veriffy.com internetinėje svetainėje sukurta sritis, skirta pateikti viešus dokumentus.
Veiklos nuostatai	Šis dokumentas
PoE	Egzistavimo įrodymas
Laiko žyma	Elektroninės formos duomenys, kuriais kiti elektroninės formos duomenys susiejami su tam tikru laiku, ir taip sukuriamas įrodymas, kad pastarieji egzistavo tuo metu
Elektroninis parašas	Elektroninės formos duomenys, kurie prijungti prie kitų elektroninės formos duomenų arba logiškai susieti su jais, ir kuriuos pasirašantis asmuo naudoja pasirašydamas
Elektroninis spaudas	Elektroninės formos duomenys, prijungti prie kitų elektroninės formos duomenų arba su jais logiškai susieti, kad būtų užtikrinta pastarųjų kilmė ir vientisumas
Kvalifikuotas elektroninis parašas	Pažangusis elektroninis parašas, sukurtas naudojant kvalifikuotą elektroninio parašo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio parašo sertifikatu
Kvalifikuotas elektroninis spaudas	Pažangusis elektroninis spaudas, sukurtas naudojant kvalifikuotą elektroninio spaudo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio spaudo sertifikatu
Laiko žymos paslaugų teikėjas	(TSA – Time-Stamping Authority) – patikimumo užtikrinimo paslaugų teikėjas, teikiantis laiko žymos formavimo paslaugas
Pasirašantis asmuo	Veiksnus fizinis asmuo, kuris sukuria elektroninį parašą
Spaudo kūrėjas	Juridinis asmuo, kuris sukuria elektroninį spaudą
Duomenų saugos nuostatai	UAB „iSense Technologies“ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI
Naudotojų administravimo taisyklės	UAB „iSense Technologies“ INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

Informacijos tvarkymo taisyklės	UAB „iSense Technologies“ INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS
Veiklos tęstinumo planas	UAB „iSense Technologies“ INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS
Incidentų valdymo taisyklės	UAB „iSense Technologies“ INFORMACINIŲ SAUGOS INCIDENTŲ VALDYMO TAISYKLĖS
eIDAS	2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB
Kvalifikuotas elektroninio parašo kūrimo įtaisas	Elektroninio parašo kūrimo įtaisas, atitinkantis eIDAS reglamento II priede nustatytus reikalavimus
Kvalifikuoto elektroninio parašo sertifikatas	Elektroninio parašo sertifikatas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, ir kuris atitinka eIDAS reglamento I priede nustatytus reikalavimus
ETSI	Europos telekomunikacijų standartizavimo institutas (angl. *European Telecommunication Standardisation Institute*)
OID	Unikalus objekto identifikatorius (angl. *Object Identifier*)
PIN	Asmens identifikacinis skaičius (angl. *Personal Identification Number*)
OCSP	Sertifikato galiojimo patvirtinimas, atitinkantis RFC 6960 rekomendacijas
CRL	Sertifikato galiojimo patvirtinimas, atitinkantis RFC 5280 rekomendacijas

1.4. Dokumento identifikavimas

Veiklos nuostatai viešai skelbiami Dokumentacijos saugykloje. Unikalus veiklos nuostatų identifikatorius (OID) - 1.3.6.1.4.1.60536.1.1

1.5. Reglamentuojančių dokumentų sąrašas

- 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (toliau – eIDAS), naujausia redakcija;
- 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos, tvarkant asmens duomenis, ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinama Direktyva 95/6/EB (toliau – Bendrasis asmens duomenų apsaugos reglamentas) naujausia redakcija;
- Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo naujausia redakcija;
- Lietuvos Respublikos 2016 m. vasario 18 d. nutarimas Nr. 144 „Dėl patikimumo užtikrinimo paslaugų priežiūros įstaigos ir įstaigos, atsakingos už nacionalinio patikimo sąrašo sudarymą, tvarkymą ir skelbimą, paskyrimo“;
- Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo naujausia redakcija;
- Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. birželio 21 d. įsakymas Nr.1V-588 „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 2019 m. birželio 4 d. įsakymas Nr. 1V-594 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo“;
- ETSI EN 319 403 v2.3.1: Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 401 v2.3.1: General Policy Requirements for Trust Service Providers;

- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI). Policy requirements for TSP providing signature validation services.

1.6. Veiklos nuostatus tvarkanti organizacija

UAB „iSense Technologies“

Įmonės kodas: 302553999

Adresas: Mėnulio g. 7, 04326 Vilnius

Internetinės svetainės adresas: www.isense.lt

El. pašto adresas: info@isense.lt

Veiklos nuostatus tvirtina UAB „iSense Technologies“ direktorius.

1.7. Kontaktinė informacija

Informaciją, visais klausimais susijusiais su šiuo dokumentu ir teikiamomis kvalifikuotomis paslaugomis, teikia UAB „iSense Technologies“ el. paštu: info@veriffy.com

1.8. Informacija apie Kvalifikuotas paslaugas

Informacija apie kvalifikuotas paslaugas teikiama adresu www.veriffy.com/reliability.

Informacija apie teikiamas paslaugas yra reguliariai peržiūrima ir atnaujinama bent kartą per metus.

ISENSE garantuoja Dokumentacijos saugyklos prieinamumą 99,99% laiko.

ISENSE garantuoja Paslaugų teikimo prieinamumą 99,99% laiko.

2. BENDROSIOS NUOSTATOS

2.1. Atsakomybė

2.1.1. Veiklos atsakomybė

ISENSE prisiima atsakomybę už naudotojų patirtus nuostolius eIDAS 13 str. ir Lietuvos Respublikos elektroninės atpažinties, ir patikimumo užtikrinimo paslaugų įstatyme nustatyta tvarka.

Kvalifikuotų paslaugų teikėjų atsakomybė nustatyta eIDAS naujausioje redakcijoje, Lietuvos Respublikos teisės aktuose, reglamentuojančiuose patikimumo užtikrinimo paslaugas tiek, kiek neprieštarauja eIDAS, bei sudaromose sutartyse.

2.1.2. Veiklos atsakomybės ribojimai

ISENSE atsako už teikiamų paslaugų kokybę bei prieinamumą, tačiau tik savo valdomos sistemos veikimo ribose.

ISENSE neatsako už trečiųjų šalių sisteminius gedimus, trikdžius (fiksuotus ne ISENSE veikimo ribose), dėl kurių galimai sutriko teikiamų paslaugų teikimas, kokybė bei prieinamumas.

ISENSE neatsako už Klientų sistemose atsiradusius gedimus, trikdžius, dėl kurių galimai sutriko teikiamų paslaugų teikimas, kokybė ir prieinamumas.

2.1.3. Finansinė atsakomybė

Finansinės atsakomybės įsipareigojimams užtikrinti ISENSE savo veiklą draudžia ne mažesne kaip Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo 10 str. nustatyta suma.

2.2. Teisinės nuostatos ir interpretavimas

2.2.1. Kvalifikuoto elektroninio parašo ir antspaudo teisinė galia

- Kvalifikuoto elektroninio parašo teisinė galia yra lygiavertė rašytiniam parašui. Kvalifikuotas elektroninis parašas, patvirtintas vienoje valstybėje narėje išduotu

kvalifikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kaip kvalifikuotas elektroninis parašas;

- Kvalifikuotam elektroniniam spaudui taikoma prezumpcija dėl duomenų, su kuriais susietas kvalifikuotas elektroninis spaudas, vientisumo ir tų duomenų kilmės tinkamumo. Kvalifikuotas elektroninis spaudas, patvirtintas vienoje valstybėje narėje išduotu kvalifikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kvalifikuotu elektroniniu spaudu.

2.2.2. Pagrindiniai teisės aktai

Kvalifikuotų paslaugų dalyvių teises ir atsakomybę, reikalavimus Kvalifikuotų paslaugų teikėjams bei jų atsakomybę nustato šio dokumento 1.5 punkte nurodyti teisės aktai.

2.2.3. Ginčų sprendimo tvarka

Bet kokie ginčai tarp ISENSE ir Klientų sprendžiami derybų keliu. Neišsprendus ginčo, jis sprendžiamas teismo tvarka, vadovaujantis galiojančiais Lietuvos Respublikos teisės aktais.

2.3. Kvalifikuotų paslaugų teikimo įkainiai

Kvalifikuotų paslaugų teikimo įkainiai viešai skelbiami adresu www.veriffy.com/reliability.

2.4. Informacijos teikimas

2.4.1. Informacijos teikimas priežiūros organizacijai

- ISENSE informuoja Priežiūros įstaigą nedelsiant, bet ne vėliau nei per 3 darbo dienas, apie bet kokius savo kvalifikuotų patikimumo užtikrinimo paslaugų teikimo pakeitimus, kurie gali įtakoti teikiamų Kvalifikuotų paslaugų teikimo kokybę;
- ne vėliau kaip prieš 3 darbo dienas informuoja patikimumo užtikrinimo paslaugų gavėjus ir Priežiūros įstaigą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti nepertraukiamą Kvalifikuotų paslaugų teikimą;

- iki kiekvienų metų vasario 1 d. pateikia Priežiūros įstaigai praėjusių kalendorinių metų veiklos ataskaitą, kurioje nurodomas bendras per praėjusius kalendorinius metus tikrintų kvalifikuotų elektroninių parašų ir kvalifikuotų elektroninių spaudų skaičių.

2.4.2. ISENSE viešai teikiama informacija

ISENSE viešai teikiamą informaciją sudaro:

- informacija apie Kvalifikuotų paslaugų teikimo statusą;
- Kvalifikuotų paslaugų sudarymo ir tvarkymo sąlygos;
- Kvalifikuotų paslaugų teikimo kainoraščiai;
- Kvalifikuotų paslaugų naudojimo instrukcijos vartotojams;
- įgaliotų institucijų parengtos ISENSE veiklos tikrinimo ataskaitų santraukos;
- kita įvairi organizacinės paskirties ar patikimą veiklą įrodanti informacija susijusi su Kvalifikuotų paslaugų teikimu;
- įvairūs skelbimai susiję su teikiamomis Kvalifikuotomis paslaugomis.

2.4.3. Teikiamos informacijos atnaujinimo dažnumas

ISENSE teikiama informacija atnaujinama tokiu laiku ar dažnumu:

- pakeitimai daromi, tvirtinami ir skelbiami taip, kaip numatyta Duomenų saugos nuostatuose;
- kita skelbtina ir atnaujinta informacija (pvz., ISENSE veiklos tikrinimo išvados, kt.) skelbiama ją gavus ar parengus per protingą terminą;
- kasmetinis rizikos vertinimas, vadovaujantis Duomenų saugos nuostatais, atliekamas kartą metuose, kurių metu patikrinama ir inventorizuojama naudojama programinė ir techninė įranga;

3. ATITIKTIES VERTINIMAS

ISENSE veiklos atitiktis tinkamai teikti Kvalifikuotas paslaugas, atliekama:

- vadovaujantis eIDAS 20 str. 1 d. atitikties vertinimo įstaiga kas 24 (dvidešimt keturis) mėnesius atlieka ISENSE auditą;

- vadovaujantis eIDAS 20 str. 2 d., priežiūros įstaiga bet kuriuo metu gali atlikti ISENSE auditą arba reikalauti, kad atitikties įstaiga atliktų ISENSE vertinimą (ISENSE lėšomis), siekiant patvirtinti, kad teikiamos paslaugos atitinka eIDAS nustatytus reikalavimus;
- vadovaujantis eIDAS 20 str. 3 d., kai priežiūros įstaiga reikalauja, kad ISENSE ištaisytų bet kuriuos eIDAS reikalavimų pažeidimus, ir ISENSE to nepadaro per priežiūros įstaigos nustatytą laikotarpį, priežiūros įstaiga, atsižvelgdama visų pirma į tokių pažeidimų mastą, trukmę ir pasekmes, gali panaikinti ISENSE arba pažeidimo paveiktų ISENSE teikiamų paslaugų kvalifikacijos statusą ir pranešti apie tai eIDAS 20 str. 3 d. nurodytai įstaigai, kad būtų galima atnaujinti patikimus sąrašus;

4. KONFIDENCIALUMO NUOSTATOS

4.1. Asmens duomenys

ISENSE tvarko asmens duomenis, vadovaudamasi Bendrojo asmens duomenų apsaugos reglamento bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kuris įgyvendina 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmenų apsaugos, tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kiek jis neprieštarauja Bendrajam asmens duomenų apsaugos reglamentui. Asmens duomenys saugomi tinkamą, reikiamą laikotarpį (įskaitant ISENSE nutraukus veiklą), bet ne ilgiau, nei to reikia duomenų tvarkymo tikslais, apie kurį asmuo yra informuojamas, kad duomenis būtų galima panaudoti teismo procese bei taip būtų užtikrinamas veiklos tęstinumas.

Kai asmens duomenys nebereikalingi jų tvarkymo tikslams, jie yra sunaikinami, išskyrus tuos, kurie įstatymų nustatytais atvejais turi būti perduodami valstybės archyvams.

4.2. Slapta informacija

Slaptoji informacija, kuri saugoma ir tvarkoma laikantis ISENSE vidaus taisyklių, yra:

- atliktų operacijų įrašai (angl. *log file*);
- įrašai apie patikimumo užtikrinimo paslaugų teikimo sutrikimus, jeigu jų paskelbimas gali sukelti pavojų Kvalifikuotų paslaugų teikimui;
- įrašai apie vidinius ir išorinius ISENSE veiklos patikrinimus, jei jų paskelbimas gali sukelti pavojų ISENSE teikiamų paslaugų saugumui;
- veiksmų avariniais atvejais planai;
- informacija apie aparatinės ir programinės įrangos apsaugojimo būdus ir patikimumo užtikrinimo paslaugų operacijų atlikimą.

4.3. Neslapta informacija

- Kvalifikuotų paslaugų sudarymo ir tvarkymo sąlygos;
- Kvalifikuotų paslaugų kainoraščiai;
- instrukcijos vartotojams;
- įgaliotų institucijų parengtos ISENSE veiklos tikrinimo ataskaitų santraukos.

4.4. Informacijos teikimas teisėsaugai

Slaptoji ISENSE informacija gali būti teikiama teisėsaugos institucijų pareigūnams, tik laikantis Lietuvos Respublikos teisės aktų reikalavimų.

5. REIKALAVIMAI KVALIFIKUOTŲ PASLAUGŲ TEIKIMUI

5.1. Bendrieji reikalavimai Kvalifikuotų paslaugų teikimui

Bendri kvalifikuotų tiekėjų reikalavimai teikti Kvalifikuotas paslaugas yra aprašyti ETSI EN 319 401 standarte.

Kvalifikuotos paslaugos, tai yra patikrinimas, atliekamas pagal eIDAS 32, 33 ir 40 straipsnių reikalavimus. Kvalifikuotos paslaugos suteikia pasikliaujančiosioms šalims galimybę galiojimo patvirtinimo procedūros rezultatą gauti automatizuotu būdu, kuris

būtų patikimas, veiksmingas ir susietas su kvalifikuotos galiojimo patvirtinimo paslaugos teikėjo pažangiuoju elektroniniu parašu arba pažangiuoju elektroniniu spaudu.

Pagrindiniai reikalavimai, kurie nustatyti Kvalifikuotoms paslaugoms:

- sertifikatas, kuriuo tvirtinamas parašas, pasirašymo metu buvo kvalifikuotas elektroninio parašo sertifikatas;
- kvalifikuotą sertifikatą išdavė kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, ir jis galiojo pasirašymo metu;
- parašo patvirtinimo duomenys atitinka pasikliaujančiajai šaliai pateiktus duomenis;
- unikalus duomenų, kuriais sertifikate nurodomas pasirašantis asmuo, rinkinys tinkamai pateikiamas pasikliaujančiajai šaliai;
- jei pasirašymo metu buvo naudojamas slapyvardis, tai aiškiai nurodoma pasikliaujančiajai šaliai;
- elektroninis parašas, sukurtas naudojant kvalifikuotą elektroninio parašo kūrimo įtaisą;
- nebuvo pažeistas pasirašytų duomenų vientisumas;
- pasirašymo metu buvo laikomasi eiDAS 26 straipsnyje nurodytų reikalavimų;
- sistema, naudojama kvalifikuoto elektroninio parašo galiojimo patvirtinimo tikslais, duoda pasikliaujančiajai šaliai teisingą galiojimo patvirtinimo procedūros rezultatą ir leidžia pasikliaujančiai šaliai nustatyti bet kokias su saugumu susijusias problemas;
- parašų tikrinimas atliekamas vadovaujantis standartu ETSI TS 119 102-1;
- parašų tikrinimo ataskaitą formuojama vadovaujantis standartu ETSI TS 119 102-2.

5.2. Įrašų rinkimas ir saugojimas

5.2.1. Registruojami įvykiai

Visos kvalifikuotų paslaugų užsakymo operacijos yra fiksuojamos saugiame operacijų žurnale. Žurnalo įrašai yra saugomi ne trumpiau nei 10 (dešimt) metų. Fiksuojamos paslaugos užsakymo operacijos apima:

- kvalifikuotos paslaugos tipas patikrinimas;
- laikas ir data;
- unikalus kliento identifikatorius;
- unikalus užklausos identifikatorius;
- loginė reikšmė, ar paslauga sėkmingai suteikta.

Informacinių sistemų, jų naudotojų ir administratorių veiksmų analizei atlikti yra naudojamas informacinių sistemų komponentų įvykių žurnalas. Fiksuojami duomenys apima:

- informaciją apie informacinių sistemų tarnybinių stočių, taikomosios programinės įrangos ir kitų informacinių sistemų komponentų įjungimą, išjungimą ar perkrovimą;
- sistemų administratorių atliekami infrastruktūros konfigūracijų pakeitimų veiksmai;
- programinės įrangos naujinimo veiksmai.

Diagnostikos žurnale fiksuojami detalūs sistemų veiksmai, kurie naudojami sistemų veikimo analizei, diagnostikai ir sutrikimų šalinimui. Pagrindiniai diagnostikos žurnalo naudotojai – sistemų kūrėjai ir administratoriai. Klaidų žurnale (angl. *Error Log*) fiksuojama informacija apie sistemų sutrikimus ir klaidas, nurodant sutrikimo laiką, šaltinį, aprašymą ir detalią informaciją.

5.2.2. Įrašų peržiūros dažnumas

ISENSE sistemos operacijų ir veiklos registravimo žurnalai peržiūrimi ne rečiau kaip 1 (vieną) kartą per mėnesį. Kiekvienas didesnės svarbos įvykis ar įvykis, atsitikęs dėl netinkamo sistemų funkcionavimo, turi būti aprašytas. Informacinių sistemų komponentų įvykių žurnalų elektroninės informacijos, susijusios su informacinių sistemų naudotojų ir

informacinių sistemų administratorių atliekamais veiksmais, žurnalai peržiūrimi Duomenų saugos nuostatuose nustatytais terminais bei tvarka.

5.2.3. Įrašų saugojimo periodas

ISENSE sistemos operacijų ir veiklos registravimo žurnalai ISENSE saugomi 10 (dešimt) metų, tolesnį saugojimą reglamentuoja Lietuvos Respublikos dokumentų ir archyvų įstatymo naujausia redakcija.

5.2.4. Įrašų apsauga

ISENSE sistemų operacijų ir veiklos registravimo žurnalų atsarginės kopijos daromos kiekvieną dieną. Viršijus konkrečiam žurnalui numatytą įrašų kiekį, žurnalo turinys perkeliamas į archyvą.

5.3. Duomenų archyvavimas

Į archyvą atiduodama:

- sistemos operacijų ir veiklos registravimo žurnalai;

Duomenys archyve saugomi 10 (dešimt) metų, tolesnį saugojimą reglamentuoja Lietuvos Respublikos dokumentų ir archyvų įstatymas.

Atsarginės kopijos įgalina atstatyti sistemos darbą po sutrikimų. Tuo tikslu daromos šios programinės įrangos ir duomenų failų kopijos:

- instaliacinio disko su Veriffy sistemos programine įranga;
- Veriffy sistemų operacijų ir veiklos registravimo žurnalų.

5.4. Saugumo incidentų valdymas

Incidentai klasifikuojami ir valdomi pagal ISENSE patvirtintus dokumentus:

- incidentų klasifikavimas aprašytas Incidentų valdymo dokumente;
- kritinių saugos incidentų valdymas aprašytas Veiklos tęstinumo plane.

ISENSE vadovaujasi tokia tvarka, valdant saugumo incidentus:

- fiksavus informacinių sistemos veiklos sutrikimus/ incidentus, kurie pažymi neįprastą ar neatitinkančią informacinių sistemų komponentų veiklą, tokie sutrikimai/ incidentai visais atvejais yra registruojami įvykių žurnale, kuris turi būti

archyvuojamas ir apsaugotas nuo pažeidimo, praradimo, nesankcionuoto ar netyčinio pakeitimo, ar sunaikinimo, siekiant užtikrinti, kad elektroninės informacijos saugos (kibernetinių) incidentų metu įvykdytų nusikalstamų veikų įrodymai būtų tinkami ir pakankami teisėsaugos institucijoms nustatyti nusikalstamų veikų faktą, o nusikalstamas veikas įvykdę asmenys negalėtų jo paneigti;

- įregistravus sutrikimą/ incidentą, jie yra prioretizuojami bei identifikuojami. Identifikavimo metu įvykio įrašas yra atpažįstamas ir jam, priklausomai nuo specializuotų įvykių žurnalų analizės priemonių nustatymų, priskiriama kategorija ir prioritetas;
- analizės metu yra įvertinama, ar įvykis arba įvykių visuma duotuoju laiko momentu atitinka tam tikras specializuotų įvykių žurnalų analizės priemonių nustatytas įspėjimo generavimo taisykles. Jei analizės metu specializuotos įvykių žurnalų analizės priemonės nustato, kad tam tikras įvykis arba įvykių visuma duotuoju laiko momentu atitinka tam tikras nustatytas įspėjimo generavimo taisykles, tuomet specializuotos įvykių žurnalų analizės priemonės automatiškai sugeneruoja įspėjimą;
- informacinių sistemų komponentų administratoriai turi peržiūrėti sugeneruotą įspėjimą ir, esant reikalui, apie įspėjimą, jo turinį ir aplinkybes informuoti atsakingus asmenis;
- paskirtasis informacijos saugumo pareigūnas turi peržiūrėti sugeneruotą įspėjimą ir įvertinti, ar jis gali būti susijęs su saugumo ir vientisumo pažeidimais numatytais eIDAS 19 str. 2 d. Nustačius, jog incidentas gali būti susijęs su eIDAS 19 str. 2 d. numatytais saugumo bei vientisumo pažeidimais, saugumo pareigūnas nedelsiant, bet ne vėliau kaip per 4 (keturias) val. privalo sušaukti Veiklos tęstinumo plane numatytą darbo grupę. Apie paminėtus incidentus priežiūros įstaiga ir fiziniai ar juridiniai asmenys informuojami pagal Incidentų valdymo dokumente aprašytą tvarką ne vėliau kaip per 24 (dvidešimt keturias) val.;

- turi užregistruoti atitinkamą incidentą su žyma, jog jis yra susijęs su eIDAS 19 str. 2 d. numatytu saugumo bei vientisumo pažeidimu;
- ne vėliau nei per 3 darbo dienas nuo įregistruoto pažeidimo, turėjusio didelį poveikį, suvaldymo ar pasibaigimo, informuoja priežiūros tarnybą, pateikdama nustatytos formos pranešimą.

5.5. Paslaugų teikimo nutraukimas

5.5.1. Visiškas paslaugų teikimo nutraukimas

ISENSE, prieš nutraukdama Kvalifikuotų paslaugų teikimo veiklą, įsipareigoja veikti pagal su priežiūros įstaiga suderintą veiklos nutraukimo planą (toliau – Suderintas planas), įskaitant šiuos veiksmus (kiek jie neprieštarauja suderintam planui):

- apie Kvalifikuotų paslaugų nutraukimą reikia informuoti visus susijusius asmenis bei organizacijas, taip pat priežiūros įstaigą ne vėliau kaip prieš 3 (tris) mėnesius prieš planuojamą Kvalifikuotų paslaugų nutraukimo terminą;
- atsižvelgiant į numatytą paslaugų nutraukimo datą, tačiau ne vėliau kaip prieš 2 (du) mėnesius, priežiūros įstaigai pateikia:
    - informaciją apie veiklos perėmėją;
    - veiklos perėmimo sutartį;
    - detalųjį Kvalifikuotų paslaugų teikimo veiklos nutraukimo planą.
- jei nusprendus nutraukti Kvalifikuotų paslaugų teikimą, veikla nėra perduodama trečiajai šaliai, ISENSE turi užtikrinti veiklos įrašų išsaugojimą.

5.5.2. Paslaugų teikimo nutraukimas dėl ES taikomų sankcijų

Kvalifikuotų paslaugų teikimas gali būti nutrauktas, jeigu pradėjus teikti Kvalifikuotas paslaugas Klientui bus pradėtos taikyti ES sankcijos.

5.6. Trečiųjų šalių įtraukimas, teikiant Kvalifikuotas paslaugas

ISENSE, pasitelkdama trečiųjų šalių sprendimus ar paslaugas, visada tikrina ir užtikrina, kad trečiųjų šalių naudojamos techninės ir organizacinės priemonės,

užtikrinančios paslaugų teikimo kokybę bei informacijos saugą, būtų ne žemesnio lygio nei ISENSE nustatytas būtinas informacijos saugos lygis.

Kvalifikuotų paslaugų teikimui naudojami Microsoft Azure siūlomi sprendimai ir paslaugos.

Kvalifikuoto patikrinimo ataskaitoje naudojamos kvalifikuotos laiko žymos, kurios užtikrina ataskaitų autentiškumą (PoE). Kvalifikuotų laiko žymų tiekėjas yra Kingdom of Belgium - Federal Government (https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/BE/11).

6. FIZINIO SAUGUMO KONTROLĖ

Veriffy informacinė sistema, operatorių darbo vietos, informacijos resursai yra įrengti ir laikomi tam tikslui skirtoje vietoje, kuri yra fiziškai apsaugota nuo neleistino patekimo į ją, įrangos sunaikinimo ar išnešimo. Prieiga prie kertinių sistemos elementų yra stebima. Kiekvienas asmenų patekimas į ją Duomenų centre yra registruojamas, stebimas elektros energijos tiekimo stabilumas, temperatūra ir drėgmė.

Kvalifikuotų paslaugų teikimą užtikrinanti techninė ir programinė įranga veikia Duomenų centre, kuriame užtikrintas fizinės prieigos ribojimas.

Kvalifikuotų paslaugų teikimą užtikrinanti techninė ir programinė įranga veikia Duomenų centre, kuriame užtikrintas nepertraukiamas elektros energijos tiekimas, ir veikia oro kondicionavimo įranga.

Kvalifikuotų paslaugų teikimą užtikrinanti techninė ir programinė įranga veikia Duomenų centre, kuriame užtikrinta apsauga nuo užpylimo vandeniu.

Kvalifikuotų paslaugų teikimą užtikrinanti techninė ir programinė įranga veikia Duomenų centre, kuriame įdiegtos automatinės gaisro gesinimo sistemos.

Kvalifikuotų paslaugų teikimui naudojami kriptografiniai raktai, saugomi tinkamai apsaugotoje Microsoft Azure aplinkoje. Kriptografinių raktų kopijos nedaromos.

Priklausomai nuo informacijos svarbos, laikmenos su archyvų duomenimis ir atsarginėmis duomenų kopijomis yra saugomos ugniai atspariuose seifuose.

Popierius ir elektroninės laikmenos, kuriose yra Kvalifikuotų paslaugų teikimo saugumui įtakos turinti informacija, pasibaigus tos informacijos saugojimo terminui, sunaikinamos specialiais plėšymo įrenginiais.

Prieiga prie Kvalifikuotų paslaugų teikimo infrastruktūros sistemos komponentų yra galima tik iš tam tikrų IP adreso tinklo prievadų.

7. PROCEDŪRINIO SAUGUMO KONTROLĖ

Pareigybės, nuo kurių priklauso ISENSE veikla yra:

- informacijos saugumo pareigūnas. Bendra atsakomybė už saugumo politikos vykdymą. IT Saugos įgaliotinio atsakomybės ir funkcijos yra aprašytos Duomenų saugos nuostatuose;
- pagrindinis Veriffy administratorius. Atsakingas už Kvalifikuotų paslaugų tinkamą veikimą. Instaliuoja ir konfigūruoja naudojamą įrangą; nustato sistemos ir tinklo parametrus;
- pagalbinis Veriffy administratorius. Esant poreikiui pavaduoja pagrindinį Veriffy administratorių.

ISENSE darbuotojų pareigų identifikacija ir autentiškumo tikrinimas atliekami tokiais būdais:

- sudarant asmenų sąrašą, kuriems leidžiama patekti į ISENSE patalpas;
- sudarant asmenų sąrašą, kuriems leidžiama fizinė prieiga prie Veriffy sistemos ir tinklo resursų;
- naudotojų administravimo taisyklėse nurodytos taisykles užtikrina, kad:
    - kiekvienas informacinės sistemos naudotojas yra unikalus ir betarpiškai susietas su konkrečiu asmeniu;
    - prisijungimo prie sistemos duomenimis negali būti dalijamasi su bet kuriais kitais asmenims;
    - yra numatytos ribotos funkcijos (kylančios iš konkretaus asmens pareigų).

8. PERSONALO SAUGUMO KONTROLĖ

Asmenys į darbą priimami vadovaujantis Lietuvos Respublikos darbo kodekso reikalavimais. Priėmimas į darbą įforminamas darbo sutartimi. Darbo tvarkos taisyklėse yra nurodyti bendri darbuotojams keliami kvalifikacijos reikalavimai.

Be minėtų bendrų reikalavimų garantuojama, kad ISENSE pavestas pareigas atliekantys asmenys:

- yra pasirašę susitarimą dėl pareigų vykdymo ir atsakomybės;
- yra išklausę vidinius mokymus, susijusius su jiems pavestų pareigų vykdymu;
- yra išklausę mokymus, susijusius su asmens duomenų ir konfidencialios informacijos apsauga, susipažinę su saugos dokumentais bei yra pasirašę pasižadėjimą dėl konfidencialios informacijos saugojimo, jog yra susipažinę su saugos dokumentais;
- neturi neišnykusio ar nepanaikinto teistumo už tyčinių nusikaltimų padarymą.

Samdomi asmenys, atliekantys užduotis pagal sutartis (išorinių paslaugų tiekėjai, programinės įrangos kūrėjai, kt.), tikrinami laikantis tokių pačių procedūrų, kurios taikomos ISENSE darbuotojams.

9. KVALIFIKUOTŲ PASLAUGŲ TEIKIMO REALIZACIJA

9.1. Techninė realizacija

Kvalifikuotos paslaugos rezultatas – ataskaita apie elektroninius parašus, antspauduota UAB „iSense Technologies“ pažangiuoju elektroniniu spaudu. Kvalifikuotos paslaugos ataskaitos pateikimo formatas:

- XML ataskaita pagal standartą ETSI TS 119 102-2. Ataskaitos autentiškumas patvirtinamas elektroniniu spaudu.
- PDF ataskaita. Ataskaitos autentiškumas patvirtinamas elektroniniu spaudu.

Veriffy programinė įranga atlieka patikrinimą elektroniniams parašams, paruoštiems pagal šiuos formatus:

- EN 319 122 (AdES)

- EN 319 132 (XAdES)
- EN 319 142 (PAdES)
- EN 319 162 (ASiC)

Principinė kvalifikuotos paslaugos teikimo seka pagal ETSI TS 119 102-1 standartą pateikiamos schemose:

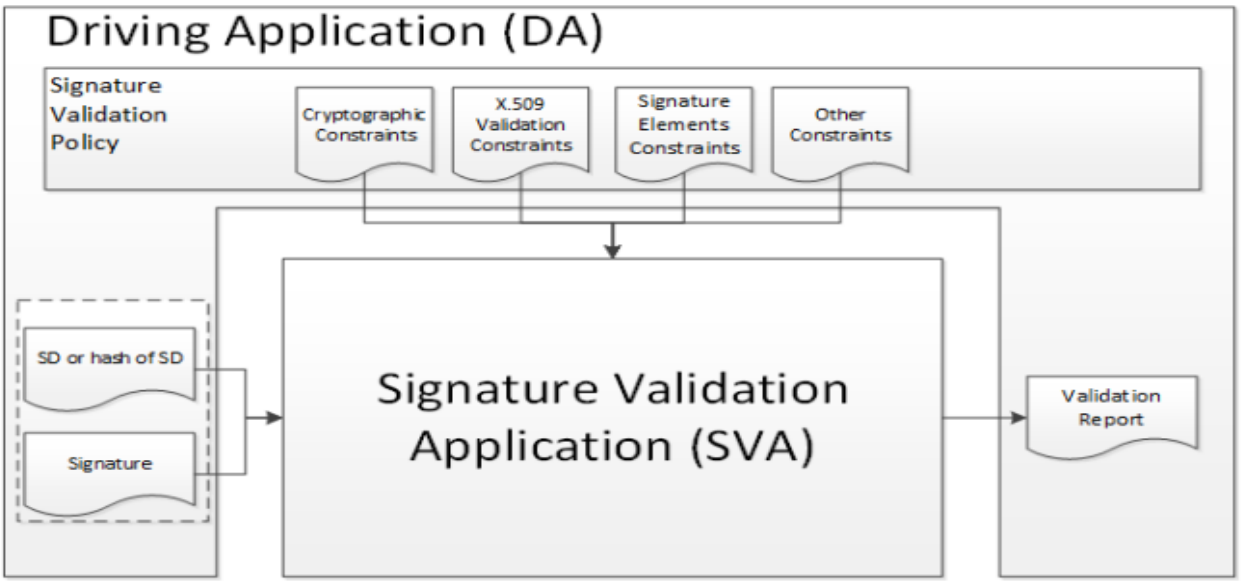

Figure 11: Conceptual Model of Signature Validation

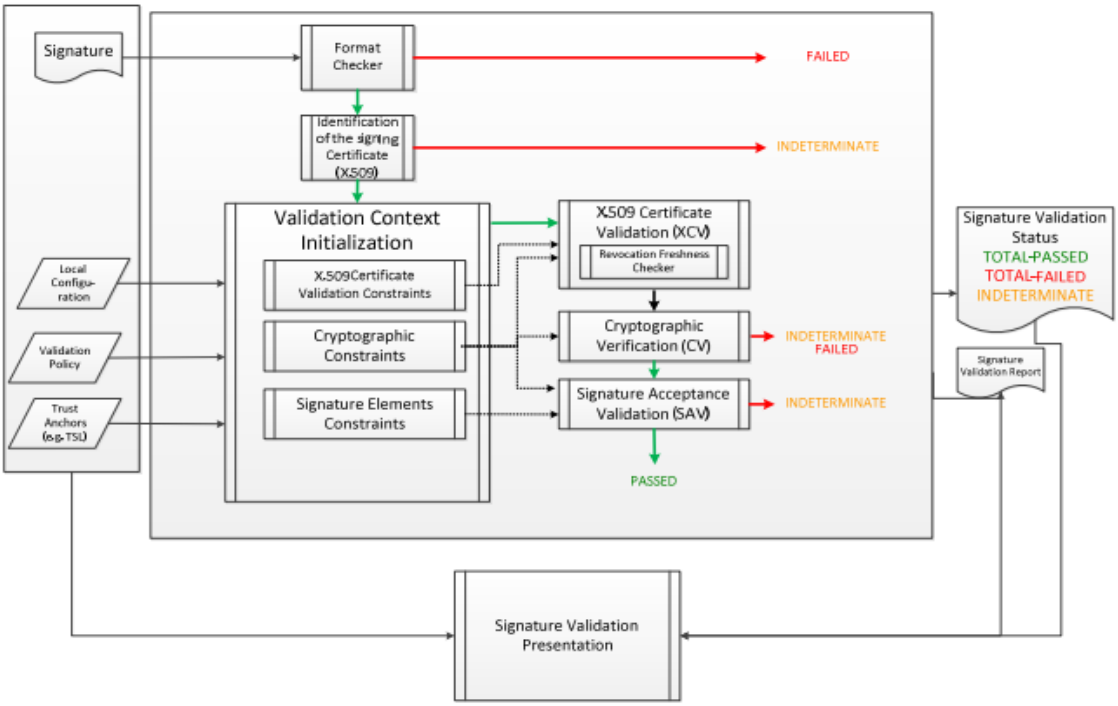

Figure 12: Basic Signature Validation

Ataskaitos autentiškumas patvirtinamas elektroniniu spaudu, papildomai parašą paženklinant kvalifikuota laiko žyma.

9.2. Patikrinimo procesas

Pagal standartą ETSI EN 319 102-1, patikrinus elektroninį parašą, yra pateikiamos trys galimos parašo ar spaudo patikros būsenos:

- TOTAL-PASSED: parašas atitinka nustatytą patikrinimo politiką ir praėjo visas patikrinimo procedūras;
- TOTAL-FAILED: parašo formatas netinkamas arba nepraėjo patikrinimo procedūrų;
- INDETERMINATE: parašo patikrinimas sėkmingas, tačiau trūksta informacijos ar elektroninis parašas tikrai galioja.

Kiekvieno patikrinimo proceso metu yra pateikiama detalizuota informacija, kuria remiantis buvo priskirta parašo būsena.

Patikrinimo procesas vyksta pagal numatytą patikrinimo politiką – patikrinami elektroniniai parašai, ar jie yra pažangieji (AdES), ar parašai patvirtinti kvalifikuotais

sertifikatais (AdES/QC), ar pilnai kvalifikuoti (QES). Visi sertifikatai ir su jais susijusios sertifikatų grandinės yra tikrinamos pagal Europos Sąjungos patikimų tiekėjų sąrašą. Į šį patikrinimą taip pat įeina ir sertifikatų patikra, kurie pasirašomi CRL, OCSP, ir laiko žymos.

Patikrinimo proceso politika gali būti keičiama iš anksto klientui suderinus reikalingus patikrinimo elementus. Visais kitais atvejais naudojama numatytoji patikrinimo politika.

Numatytosios kvalifikuoto patikrinimo politikos pagrindiniai aspektai aprašyti Šiame dokumente ir todėl papildomai neaprašoma jokiame kitame papildomame viešame dokumente.

Tikrinant parašo/laiko žymų sertifikatus, yra atsižvelgiama į ETSI TS 119 172-4 standarte aprašytas procedūras. Testavimo procedūros aprašymas pateikiamas lentelėje Nr. 1.

1 lentelė. Testavimo procedūros aprašymas

Scenarijus	Patikros būsena
Pasirašant dokumentą su kvalifikuotu parašu ir kvalifikuota laiko žyma.	TOTAL_PASSED
Pakeičiant pasirašyto dokumento turinį.	TOTAL_FAILED
Pasirašant dokumentą su nekvalifikuotu el. parašu arba spaudu.	INDETERMINATE

Patikrinimo rezultatas klientui yra pateikiamas:

- per Veriffy API integracinę sąsają. Iš kliento gavus dokumentą patikrinimui, Veriffy sistema atlieka patikrinimą nesaugant dokumento. Po patikros rezultatas yra transformuojamas į žmogaus/kompiuterio skaitomą formatą XML ir/arba PDF, ant rezultato automatizuotai yra uždedamas ISENSE spaudas. Vėliau šis kvalifikuoto patikrinimo rezultatas gali būti naudojamas transformuojant į kitas formas. Šios kvalifikuotos paslaugos ribose yra nežinoma, ką klientas darys su kvalifikuotu patikros atsakymu.

- per Veriffy portalą. Iš kliento gavus dokumentą, Veriffy atlieka patikrinimą. Po patikros rezultatas yra transformuojamas į PDF formatą, ant rezultato automatizuotai yra uždedamas ISENSE spaudas.

9.3. Autentiškumo užtikrinimas

Patikrinus parašus, yra suformuojama XML ir/arba PDF ataskaita pagal standartą ETSI TS 119 102-2. Ataskaita yra pasirašoma šiuo UAB „iSense Technologies“ pažangiuoju spaudu patvirtintu kvalifikuotu sertifikatu.

- Sertifikatas: C=LT, O= iSense Technologies, UAB, CN=Qualified Validation Service powered by Veriffy
- Sertifikatą išdavusi įstaiga: C=LT, OU=RCSC, O=VI Registru centras - i.k. 124110246, CN=RCSC IssuingCA
- Sertifikato serijinis numeris: 70944e6fb3a36b2e00000005848c
- Sertifikato SHA-256 šifras: 72a4a7e72cffef166c4105f6c6d05dca36fd0550

9.4. Kvalifikuotų paslaugų teikimo būdas

Kvalifikuotos paslaugos teikiamos šiais būdais:

- REST API programos integracija (paslaugos API);
- Žiniatinklio taikomoji programa su Naudotojo sąsaja.

10. KVALIFIKUOTŲ PASLAUGŲ BENDRIEJI REALIZACIJOS PRINCIPAI

10.1. Europos sąjungos patikimų tiekėjų sąrašas

Tam, kad kiekviena Europos Sąjungos šalis galėtų keistis patikimų tiekėjų sąrašais, Europos Komisija centralizuotai publikuoja visos Europos Sąjungos šalių patikimų tiekėjų sąrašų publikavimo vietas. Sinchronizuojant patikimų tiekėjų sąrašus, yra patikrinamas šiuose sąrašuose esančios informacijos autentiškumas. Patikimų tiekėjų sąrašuose esanti informacija yra naudojama nustatyti parašo, CRL, OCSP ir laiko žymų sertifikatų kvalifikaciją Europos Sąjungos ribose.

10.2. Duomenys ir srautai

Kvalifikuotos paslaugos klientui teikiamos jį autentifikavus. Klientui yra suteikiamas autentifikacijos raktas. Klientas atsiunčia saugiu HTTPS kanalu elektroninį dokumentą (duomenis), kuriame yra parašai/spaudai, parašo sertifikatai, sertifikato viešieji raktai. Toliau atliekamas dokumento apdorojimas pagal pasirinktą kvalifikuotą paslaugą - tikrinimas, paruošimas ilgalaikiam saugojimui. Siekiant sumažinti riziką, dokumentas saugomas tik tiek laiko, kiek reikia atlikti tam tikrą kvalifikuotą paslaugą.

Kvalifikuoto patikrinimo metu – gavus dokumentą ir parašus, yra tikrinama, ar dokumentas nebuvo pakeistas po pasirašymo, ar tikrai yra pasirašytos tos dalys, kurios yra deklaruojamos. Tikrinami pasirašiusio asmens sertifikatai. Šių patikrų metu gali būti kreipiamasi į sertifikatą išdavusią įstaigą, perduodant sertifikato identifikacinius numerius.

Sertifikatų patikimumas yra tikrinamas pagal iš anksto sinchronizuotą (vieną kartą paroje) visos Europos patikimų tiekėjų sąrašą. Sertifikato patikrinimai vyksta pagal parašo sertifikate esančią informaciją apie išdavusią įstaigą.

Elektroninis dokumentas ir jo turinys gali būti visiškai bet koks, ir mums iš anksto nežinomas. Tikrinimo metu su duomenimis automatizuotai būna atliekamos kriptografinės maišos skaičiavimo operacijos (angl. *hash*) patikrinimui, ar nebuvo pakeisti duomenys.

Elektroniniuose parašuose yra saugoma pasirašiusios šalies sertifikato informacija ir jo viešas raktas. Sertifikate gali būti nurodytas asmens vardas, pavardė, pareigos, slapyvardis, sertifikato identifikacinis numeris, asmens kodas ir pan. Šią informaciją į sertifikatus įrašo juos išduodanti įstaiga. Kiekviena sertifikatus išduodanti įstaiga įrašo skirtingą informaciją, ir ji priklauso nuo šalyje paplitusios praktikos, sertifikato profilių ir pan.

Kuriant kvalifikuoto patikrinimo ataskaitą, ji yra pasirašoma ISENSE pažangiuoju elektroniniu spaudu. Spaudo sertifikato privatus raktas yra saugomas ribotos prieigos

programinėje įrangoje. Kiekvienas el. spaudo privataus rakto panaudojimo atvejis yra fiksuojamas ir audituojamas.

Visos operacijos ir kreipiniai (iš Kliento į Veriffy informacinę sistemą) yra audituojami ir saugomi duomenų bazėje, siejant su kliento raktu.