



# **UAB „NEVDA“ VEIKLOS NUOSTATAI TEIKIANT KVALIFIQUOTAS PASLAUGAS**

**versija 1.4**

**(OID) - 1.3.6.1.4.1.57583.1.1**

**Galioja nuo 2022 01 01**

## Turinys

1. ĮVADAS .....	4
1.1 APŽVALGA .....	4
1.2 DOKUMENTO PAKEITIMAI IR TVIRTINIMAS .....	4
1.3 NAUDOJAMOS SĄVOKOS, SUTRUMPINIMAI .....	5
1.4 IDENTIFIKAVIMAS .....	7
1.5 PANAUDOTŲ DOKUMENTŲ SĄRAŠAS .....	7
1.6 KPC VEIKLOS NUOSTATUS IŠLEIDUSI IR TVARKANTI ORGANIZACIJA .....	8
1.7 KONTAKTINIAI ASMENYS .....	8
1.8 INFORMACIJA APIE KVALIFIKUOTAS PASLAUGAS .....	8
2. BENDROSIOS NUOSTATOS .....	8
2.1 ATSAKOMYBĖ .....	8
2.1.1 VEIKLOS ATSAKOMYBĖ .....	8
2.1.2 FINANSINĖ ATSAKOMYBĖ .....	9
2.2 TEISINĖS NUOSTATOS IR INTERPRETAVIMAS .....	9
2.2.1 KVALIFIKUOTO ELEKTRONINIO PARAŠO IR ANTSPAUDO TEISINĖ GALIA .....	9
2.2.2 PAGRINDINIAI TEISĖS AKTAI .....	9
2.2.3 GINČŲ SPRENDIMO TVARKA .....	9
2.3 KVALIFIKUOTŲ PASLAUGŲ TEIKIMO ĮKAINIAI .....	9
2.4 KLIENTŲ APTARNAVIMO TVARKA .....	9
2.5 INFORMACIJOS TEIKIMAS .....	10
2.5.1 INFORMACIJOS TEIKIMAS PRIEŽIŪROS ĮSTAIGAI .....	10
2.5.2 NEVDA VIEŠAI TEIKIAMA INFORMACIJA .....	10
2.5.3 TEIKIAMOS INFORMACIJOS ATNAUJINIMO DAŽNUMAS .....	10
2.6 ATITIKTIES TIKRINIMAS .....	10
2.7 KONFIDENCIALUMO NUOSTATOS .....	11
2.7.1 ASMENS DUOMENYS .....	11
2.7.2 SLAPTA INFORMACIJA .....	11
2.7.3 NESLAPTA INFORMACIJA .....	11
2.7.4 INFORMACIJOS APSAUGA .....	11
2.7.5 INFORMACIJOS TEIKIMAS TEISĖSAUGAI .....	11
3. REIKALAVIMAI KVALIFIKUOTŲ PASLAUGŲ TEIKIMUI .....	12
3.1 REIKALAVIMAI QVAL FOR QESIG IR QVAL FOR QSEAL PASLAUGŲ TEIKIMUI .....	12
3.2 ĮRAŠŲ APIE KVALIFIKUOTŲ PASLAUGŲ TEIKIMĄ RINKIMAS IR SAUGOJIMAS .....	12
3.2.1 REGISTRUOJAMI ĮVYKIAI .....	12
3.2.2 ĮRAŠŲ APIE ĮVYKIUS PERŽIŪROS DAŽNUMAS .....	13
3.2.3 ĮRAŠŲ SAUGOJIMO PERIODAS .....	13

3.2.4 ĮRAŠŲ APSAUGA.....	13
3.3 DUOMENŲ ARCHYVAVIMAS .....	13
3.3.1 Į ARCHYVĄ ATIDUODAMI DUOMENYS.....	13
3.3.2 DUOMENŲ SAUGOJIMO ARCHYVE PERIODAS.....	13
3.3.3 ATSARGINIŲ KOPIJŲ DARYMAS .....	13
3.4 SAUGUMO INCIDENTAI IR JŪ VALDYMAS.....	13
3.4.1 INCIDENTŲ REGISTRAVIMO, IDENTIFIKAVIMO BEI ANALIZĖS PROCEDŪRA.....	14
3.5 PATIKIMUMO UŽTIKRINIMO PASLAUGŲ TEIKIMO NUTRAUKIMAS .....	14
3.6 TREČIŲJŲ ŠALIŲ NAUDOJAMI SPRENDIMAI IR PASLAUGOS.....	15
3.7 BENDRI REIKALAVIMAI KVALIFIQUOTAM PASLAUGŲ TIEKĖJUI.....	15
4. FIZINIO, PROCEDŪRINIO IR PERSONALO SAUGUMO KONTROLĖ.....	15
4.1 FIZINIO SAUGUMO KONTROLĖ.....	15
4.1.1 BUVEINĖS VIETA.....	15
4.1.2 FIZINĖ PRIEIGA .....	16
4.1.3 ELEKTROS ENERGIOS TIEKIMAS IR ORO KONDICIONAVIMAS.....	16
4.1.4 APSAUGA NUO UŽPYLIMO VANDENIU.....	16
4.1.5 PRIEŠGAISRINĖ APSAUGA .....	16
4.1.6 NAUDOJAMŲ KRIPTOGRAFINIŲ RAKTŲ APSAUGA.....	16
4.1.7 INFORMACIJOS LAIKMENŲ SAUGOJIMAS .....	16
4.1.8 LAIKMENŲ NAIKINIMAS.....	16
4.2 PROCEDŪRINIO SAUGUMO KONTROLĖ.....	16
4.2.1 DARBUOTOJŲ PAREIGOS.....	16
4.2.2 PAREIGŲ IDENTIFIKACIJA IR AUTENTIŠKUMO TIKRINIMAS.....	17
4.3 PERSONALO PATIKIMUMO KONTROLĖ .....	17
4.3.1 KVALIFIKACINIAI REIKALAVIMAI .....	17
4.3.2 REIKALAVIMAI SAMDOMIEMS ASMENIMS.....	17
5. TECHNINĖ REALIZACIJA.....	17
5.1 KVALIFIQUOTOS PASLAUGOS PARAŠAMS/SPAUDAMS REALIZACIJA.....	17
5.1.1 KVALIFIQUOTOS PASLAUGOS PATIKRINIMO PROCESAS .....	19
5.1.2 PATIKRINIMO ATASKAITOS AUTENTIŠKUMAS .....	20
5.1.3 KVALIFIQUOTO PASLAUGOS TEIKIMO BŪDAS.....	20
5.2 KVALIFIQUOTŲ PASLAUGŲ TEIKIMO BENDRIEJI REALIZACIJOS PRINCIPAI .....	20
5.2.1 EUROPOS SĄJUNGOS PATIKIMŲ TIEKĖJŲ SĄRAŠAS .....	20
5.2.2 KOMUNIKACIJOS KANALAI.....	20
5.2.3 AUTENTIFIKACIJA.....	20
5.3 DUOMENYS IR SRAUTAI .....	20

## 1 ĮVADAS

NEVDA pagrindinė veikla – informacinių sistemų kūrimas, diegimas ir priežiūra viešojo sektoriaus organizacijoms ir verslo bendrovėms.

2021 UAB „Nevda“ įkūrė NEVDA Kvalifikuotų paslaugų centrą (toliau – KPC) – kvalifikuotų patikimumo užtikrinimo paslaugų, teikimui.

### 1.1 APŽVALGA

Šis dokumentas detaliai apibrėžia NEVDA ir KPC veiklą teikiant Kvalifikuotas patikimumo užtikrinimo 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 PAKEITIMAI IR TVIRTINIMAS

Dokumentų keitimo sąrašas:

Versija	Data	Apaščymas
1.1	2021-04-14	Parengta pradinė dokumento versija
1.2	2021-05-20	Papildyta versija skirta peržiūrai ir analizei
1.3	2021-09-08	Versija skirta audito peržiūrai
1.4	2021-09-10	Versija po audito pastabų skirta RRT
1.5		Galutinė versija

Paskutinės versijos dokumento tvirtinimas

Versija	Data	Tvirtinino
1.4	2021-09-10	NEVDA direktoriaus pavaduotojas Paulius Jonika

### 1.3 NAUDOJAMOS SĄVOKOS, SUTRUMPINIMAI

Sąvokų trumpiniai	Apašymas
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
Elpako	NEVDA valdoma informacinė sistema skirta Kvalifikuotoms paslaugoms teikti
NEVDA	UAB „Nevda“
KPC	NEVDA veiklos padalinys atsakingas už Kvalifikuotų paslaugų teikimą
KPC veiklos nuostatai	Šis dokumentas aprašantis KPC veiklą teikiant Kvalifikuotas paslaugas
Klientas	Juridinis arba fizinis asmuo pasirašęs sutartį su NEVDA dėl Kvalifikuotų paslaugų teikimo
TSL	Patikimumas sąrašas (angl. Trusted Services List)
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 kity elektroninės formos duomenų arba logiškai susieti su jais ir kuriuos pasirašantis asmuo naudoja pasirašydamas
Elektroninis spaudas	Elektroninės formos duomenys, prijungti prie kity 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 spudo kūrimo įtaisą ir patvirtintas kvalifikuotu elektroninio spudo sertifikatu
Laiko žymos paslaugų teikėjas	(TSA – Time-Stamping Authority) – patikumo 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	<b>NEVDA INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI</b>
Naudotojų administravimo taisyklos	<b>NEVDA INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS</b>
Informacijos tvarkymo taisyklos	<b>NEVDA INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS</b>
Veiklos tēstinumo planas	<b>NEVDA INFORMACINĖS SISTEMOS VEIKLOS TĒSTINUO VALDYMO PLANAS</b>
Incidentų valdymo taisyklos	<b>NEVDA INFORMACINIŲ SAUGOS INCIDENTŲ VALDYMO TAISYKLĖS</b>
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 nustatytais reikalavimais
Kvalifikuoto elektroninio parašo sertifikatas	Elektroninio parašo sertifikatas, kurį išduoda kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas ir kuris atitinka eIDAS reglamento I priede nustatytais reikalavimais
ETSI	Europos telekomunikacijų standartizavimo institutas (European Telecommunication Standardisation Institute)
OID	Unikalus objekto identifikatorius (Object Identifier)
PIN	Asmens identifikacinis skaičius (Personal Identification Number)
PKI	Viešojo rako infrastruktūra (Public Key Infrastructure)
OCSP	Sertifikato galiojimo patvirtinimas, atitinkantis RFC 6960 rekomendacijas
CRL	Sertifikato galiojimo patvirtinimas, atitinkantis RFC 5280 rekomendacijas
Saugykla	KPC informacijos duomenų bazė, naudotojams prieinama tiesiogiai (on-line) bet kuriuo metu internte adreso <a href="http://www.elpako.eu">www.elpako.eu</a>

Kitos šiame dokumente naudojamos sąvokos ir sutrumpinimai suprantami taip, kaip apibrėžta 2014 m. liepos 23 d. 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/EB.

## 1.4 IDENTIFIKAVIMAS

KPC veiklos nuostatai skelbiami Saugykloje.

Unikalus KPC veiklos nuostatų identifikatorius (OID) - 1.3.6.1.4.1.57583.1.1

Pavadinimas	Reikšmė
ISO	1
ISO pripažinta organizacija	3
JAV Gyvybos departamentas	6
Internetas	1
Privati įmonė	4
IANA registratoriaus privati įmonė	1
NEVDA	57583
NEVDA padalinys KPC	1
KPC veiklos nuostatų dokumentas	1

## 1.5 PANAUDOTŲ DOKUMENTŲ SĄRAŠAS

Kvalifikuotų paslaugų kūrimas bei paslaugų teikimas remiasi šiais dokumentais:

- 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 tokų 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 sgrašo 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 v2.3.0 : General Policy Requirements for Trust Service Providers;

## 1.6 KPC VEIKLOS NUOSTATUS IŠLEIDUSI IR TVARKANTI ORGANIZACIJA

UAB „Nevda“

Įmonės kodas: 121931451

Adresas: Savanorių pr. 178F 03154 Vilnius

Internetinės svetainės adresas: [www.nevda.lt](http://www.nevda.lt)

E.pašto adresas: [info@nevda.lt](mailto:info@nevda.lt)

## 1.7 KONTAKTINIAI ASMENYS

Informaciją, visais klausimais susijusiais su šiuo dokumentu ir kvalifikuotomis paslaugomis, teikia NEVDA KPC padalinys.

Kreiptis el. paštu: [eidas@elpako.lt](mailto:eidas@elpako.lt)

## 1.8 INFORMACIJA APIE KVALIFIQUOTAS PASLAUGAS

Informacija apie kvalifikuotas paslaugas teikiama adresu <https://elpako.lt/teisine-informacija/>

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

NEVDA garantuoja Saugyklos prieinamumą 99,99% laiko.

## 2 BENDROSIOS NUOSTATOS

### 2.1 ATSAKOMYBĖ

NEVDA 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.

### 2.1.1 VEIKLOS ATSAKOMYBĖ

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

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

NEVDA neatsako už Klientų sistemoje atsiradusius gedimus, trikdžius, dėl kurių galimai sutriko teikiamų paslaugų teikimas, kokybė bei prieinamumas

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

## 2.1.2 FINANSINĖ ATSAKOMYBĖ

Finansinės atsakomybės įsipareigojimams užtikrinti NEVDA 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

- Kvalikuoto elektroninio parašo teisinė galia yra lygiavertė rašytiniams parašui. Kvalikuotas elektroninis parašas, patvirtintas vienoje valstybėje narėje išduotu kvalikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kaip kvalikuotas elektroninis parašas;
- Kvalikuotam elektroniniams spaudui taikoma prezumpcija dėl duomenų, su kuriais susietas kvalikuotas elektroninis spaudas, vientisumo ir tų duomenų kilmės tinkamumo. Kvalikuotas elektroninis spaudas, patvirtintas vienoje valstybėje narėje išduotu kvalikuotu sertifikatu, visose kitose valstybėse narėse pripažįstamas kvalikuotu elektroniniu spaudu.

### 2.2.2 PAGRINDINIAI TEISĖS AKTAI

Kvalikuotų paslaugų dalyvių teises ir atsakomybę, reikalavimus Kvalikuotų paslaugų teikėjams bei jų atsakomybę nustato šio dokumento 1.5 p. nurodyti teisės aktais

### 2.2.3 GINČŲ SPRENDIMO TVARKA

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

## 2.3 KVALIFIKUOTŲ PASLAUGŲ TEIKIMO ĮKAINIAI

Kvalikuotų paslaugų teikimo įkainiai viešai skelbiami adresu <https://elpako.lt/teisine-informacija/>

## 2.4 KLIENTŲ APTARNAVIMO TVARKA

- klientas klausimus, abejones ar skundus dėl Kvalikuotų Paslaugų teikimo sąlygų, gali pateikti mūsų klientų aptarnavimo komandai el. paštu [pagalba@elpako.lt](mailto:pagalba@elpako.lt) arba interneto svetainėje <https://elpako.lt/kontaktai/> užklausos formoje. Atsakysime į kliento pateiktą užklausą ne vėliau kaip per 5 kalendorines dienas.
- klientas, nepatenkintas teikiamų Kvalikuotų paslaugų kokybe, papildomai gali pateikti skundą Lietuvos Respublikos ryšių reguliavimo tarnybai el. paštu [rrt@rrt.lt](mailto:rrt@rrt.lt) (interneto

svetainė <https://www.rrt.lt>), arba Valstybinei vartotojų teisių apsaugos tarnybai el. paštu [tarnyba@vvtat.lt](mailto:tarnyba@vvtat.lt).

## 2.5 INFORMACIJOS TEIKIMAS

### 2.5.1 INFORMACIJOS TEIKIMAS PRIEŽIŪROS ĮSTAIGAI

- NEVDA 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.

### 2.5.2 NEVDA VIEŠAI TEIKIAMA INFORMACIJA

NEVDA viešai teikiama informacija sudaro:

- informacija apie Kvalifikuotų paslaugų teikimo statusą;
- Kvalifikuotų paslaugų sudarymo ir tvarkymo sąlygos;
- Kvalifikuotų paslaugų kainoraščiai;
- instrukcijos vartotojams;
- įgaliotų institucijų parengtos NEVDA veiklos tikrinimo ataskaitų santraukos;
- kita jvairi organizacinės paskirties ar patikimų veiklų įrodanti informacija susijusi su Kvalifikuotų paslaugų teikimu:
  - neprilausomo NEVDA veiklos audito išvados;
  - jvairūs skelbimai susiję su teikiamamis Kvalifikuotomis paslaugomis.

### 2.5.3 TEIKIAMOS INFORMACIJOS ATNAUJINIMO DAŽNUMAS

NEVDA teikiama informacija atnaujinama tokiu laiku ar dažnumu:

- pakeitimai daromi, tvirtinami ir skelbiami taip, kaip numatyta Duomenų saugos nuostatuose;
- kita skelbtina ir atnaujinta informacija (pvz., NEVDA veiklos tikrinimo išvados, kt.) skelbiama ją gavus ar parengus per protinį terminą

## 2.6 ATITIKTIES TIKRINIMAS

NEVDA veiklos atitiktis tinkamai teikiti Kvalifikuotas paslaugas, atliekama:

- vadovaujantis eIDAS 20 str. 1 d. atitikties vertinimo įstaiga kas 24 (dvidešimt keturis) mėnesius atlieka NEVDA auditą;
- vadovaujantis eIDAS 20 str. 2 d., priežiūros įstaiga bet kuriuo metu gali atliskti NEVDA auditą arba reikalauti, kad atitikties įstaiga atliskytų NEVDA vertinimą (NEVDA lėšomis), siekiant patvirtinti, kad teikiamas paslaugos atitinka eIDAS nustatytus reikalavimus;
- vadovaujantis eIDAS 20 str. 3 d., kai priežiūros įstaiga reikalauja, kad NEVDA ištaisytų bet kuriuos eIDAS reikalavimų pažeidimus ir NEVDA to nepadaro per priežiūros įstaigos nustatyta laikotarpi, priežiūros įstaiga, atsižvelgdama visų pirma į tokį pažeidimų mastą, trukmę ir pasekmes, gali panaikinti NEVDA arba pažeidimo paveikty NEVDA teikiamu

paslaugų kvalifikacijos statusą ir pranešti apie tai eIDAS 20 str. 3 d. nurodytai įstaigai, kad būty galima atnaujinti patikimus sąrašus;

## 2.7 KONFIDENCIALUMO NUOSTATOS

### 2.7.1 ASMENS DUOMENYS

- NEVDA privalo tvarkyti asmens duomenis vadovaudamasi Bendrojo asmens duomenų apsaugos reglamento bei Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, kuris įgyvendina 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvą 95/46/EB dėl asmens apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kiek jis neprieštarauja Bendrajam asmens duomenų apsaugos reglamentui. Asmens duomenys saugomi tinkamą, reikiama laikotarpį (įskaitant NEVDA nutraukus veiklą), bet ne ilgiau nei to reikia duomenų tvarkymo tikslais, apie kurį asmuo yra informuojamas, kad duomenis būty galima panaudoti teismo procese bei taip būty užtikrinamas veiklos tēstinumas;
- kai asmens duomenys neberekalingi jų tvarkymo tikslams, jie yra sunaikinami, išskyrus tuos, kurie įstatymu nustatytais atvejais turi būti perduodami valstybės archyvams.

### 2.7.2 SLAPTA INFORMACIJA

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

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

### 2.7.3 NESLAPTA INFORMACIJA

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

### 2.7.4 INFORMACIJOS APSAUGA

- Siekiant apsaugoti saugomus įrašus nuo vagystės ar klastojimo, NEVDA imasi prevencinių priemonių, susijusių su tinkama bei efektyvia fizinio, techninio, procedūrinio saugumo bei personalo patikimumo kontrole;
- įrašai saugomi patikimose sistemoje taip, kad būty galima patikrinti jų tikrumą, o įrašus bei pakeitimius galėtų daryti tik NEVDA įgalioti asmenys.

### 2.7.5 INFORMACIJOS TEIKIMAS TEISÉSAUGAI

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

### 3 REIKALAVIMAI KVALIFIKUOTŲ PASLAUGŲ TEIKIMUI

Šiame skyriuje apibrėžiami reikalavimai NEVDA veiklai teikiant kvalifikuotas paslaugas.

#### 3.1 REIKALAVIMAI QVAL FOR QESIG IR QVAL FOR QSEAL PASLAUGŲ TEIKIMUI

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;
- kvalifikuotų sertifikatų išdavė kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas, ir jis galiojo pasirašymo metu;
- parašo patvirtinimo duomenys atitinka pasikliaujančiajai šalimai pateiktus duomenis;
- unikalus duomenų, kuriais sertifikate nurodomas pasirašantis asmuo, rinkinys tinkamai pateikiamas pasikliaujančiajai šalimai;
- jei pasirašymo metu buvo naudojamas slapyvardis, tai aiškiai nurodoma pasikliaujančiajai šalimai;
- 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 šalimai teisingą galiojimo patvirtinimo procedūros rezultatą ir leidžia pasikliaujančiai šalimai 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*.

#### 3.2 ĮRAŠŲ APIE KVALIFIKUOTŲ PASLAUGŲ TEIKIMĄ RINKIMAS IR SAUGOJIMAS

##### 3.2.1 REGISTRUOJAMI ĮVYKIAI

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

- kvalifikuotos paslaugos tipas patikrinimas;
- laikas ir data;
- unikalus kliento identifikatorius;
- unikalus užklausos identifikatorius;
- loginė reikšmė ar paslauga sékmingai 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 fiksujami detalūs sistemų veiksmai, kurie naudojami sistemų veikimo analizei, diagnostikai ir sutrikimų šalinimui. Pagrindiniai diagnostikos žurnalo naudotojai – sistemų kūrėjai ir administratoriai. Klaidų žurnale (Error Log) fiksujama informacija apie sistemų sutrikimus ir klaidas, nurodant sutrikimo laiką, šaltinį, aprašymą ir detalią informaciją.

### 3.2.2 ĮRAŠŲ APIE ĮVYKIUS PERŽIŪROS DAŽNUMAS

NEVDA 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 žurnaluose elektroninės informacijos, susijusios su informacinių sistemų naudotojų ir informacinių sistemų administratorių atliekamais veiksmais, žurnalai peržiūrimi Duomenų saugos nuostatuose nustatytais terminais bei tvarka.

### 3.2.3 ĮRAŠŲ SAUGOJIMO PERIODAS

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

### 3.2.4 ĮRAŠŲ APSAUGA

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

## 3.3 DUOMENŲ ARCHYVAVIMAS

### 3.3.1 Į ARCHYVĄ ATIDUODAMI DUOMENYS

Į archyvą atiduodama:

- sistemos operacijų ir veiklos registravimo žurnalai;

### 3.3.2 DUOMENŲ SAUGOJIMO ARCHYVE PERIODAS

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

### 3.3.3 ATSARGINIŲ KOPIJŲ DARYMAS

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

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

## 3.4 SAUGUMO INCIDENTAI IR JŲ VALDYMAS

Incidentai klasifikuojami ir valdomi pagal NEVDA patvirtintus dokumentus:

- incidentų klasifikavimas aprašytas Incidentų valdymo dokumente;

- kritinių saugos incidentų valdymas aprašytas Veiklos tēstinumo planas.

### 3.4.1 INCIDENTŲ REGISTRAVIMO, IDENTIFIKAVIMO BEI ANALIZĖS PROCEDŪRA

NEVDA vadovaujasi tokia tvarka:

- 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 netycinio 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;
- registravus 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. Nuostacių, 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 tēstinumo plane numatyta darbo grupę. Apie minėtus 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 užregistruoto pažeidimo, turėjusio didelj poveikį, suvaldymo ar pasibaigimo informuoja priežiūros tarnybą pateikdama nustatytos formos pranešimą.

### 3.5 PATIKIMUMO UŽTIKRINIMO PASLAUGŲ TEIKIMO NUTRAUKIMAS

NEVDA, 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 numatyta paslaugų nutraukimo datą, tačiau ne vėliau kaip prieš 2 (du) mėnesius, priežiūros įstaigai pateikia:
  - informaciją apie veiklos perėmėją;
  - veiklos perėmimo sutartį;
  - detaliųj Kvalifikuotų paslaugų teikimo veiklos nutraukimo planą.
- jei nusprendus nutraukti Kvalifikuotų paslaugų teikimą, veikla nėra perduodama trečiajai šaliai, NEVDA turi užtikrinti veiklos įrašą išsaugojimą.

### 3.6 TREČIŲJŲ ŠALIŲ NAUDOJAMI SPRENDIMAI IR PASLAUGOS

NEVDA, 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 NEVDA nustatytas būtinės informacijos saugos lygis.

Kvalifikuotų paslaugų teikimui naudojamos Microsoft Azure siūlomi sprendimai ir paslaugos

Kas	Fizinė vieta	Saugumo užtikrinimas
Produkcinė aplikacija	„Microsoft Azure“ duomenų centras, šiaurės Europos regionas. PaaS paslauga „App service“	Microsoft valdomi duomenų centrai atitinka visus modernius saugomo standartus ( <a href="https://docs.microsoft.com/en-us/azure/compliance">https://docs.microsoft.com/en-us/azure/compliance</a> ). Prieigos teisės ribotos.
Produkcinė duomenų bazė	„Microsoft Azure“ duomenų centras, šiaurės Europos regionas. „Microsoft SQL Server“	Microsoft valdomi duomenų centrai atitinka visus modernius saugomo standartus ( <a href="https://docs.microsoft.com/en-us/azure/compliance">https://docs.microsoft.com/en-us/azure/compliance</a> ). Prieigos teisės ribotas. Ugniasienė riboja prieigą tik iš produkcinės aplikacijos ir iš NEVDA vidinio tinklo.
NEVDA pažangusis spaudas	„Microsoft Azure“ duomenų centras, šiaurės Europos regionas. Raktų saugyklos paslauga „Azure KeyVault“	Microsoft valdomi duomenų centrai atitinka visus modernius saugomo standartus ( <a href="https://docs.microsoft.com/en-us/azure/compliance">https://docs.microsoft.com/en-us/azure/compliance</a> ). Azure KeyVault paslaugoje laikomo įmonės spaudo sertifikato visos operacijos yra audituojamos. Prieiga ribojama.

### 3.7 BENDRI REIKALAVIMAI KVALIFIQUOTAM PASLAUGŲ TIEKĖJUI

Bendri kvalifikuotų tiekėjų reikalavimai yra aprašyti [ETSI EN 319 401](#) standarte.

## 4 FIZINIO, PROCEDŪRINIO IR PERSONALO SAUGUMO KONTROLĖ

### 4.1 FIZINIO SAUGUMO KONTROLĖ

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

#### 4.1.1 BUVEINĖS VIETA

Savanorių pr. 178F, 03154 Vilnius, Lithuania

#### 4.1.2 FIZINĖ PRIEIGA

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

#### 4.1.3 ELEKTROS ENERGIOS TIEKIMAS IR ORO KONDICIONAVIMAS

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

#### 4.1.4 APSAUGA NUO UŽPYLIMO VANDENIU

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

#### 4.1.5 PRIEŠGAISRINĖ APSAUGA

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

#### 4.1.6 NAUDOJAMŲ KRIPTOGRAFINIŲ RAKTŲ APSAUGA.

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

#### 4.1.7 INFORMACIJOS LAIKMENŲ SAUGOJIMAS

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

#### 4.1.8 LAIKMENŲ NAIKINIMAS

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

### 4.2 PROCEDŪRINIO SAUGUMO KONTROLĖ

#### 4.2.1 DARBUOTOJŲ PAREIGOS

Pareigybės, nuo kurių priklauso KPC veikla yra:

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

## 4.2.2 PAREIGŲ IDENTIFIKACIJA IR AUTENTIŠKUMO TIKRINIMAS

KPC darbuotojų pareigų identifikacija ir autentiškumo tikrinimas atliekami tokiais būdais:

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

## 4.3 PERSONALO PATIKIMUMO KONTROLĖ

### 4.3.1 KVALIFIKACINIAI REIKALAVIMAI

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:

- mokėti lietuvių kalbą;
- turėti reikalingą išsilavinimą arba kvalifikaciją;
- mokėti dirbti kompiuteriu ir kita organizacine technika;
- mokėti užsienio kalbą (jeigu reikalinga).

Be minėtų bendrų reikalavimų garantuojama, kad KPC 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 konfencialios informacijos apsauga, susipažinę su saugos dokumentais bei yra pasirašę pasižadėjimą dėl konfencialios informacijos saugojimo jog yra susipažinę su saugos dokumentais.
- neturi neišnykusio ar nepanaikinto teistumo už tyčinių nusikaltimų padarymą.

### 4.3.2 REIKALAVIMAI SAMDOMIEMIS ASMENIMS

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

## 5 TECHNINĖ REALIZACIJA

### 5.1 KVALIFIUOTOS PASLAUGOS PARAŠAMS/SPAUDAMS REALIZACIJA

Kvalifiuotos paslaugos rezultatas – ataskaita apie elektroninius parašus antspauduota NEVDA pažangiuoju elektroniniu spaudu. Kvalifiuotos paslaugos ataskaitos pateikimo formatas: XML ataskaita pagal standartą ETSI TS 119 102-2. Ataskaitos autentiškumas patvirtinamas elektroniniu spaudu.

Elpako 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)

### Paslaugos veikimo schema:



Principinės paslaugos veikimo schemas pagal ETSI TS 119 102-1 standartą pateikiamos schemose:

30

ETSI TS 119 102-1 V1.2.1 (2018-08)

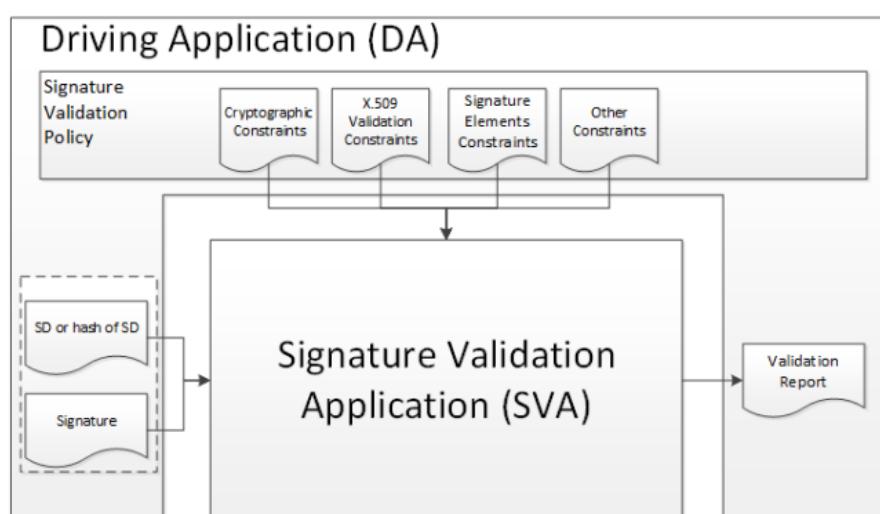


Figure 11: Conceptual Model of Signature Validation

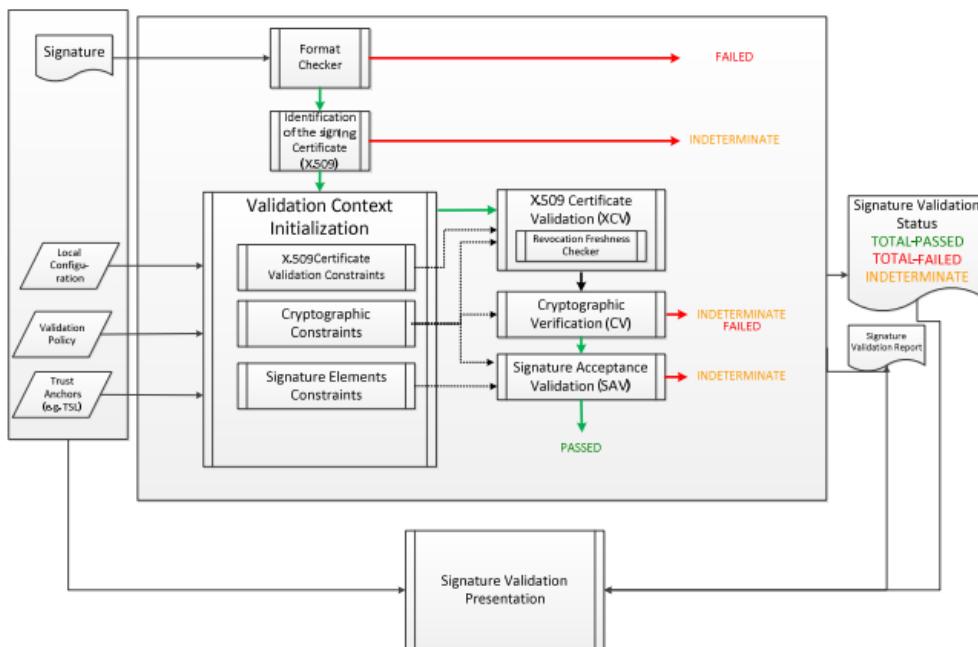


Figure 12: Basic Signature Validation

### 5.1.1 KVALIFIKUOTOS PASLAUGOS PATIKRINIMO PROCESAS

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

- TOTAL-PASSED: parašas atitinka nustatyta patikrinimo politiką ir praėjo visas patikrinimo procedūras;
- TOTAL-FAILED: parašo formatas netinkamas arba nepraejo patikrinimo procedūry;
- 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 numatyta 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. Iš šių patikrinimų taip pat jeina 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.

Numatytojos kvalifikuoto patikrinimo politikos unikalus identifikatorius yra žymimas šiuo žymeniu: 1.3.6.1.4.1.57583.1.1

Tikrinant parašo/laiko žymų sertifikatus yra atsižvelgiama į ETSI TS 119 172-4 standarte aprašytas procedūras. Kvalifikuoto patikrinimo testai yra prieinami šioje [nuorodoje](#).

Patikrinimo rezultatas klientui yra pateikiamas per Elpako API integracinię sąsają. Iš kliento gavus dokumentą patikrinimui, Elpako sistema atlieka patikrinimą nesaugant dokumento. Po patikros rezultatas yra transformuojamas į žmogaus/kompiuterio skaitomą formatą XML ir ant rezultato automatizuotai yra uždedamas NEVDA spaudas. Vėliau šis kvalifikuoto patikrinimo rezultatas gali būti naudojamas transformuojant į kitas formos. Šios kvalifikuotos paslaugos ribose

yra nežinoma, ką klientas darys su kvalifikuotu patikros atsakymu.

### 5.1.2 PATIKRINIMO ATASKAITOS AUTENTIŠKUMAS

Patikrinus parašus yra suformuojama XML ataskaita pagal standartą ETSI TS 119 102-2. Ataskaita yra pasirašoma šiuo NEVDA pažangiuoju spaudu patvirtintu kvalifikuotu sertifikatu.

Sertifikatas: E=info@nevda.lt, C=LT, CN=UAB „NEVDA“, SERIALNUMBER=121931451

Sertifikatą išdavusi įstaiga: C=LT, OU=RCSC, O=VI Registrų centras - i.k. 124110246, CN=RCSC IssuingCA

Sertifikato serijinis numeris: 70944e6fb3a36b2e000000038002

Sertifikato SHA-1 šifras (thumbrint):  
9DB02F1970714EE4CD623F380ACBA8C4BF8245AE

### 5.1.3 KVALIFIKUOTO PASLAUGOS TEIKIMO BŪDAS

Kvalifikuotos paslaugos teikiamos per integracinię sąsają (ang. API). Integracinių sąsajos užklausos pavyzdžiai yra nurodyti šioje [nuorodoje](#).

## 5.2 KVALIFIKUOTŲ PASLAUGŲ TEIKIMO BENDRIEJI REALIZACIJOS PRINCIPAI

### 5.2.1 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. Sinchronizujant patikimų tiekėjų sąrašus, yra patikrinamas šiuose sąrašuose esančios informacijos autentišumas. Patikimų tiekėjų sąrašuose esanti informacija yra naudojama nustatyti parašo, CRL, OCSP ir laiko žymų sertifikatų kvalifikaciją Europos Sąjungos ribose.

### 5.2.2 KOMUNIKACIJOS KANALAI

Komunikacijai tarp kliento ir kvalifikuotos paslaugos visada yra naudojamas saugus šifruotas HTTPS TLS kanalas. Taip yra užtikrinamas perduodamų duomenų konfidentialumas. Visos kliento užklausos yra autentifikuojamos pagal klientui suteiktą raktą.

Komunikacija tarp kvalifikuotos paslaugos ir išorinių patikimų sistemų (laiko žymos, sertifikavimo centrai) yra vykdoma pagal protokolus kuriuos skelbia išoriniai patikimi tiekėjai.

### 5.2.3 AUTENTIFIKACIJA

Visos užklausos gauti kvalifikuotas paslaugas yra autentifikuojamos klientui suteiktu autorizacijos raktu.

## 5.3 Duomenys ir srautai

Kvalifikuotos paslaugos klientui teikiamos jų autentifikavus. Klientai – kitos sistemos, kurioms yra suteikiamas autentifikacijos raktas. Klientas atsiuncia 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 ilgalaikiams 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 deklaruoamos. Tirkinami pasirašiusio asmens sertifikatai. Šių patikryų metu gali būti kreipiamasi į sertifikatą išdavusią jstaigą, perduodant sertifikato identifikacinius numerius.

Kvalifikuoto paruošimo ilgalaikiam saugojimui metu – atliekamos operacijos kaip ir patikrinimo metu. Papildomai į dokumentą yra įtraukama informacija, kuri ateityje galima bus naudoti patikrinimui. Ant šios informacijos yra uždedamos kvalifikuotos laiko žymos. Uždedant laiko žymą – kvalifikuotam laiko žymę tiekėjui yra perduodama kriptografinėmis maišos operacijomis užkoduota informacija.

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 jstaigą.

Elektroninis dokumentas ir jo turinys gali būti visiškai bet koks, ir mums iš anksto nežinomas. Tirkinimo, bei paruošimo ilgalaikiam saugojimui metu su duomenimis automatizuotai būna atliekamos kriptografinės maišos skaičiavimo operacijos (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 jstaiga. Kiekviena sertifikatus išduodanti jstaiga įrašo skirtinę informaciją, ir ji priklauso nuo šalyje paplitusios praktikos, sertifikato profilių ir pan.

Kuriant kvalifikuoto patikrinimo ataskaitą, ji yra pasirašoma NEVDA pažangiuoju elektroniniu spaudu. Spaudo sertifikato privatus raktas yra saugomas ribotos prieigos programinėje įrangoje. Kiekvienas el. spaudo privataus rakto panaudojimo atvejis yra fiksujamas ir audituojamas.

Visos operacijos ir kreipiniai (iš Kliento į Elpako informacinių sistemų) yra audituojami ir saugomi duomenų bazėje siejant su kliento raktu.