Pažangusis el. spaudas patvirtintas kvalifikuotu sertifikatu
DOKOBIT
2025-12-08 16:51:34 GMT+2
Paskirtis: Spaudas
Dokobit
By Signicat

Dokobit
By Signicat

Kvalifikuotos parašų ir spaudų galiojimo patvirtinimo paslaugos praktiniai nuostatai ir politika v1.16

Dokumento numeris: DKB-VSP-06122019 v1.16

Unikalus objekto ID (OID): 1.3.6.1.4.1.54720.1.1

Įsigalioja nuo 2026-01-09

Vertimas iš anglų kalbos

© 2025 — Dokobit, UAB — paprasčiau nei pasirašyti ranka.

https://www.dokobit.com

Dokobit
By Signicat

Turinys

1 Pakeitimų istorija 5
2 Įžanga 7
2.1 Apžvalga 7
2.1.1 TSP identifikacija 8
2.1.2 Palaikoma galiojimo patvirtinimo paslaugos politika 8
2.2 Galiojimo patvirtinimo paslaugos komponentai 9
2.2.1 SVS dalyviai 9
2.2.2 Paslaugos struktūra 9
2.3 Sąvokos ir santrumpos 10
2.3.1 Sąvokos 10
2.3.2 Santrumpos 11
2.4 Politika ir praktika 13
2.4.1 TSP dokumentus administruojanti organizacija 13
2.4.2 Kontaktinis asmuo 13
2.4.3 TSP dokumentacijos taikomumas 13
Galiojimo patvirtinimo paslaugos praktiniai nuostatai ir paslaugos politika 13
Paslaugų teikimo sąlygos 14
Rizikos vertinimas ir informacijos saugumo politika 14
2.4.4 „Dokobit" kvalifikuotos galiojimo patvirtinimo paslaugos naudojimo apribojimai 14
3 Patikimumo užtikrinimo paslaugos valdymas ir veikla 16
3.1 Vidinė organizacija 16
3.1.1 Organizacijos patikimumas 16
3.1.2 Pareigų atskyrimas 17
3.2 Žmogiškieji ištekliai 17
3.3 Turto valdymas 17
3.3.1 Bendrieji reikalavimai 17
3.3.2 Laikmenų naudojimas 18
3.4 Prieigos kontrolė 18
3.5 Kriptografinės kontrolės priemonės 19
3.6 Fizinis ir aplinkos saugumas 19
3.7 Operacijų saugumas 19
3.8 Tinklo saugumas 20

3.9 Pažeidžiamumų ir incidentų valdymas ... 20
3.9.1 Stebėsena ir registravimas žurnaluose ... 20
3.9.2 Atsakas į incidentus ... 20
3.9.3 Ataskaitų teikimas ... 20
3.9.4 Įvykių vertinimas ir klasifikavimas ... 21
3.9.5 Vėlesnė incidentų peržiūra ... 21
3.10 Įrodymų rinkimas ... 21
3.11 Veiklos tęstinumo valdymas ... 22
3.11.1 Bendrieji principai ... 22
3.11.2 Atsarginis kopijavimas ... 22
3.11.3 Krizių valdymas ... 22
3.12 TSP nutraukimas ir nutraukimo planai ... 23
3.13 Atitiktis ... 23
3.14 Tiekimo grandinė ... 23
4 Patvirtinimo paslaugos struktūra ... 24
4.1 Parašo galiojimo patvirtinimo proceso reikalavimai ... 24
4.1.1 Parašo galiojimo patvirtinimo modelis ... 25
4.1.2 Parašo galiojimo patvirtinimo proceso būsenos indikacija ir parašo galiojimo patvirtinimo ataskaita ... 26
4.1.3 Galiojimo patvirtinimo procesas ... 31
4.1.4 Elektroniniu būdu pasirašytų dokumentų galiojimo patvirtinimo apribojimai ... 33
Bendrieji apribojimai ... 33
X.509 Galiojimo patvirtinimo apribojimai ... 33
Kriptografiniai apribojimai ... 36
Parašo ir spaudo elementų apribojimai ... 36
4.2 Parašo galiojimo patvirtinimo protokolo reikalavimai ... 37
4.3 Sąsajos ... 37
4.3.1 Ryšio kanalas ... 37
4.3.2 SVSP - kiti patikimumo užtikrinimo paslaugų teikėjai ... 38
4.4 Parašo galiojimo patvirtinimo ataskaitos reikalavimai ... 38
5 A priedas ... 40
6 B priedas ... 46

Dokumento numeris: DKB-VSP-06122019 v1.16

Unikalus objekto identifikatorius (OID): 1.3.6.1.4.1.54720.1.1

Galioja nuo 09.01.2026

1 Pakeitimų istorija

Data	Versija	Pakeitimo aprašymas
03/08/2018	1.0	Pradinė versija „Dokobit“ Parašų galiojimo patvirtinimo paslaugos
10/10/2019	1.2	Dokumentas peržiūrėtas, kad atitiktų ETSI TS 119 441 reikalavimus
03/12/2019	1.5	• Atnaujinta, kad atitiktų rekomenduojamą dokumento struktūrą (ETSI TS 119 441 V1.1.1 (2018-08) A priedas) • Sąsajos su ISO 27001 *SoA* dokumentu
06/12/2019	1.6	Įtraukti parašo patvirtinimo paslaugos komponentai ir paslaugos struktūros schema, atlikti reikiami pakeitimai dėl Kvalifikuotos patikimumo užtikrinimo paslaugos teikimo
17/04/2020	1.7	Smulkūs atnaujinimai • Patikslinta 2.1.2 dalis – nurodytas šio Politikos dokumento OID • Patikslinta 2.1.1 dalis – nurodytas Kvalifikuotos parašo galiojimo patvirtinimo paslaugos teikėjo OID • Patikslintos 4.1.3 ir 4.3.1 dalys, nurodant, kad naudotojai paslaugai yra autentifikuojami naudojant el. atpažinties priemones • Patikslinta 2.4.3 dalis – įtrauktas Pranešimas Priežiūros įstaigai • Patikslinta 4.1.2 dalis – apibrėžtas slapyvardžio naudojimas Parašo galiojimo patvirtinimo ataskaitose • Patikslinta 3.12 dalis – įtraukta nuostata dėl pranešimo apie paslaugos nutraukimą • Patikslinta 2.1 dalis – patikslintas taikomų Lietuvos Respublikos teisės aktų sąrašas
26/11/2020	1.8	• Patikslinta – įtraukti išsamūs aprašymai Patikimumo užtikrinimo paslaugos valdymo ir veiklos dalyse, kad jas būtų lengviau skaityti ir suprasti trečiosioms šalims • Patikslinta 4.1.1 dalis – įtraukti nauji Aktyvavimo programos ir išplėstinės Aktyvavimo programos aprašymai Parašo patvirtinimo modelyje • Patikslinta 4.1.3 dalis – įtrauktas „Dokobit“ Galiojimo patvirtinimo paslaugos naudojimas • Patikslinta 4.2 dalis – įtrauktas „Dokobit“ Galiojimo patvirtinimo paslaugos naudojimas • Patikslinta 4.3.1 dalis – įtrauktas QWAC sertifikato naudojimas
01/05/2021	1.9	• Patikslinta – įtraukti „Dokobit“ Galiojimo patvirtinimo paslaugos apribojimai 2.4 dalyje: Politika ir praktika • Įtraukti Galiojimo patvirtinimo politikos apribojimai, pateikiami A ir B prieduose
08/07/2021	1.10	Dokumento pavadinime įtrauktas žodis „spaudų“ - Kvalifikuotos parašų ir spaudų galiojimo patvirtinimo paslaugos praktiniai nuostatai ir politika
07/11/2022	1.11	Pakeistas įmonės registracijos adresas.

Data	Versija	Pakeitimo aprašymas
05/06/2023	1.12	Pridėtas Ukrainos TSL.
08/05/2024	1.13	• Atnaujintos nuorodos į pasikeitusius teisės aktus. • Patikslintos atsakomybės dėl dokumentacijos tvirtinimo. • Įtrauktas naujas įspėjimo (WARN) lygio apribojimas dėl aptiktų vizualų dokumento turinį keičiančių elementų. • Pašalinta fiksuota TL atnaujinimo reikšmė. • Atliktos minimalios kalbinės korekcijos.
09/01/2025	1.14	• Atlikti pakeitimai, susiję su atnaujinta ISVS ir perėjimu prie ISO/IEC 27001 ir 27002:2022 standartų naujų versijų • Atlikti pakeitimai, susiję su naujomis standartų ETSI EN 310 401 ir ETSI TS 119 441 versijomis • Atlikti pakeitimai, susiję su eIDAS v2 ir NIS 2 bei atitinkamų Lietuvos Respublikos įstatymų pakeitimais
30/06/2025	1.15	• Atnaujinimai, susiję su Dokobit, UAB perėjimu iš atskiros ISVS sistemos į bendrą „Signicat“ grupės ISVS sistemą. • Nedideli pakeitimai pagerinantys skaitomumą. • Nedideli pakeitimai, susiję su prekės ženklo pasikeitimais.
26/11/2025	1.16	• Atnaujinimai, susiję su spaudo sertifikatu

2 Įžanga

2.1 Apžvalga

Šiame dokumente apibūdinamos „Dokobit“, UAB (toliau – „Dokobit“) taikomos praktikos,

teikiant **Kvalifikuotas parašo ir spaudo galiojimo patvirtinimo paslaugas (toliau – Kvalifikuotos galiojimo patvirtinimo paslaugos)** pagal:

- 2014 m. liepos 23 d. Europos Parlamento ir *Tarybos reglamentą (ES) Nr. 910/2014* dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, su pakeitimais, padarytais 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos *reglamentu (ES) 2024/1183*, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės atpažinties sistemos sukūrimu, į konsoliduotą tekstą *iš dalies pakeisto eIDAS reglamento* (eIDAS v2) tekstą;
- 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos *direktyvą (ES) 2022/2555* dėl aukšto bendro kibernetinio saugumo lygio visoje Sąjungoje priemonių, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (NIS 2 direktyva);
    - *Komisijos įgyvendinimo reglamentą C(2024) 7151*, kuriuo nustatomos Direktyvos (ES) 2022/2555 taikymo taisyklės, susijusios su kibernetinio saugumo rizikos valdymo priemonių techniniais ir metodiniais reikalavimais, ir išsamiau apibrėžiami atvejai, kai incidentas laikomas reikšmingu, kiek tai susiję su DNS paslaugų teikėjais, aukščiausio lygio domenų vardų registrais, debesų kompiuterijos paslaugų teikėjais, duomenų centrų paslaugų teikėjais, turinio pristatymo tinklų teikėjais, valdomų paslaugų teikėjais, valdomų saugumo paslaugų teikėjais, internetinių prekyviečių, internetinių paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjais ir patikimumo užtikrinimo paslaugų teikėjais, ir jo *priedą*;
- 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos *direktyvą (ES) 2019/882* dėl gaminių ir paslaugų prieinamumo reikalavimų;
- Lietuvos Respublikos teisės aktus:
    - Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymą;
    - Ryšių reguliavimo tarnybos direktoriaus 2018 m. birželio 21 d. įsakymą 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 tarybos 2023 m. gruodžio 21 d. nutarimą Nr. TN-708 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų ir prižiūrimų elektroninės atpažinties priemonių saugumo ir (ar) vientisumo pažeidimus pateikimo tvarkos aprašo patvirtinimo“;
    - Lietuvos Respublikos *kibernetinio saugumo įstatymą Nr. XII-1428* su pakeitimais, padarytais *Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymu Nr. XIV-2902* (NIS 2 Lietuvos teisėje).
- Europos standartą *ETSI EN 319 401* - Elektroniniai parašai ir patikimumo užtikrinimo infrastruktūros (EPI); bendrieji politikos reikalavimai patikimumo užtikrinimo paslaugos teikėjams, V3.1.1, 2024 m. birželis;
- ETSI techninę specifikaciją *ETSI TS 119 441* - Elektroniniai parašai ir patikimumo užtikrinimo infrastruktūros (EPI); politikos reikalavimai patikimumo užtikrinimo paslaugos teikėjams, teikiantiems parašo galiojimo patvirtinimo paslaugas, V1.2.1, 2023 m. spalis;
    - Šio dokumento struktūra atitinka ETSI TS 119 441 A priedą;

- ETSI techninę specifikaciją *ETSI TS 119 442* - Elektroniniai parašai ir infrastruktūros (EPI); Protokolo profiliai patikimumo užtikrinimo paslaugos teikėjams, teikiantiems skaitmeninio AdES parašo galiojimo patvirtinimo paslaugas, V1.1.1, 2019 m. vasaris
- Europos standartą *ETSI EN 319 102-1* - Elektroniniai parašai ir patikimumo užtikrinimo infrastruktūros (EPI); elektroninių parašų kūrimo ir galiojimo patvirtinimo procedūros; 1 dalis: kūrimas ir galiojimo patvirtinimas, V1.4.1, 2024 m. birželis
- ETSI techninę specifikaciją *ETSI TS 119 102-2* - Elektroniniai parašai ir infrastruktūros (ESI); AdES skaitmeninių parašų sukūrimo ir tikrinimo procedūros; 2 dalis: parašo galiojimo patvirtinimo ataskaita, V1.4.1, 2023 m. birželis
- ETSI techninę specifikaciją *ETSI TS 119 172-1* - Elektroniniai parašai ir infrastruktūros (ESI); parašų politikos; 1 dalis: žmogui suprantamų parašų politikos dokumentų struktūriniai elementai ir turinys, V1.1.1, 2015 m. liepa
- ETSI techninę specifikaciją *ETSI TS 119 172-4* - Elektroniniai parašai ir infrastruktūros (ESI); parašų politikos; 4 dalis: Parašų taikymo taisyklės (galiojimo patvirtinimo politika) Europos kvalifikuotiems elektroniniams parašams/spaudams, naudojant patikimus sąrašus, V1.1.1, 2021 m. gegužė
- ETSI techninę specifikaciją *ETSI TS 119 312* - Elektroniniai parašai ir patikimumo infrastruktūros (ESI); Kriptografiniai rinkiniai, V1.5.1, 2024 m. gruodis

2.1.1 TSP identifikacija

„Dokobit“, UAB

Įmonės kodas 301549834

Paupio g. 50-136, LT-11341 Vilnius

El. paštas *info@dokobit.com*

www.dokobit.com

Paslaugos teikėjo registruotas oficialus objekto identifikatorius (OID) - 1.3.6.1.4.1.54720

2.1.2 Palaikoma galiojimo patvirtinimo paslaugos politika

„Dokobit“ kvalifikuotos elektroninių parašų ir spaudų galiojimo patvirtinimo paslaugos politika identifikuojama pagal registruotą oficialų objekto identifikatorių (OID) 1.3.6.1.4.1.54720.1.1.

Ši politika pagrįsta kvalifikuota galiojimo patvirtinimo politika, apibrėžta ETSI TS 119 441 su OID 0.19441.1.2.

„Dokobit“ kvalifikuotos parašo ir antspaudo galiojimo patvirtinimo paslaugos politika nuo ETSI TS 119 441 apibrėžtos politikos skiriasi toliau nurodytais elementais: „Dokobit“ dokumentas taip pat yra praktikos aprašas, be to, jame yra skyriai, nustatantys naudojimo / įsipareigojimų apribojimus, reikalavimus galiojimo patvirtinimo ataskaitai, galiojimo patvirtinimo apribojimus ir palaikomus formatus.

2.2 Galiojimo patvirtinimo paslaugos komponentai

2.2.1 SVS dalyviai

Parašo galiojimo patvirtinimo klientas (SVC)

- Programinės įrangos komponentas, suteikiantis Aktyvavimo programos, naudojamos „Dokobit“ Paslaugų abonentų, naudotojo sąsają.

Aktyvavimo programa (DA)

- Programa, kuri suteikia parašo galiojimo patvirtinimo funkcionalumą Parašo galiojimo patvirtinimo klientui.

Parašo galiojimo patvirtinimo paslaugos protokolas (SVP)

- Saugusis ryšio kanalas, per kurį keičiamasi informacija su Parašo galiojimo patvirtinimo paslaugos serveriu (SVSServ).

Parašo galiojimo patvirtinimo paslaugos serveris (SVSServ)

- Komponentas, įgyvendinantis parašo galiojimo patvirtinimo protokolą parašo galiojimo patvirtinimo paslaugos teikėjo (SVSP) pusėje.

Parašo galiojimo patvirtinimo programa (SVA)

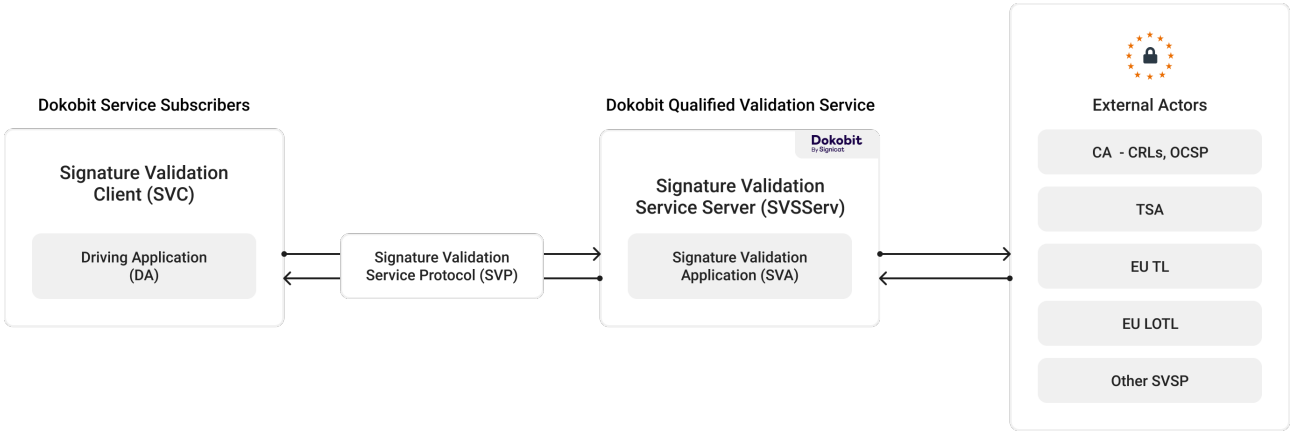
- Už parašo galiojimo patvirtinimą atsakingas programinės įrangos komponentas, kuris vykdo patvirtinimo algoritmą ir sukuria parašo galiojimo patvirtinimo ataskaitą.

Išoriniai dalyviai

- Kiti patikimumo užtikrinimo šaltiniai – Sertifikavimo institucijos, Laiko žymų tarnybos, tiekėjai, įrašyti į Europos Patikimą sąrašą, Europos Komisija, sudaranti Patikimų sąrašų sąrašą, į kuriuos kreipiamasi siekiant įgyvendinti atitinkamus tikslus.

2.2.2 Paslaugos struktūra

Toliau esančioje schemoje parodyta supaprastinta „Dokobit“ Kvalifikuotos galiojimo patvirtinimo paslaugos struktūra ir jos dalyviai.



2.3 Sąvokos ir santrumpos

2.3.1 Sąvokos

Pavadinimas	Santrumpa	Apibrėžtis
eIDAS reglamentas	eIDAS	2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, su pakeitimais, padarytais 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentu (ES) Nr. 2024/1183, kuriuo iš dalies keičiamos Reglamento (ES) Nr. 910/2014 nuostatos dėl Europos skaitmeninės atpažinties sistemos sukūrimo.
Bendrasis duomenų apsaugos reglamentas	BDAR	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
Tinklų ir informacinių sistemų saugumo direktyva	NIS 2	2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių, skirtų aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (NIS 2 direktyva).
Informacijos saugumo valdymo sistema	ISVS	„Signicat“ grupės informacijos saugos valdymo sistema, sertifikuota pagal ISO/IEC 27001:2022 standartą. „Dokobit“, UAB yra įtraukta į sertifikavimo taikymo sritį, kaip nurodyta sertifikato priede, kuriame pateiktas įtrauktų grupei priklausančių dukterinių įmonių sąrašas.
Patikimumo užtikrinimo paslaugos teikėjas	TSP	Subjektas, teikiantis patikimumo užtikrinimo paslaugą.

Pavadinimas	Santrumpa	Apibrėžtis
Kvalifikuotų patikimumo užtikrinimo paslaugos teikėjas	QTSP	Subjektas, teikiantis vieną ar daugiau kvalifikuotų patikimumo užtikrinimo paslaugų ir turintis priežiūros institucijos suteiktą kvalifikuotos paslaugos statusą.
Priežiūros įstaiga		Institucija, kurią valstybė narė skiria vykdyti patikimumo užtikrinimo paslaugų ir patikimumo užtikrinimo paslaugų teikėjų priežiūros veiklą pagal eIDAS tos valstybės narės teritorijoje.
„Dokobit“ galiojimo patvirtinimo paslaugų nuostatai	Dokobit PS	Nuostatai, kuriuose aprašomos praktikos, kurias „Dokobit“ taiko teikdama Kvalifikuotas galiojimo patvirtinimo paslaugas.
Parašo galiojimo patvirtinimo paslauga	SVS	Patikimumo užtikrinimo paslauga - parašo ir (arba) spaudo galiojimo patvirtinimas.
Pasikliaujančioji šalis	RP	Fizinis ar juridinis asmuo, kuris pasikliauja patikimumo užtikrinimo paslauga.
„Signicat“ grupė		„Signicat AS“ ir jos dukterinės įmonės, įskaitant ir Dokobit, UAB.
Abonentas		Juridinis ar fizinis asmuo, sutartimi su „Dokobit“ įsipareigojęs vykdyti Abonento pareigas.
Sertifikavimo institucija	CA	Patikimumo užtikrinimo paslaugos teikėjas, išduodantis sertifikatus el. parašui ir (arba) el. spaudui.
Kvalifikuota sertifikavimo institucija	QCA	Kvalifikuotos patikimumo užtikrinimo paslaugos teikėjas, išduodantis kvalifikuotus sertifikatus el. parašui ir (arba) el. spaudui.

2.3.2 Santrumpos

DA	Aktyvavimo programa
PoE	Egzistavimo įrodymas
QES	Kvalifikuotas elektroninis parašas arba Kvalifikuotas elektroninis spaudas
AdES	Pažangusis elektroninis parašas
AdES/QC	Pažangusis elektroninis parašas, sukurtas su Kvalifikuotu sertifikatu

(Q)SCD	(Kvalifikuotas) parašo kūrimo įtaisas
QSVSP	Kvalifikuotos parašo galiojimo patvirtinimo paslaugos teikėjas
SD	Pasirašiusiojo dokumentas
SDO	Pasirašytas duomenų objektas
SDR	Pasirašyto dokumento atstovavimas
SVA	Parašo galiojimo patvirtinimo programa
SVP	Parašo galiojimo patvirtinimo protokolas
SVR	Parašo galiojimo patvirtinimo ataskaita
SVSP	Parašo galiojimo patvirtinimo paslaugos teikėjas
SVSServ	Parašo galiojimo patvirtinimo paslaugos serveris
TSA	Laiko žymų tarnyba
VPR	Parašo galiojimo patvirtinimo procesas
OID	Objekto identifikatorius
PKI	Viešojo rakto infrastruktūra
OCSP	Sertifikato būsenos protokolas tinkle
HSM	Aparatinės įrangos saugumo modulis
ISM	Informacijos saugumo vadovas („Signicat“ grupės CISO)
qVAL vadovas	Kvalifikuotos parašų ir spaudų galiojimo patvirtinimo paslaugos vadovas
ISVS	Informacijos saugumo valdymo sistema

2.4 Politika ir praktika

2.4.1 TSP dokumentus administruojanti organizacija

Šį dokumentą administruoja „Dokobit“.

„Dokobit“, UAB

Įmonės kodas 301549834

Paupio g. 50-136, LT-11341 Vilnius

El. paštas *info@dokobit.com*

www.dokobit.com

2.4.2 Kontaktinis asmuo

Kontaktinis asmuo dėl šio dokumento yra „Dokobit“ kvalifikuotos parašų ir spaudų galiojimo patvirtinimo paslaugos vadovas.

Dėl papildomos informacijos galima kreiptis el. paštu *compliance@dokobit.com*.

2.4.3 TSP dokumentacijos taikomumas

Galiojimo patvirtinimo paslaugos praktiniai nuostatai ir paslaugos politika

„Dokobit“ atsako už „Dokobit“ Galiojimo patvirtinimo paslaugos praktinių nuostatų, kurie apima ir paslaugos politiką, tvarkymą. Šį dokumentą tvirtina vadovybė ir jis viešai skelbiamas „Dokobit“ Standartų atitikties interneto svetainėje (*https://www.dokobit.com/lt/patikimumas*).

„Dokobit“ informuos Priežiūros įstaigą apie bet kokius kvalifikuotų patikimumo užtikrinimo paslaugų teikimo pakeitimus nedelsiant, bet ne vėliau kaip per 3 darbo dienas. „Dokobit“ informuos Priežiūros įstaigą apie numatomą paslaugos nutraukimą ne mažiau kaip prieš 3 mėnesius iki veiklos nutraukimo dienos.

Pranešimas Priežiūros įstaigai turėtų būti išsiųstas nedelsiant ir ne vėliau kaip per 3 darbo dienas nuo bet kokių Galiojimo patvirtinimo paslaugos praktiniuose nuostatose pakeitimų.

Abonentai ir Pasikliaujančiosios šalys turi vadovautis tik galiojančia „Dokobit“ praktinių nuostatų versija nuo tada, kai ima naudotis „Dokobit“ teikiamomis paslaugomis. Atnaujinta „Dokobit“ praktinių nuostatų versija kartu su įsigaliojimo datomis paskelbiama bent 30 dienų iki įsigaliojimo.

Paslaugų teikimo sąlygos

„Dokobit“ pateikia Paslaugų teikimo sąlygas ir Duomenų tvarkymo sutartį savo interneto svetainėje (*https://www.dokobit.com/lt/patikimumas*).

Rizikos vertinimas ir informacijos saugumo politika

„Dokobit“ veikia pagal „Signicat“ grupės ISVS. „Signicat AS“, motininė Dokobit, UAB bendrovė, yra sertifikavusi ISVS pagal ISO/IEC 27001:2022 standartą, kurio taikymo sritis apima: „Skaitmeninės tapatybės ir elektroninio parašo sprendimų teikimą, įskaitant kvalifikuotąsias paslaugas (kvalifikuotą laiko žymą, kvalifikuoto parašo ir antspaudo tikrinimą bei kvalifikuotų sertifikatų išdavimą kvalifikuotiems elektroniniams parašams), naudojant ISO/IEC 27018:2019 ir vadovaujantis naujausia Taikymo srities deklaracijos versija“. Dokobit, UAB yra įtraukta į sertifikavimo taikymo sritį, kaip nurodyta sertifikato priede, kuriame pateikiamas įtrauktų grupei priklausančių įmonių sąrašas.

ISVS ir ISO/IEC 27001:2022 sertifikatas apima rizikos vertinimo ir rizikos valdymo metodiką bei informacijos saugumo, informacijos saugumo organizavimo ir atitikties politikas. Politikos ir rizikos vertinimo metodika taikoma kvalifikuotai galiojimo patvirtinimo paslaugai. Rizikos vertinimas apima grėsmių žvalgybą.

Visos būtinos saugumo priemonės, kurių reikalaujama pagal eIDAS, BDAR ir kitus taikomus teisės aktus ir atitinkamus standartus (t.y. ETSI EN 319 401), yra įdiegtos ir palaikomos ISVS. Taip pat, NIS 2 kontekste, Dokobit, UAB yra klasifikuota kaip svarbus subjektas ir yra įpareigota laikytis Lietuvos Nacionalinio kibernetinio saugumo centro atitikties reikalavimų.

Politikas ir nuostatus, susijusius su informacijos saugumu, tvirtina „Signicat“ grupės informacinio saugumo valdyba (ISV). qVAL vadovas yra atsakingas už su Kvalifikuotomis galiojimo patvirtinimo paslaugomis susijusias politikas ir praktikas.

2.4.4 „Dokobit“ kvalifikuotos galiojimo patvirtinimo paslaugos naudojimo apribojimai

„Dokobit“ kvalifikuota galiojimo patvirtinimo paslauga teikia galiojimo patvirtinimo ataskaitas su trimis skirtingais apribojimais:

- 1 pakopa (standartinė atsakomybė). Ši pakopa skirta dokumentams, kurių vertė neviršija 100 EUR, „Dokobit“ prisiimama atsakomybė – iki 100 EUR už galiojimo patvirtinimo ataskaitą.
- 2 pakopa (padidinta atsakomybė). Ši pakopa skirta dokumentams, kurių vertė neviršija 10 000 EUR, „Dokobit“ prisiimama atsakomybė – iki 10 000 EUR už galiojimo patvirtinimo ataskaitą.
- 3 pakopa (aukščiausia atsakomybė). Ši pakopa skirta dokumentams, kurių vertė neviršija 100 000 EUR, „Dokobit“ prisiimama atsakomybė – iki 100 000 EUR už galiojimo patvirtinimo ataskaitą.

Apribojimai nurodomi kiekvienoje „Dokobit“ kvalifikuotos galiojimo patvirtinimo paslaugos sugeneruojamoje galiojimo patvirtinimo ataskaitoje.

3 Patikimumo užtikrinimo paslaugos valdymas ir veikla

„Dokobit“ veikia pagal „Signicat“ grupės ISVS, kuriai akredituota tarptautinė sertifikavimo įstaiga suteikė *ISO/IEC 27001:2022 sertifikatą*. „Dokobit“ yra įtraukta į ISO/IEC 27001:2022 sertifikavimo apimtį kaip „Signicat AS“ (motininė „Signicat“ grupės įmonė) dukterinė įmonė. Kvalifikuotos galiojimo patvirtinimo paslaugos apima šį sertifikatą. ISVS apima visas taikytinas saugumo kontrolės priemones, nurodytas ISO/IEC 27001:2022 A priede. ETSI EN 319 401 standarto saugumo kontrolės priemonės yra grindžiamos standarto ISO/IEC 27002:2022 saugumo kontrolės priemonėmis, todėl ISVS apima bendruosius ETSI EN 319 401 reikalavimus. Be to, siekiant užtikrinti aukščiausio lygio asmens duomenų apsaugą debesijos aplinkose, buvo įdiegtos ISO/IEC 27018 kontrolės priemonės.

Toliau apibendrinamas patikimumo užtikrinimo paslaugos valdymas ir veikla, įskaitant taikomas saugumo kontrolės priemones.

3.1 Vidinė organizacija

„Dokobit“ vykdo visus teisinius įsipareigojimus, taikomus teikiant patikimumo užtikrinimo paslaugas. Bendrovė veikia laikydamasi priimtų politikos dokumentų ir praktinių nuostatų, kurie parengti atsižvelgiant į taikomų standartų reikalavimus. „Dokobit“ užtikrina, kad visi reikalavimai, nustatyti ISVS pareiškime ir šiuose praktiniuose nuostatuose, būtų įgyvendinami ir visuomet taikomi teikiamoms patikimumo užtikrinimo paslaugoms.

Patikimumo užtikrinimo paslaugų teikimui taikomas išorės auditas. Jį bent kartą per 24 mėnesius atlieka atitikties vertinimo įstaiga (CAB).

3.1.1 Organizacijos patikimumas

„Dokobit“ turi šiame dokumente aprašytai veiklai vykdyti būtiną finansinį stabilumą ir išteklius. Bendrovė yra įsigijusi civilinės atsakomybės draudimą pagal galiojančius įstatymus, kad padengtų įsipareigojimus, susijusius su savo veikla ir kylančius iš eIDAS reglamento 13 straipsnio. „Dokobit“ gali pateikti daugiau informacijos apie konkrečias organizacijos patikimumo priemones, gavusi konkretų teisėtą suinteresuotosios šalies prašymą.

3.1.2 Pareigų atskyrimas

ISVS pagal tarptautinį standartą ISO/IEC 27001:2022 užtikrina, kad būtų tikrinamas ir išlaikomas būtinas pareigų atskyrimas. Kalbant konkrečiai apie kvalifikuotą galiojimo patvirtinimo paslaugą, atskiriamos informacijos saugumo vadovo (ISM), qVAL vadovo ir vidaus auditoriaus funkcijos. Svarbiausiose srityse užtikrinamas keturių akių principas:

- Saugus kūrimas ir kodo peržiūros
- Programinės įrangos diegimas

3.2 Žmogiškieji ištekliai

Įdiegta ir sertifikuota ISVS užtikrina, kad „Dokobit“ yra įdiegusi reikiamas žmogiškųjų išteklių saugumo kontrolės priemones.

Saugumo kontrolės priemonės yra dokumentuotos ISVS taikymo pareiškime ir apima šias temas:

- Atranka
- Įdarbinimo sąlygos
- Informacijos neatskleidimas nutraukus darbo sutartį arba pakeitus darbo pareigas
- Darbuotojų mokymas ir kvalifikacija
- Drausminės nuobaudos
- Patikimų pareigų apibrėžtys ir pareigybių aprašymai
- Paskyrimo į patikimas pareigas tvarka ir atsakomybė (vadovybės ir qVAL vadovo atsakomybė)
- Nuotolinis darbas

Darbuotojai ir rangovai gauna tinkamą mokymą ir turi reikiamą patirtį, kad galėtų atlikti pareigas, nurodytas įdarbinimo ar rangos sutartyse, kaip apibrėžta „Signicat“ grupės Žmogiškųjų išteklių saugumo politikoje.

3.3 Turto valdymas

3.3.1 Bendrieji reikalavimai

„Dokobit“ nuolat atnaujina turto sąrašus, įskaitant informacinius išteklius, nurodydama visų išteklių atsakingus asmenis. Rizikos valdymas yra grindžiamas turto identifikavimu. Rizikos vertinimas yra suderintas su turto identifikavimu, o turtui aktuali grėsmė nustatoma pasitelkiant išsamią sąsajų analizę. Turtas klasifikuojamas pagal konfidencialumo, vientisumo ir prieinamumo apsaugos reikalavimus.

Turto valdymas yra „Signicat“ grupės ISVS dalis, reglamentuojamas pagal „priimtino naudojimo politiką, informacijos klasifikavimo politiką ir rizikos valdymo metodiką. Darbuotojai ir kitos šalys privalo grąžinti turtą pasikeitus ar pasibaigus darbo santykiams.

qVAL vadovas yra atsakingas už Kvalifikuotą galiojimo patvirtinimo paslaugą kaip turto vienetą bei kitus su paslauga susijusius svarbius turto vienetus.

3.3.2 Laikmenų naudojimas

Laikmenos, kuriose yra neskelbtinos informacijos, tvarkomos saugiai ir laikantis ISVS turto valdymo, komunikacijų saugumo ir operacijų saugumo politikos dalių. Laikmenų tvarkymą, susijusį su kvalifikuotos galiojimo patvirtinimo paslaugos veikla, atlieka debesijos prieglobos operatorius.

3.4 Prieigos kontrolė

Prieigos kontrolės politika, kuri yra „Signicat“ grupės ISVS dalis, užtikrina, kad prieiga prie sistemos būtų suteikta tik įgaliotiems asmenims ir kad būtų įdiegtos visos būtinos saugios prieigos kontrolės priemonės.

Pagrindinis prieigos kontrolės principas yra tas, kad prieiga prie visų sistemų, tinklų, paslaugų ir informacijos pagal numatytuosius nustatymus yra draudžiama, nebent aiškiai suteikta konkretiems naudotojams arba naudotojų grupėms remiantis būtinybės žinoti principu. Bet kokia suteikta prieiga papildomai ribojama vadovaujantis mažiausios privilegijos principu. Prieigos kontrolės politikoje apibrėžtos išsamios (elektroninės) prieigos suteikimo gairės, reikalavimai įmonės paskyros saugumo nustatymams, privilegijų valdymui ir reguliariam prieigos teisių peržiūrėjimui. Pagal šią politiką turi būti užtikrinti ir saugomi susieti atsekami prieigos kontrolės įrašai. Nuotolinė prieiga palaikoma tik šifruotu būdu (pagal mobiliojo ryšio įrenginių ir nuotolinio darbo politiką) ir jai taikoma priimtino naudojimo politika.

Prieigos kontrolės politikoje nustatytos naudotojo registravimo įmonės sistemose, vidiniame tinkle ir informacinėse sistemose gairės. Be to, naudotojo registracijos procesą papildo rekomenduojami techniniai (saugumo) parametrai. Prieigos kontrolės politikoje taip pat apibrėžiamas naudotojo išregistravimo procesas, įskaitant paskyros pašalinimo reikalavimus. Prieigos leidimą turi suteikti sistemos (turto) savininkas ir, priklausomai nuo procesų informacijos klasifikavimo ir informacijos, kuri turi būti saugoma, papildomai autorizuoti valdyba.

Priimtino naudojimo politikoje pateikiami išsamūs reikalavimai naudotojams dėl slaptos autentifikavimo informacijos valdymo ir naudojimo. Ji užtikrina geriausios industrijos praktikos, pavyzdžiui, privalomos 2FA ir šifruotų slaptažodžių valdymo priemonių, taikymą. Išsamūs reikalavimai įmonės paskyrų saugumo nustatymams išvardyti prieigos kontrolės politikoje, kuri atspindi geriausią industrijos praktiką.

3.5 Kriptografinės kontrolės priemonės

Kriptografinės kontrolės priemonės yra apibrėžiamos laikantis kriptografijos politikos, kuri yra ISVS dalis. Ryšys su kvalifikuota galiojimo patvirtinimo paslauga yra apsaugotas TLS protokolu, naudojant patvirtintas kriptografijos priemones. Galiojimo patvirtinimo ataskaitų spaudai kuriami taikant patvirtintas kriptografijos priemones, naudojant privatų raktą, saugomą debesijos prieglobos operatoriaus suteiktame HSM.

3.6 Fizinis ir aplinkos saugumas

Operacijų saugumo politika reglamentuoja fizinę prieigą prie informacijos ir įrangos. Kvalifikuotai galiojimo patvirtinimo paslaugai teikti naudojamos įrangos fiziniu ir aplinkos saugumu rūpinasi debesijos prieglobos paslaugų teikėjas, kurio veiklą reglamentuoja sutarties nuostatos ir tiekėjų valdymo politika.

Atitinkama vidaus įranga gali būti laikoma tik saugiose vietose. ISVS taikymo srities dokumente aprašomas saugių zonų sąrašas ir susijusios saugumo kontrolės priemonės bei procedūros.

„Dokobit“ patalpų fizinės apsaugos perimetras apibrėžtas ISVS taikymo srities dokumente. Remiantis rizikos vertinimu, įdiegiamos fizinio saugumo kontrolės priemonės, kad būtų užtikrintas reikiamas apsaugos lygis. Fizinio saugumo kontrolės priemonės vertinamos atliekant detalias rizikos valdymo ir vertinimo veiklas. Bendrai, skirtingo lygmens fizinio įėjimo kontrolės priemonės, apibrėžtos prieigos kontrolės politikoje bei fizinio ir aplinkos saugumo politikoje, priklauso nuo objekto svarbos. Pavyzdžiui, prieiga prie saugių zonų yra „draudžiama pagal numatytąją nuostatą“ (pvz., „užrakinta“), išskyrus leidžiamus atvejus. Dėl „Dokobit“ veiklos pobūdžio ir naudojimosi viešųjų debesijos IaaS paslaugų teikėjų paslaugomis bendrovė nėra priklausoma nuo vienos ar kelių pastovių fizinių vietų.

Viešosios prieigos zonas, įskaitant pristatymo ir pakrovimo zoną (įėjimą į biurų pastatą), dieną kontroliuoja biurų pastato apsaugos darbuotojas, o naktį jos užrakinamos.

3.7 Operacijų saugumas

„Signicat“ grupės ISVS šią sritį apima operacijų saugumo politika, komunikacijos saugumo politika, sistemų įsigijimo, kūrimo ir priežiūros politika, tiekėjų valdymo politika, incidentų valdymo politika, prieigos kontrolės politika, mobiliojo ryšio įrenginių ir nuotolinio darbo politika, privatumo politika.

Dokumentacija, be kita ko, apima:

- Pakeitimų kontrolę
- Apsaugą nuo kenkėjiškų programų
- Autentiškumo nustatymą, autorizavimą ir prieigos kontrolę

- Pataisų valdymą
- Konfigūracijos valdymą
- Stebėsenos sistemas ir pavojaus signalus
- Konfigūracijos ir kitas peržiūras

3.8 Tinklo saugumas

„Signicat“ grupės ISVS šią sritį apima operacijų saugumo politika ir komunikacijos saugumo politika. Skiriamas didelis dėmesys tinklų atskyrimui, todėl gamybinė, parengiamoji / prieš gamybinė, kūrimo / testavimo ir biuro aplinkos yra atskirtos. Visiems tinklo prievadams taikomas principas „pagal numatytąsias nuostatas drausti“, išskyrus atvejus, kai „būtina naudoti“. Tinklo prievadų taisyklių rinkiniai reguliariai peržiūrimi. Reguliariai atliekami pažeidžiamumo patikrinimai ir įsiskverbimo testai.

3.9 Pažeidžiamumų ir incidentų valdymas

3.9.1 Stebėsena ir registravimas žurnaluose

„Signicat“ grupės ISVS šią sritį apima operacijų saugumo politika, į kurią įtrauktos išsamios stebėsenos, pavojaus signalų ir registravimo procedūros. Saugumo žurnalai reguliariai peržiūrimi, kad būtų galima aptikti ir ištirti įtartinus įvykius produkcinėse ir įmonės sistemose. Visi žurnalai siunčiami į nuotolines žurnalų kaupimo sistemas.

3.9.2 Atsakas į incidentus

„Signicat“ grupės ISVS šią sritį apima incidentų valdymo politika, kurioje nustatyta detali informacijos saugumo incidentų valdymo eiga. Procedūra suderinta su BDAR, NIS 2 ir eIDAS reikalavimais, nustatytais kvalifikuotų patikimumo užtikrinimo paslaugų teikėjams, atitinka kontekstą ir apima visas būtinas „Dokobit“ pareigas, susijusias su pranešimu apie incidentą ir jo tvarkymu. Iš ankstesnių incidentų išmoktos pamokos integruojamos į „Dokobit“ veiklą. Į incidentų valdymo procedūrą įtraukti skyriai apie incidentų suvaldymą ir likvidavimą bei veiklos atkūrimą po incidentų.

3.9.3 Ataskaitų teikimas

Kaip numatyta „Signicat“ grupės incidentų valdymo politikoje ir „Dokobit“ incidentų valdymo procedūroje, informacijos saugumo įvykiai gali būti aptikti „Dokobit“ vidaus kontrolės priemonėmis arba apie juos gali pranešti vidaus ar išorės šalys.

Incidentų valdymo procedūros pradinės analizės etapas nustato saugumo įvykio vertinimo kriterijus. Jei įvykis patvirtinamas kaip saugumo incidentas, pradedami tolesni reagavimo veiksmai (dokumentuoti procedūroje), pagrįsti geriausia tarptautine praktika (visų pirma ENISA, BDAR, NIS 2 ir eIDAS gairėmis).

ISM ir qVAL vadovas yra atsakingi už ryšius su informacijos saugumu susijusiomis institucijomis, pavyzdžiui, CERT institucijomis, Asmens duomenų apsaugos inspekcija ir priežiūros institucija pagal eIDAS reglamentą. Incidentų valdymo procedūroje numatytas specialus komunikacijos protokolas iš anksto nustatytų šablonų pavidalu, kad incidento atveju būtų užtikrintas savalaikis, tikslus ir galiojančius teisės aktus atitinkantis kontaktas su institucijomis. Teisinių, reguliavimo, sutartinių ir kitų reikalavimų sąraše apibrėžti taikytini įstatymai.

ISM ir qVAL vadovas yra atsakingi už ryšius su specialiųjų interesų grupėmis, susijusiomis su jų vaidmeniu informacijos saugumo srityje. ISM taip pat yra atsakingas už Atsakingo pažeidžiamumų atskleidimo politiką, kuri naudojasi saugumo bendruomenės (etinių įsilaužėlių) indėliu nustatant „Dokobit“ turto pažeidžiamumus.

3.9.4 Įvykių vertinimas ir klasifikavimas

Incidentų valdymo procedūros pradinės analizės etape apibrėžiami saugumo įvykio vertinimo kriterijai. Įvykis perklasifikuojamas, jei įvykio nagrinėjimo metu gauta informacija rodo, kad atvejis yra rimtesnis arba mažiau rimtas, palyginus su pradinės analizės išvada.

3.9.5 Vėlesnė incidentų peržiūra

Incidentų valdymo procedūroje apibrėžiamos po incidento atliekamos veiklos, įskaitant išmoktų pamokų analizę, kurios metu gali būti iš naujo įvertinama rizika, peržiūrimos saugumo kontrolės priemonės, atnaujinami ISVS dokumentai arba atliekami konkretūs tobulinimo veiksmai.

3.10 Įrodymų rinkimas

Įrodymų rinkimui „Dokobit“ taiko ETSI EN 319 401 7.10 punkte nurodytus reikalavimus. Šie įrašai atskleidžiami tik teisėsaugos institucijoms teismo nutartimi ir teisėtą reikalavimą pateikusiems asmenims. Tokia informacija tvarkoma vadovaujantis privatumo ir atitikties politikomis, kurios yra „Signicat“ grupės ISVS dalis.

Incidentų atveju įrodymai renkami jam vykstant ar pasibaigus, remiantis gairėmis, nurodytomis incidentų valdymo procedūros dalyse, skirtose incidentų suvaldymui ir likvidavimui bei veiklos po incidentų atkūrimui.

3.11 Veiklos tęstinumo valdymas

3.11.1 Bendrieji principai

„Dokobit“ įdiegė veiklos atkūrimo po ekstremaliųjų įvykių / veiklos tęstinumo valdymo planą ir yra įtraukta į grupės krizių valdymo tvarką, kuris yra „Signicat“ grupės ISVS dalis. Šio plano tikslas yra aiškiai apibrėžti, kaip „Dokobit“ atkurs savo paslaugas per nustatytą terminą įvykus ekstremaliajam ar kitam katastrofiniam įvykiui, nustatytam atliekant rizikos vertinimą, ir užbaigs paslaugų atkūrimą per nustatytą atkūrimo laiko tikslą (RTO) ir atkūrimo taško tikslą (RPO). Plane aiškiai nurodytos funkcijos ir atsakomybės bei kiekvienos paslaugos planui būdingos aplinkybės, kurioms atsiradus paslaugos automatiškai atkuriamos alternatyvioje iš anksto parinktoje vietoje.

Veiklos atkūrimo po ekstremaliųjų įvykių / veiklos tęstinumo plane išdėstyti visi aktualūs informacijos saugumo tęstinumo aspektai, kurie įtraukti į susijusias procedūras. Šie aspektai apibūdinti atskirame skyriuje „Informacijos saugumo tęstinumo aspektai“.

Veiklos atkūrimo po ekstremaliųjų įvykių / veiklos tęstinumo planas sukurtas remiantis tam tikram turtui aktualiais rizikos scenarijais, nustatytais atliekant rizikos vertinimą. Remiantis saugumo reikalavimais, veiklos atkūrimo po ekstremaliųjų įvykių / veiklos tęstinumo plane nustatyti informacijos, reikalingos veiklai palaikyti sutrikimo metu, RTO ir RPO tikslai.

Dėl „Dokobit“ veiklos pobūdžio teikiant debesijos infrastruktūra pagrįstas paslaugas informacijos saugumas yra atsparus trikdantiems įvykiams.

3.11.2 Atsarginis kopijavimas

Operacijų saugumo politikoje apibrėžiami reikalavimai ir įprastinės veiklos, susijusios su informacijos atsarginėmis kopijomis. „Dokobit“ kuria visų internetu pasiekiamų produktų ir klientams teikiamų paslaugų atsargines kopijas. Atsarginių kopijų kūrimo procesas yra automatizuotas, suderintas su atkūrimo tikslais ir išbandytas, kad būtų laikomasi paskelbtų RPO ir RTO, reikalingų paslaugoms atkurti nutrūkus ar įvykus nelaimei. Atsarginių kopijų vientisumo tikrinimas ir testavimas yra rutininių operacijų dalis.

3.11.3 Krizių valdymas

Tai numatyt „Signicat“ grupės krizių valdymo plane. Taip pat, „Dokobit“ grėsmių žvalgybos procesai skirti ankstyvam grėsmių, kurios potencialiai gali sukelti krizę, aptikimui.

3.12 TSP nutraukimas ir nutraukimo planai

„Dokobit“ turi aktualų paslaugų nutraukimo planą pagal ETSI EN 319 401 7.12 punktą. Į nutraukimo planą įtraukiamos procedūros, kaip informuoti visas susijusias šalis apie nutraukimą, ir nuostatos, užtikrinančios tęstinį reikiamos informacijos prieinamumą.

„Dokobit“ turi papildomų trečiųjų šalių garantijas, kad bus padengiamos išlaidos, susijusios su šių minimalių reikalavimų vykdymu, jei TSP bankrutuotų arba jei dėl kitų priežasčių negalėtų padengti išlaidų pati.

„Dokobit“ pasilieka teisę nutraukti patvirtinimo paslaugos teikimą, apie tai pranešus Paslaugos gavėjams ir Priežiūros įstaigai ne mažiau kaip prieš 3 mėnesius.

3.13 Atitiktis

„Signicat“ grupės ISVS šią sritį apima Atitikties politika. Procedūros apraše nustatomas suinteresuotųjų šalių atpažinties procesas, nurodomi teisiniai, norminiai, sutartiniai ir kiti reikalavimai ir jų vykdymo atsakomybės. Teisiniai ir standartiniai dokumentai, kurie yra svarbūs kvalifikuotos galiojimo patvirtinimo paslaugos atitikčiai, išvardyti šio praktinių nuostatų aprašo pradžioje. Prieiga žmonėms su negalia yra visų „Dokobit“ paslaugų atitikties reikalavimas.

3.14 Tiekimo grandinė

„Signicat“ grupės ISVS apima tiekėjų valdymo politiką, taikomą visų tiekėjų atrankai ir valdymui. Tiekimo grandinės vientisumo patikros užtikrina, kad trečiųjų šalių komponentų, naudojamų „Dokobit“ paslaugose, programinis kodas ir dvejetainės programos būtų patikrintos ir išlaikytų atestavimo testus. Atliekamas visų tiekėjų saugumo vertinimas, kuris apima ir susijusius subtiekėjus.

Visos sutartys su tiekėjais turi priskirtą atsakingą asmenį, kuris yra atsakingas už reguliarius (dažniausiai kasmetinius) tiekėjų būklės patikrinimus. Esant sutarties pažeidimo požymių ar padidėjus rizikai, sutarties atsakingas asmuo gali prašyti atlikti tiekėjo auditą.

Laikydamasi BDAR, „Dokobit“ pasirašo Duomenų tvarkymo sutartis su pagalbiniais duomenų tvarkytojais (pasirašoma standartinė sutartis arba peržiūrėta subtvarkytojo sutartis).

4 Patvirtinimo paslaugos struktūra

Šia paslauga gali naudotis tik sutartis su „Dokobit“ sudarę klientai. Paslauga prieinama tik naudojant galiojimo patvirtinimo paslaugos teikėjo sąsajas ir programas.

Paslaugos abonentas privalo saugoti paslaugos sąsają nuo neteisėto naudojimo ir užtikrinti reikiamą saugumą naudodamasis paslaugomis. Tai taikoma visoms sąsajoms, naudojamoms norint pasiekti paslaugą.

Ši sąsaja visų pirma reiškia žiniatinklio programą, skirtą paslaugai naudoti, arba bet kurią programą ar integracijos sąsają, kurią pateikia tik „Dokobit“ arba paslaugos teikėjo nurodytas integruotojas.

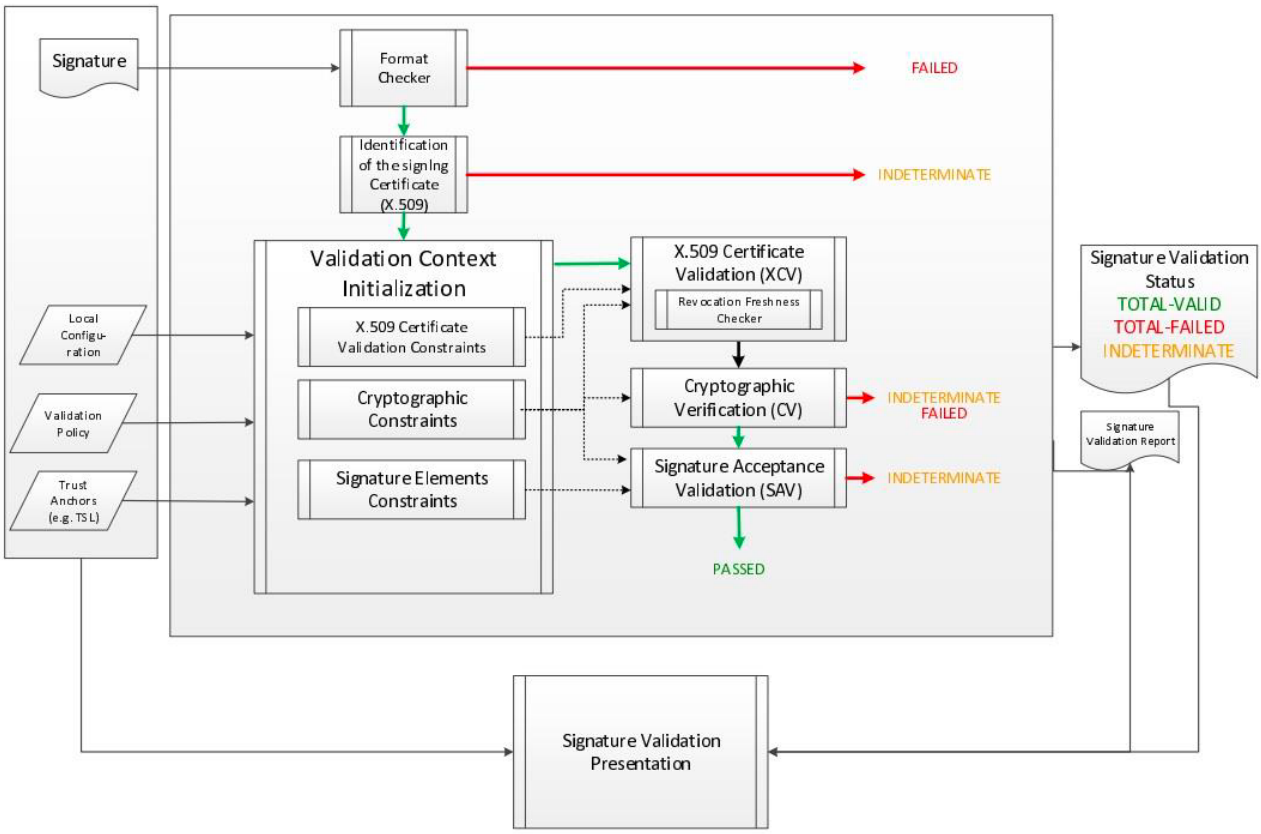
4.1 Parašo galiojimo patvirtinimo proceso reikalavimai

„Dokobit“ galiojimo patvirtinimo paslaugos procedūros, skirtos nustatyti, ar elektroninis parašas arba elektroninis spaudas yra techniškai galiojantis, grindžiamos procesu, aprašytu ETSI EN 319 102-1.

Toliau paaiškinama, kaip „Dokobit“ galiojimo patvirtinimo paslauga vykdo atskirus patvirtinimo procedūrų komponentus, ir nurodomi atsirandantys procesai ir apribojimai. Kai šiame dokumente nenustatytas joks specialus reikalavimas, taikomi visi ETSI EN 319 102-1 5 punkto reikalavimai ir taisyklės.

Kai šioje specifikacijoje nustatyti konkretūs reikalavimai ir taisyklės, jie turi pirmenybę prieš atitinkamus ETSI EN 319 102-1 reikalavimus. Esant neatitikimų tarp šios specifikacijos ir ETSI EN 319 102-1 specifikacijų, pirmenybė teikiama šiai specifikacijai.

4.1.1 Parašo galiojimo patvirtinimo modelis



Pagal minėtoje specifikacijoje apibrėžtą Parašo galiojimo patvirtinimo koncepcinį modelį, „Dokobit“ Galiojimo patvirtinimo paslauga veikia kaip parašo Galiojimo patvirtinimo programa (SVA). Ją įjungia Aktyvavimo programa (DA). SVA turi grąžinti DA galiojimo patvirtinimo proceso rezultatus galiojimo patvirtinimo ataskaitos forma.

Aktyvavimo programa (DA) „Dokobit“ Galiojimo patvirtinimo paslaugai gali būti:

- „Dokobit“ portalas – pasiekiamas adresu *https://app.dokobit.com*;
- „Dokobit“ Galiojimo patvirtinimo paslauga – pasiekiama adresu *https://validation.dokobit.com* ir per integracijas į kitas informacijos sistemas;
- „Dokobit Gateway“ – pasiekiamas adresu *https://gateway.dokobit.com*;
- „Dokobit“ Galiojimo patvirtinimo paslaugos API.

„Dokobit“ Galiojimo patvirtinimo paslauga priima tvirtinti tik vieną failą, kuris turėtų būti su parašais ir pasirašytais turinio failais.

4.1.2 Parašo galiojimo patvirtinimo proceso būsenos indikacija ir parašo galiojimo patvirtinimo ataskaita

„Dokobit“ galiojimo patvirtinimo paslauga apima išsamią galiojimo patvirtinimo ataskaitą, leidžiančią DA patikrinti išsamią informaciją apie sprendimus, priimtus patikrinimo metu, ir ištirti išsamias paslaugos nurodomos būsenos indikacijos priežastis.

„Dokobit“ portalas, „Dokobit“ Galiojimo patvirtinimo paslauga ir „Dokobit Gateway“ pateikia ataskaitą naudotojui suprantamu būdu – žmonėms įskaitomame HTML puslapyje su galimybe atsisiųsti spaudu patvirtintą parašo galiojimo patvirtinimo ataskaitą.

Parašo galiojimo patvirtinimo proceso išvestį sudaro šie elementai:

- parašų sąrašas;
- būsena, nurodanti parašo galiojimo patvirtinimo proceso rezultatus;
- klaidos, nurodančios, kodėl parašas negalioja (TOTAL-FAILED), arba įspėjimai, paaiškinantys, kodėl SVS negalėjo nustatyti parašo būsenos (INDETERMINATE);
- nuoroda į politiką, kuria patvirtintas parašas;
- jei pasirašymo metu buvo naudojamas slapyvardis, tai yra aiškiai nurodoma pasikliaujančiajai šaliai.

Pagal algoritmą, nurodytą ETSI EN 319 102-1, parašo patvirtinimo būsena gali būti viena iš nurodytųjų toliau.

1 lentelė. Galiojimo patvirtinimo ataskaitos struktūra ir semantika

Būklės indikacija	Semantika	Susiję Galiojimo patvirtinimo ataskaitos duomenys
TOTAL-PASSED	Parašo galiojimo patvirtinimo proceso rezultatas yra TOTAL-PASSED, remiantis šiais argumentais: • pavyko atlikti kriptografinius parašo patikrinimus (įskaitant netiesiogiai pasirašytų atskirų duomenų objektų santraukos patikrinimą); • visi pasirašančiojo asmens tapatybės sertifikavimui taikomi apribojimai buvo patvirtinti (t. y. pasirašymo sertifikatas buvo pripažintas patikimu); • parašas buvo patvirtintas atsižvelgiant į patvirtinimo apribojimus, todėl laikomas atitinkančiu šiuos apribojimus.	Galiojimo patvirtinimo proceso rezultatas yra pasirašymo sertifikatas, naudotas galiojimo patvirtinimo procese, kartu su konkrečiu požymiu, jei jis yra, ir patvirtinimo įrodymais, į kuriuos atsižvelgta.
TOTAL-FAILED	Parašo galiojimo patvirtinimo proceso rezultatas yra TOTAL-FAILED, nes nepavyko atlikti kriptografinių parašo patikrinimų (įskaitant netiesiogiai pasirašytų atskirų duomenų objektų santraukos patikrinimą) arba buvo įrodyta, kad parašas buvo sugeneruotas po pasirašymo sertifikato panaikinimo.	Galiojimo patvirtinimo proceso metu kaip išvestis pateikiama papildoma informacija, paaiškinanti TOTAL-FAILED indikaciją dėl kiekvieno patvirtinimo apribojimo, į kurį buvo atsižvelgta ir dėl kurio buvo gautas neigiamas rezultatas.

Būklės indikacija	Semantika	Susiję Galiojimo patvirtinimo ataskaitos duomenys
INDETERMINATE	Turimos informacijos nepakanka, kad būtų galima nustatyti, ar parašo būsena turi būti TOTAL-PASSED, ar TOTAL-FAILED.	Galiojimo patvirtinimo procese kaip išvestis pateikiama papildoma informacija, siekiant paaiškinti INDETERMINATE indikaciją ir padėti vertintojui nustatyti, kokių duomenų trūksta galiojimo patvirtinimo procesui užbaigti.

Be pagrindinės būsenos, parašo galiojimo patvirtinimo ataskaitoje pateikiama antrinė indikacija, kurios semantika yra tokia, kaip nurodyta toliau.

2 lentelė. Galiojimo patvirtinimo ataskaitos struktūra ir semantika

Pagrindinė indikacija	Antrinė indikacija	Susiję galiojimo patvirtinimo ataskaitos duomenys	Semantika
TOTAL-FAILED	FORMAT_FAILURE	Kaip galiojimo patvirtinimo proceso išvestis pateikiama visa turima informacija, kodėl nepavyko išnagrinėti parašo.	Parašas neatitinka vieno iš bazinių standartų tiek, kad kriptografinės patikros blokas negali jo apdoroti.
	HASH_FAILURE	Kaip galiojimo patvirtinimo proceso išvestis pateikiami šie duomenys: identifikatorius (-iai) (pvz., URI arba OID), vienareikšmiškai identifikuojantis (-ys) pasirašyto duomenų objekto elementą (pvz., parašo požymius ar SD), dėl kurio vykdymas nepavyko.	Parašo patvirtinimo proceso rezultatas yra TOTAL-FAILED, nes bent viena pasirašyto duomenų objekto (-ų) santrauka, įtraukta į pasirašymo procesą, neatitinka atitinkamos parašo santraukos vertės.
	SIG_CRYPTO_FAILURE	Kaip patvirtinimo proceso išvestis pateikiamas pasirašymo sertifikatas, naudotas patvirtinimo procese.	Parašo patvirtinimo proceso rezultatas yra TOTAL-FAILED, nes parašo vertė paraše negalėjo būti patikrinta naudojant pasirašančiojo asmens viešąjį raktą pasirašymo sertifikate.
	REVOKED	Kaip galiojimo patvirtinimo proceso išvestis pateikiami šie duomenys: • sertifikatų seka, naudota galiojimo patvirtinimo procese; • pasirašymo sertifikato panaikinimo laikas ir, jei yra, priežastis.	Parašo galiojimo patvirtinimo proceso rezultatas yra TOTAL-FAILED, nes: • pasirašymo sertifikatas buvo panaikintas; ir • yra įrodymų, kad parašas sukurtas po panaikinimo laiko.

Pagrindinė indikacija	Antrinė indikacija	Susiję galiojimo patvirtinimo ataskaitos duomenys	Semantika
	EXPIRED	Kaip proceso išvestis pateikiama patvirtinta sertifikatų seka.	Parašo galiojimo patvirtinimo proceso rezultatas yra TOTAL-FAILED, nes yra įrodymų, kad parašas sukurtas pasibaigus pasirašymo sertifikato galiojimo laikui (*notAfter*).
	NOT_YET_VALID		Parašo galiojimo patvirtinimo proceso rezultatas yra TOTAL-FAILED, nes yra įrodymų, kad parašas sukurtas prieš pasirašymo sertifikato išdavimo datą (*notBefore*).
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	Kaip galiojimo patvirtinimo proceso išvestis pateikiamas apribojimų rinkinys, kurio parašas neatitinka.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes vienas ar keli parašo požymiai neatitinka patvirtinimo apribojimų.
	CHAIN_CONSTRAINTS_FAILURE	Kaip galiojimo patvirtinimo proceso išvestis pateikiama: • sertifikatų seka, naudota galiojimo patvirtinimo procese; • apribojimų rinkinys, kurio seka neatitinka.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes patvirtinimo procese naudota sertifikato seka neatitinka su sertifikatu susijusių patvirtinimo apribojimų.
	CERTIFICATE_CHAIN_GENERAL_FAILURE	Kaip galiojimo patvirtinimo proceso išvestis pateikiama papildoma informacija apie priežastį.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes sekai tvirtinti prieinamų sertifikatų rinkinys sukėlė klaidą, kurios priežastis nenustatyta.
	CRYPTO_CONSTRAINTS_FAILURE	Kaip proceso išvestis pateikiama: • Medžiagos (parašo, sertifikato), sukurtos naudojant algoritmą ar rakto dydį, kurio saugumas mažesnis nei reikalaujamas kriptografinio saugumo lygis, atpažinties duomenys; • Jei žinoma, laikas, iki kurio algoritmas ar rakto dydis buvo laikomas saugiu.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes bent vienas iš algoritmų, kurie buvo naudojami medžiagoje (pvz., parašo vertė, sertifikatas ir t. t.), naudotas patvirtinant parašą, arba rakto, naudoto su tokiu algoritmu, dydis neatitinka reikalaujamo kriptografinio saugumo lygio ir: • ši medžiaga buvo sukurta po laiko, iki kurio šis algoritmas (raktas) buvo laikomas saugiu (jei toks laikas yra žinomas), ir • medžiaga nėra apsaugota pakankamai stipria laiko žyma, uždėta prieš laiką, iki kurio algoritmas (raktas) buvo laikomas saugiu (jei toks laikas žinomas).

Pagrindinė indikacija	Antrinė indikacija	Susiję galiojimo patvirtinimo ataskaitos duomenys	Semantika
	POLICY_PROCESSING_ERROR	Galiojimo patvirtinimo procesas suteikia papildomos informacijos apie problemą.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes nurodytas oficialios politikos failas negalėjo būti apdorojamas dėl kokių nors priežasčių (pvz., neprieinamas, negalimas nagrinėti, su neatitikimais ir pan.).
	SIGNATURE_POLICY_NOT_AVAILABLE		Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes nėra elektroninio dokumento, kuriame būtų pateikiama išsami informacija apie politiką.
	TIMESTAMP_ORDER_FAILURE	Kaip galiojimo patvirtinimo proceso išvestis pateikiamas laiko žymų, neatitinkančių tvarkos apribojimų, sąrašas.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes nesilaikoma kai kurių parašo laiko žymų ir (arba) pasirašytų duomenų objekto (-ų) laiko žymų tvarkos apribojimų.
	NO_SIGNING_CERTIFICATE_FOUND		Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes nepavyksta identifikuoti pasirašymo sertifikato.
	NO_CERTIFICATE_CHAIN_FOUND		Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes nerasta su atpažintu pasirašymo sertifikatu susijusios sertifikato sekos.
	REVOKED_NO_POE	Kaip galiojimo patvirtinimo proceso išvestis pateikiama: • sertifikatų seka, naudota galiojimo patvirtinimo procese; • pasirašymo sertifikato panaikinimo laikas ir priežastis.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes pasirašymo sertifikatas buvo panaikintas konkrečią patvirtinimo datą ar konkrečiu patvirtinimo laiku. Tačiau parašo patvirtinimo algoritmas negali nustatyti, ar pasirašymo laikas yra prieš, ar po panaikinimo laiko.
	REVOKED_CA_NO_POE	Kaip galiojimo patvirtinimo proceso išvestis pateikiama: • sertifikatų seka, apimanti panaikintą CA sertifikatą; • sertifikato panaikinimo laikas ir priežastis.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes bent viena sertifikatų seka rasta, tačiau panaikintas tarpinis CA sertifikatas.

Pagrindinė indikacija	Antrinė indikacija	Susiję galiojimo patvirtinimo ataskaitos duomenys	Semantika
	OUT_OF_BOUNDS_NOT_REVOKED		Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes pasirašymo sertifikato galiojimo laikas pasibaigė arba sertifikatas patvirtinimo metu dar negalioja, o Parašo galiojimo patvirtinimo algoritmas negali nustatyti, ar pasirašymo laikas patenka į pasirašymo sertifikato galiojimo laiko intervalą. Žinoma, kad sertifikatas nėra panaikintas.
	OUT_OF_BOUNDS_NO_POE		Parašo galiojimo patvirtinimo procesas yra INDETERMINATE, nes pasirašymo sertifikato galiojimo laikas pasibaigė arba sertifikatas patvirtinimo metu dar negaliojo, o Parašo galiojimo patvirtinimo algoritmas negali nustatyti, kad pasirašymo laikas patenka į pasirašymo sertifikato galiojimo laiko intervalą.
INDETERMINATE	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	Proceso išvestis: • Medžiagos (parašo, sertifikato), sukurtos naudojant kriptografinio saugumo lygio neatitinkantį algoritmą ar rakto dydį, identifikavimas. Jei žinoma, laikas, iki kurio algoritmas ar rakto dydis buvo laikomas saugiu.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes bent vienas iš algoritmų, kurie buvo naudojami objektuose (pvz., parašo vertė, sertifikatas ir t. t.), susijusiuose su parašo patvirtinimu, arba rakto, naudoto su tokiu algoritmu, dydis neatitinka reikalaujamo kriptografinio saugumo lygio ir nėra įrodymų, kad ši medžiaga buvo sukurta anksčiau laiko, iki kurio šis algoritmas (raktas) buvo laikomas saugiu.
	NO_POE	• Galiojimo patvirtinimo procese turi būti nustatyti bent jau tie pasirašyti objektai, kurių POE trūksta. • Galiojimo patvirtinimo procesas turėtų suteikti papildomos informacijos apie problemą.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes trūksta įrodymų, kad būtų galima nustatyti, ar pasirašytas objektas buvo sukurtas prieš kokį nors pavojų keliantį įvykį (pvz., algoritmo pažeidimas).
	TRY_LATER	Galiojimo patvirtinimo proceso išvestis: laikas, kai tikimasi gauti reikiamą panaikinimo informaciją.	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes ne visus apribojimus galima įvykdyti naudojant turimą informaciją. Tačiau gali būti įmanoma tai padaryti naudojant papildomą panaikinimo informaciją, kuri bus prieinama vėliau.

Pagrindinė indikacija	Antrinė indikacija	Susiję galiojimo patvirtinimo ataskaitos duomenys	Semantika
	SIGNED_DATA_NOT_FOUND	Kai įmanoma, proceso išvestis turėtų būti tokia: pasirašytų duomenų, sukėlusių klaidą, identifikatorius (-iai) (pvz., URI).	Parašo galiojimo patvirtinimo proceso rezultatas yra INDETERMINATE, nes nepavyksta gauti pasirašytų duomenų.

- „Dokobit“ kiekvienai politikai priskiria objekto identifikatorių (OID) ir palaiko dvi galiojimo patvirtinimo politikas:

Galiojimo patvirtinimo politika	Objekto identifikatorius
QES galiojimo patvirtinimo politika • Griežtesnis galiojimo patvirtinimas: reikalingi galiojantys Kvalifikuoti elektroniniai parašai ir spaudai. Pagal ES reglamentą Nr. 910/2014 (*eIDAS*) kvalifikuoti elektroniniai parašai turi tokią pačią teisinę galią kaip ir ranka rašyti parašai. Ši politika yra numatytoji „Dokobit“ Galiojimo patvirtinimo paslaugos API programoje. *Išsamūs galiojimo patvirtinimo apribojimai apibrėžti 1 priede.*	1. 3.6.1.4.1.54720.1.2
AdES galiojimo patvirtinimo politika • Pradinis patvirtinimas: patikrinama, ar dokumentas nebuvo pakeistas, ir pateikiama būtinoji informacija apie elektroninių parašų ir spaudų teisinį pobūdį ir galiojimo patvirtinimą pagal ES reglamentą Nr. 910/2014 (*eIDAS*). Ši politika yra numatytoji „Dokobit“ portale ir „Dokobit Gateway“. *Išsamūs galiojimo patvirtinimo apribojimai apibrėžti 2 priede.*	1. 3.6.1.4.1.54720.1.3

- Galiojimo patvirtinimo paslauga nepriima kitų patvirtinimo politikos šaltinių;
- Parašo galiojimo patvirtinimo politikos negalima nepaisyti ir pakeisti parašo galiojimo patvirtinimo taisyklėmis pagal protokolą, nurodytą ETSI TS 119 442;
- Galiojimo patvirtinimo procesas užtikrina, kad naudojama parašo galiojimo patvirtinimo politika atitiktų SVS politikoje apibrėžtą strategiją arba galiojimo patvirtinimo paslaugos naudojimo sąlygas;
- SVS politikoje apibrėžtoje strategijoje arba SVS naudojimo sąlygose laikomasi šių principų:
  - Pagal tą pačią įvestį, įskaitant galiojimo patvirtinimo politiką, parašo galiojimo patvirtinimo paslauga pateiks tą pačią išvestį.
  - Kaip parašo egzistavimo įrodymą SVS gali priimti skirtingus elementus.

4.1.3 Galiojimo patvirtinimo procesas

„Dokobit“ galiojimo patvirtinimo paslauga palaiko Pagrindinių parašų galiojimo patvirtinimo procesą ir Parašų su laiko žyma bei parašų su ilgalaikio galiojimo patvirtinimo duomenimis galiojimo patvirtinimo procesą. Nėra galimybės nurodyti procesą, kurį DA turėtų naudoti kitoms paslaugoms. Patvirtinant parašo ar spaudo galiojimą, „Dokobit“ galiojimo patvirtinimo paslauga veikia taip:

1. SVA vykdo visų parašų Galiojimo patvirtinimo procesą, nepriklausomai nuo jų lygio.
2. Kai galiojimo patvirtinimo būsena, kurią nurodo pasirinktas patvirtinimo procesas, nurodo būsenos indikaciją PASSED, SVA pateikia DA būsenos indikaciją TOTAL-PASSED.

3. Kai galiojimo patvirtinimo būsena, kurią nurodo pasirinktas patvirtinimo procesas, nurodo būsenos indikaciją FAILED, SVA pateikia DA būsenos indikaciją TOTAL-FAILED.
4. Kitu atveju SVA pateikia būsenos indikaciją INDETERMINATE.

„Dokobit“ galiojimo patvirtinimo paslauga palaiko ETSI formatų standartuose nurodytus formatus:

1. ETSI EN 319 122-1 (2023-06) Elektroniniai parašai ir infrastruktūros (ESI); CAdES skaitmeniniai parašai; 1 dalis: Struktūriniai elementai ir CAdES baziniai parašai
2. ETSI EN 319 132-1 (2024-07) Elektroniniai parašai ir patikimumo infrastruktūros (ESI); XAdES skaitmeniniai parašai; 1 dalis: Struktūriniai elementai ir XAdES baziniai parašai
3. ETSI EN 319 142-1 (2024-01) Elektroniniai parašai ir infrastruktūros (ESI); PAdES skaitmeniniai parašai; 1 dalis: Struktūriniai elementai ir PAdES baziniai parašai
4. ETSI EN 319 162-1 (2016-04) Elektroniniai parašai ir infrastruktūros (ESI); Susijusios parašo talpyklos (ASiC); 1 dalis: Struktūriniai elementai ir ASiC bazinės talpyklos

„Dokobit“ deda geriausias pastangas, kad galiojimo patvirtinimo paslauga palaikytų pirmiau minimų dokumentų 2-osiose dalyse (papildomuose profiliuose) bei ankstesnėse šių standartų versijose nurodytus formatų standartus. „Dokobit“ deda geriausias pastangas, kad galiojimo patvirtinimo paslauga palaikytų ir kitus parašo formatus.

Atsižvelgiant į ES teisės aktus [CID (EU) 2015/1506] taikomi ir su „Dokobit“ galiojimo patvirtinimo paslauga yra suderinami šie elektroninio parašo ir elektroninio spaudo formatai:

1. ETSI TS 103 171 V2.1.1 (2012-03) Elektroniniai parašai ir infrastruktūra (ESI); XAdES pradinis profilis
2. ETSI TS 103 172 V2.2.2 (2013-04) Elektroniniai parašai ir infrastruktūra (ESI); PAdES pradinis profilis
3. ETSI TS 103 173 V2.1.1 (2012-03) Elektroniniai parašai ir infrastruktūra (ESI); CAdES pradinis profilis
4. ETSI TS 103 174 V2.2.1 (2013-06) Elektroniniai parašai ir infrastruktūra (ESI); ASiC pradinis profilis

Galiojimo patvirtinimo procesą „Dokobit“ portale sudaro šie etapai:

1. Abonentas autentifikuojasi Paslaugai naudojant elektroninės atpažinties priemonę.
2. Abonentas pasirenka galiojimo patvirtinimo politiką ir įkelia elektroniniu būdu pasirašytą dokumentą. „Dokobit“ galiojimo patvirtinimo paslauga leidžia naudoti QES galiojimo patvirtinimo politiką arba *AdES* galiojimo patvirtinimo politiką;
3. „Dokobit“ galiojimo patvirtinimo paslauga patvirtina dokumentą pagal ETSI EN 319 102-1, naudodama pasirinktą patvirtinimo politiką.
4. Abonentui pateikiama ataskaita;

Galiojimo patvirtinimo procesas „Dokobit“ Galiojimo patvirtinimo paslaugoje apima šiuos veiksmus:

1. Abonentas autentifikuojasi Paslaugai naudojant elektroninės atpažinties priemonę;
2. Abonentas įkelia arba pasirenka elektroniniu būdu pasirašytą dokumentą ir pasirenka galiojimo patvirtinimo politiką. „Dokobit“ galiojimo patvirtinimo paslauga leidžia naudoti QES galiojimo patvirtinimo politiką arba *AdES* galiojimo patvirtinimo politiką;
3. „Dokobit“ galiojimo patvirtinimo paslauga patvirtina dokumentą pagal ETSI EN 319 102-1 ir naudojant pasirinktą patvirtinimo politiką.
4. Abonentui pateikiama ataskaita.

Patvirtinimo procesas „Dokobit Gateway“ ir „Dokobit“ galiojimo patvirtinimo paslaugos API programoje apima šiuos veiksmus:

1. Abonentas įkelia elektroniniu būdu pasirašytą dokumentą ir pasirenka norimą galiojimo patvirtinimo politiką. „Dokobit“ galiojimo patvirtinimo paslauga leidžia naudoti QES galiojimo patvirtinimo politiką arba *AdES* galiojimo patvirtinimo politiką.
2. „Dokobit“ galiojimo patvirtinimo paslauga patvirtina dokumentą pagal ETSI EN 319 102-1, naudodama pasirinktą patvirtinimo politiką.
3. JSON atsakyme, apimančiame parašų sąrašą ir parašo galiojimo patvirtinimo klaidų ar įspėjimų sąrašą, pateikiama ataskaita.

4.1.4 Elektroniniu būdu pasirašytų dokumentų galiojimo patvirtinimo apribojimai

„Dokobit“ galiojimo patvirtinimo paslaugos patvirtinimo apribojimai yra aiškiai apibrėžti konkrečiuose sistemos valdymo duomenyse ir pačioje vykdymo procedūroje.

Bet kokie galiojimo patvirtinimo apribojimai, kurie nepaaiškėja per vykdymo procedūrą, kyla iš paties parašo turinio tiesiogiai (yra pasirašymo atributuose) arba netiesiogiai, tai yra nurodant į išorinį dokumentą, pateiktą mašininiu būdu apdorojama forma. DA gali pateikti papildomų apribojimų SVA per programos ar naudotojo pasirinktus parametrus.

Šis papildomas apribojimas galėtų būti pateikiamas abipusiu „Dokobit“ galiojimo patvirtinimo paslaugų teikėjo ir pasikliaujančiosios šalies susitarimu.

Bendrieji apribojimai

„Dokobit“ galiojimo patvirtinimo paslauga palaiko toliau nurodytus bendruosius apribojimus.

Apribojimas	Apribojimo reikšmė patvirtinant parašą (SVA arba DA)
Maksimalus palaikomų dokumentų failo dydis	300 MB („Dokobit“ Galiojimo patvirtinimo paslaugos API, „Dokobit Gateway“), 100MB („Dokobit“ portalas)

X.509 Galiojimo patvirtinimo apribojimai

„Dokobit“ galiojimo patvirtinimo paslauga palaiko šiuos X.509 galiojimo patvirtinimo apribojimus, kurie nurodo naudojimo reikalavimus sertifikato kelio patvirtinimo procese, kaip nurodyta ETSI TS 119 172-1 A.4.2.1 punkto A.2 lentelės (m) eilutėje.

Apribojimas (-ai)	Apribojimo vertė patvirtinant parašą (SVA arba DA)
(m)1. *X509CertificateValidationConstraints*. Šis apribojimų rinkinys nurodo naudojimo reikalavimus sertifikato kelio patvirtinimo procese, kaip apibrėžta IETF RFC 5280. Šie apribojimai gali būti skirtingi skirtingiems sertifikatų tipams (pvz., sertifikatai, išduodami pasirašiusiajam, CA, OCSP užklausų adresatams, CRL Išdavėjams, Laiko žymų įrenginiams). Galimų reikalavimų verčių, naudojamų tokiems reikalavimams išreikšti, semantika apibrėžiama taip: (m)1.1. *SetOfTrustAnchors*. Šis apribojimas nurodo priimtinų patikimumo požymių rinkinį (TAs) kaip patvirtinimo proceso apribojimą.	EU TSL UA TSL
(m)1.2. *CertificationPath.* Šis apribojimas nurodo sertifikavimo kelią, kurį SVA turi naudoti parašo galiojimui patvirtinti. Sertifikato kelio ilgis yra „n“ nuo patikimumo požymio (TA) iki sertifikato, naudojamo patvirtinant pasirašytą objektą (pvz., pasirašiusiojo sertifikatą arba laiko žymos sertifikatą). Šis apribojimas gali apimti kelią, į kurį reikia atsižvelgti, arba gali nurodyti, kad reikia atsižvelgti į kelią, nurodytą paraše, jei toks yra. • (m)1.3. *user-initial-policy-set.* Šis apribojimas aprašytas IETF RFC5280 6.1.1 punkto c papunktyje. • (m)1.4. *initial-policy-mapping-inhibit*. Šis apribojimas aprašytas IETF RFC 5280 6.1.1 punkto e papunktyje. • (m)1.5. *initial-explicit-policy*. Šis apribojimas aprašytas IETF RFC 5280 6.1.1 punkto f papunktyje. • (m)1.6. *initial-any-policy-inhibit.* Šis apribojimas aprašytas IETF RFC 5280 6.1.1 punkto g papunktyje. • (m)1.7. *initial-permitted-subtrees.* Šis apribojimas aprašytas IETF RFC 5280 6.1.1 punkto h papunktyje. • (m)1.8. *initial-excluded-subtrees*. Šis apribojimas aprašytas IETF RFC 5280 6.1.1 punkto i papunktyje. • (m)1.9. *path-length-constraints*. Šis apribojimas nurodo CA sertifikatų skaičiaus apribojimus sertifikavimo kelyje. Tam gali tekti apibrėžti pradines vertes arba su tokiu apribojimu elgtis kitaip (pvz., ignoruoti). • (m)1.10. *policy-constraints*. Šis apribojimas nurodo reikalavimus, taikomus sertifikatų politikai, nurodytai sertifikatuose. Tam gali tekti apibrėžti pradines vertes arba su tokiu apribojimu elgtis kitaip (pvz., ignoruoti). Tai taip pat turėtų suteikti galimybę reikalauti konkretaus sertifikato politikos pratęsimo vertės (-ių) (galimo jų rinkinio) galutinio subjekto sertifikatuose (nereikalaujant, kad tokios vertės būtų nurodytos valdžios institucijų sertifikatų sertifikavimo kelyje).	Nėra

Apribojimas (-ai)	Apribojimo vertė patvirtinant parašą (SVA arba DA)
(m)2. *RevocationConstraints*. Šis apribojimų rinkinys nurodo reikalavimus, taikomus tikrinant sertifikatų galiojimo būseną sertifikato kelio patvirtinimo proceso metu. Šie apribojimai skirtingiems sertifikatų tipams gali būti skirtingi (pvz., sertifikatai, išduodami pasirašiusiajam, CA, OCSP užklausų gavėjams, CRL Išdavėjams, Laiko žymų įrenginiams). Galimų reikalavimų verčių, naudojamų tokiems reikalavimams išreikšti, semantika apibrėžiama taip: (m)2.1. *RevocationCheckingConstraints*. Šis apribojimas nurodo sertifikato panaikinimo tikrinimo reikalavimus. Tokie apribojimai gali nurodyti, ar reikia panaikinimo tikrinimo, ar ne, ir ar reikia naudoti OCSP atsakymus, ar CRL. Galimų reikalavimų verčių, naudojamų tokiems reikalavimams išreikšti, semantika apibrėžiama taip: • *clrCheck*. Tikrinama pagal esamus CRL (arba Institucijos panaikinimo sąrašus). • *ocspCheck*. Panaikinimo būsena tikrinama naudojant OCSP IETF RFC 6960. • *bothCheck*. Turi būti atliekami ir OCSP, ir CRL patikrinimai. • *eitherCheck*. Turi būti atliekami arba OCSP, arba CRL patikrinimai. • *noCheck*. Nėra privalomas joks patikrinimas.	*eitherCheck*
(m)2.2. *RevocationFreshnessConstraints.* Šis apribojimas nurodo panaikinimo informacijos laiko reikalavimus. Apribojimai gali reikšti maksimalų priimtą skirtumą tarp sertifikato panaikinimo būsenos informacijos išdavimo datos ir patvirtinimo laiko arba reikalavimą, kad SVA priimtų panaikinimo informaciją tik tam tikrą laiką po to, kai buvo sukurtas parašas.	Nėra
(m)2.3. *RevocationInfoOnExpiredCerts*. Šis apribojimas įpareigoja, kad pasirašančiojo asmens sertifikatas, naudojamas patvirtinant parašą, būtų išduotas sertifikavimo institucijos, kuri saugo pranešimus apie panaikintus sertifikatus net kai jų galiojimo pabaigos laikotarpis viršija nurodytą žemiausią ribą.	Nėra
(m)3. *LoAOnTSPPractices*. Šis apribojimas nurodo reikiamą *LoA* dėl praktikos, kurią įgyvendina TSP, išdavusi (-ios) sertifikatus, kuriuos reikia patvirtinti sertifikato kelio patvirtinimo procese, t. y. sertifikatus, esančius pasirašančiojo asmens sertifikato kelyje, ir pasirinktinai tuos sertifikatus, kurie yra visose arba kurioje nors kitoje sertifikato sekoje.	Nėra

1. Remiantis ETSI 119 172-1 C priedu. Šie apribojimai nurodo reikalavimus specifiniams sertifikatų metaduomenims, kurių semantika taikoma ES teisės aktų kontekste:
a) *EUQualifiedCertificateRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti kvalifikuotas sertifikatas, kaip apibrėžta galiojančiuose ES teisės aktuose; išreiškiamas kaip loginis.
b) *EUQualifiedCertificateSigRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti kvalifikuotas elektroninio parašo sertifikatas, kaip apibrėžta *eIDAS*; išreiškiamas kaip loginis.
c) *EUQualifiedCertificateSealRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti kvalifikuotas elektroninio spaudo sertifikatas, kaip apibrėžta *eIDAS*; išreiškiamas kaip loginis.
d) *EUQSCDRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti susijęs su privačiu raktu, kuris laikomas Kvalifikuotame parašo kūrimo įtaise, kaip apibrėžta *eIDAS*; išreiškiamas kaip loginis.

Kriptografiniai apribojimai

„Dokobit“ galiojimo patvirtinimo paslauga palaiko šiuos kriptografinius apribojimus, kurie nurodo algoritmų ir parametrų, naudojamų kuriant parašus arba naudojamų patvirtinant pasirašytą objektą, reikalavimus, kaip nurodyta ETSI TS 119 172-1 A.4.2.1 punkto A2 lentelės p eilutėje.

Apribojimas (-ai)	Apribojimo vertė patvirtinant parašą (SVA arba DA)
(p)1. *CryptographicSuitesConstraints*. Šis apribojimas nurodo reikalavimus algoritmams ir parametrams, naudojamiems kuriant parašus arba tvirtinant pasirašytus objektus, įtrauktus į patvirtinimo arba papildymo procesą (pvz., parašą, sertifikatus, CRL, OCSP atsakymus, laiko žymas). Paprastai jie pateikiami kaip įrašų sąrašas, kaip A.3 lentelėje.	Remiantis ETSI TS 119 312

Parašo ir spaudo elementų apribojimai

„Dokobit“ galiojimo patvirtinimo paslauga palaiko šiuos parašo elemento apribojimus, kurie nurodo reikalavimus dėl DTBS, kaip nurodyta ETSI TS 119 172-1 A.4.2.1 punkto A.2 lentelėje, b eilutėje.

Apribojimas (-ai)	Apribojimo vertė patvirtinant parašą (SVA arba DA)
(b)1. *ConstraintOnDTBS*. Šis apribojimas nurodo duomenų, kuriuos turi pasirašyti pasirašantysis asmuo, tipo reikalavimus.	Nėra
(b)2. *ContentRelatedConstraintsAsPartOfSignatureElements*. Šis apribojimų rinkinys nurodo reikiamus su turiniu susijusius informacijos elementus pagal pasirašytas ar nepasirašytas kvalifikacines savybes, kurios privalo būti paraše. Tai apima: (b)2.1 *MandatedSignedQProperties-DataObjectFormat*, kad būtų reikalaujama konkretaus formato dėl turinio, kurį pasirašo pasirašantysis asmuo; (b)2.2 *MandatedSignedQProperties-content-hints*, kad būtų reikalaujama konkrečios informacijos, apibūdinančios vidinį pasirašytą daugiasluoksnio pranešimo turinį, kai vienas turinys yra kitame, dėl turinio, kurį pasirašo pasirašantysis asmuo; (b)2.3 *MandatedSignedQProperties-content-reference*, kad būtų reikalaujama įtraukti informaciją apie tai, kaip susieti užklausų ir atsakymų pranešimus dalyvaujant dviem šalims, arba apie tai, kaip toks ryšys turi būti sukuriamas ir t. t.; (b)2.4 *MandatedSignedQProperties-content-identifier*, kad būtų reikalaujama, jog būtų identifikatorius, kurį vėliau būtų galima naudoti parašui, ir, pasirinktinai, tam tikra vertė.	Nėra

Apribojimas (-ai)	Apribojimo vertė patvirtinant parašą (SVA arba DA)
(b)3. *DOTBSAsAWholeOrInParts*. Šis apribojimas parodo, ar turi būti pasirašyti visi duomenys, ar tik tam tikra (-os) jų dalis (-ys). Galimų reikalavimų verčių, naudojamų tokiems reikalavimams išreikšti, semantika apibrėžiama taip: • visi: turi būti pasirašyti visi duomenys; • dalys: turi būti pasirašyta (-os) tik tam tikra (-os) duomenų dalis (-ys). Pastaruoju atveju turėtų būti naudojama papildoma informacija, nurodant, kurios dalys turi būti pasirašytos.	Nėra

4.2 Parašo galiojimo patvirtinimo protokolo reikalavimai

Ryšio kanalu tarp kliento ir galiojimo patvirtinimo paslaugos elektroninio parašo galiojimo patvirtinimo užklausos perduodamos viena kryptimi ir pateikiamas atsakymas. Jis gali būti sinchroninis arba asinchroninis. Galiojimo patvirtinimo protokolas atitinka ETSI TS 119 442.

„Dokobit“ galiojimo patvirtinimo paslaugos teikiamos šiomis priemonėmis:

- kaip REST API programos integracija („Dokobit Gateway“ arba „Dokobit“ Galiojimo patvirtinimo paslaugos API);
- kaip Žiniatinklio taikomoji programa su Naudotojo sąsaja („Dokobit“ portalas arba „Dokobit“ Galiojimo patvirtinimo paslauga).

4.3 Sąsajos

4.3.1 Ryšio kanalas

Ryšio kanalas tarp kliento ir SVSP užtikrinamas naudojant patikimai apsaugotą kanalą pagal HTTPS protokolą ir naudojant TLS šifravimą su QWAC sertifikatu. SVSP garantuoja, kad jis gali sukurti saugų kanalą ryšiui su klientu ir išsaugoti duomenų konfidencialumą.

„Dokobit“ portale reikalaujama, kad klientas savo tapatybę patvirtintų naudodamas el. atpažinties priemonę (tik tada jis gali naudotis galiojimo patvirtinimo paslauga). Tai užtikrina, kad įkelta informacija būtų prieinama tik konkrečiam klientui.

„Dokobit Gateway“ ir „Dokobit“ Galiojimo patvirtinimo paslaugos API reikia, kad naudotojas autorizuotųsi naudodamas leidimo prieigos raktą, kuris užtikrina, kad įkelta informacija būtų prieinama tik konkrečiam klientui. Galima naudoti ir IP apsaugą.

4.3.2 SVSP - kiti patikimumo užtikrinimo paslaugų teikėjai

Parašo patikrinimo būsenai ir parašo galiojimo patvirtinimo ataskaitai gali turėti įtakos praktika, politika ir susitarimai dėl atitikties su kitais paslaugų teikėjais, kurių SVSP kontroliuoti negali. Kiti patikimumo užtikrinimo paslaugų teikėjai yra laiko žymų tarnybos, CRL ir OCSP teikėjai, kiti galiojimo patvirtinimo paslaugų teikėjai. SVSP pateikiama parašo tikrinimo būsena ir parašo galiojimo patvirtinimo ataskaita galioja tik realiu patvirtinimo metu.

Ryšio kanalas tarp SVSP ir kito TSP nepatenka į šio dokumento taikymo sritį.

4.4 Parašo galiojimo patvirtinimo ataskaitos reikalavimai

SVSP teikia trijų rūšių patvirtinimo ataskaitas:

1. Sutrumpinta galiojimo patvirtinimo ataskaita, kurioje pateikiama reikiama informacija apie Pasirašančiojo asmens tapatybę ir kiekvieno patvirtinto parašo būsenos indikaciją, įskaitant papildomą indikaciją;
2. Išplėstinė galiojimo patvirtinimo ataskaita, kurioje pateikiama ataskaita apie kiekvieną galiojimo patvirtinimo apribojimą, kuris yra apdorojamas, įskaitant visus galiojimo patvirtinimo apribojimus, kurie buvo taikomi vykdymo metu;
3. Kompiuterio skaitoma galiojimo patvirtinimo ataskaita, kurioje pateikiama išsami galiojimo patvirtinimo ataskaita kompiuterio skaitomu XML formatu.

Visos SVSP pateiktos galiojimo patvirtinimo ataskaitos turi būti antspauduojamos naudojant Pažangųjį elektroninį spaudą su Kvalifikuotu sertifikatu.

Kvalifikuotą spaudo sertifikatą išduoda Kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas „SK ID Solutions“ pagal „SK ID Solutions“ Sertifikavimo veiklos nuostatus, kuriuos galima rasti adresu *https://www.skidsolutions.eu/resources/certification-practice-statement/*.

Spaudo sertifikato duomenys:

cn=Dokobit Qualified Validation Service

o=Dokobit, UAB

c=LT

l=Vilnius

st=Vilnius

serialNumber=301549834

2.5.4.97=NTRLT-301549834

Išdavėjo duomenys:

cn=SK ID Solutions ORG 2021E

2.5.4.97=NTREE-10747013

o=SK ID Solutions AS

c=EE

5 A priedas

Bendrieji parašo galiojimo patvirtinimo apribojimai, naudojami QES galiojimo patvirtinimo politikoje (1.3.6.1.4.1.54720.1.2):

Apribojimas	Indikacija
Konteinerio apribojimai	
Acceptable container types: ASiC-S ASiC-E	FAIL
MimeType file is present	FAIL
Acceptable MimeType file content: application/vnd.etsi.asic-s+zip application/vnd.etsi.asic-e+zip	WARN
Manifest file is present	FAIL
All files are signed	WARN
Parašo apribojimai	
Acceptable policies: ANY_POLICY NO_POLICY	FAIL
Policy is available	FAIL
Policy hash matches	FAIL
Reference data exists	FAIL
Reference data is intact	FAIL
Manifest entry object exists	WARN

Signature is intact	FAIL
Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL
Signing certificate qualification	FAIL
Signing certificate is supported by QSCD	FAIL
Signing certificate is not expired	WARN
Signing certificate authority info access is present	WARN
Signing certificate revocation info access is present	WARN
Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “nonRepudiation“	WARN
Signing certificate serial number is present	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	FAIL
Certification authority certificate revocation data next update is present	WARN

Certification authority certificate revocation data freshness	WARN
Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Signed attributes contain signing certificate	FAIL
Signed attributes contain signing certificate digest	FAIL
Signing certificate digest in signed attributes matches	FAIL
Issuer serial digest in signed attributes matches	WARN
Signed attributes contain signing time	FAIL
Signed attributes contain message digest or signed properties	FAIL
Elements that might change the visual content of the signed document were detected	WARN
Laiko žymos apribojimai	
Revocation time is against best signature time	FAIL
Best signature time is before issuance date of signing certificate policy	FAIL
Coherence	WARN
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL

Signing certificate is not expired	WARN
Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “timeStamping“	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	WARN
Certification authority certificate revocation data next update is present	WARN
Certification authority certificate revocation data freshness	WARN
Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Atšaukimo duomenų apribojimai	
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	WARN
Signing certificate recognition	FAIL

Signing certificate signature	FAIL
Signing certificate is not expired	WARN
Signing certificate revocation data is available	IGNORE
Signing certificate revocation data next update is present	IGNORE
Signing certificate revocation data freshness	IGNORE
Signing certificate is not revoked	IGNORE
Signing certificate is not on hold	IGNORE
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	IGNORE
Certification authority certificate revocation data is available	IGNORE
Certification authority certificate revocation data next update is present	IGNORE
Certification authority certificate revocation data freshness	IGNORE
Certification authority certificate is not revoked	IGNORE
Certification authority certificate is not on hold	IGNORE
Patikimo sąrašo apribojimai	
Trusted list freshness	WARN
Trusted list is not expired	WARN
Trusted list is well signed	FAIL
Trusted list version 5	FAIL
Trusted list consistency	FAIL
Kriptografiniai apribojimai	

Acceptable encryption algorithms: RSA - (minimum key size 1024) DSA - (minimum key size 160) ECDSA - (minimum key size 160) PLAIN-ECDSA - (minimum key size 160)	FAIL
Acceptable digest algorithms: SHA1, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD160, WHIRLPOOL	FAIL
Algorithm expiration date: SHA1 - 2009 SHA224 - 2023 SHA256 - 2026 SHA384 - 2026 SHA512 - 2026 SHA3-224 - 2026 SHA3-256 - 2026 SHA3-384 - 2026 SHA3-512 - 2026 RIPEMD160 - 2011 WHIRLPOOL - 2015 DSA 160 - 2013 DSA 192 - 2013 DSA 224 - 2023 DSA 256 - 2026 RSA 1024 - 2009 RSA 1536 - 2016 RSA 2048 - 2023 RSA 3072 - 2026 RSA 4096 - 2026 ECDSA 160 - 2013 ECDSA 192 - 2013 ECDSA 224 - 2016 ECDSA 256 - 2026 ECDSA 384 - 2026 ECDSA 512 - 2026 PLAIN-ECDSA 160 - 2013 PLAIN-ECDSA 192 - 2013 PLAIN-ECDSA 224 - 2016 PLAIN-ECDSA 256 - 2026 PLAIN-ECDSA 384 - 2026 PLAIN-ECDSA 512 - 2026	FAIL

- *FAIL - jei aptiktas apribojimo neatitikimas, galiojimo patvirtinimo metu rodoma klaida*
- *WARN - jei aptiktas apribojimo neatitikimas, galiojimo patvirtinimo metu rodomas įspėjimas*
- *IGNORE - apribojimas ignoruojamas*

6 B priedas

Bendrieji parašo galiojimo patvirtinimo apribojimai, naudojami AdES galiojimo patvirtinimo politikoje (1.3.6.1.4.1.54720.1.3):

Apribojimas	indikacija
Konteinerio apribojimai	
Acceptable container types: ASiC-S ASiC-E	FAIL
MimeType file is present	FAIL
Acceptable MimeType file content: application/vnd.etsi.asic-s+zip application/vnd.etsi.asic-e+zip	WARN
Manifest file is present	FAIL
All files are signed	WARN
Parašo apribojimai	
Acceptable policies: ANY_POLICY NO_POLICY	FAIL
Policy is available	FAIL
Policy hash matches	FAIL
Reference data exists	FAIL
Reference data is intact	FAIL
Manifest entry object exists	WARN

Signature is intact	FAIL
Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL
Signing certificate qualification	IGNORE
Signing certificate is supported by QSCD	IGNORE
Signing certificate is not expired	FAIL
Signing certificate authority info access is present	WARN
Signing certificate revocation info access is present	WARN
Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “nonRepudiation“	WARN
Signing certificate serial number is present	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	FAIL
Certification authority certificate revocation data next update is present	WARN

Certification authority certificate revocation data freshness	WARN
Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Signed attributes contain signing certificate	FAIL
Signed attributes contain signing certificate digest	FAIL
Signing certificate digest in signed attributes matches	FAIL
Issuer serial digest in signed attributes matches	WARN
Signed attributes contain signing time	FAIL
Signed attributes contain message digest or signed properties	FAIL
Elements that might change the visual content of the signed document were detected	WARN
Laiko žymos apribojimai	
Revocation time is against best signature time	FAIL
Best signature time is before issuance date of signing certificate policy	FAIL
Coherence	WARN
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	FAIL
Signing certificate recognition	FAIL
Signing certificate signature	FAIL

Signing certificate is not expired	WARN
Signing certificate revocation data is available	FAIL
Signing certificate revocation data next update is present	WARN
Signing certificate revocation data freshness	WARN
Signing certificate key usage contains “timeStamping“	WARN
Signing certificate is not revoked	FAIL
Signing certificate is not on hold	FAIL
Signing certificate is not self-signed	WARN
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	WARN
Certification authority certificate revocation data is available	WARN
Certification authority certificate revocation data next update is present	WARN
Certification authority certificate revocation data freshness	WARN
Certification authority certificate is not revoked	FAIL
Certification authority certificate is not on hold	FAIL
Atšaukimo duomenų apribojimai	
Reference data exists	FAIL
Reference data is intact	FAIL
Signature is intact	FAIL
Prospective certificate chain	WARN
Signing certificate recognition	FAIL

Signing certificate signature	FAIL
Signing certificate is not expired	WARN
Signing certificate revocation data is available	IGNORE
Signing certificate revocation data next update is present	IGNORE
Signing certificate revocation data freshness	IGNORE
Signing certificate is not revoked	IGNORE
Signing certificate is not on hold	IGNORE
Certification authority certificate signature	FAIL
Certification authority certificate is not expired	IGNORE
Certification authority certificate revocation data is available	IGNORE
Certification authority certificate revocation data next update is present	IGNORE
Certification authority certificate revocation data freshness	IGNORE
Certification authority certificate is not revoked	IGNORE
Certification authority certificate is not on hold	IGNORE
Patikimo sąrašo apribojimai	
Trusted list freshness	WARN
Trusted list is not expired	WARN
Trusted list is well-signed	FAIL
Trusted list version 5	FAIL
Trusted list consistency	FAIL
Kriptografiniai apribojimai	

Acceptable encryption algorithms: RSA - (minimum key size 1024) DSA - (minimum key size 160) ECDSA - (minimum key size 160) PLAIN-ECDSA - (minimum key size 160)	FAIL
Acceptable digest algorithms: SHA1, SHA224, SHA256, SHA384, SHA512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, RIPEMD160, WHIRLPOOL	FAIL
Algorithm expiration date: SHA1 - 2009 SHA224 - 2023 SHA256 - 2026 SHA384 - 2026 SHA512 - 2026 SHA3-224 - 2026 SHA3-256 - 2026 SHA3-384 - 2026 SHA3-512 - 2026 RIPEMD160 - 2011 WHIRLPOOL - 2015 DSA 160 - 2013 DSA 192 - 2013 DSA 224 - 2023 DSA 256 - 2026 RSA 1024 - 2009 RSA 1536 - 2016 RSA 2048 - 2023 RSA 3072 - 2026 RSA 4096 - 2026 ECDSA 160 - 2013 ECDSA 192 - 2013 ECDSA 224 - 2016 ECDSA 256 - 2026 ECDSA 384 - 2026 ECDSA 512 - 2026 PLAIN-ECDSA 160 - 2013 PLAIN-ECDSA 192 - 2013 PLAIN-ECDSA 224 - 2016 PLAIN-ECDSA 256 - 2026 PLAIN-ECDSA 384 - 2026 PLAIN-ECDSA 512 - 2026	FAIL

- *FAIL - jei aptiktas apribojimo neatitikimas, galiojimo patvirtinimo metu rodoma klaida*
- *WARN - jei aptiktas apribojimo neatitikimas, galiojimo patvirtinimo metu rodomas įspėjimas*
- *IGNORE - apribojimas ignoruojamas*