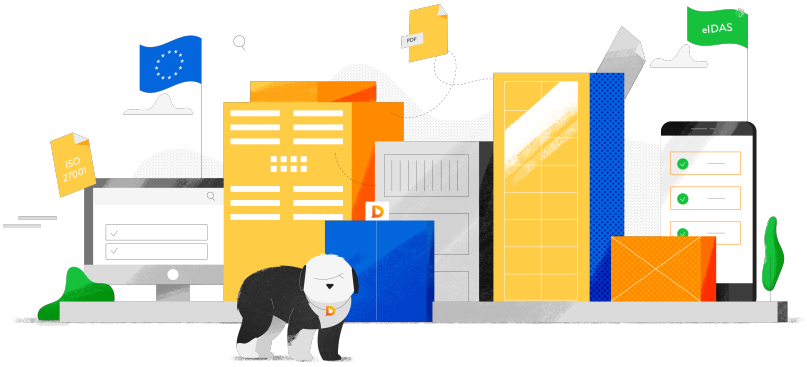


Kvalifikuotos parašų ir spaudų galiojimo patvirtinimo paslaugos praktiniai nuostatai ir politika v1.11

Document Number: DKB-VSP-06122019 v1.11

Unique object ID (OID): 1.3.6.1.4.1.54720.1.1

Effective from 2021-08-02

© 2022 — Dokobit UAB — e-signing as an everyday service.

https://www.dokobit.com

Table of Contents

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 Kvalifikuoto 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 1 ir 2 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.

2 Įžanga

2.1 Apžvalga

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

teikiant **Kvalifikuotas parašo ir spaudo galiojimo patvirtinimo paslaugas** 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;
- 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“;
  - Ryšių reguliavimo tarnybos direktoriaus 2019 m. birželio 4 d. įsakymą Nr. 1V-594 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo“.
- Europos standartą *ETSI EN 319 401 (elektroniniai parašai ir infrastruktūra (EPI)*;
  - Bendruosius politikos reikalavimus patikimumo užtikrinimo paslaugos teikėjams ir kitus susijusius reikalavimus.

Šio dokumento struktūra atitinka *ETSI TS 119 441 V1.1.1 (2018-08) A priedą*.

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 parašo galiojimo patvirtinimo paslauga

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

2.2 Parašo galiojimo patvirtinimo paslaugos komponentai

2.2.1 SVS dalyviai

Parašo galiojimo patvirtinimo paslaugos 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 patvirtinimo paslaugos teikėjo (SVSP) pusėje.

Parašo galiojimo patvirtinimo programa (SVA)

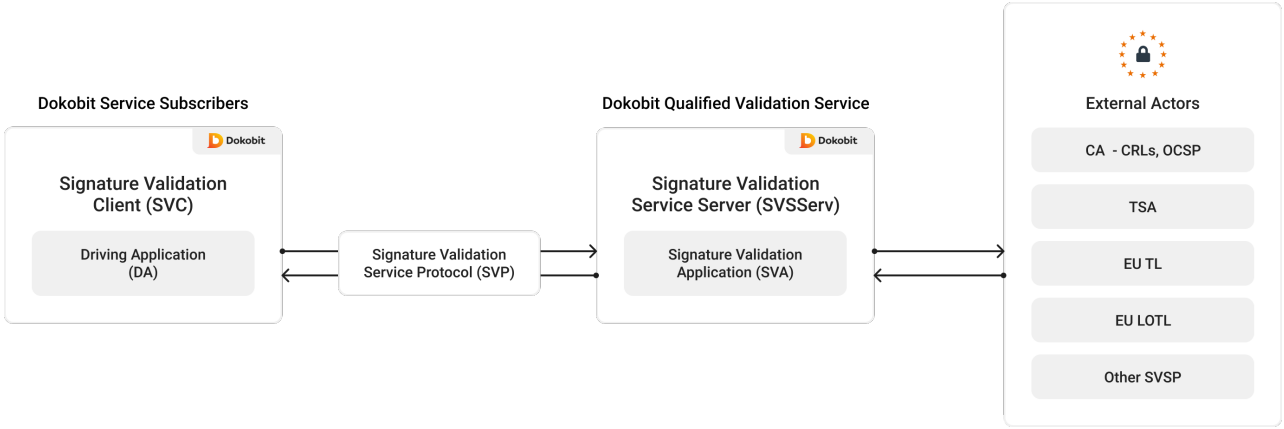
- Už parašo galiojimo patvirtinimą atsakingas programinės įrangos komponentas, kuris vykdo patvirtinimo algoritmą ir sukuria parašo galiojimo patvirtinimo ataskaitą.

Išoriniai dalyviai

- Kiti patikimumo užtikrinimo šaltiniai – Sertifikavimo institucijos, Laiko žymų tarnybos, tiekėjai įrašyti į Europos Patikimą sąrašą, Europos Komisija sudaranti Patikimą sąrašą pagal jų siekiamus įgyvendinti 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
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)
Informacijos saugumo valdymo sistema	ISMS	Sertifikuota „Dokobit“ informacijos saugumo valdymo sistema, atitinkanti ISO/IEC 27001:2013
Patikimumo užtikrinimo paslaugos teikėjas	TSP	Subjektas, teikiantis patikimumo užtikrinimo paslaugą
Kvalifikuotų patikimumo užtikrinimo paslaugos teikėjas	QTSP	Subjektas, teikiantis vieną ar daugiau kvalifikuotų patikimumo užtikrinimo paslaugų ir turintis priežiūros institucijos suteiktą kvalifikaciją
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“ el. parašų galiojimo patvirtinimo praktiniai nuostatai ir politika	Dokobit PP	Nuostatai, kuriuose aprašomos praktikos, kurias „Dokobit“ taiko teikdamas patikimumo užtikrinimo paslaugą
Parašo galiojimo patvirtinimo paslauga	SVS	Patikimumo užtikrinimo paslauga, susijusi su Parašo ir (arba) Spaudo galiojimo patvirtinimu
Pasikliaujančioji šalis		Fizinis ar juridinis asmuo, kuris pasikliauja Patikimumo užtikrinimo paslauga
Abonentas		Juridinis ar fizinis asmuo, sutartimi su „Dokobit“ įsipareigojęs vykdyti Abonento pareigas
Sertifikavimo institucija	CA	Kvalifikuotas patikimumo užtikrinimo paslaugos teikėjas, išduodantis 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

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“ Atitikties vadovas.

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

2.4.3 TSP dokumentacijos taikomumas

Parašo galiojimo patvirtinimo paslaugos praktiniai nuostatai

„Dokobit“ atsako už „Dokobit“ Galiojimo patvirtinimo paslaugos praktinių nuostatų tvarkymą. Šį dokumentą tvirtina Vadovybė ir jis viešai skelbiamas „Dokobit“ Patikimumo 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“ Veiklos nuostatų versija nuo tada, kai ima naudotis „Dokobit“ teikiamomis paslaugomis. „Dokobit“ Veiklos nuostatai kartu su įsigaliojimo datomis paskelbiami ne vėliau kaip 30 dienų iki įsigaliojimo.

Informacijos saugumo politika

„Dokobit“ įdiegė Informacijos saugumo valdymo sistemą (ISMS) pagal ISO/IEC-27001:2013 standartą. Pagal ISO/IEC-27001:2013 bendrovei „Dokobit“ išduotas ISMS sertifikatas apima šią sertifikavimo sritį: „Debesijos pagrindu teikiamos elektroninio pasirašymo, elektroninio spaudo naudojimo, elektroninio identifikavimo paslaugos, elektroninio parašo ir elektroninio spaudo galiojimo patvirtinimo paslaugos ir susijusios programinės įrangos kūrimo, pristatymo ir palaikymo paslaugos“.

„Dokobit“ į ISMS įdiegė visas būtinas kontrolės priemones, kurių reikalaujama pagal *eIDAS* bei BDAR ir atitinkamus standartus (t. y. ETSI EN 319 401).

Politikas ir nuostatus, susijusius su informacijos saugumu, tvirtina „Dokobit“ Generalinis direktorius.

Paslaugų teikimo sąlygos

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

2.4.4 „Dokobit“ Kvalifikuotos galiojimo patvirtinimo paslaugos naudojimo apribojimai

„Dokobit“ Kvalifikuota galiojimo patvirtinimo paslauga teikiamos Galiojimo patvirtinimo ataskaitos 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“ įdiegė Informacijos saugumo valdymo sistemą pagal ISO/IEC 27001:2013 standartą ir gavo *ISO/IEC 27001:2013 sertifikatą*, kurį išdavė akredituota tarptautinė sertifikavimo įstaiga. Šis sertifikatas apima Kvalifikuotas parašo ir spaudo galiojimo patvirtinimo paslaugas. 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 visus savo veiksmus atlieka laikydamasi priimtų politikos dokumentų ir nuostatų. „Dokobit“ užtikrina, kad visi reikalavimai, nustatyti ISO 27001:2013 Taikomumo pareiškime ir šiuose Veiklos 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

Įdiegta ir sertifikuota Informacijos saugumo valdymo sistema pagal ISO/IEC 27001:2013 užtikrina, kad būtų tikrinamas ir išlaikomas pareigų atskyrimas. Kalbant konkrečiau, atskiriami Informacijos saugumo vadovo (ISM) ir vidaus auditoriaus vaidmenys. Konkrečiai:

A.6.1.2	Pareigų atskyrimas	ISM ir Vidaus auditoriaus vaidmenys yra atskirti. Svarbiausiems klausimams, įskaitant informacinio saugumo klausimus, spręsti taip pat įsteigta Valdymo grupė. ISM yra Valdymo grupės dalis. Gyvybiškai svarbiose srityse užtikrinamas keturių akių principas: • Saugus kūrimas ir kodų peržiūros • Programinės įrangos diegimas

3.2 Žmogiškieji ištekliai

Įdiegta ir sertifikuota Informacijos saugumo valdymo sistema, atitinkanti ISO/IEC 27001:2013 reikalavimus, garantuoja, kad „Dokobit“ yra įdiegusi visas saugiai veiklai reikalingas kontrolės priemones. Darbuotojai ir rangovai gauna tinkamą mokymą ir turi reikiamą patirtį, kad galėtų atlikti pareigas, nurodytas įdarbinimo ar rangos sutartyse, kaip apibrėžta „Dokobit“ Žmogiškųjų išteklių valdymo politikoje. Konkrečiai:

A.7.1	Prieš įdarbinimą	
A.7.1.1	Atranka	Žmogiškųjų išteklių valdymo politika yra ISMS dalis. Ji apibrėžia įdarbinimo, integravimo ir darbo nutraukimo procesus. Patikra ir tinkamumo patikrinimai iki įdarbinimo, įskaitant teistumo patikras, kurių reikia Kvalifikuotos patikimumo užtikrinimo paslaugos teikėjams, darbinės veiklos istorija ir rekomendacijos yra „Dokobit“ įdarbinimo proceso dalis.
A.7.1.2	Įdarbinimo sąlygos ir tvarka	Prieš įdarbinimą ir faktines su darbu susijusias veiklas visi darbuotojai pasirašo standartinę darbo sutarties ir konfidencialumo susitarimo formą. Be to, darbuotojas yra supažindinamas su verslo paslapčių sąrašu, kurį patvirtina organizacijos valdyba, ir visa informacija bei duomenimis, priklausančiais nustatytoms kategorijoms, kurios turi būti laikomos verslo paslaptimi ir būti saugomomis.
A.7.2	Įdarbinimo laikotarpiu	
A.7.2.1	Vadovaujančiojo personalo atsakomybė	Vadovybė valdo ISMS ir palaiko jos veiklą, o darbuotojai yra viena esminių ISMS dalių. Valdymo procesas ir vadybinės atsakomybės pateikiami Informacijos saugumo politikoje ir valdymo praktikos dokumente.
A.7.2.2	Informacijos saugumo suvokimas, švietimas ir mokymas	Mokymo ir vidinio informavimo veiklos yra būtinos, kad darbuotojai suprastų informacijos saugumo valdymo ir savo indėlio į ISMS svarbą, priimtų politikas ir planus bei suprastų informacijos saugumo taisyklių pažeidimo pasekmes. Todėl mokymo ir informavimo planą rengia ir koordinuoja ISM. Jo vykdymo rezultatas –susiję realūs įrašai. Be to, saugaus programinės įrangos kūrimo praktikos, įskaitant susijusį informuotumą, pateiktos Saugaus programinės įrangos kūrimo politikoje.
A.7.2.3	Drausminis procesas	Pagal Žmogiškųjų išteklių valdymo politiką drausminės priemonės yra dalis: · Lietuvos Respublikos darbo kodekso; · Darbo sutarties; · Specialiųjų konfidencialumo susitarimo, kurį pasirašė darbuotojas, straipsnių. Ši politika numato drausminio proceso procedūrą, pagal kurią gali būti nutraukta darbo sutartis ir skirtos baudos, nustatytos konfidencialumo susitarime.

A.7.3	Darbo santykių nutraukimas ir darbo pareigų pakeitimas	
A.7.3.1	Darbo sutarties nutraukimas ar pareigų pakeitimas	Pagal konfidencialumo susitarimus su darbuotojais konfidencialumo sąlygos galioja ir nutraukus darbo santykius. Darbo santykių nutraukimo procedūra ir su tuo susiję būtini veiksmai, kaip antai, prieigos teisių panaikinimas, aprašyti Žmogiškųjų išteklių valdymo politikoje ir Prieigos kontrolės politikoje. Be to, pasikeitus darbo įsipareigojimams, prieigos teisės turi būti peržiūrimos pagal Prieigos kontrolės politiką.

3.3 Turto valdymas

3.3.1 Bendrieji reikalavimai

„Dokobit“ nuolat atnaujina turto sąrašus, įskaitant informacinius išteklius. Rizikos valdymas yra grindžiamas Turto identifikavimu. Rizikos vertinimas yra suderintas su turto identifikavimu, o turto grėsmė nustatoma pasitelkiant išsamų kartografavimą. Tai yra sertifikuotos „Dokobit“ ISMS dalis, t.y., „Dokobit“ Priimtino naudojimo politika, „Dokobit“ Informacijos klasifikavimo politika ir „Dokobit“ Rizikos valdymo metodika. Konkrečiai:

A.8.1	Atsakomybė už turtą	
A.8.1.1	Turto inventorius	„Dokobit“ nuolat atnaujina turto sąrašus, įskaitant virtualius ir fizinius, taip pat ir tokio turto savininkų sąrašus. Organizacijos Rizikos vertinimas suderinamas su turto identifikavimu, o grėsmės nustatomos kaip susijusios su turtu, naudojant išsamų kartografavimą.
A.8.1.2	Turto nuosavybė	„Dokobit“ turi naujausius viso (virtualaus ir fizinio) turto bei jo savininkų sąrašus. Lentelėje „Turto sąrašas“ pateikti turto savininkai.
A.8.1.3	Priimtinas turto naudojimas	Priimtino naudojimo politikoje apibrėžtos aiškios „Dokobit“ informacijos sistemų ir kito informacinio turto naudojimo taisyklės. Joje taip pat nustatyti įsipareigojimai, draudžiama veikla, turto išsinešimas, turto grąžinimas, atsarginės kopijos, interneto naudojimas turte, mobiliojoje kompiuterijoje, nuotoliniame darbe.
A.8.1.4	Turto grąžinimas	„Dokobit“ užtikrina, kad visa įranga, programos ir elektroninės bei popierinės formos informacija, jei reikia, būtų grąžinta. Turto grąžinimas yra numatytas konfidencialumo susitarimuose (būtinuose pagal Žmogiškųjų išteklių valdymo politiką), Priimtino naudojimo politikoje, Tiekėjų sutartyse (būtinose pagal Tiekėjų saugumo politiką).

3.3.2 Laikmenų naudojimas

Laikmenos, kuriose yra neskelbtinos informacijos, naudojamos saugiai, laikantis ISMS „Dokobit“ Informacijos klasifikavimo politikos ir „Dokobit“ IRT naudojimo procedūrų. Konkrečiai:

A.8.3	Laikmenų naudojimas	
A.8.3.1	Išimamųjų laikmenų tvarkymas	Informacijos klasifikavimo politika apibrėžia, kaip tvarkyti informaciją popieriniu, elektroniniu, elektroniniu informacinėse sistemose ir elektroniniuose laiškuose formatu, įskaitant keičiamąsias laikmenas (ir saugojimą). Ji apima prieigą, slaptažodžių naudojimą ir šifravimą.
A.8.3.2	Laikmenos šalinimas	IRT naudojimo procedūrų dokumente nustatytos įrangos bei laikmenų šalinimo ir sunaikinimo kontrolės priemonės. Bendrai, visą įrangą, kurioje yra saugojimo laikmenų (pvz., kompiuterius, mobiliuosius telefonus ir kt.), reikia išvalyti prieš naudojant dar kartą, o laikmenas sunaikinti prieš šalinimą.
A.8.3.3	Fizinės laikmenos perdavimas	Informacijos klasifikavimo politikoje nustatytos techninio saugumo kontrolės priemonės, apsaugančios informaciją laikmenose, įskaitant jos perdavimą, priklausančios nuo klasifikavimo lygmens. IRT naudojimo procedūrų dokumente nustatytas reikalavimas išvalyti bet kurias laikmenas prieš jas naudojant dar kartą.

3.4 Prieigos kontrolė

„Dokobit“ Prieigos kontrolės politika, kuri yra sertifikuotos „Dokobit“ ISMS dalis, užtikrina, kad prieiga prie sistemos būtų suteikta tik įgaliotiems asmenims ir kad būtų įdiegtos visos būtinos saugios prieigos kontrolės priemonės. Konkrečiai:

A.9	Prieigos kontrolė	
A.9.1	Įmonių reikalavimai dėl prieigos kontrolės	
A.9.1.1	Prieigos kontrolės politika	Pagal pagrindinį principą prieiga prie visų sistemų, tinklų, paslaugų ir informacijos yra draudžiama („pagal numatytąją nuostatą atmetama“), išskyrus atvejus, kai tai aiškiai leidžiama („reikia žinoti“) pavieniams naudotojams ar jų grupėms. Prieigos kontrolės politika pateikia išsamią (elektroninės) prieigos suteikimo, reikalavimų dėl įmonių paskyrų saugumo nustatymų, pirmenybės valdymo ir reguliarios prieigos teisių peržiūros sistemą. Pagal šią politiką turi būti užtikrinami ir tvarkomi susiję atsekami prieigos kontrolės įrašai.

A.9.1.2	Prieiga prie tinklų ir tinklo paslaugų	Pagal pagrindinį principą prieiga prie visų sistemų, tinklų, paslaugų ir informacijos yra draudžiama („pagal numatytąją nuostatą atmetama“), išskyrus atvejus, kai tai aiškiai leidžiama („reikia žinoti“) pavieniams naudotojams ar jų grupėms. Nuotolinė prieiga palaikoma tik šifravimo būdu (IRT naudojimo procedūros) ir jai taikoma „Dokobit“ Priimtino naudojimo politika.
A.9.2	Naudotojo prieigos valdymas	
A.9.2.1	Naudotojo registracija ir išregistravimas	„Dokobit“ Prieigos kontrolės politikoje nustatyta naudotojo registracijos įmonės kataloge, vidaus tinkle ir informacinėse sistemose sistema. Naudotojo registracijos procesas papildytas rekomenduojamais techniniais (saugumo) parametrais. Prieigos kontrolės politikoje taip pat numatytas naudotojo išregistravimo procesas, įskaitant paskyrų šalinimo reikalavimus.
A.9.2.2	Naudotojo prieigos teikimas	Pagal pagrindinį principą prieiga prie visų sistemų, tinklų, paslaugų ir informacijos yra draudžiama („pagal numatytąją nuostatą atmetama“), išskyrus atvejus, kai tai aiškiai leidžiama („reikia žinoti“) pavieniams naudotojams ar jų grupėms. Nuotolinė prieiga palaikoma tik šifravimo būdu (IRT naudojimo procedūros) ir jai taikoma „Dokobit“ Priimtino naudojimo politika. Šiame dokumente taip pat pateikiami įmonių paskyros saugos nustatymams reikalavimai.
A.9.2.3	Išimtinių prieigos teisių valdymas	Pagal „Dokobit“ Prieigos kontrolės politiką išimtis kiekvienai sistemai (turtui) gali suteikti tik jų atitinkami savininkai arba ISM.
A.9.2.4	Slaptos naudotojų atpažinimo informacijos valdymas	Išsamūs reikalavimai, kaip naudotojai turėtų valdyti slaptą atpažinimo informaciją ir ją naudoti, nustatyti „Dokobit“ Priimtino naudojimo politikoje. Ji užtikrina geriausias srities praktikas, pavyzdžiui, taikomą 2F.
A.9.2.5	Naudotojo prieigos teisių peržiūra	Reguliari prieigos teisių peržiūra apibrėžiama Prieigos kontrolės politikoje.
A.9.2.6	Prieigos teisių panaikinimas arba koregavimas	Prieigos teisės panaikinamos arba koreguojamos laikantis Prieigos kontrolės politikos. Nepaisant prieigos teisių pakeitimo laiku, esant įmonių prašymams, atsakingas administratorius užtikrina, kad kiekvienos sistemos, posistemės ir komponento prieigos teisės būtų peržiūrimos bent kartą per metus.
A.9.3	Naudotojo atsakomybė	
A.9.3.1	Slaptos atpažinimo informacijos naudojimas	„Dokobit“ Priimtino naudojimo politikoje nustatyti išsamūs reikalavimai naudotojams dėl slaptos atpažinimo informacijos valdymo ir naudojimo. Joje taikoma geriausia šios srities patirtis, pavyzdžiui, užšifruotų slaptažodžių valdymo įrankių, naudojimas.

A.9.4	Sistemos ir programų prieigos kontrolė	
A.9.4.1	Prieigos prie informacijos apribojimas	Prieigos prie informacijos apribojimas ir teikimo procedūros nustatyti Informacijos klasifikavimo politikoje. Be to, Prieigos kontrolės politikoje apibrėžtas pagrindinis principas, kad prieiga prie visų sistemų, tinklų, paslaugų ir informacijos yra draudžiama („pagal numatytąją nuostatą atmetama“), išskyrus atvejus, kai tai aiškiai leidžiama („reikia žinoti“) pavieniams naudotojams ar jų grupėms.
A.9.4.2	Saugaus prisijungimo procedūros	Pagal (elektroninės) prieigos teikimo taisykles, pateikiamas Prieigos kontrolės politikoje, reikalaujama, kad prieiga prie vidinių, išorinių ar trečiųjų šalių paslaugų / programų būtų teikiama naudojant išorinę įmonės paskyros atpažinimo paslaugą. Čia taip pat įtraukta geriausia šios srities patirtis, pavyzdžiui, 2F taikymas.
A.9.4.3	Slaptažodžių valdymo sistema	Išsamūs įmonių paskyrų saugos nustatymų reikalavimai, atspindintys geriausias šios srities praktikas, išdėstyti Prieigos kontrolės politikoje.
A.9.4.4	Naudojimasis privilegijuotosiomis tinklo įrangos programomis	Priimtino naudojimo politikoje yra nustatytas apribojimas, kad naudotojai neturi dalyvauti veikloje, kuria siekiama apeiti informacinės sistemos saugumo kontrolės priemones.
A.9.4.5	Prieigos prie programinės įrangos pradinio kodo kontrolė	Programinės įrangos pradinis kodas yra intelektinė nuosavybė ir jis prieinamas tik „būtina žinoti“ pagrindais. Informacijos klasifikavimo politikoje nurodomi įgalioti asmenys ir prieigos prie komercinių paslapčių apribojimai (programos pradinis kodas yra komercinės paslapties dalis). Fiziškai pradinis kodas saugomas Pradinio kodo versijų kūrimo sistemoje. ISM suteikia raktu pagrįstą prieigą prie reikiamų šaltinių.

3.5 Kriptografinės kontrolės priemonės

„Dokobit“ Kriptografinių kontrolės priemonių, kurios yra sertifikuotos „Dokobit“ ISMS dalis, naudojimo politika užtikrina saugiųjų kriptografinių algoritmų, raktų dydžių ir kriptografinių prietaisų naudojimą teikiant visas „Dokobit“ Paslaugas.

A.10	Kriptografija	
A.10.1	Kriptografinės kontrolės priemonės	
A.10.1.1	Kriptografinių kontrolės priemonių naudojimo politika	Kriptografinių kontrolės priemonių naudojimo politikoje apibrėžtos kriptografinių kontrolės priemonių naudojimo, taip pat kriptografinių raktų naudojimo taisyklės, siekiant apsaugoti informacijos konfidencialumą, vientisumą, tikrumą ir nepaneigiamumą.

A.10.1.2	Rakto valdymas	Kriptografinių kontrolės priemonių naudojimo politikoje apibrėžtas raktų valdymas, įskaitant jų paskirstymo praktiką.

3.6 Fizinis ir aplinkos saugumas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit“ Tiekėjų saugumo politika, „Dokobit“ Darbo saugiose zonose procedūros ir „Dokobit“ IRT naudojimo procedūros. Konkrečiai:

A.11	Fizinis ir aplinkos saugumas	
A.11.1	Saugios zonos	
A.11.1.1	Fizinio saugumo perimetras	„Dokobit“ fizinio saugumo perimetras apibrėžtas Prieigos kontrolės politikoje. Konkrečios, fiziniam saugumui labai svarbios zonos, vadinamos „saugiomis zonomis“, apibūdintos dokumente „Darbo saugiose zonose procedūros“.
A.11.1.2	Fizinio įėjimo kontrolė	Fizinėms saugumo kontrolės priemonėms taikomos išsamios rizikos valdymo ir vertinimo veiklos. Bendrai, yra skirtingo lygmens fizinio įėjimo kontrolės priemonių, apibrėžtų Prieigos kontrolės politikoje ir Darbo saugiose zonose procedūrose, priklausančių nuo objekto gyvybingumo. Pavyzdžiui, prieiga prie saugių zonų yra „draudžiama pagal numatytąją nuostatą“ (pvz., „užblokuota“), išskyrus atvejus, kai ją leidžia atsakinga grupė.
A.11.1.3	Biurų, kambarių ir patalpų apsauga	Biuro patalpų saugumo kontrolės priemonės vertinamos atliekant rizikos vertinimą. Kai nustatoma didesnė nei toleruotina rizika, imamasi reikiamų veiksmų. Saugumo kontrolės priemonės aprašytos Prieigos kontrolės politikoje ir Darbo saugiose zonose procedūrose.
A.11.1.4	Apsauga nuo išorinių ir aplinkos grėsmių	Biuro patalpų saugumo kontrolės priemonės vertinamos atliekant rizikos vertinimą ir, kai nustatoma didesnė nei toleruotina rizika, imamasi reikiamų veiksmų. Tačiau dėl „Dokobit“ veiklos pobūdžio ir dėl to, kad naudojami viešosios debesijos IaaS teikėjai, tai nėra pagrįsta viena ar keliomis pastoviomis fizinėmis vietomis.
A.11.1.5	Darbas saugiose zonose	Darbo saugiose zonose taisyklės aprašytos Darbo saugiose zonose procedūrų dokumente. Jame pateiktas šių zonų sąrašas, įėjimo kontrolės priemonės, prieigos procedūros, įskaitant skirtąsias lankytojams, bei draudžiamos veiklos sąrašas.
A.11.1.6	Pristatymo ir pakrovimo vietos	Viešo naudojimo zonos, įskaitant pristatymo ir pakrovimo zonas (įėjimas į biurų pastatą), kontroliuojamos biuro pastato apsaugos darbuotojo.
A.11.2	Įranga	

A.11.2.1	Įrangos išdėstymas ir apsauga	„Dokobit“ paslaugos priklauso nuo didžiųjų debesijos teikėjų, kurie buvo objektyviai įvertinti ir atrinkti, taikant kriterijus, apibrėžtus vidaus Tiekėjų saugumo politikoje (taikomoje IaaS ir SaaS). Debesijos teikėjų deklaracijos dėl įvairių susijusių sertifikatų užtikrina įrangos ir duomenų apsaugą debesijos duomenų centruose. Be to, aktuali vietinė įranga išdėstyta tik saugiose zonose. Darbo saugiose zonose procedūrų dokumente pateiktas saugių zonų sąrašas ir susijusios apsaugos kontrolės priemonės bei procedūros. Saugios zonos patenka į „Dokobit“ ISO27001 taikymo apimtį ir sertifikavimą, ir jas periodiškai vertina parinkta sertifikavimo įstaiga.
A.11.2.2	Pagalbinės priemonės	„Dokobit“ paslaugos priklauso nuo didžiųjų debesijos teikėjų, kurie buvo objektyviai įvertinti ir atrinkti, taikant kriterijus, apibrėžtus vidaus Tiekėjų saugumo politikoje (taikomoje IaaS ir SaaS). Debesijos teikėjų deklaracijos dėl įvairių susijusių sertifikatų užtikrina pagalbines priemones debesijos duomenų centruose. Vidaus įrangos atžvilgiu, pagalbinėms priemonėms taikytinos rizikos, nustatytos vykdant rizikos vertinimo veiklą, ir jos yra implementuojamos kaip rizikos apdorojimo veiklos.
A.11.2.3	Kabelių saugumas	Kabelių saugumo kontrolės priemonės vertinamos atliekant rizikos vertinimą. Kai nustatoma didesnė nei toleruotina rizika, imamasi reikiamų veiksmų.
A.11.2.4	Įrangos priežiūra	Priimtino naudojimo politikoje nustatyta, kad įranga turi būti prižiūrima pagal gamintojo instrukcijas. Taip pat taikomi specialieji su priežiūra, pvz., pataisomis, susiję reikalavimai.
A.11.2.5	Turto pašalinimas	IRT naudojimo procedūrų dokumente nustatyti reikalavimai, taikomi laikmenų (kurios yra turto dalis) išvalymui (jei turtas pašalinamas pakartotiniam naudojimui) ir sunaikinimui (šalinimo atveju).
A.11.2.6	Įrangos ir turto saugumas ne patalpose	„Dokobit“ Priimtino naudojimo politikoje nustatyta, kaip turtą galima išnešti iš patalpų. Joje taip pat apibrėžtos taisyklės, kaip turtas turi būti tvarkomas ir saugomas ne biuro patalpose.
A.11.2.7	Saugus įrangos šalinimas ar pakartotinis naudojimas	IRT naudojimo procedūrų dokumente nustatytos įrangos bei laikmenų šalinimo ir sunaikinimo kontrolės priemonės. Bendrai, visą įrangą, kurioje yra saugojimo laikmenų (pvz., kompiuterius, mobiliuosius telefonus ir kt.), reikia išvalyti prieš naudojant dar kartą arba laikmenas sunaikinti prieš jų pašalinimą.
A.11.2.8	Neprižiūrima naudotojo įranga	Priimtino naudojimo politikoje apibrėžta Švaraus stalo ir švaraus ekrano politika. Šioje politikoje nustatyta, kaip galima naudoti naudotojo asmeninę įrangą darbui. Be to, „Dokobit“ taiko konfidencialios informacijos valdymą, įskaitant specialiąsias kontrolės priemones, skirtas „naudojami duomenys“, „perduodami duomenys“ ir „saugomi duomenys“ būsenoms.

A.11.2.9	Švaraus stalo ir švaraus ekrano politika	Priimtino naudojimo politikoje apibrėžti švaraus stalo ir švaraus ekrano reikalavimai. Ji apima tokias praktines kontrolės priemones, kaip slapto pobūdžio dokumentų nebuvimas ant stalo, kol nėra naudotojo. Taip pat reikalaujama užrakinti kompiuterių ekranus, prieš paliekant kompiuterių darbo vietą.

3.7 Operacijų saugumas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit“ IRT naudojimo procedūros, „Dokobit“ Saugios programinės įrangos kūrimo politika, „Dokobit“ Tiekėjų saugumo politika, „Dokobit“ Incidentų valdymo procedūra, „Dokobit“ Priimtino naudojimo politika, „Dokobit“ BYOD politika ir „Dokobit“ Asmens duomenų apsaugos politika. Konkrečiai:

A.12	Operacijų saugumas	
A.12.1	Darbo procedūros ir atsakomybė	
A.12.1.1	Dokumentuotos darbo procedūros	„Dokobit“ IRT naudojimo procedūrų dokumente nustatytos reikiamos darbo procedūros. Į jį įtrauktas pokyčių valdymas, techninio pažeidžiamumo valdymas, atsarginių kopijų darymas, tinklo saugumo valdymas, įrangos ir laikmenų šalinimas ir sunaikinimas bei kitos susijusios aktualios procedūros.
A.12.1.2	Pokyčių valdymas	Pokyčių valdymo procedūra aprašyta IRT naudojimo procedūrų dokumente. Jos esmė ta, kad kiekvienas pokytis, prieš jį išleidžiant, privalo turėti autorių, būti atsekamas ir dokumentuotas (sekimo sistemoje), ir testuotas bei patvirtintas. Kad būtų užtikrinamas tinkamas galiojimo patvirtinimo paslaugos veikimas, „Dokobit“ po kiekvieno patvirtinimo paslaugos funkcionalumo pakeitimo atlieka teigiamus ir neigiamus testus (pavyzd žiui, *XAdES*, *PAdES*, *CAdES* parašo galiojimo patvirtinimo testus, funkcijų logikos, naudotojo sąsajos testus, saugumo testus ir t. t.).
A.12.1.3	Pajėgumų valdymas	Pajėgumai užtikrinami ir valdomi atliekant paslaugos / programos registravimą ir stebėjimą (kas yra IaaS / SaaS atrankos kriterijų, apibrėžtų Tiekėjų saugumo politikoje, dalis). Išsamesnė informacija pateikiama: · IRT naudojimo procedūrose; · Saugios programinės įrangos kūrimo politikoje. Šių reikalavimų išdava buvo išmani vidaus paslaugų stebėjimo sistema, kuri naudojama „Dokobit“.
A.12.1.4	Kūrimo, testavimo ir naudojimo aplinkos atskyrimas	Saugios programinės įrangos kūrimo politikoje apibrėžti reikalavimai taikomi atskyrimui, atskiro kūrimo stebėjimui, testavimui ir gamybos aplinkai. Šie reikalavimai yra saugios inžinerijos principų, kurie įgyvendinti „Dokobit“, dalis.

A.12.2	Apsauga nuo kenkimo programinės įrangos	
A.12.2.1	Kontrolės priemonės apsaugai nuo kenkėjiškos programinės įrangos	Apsaugai nuo kenkėjiškos programinės įrangos „Dokobit“ taiko kelių lygmenų saugumo metodą. Priimtino naudojimo politikoje ir BYOD politikoje aprašyti apsaugos nuo kenkėjiškos programinės įrangos mechanizmai, skirti galiniams įrenginiams (pvz., antivirusinės programos; mažiausia galima pirmenybė, būtina veiklai vykdyti), pagrįsti draudžiamos veikos sąrašu (pvz., draudžiama nuolat būti išjungus antivirusines programas galiniuose įrenginiuose; diegti nelegalią programinę įrangą arba programas iš nepatikimų šaltinių). Tinklo lygmenyje IRT naudojimo procedūros reguliuoja tinklo saugumą (pvz., „pagal numatytąsias nuostatas drausti visus tinklo prievadus, išskyrus „būtinybę naudoti“). Programų / paslaugų lygmenyje Saugios programinės įrangos kūrimo politikoje pateikta geriausia patirtis ir pagrindiniai reikalavimai, keliami saugios programinės įrangos kūrimui, leidžiantys sukurti kenkimo veiksmams atsparesnę programinę įrangą, įskaitant kenkimo programinę įrangą (pvz., reikalavimas naudotis OWASP gairėmis; specialus kontrolinis sąrašas, skirtas esminiams komponentams, kaip antai API, saugumo antraštės ir konfigūracijos, prisijungimas ir kt.). Be to, Pažeidžiamumo atskleidimo politika leidžia nustatyti „Dokobit“ turto vietinio lygio („gerųjų ir blogųjų įsilaužėlių“) pažeidžiamumą. Kartu su veiksminga techninio pažeidžiamumo valdymo praktika, aprašyta IRT naudojimo procedūrose, tai pašalina galimas pagrindines kenkėjiškų veiksmų, įskaitant kenkėjišką programinę įrangą ir jos patvarumą, priežastis.
A.12.3	Atsarginės kopijos	
A.12.3.1	Informacijos atsarginės kopijos	IRT naudojimo procedūros apibrėžia reikalavimus ir įprastas veiklas, susijusias su informacijos atsarginių kopijų kūrimu. Atsarginės kopijos yra užtikrintos visiems klientams teikiamiems „Dokobit“ internetiniams produktams ir paslaugoms. Atsarginio kopijavimo procesas yra automatizuotas ir visiškai suderintas bei patikrintas, kad jis atitiktų deklaruotus RPO ir RTO paslaugų atkūrimui nutraukimo ar avariniu atveju. Be to, „Dokobit“ patikrina ir testuoja atsarginių kopijų vientisumą savo įprastinėje veikloje.
A.12.4	Registravimas ir stebėjimas	
A.12.4.1	Įvykių registravimas	Saugios programinės įrangos kūrimo politikoje nustatytos taisyklės, taikomos saugiam programinės įrangos ir sistemų kūrimui. Joje numatytos išsamios paslaugų / programų registravimo ir stebėjimo gairės.
A.12.4.2	Registruojamos informacijos apsauga	Pagal Saugios programinės įrangos kūrimo politiką turi būti užtikrintas registruojamos informacijos atskyrimas nuo paslaugų ir programų aplinkos (arba per dauginimo mechanizmus).

A.12.4.3	Administratoriaus ir naudotojo registruojama informacija	Pagal Saugios programinės įrangos kūrimo politiką turi būti užtikrintas registruojamos informacijos atskyrimas nuo paslaugų / programų aplinkos (arba per dauginimo mechanizmus). Be to, „Dokobit“ turi vidinę registruojamos infromacijos valdymo sistemą, kuri leidžia laiku ir profilaktiškai prižiūrėti jos klientams teikiamas paslaugas.
A.12.4.4	Laikrodžio sinchronizavimas	Sistemų laikrodžius sinchronizuoja IaaS pardavėjas. Sinchronizavimo nuostatas reikia tikrinti pagal Saugios programinės įrangos kūrimo politikos reikalavimus. Be to, yra naudojama Kvalifikuota laiko žymos priskyrimo institucija.
A.12.5	Operacinės programinės įrangos kontrolė	
A.12.5.1	Programinės įrangos diegimas operacinėse sistemose	Norint įdiegti bet kokią programinę įrangą informacinėse sistemose turi būti taikomas pokyčių valdymas, aprašytas IRT naudojimo procedūrų dokumente. Pokyčių valdymo esmė yra ta, kad kiekvienas pokytis, prieš jį išleidžiant, privalo turėti autorių, būti atsekamas ir dokumentuotas (sekimo sistemoje) ir testuotas bei patvirtintas. Tai yra dokumentuota Priimtino naudojimo ir BYOD politikose.
A.12.6	Techninio pažeidžiamumo valdymas	
A.12.6.1	Techninio pažeidžiamumo valdymas	Pažeidžiamumo atskleidimo politika leidžia bendruomenės lygiu nustatyti („gerųjų ir blogųjų įsilaužėlių“) pažeidžiamumą „Dokobit“ turtuose, kas kartu su proaktyvia techninio pažeidžiamumo valdymo praktika, aprašyta IRT naudojimo procedūrose, sudaro išsamią techninio pažeidžiamumo valdymo sistemą. Už šios veiklos valdymą atsako ISM.
A.12.6.2	Programinės įrangos diegimo apribojimai	Priimtino naudojimo politikoje ir BYOD politikoje nustatyta, kad kompiuteryje draudžiama diegti nelegalią programinę įrangą arba programinę įrangą iš nepatikimų šaltinių. Programinės įrangos diegimui serveriuose taikoma Pokyčių valdymo procedūra, kuri aprašyta IRT naudojimo procedūrų dokumente.
A.12.7	Informacinių sistemų audito apžvalga	

A.12.7.1	Informacinių sistemų audito kontrolės priemonės	„Dokobit“ taiko kelių lygmenų metodą informacinių sistemų audito kontrolės priemonėms. Kūrimo ir išdėstymo metu jis užtikrinamas taikant kodų peržiūrą, testavimą ir patvirtinimą, aprašytus Saugios programinės įrangos kūrimo politikoje. Daugelis kontrolės priemonių užtikrinamos naudojant paslaugų / programų registraciją ir stebėjimą. Įgyvendintos kontrolės priemonės taip pat vertinamos atliekant rizikos vertinimą, kuris vykdomas kiekvienais metais ir specialiai, jei įvyksta didelių pokyčių. Be to, šios kontrolės priemonės vertinamos ankstesnės patirties kontekste, apibrėžtame Incidentų valdymo procedūroje. Konkrečiais atvejais vidaus auditą galima atlikti, siekiant įvertinti informacinių sistemų audito kontrolės priemonių efektyvumą.

3.8 Tinklo saugumas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit Darbo procedūros ir „Dokobit“ Priimtino naudojimo politika. Konkrečiai:

A.13.1	Tinklo saugumo valdymas	
A.13.1.1	Tinklo kontrolės priemonės	ISM atsako už bendrovės tinklų saugumo valdymą ir kontrolę, įskaitant belaidę ir vidinę IaaS aplinką. Tinklo saugumo kontrolės priemonės aprašytos IRT naudojimo procedūrose.
A.13.1.2	Tinklo paslaugų saugumas	ISM atsako už bendrovės tinklų saugumo valdymą ir kontrolę, įskaitant belaidę ir vidinę IaaS aplinką. Tinklo saugumo kontrolės priemonės aprašytos IRT naudojimo procedūrose. Visur įgyvendintas principas „pagal numatytąsias nuostatas drausti“ visus tinklo prievadus, išskyrus „būtinybę naudoti“.
A.13.1.3	Tinklų atskyrimas	ISM atsako už bendrovės tinklų saugumo valdymą ir kontrolę, įskaitant belaidę ir vidinę IaaS aplinką. Tinklo saugumo kontrolės priemonės aprašytos IRT naudojimo procedūrose. Jose pabrėžiamas atskyrimas tinkluose. Todėl gamybos (IaaS), atsarginių kopijų ir biuro kūrimo / testavimo aplinkos tinklai yra atskirti kaip skirtingi tinklo lygmenys.

3.9 Incidentų valdymas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit“ Incidentų valdymo procedūra. Konkrečiai:

A.16.1	Informacijos saugumo incidentų valdymas ir patobulinimai	

A.16.1.1	Atsakomybės ir procedūros	Incidentų valdymo procedūroje nustatytas išsamus informacijos saugumo incidentų valdymo procesas. Procedūra atitinka BDAR ir eIDAS reglamentų reikalavimus, nustatytus Kvalifikuotos patikimumo užtikrinimo paslaugos teikėjams, susijusius su atitinkamu kontekstu ir iš anksto užpildytomis formomis, ir numato visas būtinas atsakomybes „Dokobit“ dėl pranešimo apie incidentus ir jų valdymą. Pavyzdžiui, Valdymo grupė yra atsakinga už: pasirengimą galimiems incidentams; kad būtų sukurta tinkama incidentų registracijos ir stebėsenos sistema; ankstesnių incidentų patirties integravimą į „Dokobit“ veiklą.
A.16.1.2	Pranešimas apie informacijos saugumo įvykius	Pagal Incidentų valdymo procedūrą informacijos saugumo įvykiai gali būti aptinkami viduje „Dokobit“ kontrolės priemonėmis arba apie juos gali pranešti vidaus ar išorės šalys.
A.16.1.3	Pranešimas apie informacijos saugumo trūkumus	Pagal Incidentų valdymo procedūrą informacijos saugumo įvykiai gali būti aptinkami viduje „Dokobit“ kontrolės priemonėmis arba apie juos gali pranešti vidaus ar išorės šalys. Trūkumais laikomos klaidos, gedimai, klaidos programoje, pažeidžiamumai ar kitos programinės ir aparatinės įrangos diegimo, kodų, dizaino ir architektūros klaidos, kurios neištaisytos ir dėl kurių sistemos, tinklai ar aparatinė įranga gali patirti ataką.
A.16.1.4	Informacijos saugumo įvykių vertinimas ir nagrinėjimas	Incidentų valdymo procedūros pradiniame analizės etape apibrėžti saugumo įvykio vertinimo kriterijai. Jei įvykis nepatvirtinamas kaip saugumo incidentas, jis perduodamas nustatyti taisomuosius veiksmus pagal „Dokobit“ Taisomųjų veiksmų procedūrą.
A.16.1.5	Reagavimas į informacijos saugumo incidentus	Incidentų valdymo procedūros pradiniame analizės etape apibrėžti saugumo įvykių vertinimo kriterijai. Jei įvykis patvirtinamas kaip saugumo incidentas, dėl jo atsiranda tolesnių (dokumentuotų) likvidavimo veiksmų, remiantis geriausia tarptautine patirtimi (pirmiausia NIST Special Publication 800-61, ENISA, BDAR ir eIDAS gairėmis). Skyriuje „Izoliavimas, likvidavimas ir atkūrimas“ reagavimas aprašytas išsamiai.
A.16.1.6	Mokymasis iš informacijos saugumo incidentų	Incidentų valdymo procedūroje nustatyti veiksmai po incidento, kai analizuojama ankstesnė patirtis ir rizika gali būti vertinama iš naujo, peržiūrimos kontrolės priemonės, atnaujinami ISMS dokumentai ir imamasi konkrečių gerinimo veiksmų.
A.16.1.7	Įrodymų rinkimas	Incidentų valdymo procedūros skyriuje „Izoliavimas, likvidavimas ir atkūrimas“ nustatyti reikalavimai, keliami įrodymų rinkimui incidento atveju ar po jo.

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 „Dokobit“ Asmens duomenų apsaugos politika, kuri yra sertifikuotos „Dokobit“ ISMS dalis.

3.11 Veiklos tęstinumo valdymas

„Dokobit“ įdiegė verslo tęstinumo valdymo sistemą, kuri yra sertifikuotos „Dokobit“ ISMS dalis ir apima rizikos vertinimo procedūras, reagavimą į incidentus, ekstremaliuosius įvykius ir atkūrimo planus, įskaitant pratybas.

Šiuose planuose aprašomi visi ištekliai ir procesai, reikalingi veiklai atkurti, ir visi verslo tęstinumo valdymo informacijos saugumo aspektai. Tokių planų tikslas yra atkurti paslaugas per nustatytą atkūrimo laiką (RTO). Veiklos atkūrimo planai išbandomi kasmet. Konkrečiai:

A.17.1	Informacijos saugumo tęstinumas	
A.17.1.1	Informacijos saugumo tęstinumo planavimas	Veiklos atkūrimo po ekstremaliųjų įvykių / Verslo tęstinumo planas. Jo tikslas yra aiškiai apibrėžti, kaip „Dokobit“ atkurs savo paslaugas per nustatytą terminą įvykus ekstremaliajam įvykiui ar kitam katastrofiniam įvykiui, nustatytam atliekant rizikos vertinimą. Šio Plano tikslas – užbaigti paslaugų atkūrimą per nustatytą atkūrimo laiką (RTO). Plane aiškiai nurodytos funkcijos ir atsakomybės bei kiekvienos paslaugos planui būdingos priežastys, kurioms atsiradus paslaugos automatiškai atkuriamos alternatyvioje iš anksto parinktoje vietoje.
A.17.1.2	Informacijos saugumo tęstinumo įgyvendinimas	Veiklos atkūrimo po ekstremaliųjų įvykių / Verslo tęstinumo plane išdėstyti visi aktualūs informacijos saugumo tęstinumo aspektai, kurie įtraukti į susijusias procedūras. Šie aspektai apibūdinti atskirame skyriuje „Informacijos saugumo tęstinumo aspektai“.
A.17.1.3	Informacijos saugumo tęstinumo patikra, peržiūra ir vertinimas	Dėl „Dokobit“ veiklos pobūdžio, debesijoje teikiamų paslaugų „Dokobit“ informacijos saugumas yra atsparus trikdantiems įvykiams, todėl, atlikus rizikos vertinimą ir atsižvelgiant į praeities įvykius, nereikia jokių specialių ISMS pakeitimų, kad sistema būtų veiksminga (aktuali ir veikianti) neigiamos situacijos atveju.
A.17.2	Perteklumas	
A.17.2.1	Informacijos tvarkymo priemonių prieinamumas	Rizika, susijusi su paslaugų prieinamumu, nustatoma atliekant rizikos vertinimą. Suplanuojami ir įgyvendinami būtini veiksmai, įskaitant veiksmus pagal Veiklos atkūrimo po ekstremaliųjų įvykių / Verslo tęstinumo planą. Paskelbti susitarimai dėl paslaugų lygio yra nuolat stebimi. Informacijos apdorojimo priemonės yra perteklinės, norint atitikti klientams praneštą RTO.

3.12 TSP nutraukimas ir nutraukimo planai

„Dokobit“ turi naujausią nutraukimo planą pagal ETSI EN 319 401 7.12 punktą.

„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 pats.

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

3.13 Atitiktis

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit Reikalavimų nustatymo procedūra. Procedūros apraše nustatomas suinteresuotųjų šalių atpažinties procesas, nurodomi teisiniai, norminiai, sutartiniai ir kiti reikalavimai ir jų vykdymo atsakomybės. Konkrečiai:

A.18.1	Teisinių ir sutartinių reikalavimų laikymasis	
A.18.1.1	Taikomų įstatymų ir sutartinių reikalavimų nustatymas	Reikalavimų nustatymo procedūroje apibrėžtas suinteresuotųjų šalių nustatymo procesas, taip pat teisiniai, reguliavimo, sutartiniai ir kiti reikalavimai, susiję su informacijos saugumu, ir jų įvykdymo įsipareigojimai. Šios veiklos rezultatas yra tvarkomas ir realus Teisinių, reguliavimo, sutartinių ir kitų reikalavimų sąrašas.
A.18.1.2	Intelektinės nuosavybės teisės	Intelektinės nuosavybės teisės yra Komercinių paslapčių, kurias nustato valdyba, dalis. Jos reguliuojamos pagal ES ir vietinius teisės aktus. Saugant intelektinės nuosavybės teises, sudaromi konfidencialumo susitarimai, nustatomi sutartiniai įsipareigojimai ir atsakomybė bei „Dokobit“ paslaugų sąlygos.
A.18.1.3	Įrašų apsauga	Dokumentų ir įrašų kontrolės procedūra užtikrina ISMS naudojamų dokumentų ir įrašų kūrimo, patvirtinimo, platinimo, naudojimo ir atnaujinimo kontrolę. Bendrai organizacijos darbuotojai gali prieiti prie saugomų dokumentų tik pagal „būtina žinoti“ principą.
A.18.1.4	Asmens tapatybės nustatymo informacijos privatumas ir apsauga	„Dokobit“ veiklai taikomas ES BDAR reglamentas, kurio reikalavimai yra tinkamai įtraukti į organizaciją, įskaitant ISMS dokumentus. Iš konkrečios paslaugos, procesų ar turto savininkų perspektyvos paslaugos, procesų ar turto savininkai yra atsakingi už kiekvieno individualaus reikalavimo nustatymą (įskaitant sutartinius) ir atitiktį turto atžvilgiu. Daugiau informacijos galima rasti Reikalavimų nustatymo procedūroje.

A.18.1.5	Kriptografinių kontrolės priemonių reguliavimas	Kriptografinių kontrolės priemonių naudojimo politikoje apibrėžtos kriptografinių kontrolės priemonių naudojimo, taip pat kriptografinių raktų naudojimo taisyklės, siekiant apsaugoti informacijos konfidencialumą, vientisumą, tikrumą ir informacijos nepaneigiamumą. Kriptografinių kontrolės priemonių naudojimo politikoje taip pat nustatytas raktų valdymas, įskaitant jų paskirstymo praktikas.

4 Parašo Galiojimo 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.

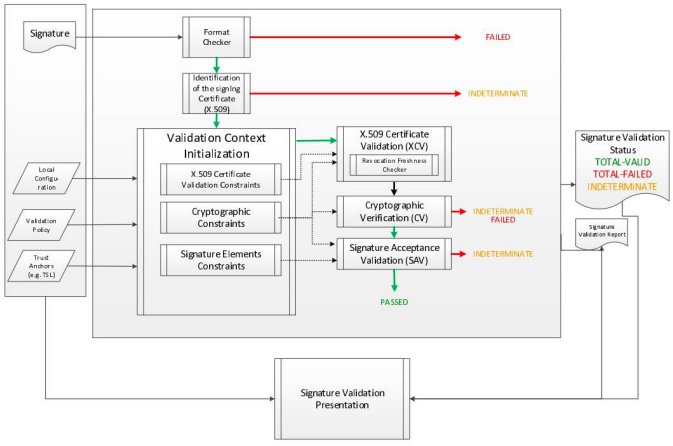
4.1 Parašo galiojimo patvirtinimo proceso reikalavimai

„Dokobit“ galiojimo patvirtinimo paslaugos procedūros, skirtos nustatyti, ar elektroninis parašas arba elektroninis spaudas yra techniškai galiojantis, grindžiamos procesu, aprašytu ETSI TS 119 102 [ETSI 119-102].

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 TS 119 102 5 punkto reikalavimai ir taisyklės.

Kai šioje specifikacijoje nustatyti konkretūs reikalavimai ir taisyklės, jie turi pirmenybę prieš atitinkamus ETSI TS 119 102 reikalavimus. Esant neatitikimų tarp šios specifikacijos ir ETSI TS 119 102 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 – prieinamas per https://app.dokobit.com;
- „Dokobit“ Galiojimo patvirtinimo paslauga – prieinama per https://validation.dokobit.com ir per integracijas į kitas informacijos sistemas;
- „Dokobit Gateway“ – prieinamas per 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 antspauduotą 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 TS 119 102-1, 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.
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.
	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).
	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.

	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.
	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.*	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.*	3.6.1.4.1.54720.1.3

- Parašo galiojimo patvirtinimo paslauga nepriima kelių patvirtinimo politikos šaltinių;
- Parašo galiojimo patvirtinimo politikos negalima nepaisyti ir pakeisti parašo galiojimo patvirtinimo funkcijomis pagal protokolą, nurodytą ETSI TS 119 442;
- Galiojimo patvirtinimo procesas užtikrina, kad naudojama parašo galiojimo patvirtinimo politika atitiktų SVS politikoje apibrėžtą strategiją arba parašo 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.

Atsižvelgiant į ES teisės aktus [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 TS 119 102-1, 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 TS 119 102-1 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 TS 119 102-1, 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 [ETSI 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

(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
(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

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 [ETSI 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 [ETSI 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 [ETSI 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
(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 EN 119 442.

„Dokobit“ parašo 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, skirtus KLASS3-SK – SK-CPS-KLASS3-v8.0, kuriuos galima rasti adresu *https://www.sk.ee/upload/files/SK-CPS-KLASS3-EN-v8_0_20190815.pdf*.

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=KLASS3-SK 2016

2.5.4.97=NTREE-10747013

ou=Sertifitseerimisteenused

o=AS Sertifitseerimiskeskus

c=EE

5 1 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 support 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
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 (6 hours)	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 2 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 support 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
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 (6 hours)	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*