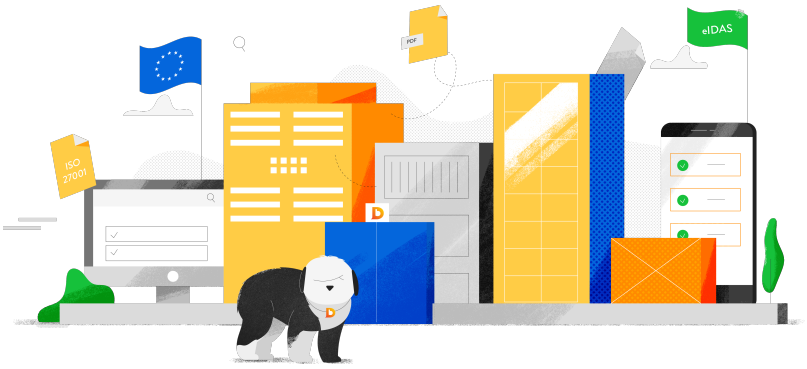


Dokobit kvalifikuotų elektroninių parašų ir spaudų kvalifikuotų galiojimo patvirtinimo paslaugų veiklos nuostatai ir politika

Šis dokumentas yra viešas.

Dokumento numeris: DKB-VSP-06122019 v1.7

Unikalus objekto ID (OID): 1.3.6.1.4.1.54720.1.1

Įsigalioja 2020 01 01

Vertimas iš anglų kalbos.

Turinys

1 Pakeitimų istorija

Date	Versija	Pakeitimo aprašymas
03/08/2018	1.0	Pradinė versija
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 paslaugų komponentai ir paslaugų struktūros schema, atlikti reikiami pakeitimai dėl kvalifikuotos patikimumo užtikrinimo paslaugos teikimo
17/04/2020	1.7	Atnaujinimai • Patikslinta 2.1.2 dalis - nurodytas šio dokumento OID • Patikslinta 2.1.1 dalis - nurodytas Kvalifikuotos parašo galiojimo patvirtinimo paslaugos teikėjo OID • Patikslintos 4.1.3 ir 4.3.1 dalys, nurodant, kad vartotojai autentifikuojami naudojant el. atpažinties priemones • Patikslinta 2.4.3 dalis - Įtrauktas pranešimas priežiūros įstaigai • Patikslinta 4.1.2 dalis - apibrėžtas slapyvardžio naudojimas ataskaitose • Patikslinta 3.12 dalis - įtraukta nuostata dėl pranešimo apie paslaugos nutraukimą • Patikslinta 2.1 dalis - patikslintas taikomų teisės aktų sąrašas

2 Įžanga

2.1 Apžvalga

Šiame dokumente apibūdinama UAB „Dokobit“ (toliau – „Dokobit“) praktika, taikoma teikiant **kvalifikuoto el. parašo ir el. 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 įstatymas*
  - *Dėl Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir kvalifikuotų patikimumo užtikrinimo paslaugų statuso suteikimo ir jų įrašymo į nacionalinį patikimą sąrašą bei kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų veiklos ataskaitų teikimo tvarkos aprašo patvirtinimo* (Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. birželio 21 d. įsakymas Nr. 1V-588)
  - Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2019 m. birželio 4 d. įsakymas Nr. 1V-594 „Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo“)
- Europos standartą *ETSI EN 319 401 (elektroniniai parašai ir infrastruktūra (EPI))*;
- bendruosius reikalavimus patikimumo užtikrinimo paslaugų teikėjams ir kitus susijusius reikalavimus.

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

2.1.1 Palaikoma parašo galiojimo patvirtinimo paslauga

UAB „Dokobit“

Įmonės kodas 301549834

Paupio g. 46, 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 Parašo galiojimo patvirtinimo paslaugos dalyviai

Parašo galiojimo patvirtinimo paslaugos klientas (SVC)

- Programinės įrangos komponentas, suteikiantis aktyvavimo programos, naudojamos „Dokobit“ paslaugų abonentų, vartotojo sąsają.

Aktyvavimo programa (DA)

- Programa, kuri suteikia parašo galiojimo patvirtinimo funkcijas parašo galiojimo patvirtinimo paslaugos 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)

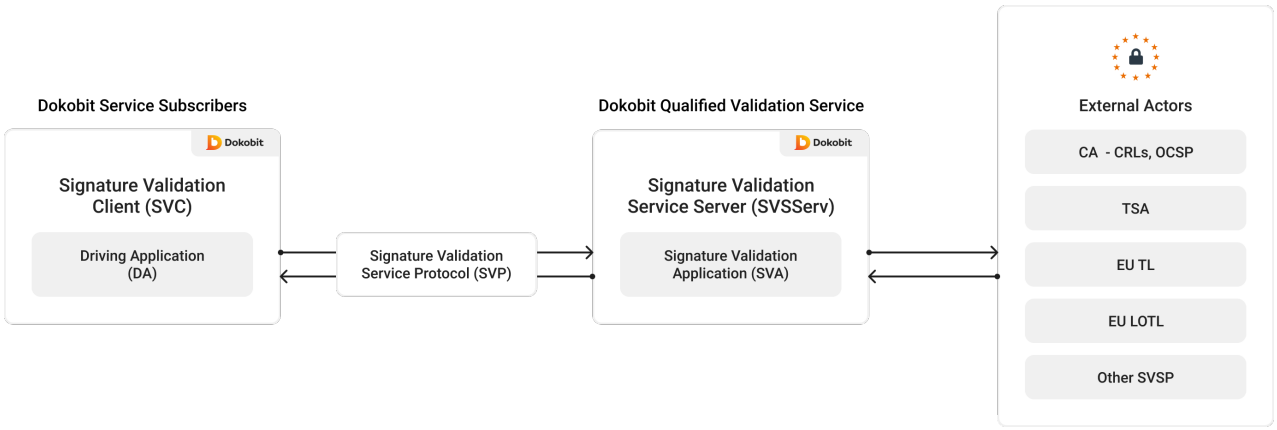
- Už parašo galiojimo patvirtinimą atsakingas programinės įrangos komponentas, kuris vykdo patvirtinimo algoritmą ir sukuria parašo galiojimo patvirtinimo ataskaitą.

Išoriniai dalyviai

- Kiti patikimumo užtikrinimo šaltiniai – sertifikavimo institucijos, laiko žymų tarnybos, tiekėjai įrašyti į Europos patikimąjį sąrašą.

2.2.2 Paslaugos struktūra

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



2.3 Apibrėžtys ir santrumpos

2.3.1 Apibrėžtys

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
Bendrieji duomenys Apsauga 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 paslaugų teikėjas	TSP	Subjektas, teikiantis patikimumo užtikrinimo paslaugą
Kvalifikuotų patikimumo užtikrinimo paslaugų 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

Pavadinimas	Santrumpa	Apibrėžtis
„Dokobit“ parašo galiojimo patvirtinimo veiklos nuostatai ir politika	„Dokobit“ PP	Nuostatai, kuriuose aprašoma praktika, kurią „Dokobit“ taiko teikdama 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 paslaugų teikėjas, išduodantis sertifikatus el. parašui ir/ar 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. 46, 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 veiklos nuostatai

„Dokobit“ atsako už „Dokobit“ galiojimo patvirtinimo paslaugos veiklos nuostatų tvarkymą. Šį dokumentą tvirtina vadovybė ir jis viešai skelbiamas „Dokobit“ interneto svetainėje *(https://www.dokobit.com/lt/patikimumas).*

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

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 likus 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*, 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*).

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. Konkrečiau:

A.6.1.2	Pareigų atskyrimas	ISM ir vidaus auditoriaus vaidmenys yra atskirti. Taip pat įsteigta valdymo grupė svarbiausiems klausimams spręsti. Srityse, kuriose organizacija įžvelgia didesnę riziką, taikomas keturių akių principas. Be to, bendrovė yra parengusi Saugios programinės įrangos kūrimo ir diegimo politiką ir taiko pradinio kodo peržiūros praktiką.

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. Konkrečiau:

A.7.1	**Prieš įdarbinimą**	
A.7.1.1	Atranka	Valdymo grupė atlieka atranką pagal galiojančius įstatymus ir taisykles. Darbuotojai turi pateikti neteistumo pažymą.
A.7.1.2	Įdarbinimo sąlygos ir tvarka	Visi darbuotojai pasirašo darbo sutartį, konfidencialumo sutartį ir visus susijusius ISMS dokumentus.
A.7.2	Įdarbinimo laikotarpiu	
A.7.2.1	Vadovaujančiojo personalo atsakomybė	Vadovybė valdo ISMS ir palaiko jos veiklą. Išsamesnė informacija pateikiama Informacijos saugumo politikoje ir Valdymo praktikos dokumente.
A.7.2.2	Informacijos saugumo suvokimas, švietimas ir mokymas	Mokymai ir instruktažas nurodyti Mokymo ir informavimo plane. Saugaus programinės įrangos kūrimo praktikos, įskaitant saugumo suvokimą, aprašytos „Dokobit“ saugios programinės įrangos kūrimo politikoje.

A.7.2.3	Drausminis procesas	Į konfidencialumo sutartį įtraukti specialūs punktai dėl drausminių priemonių. Drausminę priemonę gali inicijuoti ISM (Informacijos klasifikavimo politika).
A.7.3	Darbo santykių nutraukimas ir darbo pareigų pakeitimas	
A.7.3.1	Darbo sutarties nutraukimas ar pareigų pakeitimas	Pagal konfidencialumo sutartis su darbuotojais konfidencialumo sąlygos galioja ir nutraukus darbo sutartį. Kokius informacijos saugumo aspektus rekomenduojama įtraukti į sutartis, nurodyta Tiekėjo saugumo politikoje.

3.3 Turto valdymas

3.3.1 Bendrieji reikalavimai

„Dokobit“ nuolat atnaujina turto sąrašus, įskaitant informacinius išteklius. Turto nustatymu yra grindžiamas rizikos valdymas. Pagal turto nustatymo duomenis atliekamas rizikos vertinimas, o grėsmės identifikuojamos kaip susijusios su turtu, naudojant išsamius grafikus. Tai yra sertifikuotos „Dokobit“ ISMS dalis, t. y. „Dokobit“ priimtino naudojimo politika, „Dokobit“ informacijos klasifikavimo politika ir „Dokobit“ rizikos valdymo metodika.

A.8.1	**Atsakomybė už turtą**	
A.8.1.1	Turto inventorius	Tarnybinėje lentelėje „Turto sąrašas“ turto savininkai nurodomi abiem aspektais: procesų ir turimo turto.
A.8.1.2	Turto nuosavybė	Lentelė „Turto sąrašas“
A.8.1.3	Priimtinas turto naudojimas	Priimtino turto naudojimo reikalavimai nurodyti Priimtino naudojimo politikoje.
A.8.1.4	Turto grąžinimas	Turto grąžinimas yra numatytas konfidencialumo sutartyse, Priimtino naudojimo politikoje ir Tiekėjo saugumo politikoje.

3.3.2 Laikmenų naudojimas

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

A.8.3	**Laikmenų naudojimas**	
A.8.3.1	Išimamųjų laikmenų tvarkymas	Kaip tvarkyti informaciją, įskaitant popierinę, elektroninę, elektroninę informacinėse sistemose, el. laiškuose, (išimamajame) atminties įtaise, nustatyta Informacijos klasifikavimo politikoje.
A.8.3.2	Laikmenos šalinimas	Šalinimo ir sunaikinimo reikalavimai pateikiami Informacijos ir ryšių technologijų naudojimo procedūrų dokumente.
A.8.3.3	Fizinės laikmenos perdavimas	Taisyklės, kaip elgtis perduodant laikmenas, nustatytos Informacijos klasifikavimo politikoje ir Informacinių ir ryšių technologijų naudojimo procedūrų dokumente.

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. Konkrečiau:

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 vartotojams ar jų grupėms. Daugiau informacijos pateikiama „Dokobit“ prieigos kontrolės politikoje.

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 vartotojams ar jų grupėms. Daugiau informacijos pateikiama „Dokobit“ prieigos kontrolės politikoje.
A.9.2	Vartotojo prieigos valdymas	
A.9.2.1	Vartotojo registracija ir išregistravimas	(Elektroninės) prieigos teikimo taisyklės (įskaitant išregistravimą) išdėstytos Prieigos kontrolės politikoje.
A.9.2.2	Vartotojo prieigos teikimas	(Elektroninės) prieigos teikimo taisyklės išdėstytos Prieigos kontrolės politikoje. Šiame dokumente taip pat pateikiami įmonių paskyros saugos parametrų reikalavimai.
A.9.2.3	Išimtinių prieigos teisių valdymas	Išimtis kiekvienai sistemai (turtui) gali suteikti tik atitinkami savininkai arba ISM. Tai apibrėžiama Prieigos kontrolės politikoje.
A.9.2.4	Slaptos vartotojų atpažinimo informacijos valdymas	Kaip vartotojai turėtų valdyti slaptą atpažinimo informaciją, apibūdinama (Elektroninėse) prieigos teikimo taisyklėse, pateikiamose Prieigos kontrolės politikoje.
A.9.2.5	Vartotojo 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.
A.9.3	Vartotojo atsakomybė	
A.9.3.1	Slaptos atpažinimo informacijos naudojimas	Asmens duomenų tvarkymo užduotys aprašytos Priimtino naudojimo politikoje.

A.9.4	Sistemos ir programų prieigos kontrolė	
A.9.4.1	Prieigos prie informacijos apribojimas	Prieigos prie informacijos apribojimas ir teikimo tvarka nustatyta Informacijos klasifikavimo politikoje.
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 ir programų būtų teikiama naudojant išorinę įmonės paskyros atpažinimo paslaugą.
A.9.4.3	Slaptažodžių valdymo sistema	Įmonių paskyrų saugos nuostatų reikalavimai išdėstyti Prieigos kontrolės politikoje.
A.9.4.4	Naudojimasis privilegijuotosiomis tinklo įrangos programomis	Priimtino naudojimo politikoje yra nustatytas apribojimas, kad vartotojai neturėtų 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 prieinamas tik pagal principą „būtina žinoti“. Informacijos klasifikavimo politikoje nurodomi įgalioti asmenys ir prieigos prie komercinių paslapčių apribojimai (programos pradinis kodas yra komercinė paslaptis). Fiziškai pradinis kodas saugomas pradinio kodo versijų kūrimo sistemoje. Prieigos prie reikiamų šaltinių raktą suteikia ISM.

3.5 Kriptografinės kontrolės priemonės

„Dokobit“ kriptografinių kontrolės priemonių, kurios yra sertifikuotos „Dokobit“ ISMS dalis, naudojimo politika užtikrina saugiųjų kriptografinių algoritmų, raktų 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 politika
A.10.1.2	Raktų valdymas	Kriptografinių kontrolės priemonių naudojimo politika

3.6 Fizinis ir aplinkos saugumas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit“ tiekėjų saugumo politika, „Dokobit“ darbo saugiose zonose procedūros ir „Dokobit“ informacinių ir ryšio technologijų naudojimo procedūros. Konkrečiau:

A.11	**Fizinis ir aplinkos saugumas**	
A.11.1	Saugios zonos	
A.11.1.1	Fizinio saugumo perimetras	Saugios zonos aprašytos dokumente „Darbo saugiose zonose procedūros“.
A.11.1.2	Fizinio įėjimo kontrolė	Prieigos teisė ir įėjimo kontrolė aprašytos dokumente „Darbo saugiose zonose procedūros“.
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.
A.11.1.4	Apsauga nuo išorinių ir aplinkos grėsmių	Biuro patalpų saugumo kontrolės priemonės vertinamos atliekant rizikos vertinimą. Kai nustatoma didesnė nei toleruotina rizika, imamasi reikiamų veiksmų.
A.11.1.5	Darbas saugiose zonose	Saugių zonų taisyklės aprašytos dokumente „Darbo saugiose zonose procedūros“.
A.11.1.6	Pristatymo ir pakrovimo vietos	Viešo naudojimo zonos, įskaitant pristatymo ir pakrovimo zonas (įėjimas į biurų pastatą), kontroliuojamos apsaugos darbuotojo.

A.11.2	Įranga	
A.11.2.1	Įrangos išdėstymas ir apsauga	Labai svarbi vidinė įranga yra saugiose zonose.
A.11.2.2	Pagalbinės priemonės	Prie pradinio kodo ir atsarginių kopijų serverių prijungti nenutrūkstamo maitinimo šaltiniai.
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.
A.11.2.5	Turto pašalinimas	Kaip turtas gali būti išvežamas už įmonės ribų, nustatyta Priimtino naudojimo politikoje.
A.11.2.6	Įrangos ir turto saugumas ne patalpose	Taisyklės, kaip turtas turi būti tvarkomas ir saugomas ne biuro patalpose, pateikiamos Priimtino naudojimo politikoje.
A.11.2.7	Saugus įrangos šalinimas ar pakartotinis naudojimas	Įrangos ir laikmenų šalinimas ir sunaikinimas aprašyti dokumente „Informacijos ir ryšių technologijų naudojimo procedūros“.
A.11.2.8	Neprižiūrima vartotojo įranga	Priimtino naudojimo politika ir Švaraus stalo ir švaraus ekrano politika
A.11.2.9	Švaraus stalo ir švaraus ekrano politika	Priimtino naudojimo politika ir Švaraus stalo ir švaraus ekrano politika

3.7 Operacijų saugumas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit“ informacinių ir ryšio technologijų 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. Konkrečiau:

A.12	**Operacijų saugumas**	
A.12.1	Darbo procedūros ir atsakomybė	
A.12.1.1	Dokumentuotos darbo procedūros	Dokumente „Informacijos ir ryšių technologijų naudojimo procedūros“ yra dokumentuotos darbo procedūros.
A.12.1.2	Pokyčių valdymas	Pokyčių valdymo procedūra aprašyta dokumente „Informacijos ir ryšių technologijų naudojimo procedūros“. Kad būtų užtikrinamas tinkamas galiojimo patvirtinimo paslaugos veikimas, „Dokobit“ po kiekvieno patvirtinimo paslaugos funkcijų pakeitimo atlieka teigiamus ir neigiamus testus (*XAdES*, *PAdES*, *CAdES* parašo galiojimo patvirtinimo testus, funkcijų logikos testus, vartotojo sąsajos testus, saugumo testus ir t. t.).
A.12.1.3	Pajėgumų valdymas	Pajėgumai valdomi atliekant paslaugų ir programų registravimą ir stebėjimą. Išsamesnė informacija pateikiama šiuose dokumentuose: · „Informacijos ir ryšių technologijų naudojimo procedūros“, skyrius „Paslaugų stebėjimas“; · „Saugios programinės įrangos kūrimo politika“, skyrius „Paslaugų ir programų registravimo ir stebėjimo kontrolinis sąrašas“.
A.12.1.4	Kūrimo, testavimo ir naudojimo aplinkos atskyrimas	Vadybos grupė yra atsakinga už tai, kad kūrimo, testavimo ir gamybos aplinkos būtų atskirtos. Daugiau apribojimų ir rekomendacijų pateikiama Saugios programinės įrangos kūrimo politikoje.
A.12.2	Apsauga nuo kenkimo programinės įrangos	

A.12.2.1	Kontrolės priemonės apsaugai nuo kenkimo programinės įrangos	Konfidencialu. Apsaugai nuo kenkimo programinės įrangos bendrovėje taikomi įvairūs saugumo lygiai.
A.12.3	Atsarginės kopijos	
A.12.3.1	Informacijos atsarginės kopijos	Atsarginės kopijos yra aprašytos dokumente „Informacijos ir ryšių technologijų naudojimo procedūros“.
A.12.4	Registravimas ir stebėjimas	
A.12.4.1	Įvykių registravimas	Kaip įgyvendinamas įvykių registravimas ir kas už tai atsakingas, aprašyta saugios inžinerijos principuose ir reikalavimuose, išdėstytuose „Dokobit“ saugios programinės įrangos kūrimo politikoje.
A.12.4.2	Žurnalų informacijos apsauga	Kaip įgyvendinamas įvykių registravimas ir kas už tai atsakingas, aprašyta saugios inžinerijos principuose ir reikalavimuose, išdėstytuose „Dokobit“ saugios programinės įrangos kūrimo politikoje.
A.12.4.3	Administratoriaus ir naudotojo žurnalai	Kaip įgyvendinamas įvykių registravimas ir kas už tai atsakingas, aprašyta saugios inžinerijos principuose ir reikalavimuose, išdėstytuose „Dokobit“ saugios programinės įrangos kūrimo politikoje.
A.12.4.4	Laikrodžio sinchronizavimas	Konfidencialu
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 dokumente „Informacijos ir ryšių technologijų naudojimo procedūros“.
A.12.6	Techninio pažeidžiamumo valdymas	

A.12.6.1	Techninio pažeidžiamumo valdymas	Už techninio pažeidžiamumo valdymą atsako ISM. Techninio pažeidžiamumo valdymas aprašytas dokumente „Informacijos ir ryšių technologijų naudojimo procedūros“.
A.12.6.2	Programinės įrangos diegimo apribojimai	Priimtino naudojimo politikoje nustatyta, kad bendrovės naudojamuose įrenginiuose draudžiama diegti nelegalią programinę įrangą arba programinę įrangą iš nepatikimų šaltinių.
A.12.7	Informacinių sistemų audito apžvalga	
A.12.7.1	Informacinių sistemų audito kontrolės priemonės	Informacinės sistemos kontrolės priemonės vertinamos atliekant rizikos vertinimą, kuris vykdomas anksčiau arba greičiau, jei įvyksta didelių pokyčių.

3.8 Tinklo saugumas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit“ darbo procedūros ir „Dokobit“ priimtino naudojimo politika. Konkrečiau:

A.13.1	Tinklo saugumo valdymas	
A.13.1.1	Tinklo kontrolės priemonės	Visi prievadai ir protokolai draudžiami, nebent yra „būtinybė naudoti“.
A.13.1.2	Tinklo paslaugų saugumas	Visi prievadai ir protokolai draudžiami, nebent yra „būtinybė naudoti“. Tinklo saugumo valdymas aprašytas dokumente „Informacijos ir ryšių technologijų naudojimo procedūros“.
A.13.1.3	Tinklų atskyrimas	Gamybos (*IaaS*), atsarginių kopijų ir biuro aplinkos tinklai yra atskirti.

3.9 Incidentų valdymas

Sertifikuotoje „Dokobit“ ISMS šią sritį apima „Dokobit“ incidentų valdymo procedūra. Konkrečiau:

A.16.1	**Informacijos saugumo incidentų valdymas ir patobulinimai**	
A.16.1.1	Atsakomybė ir procedūros	Incidentų valdymo procedūra. Valdymo grupė yra atsakinga už pasirengimą galimiems incidentams. Tai apima užtikrinimą, kad būtų sukurta tinkama įvykių registracijos ir stebėsenos sistema (išsamią informaciją žr. „Dokobit“ saugios programinės įrangos kūrimo politikoje), ir „Dokobit“ veikloje pritaikoma ankstesnių incidentų patirtis.
A.16.1.2	Pranešimas apie informacijos saugumo įvykius	Incidentų valdymo procedūra. Yra dvi dalys: aptikimas ir ataskaitų teikimas.
A.16.1.3	Pranešimas apie informacijos saugumo trūkumus	Incidentų valdymo procedūra. Skyrius „Pranešimas apie incidentą“. Jis taip pat apima saugumo trūkumus ir įvykius.
A.16.1.4	Informacijos saugumo įvykių vertinimas ir nagrinėjimas	Incidentų valdymo procedūra. Skyrius „Izoliavimas, likvidavimas ir atkūrimas“.
A.16.1.5	Reagavimas į informacijos saugumo incidentus	Incidentų valdymo procedūra. Skyrius „Izoliavimas, likvidavimas ir atkūrimas“.
A.16.1.6	Mokymasis iš informacijos saugumo incidentų	Incidentų valdymo procedūra. Skyrius „Veikla po įvykio“.
A.16.1.7	Įrodymų rinkimas	Incidentų valdymo procedūra. Skyrius „Izoliavimas, likvidavimas ir atkūrimas“.

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 kasmet išbandomi. Konkrečiau:

A.17.1	**Informacijos saugumo tęstinumas**	
A.17.1.1	Informacijos saugumo tęstinumo planavimas	Veiklos atkūrimo po ekstremaliųjų įvykių planas. Veiklos atkūrimo po ekstremaliųjų įvykių plano 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 – atkurti paslaugas per nustatytą atkūrimo laiką (RTO).
A.17.1.2	Informacijos saugumo tęstinumo įgyvendinimas	Veiklos atkūrimo po ekstremaliųjų įvykių planas
A.17.1.3	Informacijos saugumo tęstinumo patikra, peržiūra ir vertinimas	Veiklos atkūrimo po ekstremaliųjų įvykių planas
A.17.2	Perteklumas	
A.17.2.1	Informacijos tvarkymo priemonių prieinamumas	Rizika, susijusi su paslaugų prieinamumu, nustatoma atliekant rizikos vertinimą. Suplanuojami būtini veiksmai.

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 patys.

„Dokobit“ pasilieka teisę nutraukti kvalifikuotų elektroninių parašų ir spaudų kvalifikuota galiojimo patvirtinimo paslaugą, apie tai pranešę Paslaugos gavėjams ir Priežiūros įstaigai ne vėliau kaip prieš 3 mėnesius.

Nuoroda: „Dokobit“ patikimumo užtikrinimo paslaugų nutraukimo planas

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 atsakomybė už jų vykdymą. Konkrečiau:

A.18.1	**Teisinių ir sutartinių reikalavimų laikymasis**	
A.18.1.1	Taikomų įstatymų ir sutartinių reikalavimų nustatymas	Reikalavimų nustatymo procedūra
A.18.1.2	Intelektinės nuosavybės teisės	Tai yra komercinių paslapčių, kurias nustato valdyba, dalis. Šis aspektas reglamentuojamas pagal ES ir vietos įstatymus.
A.18.1.3	Įrašų apsauga	Dokumentų ir įrašų kontrolės procedūra
A.18.1.4	Asmens tapatybės nustatymo informacijos privatumas ir apsauga	Už kiekvieno individualaus reikalavimo nustatymą (įskaitant sutartinius) ir laikymąsi atsakingi paslaugos, procesų ir turto savininkai. Daugiau informacijos galima rasti skyriuje „Reikalavimų nustatymo procedūra“.
A.18.1.5	Kriptografinių kontrolės priemonių reguliavimas	Kriptografinių kontrolės priemonių naudojimo politika

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 vartotojas 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.

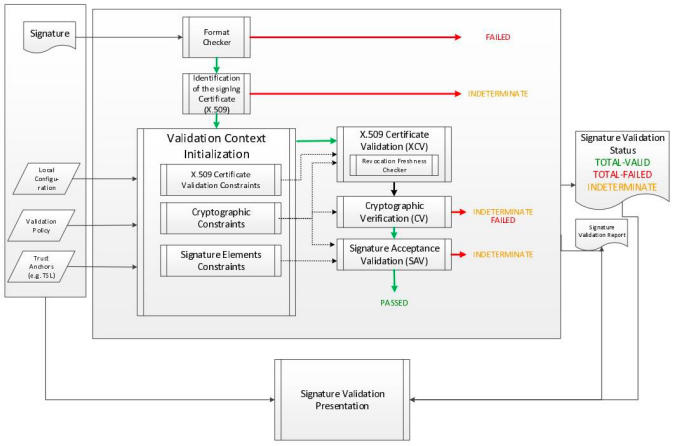
4.1 Parašo galiojimo patvirtinimo proceso reikalavimai

„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), skirta „Dokobit“ galiojimo patvirtinimo paslaugai, gali būti:

- „Dokobit“ portalas;
- „Dokobit Gateway“;
- „Dokobit“ galiojimo patvirtinimo paslaugos API sąsaja.

„Dokobit“ galiojimo patvirtinimo paslauga priima tvirtinti tik vieną failą 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 ir „Dokobit Gateway“ ataskaitą pateikia vartotojui suprantamu būdu – kaip žmonėms suprantamą HTML puslapį.

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.	1. 3.6.1.4.1.54720.1.2
AdES galiojimo patvirtinimo politika • Pradinis patvirtinimas: patikrinama, ar dokumentas nebuvo pakeistas, ir pateikiama būtinoji informacija apie elektroninių parašų ir spaudų teisinį pobūdį ir galiojimo patvirtinimą pagal ES reglamentą Nr. 910/2014 (*eIDAS*). Ši politika yra numatytoji „Dokobit“ portale ir „Dokobit Gateway“.	1. 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.
1. Kai galiojimo patvirtinimo būsena, kurią nurodo pasirinktas patvirtinimo procesas, nurodo būsenos indikaciją PASSED, SVA pateikia DA būsenos indikaciją TOTAL-PASSED.
1. Kai galiojimo patvirtinimo būsena, kurią nurodo pasirinktas patvirtinimo procesas, nurodo būsenos indikaciją FAILED, SVA pateikia DA būsenos indikaciją TOTAL-FAILED.
1. Kitu atveju SVA pateikia būsenos indikaciją INDETERMINATE.

Atsižvelgiant į ES teisės aktus [Komisijos įgyvendinimo sprendimas (ES) 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. Nustatomas kliento tapatumas naudojant elektroninės atpažinties priemonę.

2. Vartotojas 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. Klientui pateikiama ataskaita;

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

1. Klientas 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 vartotojo 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 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 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
EUQualifiedCertificateRequired	Taip
EUQualifiedCertificateSigRequired	Taip
EUQualifiedCertificateSealRequired	Taip
EUQSCDRequired [1]	Taip, jei naudojama QES patvirtinimo politika; ne, jei naudojama *AdES* patvirtinimo politika

1. Remiantis [ETSI 119 172-1] C priedu. Šie apribojimai nurodo reikalavimus specifiniams sertifikatų metaduomenims, kurių semantika taikoma ES teisės aktų kontekste:

a) *EUQualifiedCertificateRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti kvalifikuotas sertifikatas, kaip apibrėžta galiojančiuose ES teisės aktuose; išreiškiamas kaip loginis.

b) *EUQualifiedCertificateSigRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti kvalifikuotas elektroninio parašo sertifikatas, kaip apibrėžta [*eIDAS*]; išreiškiamas kaip loginis.

c) *EUQualifiedCertificateSealRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti kvalifikuotas elektroninio spaudo sertifikatas, kaip apibrėžta [*eIDAS*]; išreiškiamas kaip loginis.

d) *EUQSCDRequired*. Šis apribojimas rodo, kad pasirašiusiojo sertifikatas, naudojamas patvirtinant parašo galiojimą, turi būti susijęs su privačiu raktu, kuris laikomas kvalifikuotame parašo kūrimo įtaise, kaip apibrėžta [*eIDAS*]; išreiškiamas kaip loginis.

Kriptografiniai apribojimai

„Dokobit“ galiojimo patvirtinimo paslauga palaiko šiuos kriptografinius apribojimus, kurie nurodo algoritmų ir parametrų, naudojamų kuriant parašus arba naudojamų patvirtinant pasirašytą objektą, reikalavimus, kaip nurodyta ETSI TS 119 172-1 [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 programa);
- kaip vartotojo sąsaja („Dokobit“ portalas).

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 saugos kanalą. SVSP garantuoja, kad jis gali sukurti saugų kanalą ryšiui su klientu ir išsaugoti duomenų konfidencialumą.

„Dokobit“ portale reikalaujama, kad klientas savo tapatybę patvirtintų naudojant 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 programoje reikia, kad vartotojas 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. paprasta galiojimo patvirtinimo ataskaita, kurioje pateikiama reikiama informacija apie pasirašančiojo asmens tapatybę ir kiekvieno patvirtinto parašo būsenos indikaciją, įskaitant papildomą indikaciją;
2. išsami 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