



**LIETUVOS RESPUBLIKOS
RYŠIŲ REGULIAVIMO TARNYBOS
DIREKTORIUS**

**ĮSAKYMAS
DĖL PRANEŠIMŲ APIE PATIKIMUMO UŽTIKRINIMO PASLAUGŲ SAUGUMO IR
(AR) VIENTISUMO PAŽEIDIMUS TEIKIMO TVARKOS APRAŠO PATVIRTINIMO**

2019 m. birželio 4 d. Nr. 1V-594

Vilnius

Vadovaudamasis Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymo 4 straipsnio 2 dalies 7 punktu, 17 straipsnio 1 dalimi, 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, (OL 2014 L 257, p. 73) 19 straipsnio 2 dalimi ir atsižvelgdamas į Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) 2017 m. kovo 1 d. gaires „Pranešimas apie incidentus pagal 19 straipsnį“:

1. Tvirtinu Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašą (pridedama).

2. N u r o d a u paskelbti šį įsakymą Teisės aktų registre.

Direktorius

Feliksas Dobrovolskis

PATVIRTINTA

Lietuvos Respublikos ryšių reguliavimo
tarnybos direktoriaus 2019 m. birželio 4 d.
įsakymu Nr. 1V-594

**PRANEŠIMŲ APIE PATIKIMUMO UŽTIKRINIMO PASLAUGŲ SAUGUMO IR (AR)
VIENTISUMO PAŽEIDIMUS TEIKIMO TVARKOS APRAŠAS**

1. Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašas (toliau – Aprašas) reglamentuoja pranešimų apie saugumo ir (ar) vientisumo pažeidimus (toliau – pažeidimai) teikimo Lietuvos Respublikos ryšių reguliavimo tarnybai (toliau – Tarnyba) tvarką.

2. Apraše vartojamos sąvokos apibrėžtos Reglamente (ES) Nr. 910/2014 ir Lietuvos Respublikos elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatyme.

3. Patikimumo užtikrinimo paslaugų teikėjai privalo:

3.1. nepagrįstai nedelsdami, tačiau ne vėliau nei per 24 val. nuo to momento, kai sužino apie pažeidimą, turėjusį didelį poveikį teikiamai patikimumo užtikrinimo paslaugai arba ją teikiant naudojamiems asmens duomenims (toliau – pažeidimas, turėjęs didelį poveikį), nurodytą Aprašo 2 priede, informuoti apie jį Tarnybą elektroninio pašto adresu incidentai@rrt.lt ir pateikti tuo metu turimą informaciją apie pažeidimą;

3.2. ne vėliau nei per 3 darbo dienas nuo pažeidimo, turėjusio didelį poveikį, nurodyto Aprašo 2 priede, suvaldymo ar pasibaigimo informuoti apie tai Tarnybą elektroninio pašto adresu incidentai@rrt.lt ir pateikti užpildytą Aprašo 1 priede nustatytos formos pranešimą;

3.3. ne vėliau kaip prieš 5 darbo dienas informuoti patikimumo užtikrinimo paslaugų gavėjus ir Tarnybą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti nepertraukiamą patikimumo užtikrinimo paslaugų teikimą;

3.4. pateikti Tarnybai atsakingo asmens, su kuriuo būtų galima susisiekti, siekiant operatyviai apsikeisti informacija apie pažeidimus ir jų valdymo priemones tarp Tarnybos ir patikimumo užtikrinimo paslaugų teikėjų, kontaktinę informaciją (vardą, pavardę, telefono ryšio numerį, elektroninio pašto adresą). Pasikeitus atsakingam asmeniui ar jo kontaktinei informacijai, Tarnybai turi būti pateikta atnaujinta informacija ne vėliau kaip kitą darbo dieną nuo duomenų pasikeitimo.

4. Patikimumo užtikrinimo paslaugų teikėjai turi teisę informuoti Tarnybą apie kitus, Aprašo 2 priede nenurodytus, pažeidimus ir kitus, jų nuomone, svarbius įvykius, susijusius su patikimumo užtikrinimo paslaugų saugumu ir (ar) vientisumu.

5. Tarnyba užtikrina gautos konfidencialios informacijos apsaugą nuo neteisėto šios informacijos paviešinimo, taip pat užtikrina, kad ši informacija nebūtų atskleista, kopijuojama ar naudojama kitiems tikslams, kurie gali sukelti neigiamų padarinių konfidencialią informaciją pateikusiam asmeniui, išskyrus teisės aktuose numatytus atvejus.

6. Patikimumo užtikrinimo paslaugų teikėjai, pažeidę Aprašo reikalavimus, atsako Lietuvos Respublikos administracinių nusižengimų kodekso nustatyta tvarka.

Pranešimų apie patikimumo užtikrinimo
paslaugų saugumo ir (ar) vientisumo
pažeidimus tvarkos aprašo
1 priedas

**(Pranešimo apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimą
forma)**

(juridinio asmens pavadinimas arba fizinio asmens vardas ir pavardė)

(kontaktinis asmuo, telefono ryšio numeris, el. pašto adresas)

Lietuvos Respublikos ryšių reguliavimo tarnybai
Mortos g. 14, 03219 Vilnius
Tel. (8 5) 210 5634, faks. (8 5) 216 1564
El. paštas incidentai@rrt.lt

**PRANEŠIMAS APIE PATIKIMUMO UŽTIKRINIMO PASLAUGŲ SAUGUMO
IR (AR) VIENTISUMO PAŽEIDIMĄ**

_____Nr. _____
(data)

(sudarymo vieta)

1. Patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimo (toliau – pažeidimas) apibūdinimas	
2. Patikimumo užtikrinimo paslaugų (toliau – paslaugos) neveikimo laikotarpis (valandomis)	
3. Pažeidimo pradžios ir pabaigos data ir laikas (minučių tikslumu)	
4. Paslaugų naudotojų, kuriuos paveikė pažeidimas, skaičius	
5. Pažeidimo poveikis asmens duomenims	
6. Pažeidimo ryšys su kitais pažeidimais, jei toks yra	

7. Ar yra tarpvalstybinis poveikis? Jei taip, nurodyti valstybes	☐ Taip ☐ Ne _____		
8. Paveiktos paslaugos	Elektroninių parašų sertifikatų sudarymas	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninių parašų galiojimo patvirtinimas	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninių parašų ilgalaikė apsauga	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninių spaudų sertifikatų sudarymas	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninių spaudų galiojimo patvirtinimas	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninių spaudų ilgalaikė apsauga	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninių laiko žymų kūrimas	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninis registruotas pristatymas	☐ Kvalifikuota	☐ Nekvalifikuota
	Interneto svetainių tapatumo nustatymo sertifikatų sudarymas	☐ Kvalifikuota	☐ Nekvalifikuota
	Elektroninių parašų kūrimas		☐ Nekvalifikuota
	Elektroninių spaudų kūrimas		☐ Nekvalifikuota
	9. Pažeidimo numeris (-iai) (nurodoma pagal Aprašo 2 priedo I ir II skyrius)		
10. Paveiktos platformos	☐ Registravimo tarnybos (angl. <i>Registration Authority</i>) platforma ☐ Sertifikavimo tarnybos (angl. <i>Certification Authority</i>) platforma ☐ Sertifikatų galiojimo patvirtinimo tarnybos (OCSP/CRL) platforma ☐ Elektroninių parašų (spaudų) kūrimo platforma ☐ Elektroninių parašų (spaudų) galiojimo patvirtinimo platforma ☐ Elektroninių parašų (spaudų) ilgalaikės apsaugos platforma ☐ Laiko žymos tarnybos (angl. <i>Time Stamping Authority</i>) platforma ☐ Elektroninio registruoto pristatymo platforma ☐ Tinklo platforma ☐ Archyvas ☐ Fiziniai įrenginiai ☐ Programinė įranga ☐ Kita (įrašykite) _____		
11. Paveikta savybė ir poveikio mastas (nurodoma pagal Aprašo 2 priedo III skyrių)	Konfidencialumas	Vientisumas	Prieinamumas
	☐ Mažas ☐ Vidutinis ☐ Didelis	☐ Mažas ☐ Vidutinis ☐ Didelis	☐ Mažas ☐ Vidutinis ☐ Didelis
12. Pažeidimo priežasčių kategorijos	☐ Žmogiška klaida ☐ Sistemos klaida ☐ Nenugalimos jėgos (force majeure) aplinkybės ☐ Tyčiniai kenkėjiški veiksmai (virusai, kibernetinės atakos ir pan.) ☐ Trečiųjų šalių klaidos ☐ Kita (įrašykite) _____		

13. Detalios pažeidimo priežastys	☐ Paslaugos trikdymo ataka (angl. <i>DOS</i>) ☐ Virusai, sistemos užvaldymas ☐ Vagystė ar duomenų praradimas ☐ Elektros gedimas ☐ Fizinių įrenginių gedimas ☐ Programinės įrangos spraga ☐ Sugedusių fizinių įrenginių keitimas ☐ Programinės įrangos spragos šalinimas ☐ Asmens duomenų klastojimas ☐ Kriptoanalizė ☐ Sistemų per didelis apkrovimas (angl. <i>Overload</i>) ☐ Politikos ar procedūrų trūkumas ☐ Sistemos išjungimas saugumo tikslais ☐ Kita (įrašykite) _____
14. Veiksmai, kurių imtasi siekiant suvaldyti pažeidimą	
15. Pritaikytos (planuojamos taikyti) priemonės ir (ar) veiksmai, kurių imtasi (arba planuojama imtis), siekiant išvengti panašių pažeidimų ateityje (angl. <i>lessons learned</i>)	
16. Saugumo priemonės, pritaikytos siekiant sušvelninti pažeidimo pasekmes	
17. Asmenys, kurie buvo informuoti apie pažeidimą	☐ Valstybinė duomenų apsaugos inspekcija ☐ Nacionalinis kibernetinio saugumo centras ☐ Nukentėję paslaugos gavėjai ☐ Visuomenė ☐ Kita (įrašykite) _____

(pareigos)¹

(parašas)

(vardas pavardė)

¹ Nurodoma, jei pranešimą teikia juridinis asmuo.

Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus tvarkos aprašo
2 priedas

**PATIKIMUMO UŽTIKRINIMO PASLAUGŲ SAUGUMO IR (AR) VIENTISUMO
PAŽEIDIMŲ, TURĖJUSIŲ DIDELĮ POVEIKĮ TEIKIAMAI PATIKIMUMO
UŽTIKRINIMO PASLAUGAI ARBA JĄ TEIKIANT NAUDOJAMIEMS ASMENS
DUOMENIMS, APRAŠYMAS**

**I SKYRIUS
PAŽEIDIMŲ SĄRAŠAS**

A. PAŽEIDIMAI, TURINTYS POVEIKIO KONKREČIAI PATIKIMUMO UŽTIKRINIMO PASLAUGAI			
A.1. Sertifikatų (elektroninių parašų, spaudų ar interneto svetainių tapatumo nustatymo) sudarymas			
	A.1.1. Išdavimo procesas		
		A.1.1.1. Prašymas išduoti sertifikatą	
			A.1.1.1.1. Apsimetimas kitu žmogumi
			A.1.1.1.2. Neigimas, kad buvo teiktas prašymas išduoti sertifikatą
		A.1.1.2. Sertifikatų išdavimas	
			A.1.1.2.1. Atskleidimas
			A.1.1.2.2. Klastojimas
			A.1.1.2.3. Neteisėtas išdavimas
	A.1.2. Įtaisai (elektroninio parašo ar spaudo kūrimo įtaisai arba patikimumo užtikrinimo paslaugų teikėjų įrenginiai)		
		A.1.2.1. Vagystė	
		A.1.2.2. Atskleidimas	
		A.1.2.3. Kopijavimas	
		A.1.2.4. Slaptažodžio atskleidimas	
		A.1.2.5. Įtaiso pažeidimas neprisijungus	
		A.1.2.6. Sukčiavimas ar apgaudinėjimas	
		A.1.2.7. Apgaule įgytas pasitikėjimas	
	A.1.3. Sertifikatų, įtaisų ir autentifikavimo duomenų valdymas		
		A.1.3.1. Autentifikavimo duomenų saugojimas	
			A.1.3.1.1. Atskleidimas
			A.1.3.1.2. Klastojimas
			A.1.3.1.3. Kopijavimas
		A.1.3.2. Tikrinimas	
			A.1.3.2.1. Atskleidimas
			A.1.3.2.2. Klastojimas
			A.1.3.2.3. Nepasiekiamumas
		A.1.3.3. Išdavimas, atnaujinimas, pakartotinis išdavimas	
			A.1.3.3.1. Atskleidimas
			A.1.3.3.2. Klastojimas
			A.1.3.3.3. Neteisėtas išdavimas

		A.1.3.3.4. Pažeidžiamas protokolas
		A.1.3.4. Sertifikatų, įtaisų ir autentifikavimo duomenų atšaukimas
		A.1.3.4.1. Uždelstas sertifikatų galiojimo atšaukimas, sustabdymas
		A.1.3.4.2. Įtaiso naudojimas po jo autentifikavimo duomenų atšaukimo arba galiojimo pabaigos
		A.1.4. Sertifikatų galiojimo patvirtinimas
		A.1.4.1. Neteisingas atsakymas patvirtinant sertifikatų galiojimą
		A.1.4.2. Neatitikimas tarp CRL ir OCSP
		A.1.4.3. Pakartotinė ataka
		A.1.4.4. Nepasiekiamumas
		A.2. Elektroninių laiko žymių kūrimas
		A.2.1. Nesinchronizuotas laiko žymų tarnybų laikas
		A.2.2. Nepasiekiamumas
		A.2.3. Klaidingos laiko žymos
		A.3. Elektroninis registruotas pristatymas
		A.3.1. Nepasiekiamumas
		A.4. Elektroninių parašų, spaudų kūrimas
		A.4.1. Nepasiekiamumas
		A.4.2. Neteisingas atsakymas
		A.4.3. Neteisingas parašo, spaudo kūrimas
		A.4.4. Nėra sinchronizacijos
		A.5. Elektroninių parašų, spaudų galiojimo patvirtinimas
		A.5.1. Nepasiekiamumas
		A.5.2. Neteisingas atsakymas
		A.5.3. Nepavykęs elektroninių parašų galiojimo patvirtinimas
		A.5.4. Nėra sinchronizacijos
		A.6. Elektroninių parašų, spaudų ilgalaikė apsauga
		A.6.1. Nepasiekiamumas
		A.6.2. Prieigos teisės
		A.6.3. Duomenų vientisumas
		A.6.4. Nepavykęs elektroninių parašų galiojimo patvirtinimas
		A.6.5. Pasenę duomenų formatai
		B. PAŽEIDIMAI, TURINTYS POVEIKIO KELIOMS PATIKIMUMO UŽTIKRINIMO PASLAUGOMS
		B.1. Autentifikavimas
		B.1.1. Bandymai prisijungti spėjimo būdu
		B.1.2. Sukčiavimas ar apgaudinėjimas
		B.1.3. „Isiterpimas“ (angl. <i>eavesdropping</i>)
		B.1.4. Pakartojimai (angl. <i>replay attacks</i>)
		B.1.5. Sesijos užgrobimas (angl. <i>session hijacking</i>)
		B.1.6. Tarpininkas (angl. <i>man in the middle</i>)
		B.2. Poveikis programinei įrangai
		B.3. „Sukompromituotas“ privatus raktas
		B.4. Netinkamas algoritmų naudojimas

B.5. Netyčinis sertifikatų naudojimas kitiems tikslams
B.6. Pažeidimas įtaisuose su kriptografiniais raktais
B.7. Archyvavimo problemos
B.8. Tinklo įrangos sutrikimai

II SKYRIUS PAŽEIDIMŲ APRAŠYMAS

A. PAŽEIDIMAI, TURINTYS POVEIKIO KONKREČIAI PATIKIMUMO UŽTIKRINIMO PASLAUGAI

A.1. Sertifikatų (elektroninių parašų, spaudų ar interneto svetainių tapatumo nustatymo) sudarymas

A.1.1. Išdavimo procesas

A.1.1.1. Prašymas išduoti sertifikatą

A.1.1.1.1. Apsimetimas kitu žmogumi. Asmuo, norintis gauti sertifikatą, patikimumo užtikrinimo paslaugų teikėjui pateikia suklastotus asmens tapatybę patvirtinančius dokumentus.

A.1.1.1.2. Neigimas, kad buvo teiktas prašymas išduoti sertifikatą. Asmuo neigia, kad prašė patikimumo užtikrinimo paslaugų teikėjo išduoti sertifikatą ir (ar) kad tuo sertifikatu naudojosi.

A.1.1.2. Sertifikatų išdavimas

A.1.1.2.1. Atskleidimas. Nukopijuojamas asmens privatus kriptografinis raktas.

A.1.1.2.2. Klastojimas. Suklastojamas asmens naudojamo elektroninio parašo ar spaudo kūrimo įtaiso slaptažodis jo išdavimo ar atnaujinimo metu.

A.1.1.2.3. Neteisėtas išdavimas. Asmeniui išduodamas sertifikatas arba autentifikavimo duomenys kito asmens vardu.

A.1.2. Įtaisai (elektroninio parašo ar spaudo kūrimo įtaisai arba patikimumo užtikrinimo paslaugų teikėjų įrenginiai).

A.1.2.1. Vagystė. Įtaisas pavagiamas.

A.1.2.2. Atskleidimas. Įtaise naudojami nesaugūs kriptografiniai algoritmai (pavyzdžiui, atsakymai į įtaiso užklausas yra lengvai gaunami ieškant įvairiuose duomenų šaltiniuose).

A.1.2.3. Kopijavimas. Įtaisas ir (arba) jame esanti informacija nukopijuojami.

A.1.2.4. Slaptažodžio atskleidimas. Įtaiso informacija arba autentifikavimo duomenys atskleidžiami asmeniui, kuris neturi teisės jų gauti, kol patikimumo užtikrinimo paslaugos gavėjas tokią informaciją ar duomenis siunčia per tinklą.

A.1.2.5. Įtaiso pažeidimas neprisijungus. Įtaiso informacija atskleidžiama nenaudojant įtaiso.

A.1.2.6. Sukčiavimas ar apgaudinėjimas. Įtaiso informacija arba autentifikavimo duomenys yra gaunami automatizuotu būdu apgavus patikimumo užtikrinimo paslaugos gavėją, kai asmuo apsimeta trečiąja šalimi (angl. *phishing and pharming*).

A.1.2.7. Apgaule įgytas pasitikėjimas. Asmuo patikimumo užtikrinimo paslaugos gavėją priverčia pasitikėti juo ir įtikina atskleisti įtaiso informaciją arba autentifikavimo duomenis.

A.1.3. Sertifikatų, įtaisų ir autentifikavimo duomenų valdymas

A.1.3.1. Autentifikavimo duomenų saugojimas

A.1.3.1.1. Atskleidimas. Atskleidžiamas arba pakoreguojamas patikimumo užtikrinimo paslaugų teikėjo sistemose saugomas patikimumo užtikrinimo paslaugų gavėjo vardas ir slaptažodis.

A.1.3.1.2. Klastojimas. Pakeičiami failai, kuriame saugomi susieti patikimumo užtikrinimo paslaugų gavėjų vardai ir slaptažodžiai, nurodyti slaptažodžiai.

A.1.3.1.3. Kopijavimas. Asmens autentifikavimo duomenys buvo nukopijuoti be asmens žinios kenkėjiškais tikslais.

A.1.3.2. Tikrinimas

A.1.3.2.1. Atskleidimas. Užklauso ir atsakymai tarp sertifikavimo tarnybos ir sertifikatų galiojimo patvirtinimo tarnybos yra matomi neturintiems teisės matyti asmenims.

A.1.3.2.2. Klastojimas. Asmuo gali maskuotis kaip sertifikavimo tarnyba ir pateikti klaidingus atsakymus į sertifikatų galiojimo patvirtinimo tarnybos siunčiamas tikrinimo užklauso.

A.1.3.2.3. Nepasiekiamumas². Slaptažodžių failas arba patikimumo užtikrinimo paslaugų teikėjo informacinės sistemos nepasiekiamos ir nėra galimybės susieti patikimumo užtikrinimo paslaugų gavėjo vardą su slaptažodžiu.

A.1.3.3. Išdavimas, atnaujinimas, pakartotinis išdavimas

A.1.3.3.1. Atskleidimas. Slaptažodis, kurį patikimumo užtikrinimo paslaugų teikėjas atnaujina patikimumo užtikrinimo paslaugos gavėjui, neteisėtai nukopijuojamas, kai jis perdavinėjamas iš patikimumo užtikrinimo paslaugų teikėjo patikimumo užtikrinimo paslaugos gavėjui.

A.1.3.3.2. Klastojimas. Atnaujintas slaptažodis, sukurtas patikimumo užtikrinimo paslaugos gavėjo, neteisėtai pakeičiamas, kai jis teikiamas patikimumo užtikrinimo paslaugų teikėjui, siekiant pakeisti pasibaigusį slaptažodį.

A.1.3.3.3. Neteisėtas išdavimas. Patikimumo užtikrinimo paslaugų teikėjo sistemos pažeidžiamos per neteisėtą fizinę ar loginę prieigą ir dėl to sukuriama suklastoti autentifikavimo duomenys.

A.1.3.3.4. Pažeidžiamas protokolas. Neteisėtai pasinaudojama pažeidžiamu autentifikavimo duomenų išdavimo, atnaujinimo protokolu.

A.1.3.4. Sertifikatų, įtaisų ir autentifikavimo duomenų atšaukimas

A.1.3.4.1. Uždelstas sertifikatų galiojimo atšaukimas, sustabdymas. Laiku neatnaujintas sertifikatų atšaukimo sąrašas (angl. *certificate revocation list*) (toliau – CRL) leidžia pasinaudoti sertifikatais, kurie turėjo būti atšaukti.

A.1.3.4.2. Įtaiso naudojimas po jo autentifikavimo duomenų atšaukimo arba galiojimo pabaigos. Autentifikavimui skirtas įtaisas (pvz., kodų generatorius) naudojamas po to, kai atitinkami įtaiso autentifikavimo duomenys buvo atšaukti arba pasibaigė jų galiojimo laikas.

A.1.4. Sertifikatų galiojimo patvirtinimas

A.1.4.1. Neteisingas atsakymas patvirtinant sertifikatų galiojimą. Pateikiama klaidinga informacija apie sertifikato galiojimą.

A.1.4.2. Neatitikimas tarp CRL ir OCSP. Neatitikimas tarp CRL esančios ir OCSP (angl. *Online Certificate Status Protocol*) teikiamos informacijos apie sertifikato galiojimą.

A.1.4.3. Pakartotinė ataka. Asmuo sugeba apgaulingai pakartoti arba atidėti duomenų apie sertifikato galiojimą perdavimą.

A.1.4.4. Nepasiekiamumas². Sertifikatų galiojimo patvirtinimo platforma laikinai nepasiekiamas, o tai sukelia patikimumo užtikrinimo paslaugų gavėjų programų (pavyzdžiui, pasirašymo ar tikrinimo) neveikimą dėl to, kad negaunama reikalinga informacija.

A.2. Elektroninių laiko žymų kūrimas

A.2.1. Nesinchronizuotas laiko žymų tarnybų laikas. Trūksta sinchronizacijos tarp patikimumo užtikrinimo paslaugų teikėjo naudojamo laiko šaltinio ir pasaulinio koordinuotojo laiko (UTC).

A.2.2. Nepasiekiamumas².

² Nepasiekiamumas laikomas didelio poveikio pažeidimu, kai trunka 1 valandą ir ilgiau ir kai yra pažeidžiami patikimumo užtikrinimo paslaugos teikėjo įsipareigojimai prieš trečiąsias šalis dėl patikimumo užtikrinimo paslaugos prieinamumo.

- Laiko žymų sudarymo tarnybos platforma laikinai nepasiekiamą, o tai sukelia patikimumo užtikrinimo paslaugų gavėjų programų neveikimą dėl to, kad negaunama reikalinga laiko žyma.
- Laiko žymų patvirtinimui naudojamų sertifikatų galiojimo patvirtinimo tarnybos platforma laikinai nepasiekiamą, o tai sukelia patikimumo užtikrinimo paslaugų gavėjų programų (pavyzdžiui, pasirašymo ar tikrinimo) neveikimą dėl to, kad negaunama reikalinga informacija.

A.2.3. Klaidingos laiko žymos. Pažeistos laiko žymų tarnybos gali kurti klaidingas elektronines laiko žymas.

A.3. Elektroninis registruotas pristatymas

A.3.1. Nepasiekiamumas².

- Paslauga nepasiekiamą dėl to, kad sutrinka elektroninio registruoto pristatymo platformos veikla.
- Paslauga nepasiekiamą dėl to, kad sutrinka kitos paslaugos tinkamam veikimui užtikrinti būtinos patikimumo užtikrinimo paslaugos, pavyzdžiui, nėra galimybės atlikti elektroninio parašo, spaudo kūrimo ir galiojimo patvirtinimo, nėra galimybės naudotis elektroninėmis laiko žymomis, nėra galimybės patikrinti elektroninio parašo, spaudo sertifikato galiojimo.

A.4. Elektroninių parašų, spaudų kūrimas

A.4.1. Nepasiekiamumas².

- Paslauga nepasiekiamą dėl to, kad sutrinka elektroninių parašų ir (ar) spaudų kūrimo tarnybos platformos veikla.
- Paslauga nepasiekiamą dėl to, kad sutrinka kitos paslaugos tinkamam veikimui užtikrinti būtinos patikimumo užtikrinimo paslaugos, pavyzdžiui, nėra galimybės naudotis elektroninėmis laiko žymomis.

A.4.2. Neteisingas atsakymas. Nors elektroninio parašo, spaudo kūrimo paslaugos platforma ir pasiekia kitas paslaugos teikimui būtinas platformas (pavyzdžiui, laiko žymos), tačiau iš šių platformų gautas atsakymas yra netikslus, o tokiu atveju elektroninis parašas ar spaudas negali būti sukurtas.

A.4.3. Neteisingas parašo, spaudo kūrimas. Dėl pagal standartus neatnaujintų elektroninio parašo, spaudo formatų, sukuriama neteisingo formato elektroniniai parašai, spaudai.

A.4.4. Nėra sinchronizacijos. Patikimumo užtikrinimo paslaugų teikėjas teikia keletą elektroninių parašų, spaudų kūrimo platformų, kurios tarpusavyje nėra tinkamai sinchronizuotos, ir dėl to kyla problemų patikimumo užtikrinimo paslaugų naudotojams.

A.5. Elektroninių parašų, spaudų galiojimo patvirtinimas

A.5.1. Nepasiekiamumas².

- Paslauga nepasiekiamą dėl to, kad sutrinka elektroninių parašų ir (ar) spaudų galiojimo patvirtinimo tarnybos platformos veikla.
- Paslauga nepasiekiamą dėl to, kad sutrinka kitos paslaugos tinkamam veikimui užtikrinti būtinos patikimumo užtikrinimo paslaugos, pavyzdžiui, nėra galimybės naudotis elektroninėmis laiko žymomis ir (ar) patikrinti elektroninio parašo, spaudo sertifikatų galiojimo.

A.5.2. Neteisingas atsakymas. Nors elektroninių parašų, spaudų galiojimo patvirtinimo paslaugos platformos pasiekia sertifikatų galiojimo patvirtinimo tarnybą ir (arba) laiko žymų tarnybą, iš šių tarnybų gautas atsakymas yra netikslus, o tokiu atveju elektroninio parašo, spaudo galiojimas negali būti patvirtintas.

A.5.3. Nepavykęs elektroninių parašų galiojimo patvirtinimas. Nepavyksta tinkamai patvirtinti neteisingai sukurtų (tai yra sukurtų pagal netinkamus arba pagal standartus neatnaujintus elektroninio parašo, spaudo formatus) elektroninių parašų, spaudų.

A.5.4. Nėra sinchronizacijos. Patikimumo užtikrinimo paslaugų teikėjas teikia keletą elektroninių parašų, spaudų galiojimo patvirtinimo platformų, kurios tarpusavyje nėra tinkamai sinchronizuojamos, ir dėl to kyla problemų paslaugų naudotojams.

A.6. Elektroninių parašų, spaudų ilgalaikė apsauga

A.6.1. Nepasiekiamumas².

- Paslauga nepasiekiamą dėl to, kad sutrinka elektroninių parašų ir (ar) spaudų ilgalaikės apsaugos platformos veikla.
- Paslauga nepasiekiamą dėl to, kad sutrinka kitos paslaugos tinkamam veikimui užtikrinti būtinos patikimumo užtikrinimo paslaugos ir nėra galimybės naudotis elektroninėmis laiko žymomis, nėra galimybės patikrinti elektroninio parašo, spaudo sertifikatų galiojimo, nėra galimybės atlikti elektroninio parašo, spaudo galiojimo patvirtinimo.

A.6.2. Prieigos teisės. Asmuo sugeba neteisėtai gauti prieigą prie saugomų duomenų.

A.6.3. Duomenų vientisumas. Išsaugotos informacijos vientisumas gali būti pažeistas dėl įvairių priežasčių (pavyzdžiui, netinkamų aplinkos sąlygų, tikslinio sunaikinimo ar vagystės, kompiuterių virusų, techninės, programinės įrangos ar patikimumo užtikrinimo paslaugų teikėjo klaidų).

A.6.4. Nepavykęs elektroninių parašų galiojimo patvirtinimas. Nepavyksta tinkamai patvirtinti neteisingai sukurtų (tai yra sukurtų pagal netinkamus arba pagal standartus neatnaujintus elektroninio parašo formatus) parašų, spaudų.

A.6.5. Pasenę duomenų formatai. Įrankiai, kurie buvo naudojami pasirašytiems, patvirtintiems duomenims kurti, paseno ir nebėra palaikomi.

B. PAŽEIDIMAI, TURINTYS POVEIKIO KELIOMS PATIKIMUMO UŽTIKRINIMO PASLAUGOMS

Pažeidimai iš šios grupės nurodomi tuomet, kai pažeidimas neatitinka A incidentų grupėje nurodytų pažeidimų.

B.1. Autentifikavimas

B.1.1. Bandymai prisijungti spėjimo būdu. Asmuo, neturintis teisės prisijungti, atlieka pakartotinius prisijungimo bandymus, bandydamas atspėti autentifikavimo duomenis.

B.1.2. Sukčiavimas ar apgaudinėjimas:

- Iš paslaugos gavėjo apgaulės būdu išviliojama jo įtaisų informacija, asmeniniai duomenys ar autentifikavimo duomenys (angl. *phishing*).
- Paslaugos gavėjas nukreipiamas į apgaulingą svetainę, manipuliuojant DNS arba maršrutizavimo lentelėmis (angl. *pharming*).

B.1.3. „Isiterpimas“ (angl. *eavesdropping*). Asmuo neteisėtai įsiterpia į autentifikacijos protokolą, norėdamas perimti informaciją, kuri gali būti panaudota vėlesnėje aktyvioje atakoje apsimitant patikimumo užtikrinimo paslaugos gavėju.

B.1.4. Pakartojimai (angl. *replay attacks*). Asmuo neteisėtai pakartoja anksčiau užfiksuotus tinklo paketus, kurie atpažįstami kaip pateikti patikimumo užtikrinimo paslaugos gavėjo.

B.1.5. Sesijos užgrobimas (angl. *session hijacking*). Asmuo neteisėtai įsiterpia į sėkmingą autentifikaciją tarp abiejų šalių.

B.1.6. Tarpininkas (angl. *man in the middle*). Asmuo neteisėtai perima ir (ar) keičia autentifikavimo protokolo pranešimų žinučių turinį.

B.2. Poveikis programinei įrangai

Šis pažeidimas apima visą įmanomą poveikį programinei įrangai, naudojamai patikimumo užtikrinimo paslaugų teikėjo, ir apima sertifikatų sudarymo, elektroninio parašo, spaudo galiojimo patvirtinimo, elektroninių laiko žymų kūrimo, elektroninio parašo, spaudo kūrimo ir ilgalaikės apsaugos bei elektroninio registruoto pristatymo programinės įrangos galimus pažeidimus.

B.3. „Sukompromituotas“ privatus raktas

Šis pažeidimas apima privataus rakto slaptumo pažeidimą, kuomet juo gali neteisėtai pasinaudoti asmenys, neturintys teisės to daryti. Privataus rakto slaptumas yra ypač svarbus kiekvienai asimetrinei kriptografiniai sistemai. Bet koks privataus rakto atskleidimas stipriai paveikia patikimumo užtikrinimo paslaugų gavėjus ir paslaugas, kurie priklauso nuo šio rakto. Prarastas raktas gali būti atkuriamas priklausomai nuo patikimumo užtikrinimo paslaugų teikėjo taikomų procedūrų, bet pavogtas raktas gali turėti kritinį poveikį teikiamoms patikimumo užtikrinimo paslaugoms.

B.4. Netinkamas algoritmų naudojimas

Netinkamais laikomi nebeaktualūs, silpni arba pasenę algoritmai. Netinkamai parinkti algoritmai daro įtaką kriptografinių raktų generavimui, sertifikatų sudarymui, elektroninio parašo, spaudo kūrimui ir kitoms patikimumo užtikrinimo paslaugoms.

B.5. Netyčinis sertifikatų naudojimas kitiems tikslams

Sertifikatas panaudojamas ne pagal paskirtį, kuri nurodyta pačiame sertifikate ir sutartyje su patikimumo užtikrinimo paslaugos gavėju (pavyzdžiui, elektroninio spaudo sertifikatas negali būti panaudotas kaip elektroninio parašo sertifikatas).

B.6. Pažeidimas įtaisuose su kriptografiniais raktais

Pažeidimas įtaisuose, turinčiuose kriptografinius raktus, pavyzdžiui, HSM (aparatinuose saugumo moduluose), lustinėse kortelėse, USB kriptografiniuose raktuose. Tai reiškia, kad įtaisas yra prarastas, pavogtas, užblokuotas, nėra galimybės naudoti, susigrąžinti ar atšaukti kriptografinius duomenis įtaise.

B.7. Archyvavimo problemos

Pažeidimai, susiję su patikimumo užtikrinimo paslaugų teikėjo dokumentacija ir visų patikimumo užtikrinimo paslaugų teikėjo atliktų veiksmų įrašais, pavyzdžiui:

- įrašų, susijusių su sertifikatų gyvavimo ciklu, pakeitimais;
- sustabdytas įrašų apie prašymus atšaukti, sustabdyti sertifikatų galiojimą registravimas;
- sustabdytas saugumo įvykių, tokių kaip sistemos paleidimas, išjungimas, sistemos gedimai, aparatinės įrangos gedimai, keli prisijungimo bandymai ir panašiai, registravimas.

B.8. Tinklo įrangos sutrikimai

Tinklo infrastruktūros, įskaitant techninę įrangą (pavyzdžiui, ugniasienės, maršrutizatoriai, kabeliai), taip pat programinę įrangą (pavyzdžiui, aparatinės įrangos tvarkykles (angl. *firmware*)), neveikimas.

III SKYRIUS POVEIKIO MASTO ĮVERTINIMAS

Paslaugos, kurioms pažeidimas gali turėti poveikio	Turtas			Poveikis		
				Prieinamumas	Vientisumas	Konfidencialumas
Elektroninio parašo, elektroninio spaudo ir interneto svetainių tapatumo nustatymo sertifikatų sudarymas	Sertifikavimo tarnybos (angl. <i>certification authority</i>) platforma	Techninė įranga	Šakninės sertifikavimo tarnybos (angl. <i>root certification authority</i>) tarnybinė stotis	Didelis	Netaikoma	Netaikoma
			Šakninės sertifikavimo tarnybos aparatinis saugumo modulis (HSM)	Didelis	Netaikoma	Netaikoma
			Sertifikavimo tarnybos tarnybinė stotis	Didelis	Netaikoma	Netaikoma
			Sertifikavimo tarnybos aparatinis saugumo modulis	Didelis	Netaikoma	Netaikoma
			Kita sertifikavimo tarnybos techninė įranga	Didelis	Netaikoma	Netaikoma
		Programinė įranga	Šakninės sertifikavimo tarnybos sertifikatas	Vidutinis	Didelis	Mažas
			Aparatinio saugumo modulio, saugančio šakninės sertifikavimo tarnybos privatų raktą, programinė įranga	Didelis	Didelis	Didelis
			Sertifikavimo tarnybos sertifikatas	Vidutinis	Didelis	Mažas
			Aparatinio saugumo	Didelis	Didelis	Didelis

			modulio, saugančio sertifikavimo tarnybos privatų raktą, programinę įrangą			
			Šakninės sertifikavimo tarnybos ir sertifikavimo tarnybos programinę įrangą	Vidutinis	Didelis	Vidutinis
	Registravimo tarnybos (angl. <i>registration authority</i>) platforma	Techninė įranga	Registravimo tarnybos techninė įranga	Didelis	Netaikoma	Netaikoma
			Registravimo tarnybos darbuotojų naudojama techninė įranga	Vidutinis	Netaikoma	Netaikoma
		Programinė įranga	Registravimo tarnybos programinė įranga	Vidutinis	Didelis	Vidutinis
			Registravimo tarnybos operatoriaus sertifikatas	Vidutinis	Didelis	Mažas
Elektroninio parašo, elektroninio spaudo ir interneto svetainių tapatumo nustatymo sertifikatų sudarymas Elektroninis registruotas pristatymas Elektroninių parašų ir elektroninių spaudų galiojimo patvirtinimas Elektroninių parašų ir elektroninių spaudų ir ilgalaikė apsauga	Sertifikatų galiojimo patvirtinimo tarnybos (angl. <i>validation authority</i>) platforma	Techninė įranga	Galiojimo patvirtinimo tarnybos tarnybinė stotis	Didelis	Netaikoma	Netaikoma
			Galiojimo patvirtinimo tarnybos aparatinis saugumo modulis	Didelis	Netaikoma	Netaikoma
		Programinė įranga	Galiojimo patvirtinimo tarnybos programinė įranga	Vidutinis	Didelis	Vidutinis
			Galiojimo patvirtinimo tarnybos sertifikatas	Vidutinis	Didelis	Mažas
			Aparatinio saugumo modulio, saugančio galiojimo patvirtinimo tarnybos privatų raktą, programinę	Didelis	Didelis	Didelis

			įranga			
			Atšauktų sertifikavimo tarnybos sertifikatų sąrašas (angl. <i>certification authority revocation list</i>)	Didelis	Didelis	Mažas
			Atšauktų sertifikatų sąrašas (angl. <i>certification revocation list</i>)	Didelis	Didelis	Mažas
Elektroninių laiko žymų kūrimas Elektroninis registruotas pristatymas Elektroninių parašų ir elektroninių spaudų kūrimas Elektroninių parašų ir elektroninių spaudų galiojimo patvirtinimas Elektroninių parašų ir elektroninių spaudų ir ilgalaikė apsauga	Laiko žymų tarnybos (angl. <i>time stamping authority</i>) platforma	Techninė įranga	Laiko žymų tarnybos tarnybinė stotis	Didelis	Netaikoma	Netaikoma
			Laiko žymų tarnybos aparatinis saugumo modulis	Didelis	Netaikoma	Netaikoma
		Programinė įranga	Laiko žymų tarnybos programinė įranga	Vidutinis	Didelis	Vidutinis
			Laiko žymų tarnybos sertifikatas	Vidutinis	Didelis	Mažas
			Aparatinio saugumo modulio, saugančio laiko žymos tarnybos privatų raktą, programinė įranga	Didelis	Didelis	Didelis
Elektroninio parašo, elektroninio spaudo ir interneto svetainių tapatumo nustatymo sertifikatų sudarymas Elektroninių laiko žymų kūrimas Elektroninis registruotas pristatymas	Archyvas		Dokumentacija	Vidutinis	Didelis	Didelis
	Tinklo platforma		Ryšio linijos, ugniasienės ir kita	Didelis	Didelis	Didelis

Elektroninių parašų ir elektroninių spaudų kūrimas						
Elektroninių parašų ir elektroninių spaudų ilgalaikė apsauga						
Elektroninių parašų ir elektroninių spaudų galiojimo patvirtinimas						
Elektroninio parašo, elektroninio spaudo ir interneto svetainių tapatumo nustatymo sertifikatų sudarymas	Paslaugų naudotojų įtaisai		Lustinės kortelės, USB laikmenos, mobilieji telefonai	Didelis	Netaikoma	Netaikoma
			Paslaugų naudotojo sertifikatai	Vidutinis	Didelis	Vidutinis
			Paslaugų naudotojo privatus raktas	Didelis	Didelis	Didelis
Elektroninių parašų ir elektroninių spaudų kūrimas	Paslaugų naudotojų nuotoliniai įtaisai		Aparatinis saugumo modelis arba tarnybinė stotis, sauganti privačius raktus ir sertifikatus	Didelis	Didelis	Didelis
Elektroninių parašų ir elektroninių spaudų galiojimo patvirtinimas						
Elektroninių parašų ir elektroninių spaudų kūrimas	Elektroninių parašų ir (ar) elektroninių spaudų kūrimo platforma		Pasirašymo programinė įranga	Vidutinis	Didelis	Vidutinis
			Pasirašymo priemonės sertifikatas	Vidutinis	Didelis	Netaikoma
	Paslaugų naudotojų įtaisai lokaliai pasirašymui		Lustinių kortelių skaitytuvai, USB jungtys ir kita	Vidutinis	Didelis	Didelis
	Įkelti dokumentai		Dokumentai, pasirašyti nuotoliniu būdu	Vidutinis	Didelis	Didelis
Elektroninių	Elektroninių		Ilgalaikės	Vidutinis	Didelis	Vidutinis

parašų ir elektroninių spaudų ilgalaikė apsauga	parašų ir (ar) elektroninių spaudų ilgalaikės apsaugos platforma		apsaugos programinė įranga			
			Ilgalaikės apsaugos priemonės sertifikatas	Vidutinis	Didelis	Netaikoma
	Įkelti dokumentai		Dokumentai, saugomi nuotoliniu būdu	Vidutinis	Didelis	Vidutinis
Elektroninis registruotas pristatymas	Elektroninio registruoto pristatymo platforma		Elektroninio registruoto pristatymo programinė įranga	Vidutinis	Didelis	Vidutinis
