

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ
N U T A R I M A S

**DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2002 M. GRUODŽIO 31 D.
NUTARIMO NR. 2108 „DĖL REIKALAVIMŲ KVALIFIKUOTUS SERTIFIKATUS
SUDARANTIEMS SERTIFIKAVIMO PASLAUGŲ TEIKĖJAMS, REIKALAVIMŲ
ELEKTRONINIO PARAŠO ĮRANGAI, KVALIFIKUOTUS SERTIFIKATUS
SUDARANČIŲ SERTIFIKAVIMO PASLAUGŲ TEIKĖJŲ REGISTRAVIMO
TVARKOS IR ELEKTRONINIO PARAŠO PRIEŽIŪROS REGLAMENTO
PATVIRTINIMO“ PAKEITIMO**

2013 m. sausio 29 d. Nr. 72
Vilnius

Lietuvos Respublikos Vyriausybė n u t a r i a :

1. Pakeisti Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimą Nr. 2108 „Dėl Reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, Reikalavimų elektroninio parašo įrangai, Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir Elektroninio parašo priežiūros reglamento patvirtinimo“ (Žin., 2003, Nr. [2-47](#); 2011, Nr. [8-315](#)):

1.1. Nurodytu nutarimu patvirtintuose Reikalavimuose kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams:

1.1.1. Išdėstyti 1 punktą taip:

„1. Reikalavimai kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams (toliau vadinama – Reikalavimai) nustato kvalifikuotus sertifikatus (toliau vadinama – sertifikatai) sudarančių sertifikavimo paslaugų teikėjų (toliau vadinama – paslaugų teikėjai) veiklos, susijusios su sertifikatų sudarymu ir tvarkymu, sąlygas.“

1.1.2. Papildyti 3¹ punktu:

„3¹. Jeigu paslaugų teikėjas yra įsidiegęs informacijos saugumo valdymo sistemą, taikydamas Lietuvos standartą LST ISO/IEC 27001:2006 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001:2005)“ (toliau – LST ISO/IEC 27001:2006) ar jį pakeičiantį standartą, laikoma, kad paslaugų teikėjas yra įvykdęs Reikalavimų IV skyriaus nuostatas.“

1.1.3. Papildyti nauju IV skyriumi (ankstesnįjį IV skyrių laikyti V skyriumi, o ankstesnius 16 ir 17 punktus laikyti 24 ir 25 punktais):

„IV. INFORMACIJOS SAUGOS REIKALAVIMAI

16. Paslaugų teikėjas yra atsakingas už renkamų ir tvarkomų duomenų ir informacijos (toliau kartu vadinama – informacija) saugumo užtikrinimą. Užtikrinant informacijos saugumą, rekomenduojama vadovautis Lietuvos standartais LST ISO/IEC 27001:2006, LST ISO/IEC 27002:2009 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)“ (toliau – LST ISO/IEC 27002:2009), LST ISO/IEC 27005:2011 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo rizikos valdymas (tapatus ISO/IEC 27005:2011)“, taip pat kitais Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais.

17. Paslaugų teikėjas privalo pasitvirtinti dokumentą, nustatantį pagrindinius taikomus informacijos saugumo užtikrinimo ir valdymo principus ir taisykles, kuriais remiantis vykdomi paslaugų teikėjo veiklos procesai, procedūros ir rengiami juos reglamentuojantys dokumentai (toliau vadinama – informacijos saugumo politikos dokumentas). Informacijos saugumo politikos dokumente turi būti nurodyta:

17.1. informacijos saugumo užtikrinimo tikslai, svarba ir esama būklė;

17.2. informacijos saugumo užtikrinimo prioritetinės kryptys;

17.3. informacijos saugumo užtikrinimo reikalavimai, kurie apima:

17.3.1. paslaugų teikėjo tvarkomą informaciją ir (ar) jos kategorijas, pagrindinius tvarkomos informacijos ir (ar) tam tikrų jos kategorijų saugumo užtikrinimo reikalavimus, kuriais vadovaujantis parenkamos tinkamos informacijos saugumo užtikrinimo priemonės (įskaitant teisės aktų ir kitų dokumentų, kuriais vadovaujamasi tvarkant informaciją ir užtikrinant jos saugumą, reikalavimus, bet jais neapsiribojant);

17.3.2. paslaugų teikėjo darbuotojų, sudarančių ir tvarkančių sertifikatus, kvalifikacinius reikalavimus;

17.3.3. pagrindines nuostatas dėl informacijos saugumo rizikos (toliau vadinama – rizika) veiksnų vertinimo, pagrindinių rizikos vertinimo kriterijų apibūdinimą;

17.4. asmenų supažindinimo su informacijos saugumo užtikrinimo reikalavimais tvarka;

17.5. atsakomybė už informacijos saugumo užtikrinimo reikalavimų pažeidimus;

17.6. kiti reikalavimai.

18. Paslaugų teikėjas turi kasmet atlikti rizikos vertinimą. Prireikus paslaugų teikėjas gali organizuoti ir neeilinį rizikos vertinimą. Rizikos vertinimo rezultatai pateikiami rizikos vertinimo ataskaitoje. Rizikos vertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnus, galinčius turėti įtakos informacijos saugumui.

19. Atsižvelgdamas į rizikos vertinimo ataskaitą, paslaugų teikėjas prireikus tvirtina rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti. Rizikos valdymo priemonės, atsižvelgiant į informacijos saugumo valdymo tikslus, rekomenduojama rinktis iš Lietuvos standarto LST ISO/IEC 27002:2009.

20. Paslaugų teikėjas turi kasmet atlikti informacijos saugumo užtikrinimo atitikties vertinimą – nustatyti, ar faktinė informacijos saugumo užtikrinimo būklė atitinka saugumo užtikrinimo reikalavimus, ir pasitvirtinti vertinant informacijos saugumo užtikrinimo atitiktį nustatytą informacijos saugumo užtikrinimo trūkumų šalinimo planą.

21. Atliekant informacijos saugumo užtikrinimo atitikties vertinimą, rekomenduojama:

21.1. įvertinti informacijos saugumo užtikrinimo dokumentų ir esamos informacijos saugumo užtikrinimo būklės atitiktį;

21.2. inventorizuoti techninę ir programinę įrangą;

21.3. patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų kompiuterinių darbo vietų, jose įdiegtas programas ir jų sąranką;

21.4. patikrinti (įvertinti) darbuotojams suteiktų teisių ir atliekamų funkcijų atitiktį;

21.5. įvertinti pasirengimą užtikrinti veiklos tęstinumą įvykus informacijos saugumo incidentui.

22. Informacijos saugumo politikos dokumentas turi būti peržiūrimas ne rečiau kaip kartą per metus po rizikos ar informacijos saugumo užtikrinimo atitikties įvertinimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems paslaugų teikėjo veiklos pokyčiams.

23. Šiame skyriuje nustatyti reikalavimai nekeičia Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. [83-2075](#); 2007, Nr. 49-1891).“

1.2. Nurodytu nutarimu patvirtintuose Reikalavimuose elektroninio parašo įrangai:

1.2.1. Išdėstyti 12 punktą taip:

„12. Jeigu įvykdyti Lietuvos standartų LST CWA 14169 „Saugūs parašo kūrimo įtaisai EAL 4+“ ir LST CWA 14170 „Saugumo reikalavimai, keliami taikomosioms parašo formavimo sistemoms“ reikalavimai, laikoma, kad parašo formavimo įranga atitinka šio skyriaus nuostatas.“

1.2.2. Išdėstyti 14 punktą taip:

„14. Jeigu įvykdyti Lietuvos standarto LST CWA 14171 „Bendrosios elektroninio parašo tikrinimo gairės“ reikalavimai, laikoma, kad parašo tikrinimo įranga atitinka šio skyriaus nuostatas.“

1.3. Papildyti nurodytu nutarimu patvirtintą Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos aprašą 5.8 punktu:

„5.8. paslaugų teikėjo pasitvirtinto informacijos saugumo politikos dokumento arba akredituotos sertifikavimo įstaigos išduoto sertifikato, patvirtinančio, kad paslaugų teikėjas yra įsidiegęs informacijos saugumo valdymo sistemą, taikydamas Lietuvos standartą LST ISO/IEC 27001:2006 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001:2005)“, patvirtintą kopiją.“

2. Nustatyti, kad kvalifikuotus sertifikatus sudarantys sertifikavimo paslaugų teikėjai, iki šio nutarimo įsigaliojimo teisės aktų nustatyta tvarka užsiregistravę elektroninio parašo priežiūros institucijoje, šio nutarimo 1.3 punkte nurodytų dokumentų kopijas Lietuvos Respublikos ryšių reguliavimo tarnybai pateikia per 2 mėnesius nuo šio nutarimo įsigaliojimo.

3. Šis nutarimas įsigalioja 2013 m. gegužės 1 dieną.

MINISTRAS PIRMININKAS

ALGIRDAS BUTKEVIČIUS

SUSISIEKIMO MINISTRAS

RIMANTAS SINKEVIČIUS