Laiko žymos - reglamentavimas, naujovės, tendencijos, problematika

Dr. Antanas Mitašiūnas

Vilniaus universitetas,

UAB „MIT-SOFT“

2018 m. vasario 20 d.

Pranešimo planas

- Kas tai yra laiko žymos
- Laiko žymų naudojimas
- Laiko žymų reglamentavimas
- Centralizuotas laiko žymų paslaugų pirkimas
- Svarbiausios problemos

Kas yra elektroninė laiko žyma?

- Įrodymas, kad elektroniniai duomenys **egzistavo iki** laiko žymoje nurodyto laiko
- eIDAS:
  - Elektroninė laiko žyma – elektroninės formos duomenys, kuriais kiti elektroninės formos duomenys susiejami su tam tikru laiku ir taip sukuriamas įrodymas, kad pastarieji egzistavo tuo metu

Kas yra kvalifikuota elektroninė laiko žyma?

- Susieja datą ir laiką su duomenimis taip, kad pagrįstai neliktų galimybės **nepastebimai pakeisti** duomenų
- Grindžiama tiksliu laiko šaltiniu, **susietu** su suderintuoju pasauliniu laiku
- Pasirašyta **kvalifikuoto** patikimumo užtikrinimo paslaugų teikėjo pažangiuoju elektroniniu parašu arba patvirtinta jo pažangiuoju elektroniniu spaudu

Laiko žymos gavimas

Prašymas		Laiko žyma
Santrauka Algoritmo ID *Pastaba: santrauka yra trumpa (pvz. 32 simbolių ilgio) vienareikšmė duomenų reprezentacija*	HTTP/ HTTPS → ←	Pasirašyta: Santrauka Algoritmo ID TSA taisyklių ID Laiko žymos Nr. Tikslus laikas Skaitm. Parašas: Laiko žymos santrauka Santraukos algoritmo ID Parašo algoritmo ID [TSU sertifikatas]

Reikalavimai algoritmams

- Duomenų santraukos algoritmai laiko žymoms sudaryti:
  - SHA 1 – negalimas
  - SHA 256 privalomas
  - SHA 512 alternatyvus
- Skelbiama algoritmų galiojimo trukmė:
  - SHA 1 – negalimas
  - Silpniau nei SHA 256 – 3 metai +
  - SHA 256 arba stipriau – 6 metai +

Laiko žymų naudojimas

- Įrodymui, kad nepakitę duomenys egzistavo jau prieš nurodytą laiką, pvz., duomenų bazių įrašai
- Skaitmeninio parašo sertifikato, kuriuo patvirtinamas parašas, **galiojimo patvirtinimo metu įrodymui**, tai yra skaitmeninio parašo ir elektroninio dokumento galiojimo įrodymui
- *Pastaba: skaitmeninis parašas – tai elektroninis parašas arba elektroninis spaudas*

Skaitmeninio parašo sertifikato galiojimas

- Skaitmeninio parašo sertifikatas galioja parašo patvirtinimo metu, jeigu yra patenkintos viso šios sąlygos:
  - Parašo patvirtinimas atliktas sertifikate nurodytu sertifikato galiojimo laikotarpiu
  - Parašo patvirtinimo metu sertifikatas nebuvo atšauktas
  - Parašo patvirtinimo metu sertifikatas nebuvo sustabdytas
  - *Pastaba: Jei sustabdytas sertifikatas buvo aktyvuotas, tai buvęs sustabdymo laikotarpis įtakos galiojimui neturi*

Skaitmeninio parašo sertifikato galiojimo įrodomumas

- Skaitmeninio parašo sertifikato galiojimo parašo patvirtinimo metu įrodomumo būdai pagal sertifikato galiojimo etapus:
  - Sertifikato faktinio galiojimo dinaminis etapas
  - Sertifikato deklaruoto galiojimo statinis etapas
  - Sertifikato galiojimo įrodymas nepriklausomai nuo jo galiojimo etapų

Laiko žymų įtaka skaitmeninio parašo galiojimo įrodomumui (1)

- Bazinio formato (B, EPES) be laiko žymos parašo galiojimą galima patikrinti tol, kol galioja jį patvirtinęs sertifikatas
- Trumpo galiojimo formato (T) su viena laiko žyma parašo galiojimo patikrinimas galimas viso sertifikate nurodyto sertifikato galiojimo laikotarpio metu.
- Ilgo galiojimo formato (X-L, A) parašo galiojimą su 2 laiko žymomis apsprendžia antrosios laiko žymos galiojimo trukmė

Laiko žymų įtaka skaitmeninio parašo galiojimo įrodomumui (2)

- Laiko žymos galiojimo priklausomybė nuo TSL
- Tikslinė laiko žymos sertifikato galiojimo trukmė:
  - TSL įtaka leidžia trumpinti
  - Rizika verčia trumpinti
  - Mažiau nei 5 metai
- Ar dėti naują laiko žymą baigiantis esamos laiko žymos sertifikato galiojimui?
  - Taip, kad nepriklausyti nuo aplinkybių
  - Rizikos prarasti patikimumą

Nuo el. parašų direktyvos prie eIDAS reglamento

- Laiko žymos - nuo ETSI TS 102 023 prie TSL:
  - ETSI TS 102 023 → ETSI EN 319 421, ETSI EN 319 421
  - ETSI TS 101 861 → ETSI EN 319 422
  - Deklaravimas → Sertifikavimas (20.000 € kas 2 metai)
- Pagal sertifikavimo ataskaitą – Kvalifikuotų laiko žymų kvalifikuota patikimumo užtikrinimo paslauga
- Kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas - kvalifikuotą patikimumo užtikrinimo paslaugą teikiantis paslaugų teikėjas, kuriam priežiūros įstaiga yra suteikusi kvalifikacijos statusą
- Kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas į TSL

Laiko žymų teisiniai aspektai (1)

- Kvalifikuota elektroninė laiko žyma, išduota vienoje valstybėje narėje, pripažįstama kaip kvalifikuota elektroninė laiko žyma visose valstybėse narėse
- Kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas turi pareigą įrodyti, kad nesielgė netinkamai
- Jei patikimumo užtikrinimo paslauga nėra kvalifikuota, pareiga įrodyti, kad nesielgė netinkamai, tenka naudotojui

Laiko žymų teisiniai aspektai (2)

- Oficialus elektroninis dokumentas - Lietuvos vyriausiojo archyvaro nustatyta tvarka valstybės ar savivaldybės institucijos, įstaigos ar įmonės, valstybės įgalioto asmens informacinių technologijų priemonėmis sudarytas, patvirtintas ar gautas elektroninis dokumentas, pasirašytas elektroniniu parašu ir įtrauktas į apskaitą. (LR dokumentų ir archyvų įstatymas)
- (Oficialių elektroninių dokumentų) kvalifikuotų elektroninių parašų ar kvalifikuotų elektroninių spaudų galiojimo įrodymams išsaugoti gali būti naudojamos tik kvalifikuotos elektroninės laiko žymos. (Elektroninių dokumentų valdymo taisyklės, 18 p.)

Laiko žymų teisiniai aspektai (3)

- Elektroninių dokumentų valdymo taisyklių reikalavimai elektroniniams dokumentams rengti taikomi tiek, kiek jie neprieštarauja Specifikacijose nustatytiems reikalavimams ar kitiems teisės aktams. (Elektroninių dokumentų valdymo taisyklės, 12 p.)
- Elektroniniame paraše esančios laiko žymos yra kvalifikuotos ar išduotos patikimumo užtikrinimo paslaugų teikėjų, kuriais elektroninio parašo tikrintojas pasitiki. (Elektroninių dokumentų specifikacija ADOC-V1.0, 74.3 p.)
- Tačiau pagrindo nenaudoti kvalifikuotų laiko žymų nėra

Kvalifikuoti laiko žymų paslaugų teikėjai

- Kvalifikuoti laiko žymų paslaugų teikėjai gali pradėti teikti kvalifikuotų laiko žymų kvalifikuotas paslaugas tik po to, kai jų **kvalifikuotumo statusas yra paskelbtas TSL**
- Artimiausi kvalifikuoti laiko žymų paslaugų teikėjai paskelbti TSL:
  - BalTstamp, Lietuva
  - Registrų centras, Lietuva
  - SK ID Solutions, Estija
  - Asseco (Certum), Lenkija

Laiko žymų naudojimas Lietuvoje

- Intensyvumas – nuo 100 iki 2 mln. per mėnesį
- Vieneto kaina - nuo 0,07 € iki 0,0012 € priklausomai nuo intensyvumo
- Kaina už paslaugas per mėn. – nuo 7 € iki 2500 €
- Pagrindiniai laiko žymų naudotojai:
  - SoDra
  - VRM IRD
  - Lietuvos paštas

Laiko žymų rinkos charakteristika

- Laiko žymų paslaugų kaina arti savikainos
- Laiko žymų kainų mažinimo išorinės priemonės nėra prasmingos
- Įstaigų lūkesčiai – nemokamos laiko žymos
- Poreikiai:
  - 85 proc. - vienai įstaigai
  - 15 proc. – visoms likusioms kartu paėmus
  - Galima analogija – perkamas traukinio sąstatas kuro, kurio 15 proc. perkama degalinėse
  - Iš esmės skirtingo intensyvumo laiko žymų paslaugos yra skirtingi objektai su iš esmės besiskiriančia (40-50 kartų) vieneto kaina

Centralizuotas laiko žymų pirkimas (1)

- Pirkimo tikslas:
  - Užtikrinti, kad būtų racionaliai naudojamos viešojo sektoriaus biudžeto lėšos
  - Užtikrinti paslaugų teikėjų konkurencingumą
  - Užtikrinti korupcijos prevenciją
- Pirkimo paskirtis - atrinkti tiekėjus ir jų siūlomas kainas, kurios negali būti viršytos aukcione dėl laiko žymų paslaugų teikimo konkrečiam paslaugų gavėjui.
- Atrankos kriterijus – jeigu dalyvių daugiau kaip 3, tai vienas, pasiūlęs didžiausią kainą, pašalinamas

Centralizuotas laiko žymų pirkimas (2)

- Tikėtini rezultatai:
  - Dėl centralizuoto pirkimo atrankos taisyklių (teikėjo pašalinimas, aukciono kainos ribojimas atrankos kaina, kainų nepalyginamumas) bus iš esmės apribota laiko žymų paslaugų teikėjų konkurencija
  - 95 proc. įstaigų aukcione įsigys laiko žymų paslaugas iš vienintelio teikėjo
  - Įstaigoms laiko žymų kainos išaugs kelis kartus lyginant su dabartinėmis
- Išvada: tikėtina, kad centralizuoto laiko žymų paslaugų pirkimo įgyvendinimu pirkimo tikslai ne tik, kad nebus pasiekti, o turės priešingą poveikį.

Svarbiausios problemos

- Problema Nr.1 – yra saugoma daugybė elektroninių dokumentų, kurių parašų galiojimo patikrinimas nebegalimas programinės įrangos priemonėmis dėl galiojimo įrodymų neišsaugojimo
- Problema Nr.2 – įstaigose nėra priemonių sukurti, priimti ir patikrinti tarpvalstybinius elektroninius dokumentus, parengtus pagal eIDAS reikalavimus
- Problema Nr.3 – skatinama anti-inovacija rengti teisinę galią turinčius dokumentus popieriuje

Klausimai

?

Antanas Mitašiūnas

antanas.mitasiunas@mitsoft.lt

+370-611-52966