# Kvalifikuotų elektroninių parašų ir spaudų kvalifikuotos ilgalaikės apsaugos paslaugos

**UAB MIT-SOFT**

**info@mitsoft.lt**

**2024**

# El. dokumentų naudojimo problemos

- Klaidos pasirašymo metu
  - Kriptografinės el. parašų klaidos
  - Pasirašymo įrenginių palaikymas (tvarkyklės)
- El. dokumentų interoperabilumo trūkumas
  - Nepalaikoma el. dokumentų specifikacija
  - Neatitinka el. dokumentų specifikacijos reikalavimų
- El. parašų interoperabilumo trūkumas
  - Nepatikimas, nekvalifikuotas sertifikatas
  - Neatitinka el. parašų standartų reikalavimų
- El. paraše trūksta galiojimą patvirtinančių duomenų arba jie yra netinkami

# Priežastys

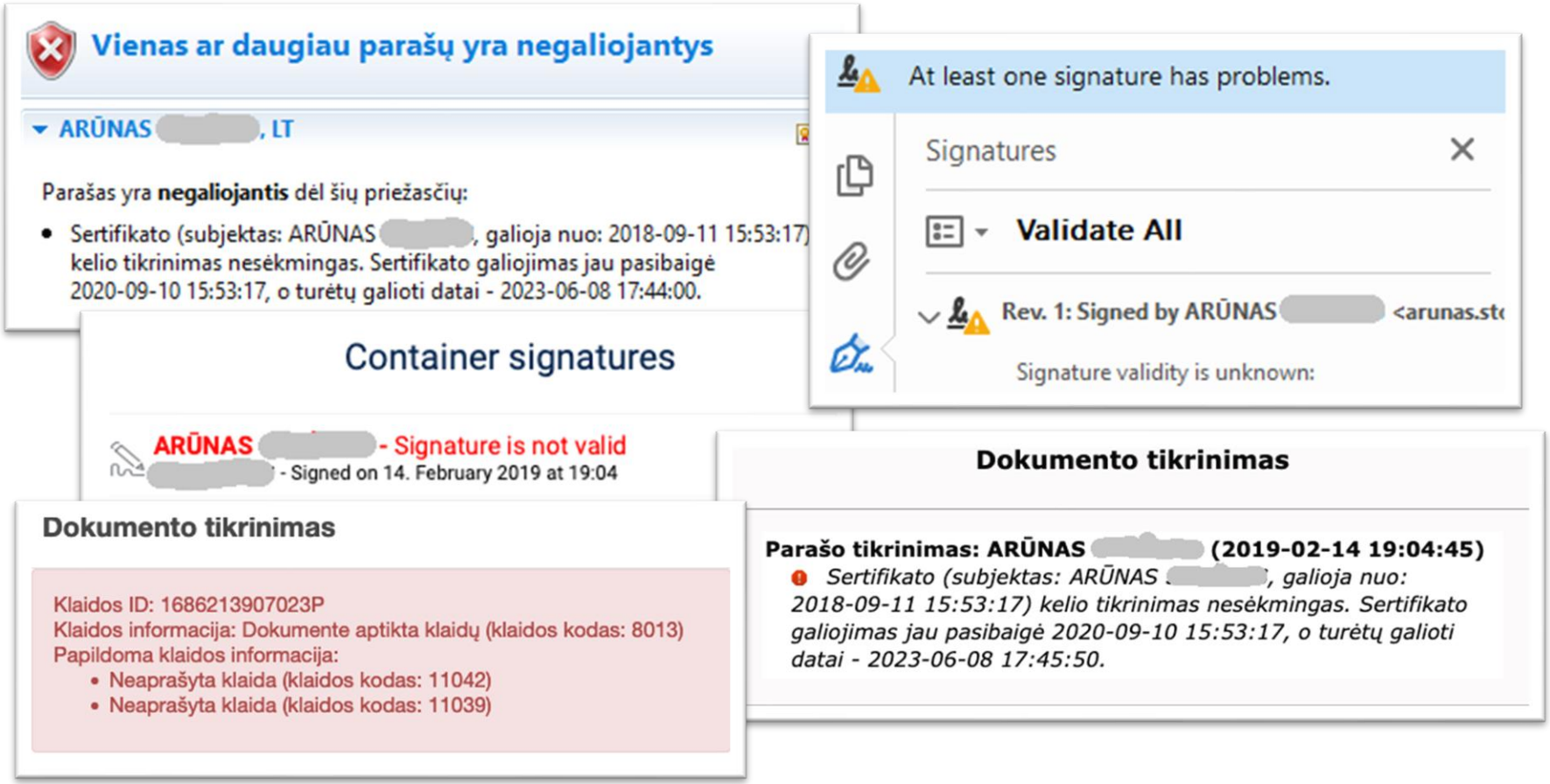
- Remiamasi ne standartais, o produktais
- Netikslių ar neaiškių standartų nuostatų taikymas praktikoje ir jų interpretavimas sau palankiu būdu
- Specifinių reikalavimų taikymas tikrinime
- Netinkama elektroninių dokumentų ilgalaikė apsauga
  - Pradelsta su el. parašo augmentavimu
  - Netinkamai atliktas augmentavimas
- Problemos nematymas ar ignoravimas

# Galiojimo užtikrinimas laike

- Kvalifikuoto elektroninio parašo ar spaudo galiojimo trukmė yra ribota
  - Sertifikatai (asmens, OCSP, laiko žymų) nustoja galioti, nusilpsta kriptografiniai algoritmai
  - Tai nepriklauso nuo dokumentų ir parašų formato
  - Nėra galimybės vienkartiniu veiksmu užtikrinti ilgalaikį elektroninio parašo, spaudo galiojimą
- Neprižiūrint elektroninių dokumentų ir pradelsus, galiojimo atstatyti nebegalima
- Rezultatas: programinės priemonės nebepatvirtina parašų galiojimo ir dokumentų teisinės galios

# Kaip nutinka?

Programinės priemonės nepatvirtina parašų galiojimo



# Saugojimo trukmė

- Vienkartinis elektroninio parašo formato užkėlimas:
  - Prailgina galiojimą 1-2 metais (priklauso nuo aplinkybių)
  - Geriausiu atveju iki 5 metų
- El. dokumentų saugojimo laikas:
  - Trumpo saugojimo – iki 10 metų
  - Ilgo saugojimo – iki 100 metų
  - Nuolat saugomi
- Dokumentų ir archyvų įstatymo 12 str. reikalauja:
  - „užtikrinti, kad turimi elektroniniai ir kiti dokumentai [...] išliktų autentiški, patikimi ir prieinami visą jų saugojimo laiką“

# Lietuvoje

- Daugeliui parašų formatas užkeliamas
  - Tik vieną kartą (pvz., ADOC iki XAdES-X-L) ir...
  - Dokumentas užmirštamas saugykloje (be el. parašų galiojimo priežiūros) iki pareikalavimo
- Saugomų dokumentų viešajame sektoriuje pagal DBSIS projekto 2020 m. duomenis:
  - Iki 10 metų – 35,5 mln.
  - Iki 25 metų – 1,5 mln.
  - Iki 100 metų – 0,94 mln.
- Kiek iš jų jau pradelsti?
- *Mitas: el. parašų apsauga – tik laiko žymų dėjimas*

# Europoje

ETSI Augmentavimo PlugTestai:

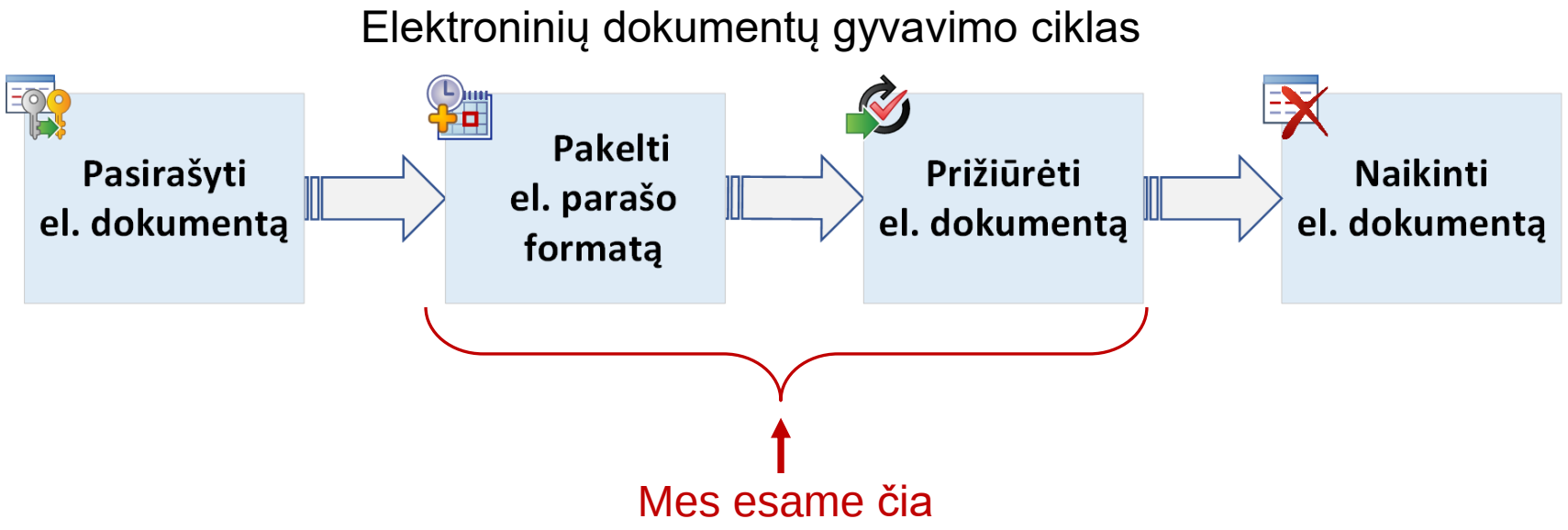
- Tikslas: patikrinti parašų augmentavimo iki LTA lygmens interoperabilumą
  - Testuota: ASiC, XAdES, PAdES, CAdES, JAdES
- Dalyvavo 122 organizacijos iš 38 šalių
  - Augmentuota el. parašų: > 2 000
  - Patikrinta el. parašų: > 35 000
  - Identifikuota aibė probleminių interoperabilumo aspektų. Prie šio darbo ženkliai prisidėjo MIT-SOFT
- *Mitas: augmentavimas iki LTA yra nesudėtingas*
  - „Probleminių“ LTA lygmens el. parašų kiekis (neoficiali statistika): 50-60%

# Ką daryti dokumentų šeimininkams?

- Naudoti įrangą ar paslaugas, kurias teikia patikimi (kvalifikuoti) paslaugų tiekėjai galintys užtikrinti:
  - Atitikimą standartų reikalavimams
  - Savalaikį ir tinkamą el. parašų ir spaudų galiojimo užtikrinimo veiksmų atlikimą (augmentavimą)
  - Stebėseną ir reakciją į besikeičiančią PKI:
    - patikimi sąrašai, sertifikavimo centrai, laiko žymų tarnybos
    - standartų reikalavimai,
    - kriptografinių algoritmų patikimumas

# Ką siūlo MIT-SOFT?

- **Kvalifikuotų el. parašų ir kvalifikuotų el. spaudų kvalifikuotas ilgalaikės apsaugos paslaugas**
- Įtrauktos į Lietuvos nacionalinį patikimą sąrašą (2023-05-11 d. RRT tarybos nutarimas)

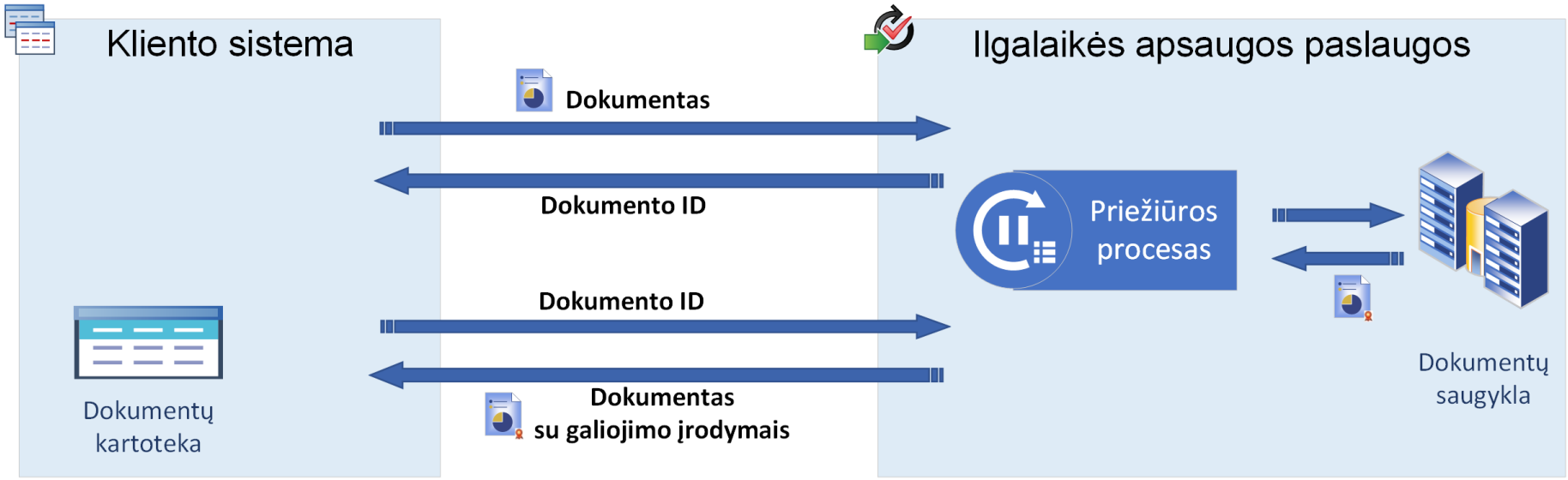


# Kam skirtos paslaugos?

- Dokumentų valdymo sistemų ir kitų informacinių sistemų valdytojams
  - Kuria arba gauna elektroninius dokumentus
  - Kaupia elektroninius dokumentus
- Išsprendžia elektroninių dokumentų teisinės galios užtikrinimo rūpesčius
  - Užkelti parašų formatus
  - Vykdyti savalaikį parašų galiojimo pratęsimą
  - Stebėti PKI pasikeitimus: standartai, kriptografiniai algoritmai, patikimi sąrašai (TSL)

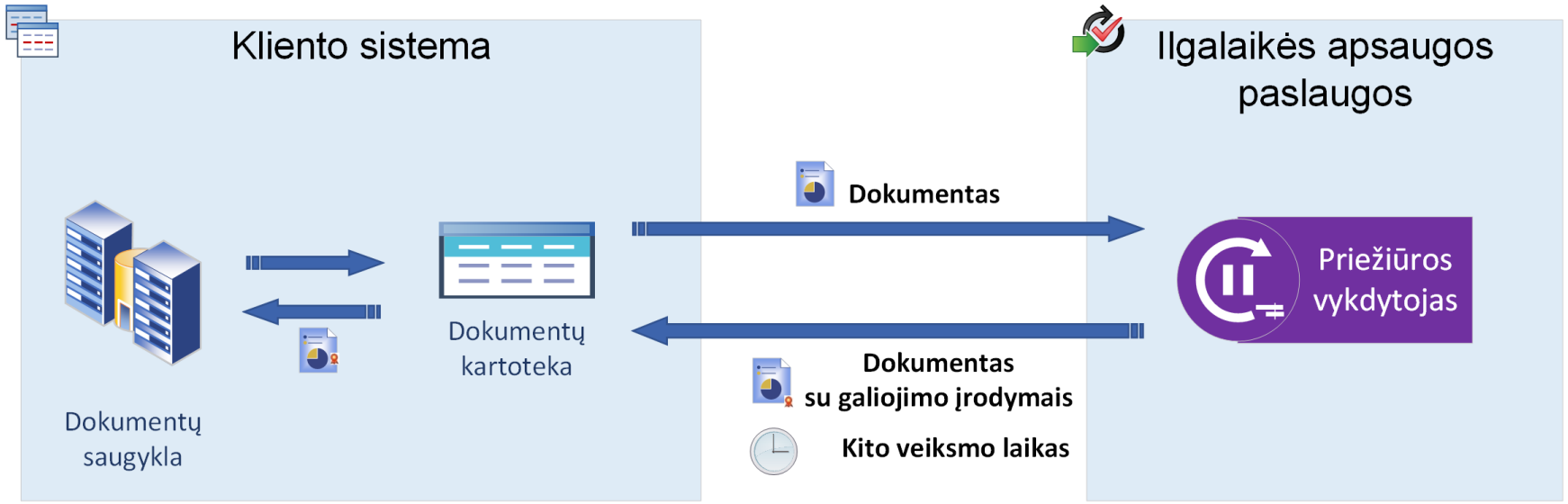
# Kaip naudoti: „su saugykla“

- Naudojimo būdas „su saugykla“:
  - Dokumentai saugomi paslaugos sistemoje
  - Apsaugos profilis su saugykla (WST: With Storage)



# Kaip naudoti: „be saugyklos“

- Naudojimo būdas „be saugyklos“:
  - Dokumentai saugomi kliento sistemoje
  - Apsaugos profilis be saugyklos (WOS: Without Storage)



# Ką galima saugoti?

15 skirtingų dokumentų ir konteinerių formatų:

- Visų Lietuvos specifikacijų dokumentai

  - ADOC-V1.0, ADOC-V2.0, EGAS-V1.0, MDOC-V1.0, PDF-LT-V1.0, PDF-RC-V1.0
- eIDAS reglamentuojami ir ES šalyse naudojami dokumentai

  - ASiC-E ir ASiC-S su XAdES ir CAdES parašais
  - PDF su PAdES parašais
- Su Adobe Acrobat pasirašyti dokumentai

  - PDF su CMS parašais

**Daugiau informacijos ir kontaktai**

**https://www.mitsoft.lt/paslaugos/**

**info@mitsoft.lt**