

Duomenų, teikiamų XML formatu, paketų paruošimas *Windows aplinkoje*

Instrukcija skirta paruošti paketą rankiniu būdu *OpenSSL* ir *Notepad++* priemonėmis *Windows* operacinėje sistemoje. Prisegami ir kiekviename žingsnyje sukuriami pavyzdiniai failai.

1. Paruošti konkretaus duomenų rinkinio XML failą, jį validuoti pagal XML schemą (XSD). Prisegamas CRS-DAC2-LT duomenų rinkinio pavyzdys *test_xml.xml*.

2. Sugeneruoti raktų porą:

```
OpenSSL> req -newkey rsa:2048 -nodes -keyout test_private_key.key -x509 -days 365 -out  
ties_imone.der -sha256 -subj "/C=LT/ST=Vilnius  
municipality/L=Vilnius/O=FINANSUISTAIGA/CN=TEST-IMONE"
```

OpenSSL

SVARBU

- Nurodant finansų įstaigos ir įmonės pavadinimus, norint panaudoti kabutes („“) pavadinime, kodo dalį *"/C=LT/ST=Vilnius municipality/L=Vilnius/O=FINANSUISTAIGA/CN=TEST-IMONE"*, vietoj dvigubų kabučių („“) apvilkti viengubomis (,'). Pvz. *"/C=LT/ST=Vilnius municipality/L=Vilnius/O="FINANSUISTAIGA"/CN="TEST-IMONE"'*.

Šia *OpenSSL* komanda sukuriamas privatus - *test_private_key.key*, saugotinas asmeninėje kompiuterinėje darbo vietoje, ir sertifikatas su viešu raktu *ties_imone.der*, kuris įkeliamas į TIES portalą (*TIES > Viešieji raktai > Įkelti naują*). Ši raktų pora bus reikalinga skaitmeninio parašo formavimui ir patikrai.

SVARBU

- Įsitikinti, kad privatų raktą atitinkantis viešasis raktas (sertifikatas) yra galiojantis, patalpintas į TIES portalą ir nebuvo TIES portale atšauktas.

3. Prieš skaičiuojant XML SHA256 maišos reikšmę, paaimamas visas XML turinys ir transformuojamas (*Exclusive XML Canonicalization*) pagal W3C specifikaciją, pasiekiamą adresu <https://www.w3.org/2001/10/xml-exc-c14n>:

Prisegami pavyzdžiai (pirminis failas → transformuotas): *test_xml.xml* → *test_xml_canonicalize.xml*

Įrankis, kurio pagalba galima greitai atlikti reikalingą transformavimą:

XmlStarlet - <https://sourceforge.net/projects/xmlstar/files/latest/download> (open source freeware under MIT license):

- Parsisiuntus įrankį, jį išsarchyvuoti.
- Į išsarchyvuotą aplanką įkelti norimą konvertuoti paruoštą XML failą.
- Atsidaryti komandinę eilutę (Start > Command Prompt), įeiti į tą patį aplanką, kur yra XmlStarlet įrankis ir jūsų paruoštas XML failas.
- Įvesti žemiau esančią komandą, vietoj *test_xml.xml* turi būti nurodytas jūsų paruoštas XML failas, vietoj *test_xml_canonicalize.xml* - sukuriama, konvertuoto XML failo pavadinimas.
- Įvykdžius žingsnius teisingai, tame pačiame aplanke bus sukurtas naujas, konvertuotas į kanoninę formą, XML failas.

```
xml c14n --exc-without-comments test_xml.xml > test_xml_canonicalize.xml
```



4. Transformuotą XML apvilkti *<Object>* elementu su pasirinktinu ID (šiam pavyzdyje tai „TIES“), išlaikant kanoninę formą:

Prisegami pavyzdžiai: *test_xml_canonicalize.xml* → *test_xml_object.xml*

| test_xml_canonicalize.xml | test_xml_object.xml |
|--|--|
| <pre><ns0:CRS-DAC2-LT xmlns:ns0="urn:sti:ties:crsdac2:v1" version="1.0"> <ns0:MessageSpec> ... </ns0:MessageBody> </ns0:CRS-DAC2-LT></pre> | <pre><Object xmlns="http://www.w3.org/2000/09/xmldsig#" Id="TIES"><ns0:CRS-DAC2-LT xmlns:ns0="urn:sti:ties:crsdac2:v1" version="1.0"> <ns0:MessageSpec> ... </ns0:MessageBody> </ns0:CRS-DAC2-LT></Object></pre> |

SVARBU

- Atkreipti dėmesį, kad *<Object>* *Id* parametro reikšmė turės sutapti su vėliau minimo *<Reference>* *URI* parametro reikšme.

5. Sugeneruoti *<Object>* elemento (*test_xml_object.xml*) SHA256 maišos reikšmę naudojant OpenSSL:

- Atlikus 4 žingsnio veiksmus, išsaugoti transformuotą ir apvilktą *<Object>* elementu XML failą. (Pateiktas pvz. *test_xml_object.xml*)
- Naudojant OpenSSL, komanda „*dgst -sha256 test_xml_object.xml*“ gauname SHA256 reikšmę.
- Vietoje „*test_xml_object.xml*“ nurodykite jūsų išsaugotą failą, kurį gavote atlikus 4 žingsnio veiksmus.

```
OpenSSL> dgst -sha256 test_xml_object.xml
SHA256(test_xml_object.xml)=
2cafe9a7d9b741402e2ff75defa039bd524cbc54a863b2194995160c7d055650
```



Šiuo atveju rezultatas *hexadecimal* reikšme yra:

2cafe9a7d9b741402e2ff75defa039bd524cbc54a863b2194995160c7d055650 Ją

reikia konvertuoti *base64* koduote, pavyzdžiui, su *Notepad++*:

Notepad++ >

1. File > New > Įkelkite gautą hexadecimal reikšmę
2. Pažymėkite įkeltą reikšmę kairiu pelės klavišu, įrankiu juostoje pasirinkite Plugins > Converter > HEX to ASCII
3. Pažymėti gautą reikšmę su pele ir paspaudus ant pažymėtos reikšmės dešinį pelės klavišą spausti Plugin commands > Base64 Encode



Rezultatas *base64*: LK/pp9m3QUAuL/dd76A5vVJMvFSOY7IZSZUWDH0FVIA=

SVARBU

- Gauta *base64* reikšmė privalo gale turėti lygybės simbolį „=“, gavus reikšmę be lygybės simbolio patikrinti ar teisingai atlikti 1, 3, 4 ir 5 žingsniai.

Sukurti naują XML failą ir į jį įkelti tik žemiau pateiktą XML struktūros dalį, į *<DigestValue>* elementą įkelti gautą maišos reikšmę *base64* formatu. (prisegamas pavyzdys: *canonicalized_sig.xml*):

canonicalized_sig.xml

```
<SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#"><CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></CanonicalizationMethod><SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"></SignatureMethod><Reference
URI="#TIES"><Transforms><Transform Algorithm="http://www.w3.org/2001/10/xml-
excc14n#"></Transform></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmenc#sha256"></DigestMethod><DigestValue>LK/pp9m3QU
AuL/dd76A5vVJMvFSOY7IZSZUWDH0FVIA=</DigestValue></Reference></SignedInfo>
```

6. Naudojant siuntėjo 2048 bitų privatuojį raktą (pavyzdys: *test_private_key.key*), kuris sudaro porą su siuntėjo viešuoju raktu, visą *<Signedinfo>* bloką (failas *canonicalized_sig.xml*) pasirašyti RSA skaitmeniniu parašu. Tinkami maišos algoritmai šiuo atveju yra RIPEMD160, SHA1, SHA256, SHA512. Pavyzdyje pasirašome su privačiu raktu *test_private_key.key*:

```
OpenSSL> dgst -sha256 -sign test_private_key.key -out canonicalized_sig_test.xml.sha256
canonicalized_sig.xml
```



Gautą failą paversti *base64* koduote:

```
OpenSSL> enc -base64 -in canonicalized_sig_test.xml.sha256 -out
canonicalized_sig_test.xml.base64
```



Skaitmeninis parašas turi būti įtrauktas į XML failą, naudojant „Enveloping“ parašo tipą (pats duomenų paketas įtrauktas į *<Object>* elemento vidų):

- *canonicalized_sig_test.xml.base64* turinį įsikelti į `<SignatureValue>` elementą.
- `<Object>` elementą apvilkti `<Signature>` elementu. Remiantis gautomis maišos ir parašo reikšmėmis suformuojamas galutinis failas - **00123456789_Payload.xml** (žiūrėti pridėtą pavyzdį ir prisegtą failą, kad įsitikinti teisinga struktūra).
- Failo pavadinimas privalo turėti 11 skaitmenų ir `_Payload.zip`. 11 skaitmenų sudaro jūsų įmonės kodas ir papildomi nuliai prieš įmonės kodą, kad pasiekti 11 skaitmenų ilgį. (Pvz jei jūsų įmonės kodas yra 123456789, failas privalo būti pavadintas 00123456789_Payload.xml. Taip pat žodis *Payload* privalo būti iš didžiosios raidės.
- Atkreipti dėmesį, kad `<Object>` *Id* parametro reikšmė turi sutapti su `<Reference>` *URI* parametro reikšme.

Daugiau apie parašo formavimą galima rasti W3C specifikacijoje: <https://www.w3.org/TR/xmlsig-core/>

0012345789_Payload.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /><Reference
URI="#FATCA"><Transforms><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" /></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-sha256" /><DigestValue>LK/pp9m3QUAuL/dd76A5vVJM
vFSoy7IZSZUWDH0FVLA=</DigestValue></Reference></SignedInfo><SignatureValue>laHw3PpaSuDHliZSd
gaeyEVQQBLo/37u7NwxEkkRdW+WTsrNLFJOsepsmilo4MXHHRDGPgIYzk9UrUoNKZx+L//SELaZkiH71V6+V62
6LwlmWF4/GvusxKA13KLsdm9nQ245kMMZDGV51b6ZWEeRRFObhVvdKhkkKcL77WcsFI2Vc+4chpXF15RCdGJ
b44Je4+dqRJmlooxNz+Xv1opUYhKc2e6BEHJU24Uoe29x1d1hy8p+zuTT8XpqlDJVcX8Pov0E/Vw+n7BKHX7LzJ
5rpxZPviXefdqwm2w5S1pqjwmEdcZ61wg35ObYznqhXLBsvU9lJt4yFO+do0r12WjxA==</SignatureValue>
....
....
....
</Signature>
```

7. Suarchyvuoti *zip* formatu - prisegamas pavyzdys - **00123456789_Payload.zip** (rekomenduojamas suspaudimo algoritmas (*compression method*) - *Deflate*).

SVARBU

- Įsitikinti, kad *zip* archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "*Deflate*" suspaudimo algoritmą.
- Failo pavadinimas privalo turėti 11 skaitmenų ir `_Payload.zip`. 11 skaitmenų sudaro jūsų įmonės kodas ir papildomi nuliai prieš įmonės kodą, kad pasiekti 11 skaitmenų ilgį.

8. Gautą suarchyvuotą failą užšifruojame AES raktu ir pradiniu vektoriumi (IV):

- AES rakto reikšmę galima gauti naudojant OpenSSL įrankį.
- OpenSSL> rand -hex 32
- Gaunama 64 simbolių reikšmė pavyzdžiui -
A604DB1C342735ACEDFC4DBA82051421285C9B346E2E6C2512348568B7DE5316
- Pradinį vektorių taip pat galima gauti naudojant OpenSSL įrankį.
- OpenSSL> rand -hex 16
- Gaunama 32 simbolių reikšmė pavyzdžiui - A22B0A0E8A440BD0CF829ED3BF22E151



```
OpenSSL> aes-256-cbc -p -nosalt -K
A604DB1C342735ACEDFC4DBA82051421285C9B346E2E6C2512348568B7DE5316 -iv
A22B0A0E8A440BD0CF829ED3BF22E151 -in 00123456789_Payload.zip -out
00123456789_Payload
```

```
key=A604DB1C342735ACEDFC4DBA82051421285C9B346E2E6C2512348568B7DE5316
iv =A22B0A0E8A440BD0CF829ED3BF22E151
```



AES rakta ir pradinį vektorių sujungti (*concatenate*), galima ir su *Notepad++*:

```
A604DB1C342735ACEDFC4DBA82051421285C9B346E2E6C2512348568B7DE5316A22B0A0E8A440B
D0CF829ED3BF22E151
```

Paversti į *binary* formatą:

- Notepad++ >
1. Sukūrus naują tekstinį failą ir įkėlus sujungtas AES rakto ir
IV reikšmes, pažymėti visą tekstą, iš įrankių juostos
pasirinkti Plugins > Converter > HEX to ASCII
 2. Išsisaugome pvz., kaip **aesKey.bin**



9. Atsisiųsti VMI sertifikatą iš TIES portalą ir išsieksportuoti viešą raktą (*TIES > Viešieji raktai > VMI raktai*).

```
OpenSSL> rsautl -encrypt -out 00123456789_Key -certin -inkey ties.vmi.lt_viesas.der -
keyform DER -in aesKey.bin
```

- Žodis **Key** privalo būti rašomas iš didžiosios raidės.



SVARBU

- Įsitikinti, kad naudojamas aktualus VMI viešasis raktas, kurį atsisiųsti galima prisijungus prie TIES portalą

10. 00123456789_Payload ir 00123456789_Key suarchyvuoti:

Prisegami pavyzdžiai: 00123456789_Payload ir 00123456789_Key → 20171027T074201890Z_00123456789.zip

- Suarchyvuoto failo pavadinimas sudaromas iš metų, mėnesio, dienos, T, valandos, minutės, sekundės, milisekundės (gali būti 000), Z, _ ir jūsų įmonės kodo (11 skaitmenų formatu).

11. Teikti gautą paketą į TIES portalą arba žiniatinklio būdu:

TIES > Duomenų paketai > Pateikti naują

Duomenų paketo pateikimas

Ataskaitinio laikotarpio pabaiga * 2016-12-31

Toliau

Pateikti paketai

TIES > Duomenų paketai > Pateikti naują

Duomenų paketo pateikimas

Ataskaitinio laikotarpio pabaiga 2016-12-31

| Duomenų rinkinio kodas, pavadinimas | XML schemos bylos pavadinimas, versija | Duomenų teikimo laikotarpis |
|---|--|-----------------------------|
| <input type="radio"/> MAI55-SLIK, MAI55-SLIK | M55Slik, 0.5 | 2017-01-01 - (nenurodyta) |
| <input type="radio"/> MAI55-SKIS, MAI55-SKIS | M55Skis, 0.4 | 2017-01-01 - (nenurodyta) |
| <input type="radio"/> MAI55-SIPL, MAI55-SIPL | M55Sipl, 0.5 | 2017-01-01 - (nenurodyta) |
| <input checked="" type="radio"/> CRS-DAC2-LT, CRS-DAC2-LT | , 0.5 | 2017-07-17 - (nenurodyta) |

Duomenų rinkinio aprašymas Duomenų rinkinys, kurį turi paruošti FĮ už ataskaitinį laikotarpį apie praneštinus asmenis (pagal duomenų teikimo taisykles) bei su jais susijusias finansines sąskaitas.

Rinkinio galiojimo laikotarpis 2016-01-01 - (nenurodyta)

Rinkinio nuoroda

Schemos pastabos Test 4.8.2

TIES > Duomenų paketai > Pateikti naują

Duomenų paketo pateikimas



Ataskaitinio laikotarpio pabaiga 2016-12-31
Duomenų rinkinio kodas CRS-DAC2-LT

Paketo failas * **Pasirinkti failą** 20171020T1... zip

Atgal

Įkelti

Pateikti paketą

TIES > Duomenų paketai > Pateikti naują

Duomenų paketo pateikimas



Paketas sėkmingai įkeltas ir šiuo metu yra apdorojamas. Peržiūrėti paketo būseną galite paspaudę [šia nuoroda](#)

Pateikti paketą

TIES > Duomenų paketai > [Pateikti paketą](#) > Paketo peržiūra

Paketo peržiūra

Duomenų paketo informacija

[Atsisiųsti paketą](#)

| | | | |
|-------------------------------|---|----------------------------|-----------------------------|
| Pateikimo data | 2017-10-20 15:56:49 | Apdorojimo ID | #579510-1ae5-496f-8b65-2ba6 |
| Pateikęs naudotojas | | Paketo pavadinimas | 20171020T125531653Z |
| Pateikimo būdas | Per TIES portalą | Paketo dydis (kilobaitais) | 3 |
| Paketo būsena | Pateiktas | Būsenos data | 2017-10-20 15:56:49 |
| Tipas | CRS-DAC2-LT | Atšaukimo data | |
| Duomenų rinkinio pavadinimas | CRS-DAC2-LT | Atšaukęs naudotojas | |
| Pranešimo Ref ID | LT_2016_LT_1000000001_RDBGOSD 201701150730 | | |
| Ataskaitinio laikotarpio data | 2016-12-31 | | |

| Klaidos kodas | Pavadinimas | Aprašymas | Užfiksuota |
|---------------|-------------|-----------|------------|
|---------------|-------------|-----------|------------|

Paketo failo klaidų nėra

Atšaukti paketą