

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*.

Galimos klaidos, veiksmą atlikus nekorektiškai:

20006 Nekorektiška XML pranešimo struktūra
Pranešimas neatitinka XML schemoje numatytos struktūros
20007 Nesutampa pranešimo tipas
Pranešime įrašytas pranešimo tipas (MessageType) nesutampa su nurodytu pateikiant duomenų paketą
20008 Nesutampa pranešimo identifikacinis numeris
Pranešime įrašytas pranešimo unikalus identifikavimo numeris (MessageRefID) nesutampa su nurodytu pateikiant duomenų paketą
20009 Nesutampa laikotarpio pabaigos data
Pranešime įrašyta ataskaitinio laikotarpio pabaigos data (ReportingPeriodEnd) nesutampa su nurodyta pateikiant duomenų paketą

SVARBU

- Naudojant įvairias XML validavimo su XSD schemomis programas įsitikinti, kad XML failas atitinka XSD schemas. Įsitikinti, kad naudojamos naujausios XSD schemų versijos, kurias galima atsisiųsti iš TIES portalas.

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 („“) apvilkkti 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, paimamas 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*

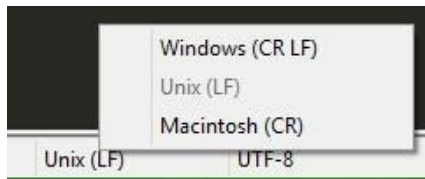
Žemiau paveiksluke nr. 1 parodomi skirtumai transformavus failą *test_xml.xml* į kanoninę formą *test_xml_canonicalize.xml*.

test_xml.xml	test_xml_canonicalize.xml
<pre> 1. <?xml version="1.0" encoding="UTF-8"?><ns0:CRS-DAC2-LT xmlns:ns0="urn:sti:ties:crsdac2:v1" version="1.0" xmlns:ns1="urn:sti:ties:crstypessti:v1" xmlns:ns2="urn:sti:ties:commontypessti:v1" xmlns:xsi="http:// www.w3.org/2001/XMLSchema-instance"> 2. <ns0:MessageSpec> 3. <ns1:Timestamp>2017-10-12T09:30:47Z</ns1:Timestamp> 4. <ns1:SendingCompanyIN>123456789</ns1:SendingCompanyIN> 5. <ns1:ReceivingCountry>LT</ns1:ReceivingCountry> 6. <ns1:MessageType>CRS-DAC2-LT</ns1:MessageType> 7. <ns1:Contact>Phone no:xxxxxxx</ns1:Contact> 8. <ns1:MessageRefId>LT_2016_LT_1000000001_RDBGOSD201701150732</ns1:MessageRefId> 9. <ns1:MessageTypeIndic>CRS701</ns1:MessageTypeIndic> 10. <ns1:ReportingPeriod>2016-12-31</ns1:ReportingPeriod> 11. </ns0:MessageSpec> 12. <ns0:MessageBody> 13. <ns1:ReportingFI> 14. <ns1:ResCountryCode>LT</ns1:ResCountryCode> 15. <ns1:IN INType="Tax payer code" issuedBy="LT">123456789</ns1:IN> 16. <ns1:Name>UAB "TEST_IMONE"</ns1:Name> 17. <ns1:Address legalAddressType="OECD301"> 18. <ns1:CountryCode>LT</ns1:CountryCode> 19. <ns1:AddressFix> 20. <ns1:Street>Adresu g.</ns1:Street> 21. <ns1:BuildingIdentifier>111111</ns1:BuildingIdentifier> 22. <ns1:SuiteIdentifier>111</ns1:SuiteIdentifier> 23. <ns1:DistrictName>Vilniaus m. sav.</ns1:DistrictName> 24. <ns1:PostCode>LT-11111</ns1:PostCode> 25. <ns1:City>Vilnius</ns1:City> 26. </ns1:AddressFix> 27. </ns1:Address> 28. <ns1:DocSpec> 29. <ns1:DocTypeIndic>OECD1</ns1:DocTypeIndic> 30. <ns1:DocRefId>LT_2017_LT_1000000001_VHJJN14882371</ns1:DocRefId> 31. </ns1:DocSpec> 32. </ns1:ReportingFI> 33. <ns1:ReportingGroup> 34. <ns1:AccountReport> </pre>	<pre> 1. <ns0:CRS-DAC2-LT xmlns:ns0="urn:sti:ties:crsdac2:v1" version="1.0"> 2. <ns0:MessageSpec> 3. <ns1:Timestamp xmlns:ns1="urn:sti:ties:crstypessti:v1">2017-10-12T09:30:47Z</ns1:Time p> 4. <ns1:SendingCompanyIN xmlns:ns1="urn:sti:ties:crstypessti:v1">123456789</ns1:SendingCompanyIN> 5. <ns1:ReceivingCountry xmlns:ns1="urn:sti:ties:crstypessti:v1">LT</ns1:ReceivingCountry> 6. <ns1:MessageType xmlns:ns1="urn:sti:ties:crstypessti:v1">CRS-DAC2-LT</ns1:MessageType> 7. <ns1:Contact xmlns:ns1="urn:sti:ties:crstypessti:v1">Phone no:xxxxxxx</ns1:Contact> 8. <ns1:MessageRefId xmlns:ns1="urn:sti:ties:crstypessti:v1">LT_2016_LT_1000000001_RDBGOSD201701150732</ MessageRefId> 9. <ns1:MessageTypeIndic xmlns:ns1="urn:sti:ties:crstypessti:v1">CRS701</ns1:MessageTypeIndic> 10. <ns1:ReportingPeriod xmlns:ns1="urn:sti:ties:crstypessti:v1">2016-12-31</ns1:ReportingPeriod> 11. </ns0:MessageSpec> 12. <ns0:MessageBody> 13. <ns1:ReportingFI xmlns:ns1="urn:sti:ties:crstypessti:v1"> 14. <ns1:ResCountryCode>LT</ns1:ResCountryCode> 15. <ns1:IN INType="Tax payer code" issuedBy="LT">123456789</ns1:IN> 16. <ns1:Name>UAB "TEST_IMONE"</ns1:Name> 17. <ns1:Address legalAddressType="OECD301"> 18. <ns1:CountryCode>LT</ns1:CountryCode> 19. <ns1:AddressFix> 20. <ns1:Street>Adresu g.</ns1:Street> 21. <ns1:BuildingIdentifier>111111</ns1:BuildingIdentifier> 22. <ns1:SuiteIdentifier>111</ns1:SuiteIdentifier> 23. <ns1:DistrictName>Vilniaus m. sav.</ns1:DistrictName> 24. <ns1:PostCode>LT-11111</ns1:PostCode> 25. <ns1:City>Vilnius</ns1:City> 26. </ns1:AddressFix> 27. </ns1:Address> 28. <ns1:DocSpec> 29. <ns1:DocTypeIndic>OECD1</ns1:DocTypeIndic> 30. <ns1:DocRefId>LT_2017_LT_1000000001_VHJJN14882371</ns1:DocRefId> 31. </ns1:DocSpec> 32. </ns1:ReportingFI> 33. <ns1:ReportingGroup xmlns:ns1="urn:sti:ties:crstypessti:v1"> 34. <ns1:AccountReport> </pre>

Pagrindiniai transformacijos metu atliekami keitimai:

- Naikinamas XML deklaravimas `<?xml version="1.0" encoding="UTF-8"?>`
- *Newline* turi būti *Unix* formato - *LF* (unicode U+000A), galima pakeisti

Notepad++
apatiname dešiniajame kampe.



- Koduotė UTF-8. *Notepad++* > *Encoding* > *UTF-8*
- *Namespace* perkeliama prie elementų, naudojančių juos faktiškai. Perkėlus *namespace*, į vaikius elementus jų kopijuoti nebereikia.
- Kiti reikalavimai, nurodyti <https://www.w3.org/2001/10/xml-exc-c14n>

Įrankiai, kurių pagalba galima greitai atlikti reikalingą transformavimą:

XmlStarlet - <http://xmlstar.sourceforge.net/> (open source freeware under MIT license):

```
C:\...\> xml c14n --exc-without-comments test_xml.xml > test_xml_canonicalize.xml
```

C:\>

Galima klaida, veiksmą atlikus nekorektiškai:

20010 "Iššifruotas failas nėra XML skaitmeniniu parašu pasirašytas XML failas"

Duomenų gavėjui nepavyko nuskaityti xml.

SVARBU

{SenderID}_Payload.zip archyvo faile turi būti patalpintas skaitmeniniu parašu pasirašytas xml dokumentas. Failas turi būti xml formatu, papildomai neužrakintas, nešifruotas, nepaverstas į BASE64 formatą ir pan.

- ☐ Įsitikinti, kad koduotė yra UTF-8
- ☐ *Newline* yra Unix formato
- ☐ Įsitikinti, ar *namespace* atitinka *Exclusive XML Canonicalization* reikalavimus

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>
--	--

Galima klaida, veiksmą atlikus nekorektiškai:

20010 "Iššifruotas failas nėra XML skaitmeniniu parašu pasirašytas XML failas

Duomenų gavėjui nepavyko nuskaityti xml.

SVARBU

- ☐ Įsitikinti, kad koduotė yra UTF-8
- ☐ *Newline* yra Unix formato (žr. žingsnį nr. 3)
- ☐ 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
```

OpenSSL

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/dd76A5vVJMvFS0Y7IZSZUWDH0FVIA=*

□ *<DigestValue>* reikšmė turi būti gauta paėmus *<Object>* elementą su visu duomenų XML, kuris yra *<Object>* elemento viduje, ir pavertus tokį XML į kanoninę formą xmlexc-c14n algoritmu. Apskaičiuota kanoninės formos XML teksto SHA256 maišos reikšmė turi būti paversta į BASE64 tekstą.

Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo su teikėjo viešuoju raktu.

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/xmlexcc14n#"></Transform></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"></DigestMethod><DigestValue>LK/pp9m3QU
AuL/dd76A5vVJMvFSoyY7IZSZUWDHOFVIA=</DigestValue></Reference></SignedInfo>
```

Galimos klaidos, veiksmą atlikus nekorektiškai:

20012 - "XML pranešimo skaitmeninio parašo DigestValue reikšmė netinkama"

6. Naudojant siuntėjo 2048 bitų privatųjį 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
```

OpenSSL

Gautą failą paversti *base64* koduote:

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

OpenSSL

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 apvilkkti *<Signature>* elementu. Remiantis gautomis maišos ir parašo reikšmėmis suformuojamas galutinis failas - *00123456789_Payload.xml*.
- 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/core/>

Galimos klaidos, veiksmą atlikus nekorektiškai:

20011 "XML pranešimo skaitmeninis parašas pasirašytas netinkamu algoritmu"

Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo.

SVARBU

- XML skaitmeninis parašas turi būti suformuotas naudojant "Enveloping" pasirašymo algoritmą. "Enveloped" ir "Detached" algoritmais pasirašytų XML dokumentų TIES sistema nepriima. Įsitikinti, kad pasirašytame XML faile duomenų XML dalis yra *<Object>* elemento viduje.

20013 "XML pranešimo skaitmeninio parašo SignatureValue reikšmė netinkama"

Duomenų gavėjui nepavyko patikrinti xml pranešimo skaitmeninio parašo.

SVARBU

- XML skaitmeninis parašas turi būti suformuotas naudojant "Enveloping" pasirašymo algoritmą. "Enveloped" ir "Detached" algoritmais pasirašytų XML dokumentų TIES sistema nepriima. Įsitikinti, kad pasirašytame XML faile duomenų XML dalis yra *<Object>* elemento viduje.

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

Galima klaida, veiksmą atlikus nekorektiškai:

20004 Nekorektiškas Payload zip failas

Duomenų gavėjui nepavyko išpakuoti gauto failo 00000000000_Payload.zip į 00000000000_Payload.xml

- 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

Cipher mode: CBC

Salt: No salt

Pradinis vektorius (PV): 16 byte IV

Key size: 256 bits/32 bytes

Encoding: None

Padding: PKCS#5 or PKCS#7

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

key=A604DB1C342735ACEDFC4DBA82051421285C9B346E2E6C2512348568B7DE5316
iv =A22B0A0E8A440BD0CF829ED3BF22E151
```

OpenSSL

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

```
A604DB1C342735ACEDFC4DBA82051421285C9B346E2E6C2512348568B7DE5316A22B0A0E8A440B
D0CF829ED3BF22E151
```

Paversti į *binary* formatą:

Notepad++ > Sukūrus naują tekstinį failą ir įkėlus sujungtas AES rakto ir

1. IV reikšmes, pažymėti visą tekstą, iš įrankių juostos pasirinkti Plugins > Converter > HEX to ASCII
2. Išsisaugome pvz., kaip **aesKey.bin**



arba

Linux Shell > xxd -r -p input.txt aesKey.bin



Galima klaida, veiksmą atlikus nekorektiškai:

20003 Nepavyko iššifruoti Payload failo

Duomenų gavėjui nepavyko iššifruoti gauto failo 00000000000_Payload į 00000000000_Payload.zip

SVARBU

- Įsitikinti, kad rakto faile (prieš užšifravimą) yra 48 baitų ilgio turinys. Tai yra, 32 baitų AES raktas, sujungtas su 16 baitų pradiniu vektoriumi (PV) (angl. "Initial Vector (IV)"
- Įsitikinti, kad naudojami tokie {SenderID}_Payload failo šifravimo su AES-256 sugeneruotu raktu nustatymai:
 - Cipher Mode: CBC ○ Salt: No Salt
 - Initialization Vector: 16 byte IV ○
 - Key size: 256 bits/32 bytes ○
 - Encoding: None ○ Padding: PKCS#5 or PKCS#7

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

Pirmas būdas, kuriuo iškart ir pasirašomas simetrinis raktas (nebereikalingas 10 žingsnis):

```
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.

Antrasis būdas:

Konvertuojame iš DER į PEM formatą:

```
OpenSSL> x509 -inform der -in ties.vmi.lt_viesas.der -out ties.vmi.lt_viesas.pem
```



Eksportuojame viešą raktą (p. s. rakto reikšmė čia yra reali ir aktuali 2017 10 23 dienai):

```
OpenSSL> x509 -pubkey -noout -in ties.vmi.lt_viesas.pem
```

```
-----BEGIN PUBLIC KEY-----
```

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1PAKIVxlv0sEZzt74NP  
RbcZNhhZI3SFLAUB4c00f+9YCAGas45DUVEk4vJX9HPGkg9Ay7Q08MeSCrtj0mTW  
7DZUjyS0lpPvSnX2m/Hb7ljpA4AB3FvqzJk8jbUMiYdqXrx3mJgPOFGSSn+4bdvn  
bWljEBeejOU+rvOF9gKXNnyzZFs9yLiZ74GVWXhJERzQA0A8DS0b5uyNhS4joMWz  
4WzmYclF+gGPweP/+2/pFJniFlivNyy/L/rRKvhseLDw+NS/Uiqoazfcxna1bwZ  
gtjSjNOvAOvDAUFM/aC/H+cnTyheG+nQMs2gkdgoW5cyfTPsd4zqBRZ/4Ji2M14K RQIDAQAB  
-----END PUBLIC KEY-----
```

OpenSSL

...ir gautą rezultatą išsisaugome kaip failą **ties_pubkey.pem** arba su

Windows komandine eilute:

```
C:\...\bin>openssl x509 -pubkey -noout -in ties.vmi.lt_viesas.pem > ties_pubkey.pem
```

C: \>

Galima klaida, veiksmą atlikus nekontroliškai:

20002 Nepavyko iššifruoti AES rakto

Duomenų gavėjui nepavyko iššifruoti AES rakto 000000000000_Key

SVARBU

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

10. AES rakto ir pradinio vektoriaus kombinaciją **aesKey.bin** pasirašyti viešu VMI raktu (9 žingsnio 2 būdo tęsinys): Užšifruoti anksčiau sugeneruotą AES raktą ir pradinį vektorius (PV) (48 bytes total - 32 byte AES key and 16 byte PV) su viešu VMI raktu. Prisegami pavyzdžiai: **aesKey.bin > 00123456789_Key**

- Padding: PKCS#1 v1.5
- Key size: 2048 bits

```
OpenSSL> rsautl -encrypt -inkey ties_pubkey.pem -pubin -in aesKey.bin -out  
00123456789_Key
```

OpenSSL

Galima klaida, veiksmą atlikus nekontroliškai:

20002 Nepavyko iššifruoti AES rakto

Duomenų gavėjui nepavyko iššifruoti AES rakto 000000000000_Key

SVARBU

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

11. **00123456789_Payload** ir **00123456789_Key** suarchyvuoti:

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

Galima klaida, veiksmą atlikus nekontroliškai:

20001 Nekorektiškas paketo zip failas

Duomenų gavėjui nepavyko išpakuoti zip arba nerastas Key/Payload failas.

SVARBU

- ☐ Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "Deflate" suspaudimo algoritmą.
- ☐ Įsitikinti, kad galutiniame archyve yra patalpintas **{SenderID}_Payload** failas. Atkreipti dėmesį į didžiąsias/mažąsias failo pavadinimo raides.
- ☐ Įsitikinti, kad galutiniame archyve yra patalpintas **{ReceiverID}_Key** failas. Atkreipti dėmesį į didžiąsias/mažąsias failo pavadinimo raides.

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

Duomenų paketo pateikimas



Ataskaitinio laikotarpio pabaiga *

2016-12-31



Toliau

Pateikti paketai

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

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](#)

Duomenų paketo pateikimas



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

[Pateikti paketą](#)

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 būseną	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](#)