

## MAI55 ir CRS-DAC2-LT duomenų paketų paruošimas *OpenSSL* ir *Notepad++* įrankiais

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 portalų.

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**

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*

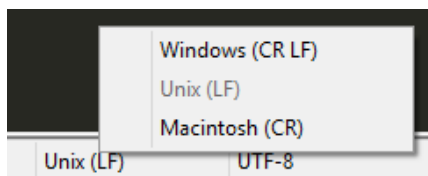
Žemiau paveiksluke nr. 1 parodomi skirtumai transformavus failą *test\_xml.xml* į kanoninę formą *test\_xml\_canonicalize.xml*.

test_xml.xml	test_xml_canonicalize.xml
<pre> 1. &lt;?xml version="1.0" encoding="UTF-8"?&gt;&lt;ns0:CRS-DAC2-LT xmlns:ns0="urn:sti:ties:crsdac2:v1" version="1.0" 2.   xmlns:ns1="urn:sti:ties:crstypessti:v1" xmlns:ns2="urn:sti:ties:commontypessti:v1" xmlns:xsi="http:// 3.     w3.org/2001/XMLSchema-instance"&gt; 4.     &lt;ns0:MessageSpec&gt; 5.       &lt;ns1:Timestamp&gt;2017-10-12T09:30:47Z&lt;/ns1:Timestamp&gt; 6.       &lt;ns1:SendingCompanyIN&gt;123456789&lt;/ns1:SendingCompanyIN&gt; 7.       &lt;ns1:ReceivingCountry&gt;LT&lt;/ns1:ReceivingCountry&gt; 8.       &lt;ns1:MessageType&gt;CRS-DAC2-LT&lt;/ns1:MessageType&gt; 9.       &lt;ns1:Contact&gt;Phone no:xxxxxxx&lt;/ns1:Contact&gt; 10.      &lt;ns1:MessageRefId&gt;LT_2016_LT_100000001_RDBGOSD201701150732&lt;/ns1:MessageRefId&gt; 11. 12.      &lt;ns1:MessageTypeIndic&gt;CR5701&lt;/ns1:MessageTypeIndic&gt; 13.      &lt;ns1:ReportingPeriod&gt;2016-12-31&lt;/ns1:ReportingPeriod&gt; 14.    &lt;/ns0:MessageSpec&gt; 15.    &lt;ns0:MessageBody&gt; 16.      &lt;ns1:ReportingFI&gt; 17.        &lt;ns1:ResCountryCode&gt;LT&lt;/ns1:ResCountryCode&gt; 18.        &lt;ns1:IN INType="Tax payer code" issuedBy="LT"&gt;123456789&lt;/ns1:IN&gt; 19.        &lt;ns1:Name&gt;UAB "TEST_IMONE"&lt;/ns1:Name&gt; 20.        &lt;ns1:Address legalAddressType="OECD301"&gt; 21.          &lt;ns1:CountryCode&gt;LT&lt;/ns1:CountryCode&gt; 22.          &lt;ns1:AddressFix&gt; 23.            &lt;ns1:Street&gt;Adresu g.&lt;/ns1:Street&gt; 24.            &lt;ns1:BuildingIdentifier&gt;111111&lt;/ns1:BuildingIdentifier&gt; 25.            &lt;ns1:SuiteIdentifier&gt;111&lt;/ns1:SuiteIdentifier&gt; 26.            &lt;ns1:DistrictName&gt;Vilniaus m. sav. &lt;/ns1:DistrictName&gt; 27.            &lt;ns1:PostCode&gt;LT-11111&lt;/ns1:PostCode&gt; 28.            &lt;ns1:City&gt;Vilnius&lt;/ns1:City&gt; 29.          &lt;/ns1:AddressFix&gt; 30.        &lt;/ns1:Address&gt; 31.        &lt;ns1:DocSpec&gt; 32.          &lt;ns1:DocTypeIndic&gt;OECD1&lt;/ns1:DocTypeIndic&gt; 33.          &lt;ns1:DocRefId&gt;LT_2017_LT_100000001_VHJJN14882371&lt;/ns1:DocRefId&gt; 34.        &lt;/ns1:DocSpec&gt; 35.      &lt;/ns1:ReportingFI&gt; 36.    &lt;/ns1:ReportingGroup&gt; 37.  &lt;/ns0:AccountReport&gt; </pre>	<pre> 1. &lt;ns0:CRS-DAC2-LT xmlns:ns0="urn:sti:ties:crsdac2:v1" version="1.0"&gt; 2.   &lt;ns0:MessageSpec&gt; 3.     &lt;ns1:Timestamp xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;2017-10-12T09:30:47Z&lt;/ns1:Timestamp&gt; 4.     &lt;ns1:SendingCompanyIN xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;123456789&lt;/ns1:SendingCompanyIN&gt; 5.     &lt;ns1:ReceivingCountry xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;LT&lt;/ns1:ReceivingCountry&gt; 6.     &lt;ns1:MessageType xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;CRS-DAC2-LT&lt;/ns1:MessageType&gt; 7.     &lt;ns1:Contact xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;Phone no:xxxxxxx&lt;/ns1:Contact&gt; 8.     &lt;ns1:MessageRefId xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;LT_2016_LT_100000001_RDBGOSD201701150732&lt;/ns1: 9.     MessageRefId&gt; 10.    &lt;ns1:MessageTypeIndic xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;CR5701&lt;/ns1:MessageTypeIndic&gt; 11.    &lt;ns1:ReportingPeriod xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt;2016-12-31&lt;/ns1:ReportingPeriod&gt; 12.  &lt;/ns0:MessageSpec&gt; 13.  &lt;ns0:MessageBody&gt; 14.    &lt;ns1:ReportingFI xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt; 15.      &lt;ns1:ResCountryCode&gt;LT&lt;/ns1:ResCountryCode&gt; 16.      &lt;ns1:IN INType="Tax payer code" issuedBy="LT"&gt;123456789&lt;/ns1:IN&gt; 17.      &lt;ns1:Name&gt;UAB "TEST_IMONE"&lt;/ns1:Name&gt; 18.      &lt;ns1:Address legalAddressType="OECD301"&gt; 19.        &lt;ns1:CountryCode&gt;LT&lt;/ns1:CountryCode&gt; 20.        &lt;ns1:AddressFix&gt; 21.          &lt;ns1:Street&gt;Adresu g.&lt;/ns1:Street&gt; 22.          &lt;ns1:BuildingIdentifier&gt;111111&lt;/ns1:BuildingIdentifier&gt; 23.          &lt;ns1:SuiteIdentifier&gt;111&lt;/ns1:SuiteIdentifier&gt; 24.          &lt;ns1:DistrictName&gt;Vilniaus m. sav. &lt;/ns1:DistrictName&gt; 25.          &lt;ns1:PostCode&gt;LT-11111&lt;/ns1:PostCode&gt; 26.          &lt;ns1:City&gt;Vilnius&lt;/ns1:City&gt; 27.        &lt;/ns1:AddressFix&gt; 28.      &lt;/ns1:Address&gt; 29.      &lt;ns1:DocSpec&gt; 30.        &lt;ns1:DocTypeIndic&gt;OECD1&lt;/ns1:DocTypeIndic&gt; 31.        &lt;ns1:DocRefId&gt;LT_2017_LT_100000001_VHJJN14882371&lt;/ns1:DocRefId&gt; 32.      &lt;/ns1:DocSpec&gt; 33.    &lt;/ns1:ReportingFI&gt; 34.  &lt;/ns1:ReportingGroup xmlns:ns1="urn:sti:ties:crstypessti:v1"&gt; 35.    &lt;ns1:AccountReport&gt; </pre>

Pav. nr. 1

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++* apatiniame dešiniajame kampe.



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

[rankiai, 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
```



Galima klaida, veiksmą atlikus nekorektiškai:

#### 20005 Nepavyko patikrinti xml pranešimo skaitmeninio parašo

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

#### SVARBU

- 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 (šiuo pavyzdyje tai „FATCA“), išlaikant kanoninę formą:

Prisegami pavyzdžiai: *test\_xml\_canonicalize.xml* → *test\_xml\_object.xml*

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

#### 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:

```
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. Plugins > Converter > HEX to ASCII
2. Select text and click right mouse button > Plugin commands > Base64
Encode
```



Rezultatas *base64*: *LK/pp9m3QUAuL/dd76A5vVJmVFSoY7IZSZUWDH0FVIA=*

Įdėti maišos reikšmę į taip pat transformuoto *<SignedInfo>* elemento vaikinį elementą *<DigestValue>* (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="#FATCA"><Transforms><Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></Transform></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></DigestMethod><DigestValue>LK/pp9m3QU
AuL/dd76A5vVJmVFSoY7IZSZUWDH0FVIA=</DigestValue></Reference></SignedInfo>
```

Galima klaida, veiksmą atlikus nekorektiškai:

**20005 Nepavyko patikrinti xml pranešimo skaitmeninio parašo**

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

#### SVARBU

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

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
```



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 apvilkkti *<Signature>* elementu. Remiantis gautomis maišos ir parašo reikšmėmis suformuojamas galutinis failas - *123456789\_Payload.xml*. 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/xmldsig-core/>

Galima klaida, veiksmą atlikus nekorektiškai:

#### 20005 Nepavyko patikrinti xml pranešimo skaitmeninio parašo

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

#### 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.
- 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.
- *<DigestValue>* reikšmė turi būti gauta paėmus *<Object>* elementą su visu duomenų XML, kuris yra *<Object>* elemento viduje, ir pavertus tokį XML į kanoninę formą *xml-exc-c14n* algoritmu. Apskaičiuota kanoninės formos XML teksto *SHA256* maišos reikšmė turi būti paversta į *base64* tekstą.
- *<SignatureValue>* reikšmė turi būti gauta paėmus *<SignedInfo>* bloką su jo viduje esančiu apskaičiuotu *<DigestValue>* ir kitais elementais pagal aprašymą <https://www.w3.org/TR/xmldsig-core/#sec-SignedInfo>
- *<SignedInfo>* blokas turi būti paverstas į kanoninę formą *xml-exc-c14n* algoritmu. Gauta kanoninė forma turi būti užšifruota su siuntėjo privačiu raktu *RSA-SHA256* algoritmu. Svarbu įsitikinti, kad privatų raktą atitinkantis viešasis raktas (sertifikatas) yra galiojantis, patalpintas į TIES portalą ir nebuvo TIES portale atšauktas.
- Atkreipti dėmesį, kad *<Object>* *Id* parametro reikšmė turi sutapti su *<Reference>* *URI* parametro reikšme.

7. Suarchyvuoti zip formatu - prisegamas pavyzdys - **123456789\_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

#### SVARBU

- Įsitikinti, kad zip archyvas atsidaro su populiariomis archyvavimo programomis. Patartina naudoti "*Deflate*" suspaudimo algoritmą.

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

*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 123456789_Payload.zip -out
123456789_Payload
```

OpenSSL

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

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

```
A604DB1C342735ACEDFC4DBA82051421285C9B346E2E6C2512348568B7DE5316A22B0A0E8A440B
D0CF829ED3BF22E151
```

Paversti į *binary* formatą:

Notepad++ >

1. 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 portalio ir išieksportuoti viešą raktą (*TIES > Viešieji raktai > VMI raktai*).

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

```
OpenSSL> rsautl -encrypt -out 188659752_Key -certin -inkey ties.vmi.lt_viesas.der -keyform DER -in aesKey.bin
```



**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-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE1PAKIVxlv0sEZzlt74NP
RbcZNhhZI3SFLAUb4c00f+9YCAGas45DUVEk4vJX9HPGkg9Ay7Q08MeSCrtj0mTW
7DZUjyS0lpPvSnX2m/Hb7ljPA4AB3FvqzJk8jbUMiYdqXrx3mJgPOFGSSn+4bdvn
bWljEBeejOU+rvOF9gKXNnyzZFs9yLiZ74GVWXhJERzQA0A8DS0b5uyNhS4joMWz
4WzmYcIF+gGPweP/+2/pFJniFliVNyv/L/rRKvhseLDw+NS/Uiqoazfcxbna1bwZ
gtjSjNOvAOvDAUFM/aC/H+cnTyheG+nQMs2gkdgoW5cyfTPSd4zqBRZ/4Ji2M14K
RQIDAQAB
-----END PUBLIC KEY-----
```



...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
```



Galima klaida, veiksmą atlikus nekorektiškai:

### 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 portalo

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** > **188659752\_Key**

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

```
OpenSSL> rsautl -encrypt -inkey ties_pubkey.pem -pubin -in aesKey.bin -out  
188659752_Key
```



Galima klaida, veiksmą atlikus nekorektiškai:

### 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 portalo

11. **123456789\_Payload** ir **188659752\_Key** suarchyvuoti:

Prisegami pavyzdžiai: **123456789\_Payload** ir **188659752\_Key** → **20171027T074201890Z\_123456789.zip**

Galima klaida, veiksmą atlikus nekorektiškai:

### 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:

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 schemas 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 FJ 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

Schemas pastabos Test 4.8.2

TIES &gt; Duomenų paketai &gt; 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 paketai

TIES &gt; Duomenų paketai &gt; Pateikti naują

## Duomenų paketo pateikimas



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

Pateikti paketai

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

## Paketo peržiūra

## Duomenų paketo informacija

[Atsisųsti paketa](#)

Pateikimo data	2017-10-20 15:56:49	Apdorojimo ID	#579510-1ae5-496f-8b65-2ba6
Pateikęs naudotojas	<span style="background-color: red; color: black;">[redacted]</span>	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 paketa