




Praktikum 15


<https://courses.cs.ut.ee/2024/turve/spring/Main/Praktikum15>


ÜL 1

 DIGIDOC

 ALLKIRI

 KRÜPTO

 Minu eID


RICHARD-SVEN RIVIK
[redacted] |  Lugejas on ID-kaart


Ümbrik: [/home/kasutaja/Desktop/Richard-Sven Rivik.cdok](#)

Krüpteeritud failid

Richard-Sven Rivik.txt

Adressaadid ⓘ

 **ALO PEETS** 38701112750
ID-kaart - Aegub 23. veebruar 2027

 **RICHARD-SVEN RIVIK** [redacted] (Sina ise)
ID-kaart - [redacted]

Ver. 4.5.1.4455

[← ALGUSESSE](#)

[ALLKIRJASTA](#)

[SALVESTA](#)

[EDASTA E-POSTIGA](#)

DEKRÜPTEERI
ID-KAARDIGA

ÜL 2

```
kasutaja@rivik: ~  
File Edit View Search Terminal Help  
kasutaja@rivik:~$ LDAPTLS_REOCERT=allow ldapsearch -H ldaps://esteid.ldap.sk.ee/ -x -b c=EE serialNumber="PN0EE-50307142730" > sert.txt  
kasutaja@rivik:~$ nano sert.txt  
kasutaja@rivik:~$ base64 -d < sert.txt | openssl x509 -inform der -text  
base64: invalid input  
Could not read certificate from <stdin>  
Unable to load certificate  
kasutaja@rivik:~$ nano sert.txt  
kasutaja@rivik:~$ base64 -d < sert.txt | openssl x509 -inform der -text  
base64: invalid input  
Certificate:  
Data:  
  Version: 3 (0x2)  
  Serial Number:  
    51:49:04:a6:53:d0:59:34:61:a8:76:58:ed:07:38:3e  
  Signature Algorithm: ecdsa-with-SHA512  
  Issuer: C = EE, O = SK ID Solutions AS, organizationIdentifier = NTREE-10747013, CN = ESTEID2018  
  Validity  
    Not Before: Dec  2 07:31:36 2021 GMT  
    Not After : Dec  1 21:59:59 2026 GMT  
  Subject: C = EE, CN = "RIVIK,RICHARD-SVEN,50307142730", SN = RIVIK, GN = RICHARD-SVEN, serialNumber = PN0EE-50307142730  
  Subject Public Key Info:  
    Public Key Algorithm: id-ecPublicKey  
    Public-Key: (384 bit)  
    pub:  
      04:47:53:6a:7b:23:27:60:0c:f8:63:05:f3:03:5c:  
      0e:83:c4:a7:7b:81:30:23:ab:92:c4:c5:5b:cc:ab:  
      3c:72:0b:e4:99:27:fd:5f:9a:ce:ed:f7:cd:5f:5f:  
      fc:ba:a7:b3:63:ab:0a:d7:71:a7:13:37:d2:bb:20:  
      b9:b1:81:fd:35:21:bd:01:49:79:ae:f8:28:13:29:  
      c2:eb:3b:32:dc:e8:94:66:27:2b:f4:c3:70:09:71:  
      e9:da:37:c9:c1:7b:71  
    ASN1 OID: secp384r1  
    NIST CURVE: P-384  
  X509v3 extensions:  
    X509v3 Basic Constraints:  
      CA:FALSE  
    X509v3 Key Usage: critical  
      Digital Signature, Key Agreement  
    X509v3 Certificate Policies:  
      Policy: 1.3.6.1.4.1.51361.1.1.1  
      CPS: https://www.sk.ee/CPS  
      Policy: 0.4.0.2042.1.2  
    X509v3 Subject Alternative Name:  
      email:50307142730@eesti.ee  
    X509v3 Subject Key Identifier:  
      68:ED:10:08:92:31:D8:E2:1D:79:8F:68:7B:0D:6B:FD:CB:EC:FF:BB  
    qcStatements:  
      0500....F..0G0E.7https://sk.ee/en/repository/conditions-for-use-of-certificates/..EN  
    X509v3 Extended Key Usage: critical  
      TLS Web Client Authentication, E-mail Protection  
    X509v3 Authority Key Identifier:  
      D9:AC:70:DB:5F:7E:BE:94:F8:A0:E4:BE:47:A2:D0:34:AD:9A:2A:12  
  Authority Information Access:  
    OCSP - URI:http://aia.sk.ee/esteid2018
```

ÜL 3

The screenshot shows the DIGIDOC application interface. The top bar displays the user name 'RICHARD-SVEN RIVIK' and the ID number '50307142730'. The left sidebar contains navigation icons for 'ALLKIRI', 'KRÜPTO', and 'Minu eID'. The main area shows the document 'matrikkel.txt' and the signing status 'Ümbriku allkirjad'. A terminal window shows the command 'sha256sum matrikkel.txt' and its output: 'nSbphxpPBpO5QvS6Usr6+R4Rxn/Qjd+sdDkyL3RyTLc=se64'. A separate window shows the XML signature file 'signatures0.xml' with its content.

Terminal Output:

```
kasutaja@rivik: ~/Desktop
File Edit View Search Terminal Help
kasutaja@rivik:~/Desktop$ sha256sum matrikkel.txt | cut -f1 -d\ | xxd -r -p | ba
se64
nSbphxpPBpO5QvS6Usr6+R4Rxn/Qjd+sdDkyL3RyTLc=
kasutaja@rivik:~/Desktop$
```

XML Signature Content:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<asic:XAdESSignatures xmlns:asic="http://uri.etsi.org/02918/v1.2.1#" xmlns:ds="http://www.w3.org/2000/09/
xmldsig#" xmlns:xades="http://uri.etsi.org/01903/v1.3.2#">
  <ds:Signature Id="S0">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
      <ds:Reference Id="S0-RefId0" URI="matrikkel.txt">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
        <ds:DigestValue>nSbphxpPBpO5QvS6Usr6+R4Rxn/Qjd+sdDkyL3RyTLc=
      </ds:DigestValue>
      </ds:Reference>
      <ds:Reference Id="S0-RefId1" Type="http://uri.etsi.org/01903#SignedProperties" URI="#S0-
SignedProperties">
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
        <ds:DigestValue>w5SYneLvGf9q20UUE7wpm19gIeBVyl9XL012pP9pI9c=
      </ds:DigestValue>
      </ds:Reference>
      <ds:SignedInfo>
        <ds:SignatureValue Id="S0-SIG">cYRFv1pPhI0khysbHecU12YHbdAX8MlwUteAGiemPH6hsNQMb9qderQkmbG+
09ksE1+i+/oImYJvSYWyH0+p8uZx7L2crUKX+xdCFHHlnepznPM/1WnMbVbE
H5suWiDI
        </ds:SignatureValue>
      </ds:KeyInfo>
    </ds:SignedInfo>
  </ds:Signature>
</asic:XAdESSignatures>
```