X509 Certificate:

Version: 3

Serial Number: 1b4cbd994211a18db387bb139ca094ca

Signature Algorithm:
  Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
  Algorithm Parameters: 05 00

Issuer:
  CN=E-GUVEN Nitelikli Elektronik Sertifika Hizmet Saglayicisi S2
  O=Elektronik Bilgi Guvenligi A.S.
  C=TR

NotBefore: 24.07.2020 20:29
NotAfter: 24.07.2021 20:29

Subject:
  CN=CANSU YILDIRICI
  SERIALNUMBER=47881134578
  C=TR
  O=TÜRKKEP KAYITLI ELEKTRONİK POSTA HİZMETLERİ A.Ş.
  OU=Bu sertifika,kayıtlı elektronik posta hizmet sağlayıcısının hizmetlerine ilişkin işlem verilerini imzalamak için kullanılır.

Public Key Algorithm:
  Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
  Algorithm Parameters:
  05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
  0000 30 82 01 0a 02 82 01 01 00 ea 78 71 a7 4e 63 0b
  0010 8d 18 39 da 73 5e e5 04 97 86 53 a6 80 8e 4e 26
  0020 e8 4d e8 db 85 a0 a3 c2 ac b9 fd 0a 4e e2 b2 1c
  0030 f1 c1 21 06 5d 0f 87 c6 b9 cc ef ce e6 fe 54 a0
  0040 13 84 4d cf 46 42 93 2f a8 34 8a 99 4b e1 12 e9
  0050 fd 38 3d e5 08 56 ac 6f c7 90 f5 01 53 d7 66 6c
  0060 fb 24 f5 8e 08 d4 54 21 13 82 ce 38 ce ba 65 ce
  0070 95 65 34 5b 9f f7 7f 9c c3 9c 41 b5 8c c6 bb 66
  0080 d6 0d ec 57 ab 28 8a 7d 90 81 d6 3a e3 31 56 91
  0090 64 63 82 56 ba 5b 3a b0 d8 5a 37 28 90 61 1e 48
  00a0 5a 3a aa 98 95 76 5f 88 17 ee 6e f1 9c 8d 2f 34
  00b0 43 3c 42 1a b9 33 88 1a 2a 86 e9 83 6c f1 b6 c4
  00c0 5a 59 d1 27 56 46 14 13 ff d7 71 e4 f5 50 23 f9
  00d0 44 64 11 74 61 2e 71 fa 5c ba a9 3d ec ae fd 0d
  00e0 07 6b 71 10 e7 57 ae d9 1b c4 1b 7d b1 6a 8b 8b
  00f0 de 4b 2d 5e 42 66 77 9e ee 94 98 68 fc 3d 83 d9
  0100 4c cf d8 88 1e c2 13 d3 07 02 03 01 00 01
Certificate Extensions: 9
  2.5.29.15: Flags = 1(Critical), Length = 4
  Key Usage

Digital Signature, Non-Repudiation (c0)

1.3.6.1.5.5.7.1.3: Flags = 0, Length = 12f
Qualified Certificate Statements
Unknown Extension type

```
0000  30 82 01 2b 30 08 06 06  04 00 8e 46 01 01 30 14   0..+0......F..0.
0010  06 06 04 00 8e 46 01 02  30 0a 02 02 03 18 02 01   .....F..0.......
0020  00 02 01 03 30 6d 06 0b  60 86 18 01 3d 00 01 a7   ....0m..`...=...
0030  4e 01 01 0c 5e 42 75 20  73 65 72 74 69 66 69 6b   N...^Bu sertifik
0040  61 2c 20 35 30 37 30 20  73 61 79 c4 b1 6c c4 b1   a, 5070 say..l..
0050  20 45 6c 65 6b 74 72 6f  6e 69 6b 20 c4 b0 6d 7a    Elektronik ..mz
0060  61 20 4b 61 6e 75 6e 75  6e 61 20 67 c3 b6 72 65   a Kanununa g..re
0070  20 6e 69 74 65 6c 69 6b  6c 69 20 65 6c 65 6b 74    nitelikli elekt
0080  72 6f 6e 69 6b 20 73 65  72 74 69 66 69 6b 61 64   ronik sertifikad
0090  c4 b1 72 30 81 99 06 0b  60 86 18 01 3d 00 01 a7   ..r0....`...=...
00a0  4e 01 02 0c 81 89 42 75  20 73 65 72 74 69 66 69   N.....Bu sertifi
00b0  6b 61 2c 20 6b 61 79 c4  b1 74 6c c4 b1 20 65 6c   ka, kay..tl.. el
00c0  65 6b 74 72 6f 6e 69 6b  20 70 6f 73 74 61 20 68   ektronik posta h
00d0  69 7a 6d 65 74 20 73 61  c4 9f 6c 61 79 c4 b1 63   izmet sa..lay..c
00e0  c4 b1 73 c4 b1 6e c4 b1  6e 20 68 69 7a 6d 65 74   ..s..n..n hizmet
00f0  6c 65 72 69 6e 65 20 69  6c 69 c5 9f 6b 69 6e 20   lerine ili..kin
0100  69 c5 9f 6c 65 6d 20 76  65 72 69 6c 65 72 69 6e   i..lem verilerin
0110  69 20 69 6d 7a 61 6c 61  6d 61 6b 20 69 c3 a7 69   i imzalamak i..i
0120  6e 20 6b 75 6c 6c 61 6e  c4 b1 6c c4 b1 72 2e      n kullan..l..r.
0000: 30 82 01 2b                    ; SEQUENCE (12b Bytes)
0004:    30 08                       ; SEQUENCE (8 Bytes)
0006:    |  06 06                    ; OBJECT_ID (6 Bytes)
0008:    |     04 00 8e 46 01 01
       |      ; 0.4.0.1862.1.1 European Qualified Certificate
000e:    30 14                       ; SEQUENCE (14 Bytes)
0010:    |  06 06                    ; OBJECT_ID (6 Bytes)
0012:    |  |  04 00 8e 46 01 02
       | |    ; 0.4.0.1862.1.2
0018:    |  30 0a                    ; SEQUENCE (a Bytes)
001a:    |     02 02                 ; INTEGER (2 Bytes)
001c:    |     |  03 18
001e:    |     02 01                 ; INTEGER (1 Bytes)
0020:    |     |  00
0021:    |     02 01                 ; INTEGER (1 Bytes)
0023:    |        03
0024:    30 6d                       ; SEQUENCE (6d Bytes)
0026:    |  06 0b                    ; OBJECT_ID (b Bytes)
0028:    |  |  60 86 18 01 3d 00 01 a7  4e 01 01
       | |    ; 2.16.792.1.61.0.1.5070.1.1
0033:    |  0c 5e                    ; UTF8_STRING (5e Bytes)
0035:    |     42 75 20 73 65 72 74 69  66 69 6b 61 2c 20 35 30  ; Bu sertifika,
50
0045:    |     37 30 20 73 61 79 c4 b1  6c c4 b1 20 45 6c 65 6b  ; 70 say..l.. E
lek
0055:    |     74 72 6f 6e 69 6b 20 c4  b0 6d 7a 61 20 4b 61 6e  ; tronik ..mza
Kan
```

```
0065:   |    75 6e 75 6e 61 20 67 c3  b6 72 65 20 6e 69 74 65  ; ununa g..re n
ite
0075:   |    6c 69 6b 6c 69 20 65 6c  65 6b 74 72 6f 6e 69 6b  ; likli elektro
nik
0085:   |    20 73 65 72 74 69 66 69  6b 61 64 c4 b1 72       ;  sertifikad..
r
        |       ; "Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nit
elikli elektronik sertifikadır"
0093:   30 81 99                          ; SEQUENCE (99 Bytes)
0096:     06 0b                           ; OBJECT_ID (b Bytes)
0098:     | 60 86 18 01 3d 00 01 a7  4e 01 02
          |    ; 2.16.792.1.61.0.1.5070.1.2
00a3:     0c 81 89                        ; UTF8_STRING (89 Bytes)
00a6:       42 75 20 73 65 72 74 69  66 69 6b 61 2c 20 6b 61  ; Bu sertifika,
ka
00b6:       79 c4 b1 74 6c c4 b1 20  65 6c 65 6b 74 72 6f 6e  ; y..tl.. elekt
ron
00c6:       69 6b 20 70 6f 73 74 61  20 68 69 7a 6d 65 74 20  ; ik posta hizm
et
00d6:       73 61 c4 9f 6c 61 79 c4  b1 63 c4 b1 73 c4 b1 6e  ; sa..lay..c..s
..n
00e6:       c4 b1 6e 20 68 69 7a 6d  65 74 6c 65 72 69 6e 65  ; ..n hizmetler
ine
00f6:       20 69 6c 69 c5 9f 6b 69  6e 20 69 c5 9f 6c 65 6d  ;  ili..kin i..
lem
0106:       20 76 65 72 69 6c 65 72  69 6e 69 20 69 6d 7a 61  ;  verilerini i
mza
0116:       6c 61 6d 61 6b 20 69 c3  a7 69 6e 20 6b 75 6c 6c  ; lamak i..in k
ull
0126:       61 6e c4 b1 6c c4 b1 72  2e                      ; an..l..r.
            ; "Bu sertifika, kayıtlı elektronik posta hizmet sağlayıcısını
n hizmetlerine ilişkin işlem verilerini imzalamak için kullanılır."
```

2.5.29.14: Flags = 0, Length = 16
Subject Key Identifier
64 27 8d cb 22 ff 33 f4 71 fd aa 01 b2 47 19 4b 69 28 44 fe

2.5.29.17: Flags = 0, Length = 22
Subject Alternative Name
RFC822 Name=cansu.yildirici@turkkep.com.tr

2.5.29.9: Flags = 0, Length = 33
Unknown Extension type

```
0000  30 31 30 1d 06 08 2b 06  01 05 05 07 09 01 31 11   010...+.......1.
0010  18 0f 31 39 39 33 30 37  31 35 30 30 30 30 30 30   ..19930715000000
0020  5a 30 10 06 08 2b 06 01  05 05 07 09 04 31 04 13   Z0...+.......1..
0030  02 54 52                                          .TR
0000: 30 31                               ; SEQUENCE (31 Bytes)
0002:   30 1d                             ; SEQUENCE (1d Bytes)
0004:   | 06 08                           ; OBJECT_ID (8 Bytes)
0006:   | | 2b 06 01 05 05 07 09 01
```

```
      | |    ; 1.3.6.1.5.5.7.9.1
000e:   | 31 11                    ; SET (11 Bytes)
0010:   |    18 0f                 ; GENERALIZED_TIME (f Bytes)
0012:   |       31 39 39 33 30 37 31 35  30 30 30 30 30 30 5a    ; 1993071500
0000Z
      |        ;  15.07.1993 03:00
0021:   30 10                     ; SEQUENCE (10 Bytes)
0023:     06 08                   ; OBJECT_ID (8 Bytes)
0025:     | 2b 06 01 05 05 07 09 04
        |    ; 1.3.6.1.5.5.7.9.4
002d:     31 04                   ; SET (4 Bytes)
002f:       13 02                 ; PRINTABLE_STRING (2 Bytes)
0031:         54 52                         ; TR
              ; "TR"
```

1.3.6.1.5.5.7.1.1: Flags = 0, Length = 70
Authority Information Access
[1]Authority Info Access
Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48
.1)
Alternative Name:
URL=http://ocsp2.e-guven.com/ocsp.xuda
[2]Authority Info Access
Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
Alternative Name:
URL=http://www.e-guven.com/documents/NESS2AltKok.crt

2.5.29.35: Flags = 0, Length = 18
Authority Key Identifier
KeyID=2d c5 e9 4b 22 39 40 88 a4 16 2b ce bd 46 07 f4 ac de bf a9

2.5.29.32: Flags = 0, Length = 169
Certificate Policies
[1]Certificate Policy:
Policy Identifier=2.16.792.3.0.1
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.e-guven.com/documents/NESUE.pdf
[1,2]Policy Qualifier Info:
Policy Qualifier Id=User Notice
Qualifier:
Notice Text=Bu sertifika, 5070 sayılı Elektronik İmza Kan
ununa göre nitelikli elektronik sertifikadır
[2]Certificate Policy:
Policy Identifier=2.16.792.3.0.1.1.1.2
[2,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.e-guven.com/documents/GKNESI.pdf
[2,2]Policy Qualifier Info:
Policy Qualifier Id=User Notice

```
            Qualifier:
                Notice Text=Bu sertifika, GKNESI kapsamında yayınlanmış b
ir nitelikli elektronik sertifikadır.

  2.5.29.31: Flags = 0, Length = 51
  CRL Distribution Points
    [1]CRL Distribution Point
      Distribution Point Name:
        Full Name:
          URL=http://sil.e-guven.com/ElektronikBilgiGuvenligiASGKNE
SIS2/LatestCRL.crl

Signature Algorithm:
  Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
  Algorithm Parameters:
  05 00
Signature: UnusedBits=0
  0000  f8 0b 9b e7 20 7c e7 65  5b 95 21 1c c1 0b c1 39
  0010  b6 e3 a7 d2 30 15 73 5e  bf 6d cf a2 9f e4 54 30
  0020  5f 38 53 5d e8 45 dd b5  a3 b9 98 a4 7d 23 cd 55
  0030  29 ae 34 01 13 29 fd df  be 78 1a df 27 77 ca fc
  0040  fe 22 96 19 ae cf 22 97  6f d2 22 77 d0 66 38 6d
  0050  3d e0 29 69 55 ac f5 b7  3c db c2 d1 e4 c7 21 96
  0060  8a f7 fe 36 45 3f 85 a0  e6 b1 70 5a 91 36 2b 72
  0070  6d 6e 03 19 a2 dc 67 62  cd a3 85 8f 91 85 7f eb
  0080  35 79 dd 4f 3c 26 d1 be  77 c3 53 45 fb 15 ec 6e
  0090  87 48 8a 52 7d df bd 75  22 af e8 50 fc f9 64 6d
  00a0  96 7e f8 27 57 48 4a 26  df 41 bf ce e6 5a eb 8c
  00b0  42 73 3e fd 25 d3 d6 4e  f3 5f 6f 0e d5 c4 19 bc
  00c0  19 03 3c d0 4b ab c8 aa  62 65 69 4b a3 f2 77 e4
  00d0  db 41 30 f3 63 7d ef 99  32 93 c1 0b 10 1d 4e dc
  00e0  c5 0f df 15 1b 28 be 07  bd 03 66 8e 03 ce b4 a2
  00f0  42 89 55 08 4b de 0a 84  13 cb b0 08 68 1e 30 3c
Non-root Certificate
Key Id Hash(rfc-sha1): 64 27 8d cb 22 ff 33 f4 71 fd aa 01 b2 47 19 4b 69 28 44
fe
Key Id Hash(sha1): 6b e0 dc 13 da e8 31 5e f3 87 91 26 42 17 5a 83 d4 25 b7 22
Cert Hash(md5): 4e fb 96 ec 1c 29 1f 6d 73 93 d3 79 de dc b8 2b
Cert Hash(sha1): d8 dc 82 00 6e 25 4e e3 8f ff 52 a6 86 40 c4 42 88 c2 68 d5
CertUtil: -dump command completed successfully.
```