X509 Certificate:

Version: 3

Serial Number: 06620766c7d16cd4fdbaffa14a56fec7

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

Name Hash(sha1): 369f024c45f86418ae48beae678da266bc9bb141

Name Hash(md5): fe41a2a9f95d8e59d506b8eda3df10c9

NotBefore: 15.08.2017 17:34

NotAfter: 15.08.2018 17:34

Subject:

CN=GAMZEGÜL YAVUZER

SERIALNUMBER=34322006662

C=TR

O=TÜRKKEP KAYITLI ELEKTRONİK POSTA HİZMETLERİ SAN VE TİC. A.Ş.

OU=Bu sertifika kayıtlı elektronik posta hizmet sağlayıcısının hizmetlerine ilişkin işlem verilerini imzalamak için kullanılır.

Name Hash(sha1): 4180ee9726c1ee9a64002c7b99821465679b91d5

Name Hash(md5): 4646b56c01b55b590ddb398e1b0ec189

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 d4 ac 50 f2 4e 5c 85

0010 f8 71 08 2a 21 81 fe 9f ef 00 ef 10 92 63 e2 d3

0020 6c 89 21 5a af fb 4c 4c 55 b7 62 7a c3 ca 8e c0

0030 71 1f 9b 51 04 64 b2 1f c5 e2 55 1e f7 48 0d e3

0040 0f 60 0a 00 2e 2a bc bc 4e 1d 7b 35 a8 e8 ae e7

0050 f6 2d 81 9d 01 c0 a3 32 de 6c 12 9d d7 9b c9 f9

0060 eb c4 ba 0b d1 83 cd 7f fe 23 a3 48 4e 51 74 8e

0070 15 be 76 3d d0 4b a9 71 21 8d 78 90 af 2d 4b 0a

0080 2d d0 6b 92 25 e6 e3 b8 5b 6b f1 1b 0d 00 a7 4b

0090 65 4f cf 03 68 74 b4 46 de d8 14 38 1c 31 b1 fd

00a0 52 37 77 1e 41 50 04 c1 0f bc 69 04 71 09 3d 42

00b0 78 06 ac ff 41 3d a0 33 98 66 94 f8 0b bf 31 34

00c0 9a 7a 41 47 7e 5d 49 f8 6c 30 7c 1b ba 24 f9 7d

00d0 60 50 3e 41 f9 82 71 ac 1e 64 e6 9a 2d fe 0b 4d

00e0 b3 5c 45 0e e8 8b 77 db 8e 49 4f d3 ac 49 d9 3e

00f0 be 24 4e 20 25 a6 23 22 b8 05 de 0e e3 2a 03 d4

0100 14 8d b9 97 f3 07 12 ce 47 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

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.. Elek

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 nite

0075: | 6c 69 6b 6c 69 20 65 6c 65 6b 74 72 6f 6e 69 6b ; likli elektronik

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 nitelikli 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.. elektron

00c6: 69 6b 20 70 6f 73 74 61 20 68 69 7a 6d 65 74 20 ; ik posta hizmet

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 hizmetlerine

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 imza

0116: 6c 61 6d 61 6b 20 69 c3 a7 69 6e 20 6b 75 6c 6c ; lamak i..in kull

0126: 61 6e c4 b1 6c c4 b1 72 2e ; an..l..r.

; "Bu sertifika, kayıtlı elektronik posta hizmet sağlayıcısının hizmetlerine ilişkin işlem verilerini imzalamak için kullanılır."

2.5.29.14: Flags = 0, Length = 16

Subject Key Identifier

9f a0 09 f8 60 76 fc ec bf f7 c0 31 b4 23 96 10 c9 06 26 e7

2.5.29.17: Flags = 0, Length = 23

Subject Alternative Name

RFC822 Name=gamzegul.yavuzer@turkkep.com.tr

2.5.29.9: Flags = 0, Length = 33

Subject Directory Attributes

2 attributes:

Attribute[0]: 1.3.6.1.5.5.7.9.1

Value[0][0], Length = 11

0000 18 0f 31 39 39 31 30 33 31 31 30 30 30 30 30 30 ..19910311000000

0010 5a Z

0000: 18 0f ; GENERALIZED_TIME (f Bytes)

0002: 31 39 39 31 30 33 31 31 30 30 30 30 30 30 5a ; 19910311000000Z

; 11.03.1991 03:00

Attribute[1]: 1.3.6.1.5.5.7.9.4

Value[1][0], Length = 4

0000 13 02 54 52 ..TR

0000: 13 02 ; PRINTABLE_STRING (2 Bytes)

0002: 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 Kanununa 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 bir 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/ElektronikBilgiGuvenligiASGKNESIS2/LatestCRL.crl

Signature Algorithm:

Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA

Algorithm Parameters:

05 00

Signature: UnusedBits=0

0000 8c 57 c9 1a aa 9d 0d 3a f6 fe b6 b1 3d ee 11 99

0010 71 57 4a 76 62 5c 03 4f f4 8a 7c 87 79 d2 cb 73

0020 20 ab 49 de 58 9a 91 da 1c 62 0e a3 d6 d6 d2 24

0030 64 ab 8f 6c cd 3f cc 9c f1 cd ce 23 97 06 af 09

0040 1f e1 bd 01 32 00 28 9c 55 ee b7 3e ce 77 35 7e

0050 a7 ee 01 f7 32 4b 57 dc 9b 08 f1 dd d4 8f 9e 16

0060 57 65 86 c9 48 e8 44 54 83 e2 98 22 53 31 de 1a

0070 59 72 d8 dc ec 52 1e 23 3d b8 6e 6c 61 5f 90 b8

0080 8c 5a bf be 4a 4d d9 cb fa ec 63 08 75 3c 66 eb

0090 46 19 ee 59 be 80 9b 23 33 d6 78 5c 7f cc 98 56

00a0 57 8f e6 ea d2 dc 4e f4 72 4f 76 21 4e 3d 17 18

00b0 75 3d c0 1b 48 b6 6b 02 2e 24 4d db a5 2b ef fa

00c0 44 6d 63 1e 1e 7c 61 8b 81 2d 76 38 33 e1 e4 9e

00d0 55 0b ee 45 96 7b 60 d6 df fb de a6 c0 4c 08 43

00e0 aa 5a fd c2 dd 0c a8 4c 8f 44 6b f8 a9 4f 99 0d

00f0 37 f8 b3 8f 91 fb 66 0e 54 45 0a 52 3f ce 46 50

Non-root Certificate

Key Id Hash(rfc-sha1): 9fa009f86076fcecbff7c031b4239610c90626e7

Key Id Hash(sha1): 0544dd80bcb31d80a8d5dba3db51854dfe2d62c9

Key Id Hash(md5): 981191bed00638008b08c32269561520

Key Id Hash(sha256): 0c6b3a84d5e8aa50047408d59872d45e58b75279e443f43e4406acc5dd813ed5

Cert Hash(md5): aadf6fb0eb4a50b35a2dbd6e32cfb3db

Cert Hash(sha1): 24394a2d61e2df9d55f508d3fe0282f52ee08f41

Cert Hash(sha256): e9d027b521cc5f55a44b3e2baf67fc0257965312718fe674bd475860e8b45301

Signature Hash: d833bc4d43f65dd1c1680aaf179e8dfa1f07ba515cbcaadd1cd743f6c812084f

CertUtil: -dump command completed successfully.