X509 Certificate:

Version: 3

Serial Number: 7f02eae2d58694e2cdda7d66d15878cf

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 17:14

NotAfter: 15.08.2018 17:14

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 d6 22 08 e3 98 de ba

0010 4a eb 7d a9 72 1a 8c f7 fd 39 33 3f 48 85 d0 6d

0020 a6 0d 78 f6 88 9b 9b c3 2e 5a 3f cb 99 a3 51 8e

0030 69 35 6f 0c 9a f0 3e e8 5e 8a 06 28 d8 52 17 7c

0040 ed 08 96 49 33 ab a6 2e f0 59 b2 40 0c 87 fa 37

0050 c8 d6 ad e8 e9 95 89 de d5 4e 98 7f 7b 17 6b 38

0060 90 b8 94 3e f2 c4 d6 a7 d3 5a ca 57 fc ce b8 fd

0070 e2 f7 8e 53 65 dd 4a 57 59 cc 40 26 35 22 93 ea

0080 d1 14 bc 69 56 56 85 1b 69 96 55 ed 1e 52 c1 9a

0090 24 75 cd 15 5c bf bf 6c 2f 5c 58 67 8f 8e ab 19

00a0 c3 97 23 1b 01 5c f7 89 06 8b a9 55 ac a2 f2 87

00b0 fc fb d1 ec 3a ec a2 e2 8c e8 14 28 10 e0 50 39

00c0 78 1b 6e 2b b4 ae e0 c9 33 33 90 20 b6 2f 44 37

00d0 41 bf b0 a4 d2 b3 f2 ae 28 a0 20 57 9e 11 df 96

00e0 0a 0b 1b 50 b1 ff 98 37 16 e5 ac db 84 5b d1 ef

00f0 7f 04 14 53 f7 e6 d3 1b 24 5b 97 53 b5 c2 7b 8a

0100 16 76 5a bb a4 d7 a4 3d dd 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

2f 8f 93 30 37 73 40 90 b4 d2 3d 2a a2 5c 6c c6 ed 75 f3 46

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 93 b9 8d 50 93 d4 c7 35 c0 69 de 59 fa ab f6 31

0010 12 34 e9 9a c2 f2 43 20 93 fc c3 dd cd 45 f5 91

0020 d1 6e c2 eb a2 51 b7 c9 23 b2 7f 42 88 6a c5 97

0030 51 a8 fd ab 26 d5 b1 03 02 85 94 e3 2a 89 59 e5

0040 b2 8a 1b 35 f5 a8 ea 7d 01 40 35 d5 4e 3f fc 54

0050 49 66 12 e6 ea e0 cd 3a d3 f7 06 80 58 d9 6b 02

0060 1e 8a cf 5a 77 12 ce be c6 62 c8 a0 8f 35 9f a7

0070 0d ee 68 6f 5e e4 d2 f8 49 4c f1 fc d6 7e 88 b1

0080 70 d0 d2 bf 75 95 5b 4f f5 7e 89 53 37 85 3d a4

0090 73 9d d5 10 29 1f 9a e3 bc 19 5a 83 ac 73 4f 43

00a0 19 2d 31 a5 ad 01 39 32 1a 89 48 e5 49 6a 30 da

00b0 1a 87 cb c7 6f f3 b7 96 2d 5b 2c 75 9a ef d1 e7

00c0 8d f8 8d f4 5b 01 91 c7 2d 56 33 55 5c a9 1f 07

00d0 b2 7e 1a bd 43 d3 f5 7d b3 11 60 e4 8b 60 cd 02

00e0 0f fa e3 5e 3f 51 aa cd c3 35 ba ab a3 c2 30 17

00f0 f3 cd c6 ac 1e 31 4e 1f 86 4a 49 e2 ee 7f 17 62

Non-root Certificate

Key Id Hash(rfc-sha1): 2f8f933037734090b4d23d2aa25c6cc6ed75f346

Key Id Hash(sha1): 7705240ef3a94200ae48637da5ee549e241b2e82

Key Id Hash(md5): 17b6e2ad4f1b6bd3305bd70024c77086

Key Id Hash(sha256): 0b24f92b7683333761be23e3e519f943f6b7720bd37eeea909c8e24b00346150

Cert Hash(md5): 357c3794968fa9ae6863d3294edc055c

Cert Hash(sha1): d81c7e208dfc348f2859d850539acb8d9887547c

Cert Hash(sha256): dc8dd4d99f129f2f44a103a31bde1440f4172d3a12c686eca5facdf7dfe7b522

Signature Hash: 6811f4cbb8b78b3f8ad5d4c5f29fd3c9acb6f1178dc20e7f97d43ef27ef1b071

CertUtil: -dump command completed successfully.