X509 Certificate:

Version: 3

Serial Number: 25b3d86c971884a3d6e333e3067ca2b9

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 17:58

NotAfter: 15.08.2018 17:58

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 b0 32 9b 0d 63 d6 44

0010 27 ea 84 cc 3d 6a 88 59 4f 07 db 94 91 67 e8 7d

0020 81 83 3b 18 11 95 c6 fe 77 d4 68 93 95 fa 3e 97

0030 a6 67 e9 cc 6b 23 ba 75 d9 1e c2 cf a4 69 a3 38

0040 30 f0 b4 a6 ff 24 7d 47 44 6c 4a 3f 6d 33 17 d0

0050 79 3d 23 d8 51 cd df 23 0d 5b 0d 6d 74 1e b4 0f

0060 e2 57 62 5c b7 91 1d 38 21 1a d1 37 93 b0 e0 ec

0070 9b dd cd 87 b5 25 ab 3d 7c d6 6a 83 07 9c 6a 42

0080 66 69 56 59 50 b6 f2 54 cc e3 98 0b 8f f7 a2 3e

0090 27 e0 b4 fe e8 4b f4 2a 6e 68 f6 e9 69 d3 12 47

00a0 d6 da 49 28 e0 06 23 44 1f 8f ee 9d 85 94 91 3d

00b0 24 d3 be 12 7d c1 a9 ca 47 b1 42 f8 46 70 a4 8d

00c0 07 5f 21 5b bc 9f a1 5d 71 a8 00 5f f0 a3 cd 59

00d0 f4 54 03 90 3c 6e 85 fa 1b 5b 66 3c e0 bd fa 73

00e0 3e 1c 24 6e ee 1c b4 7f 50 d3 44 52 bb 14 3d f8

00f0 fb 95 15 ff 27 dd e4 56 d3 79 d1 51 17 28 8e ca

0100 b0 58 65 c7 4f a1 db c7 af 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

e0 57 8b b1 f5 cd 62 8b cd f2 72 84 17 77 07 e7 38 88 d6 2c

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 5a ; 199103110000000Z

; 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 43 0a bc a5 d7 b5 65 1a 7a 8a 87 35 6b 28 0d 91

0010 b6 57 d7 a9 e3 e1 9f 93 4a 33 53 52 53 39 1e d6

0020 bc 27 5e 5b a4 68 30 f2 57 78 74 93 4e db 71 11

0030 79 12 b6 63 34 35 49 a1 e8 09 4b 1f bf 26 f8 f8

0040 82 09 69 e5 e6 90 50 af be 56 75 77 f3 93 90 4f

0050 72 f7 7f ed 30 68 99 8b bf cb ad e3 0d 8a 4f 5a

0060 0c 55 53 64 3e 3d 98 f9 d5 46 3f 79 7c 3d 22 6a

0070 5e 14 57 b1 2d 37 ec ff 5f 2a 9f bd 81 61 66 7b

0080 d1 de 8b bd 99 8c 7a 71 2b b6 03 e0 74 1b fb 60

0090 3a 8b 47 35 c4 9c 8b b4 07 2d 27 d0 26 a3 e7 bf

00a0 bd c0 3c 20 74 2b ca 85 96 9c de dc e3 6d 8c 07

00b0 92 a8 8a 77 76 77 aa 86 f4 44 29 8f 28 84 97 ba

00c0 ac ea 34 d3 f5 2b 22 49 04 d2 0e 41 34 f3 af cd

00d0 e6 94 14 fb ed 5b 35 2c 90 e4 fa 77 fb ae 75 d7

00e0 43 c9 04 19 31 84 ef 16 97 b3 ab ad d8 55 49 51

00f0 83 8f 93 40 6d b0 2e 97 9b ca a6 94 3d 57 0c 6d

Non-root Certificate

Key Id Hash(rfc-sha1): e0578bb1f5cd628bcdf27284177707e73888d62c

Key Id Hash(sha1): 17eb423b0dcf7edf75676161cd20c31fdb42bb04

Key Id Hash(md5): 63f50fff4f32e6a36fbd6ff4706867c9

Key Id Hash(sha256): befc8af30717b3221c7d612c1cbc4e973ba5808207b18056bc49855b6d7786fb

Cert Hash(md5): 6b303f69b16ba451e9f00400f40d189c

Cert Hash(sha1): c6e4de0483ebc1d25f4fd70848ab4fa7955e4aca

Cert Hash(sha256): 1c8ce0f6a299006d22f715b3a6eaf4dac613048595089f75e0109b6250b4830e

Signature Hash: 857a87d99b6233115af204f54c90a951dbc4b9e3fc5bc935edc643e58819e7fd

CertUtil: -dump command completed successfully.