Bugzilla ID: 476428 -- Add Turkish E-Guven root CA cert

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	**Data**
CA Name	E-Guven
Website URL	www.e-guven.com
Organizational type	private corporation
Primary market / customer base	E-Guven is a private corporation that serves certificates mainly to the Turkish market and they plan to expand their market to other countries. E-Guven certificates are used in Public projects as www.turkiye.gov.tr and Mobile Signature as well. E-Guven also develops B2B secure transaction projects.

Info Needed	**Data**
Certificate Name	e-Guven Kok Elektronik Sertifika Hizmet Saglayicisi
Cert summary / comments	This root certificate signs SSL certificates directly. Additionally, this root has the following three intermediate CAs: E-Guven Mobile CA issues mobile certificates for end users; E-Guven NES CA issues qualified electronic certificates for Turkish citizens; and E-Guven Secure Client Certificates issues Class 3 certificates. All of the intermediate CAs chaining up to this root are operated internally by e-Guven.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=367292
SHA-1 fingerprint.	dd:e1:d2:a9:01:80:2e:1d:87:5e:84:b3:80:7e:4b:b1:fd:99:41:34
Valid from	2007-01-04
Valid to	2017-01-04
Cert Version	3
Modulus length	2048
Test Website	https://www.e-guven.com/popup_pnbf.asp
CRL URL End-entity CRL update frequency	http://sil.e-guven.com/ElektronikBilgiGuvenligiASSSLClient/LatestCRL.crl (NextUpdate: 24 hours) http://sil.e-guven.com/ElektronikBilgiGuvenligiASRoot/LatestCRL.crl http://sil.e-guven.com/ElektronikBilgiGuvenligiASGKNESI/LatestCRL.crl
OCSP Responder URL	http://ocsp2.e-guven.com/ocsp.xuda
List or description of subordinate CAs operated internally	CA Hierarchy: https://bug476428.bugzilla.mozilla.org/attachment.cgi?id=360065 There is no subordinate-CA for issuing SSL certificates. SSL certificates are issued directly from the root. E-Guven root certificate has 3 intermediate CA: 1. E-Guven Mobile CA: Issues mobile certificates for end users. 2. E-Guven NES CA: Issues qualified electronic certificates for Turkish citizens. 3. E-Guven Secure Client Certificates: Used to issue Class3 certificates.

SubCA's operated by 3rd parties	None. All of the sub-CAs of this root are operated internally by e-Guven.
Cross-Signing	none
Requested Trust Bits	Websites Email
For SSL: DV, OV, and/or EV	OV
EV policy OID	Not EV
CP/CPS	All documents are in Turkish. Qualified Electronic CP (GKNESI): http://www.e-guven.com/Documents/genel_kullanima_iliskin_nes_ilkeleri.pdf Mobility Qualified Electronic CP: http://www.e-guven.com/Documents/MKNESI_1.1.pdf Qualified Electronic Cert Application Basics: http://www.e-guven.com/Documents/NESUE_2.1.pdf SSL Cert Application Basics: http://www.e-guven.com/Documents/SUE_1.0.pdf Attached to bug to enable copy-and-paste for translation purposes: Qualified Electronic CP (GKNESI): https://bugzilla.mozilla.org/attachment.cgi?id=400444 Mobility Qualified Electronic CP (MKNESI): https://bugzilla.mozilla.org/attachment.cgi?id=400445 Qualified Electronic Cert Application Basics (NESUE): https://bugzilla.mozilla.org/attachment.cgi?id=400445 SSL Cert Application Basics (SUE) https://bug476428.bugzilla.mozilla.org/attachment.cgi?id=403222
AUDIT	Audit Type: ETSI 101 456 Auditor: Turkey Government's Information Technologies and Communications Authority Auditor Website: http://www.tk.gov.tr Audit: https://bugzilla.mozilla.org/attachment.cgi?id=421006 (2009.11.06) Confirmed authenticity of the new audit statement by sending email to a known contact at the ICTA: Subject: RE: Confirming Authenticity of Audit Statement provide by E-Guven Date: Tue, 12 Jan 2010 10:19:35 +0200 From: Demet KABASAKAL dkabasakal@btk.gov.tr To: Kathleen Wilson kwilson@mozilla.com Dear Mr Wilson I have been working as a Informatics Expert and member of electronic signature audit team at the Turkish Information and Communication Technologies Authority (hereafter ICTA). As one of the electronic signature audit team members I would like to confirm that we (ICTA) have issued the audit statement at the mentioned URL. In Turkey, electronic certificate service provider such as e-Guven shall be inspected by the ICTA when it is necessary and at least biannual at the ICTA's own initiative. Yours sincerely Demet KABASAKAL Informatics Expert, Inormation technologies and Communication Authority

	Comment #10: Our latest audit document from Turkish Standards Institute (audited yearly for ISO:27001 criterias.) https://bugzilla.mozilla.org/attachment.cgi?id=367583 (ISO 27001) ISO Auditor Website: http://www.tse.gov.tr
Verification of Identity and Organization	Comment #15: E-Güven may use Dun & Bradstreet (D&B) or TOBB database to check company registration. The name appearing in the distinguished name in the certificate application must match the name on file with D&B or TOBB database with the exception of the organization's extension (for example: Inc., Co, Ltd, N.V., B.V., etc.). We do not require the customer to include their company's extension. For instance, if a customer enrolled as XYZ and the name on the D&B or TOBB database report is XYZ A.S. , this would be accepted since the 'A.S. can be dropped. If the name does not match or the organization does not have a D&B number or TOBB database, notify the customer to correct the incorrect information or submit an alternative proof of right document.
Domain Name Ownership/Control	Comment #15: Verify that the organization requesting the ID also owns the domain name that appears in the common name field in the distinguished name as with the validation of the organization name. The common name cannot be an IP address or include spaces, commas, slashes or other similar characters. We find the appropriate domain registry for the domain in the request. To check a .com, .net, or .org domain, go to Checkdomain's whois http://www.name.com.. Or , go to https://www.nic.tr or an ICANN-Accredited registrar Google Translation of Annex C (EK-C) of SUE_1 0_v2 APPENDIX C - SSL Certificate Application Required Documents – E-Guven will verify the information and official documents as follows. Name-Surname/Company Name: National ID, Passport, Driving License, Lawyer Identity Certificate (For Lawyers), or Certified Copies of Aslı http://www.sanayi.gov.tr/Sirket/UnvanSorgulama.aspx?menuSec=234 http://www.ticaretsicil.gov.tr/ http://sanayi.tobb.org.tr/ T.C. ID: http://www.tckimlik.nvi.gov.tr Identity: National ID, Passport, Lawyer Identity Certificate (For Lawyers) Drivers License or Notary Certified Copies of Aslı or Notary Certified Copies of passport Domain Name: www.name.com veya .com.tr uzantılı alan adları için www.nic.tr gibi kayıtlı whois sunucularından kontrol edilebilir. (Google Translation: www.name.com or .com.tr extension for domain names registered whois servers as www.nic.tr can be controlled.
Email Address Ownership/Control	Comment #15: E-Guven makes confirmation of the applicant's e-mail address by requiring the applicant to be able to answer an e-mail to relevant address. Google Translation of SUE_1 0_v2.doc 3.2.2 Verification of Identity of Legal Persons

	SSL certificate to be granted to legal entities in the commercial register recording the identity of certificate applicants, the signature is verified through official documents such as sürküleri. As well as knowledge of electronic mail sent from the user to control up to e-mail with the correct response is to be taken. 3.2.3 Identity Verification of Real People e-Guven, a certificate to apply for real people credentials of birth, passport, driver's license with a photo such as the current official documents, depending on credentials other than a certificate will be included within other information e-Guven is determined by the official documents based on checks. As well as knowledge of electronic mail sent from the user to control up to e-mail with the correct response is to be taken.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV o Comment #9: We issue 1-3 years of SSL certificates. and require applicant to prove his/her organization infor and domain info. • Wildcard DV SSL certificates o SSL certs are OV • Delegation of Domain / Email validation to third parties o Comment #9: We do not delegated validation procedures to any other third party for email /domain validation. • Issuing end entity certificates directly from roots o Comment #9: Our root certs are stored in HSM 's. **We only issue SSL certs from our root**. • Allowing external entities to operate unconstrained subordinate CAs o Not applicable • Distributing generated private keys in PKCS#12 files o Comment #9: In every key generation scenario keys are generated in client side by enrollment pages. • Certificates referencing hostnames or private IP addresses o Comment #15: The common name cannot be an IP address. • OCSP Responses signed by a certificate under a different root o I am able to go to the test website with OCSP enforced. • CRL with critical CIDP Extension o CRLs imported into Firefox without error. • Generic names for CAs o Root CA name is not generic.
English Translations GKNESI_2.0_29_01_2007_temiz.doc	The following are Google Translations of the document: E-Guven Qualified Electronic Certificate Policy (GKNESI_2.0_29_01_2007_temiz.doc)

	7. NES Application Under GKNESİ NES application and how to make the identification of the NES User Agreement / Undertaking in the Agreement and GKNESİ Enterprise Application describes in detail. Applications for individual and institutional applications under GKNESİ NES as a direct e-Trust or register to be contacted by the Authority is scheduled. 7.1 Enterprise Applications Enterprise applications, in general, in accordance with the following process is carried out; • the person who has applied for NES NES's institutional applicants have to declare the will related to the (front contact) • Corporate applicant's e-Trust Agreement entered into with the application of Corporate • Corporate applicant's behalf to the certificate holder to apply for NES e-Trust NES User Agreement / Undertaking of the 'ni signed • Corporate applicants, NES, contact the person relating to the authentication procedures Nesu 3.2, as set forth in the fulfilling, • Corporate applicants to apply for NES by the person signing the NES and stuffed User Agreements / Undertaking relevant copies of the NES application and the person by his message to the owner of the NES, NES will be included within the information used to verify the documents of the collection. 7.2 Individual Applicants Individual application in general is subject to the following procedures; • The person's e-Trust NES claim or authority in the presence of KM will be included within the certificate information Nesu 3.2.3.1 according to the evidence • NES request of the person NES User Agreement / Undertaking of the 'ni to sign, NES Owner keeping copies on their own seven copies of the contract with the certificate within ESHS where you want to receive information that the expansion will be e-trust certificates, or be handed over to authorities in KM 7.3 Application Process e-Trust, km's or corporate references officials Nesu 3.2 as set forth identification and authentication methods are required to do. KM or e-Trust in ensuring that the following conditions NES accept applications; • Nesu 3.2, as set forth identification and authentication procedures have been fully met, • NES is fee paid KM or e-Trust in the following cases of NES reject the application; • Nesu 3.2, as set forth identification and authentication procedures have not been fully met, • the person on the NES application or the applicant's own corporate information and documents requested have not

	fully provided, • the person or enterprise to apply for NES applicants were notified to him or any warning or notice mentioned does not respond timely reminder and notification is not fulfill the issues,
English Translations NESUE_2.1_03_08_2007_temiz.doc	The following are Google Translations of the document: E-Guven Qualified Electronic Certificate Application Basics (NESUE_2.1_03_08_2007_temiz.doc) 3.2.3 Identity Verification of Real People e-Trust, NES applies for the persons who have the credentials of birth, passport, driver's license with a photo such as the current official documents, depending on credentials outside the NES will be included within other information e-Trust is determined by the official documents based on km's or corporate contact authorities through checks. NES application in anyone's identity and credentials outside the NES will be included within other information, contact the main person other than e-Trust established by official documents based in another application has been determined or the application in question is corporate applications; NES application during the person's person need not exist. NES in terms of detection of the information contained within e-trust application to individual and institutional functioning of the two reference model is envisaged. 3.2.3.2 Enterprise Application Enterprise application model, a legal entity employees or customers or members or shareholders on behalf of the application is located in the NES. Corporate e-trust conditions relating to the application or to be concluded between the applicant KM institutional and corporate contracts is determined by the application. Enterprise application contracts, corporate models, taking into account the application is being prepared. Corporate reference model, e-Trust will apply the corporate communities (eg Financial Institutions, such as GSM operator) is applied in specific business processes or enterprise applications to be found in corporate annual application of institutions taking into consideration the demands are determined. Corporate reference model, e-trust, KM and enterprise search applicant's institutional application be made, the certificate holder's identity is determined, the necessary documents for the preparation of the certification fees to be paid, documents preservation of qualified electronic publication of certificates and certificates to be forwarded to the owner, certificate revocation, renewal and suspension of matters such as claims procedures determined by the transmission of technical and administrative processes can be described as consisting of business model. NES will be in contact with corporate credentials within the NES and other information to identify the necessary documents to be taken by processes such as corporate applicant is satisfied. Corporate applicant, e-KM with the Trust or the Company signed a contract application determined in accordance with the provisions of the enterprise application model according to the e-between with the Trust which was established through a secure system, e-trust by arranging NES will basis NES NES within the owner's information will be e - transmits to the Trust.

	Corporate applicant, NES applicant's identity and the certificate will be included within the information used in the determination and application from him during a requested all information, records and documents of the NES by institutional applicant transmitted any information, documents and request e-Trust name and account to hide required whether or not issues with e-Confidence 4.1.2.2 Individual Application Individual application in general is subject to the following procedures; • The person's e-Trust NES claim or authority in the presence of KM will be included within the certificate information Nesu 3.2.3.1 according to the evidence • NES request of the person NES User Agreement / Undertaking of the 'ni to sign, NES Owner keeping copies on their own seven copies of the contract with the certificate within ESHS where you want to receive information that the expansion will be e-trust certificates, or be handed over to authorities in KM NES 4.2 Application Process 4.2.1 Identification and Authentication Process Functions e-Trust km's or corporate contact officials Nesu 3.2 as set forth identification and authentication methods are required to do. 4.2.2 Acceptance and Rejection of Application NES KM or e-Trust in ensuring that the following conditions NES accept applications; • Nesu 3.2, as set forth identification and authentication procedures have been fully met, • NES is fee paid KM or e-Trust in the following cases of NES reject the application; • Nesu 3.2, as set forth identification and authentication procedures have not been fully met, • the person on the NES application or the applicant's own corporate information and documents requested have not fully provided, • the person or enterprise to apply for NES applicants were notified to him or any warning or notice mentioned does not respond timely reminder and notification is not fulfill the issues, NES 4.2.3 Application Process Scheduling e-Trust NES contracts related to the application of a provision is not specific as possible will respond as soon as possible.