e-tuğra

CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
(E-Tugra EBG Information Technologies and Services Corp.)
Version: 3.0
Validity Date: March, 2020
Update Date: 30/03/2020

Ceyhun Atıf Kansu Cad. 130/58
Balgat / ANKARA
TURKEY

Phone: 90.850.532.23.14
Phone: 90.850.532.23.12
Fax: 90.312.473.56.91
www.e-tugra.com.tr

Certificates

E-Tugra Certification Authority

SHA-1 Fingerprint: *51:C6:E7:08:49:06:6E:F3:92:D4:5C:A0:0D:6D:A3:62:8F:C3:52:39*
SHA-256 Fingerprint : *B0:BF:D5:2B:B0:D7:D9:BD:92:BF:5D:4D:C1:3D:A2:55:C0:2C:54:2F:37:83:65:EA:89:39:11:F5:5E:55:F2:3C*
Certificate ID : *E7:4F:96:BD:9C:3E:CB:DF:0F:E0:D5:69:69:BE:3B:56:A6:13:07:95:A4:F3:40:2A:C9:93:95:16:74:D4:62:1A*

E-Tugra Domain Validated CA

SHA-1 Fingerprint : *72:20:2D:58:4B:CB:71:4D:F7:78:26:9C:46:09:17:AF:FE:05:0A:42*
SHA-256 Fingerprint : *CB:6F:CE:E4:1C:55:E2:47:74:DF:02:BE:35:DE:6D:41:8E:94:EF:58:11:F7:DB:13:73:AF:88:09:CF:70:7F:2A*
Certificate ID : *AE:D3:A9:38:59:D9:62:F7:36:B8:28:C8:BD:D3:5B:98:F9:28:82:A9:8A:FE:20:D7:85:86:22:75:AC:EE:CF:75*

E-Tugra Organization Validated CA

SHA-1 Fingerprint : *35:D4:FB:C1:C2:7B:25:96:D9:40:75:ED:8D:7D:63:D9:CC:1B:C3:BC*
SHA-256 Fingerprint : *11:47:53:E8:8D:00:0E:75:99:61:5A:99:07:E2:6B:73:B6:D8:51:31:7F:F2:B2:7A:CA:9D:B8:FC:50:56:92:A7*
Certificate ID : *64:43:81:45:0A:9C:49:9F:26:F6:38:18:9F:D3:B2:CC:26:53:8F:9C:27:22:C4:E6:95:B3:8C:D7:9F:B0:DC:B8*

E-Tugra Extended Validated CA

SHA-1 Fingerprint : *56:98:BD:0A:31:1D:2C:28:15:05:6D:AB:5A:83:18:C9:E5:4A:11:7E*
SHA-256 Fingerprint : *CE:7A:DC:19:77:57:A5:2E:69:A2:01:4C:CE:03:D9:80:63:25:02:76:47:42:C2:92:3D:73:80:56:8E:21:00:A6*
Certificate ID : *CF:01:00:C3:03:79:51:92:C9:D2:EC:52:A2:75:09:52:8E:F8:A5:65:A2:61:42:34:9A:61:E7:62:7A:73:B6:69*

E-Tugra Global Root CA RSA v3

SHA-1 Fingerprint: *E9:A8:5D:22:14:52:1C:5B:AA:0A:B4:BE:24:6A:23:8A:C9:BA:E2:A9*
SHA-256 Fingerprint : *EF:66:B0:B1:0A:3C:DB:9F:2E:36:48:C7:6B:D2:AF:18:EA:D2:BF:E6:F1:17:65:5E:28:C4:06:0D:A1:A3:F4:C2*
Certificate ID : *?*
Serial Number: *0D:4D:C5:CD:16:22:95:96:08:7E:B8:0B:7F:15:06:34:FB:79:10:34*
Subject: *CN = E-Tugra Global Root CA RSA v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.
L = Ankara
C = TR

E-Tugra Domain Validated CA RSA v3

SHA-1 Fingerprint : *1D:C7:6E:17:04:B1:39:FF:C4:AA:05:49:6D:BB:A0:17:63:2F:0F:CA*
SHA-256 Fingerprint : *9D:C9:46:CD:46:62:BE:72:B3:59:70:50:EE:3A:31:7D:83:7A:CC:7C:0F:CE:51:54:D4:68:85:E0:FE:F4:89:39*
Certificate ID : *?*
Serial Number: *49:28:FE:65:65:97:40:8D:4D:7A:24:2C:2E:91:BB:E7:FD:CB:0B:D7*
Subject: *CN = E-Tugra Domain Validated CA RSA v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.
L = Ankara
C = TR

E-Tugra Organization Validated CA RSA v3

SHA-1 Fingerprint : *C7:4A:BC:20:81:DF:CB:41:B2:EB:02:F2:DE:4E:66:95:11:D3:B6:75*
SHA-256 Fingerprint : *D4:C4:CA:F9:A1:B2:E2:0A:AF:77:E9:39:51:EF:B6:97:3A:3B:AC:9D:26:1D:67:46:AA:C4:A4:9E:07:85:AA:DD*
Certificate ID : *?*
Serial Number: *55:E1:B4:43:9D:B2:A1:B7:12:13:48:D6:35:AA:77:12:B6:DF:42:B4*
Subject: *CN = E-Tugra Organization Validated CA RSA v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.

L = Ankara
C = TR

E-Tugra Extended Validated CA RSA v3

SHA-1 Fingerprint : *58:4B:7C:19:78:87:1D:A1:AE:17:88:07:AC:64:E8:EA:D8:94:D0:EC*
SHA-256 Fingerprint : *5F:4F:81:D8:85:65:3A:50:3A:9E:4D:23:56:19:49:BE:ED:9A:5B:72:34:98:5E:EC:23:00:20:BE:3D:79:1A:81*
Certificate ID : *?*
Serial Number: *31:38:FF:98:B1:AC:CC:72:BD:FB:C6:5D:2B:D8:CB:C8:3F:35:FE:CF*
Subject: *CN = E-Tugra Extended Validated CA RSA v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.
L = Ankara
C = TR

E-Tugra Global Root CA ECC v3

SHA-1 Fingerprint: *8A:2F:AF:57:53:B1:B0:E6:A1:04:EC:5B:6A:69:71:6D:F6:1C:E2:84*
SHA-256 Fingerprint : *87:3F:46:85:FA:7F:56:36:25:25:2E:6D:36:BC:D7:F1:6F:C2:49:51:F2:64:E4:7E:1B:95:4F:49:08:CD:CA:13*
Certificate ID : *?*
Serial Number: *26:46:19:77:31:E1:4F:6F:28:36:DE:39:51:86:E6:D4:97:88:22:C1*
Subject: *CN = E-Tugra Global Root CA ECC v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.
L = Ankara
C = TR

E-Tugra Domain Validated CA ECC v3

SHA-1 Fingerprint : *72:5B:E4:A5:A6:3B:DD:FF:A6:39:86:64:59:56:1C:34:6A:3A:71:38*
SHA-256 Fingerprint : *51:10:1F:AA:96:31:29:31:9A:4A:07:75:3F:B3:BA:D3:90:1C:BA:CF:6F:19:03:9F:A0:E0:56:35:AF:AD:58:FC*
Certificate ID : *?*
Serial Number: *4F:EE:B0:CC:9B:2B:77:DB:54:20:CD:4D:64:75:09:E3:B3:B3:2A:DE*
Subject: *CN = E-Tugra Domain Validated CA ECC v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.
L = Ankara
C = TR

E-Tugra Organization Validated CA ECC v3

SHA-1 Fingerprint : *69:9B:E3:F0:5E:E6:64:58:2C:16:1F:C5:B9:D7:F7:6C:46:27:7A:5E*
SHA-256 Fingerprint : *87:EC:80:B7:06:20:53:FE:5A:CD:4A:BE:84:B0:1E:BF:34:04:A6:4C:6B:27:CE:AB:53:1E:A7:50:90:AA:43:F1*
Certificate ID : *?*
Serial Number: *15:53:3C:F8:96:7C:68:15:1E:89:AA:38:86:BF:4B:92:7E:3E:16:7E*
Subject: *CN = E-Tugra Organization Validated CA ECC v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.
L = Ankara
C = TR

E-Tugra Extended Validated CA ECC v3

SHA-1 Fingerprint : *29:57:40:15:D8:D3:F9:62:70:83:61:2B:B0:9B:9F:4C:5A:46:23:BB*
SHA-256 Fingerprint : *80:D5:4E:E5:4C:A5:64:8C:0E:A1:4F:A5:DF:95:35:CA:53:61:55:CE:90:02:67:CB:E9:AC:B3:9E:18:2E:DC:59*
Certificate ID : *?*
Serial Number: *7B:F1:81:E3:25:1F:AB:B7:4C:B8:52:A9:53:62:81:78:DD:7D:D1:94*
Subject: *CN = E-Tugra Extended Validated CA ECC v3*
OU = E-Tugra Trust Center
O = E-Tugra EBG A.S.
L = Ankara
C = TR

Version(s) of the BRs that is used.

BR version 1.5.5.

Documents that were evaluated

E-Tugra CP version 4.4 www.e-tugra.com.tr/cps
E-Tugra CPS version 4.4 www.e-tugra.com.tr/cps

Revision Dates

Publish No	Change	Date	Publisher
00	First Publish	01.04.2018	Davut Tokgöz
01	Yearly Self Check	25.01.2019	Davut Tokgöz
02	Yearly Self Check	30.01.2020	Davut Tokgöz/ Security Board
03	New Root Added	30.03.2020	Davut Tokgöz/ Security Board

BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	*E-tugra is fully compliant with all items in the table,* “	For revision that has future effective date with in new version of BR 1.5.6 “Remove validation methods #1 and #5”; e-tugra does not use these methods currently
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	E-tugra is in compliance with each of items in table of section 1.2.2	For the item that have future effective date “stop using domain validation methods BR 3,2,2,4,1 and 3,2,2,4,5” e-tugra does not use these methods currently And the CP/CPS of e-tugra is in RFC 3647 format
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*	E-Tugra has no Delegated Third-Party partner for RA or similar functions.	No implementation
2.1. Repositories *Provide the direct URLs to the CA's repositories*	CPS 2.1	www.e-tugra.com/cps (will be redirected to http://www.e-tugra.com/en-us/support/repository/certificatepolicyandpracticestatement.aspx)
2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." *--> Copy the specific text that is used into the explanation in this row. (in English)*	The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version."	

2.2 Publication of information - RFC 3647 "Effective as of 31 May 2018, the Certificate Policy and/or Certification Practice Statement MUST be structured in accordance with RFC 3647."	CPS 1	CP and CPS are structured in accordance with RFC 3647
2.2 Publication of information - CAA Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements. It shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.	CPS 4.2.2	“e-tugra.com”, “etugra.com”, “e-tugra.com.tr”, “etugra.com.tr”.
2.2. Publication of information - BR text "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." *--> Copy the specific text that is used into the explanation in this row. (in English)*	CPS 2.2	the current version of “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.6.6” which is published by CA/Browser Forum at http://www.cabforum.org for all SSL certificates

2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." *--> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.*	Test Website - Valid https://evtest.e-tugra.com.tr Test Website - Expired https://sslev.e-tugra.com.tr Test Website - Revoked https://evtest2.e-tugra.com.tr	
2.3. Time or frequency of publication *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	CP and CPS 2.3, 9.12.1, 9.12.2	"e-tugra" evaluates its Certificate Policy and Certification Practice Statement documents in accordance with related legislation and standards at least once a year in the management review meeting. Any updates in "CP" and "CPS", new versions of the documents are published in the repository along with their old versions in 7 days
2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	CP/CPS 2.4 And Internet ISMS Documents that are not publicly available	The Repository is available to the access of all concerned parties in a manner to provide service 24 hours every day. Authorized e-tuğra staff conducts regular controls to ensure the authenticity and the validity of the published information in the repository and it takes all security measure
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	For each type of certificates, how name and address are verified is considered on CPS. A detailed instructions and procedure are applied verification processes. Address information is only accepted for EV certificates
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	e-tugra verifies any DBA will be included in a Certificate using a trusted third party or government source. A DBA and Trademark are accepted for only EV certificates.

3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	e-tugra verifies it by using address of organization who requested certificate if organization name exist in certificate otherwise uses the methods described in BR to verify country code.
3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. Section 2.2 of Mozilla's Root Store Policy states: "For a certificate capable of being used for SSL-enabled servers, the CA must ensure that the applicant has registered all domain(s) referenced in the certificate or has been authorized by the domain registrant to act on their behalf. This must be done using one or more of the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.4 it is complying with. CAs are not permitted to use 3.2.2.5 (4) ("any other method") to fulfill the requirements of method 3.2.2.4.8 (IP Address)."*	CP / CPS 3.2.7 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	E-tugra implements and uses • 3.2.2.4.2 • 3.2.2.4.4 • 3.2.2.4.7 • 3.2.2.4.8
3.2.2.4.1 Validating the Applicant as a Domain Contact *For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates..*	Not implemented / not used	
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	Email to the Domain Contact by sending a Random Value through email to the Domain Contact and receiving confirmation by their use of the Random Value, performed in accordance with BR Section 3.2.2.4.2
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	

3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an e-mail created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the e-mail, and receiving a response using the Random Value, performed in accordance with BR Section 3.2.2.4.4;
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Request Value in the "/.well-known/pki-validation" directory, performed in accordance with BR Section 3.2.2.4.6;
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	DNS Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7;
3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	

3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	
3.2.2.4.11 Any Other Method "This method has been retired and MUST NOT be used."	Not implemented / not used	
3.2.2.4.12 Validating Applicant as a Domain Contact "This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name." If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs*.	Not implemented / not used	
3.2.2.4.13 Email to DNS CAA Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs*.	Not implemented / not used	
3.2.2.4.14 Email to DNS TXT Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	
3.2.2.4.15 Phone Contact with Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, *indicate how your CA meets the requirements in this section of the BRs.*	Not implemented / not used	E-Tugra does not issue certificates that includes IP address(es)
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this section of the BRs.*	CP / CPS 3.2.2 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	All methods for domain validation on section 3.2.2, are used for Wildcard Certificate Domain Name validation along with current best practice of consulting a public suffix list.
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	Internal Documents that are not publicly available • Certificate Application Verification Procedure	All data sources are defined in instructions. A governmental paper may be produced at most 6 months ago from the date of verification. Only governmental intuitions or agencies are used as trusted source. Face to face verifications for personal verification and Domain Name control verifications are defined separately.
3.2.2.8 CAs MUST check and process CAA records ~~*Indicate your CA's understanding that this section is a requirement as of September 8, 2017, and how your CA meets the requirements in this section of the BRs.*~~ Indicate how your CA meets the requirements in this section of the BRs. Section 2.2 of the BRs states: "CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue."	CP / CPS 4.2.2 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	When the application is for Standard SSL, Premium SSL, EV SSL, e-tugra shall examine the authorized CA register, CAA, according to RFC 6844, and if the CAAs are present but do not allow e-tugra to issue the certificates because it is not registered, e-tugra will not issue the certificate but will allow applicants to make another request after e-tugra has resolved the incident.
3.2.3. Authentication of Individual Identity	CP / CPS 3.2.3 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	The acceptable official documents and face to face requirements are explain in CPS and also in internal procedure in detail.

3.2.5. Validation of Authority	CP / CPS 3.2.5 And Internal Documents that are not publicly available • Certificate Application Verification Procedure	If an organization name will be used in certificates, an official document must be provided to support that the applicant has the authority to act on behalf of the legal entity.
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	CPS 3.2.6	"e-tuğra" does not make certification transactions for easing interoperability with another electronic certificate service provider
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	CPS 4.1.1 And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	"e-tugra" maintain High Risk and Black List in internal database.
4.1.2. Enrollment Process and Responsibilities	CPS 4.1.1, CPS 4.1.2 And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	Available enrolment process is defined in detailed in CPS and more detailed in internal documents.
4.2. Certificate application processing	CPS 4.2 subsections	
4.2.1 Re-use of validation information is limited to 825 days *Indicate your CA's understanding that this is a requirement as of March 1, 2018, and indicate how your CA meets the requirements of this section.*	CPS 4.2.1 And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	Re-use of validation information is limited to 825 days for Premium SSL, EV SSL CSC and EV CSC for updated CPS and internal procedures
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.*	CPS 4.2.1 And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	"e-tugra" maintain, a database and procedure for identification and requirements additional verification activity for High Risk Certificate Requests. On approving high risk domains and applications, additional cross controls are implemented.
4.2.2. Approval or Rejection of Certificate Applications "Within 30 days after ICANN has approved a new	CPS 4.2.1	Application approval conform with BR requirements

gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4. Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name."	And Internal Documents that are not publicly available • Certificate Application Acceptance Procedure • Certificate Application Verification Procedure	
4.3.1. CA Actions during Certificate Issuance	CPS 4.2.1 And Internal Documents that are not publicly available • Certificate Issue Procedure	Certificate issuance by the Root CA is not allowed for subscriber certificates.
4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	CPS 4.9.1 And Internal Documents that are not publicly available Certificate Revocation Procedure	All reasons of revocation a certificate is listed
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*	CPS 4.9.1 And Internal Documents that are not publicly available • Certificate Revocation Procedure	All reasons of revocation a certificate is listed
4.9.2. Who Can Request Revocation	CPS 4.9.1 And Internal Documents that are not publicly available • Certificate Revocation Procedure	The parties who can request certificate revocation are listed
4.9.3. Procedure for Revocation Request	CPS 4.9.1 And Internal Documents that are not publicly available Certificate Revocation Procedure Contacts are given in section CPS1.5.2	e-tuğra" gives certificate revocation service continuously on 7 days 24 hours basis via e-tuğra's website and/or call center. And CPS detailed to process

4.9.5. Time within which CA Must Process the Revocation Request	CPS 4.9.1 And Internal Documents that are not publicly available • Certificate Revocation Procedure	Upon receiving the revocation request for server certificates revocation process is completed within 24 (twenty-four) hours.
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	CPS 4.9.7	http://crl.e-tugra.com/
4.9.9. On-line Revocation/Status Checking Availability	CPS 4.9.9	Conform with BR requirements
4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.*	CPS 4.9.10	It is recommended that when inquiring the status of certificates, third parties should prefer “OCSP”. Any change on a subscriber and all other type certificate status are published to the OCSP servers automatically. “e-tugra” supports an OCSP capability using the GET method for All Certificate. The servers will not respond with a "good" status for a certificate that has not been issued.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	CPS 4.9.1	“e-tuğra” does not use any other method than “OCSP” and “CRL” for publishing revocation status.
4.10.1. Operational Characteristics	4.10.1	Revocation status information includes information on the status of certificates at least until the certificate expires.
4.10.2. Service Availability	4.10.2	Conform with BR requirements
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS		
5.2.2. Number of Individuals Required per Task	CPS 5.2.2 And Internal Documents that are not publicly available • Physical Security Procedure • Access Control Procedure	All “e-tuğra”s critical operational procedures are performed by at least two “trusted staff” in accordance with the relevant instructions. Critical operational procedures are high-security applications that require the use of cryptographic devices.
5.3.1. Qualifications, Experience, and Clearance Requirements	CPS 5.3.1 And Internal Documents that are not publicly available • Personnel Procedures	There is a special section in personal procedure for hiring a trusted staff

5.3.3. Training Requirements and Procedures	CPS 5.3.3 And Internal Documents that are not publicly available • Training Procedure, documents and records	Prior to assignment, “e-tuğra” staff receive legal and technical training in “ECSP” services, certificate life cycle management services, professional responsibilities, core public key infrastructure framework, Registration Authority and “Trust Centre” operations, “e-tuğra” security procedures, and certificate polices
5.3.4. Retraining Frequency and Requirements	CPS 5.3.3 And Internal Documents that are not publicly available • Training Procedure	“e-tuğra” staff receives updated trainings at regular intervals. The frequency and content of the trainings are subject to change in line with the organization’s performance analyses
5.3.7. Independent Contractor Controls	CPS 5.3.3 And Internal Documents that are not publicly available • Training Procedure • External Service procedures	
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	CPS 5.4.1 And Internal Documents that are not publicly available • System Log, Log Control Procedures, documents	All event logs listed on BR with description, success/failure status and date of the event as well as information about the individuals related to the event:
5.4.3. Retention Period for Audit Logs	CPS 5.4.3 And Internal Documents that are not publicly available • System Log, Log Control Procedures, documents	Once processed, audit logs are maintained in and are accessible through the system according to the data processing storage capacity at least 7 years.
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	CPS 5.4.8, CPS 8 And Internal Documents that are not publicly available • Risk Analyses and Assessments procedures • Log Control Procedures, documents	“e-tugra” executes a risk analysis and assessments actions plans and cover all related risk triggered by log monitoring systems and routines for audit log controls
5.5.2. Retention Period for Archive	CPS 5.5.2 And Internal Documents that are not publicly available • System Log Procedures, • Backup Procedures	Records pertaining to Server Certificates must be kept for a period of not less than 10 years

5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	CPS 5.7.1 And Internal Documents that are not publicly available • Business Continuity Plan • Disaster Recovery Plan • Business Continuity Management Procedures, • Emergency Plans • Backup Procedures	"e-tugra" maintains and develops business continuity with base on ISO 22301. E-tugra satisfy all requirements on BR 5.7.1
6.1.1. Key Pair Generation	* CPS 6.1.1 * Internal Documentation • Key Ceremony instructions • Certificate Issue Procedures	Root CA keys pair generation is whole complying with BR. No RA implementation Subscribers of Server Certificates are responsible from the key generation
6.1.2. Private Key Delivery to Subscriber	CPS 6.1.2	Certificate application owners who will apply for Standard SSL, Premium SSL, EV SSL, CSC and EV CSC are responsible for a secure key generation during application.
6.1.5. Key Sizes	CPS 6.1.5	"e-tuğra"s root certificates are issued by the use of 4096 bit RSA and intermediate certificates are issued by the use of 2048 bit RSA key pair. For certificates of Standard SSL, Premium SSL, EV SSL and "CSC" issued by e-tuğra 2048-bit RSA key pair is used.
6.1.6. Public Key Parameters Generation and Quality Checking	CPS 6.1.6	"e-tuğra" checks and verifies the validity of CSR file sent by the server Certificate applicant according to key length and other parameters. "e-tugra" controls received CSR file and rejects if signs with weak private key.
6.1.7. Key Usage Purposes	CPS 6.1.7	Key Usage purpose are defined for roots, subordinate CAs and subscribers conform with BR requirements
6.2. Private Key Protection and Cryptographic Module Engineering Controls	CPS 6.2 and all sub sections	
6.2.5. Private Key Archival	CPS 6.2.5	E-tugra does not kept and archive any private key of certificate

6.2.6. Private Key Transfer into or from a Cryptographic Module	CPS 6.2.6 • Internal backup procedures	Private keys of subordinates are transferred for only backup purposes.
6.2.7. Private Key Storage on Cryptographic Module		
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	CPS 6.3.2	The CPS is adopted to the requirements and certificate issuing systems are modified for this validity period limit
6.5.1. Specific Computer Security Technical Requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance. *Indicate how your CA meets the requirements of this section.*	CPS 6.5.1	"e-tugra" enforces multi-factor authentication on any account capable of directly causing Certificate issuance. E-Tugra uses smartcards and PINS on authentications fort his kind of accounts
7.1. Certificate profile CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG. *Indicate how your CA meets the requirements of this section.*	CPS 7.1	İt is implemented by 16th April, 2018 In March 2019, It was updated to 80bit.
7.1.1. Version Number(s)	CPS 7.1.1	Certificates are type X.509 v3
7.1.2. Certificate Content and Extensions; Application of RFC 5280	CPS 7.1.2	Requirements of BR is satisfied
7.1.2.1 Root CA Certificate	CPS 7.1.2.1	Requirements of BR is satisfied
7.1.2.2 Subordinate CA Certificate	CPS 7.1.2.2	Requirements of BR is satisfied
7.1.2.3 Subscriber Certificate	CPS 7.1.2.3	Requirements of BR is satisfied
7.1.2.4 All Certificates	CPS 7.1.2.4	Requirements of BR is satisfied
7.1.2.5 Application of RFC 5280	CPS 7.1.2.4	Requirements of BR is satisfied
7.1.3. Algorithm Object Identifiers	CPS 7.1.3	Requirements of BR is satisfied
7.1.4. Name Forms	CPS 7.1.4	Requirements of BR is satisfied
7.1.4.1 Issuer Information	CPS 7.1.4	Requirements of BR is satisfied
7.1.4.2 Subject Information - Subscriber Certificates	CPS 7.1.4	Requirements of BR is satisfied
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	CPS 7.1.4	Requirements of BR is satisfied

7.1.5. Name Constraints *Indicate your CA's understanding of Mozilla's requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section.*	CPS 7.1.5	E-tugra understands of Mozilla's requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section. Current subordinates CAs for Standard SSL, Premium SSL, EV SSL, CSC and EV CSC have no name constraints defined in Baseline Requirements.
7.1.6. Certificate Policy Object Identifier	CPS 7.1.6 CPS 1.2	The relevant certificate policy object identifier numbers (OID) indicated in Section 1.2
7.1.6.1 Reserved Certificate Policy Identifiers	CPS 7.1.6	e-tugra comply with Baseline Requirements section 7.1.6.
7.1.6.2 Root CA Certificates	CPS 7.1.6	e-tugra comply with Baseline Requirements section 7.1.6.
7.1.6.3 Subordinate CA Certificates	CPS 7.1.6	e-tugra comply with Baseline Requirements section 7.1.6.
7.1.6.4 Subscriber Certificates	CPS 7.1.6	e-tugra comply with Baseline Requirements section 7.1.6.
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	CPS 8. And subsections	
8.1. Frequency or circumstances of assessment The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	* CPS 8.1 * Internal Audit / External Audit procedures and sub documents	E-tugra understand the requirements. Pursuant to the ETSI EN 319 411-1 audit standard, standard SSL, Premium SSL, EV SSL, CSC and EV CSC services are subject to full audits on an annual.
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	CPS 8.2	For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403 E-Tugra works with LSTI currently.

8.4. Topics covered by assessment	* CPS 8.4 And Internal (Audit Procedures and sub documents)	The ETSI EN 319 411-1 audit covers standard all processes related to standard SSL, premium SSL, EV SSL, CSC and EV CSC services as well as the technical infrastructure and facilities used to deliver these services.
8.6. Communication of results	CPS 8.6	On an annual basis, e-tugra submits copies of audit compliance reports to Mozilla via CCADB

Also indicate your understanding and compliance with Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers). "		E-Tugra Comply with Mozilla's Root Store Policy
8.7. Self-Audits	CPS 8.7 And Internal Documents • Internal Audit / External Audit procedures and sub documents	Regular internal audits for validations are performed against randomly selected sample of at least three percent of its server and code signing Certificates Certificate types certificates issued since the last on quarterly basis

9.6.1. CA Representations and Warranties	* CPS 9.6.1 and CPS with all section * E-Tugra SSL Warranty Documents on Repository * Certificate Application Forms (includes warranties, Subscriber agreements)	All CA Warranties are described in mentioned documents for subscriber, application software suppliers and Relying parties. According to BR 9.6.1
9.6.3. Subscriber Representations and Warranties	* CPS 9.6.3 * Certificate Application Forms (includes warranties, Subscriber agreements)	Subscriber Warranties are described in mentioned documents for subscriber, application software suppliers and Relying parties. According to BR 9.6.3
9.8. Limitations of liability	CPS 9.8 * E-Tugra SSL Warranty Documents on Repository	Limitation of liabilities are described with maximum limit and total cost are mentioned in CPS 9.8 and SSL warranty documents
9.9.1. Indemnification by CAs	CPS 9.9	Indemnification by E-tugra is explained in section for Application software's vendors on EV certificates
9.16.3. Severability	CPS 9.16.3	Where any section of the "CPS" is deemed or becomes invalid permanently or temporarily, the other sections that are not affected from such section shall remain in force.