EBG INFORMATIC TECHNOLOGIES AND SERVICES CORP (E-TUGRA)

NON QUALIFIED CERTIFICATE POLICY AND PRACTICE STATEMENT (CP-CPS)

VERSION 1.1

DATE OF ENTRY INTO FORCE : JULY, 2009

OID

2.16.792.3.0.4.1.1.6

EBG Informatic Technologies and Services Corporation

Tel: +90-312-472 21 13

www.e-tugra.com.tr

"E-Tugra" Certificate Practice Statement for NQC Certificates

Explanation and Legal Notice

CONTENTS

9.5 Intellectual Property Rights

9.6 Obligations and Warranties

9.6.1 "CSP" Obligations and Warranties

9.6.2 "RA" Obligations and Warranties

9.6.3 Obligations and Warranties of "NQC" Holders and Corporate Applicants

9.6.4 Obligations and Warranties of Third Parties

9.6.5 Obligations and Warranties of Other Parties

9.7 Warranty Waivers

9.8 Limitation of "CSP" Obligations

9.9 Compensations

9.10 Validity and Expiry of "CPS"

9.10.1 Validity

9.10.2 Expiry

9.10.3 Effects of Expiry

9.11 Individual Notifications and Communication Between the Parties

9.12 Changes

9.12.1 Change Procedures

9.12.2 Notification Mechanism and Period

9.12.2.1 Articles Which Can Be Changed Without Notification

9.12.2.2 Articles Which Can Be Changed Subject to Notification

9.12.3 Changes Requiring Modification to Principles of Certificate Identifier (OID) or "CPS" Mark

9.13 Settlement of Disputes

9.14 Applicable Law

9.15 Compliance with Legislation

9.16 Miscellaneous Provisions

9.16.1 Entirety of the Contract

9.16.2 Transfer and Assignment

9.16.3 Divisibility

9.16.4 Sanctions (Attorney's fees and waiver of rights)

9.16.5 Force majeure

9.16.6 Other Provisions

1. Introduction

EBG Bilişim Teknolojileri ve Hizmetleri AŞ (EBG Informatic Technologies and Services Corp.) (to be referred to as "E-TUGRA" hereafter) is a joint stock company (AŞ), which is incorporated and presently continues operations in compliance with the Turkish Commercial Code. It has obtained the right and powers of providing services related to electronic signatures, electronic certificates both QC and NQC and time stamps in its capacity as an Electronic Certificate Services Provider (to be referred to as "CSP" hereafter) after it has made a notification to the Telecommunication Agency and met the regal requirements in accordance with Article 8 of Law No 5070 on Electronic Signatures.

This document titled Certificate Practice Statement (to be referred to as "CPS" hereafter) has been prepared for the purpose of explaining and making public the technical and legal requirements met by E-TUGRA in its capacity as an "CSP" pursuant to the CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures operations by "CSP" and its technical and organizational structure and Obligations of the parties assuming certain roles in connection with services provided by "CSP".

This document has been prepared in compliance with the standards of CWA 14167-1 and IETF RFC 3647.

General

Electronic Certificate Services Providers are the natural persons and legal entities which provide services related to time stamps and electronic signatures.

E-TUGRA publicly discloses and brings to the attention of the parties concerned the features of "NQC's" created by it and considerations governing their use, certification processes, rights and obligations of the parties taking part in the certification process and technical and operation activities it carries out in its capacity as "CSP" under Document on the Certificate policy ("CP". In addition, E-TUGRA outlines how the aspects covered by Document "CP" are implemented in the document titled "Certification Implementation Principles" (to be referred to as "CPS" hereafter) and it also brings this document to the attention of the public and concerned parties.

E-TUGRA has developed its own certification policies in accordance with the "NonQualified Certificate requirements specified by CWA 14167-1 in accordance with [Dir.1999/93/EC] and it has published its "CP" document in line with that.

E-TUGRA issues the following NQC Certificate types:

- NQC's for Client Authentication (SSL Client)
- NQC's for E-mail Protection
- NQC's for Server Authentication (SSL Server)
- NQC's for Code Signing

NQC's issued for Client Authentication and E-mail Protection purposes, are subjected to the same procedural requirements and the same level of security that the QC certificates posses. NQC's for Client Authentication and E-mail Protection are only issued together with QC certificates in the same SSCD at the same time and they are not issued as standalone certificates without a SSCD. As per CWA 14167-1 meeting the requirements for issuing of QCs automatically implies meeting the requirements for issuing NQCs. Please refer to E-TUGRA QC CPS http://www.e-tugra.com.tr/BilgiDeposu/ApplicationFormsCPandCPS/tabid/617/Default.aspx for NQC's for Client Authentication and E-mail Protection. This CPS applies to NQC's for Server Authentication (SSL Server) and NQC's for Code Signing.

Definition

Identifiers for Non-Qualified Electronic Certificate Practice Statement

E-TUGRA Certificate Practice Statement Version 1.1

Object Identifier: ***2.16.792.3.0.4.1.1.6***

Identifier for Certificate Policy:

E-TUGRA Certificate Policy Version 1.0

Object Identifier: ***2.16.792.3.0.4.1.1.5***

Parties

The subjects defined as Parties under "CP" are the parties, which take part in E-TUGRA operations of "CSP" and hold rights and obligations with regard to such operations. The

Parties under "CP" are: E-TUGRA, registration Authorities, individual and corporate NQC applicants, NQC holders and third Parties.

Electronic Certificate Service Provider - "CSP" ("E-TUGRA")

E-TUGRA is an "CSP" for which rights and obligations are established in line with the present CP and "CPS" pursuant to CWA 14167-1 and the applicable legislation as part of "CSP" operations. NQC's created by E-TUGRA are signed by the E-TUGRA "CSP" Intermediate CA; in turn, E-TUGRA "CSP" Intermediate CA is signed by E-TUGRA Root CA.

Registration Authorities

Registration Authorities (to be referred to as "RA" hereafter) are the residential structures which perform services related to NQC applications, Revocation and renewal requests and are under direct E-TUGRA control and inspection and staff E-TUGRA affiliated staff employed directly or on contract / outsourcing within these residential structures or natural persons and/or legal entities which conclude Registration Unit Contracts with E-TUGRA. RA's the ID's of persons applying for NQC on the basis of documents established by E-TUGRA as well as the validity of the information to be incorporated in NQC. In addition, RA's can also assume responsibilities for receiving applications for operations to be carried out between "Certificate Holders" and E-TUGRA throughout the certificate life cycle and performing necessary operations for and on behalf of E-TUGRA. Further, RA's also ensure that application procedures related to NQC applications are handled in line with their work instructions.

NQC applications to be made via RA's can be either web based or based on the direct visit by the applicants to RA office for a physical application there and delivery to RA office officials of necessary information and documents. RA's are issued a photographed RA Operator card by E-TUGRA and prior to proceeding with any operations involving NQC applicants, RA's present their authorization cards issued by E-TUGRA for them to NQC applicants.

E-TUGRA makes public the addresses of residential RA offices and contact information on its Web site.

NQC Applicants / NQC Holders, Corporate Applicants

NQC Holders are the legal entities, which have met the requirements set forth by CPS and CP made public by E-TUGRA, NQC Application Form concluded with NQC Holders and the conditions specified by E-TUGRA and for which NQC's are created. NQC applications can be made in two manners: individual applications and corporate applications.

Individual applicants are the natural persons which apply for NQC for themselves and sign NQC Application Forms with E-TUGRA after having met the required procedures.

Corporate applicants are the legal entities, which apply for NQC for and on behalf of its employees or customers or members or shareholders and sign NQC Application Forms with E-TUGRA after having met the required procedures.

Third Parties

Third Parties are those persons, who conduct business and make transactions by relying on the data signed by the secure electronic signatures after establishment of the ID particulars of persons signing the data signed by secure electronic signatures by using NQC's upon the fulfillment of validity controls for NQC's and E-TUGRA root and Intermediate certificates as well as for E-Tugra time stamps or upon the fulfillment of verification operation by making use of a secure electronic signature verification tool. NQC holders act as third Parties in case they directly fulfill the verification processes mentioned above.

Other Parties

"Trust Center"

"Trust Center" is E-TUGRA Center where it performs all the certificate life cycle operations, it establishes and operates the certificate authority technical infrastructure and it meets all the necessary physical and technical security requirements. "Trust Center" holds ISO/IEC 27001 Security Certificate and it carries out all of its operations in compliance with CWA 14167-1.

Use of Certificates

Use of Authorized Certificates

E-TUGRA root and Intermediate certificates can only be used for NQC signing, CRL signing and signing of OCSP and time stamp certificates as well as in the processes of verification of subject certificates and data.

NQC's created by E-TUGRA can only be used strictly as part of the processes of developing and verifying secure electronic signatures in the framework of the limitations incorporated in the certificates concerning usage and material scope in accordance with the NQC Application form. At the same time, NQC's can also be used by third Parties for purposes of validating effectiveness of certificates and having access to the certificate contents.

Use of Banned Certificates

It is prohibited to use NQC's and root and Intermediate certificates created by E-TUGRA in the areas other than those listed by CP 1.4.1. As per Article 5 of the Electronic Signatures Law, "any legal actions and guarantee contracts subjected by laws to official methods or particular ceremonies" cannot be concluded by using secure electronic signatures. Therefore, it is prohibited to conclude the subject actions by means of secure electronic signatures and use NQC's in the processes of developing and verifying secure electronic signatures for such actions.

Policy Management

Authorized Organization Over "CPS"

E-TUGRA staff, who is specifically authorized by E-TUGRA is responsible for publication, revision and renewal of Document CP as well as for all the other operations related to this document.

Liaison Official

Forward your questions on "CPS" to the following address:
Ceyhun Atuf Kansu Cad. No : 130/58 Balgat - Ankara / TÜRKİYE
Tel : +90 312 4722113
e-mail : info@e-tugra.com.tr

Person Establishing Compliance With the Policy

Authorized E-TUGRA Auditor staff inspects compliance of CP with document CPS and E-TUGRA "CSP" processes of operation.

Procedure for Approval of CPS

E-TUGRA officials continuously conduct inspection on Document CPS and E-TUGRA "CSP" processes of operation. CPS is subject to revision or renewal in line with the outputs of inspection and / or any changes to the processes of operation. Any changes to CPS or any new versions are presented to E-TUGRA staff for approval.

Definitions and Abbreviations

CONCEPT / ABBREVIATION	EXPLANATION / DEFINITION
"Application Methods"	Methods comprising of technical and administrative processes by which an application is made by NQC Applicants to "CSP", necessary documents are drawn up, certificate charges are paid, documents are retained, Non-Qualified electronic certificates are issued and forwarded to certificate owners and aspects such as the procedures over the communication of requests for Revocation, renewal and suspension of certificates. These methods are available at www.e-tugra.com.tr .
"Individual Applicants"	They are the natural persons, which apply for NQC for themselves directly and signed NQC Application Forms with E-TUGRA by meeting the required procedures.
"CEN"	Comitee Europeen de Normalisation - European

	Standardization Committee
"CWA"	CEN Workshop Agreement
"OCSP"	Online Certificate Status Protocol
"EAL"	Evaluation Assurance Level
"E-TUGRA"	EBG Bilişim Teknolojileri ve Hizmetleri AŞ (EBG Informatic Technologies and Services Corp.)
"Electronic Signatures Law"	Law No 5070 on Electronic Signatures, which was issued in the Official Journal Issue No 25355 of January 23, 2004
"CSP"	Electronic Certificate Service Provider
"ETSI"	European Telecommunication Standardization Institute
"ETSI TS"	ETSI Technical Specifications
"Secure Electronic Signature"	Secure electronic signature is an electronic signature; a) Which is exclusively owned by its holder, b) Which is created only by the secure electronic Signature Creation tool solely available to the signature owner, c) Which provides establishment of the ID of the signature owner on the basis of Non-Qualified electronic certificate, d) Which provides determination if any changes have later been made to the signed electronic data.
"Secure Electronic Signature Verification Tool"	Secure electronic signature verification tools are CWA 14171 standard compliant signature verification tools: a) Which show the data used for verification of signature to the person performing validation without hanging them, b) Which activate the signature validation operation in a reliable and definite manner and show the validation results to the person performing validation without changing them, c) Which provide viewing of the signed data in a reliable manner when required, d) Which establish the correctness and validity of electronic certificates used for verification of signatures in a reliable manner and show the results thereof to the persons performing validation without changing them, e) Which show the ID of the signature owner to the person performing validation without making any changes, f) Which provide establishment of any changes which

	will affect the conditions related to the verification of signatures.
"Secure Electronic Signature Creation Tool"	Secure electronic Signature Creation tools are the tools at the level of minimum EAL4+ according to ISO / IEC 15408 (-1, -2 and -3) which ensure: a) That the electronic Signature Creation data they produce are unique, b) That the electronic signature formation data recorded on them are never taken out of the tools and that their confidentiality is maintained, c) That the electronic signature formation data recorded on them cannot be retrieved and used by third Parties and that they are protected against electronic signature fraudulency, d) That the data to be signed cannot be changed by any persons other than the signature owners and that such data can be viewed by the signature owners prior to development of signatures.
"Secure e-signature package"	A whole of services and equipment provided by "CSP" to Certificate Users, which comprises of Non-Qualified electronic certificates and secure electronic Signature Creation tools as a minimum. Detailed information is available at www.e-tugra.com.tr on the prices of "Secure e-signature Package" and the equipment and services contained.
"IETF RFC"	Internet Engineering Task Force Request for Comments
"ISO / IEC"	International Organization for Standardization / International Electromechanical Committee
"Registration Unit"	Authorized "CSP" Unit, which operates under "CSP" and receives NQC applications by Certificate Users and Corporate Applicants.
"ID Information"	Name and Surname, ID No Applicable In Turkey, date and place of birth and nationality of Certificate User
"Corporate Application"	Application made by a legal entity for Non-Qualified electronic certificates for its employees or customers or members or shareholders
"Corporate Applicant"	Legal entity with which a Corporate Application Contract is

	concluded with "CSP" and which applies for Non-Qualified electronic certificates for its employees or customers or members or shareholders pursuant to Articles 3 and 9 of the Regulation.
"Corporate Application Officer"	An employee of the Corporate Applicant, who determine NQC the information to be notified to "CSP" for issue of NQC for Certificate User by relying on the documents indicated by Article 9/1 of the Regulation and fulfills the operations indicated for performance by him / her as part of the "Corporate Application Contract" for and on behalf of the Corporate Applicant.
"NQC"	Non-Qualified Electronic Certificate
NQC Applicant	Person who submits individual or corporate application to "CSP"
"Non-Qualified Electronic Certificate"	Electronic Signatures, meeting [Dir.1999/93/EC], Article 5.2 as per CWA 14167-1
"OID"	Object Identifier
"CP"	Certificate policy
"Certificate policy"	Rules as a whole which designate the acceptability of certificates in view of implementations which are a certain gathering of security requirements and/or a group of general requirements are called "Certificate policy". "Certificate policy" are a document made public by electronic certificate service providers, which aim at meeting the objectives outlined above. Certificate users have to comply with CP published by "CSP". CP including any changes thereto which may be introduced from time to time is available on "CSP" web site.
"CRL"	Certificate Revocation List
"Certificate user"	Natural person for whom NQC is issued by "CSP". "Certificate Holder" and NQC Holder used in this document have a synonymous meaning.
"SSCD"	Secure Signature Creation Device
"CPS"	Certificate Practice Statement
"Certificate Practice Statement "	It is a public statement made by "CSP", which is periodically updated, whereby the requirements which have to be met by each party defined as part of CPS, particularly

	Certificate Users, in order to achieve designated operations and whereby implementations and procedures are elaborated. CPS including any changes that may be made thereto periodically is available on "CSP" web site.
"Communique"	"Communique on the Processes and Technical Criteria Applicable for Electronic Signatures", which was promulgated in the Official Journal Issue No 25692 of January 6, 2005.
"TC"	Republic of Turkey
"Regulation"	"Regulation on the Procedures and Principles Applicable for Implementation of the Electronic Signatures Law", which was issued in the Official Journal Issue No 25692 of January 6, 2005.

2. Publication and Repository Obligations

Repository

E-TUGRA publishes NQC's, CRL's, Documents CPS and CP it develops and the contracts, informative documents and relevant audio and visual publications it uses as part of "CSP" operations on the Directory. The Directory is made available for access by NQC holders, third Parties and any other interested persons in a manner to provide service on the basis of 24 hours every day.

Publication of Certificate Data

E-TUGRA publishes the following on the address, http://www.e-tugra.com.tr/BilgiDeposu/ETugraSertifikalar%C4%B1ve%C4%B0ptalListeleri/ETugraSertifikalar%C4%B1/tabid/526/Default.aspx for the Directory:

- E-TUGRA Root Certificates
- E-TUGRA Intermediate Certificates
- E-TUGRA Time Stamp Certificates
- E-TUGRA "OCSP" Certificates
- E-TUGRA CP and CPS

- E-TUGRA QC Application Forms
- E-TUGRA NQC Application Forms
- Corporate Application Contracts
- Documents related to NQC applications
- Informative documents and relevant audio and visual publications

Publication Frequency

Any updates in CPS and CP as well as any new versions thereto and amendments to the contracts are published as per CP 9.12. NQC's and E-TUGRA Root and Intermediate Certificates are issued on the date of arrangement thereof. Certificate status information is issued as per CP 4.9.7 and CP 4.9.10.

Repository Access Controls

The Repository is made available for access in a manner to provide service 24 hours every day. Authorized E-TUGRA staff conducts regular controls as to the currency and correctness of the information in the Directory.

3. Identification and Authentication

Prior to provision of NQC's to the applicants, E-TUGRA verifies the ID particulars of the applicants, information to be incorporated in the certificates and its authorities for use of NQC depending on official records.

Name Assignment (Initial Registration)

Types of Names

Only those types of Names supported by ITU X.500 format are used in the "DN" field in NQC's.

Requirement that Names Be Meaningful

The name of NQC holder on NQC's is same as the name indicated in the official documents submitted during Authentication. E-TUGRA Root and Intermediate Certificates contain a note and commercial title indicating that E-TUGRA is "CSP".

Concealment of Persons Applying for "NQC" or Use of Nicknames

According to the Law, it is prohibited to use nicknames in NQC's and/or for NQC holders to conceal their names.

Rules for Interpretation of Different Types of Names

Not applicable.

Uniqueness of Names

E-TUGRA ensures that the ID particulars pertaining to different persons are unique in NQC's. This uniqueness in NQC's is achieved by using the ID Numbers in the Republic of Turkey in the case of Turkish citizens and passport numbers in the case of those with foreign nationalities. In case any NQC holder has more than one NQC, it is then allowed that his / her ID particulars are same in NQC's.

Identification, Verification and Role of Trade Marks

It is prohibited for NQC applicants to use any Names infringing others' intellectual property rights during their individual or corporate applications.

Initial Authentication

Method for Proving the Possession of Signature Creation Data

As part of the operation of E-TUGRA "CSP", signature creation and verification data are created only by "CSP". Therefore, it is recognized that NQC holder is in possession of the signature

creation device in case NQC and secure electronic signature creation device are delivered to NQC holder against receipt of a signature.

Verification of the ID's of the Legal Entities

The ID of the relevant legal entity is verified on the basis of official documents (confirmed by notary, legal adviser, court or government institution) in case it is intended to put information on the authorization as part of corporate applications and/or in NQC on behalf of the relevant legal entity.

Verification of the ID's of the Natural Persons

In the case of individual and corporate applications, the ID of a natural person is verified by at least two copies of photographed and valid documents such as ID cards, passports and driving licenses. In Turkey validation of documents and verification of ID also can be made by face to face validation. In case if face to face validation is not possible, all submitted official documents should be confirmed by notary, legal adviser, court or government institution.

Required documents for verification

- Copy of ID document of a person responsible for the certification procedure (ID card, passport, residence permit, student's ID card, social insurance ID, etc.) to check the data given in a form filled in on a website
- Document to assure the person responsible for certification procedure is an employee or representative of company/institution
- Document to verify company/institution authenticity, e.g.:
    - DUNS number (Dun and Bradstreet)
    - Articles of Incorporation
    - Business License
    - Doing Business As (DBA) registration
    - Partnership documentation
    - Sole Proprietorship documentation
    - Factitious Name Statement
    - Assumed Name Statement
    - Seller's Permit
    - Occupational License
    - Sales Permit

- If certificate should be issued for other institution then original domain owner - copy of the document to assure right to use the domain

All international documents delivered by post must be officially confirmed (by notary, legal adviser, court or government institution) and signed by official representative. All delivered documents must be signed by official representative. Delivered documents must be in English or must be translated into English by sworn translator or certified by a notary.

Authenticity of submitted documents:

To confirm the authenticity of the submitted documents, the E-Tugra will call or send a copy of the documents back to the Third-Party Validator at the address, phone number, facsimile, to obtain confirmation from the Third-Party Validator for authenticity of submitted documents.

Verification of Third-Party Validator:

E-Tugra independently verifies that the Third-Party Validator is a legally-qualified Latin Notary or Turkish Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency, by directly contacting the authority responsible for registering or licensing such Third-Party Validator in the applicable jurisdiction.

Verification of the e-mail addresses of the Natural Persons and Legal Entities

In the case of individual and corporate applications, if the application includes e-mail protection then the e-mail address of the applicant is verified by means of an e-mail authentication and a secret question challenge. This is done by sending an e-mail to the proclaimed e-mail address which includes a challenge question which is already obtained from the NQC application form. In case a reply from the applicants proclaimed e-mail address is received and the answer to the challenge question is correct, then the verification process is successfully completed. The application failing from either of the two challenges described above is denied.

Validation of the Domain Names of the Natural Persons and Legal Entities

In the case of individual and corporate applications, if the application is for a Secure Web Server Certificate, the domain name for the application is verified. The Turkish domains which ends with .tr extension are queried from the Turkish domain names legal registrar address https://www.nic.tr/. In case the domain is a foreign domain, then the query is made in WHOIS

database to check the conformity with data given in order. If the WHOIS results do not match the information for the SSL certificate that you wish to order then applicant has to update the WHOIS information as required. E-Tugra sends metatag to be placed on the server and verifies it's presence in order to verify that if person has Access to the server with domain for requested certificate.

Unverified Application Information

It is not necessary for E-TUGRA to verify information other than those covered by NQC about NQC Holders.

Proving the Relationship of NQC Holder with The Organizations With Which He / She Is Affiliated

The ID of the relevant legal entity is verified on the basis of official documents in case it is intended to put information on the authorization as part of corporate applications and/or in NQC on behalf of the relevant legal entity.

Interoperability criteria

Not applicable.

Identification and Authentication for Re-keying

Identification and Authentication for Routine Re-keying

No re-keying is performed for NQC's as part of the operation of E-TUGRA "CSP"; Renewal is available before the expiry of NQC validity term. Renewal requests can be made via www.e-tugra.com.tr web site or via RA's. In case a renewal request is made via the web site, the form for renewal of NQC is completed, with necessary information being furnished. E-TUGRA performs verification of the ID of NQC Holder by making use of dual level identification methods. In the case of applications made to RA, RA performs verification of the ID of NQC Holder on the basis of official documents such as an ID Card, passport and driving license.

Identification and Authentication for Re-keying After Revocation of Certificate

No re-keying is performed after Revocation of NQC and the request for re-keying is treated as a new NQC application and all the procedures related to NQC application
apply.

Identification and Authentication for Request of Revocation

NQC's can be revoked by NQC Holders and also by corporate applicants and third persons if NQC Holders specifically permits this. In case the conditions laid down by CP realize, E-TUGRA can also cancel NQC on his own discretion. NQC Revocation and suspension operations can be conducted via E-TUGRA Call Center, Internet site on www.e-tugra.com.tr or application to RA's. When E-TUGRA receives a request for Revocation from the concerned parties, it verifies the ID of the person requesting for such a Revocation and his / her authority to make a request for a Revocation by means of the information received during NQC application and also passwords.

4. Certificate Life Cycle Operational Requirements

NQC applications

Who can apply for NQC applications?

Natural persons and legal entities, who will apply for corporate applications on behalf of their employees, customers, members or shareholders and have met the procedures designated by E-TUGRA can apply for NQC.

Registration Process and Obligations

NQC applications can be made by means of various Application Methods as part of the operation of E-TUGRA "CSP". Depending on the applicants, NQC applications are classified into two groups as individual applications and corporate applications.

Individual applications

Individual applications refer to NQC applications by NQC Holders in person directly in their names. E-TUGRA may envisage various models and requirements in connection with individual applications as part of "Application Methods". Any individual applications to be made to E-TUGRA can be made by following two methods basically.

Individual applications via RA

Individual applicant can directly visit RA in person to make an NQC application so that he can apply for NQC. During NQC application, RA official verifies the ID of the applicant on the basis of at least two official and photographed documents such as ID cards, passports or driving licenses. In the meantime, individual applicant fills out and signs the NQC application form. The individual applicant delivers to the RA official a copy of the contract he signs, the application form completed and other required documents, which are specified on the address, www.e-tugra.com.tr

Online Individual Applications

Individual applicants can make a preliminary application by completing the Certificate Application Form available on the web address, www.e-tugra.com.tr . After completion of the procedures on the Web, the individual applicant then gets printouts of the contract and application form and completes and signs them. After completion of the online application procedures, the individual applicant is then required to receive a declaration of signature issued by a notary public for him. Then, the individual applicant sends the following to relevant E-TUGRA unit by certified mail or courier: the notarized declaration of signature, "CSP" copies of the NQC application form just completed and signed and any other required documents specified on the address, www.e-tugra.com.tr . Individual applicant is deemed to have made an application for NQC upon the arrival of the package at E-TUGRA.

Corporate Applications

Corporate application refers to an application made by a legal entity for its employees or customers or members or shareholders. In the case of corporate applications, the corporate

applicant appoints a member of its staff, who presently has an employment contract with the Corporate Applicant and will meet the obligations it has assumed as per the Corporate Application Contract concluded with E-TUGRA on its behalf. Under E-TUGRA work model, a corporate application can be made through a single application method. The operation of this basic application method designated by E-TUGRA is as follows:

Corporate Application Via RA

Corporate applicant first signs the printed Corporate Application Contract, which is published on E-TUGRA web site or available from any RA's. Appointing a Corporate Application Official simultaneously with the signing of the Corporate Application Contract, the Corporate Applicant then ensures that the Obligations imposed on it as part of the Corporate Application Contract are carried out by the Corporate Application Official on its own behalf. The corporate applicant completes and signs the Corporate Application Form which is attached to the Corporate Application Contract. In the Corporate Application Form, the Corporate Applicant specifies the minimum number of Corporate Applications to be made throughout the term of the Corporate Application Contract, the powers conferred on the Corporate Application Official and that person's detailed ID and contract information and any other necessary information on the legal entity, which is the Corporate Applicant. The Corporate Applicant ensures that the Certificate User Declaration of Commitment, which is an annex to the Corporate Application Contract also containing the requirements that NQC applications by the Corporate Applicant are documented in writing as per Article 9.2 of the Regulation is signed by Certificate User, delivering one copy thereof to the Certificate User. The Corporate Applicant makes a Corporate Application by delivering to RA official the "CSP" copies of Certificate User Declarations of Commitments, Corporate Application Contract and annexes to it and any other required documents, which are requested during application and are communicated on the address, www.e-tugra.com.tr . RA verifies the powers of the Corporate Application Official on the basis of the Corporate Application Form and Corporate Application Contract signed by the Corporate Applicant, the ID particulars of the Corporate Application Official on the basis of the photocopies of the ID card, passport and driving license of the Corporate Application Official and the powers and ID particulars of the Corporate Applicant on the basis of the circular of signature of the Corporate Applicant, Corporate Application Contract and Certificate User Declaration/s of Commitment. In cases involving "corporate applications" for more than 10 (ten) Certificate Holders at one time, RA or RA official assists with the performance of necessary application procedures under the

supervision of the Corporate Applicant. The request by the Corporate Applicant for assistance by RA or RA official with the registration process under its supervision is met by calling E-TUGRA Call Center.

NQC Application Process

Identification and ID Evidence Functions

RA officials perform Authentication for NQC Holders, corporate applicants and corporate application officials by means of the methods prescribed by CP 3.2 and CP 4.1.

Acceptance and Rejection of NQC Applications

The concerned parties are notified of the results of their applications within the time limit set by CP 4.2.3 upon examination by E-TUGRA of NQC applications made in the framework of the processes determined by CPS, CP, NQC Application Forms and E-TUGRA in view of their compliance with the subject documents and processes. E-TUGRA is free to accept and/or reject any applications received by it. If E-TUGRA rejection of an application is based on such considerations as omission of documents, typing errors, etc., which can be completed by applicant in a certain period of time, E-TUGRA then grants the applicant a final deadline for completion of such omissions. In case NQC applicant completes such omissions in the final deadline granted, NQC application is then accepted and this acceptance is notified to the applicant and other concerned parties as per CP 4.2.3. Otherwise, the application by NQC applicant is rejected and this situation is again notified to the applicant and other concerned parties as per CP 4.2.3.

Timing of NQC Application Process

NQC applications made within the processes determined by CPS, CP, NQC Application Forms and E-TUGRA are evaluated by E-TUGRA and the result of an application is notified to the Certificate Holder and/or Corporate Applicant by phone from E-TUGRA Call Center Official or by an electronic letter bearing the secure electronic signature to be sent to the electronic mail address of the Certificate User and Corporate Application Official within 15 (fifteen) business days.

Creation of NQC

"CSP" Operations During the Creation of NQC

After acceptance of the application following completion of the application processes defined by CP 4.2, signature creation and verification data are created by E-TUGRA Secure Staff within the "Trust Center in the secure electronic signature creation device belonging to the certificate owner in accordance with the algorithms and parameters indicated by the CWA 14167-1 and upon the creation of the signature and verification data, NQC connected with the electronic signature verification data pertaining to the certificate holder is created in line with the information received from NQC applicant and/or corporate applicant. "Secure e-signature Package", which comprises of NQC created by E-TUGRA and the secure electronic device creation device on which signature creation and verification data are loaded is delivered only to the certificate owner in a location designated by the individual applicant or corporate applicant upon control of ID and receipt of a signature thereof.

4.3.2 Notification by "CSP" Creating Certificates to the Person Applying for NQC

NQC Holder in the case of individual applications and NQC Holder and Corporate Application Official in the care of corporate applications are informed of the status of the application by e-mail or phone.

4.4 Acceptance of NQC

4.4.1 Operations Deemed Acceptance of NQC

Acceptance by the Certificate Holder of the Secure e-Signature Package, which is created by E-TUGRA and comprises of the secure electronic signature creation device in which the signature creation and verification data are uploaded is deemed acceptance of NQC. After acceptance of the Secure e-signature Package, Certificate User will immediately check if the equipment inside the package are complete and in an operating condition. If the Certificate User finds out that the equipment inside the Secure e-signature Package are incomplete and not in an operating condition having defects, he will call "CSP" Call Center informing of this situation within 7

(seven) business days. After receipt of the Secure e-signature Package, the Certificate User will immediately make installation of the secure electronic signature creation device and check the data inside NQC in the device. In case the Certificate User finds out that there is difference between the data inside NQC and the data in the Certificate Application Form and the documents inside CP, which are a basis for such data, the Certificate User will then immediately call "CSP" Call Center, which operates 24 (twenty four) hours 7 (seven) days, making an application for a Revocation of NQC thereof. After completion of the Revocation procedure, the Certificate User or Corporate Applicant will complete the Certificate Application Form in line with the procedures and principles laid down by the Application Methods, delivering it to "CSP". "CSP" re-develops NQC upon the application made on the basis of this form by the Certificate User.

4.4.2 Publication of Certificates by "CSP"

NQC's can be published by "CSP" only subject to approval by NQC Holders in a directory open to the public.

4.4.3 Notification by "CSP" to Other Concerned Parties of Publication of Certificates

Not applicable.

4.5 Signature Creation / Verification Data and Use of NQC

4.5.1 Signature Creation Data of NQC Holders and Use of NQC

NQC Holders are obligated to make use of the signature creation data and their NQC's in compliance with their obligation laid down by CPS, CP, and the Application Forms they have signed. NQC Holders can use the signature creation and verification data only as part of the secure signature creation and verification processes. NQC'S must be used subject to the limitations regarding use and physical scope if any. NQC Holders are required to ensure confidentiality and security of the signature creation data and activation data and to prevent any unauthorized use thereof. NQC Holders must immediately inform "CSP" in case of any suspicion

over the confidentiality or security of the signature creation data, loss, theft or security compromise of the signature creation device or activation data.

4.5.2 Signature Verification Data of Third Parties and Use of NQC

Third Parties, who will conduct business and transactions relying on the secure electronic signatures, must first check NQC, which is associated with the secure electronic signature in question. A check to verify that NQC has actually been created by "CSP" is conducted by establishing that NQC Certificate Route comprises of E-TUGRA Root Certificate and E-TUGRA "CSP" Intermediate, which are publicly accessible on E-TUGRA Web Site and of NQC pertaining to the Certificate Holder, which is published in a publicly accessible directory on E-TUGRA Web Site. Additional checks which must be done involve establishment if the secure electronic signature has been created within NQC validity period and if NQC is presently Revoked or suspended. Finally, third Parties are also obligated to establish and confirm that the transaction to be concluded by use of a secure electronic signature is not one of the legal operations prohibited by the Law and that the transaction concluded is not in violation of the limitations concerning the physical scope or use of NQC. Third Parties must not conclude any transactions on the basis of NQC in case NQC checks and verification procedures fail.

4.6 Renewal of NQC

E-TUGRA certificate renewal operations are subject to only NQC renewal processes outlined below. NQC renewal is the extension of NQC validity term without making any changes to the signature creation and verification data.

4.6.1 Circumstances Requiring Renewal of NQC's

NQC's can be renewed only before the expiry of the validity terms of NQC's when there are no other circumstances calling for an amendment to NQC contents.

4.6.2 Who Can Apply for Renewal of NQC?

An application for renewal of NQC can be made only by NQC Holder in question.

4.6.3 Operational Process for Requests for Renewal of NQC

An e-mail is repeatedly sent to NQC Holder at certain intervals informing him that the expiry of NQC validity is approaching before NQC validity expires. Requests for renewal can be made via RA's. In case of a renewal request made at the web site, the application form concerning NQC renewal is completed, furnishing necessary information. E-TUGRA performs verification of the ID of NQC Holder using dual level identification methods. In the case of renewal application made to RA, RA official performs verification of the ID of NQC Holder on the basis of the latter's official ID documents such as ID card, passport and driving license. New NQC is created upon the fulfillment of necessary approval procedures after completion of the Authentication stage.

4.6.4 Notification to the Person Applying for NQC Renewal of the Development of New Certificate

NQC holder is notified by an e-mail after development of a new NQC.

4.6.5 Operations Deemed Acceptance of NQC Renewal

Installation of new NQC by NQC holder, which is the final step as part of NQC renewal procedures, is deemed acceptance of the renewal of NQC.

4.6.6 Publication by "CSP" of Renewed NQC's

E-TUGRA publishes renewed NQC's in a publicly accessible directory again if NQC Holders have granted permission for publication in that directory in advance. There is no need to seek permission for new NQC's if written permission has already been obtained from NQC holders in connection with the renewal of NQC's but publication of NQC can be discontinued if this is requested by NQC holder.

4.7 Re-keying of NQC's

E-TUGRA "CSP" operations do not involve any re-keying of NQC's. Renewal operations are just conducted as part of certificate renewal. NQC is revoked in cases requiring re-keying and a new NQC is created by initiating NQC application processes.

4.7.1 Circumstances Requiring Re-keying of NQC's

Not applicable.

4.7.2 Who Can Request for Certification of New Signature Verification Data?

Not applicable.

4.7.3 Treatment of the Requests for Re-keying of NQC's

Not applicable.

4.7.4 New NQC Publication Notification to Those Requesting for Re-keying

Not applicable.

4.7.5 Operations Deemed Acceptance of Re-keying of NQC's

Not applicable.

4.7.6 Publication of NQC's Re-keyed by "CSP"

Not applicable.

4.7.7 Notification by "CSP" to Other Concerned Parties of NQC Publication

Not applicable.

4.8 Modification to NQC's

4.8.1 Circumstances Requiring Modification to NQC's

Modification to the contents of NQC's is possible only when NQC is Revoked and a new NQC created. Such a modification calls for initiation of a new NQC application process.

4.8.2 Who Can Apply for Modification to NQC?

Not applicable.

4.8.3 Process for the Requests for Modification to NQC's

Not applicable.

4.8.4 Notification to Those Making NQC applications of Development of New Certificates

Not applicable.

4.8.5 Operations Deemed Acceptance of Modified NQC's

Not applicable.

4.8.6 Notification by "CSP" of Modifications to Certificates

Not applicable.

4.8.7 Notification by "CSP" to Other Organizations of Development of Certificates

Not applicable.

4.9 Revocation and Suspension of NQC

4.9.1 Circumstances Requiring Revocation of a NQC

NQC's are revoked in any of the following circumstances:

- Written consent of Certificate User in any case
- Execution by certificate user of an action constituting a crime by making use of NQC against "CSP" or the Corporate Applicant
- "CSP" or Corporate Applicant understanding at any time of the validity of the certificate that the data inside NQC do not reflect the truth
- "CSP" or Corporate Applicant establishing that NQC is used by the Certificate Holder unlawfully or for purposes against the area of use or physical scope contained by NQC
- Establishment by "CSP" or the Corporate Applicant that the signature creation data of the certificate user are captured by third Parties, disclosed or compromised
- "CSP" or the Corporate user suffering damages as a result of an intentional action performed by the certificate user through use of NQC
- Written notification to "CSP" of the unilateral cancellation of the certificate user application by the certificate user or unilateral termination by any of the parties of the certificate application in any case
- Discontinuation of the legal relationship between the Corporate Applicant and the Certificate User constituting a basis for the Corporate Application in applicable cases
- "CSP" or the Corporate Applicant having knowledge that the secure electronic signature creating device or activation data thereof belonging to the certificate user are stolen, lost or no longer functioning or having suspicion that the confidentiality or security of the secure electronic signature creation device or activation data belonging to the certificate user is compromised
- Having knowledge that NQC Holder has limited legal competence, gone bankrupt or missing or died
- E-TUGRA stopping providing "CSP" services

4.9.2 Who Can Apply for Revocation?

NQC's can be revoked by the following people:

- NQC Holders

- Corporate applicants if they have such authorization
- Thirds Parties holding powers thereto
- E-TUGRA
- Public establishments and judiciary parallel to their powers thereto

4.9.3 Certificate Revocation Procedures

NQC Holders, authorized corporate applicants or authorized third Parties can apply for Revocation of certificates via E-TUGRA web site, RA's or E-TUGRA Call Center. An application for Revocation of a certificate is fulfilled only upon the identification of the Revocation powers of the person making such a Revocation request. Personal information and any relevant confidential information are used in identification of powers.

4.9.4 Delay Period for Certificate Revocation Requests

Immediate action is taken by E-TUGRA on certificate Revocation requests. After approval of the certificate Revocation request, NQC is included in the first CRL to be published and this period cannot be longer than 24 hours.

4.9.5 Grace Period for "CSP" to Take Action on Revocation Request

Action is immediately initiated by E-TUGRA to approve NQC Revocation requests. After approval of the Revocation request, NQC is included in the first CRL to be published.

4.9.6 Third Party Control Obligation Concerning Revocation Status

Third Parties have to check the present validity status of a NQC prior to proceeding with any business or transaction based on a secure electronic signature. Third Parties must perform checks on the present validity status of a NQC by means of CRL or OCSP. E-TUGRA recommends that third Parties use CWA 14171 compliant secure electronic signature verification tools fo the purpose of meeting their control obligations specified by CPS, CP and the Regulation.

4.9.7 Frequency of Publication of Certificate Revocation List (CRL)

CRL's are published every 24 hours. E-TUGRA provides CRL services ensuring service 24 hours 7 days.

4.9.8 Timing for Publication of CRL's

CRL's are published immediately after they are created as part of the applicable automatic processes thereof.

4.9.9 Accessibility of Online Revocation Control

E-TUGRA provides OCSP service ensuring real time certificate Revocation status control. Operation of OCSP service is based on the installation by the user of appropriate software in E-TUGRA OCSP provider, transmission of status control requests and provider sending replies to the requests. NQC Holders and third Parties can use the secure electronic signature verification device to make use of OCSP service.

4.9.10 Online Revocation Control Requirements

See: CP, 4.9.6

4.9.11 Accessibility of Other Forms of Notices of Revocation

Not applicable.

4.9.12 Requirements In Case of Suspicion Over the Compromise of the Security of "CSP" Signature Creation Data

E-TUGRA can cancel "CSP" Root and Intermediate Certificates in case that there is suspicion that the confidentiality and security of the signature creation data pertaining to the root and certificates are compromised. In case of Revocation of "CSP" Root and Intermediate

Certificates, all the NQC's which are associated with these certificates are also Revoked. NQC holders and third Parties are notified of the Revocation of "CSP" Root and Intermediate Certificates and NQC's associated with them.

4.9.13 Suspension Conditions

Suspension of a NQC means that the NQC in question has been rendered ineffective for a temporary period of time. The difference between the operation of suspension and operation of Revocation is that although it is no longer possible to render the revoked NQC effective again, the suspended NQC can again be rendered effective upon the lifting of the suspension. E-TUGRA suspends any NQC's in response to requests made by those persons with powers on suspension of certificates of NQC holders.

4.9.14 Who Can Request for Suspension?

The following persons can ask for suspension of NQC's:

- NQC Holders
- Corporate applicants if they are authorized by NQC Holders for this purpose
- E-TUGRA
- Relevant public establishments and judicial organs on ground of their powers arising out of the legislation

4.9.15 Process of Request for Suspension

Procedures for suspension can be maintained via E-TUGRA Call Center and RA's. suspension procedures are fulfilled by the same operations under the Revocation procedures.

4.9.16 Limits for Periods of Suspension

The operation of suspension can continue until the end of the certificate validity term.

4.10 Certificate Status Services

4.10.1 Operational Features

E-TUGRA publishes NQC's in a publicly accessible directory subject to written consent by NQC Holders. NQC's are published by E-TUGRA via the data base and LDAP directory server. Status controls of NQC's are conducted by means of CRL's and OCSP. E-TUGRA provides CRL and OCSP services non-stop on the basis of 24 hours in 7 days.

4.10.2 Service Accessibility

E-TUGRA provides CRL and OCSP services non-stop on the basis of 24 hours in 7 days. In case CRL and OCSP services are interrupted beyond E-TUGRA control, E-TUGRA does its best to ensure resumption of the services within maximum 24 hours.

4.10.3 Optional Features

Not applicable.

4.11 End of Certificate Ownership

The ownership of NQC ends for those NQC's which expire and are revoked.

4.12 Signature Creation Data Recovery and Backup

E-TUGRA does not back up the signature creation data of NQC holders and neither it provides data recovery services.

4.12.1 Policy and Principles for Signature Creation Data Recovery and Backup

Not applicable.

4.12.2 Policy and Principles for Session Key Encapsulation and Recovery

Not applicable.

5. Facility, Management and Operational Controls

This part explains the basic physical and operational controls and procedures implemented by E-TUGRA during its fulfillment of "CSP" functions.

5.1 Physical Controls

5.1.1 Position and Construction of "Trust Center"

E-TUGRA performs all of basic "CSP" operations including NQC life cycle operations and key management within a "Trust Center", which is designed and physically protected in a manner stopping, preventing and detecting any covert or open intrusions.

5.1.2 Physical Access

It is possible to have physical access to E-TUGRA Trust Center by getting past a security system protected by multiple security levels. Security system levels are divided into two parts as access to the outer site and access to the Trust Center; it is possible to have access to the Trust Center only by completing access to the outer site.

Security officials use security methods such as ID checks and visitor cards in the outer site access levels. Access to the Trust Center where certificate life cycle services and key management operations are performed is realized by means of the employment of much more secure methods. Access to the Trust Center is done by only the biometric identification method which is accessible by "secure staff" exclusively and furthermore, all the entrances and exits are subject to a recording process. The Trust Center is constantly monitored by cameras and camera recordings are maintained.

5.1.3 Electrical and Air-conditioning Conditions

The hardware used in the Trust Center an E-TUGRA basic operations is equipped with uninterruptible power supplies to enable operation on the basis of 24 hours and 7 days and also with heating / ventilation / air conditioning systems to control temperature and relative moisture.

5.1.4 Protection against Water

E-TUGRA Trust Center has been built on an upper floor of the building as a precaution against water breakthroughs and floods and it has been further reinforced with necessary insulation systems.

5.1.5 Fire Prevention and Protection

E-TUGRA has taken and maintains all the necessary measures to prevent and extinguish fires or any flames or smokes that may cause damages. The Trust Center has been reinforced with fire alarms. In addition, fire extinguishing devices are available throughout the building and all the members of the staff have been trained on fire fighting measures.

5.1.6 Protection of Data Devices

Software and data used in production as well as all the devices incorporating audit, archive or backup data are stored and protected in the Trust Center or in those storage facilities outside the Trust Center which are designed such that access thereto is limited only to authorized persons and the devices are protected against accidents and damages (for instance water, fire and electromagnetic interferences) and which have proper physical and logical access controls.

5.1.7 Waste Control

All the documents, which were used in the certificate life cycle services and in other "CSP" operations by E-TUGRA and have become ineffective and/or unnecessary, are destroyed in line with the applicable processes. Any secure electronic signature creation devices and other relevant cryptographic hardware are physically destroyed or they are fundamentally reset in line

with the manufacturer's instructions; all the other wastes are taken out of the building under normal procedures.

5.1.8 Off-Site Backup

As a precaution against any possible failures and / or disasters, E-TUGRA have and store backups of the electronic records / operations of saving data routinely both inside and outside the Trust Center in line with the "Business Continuity and Disaster RecoveryPlan" for the purpose of maintaining business Continuity of the certificate management processes.

5.2 Procedure Controls

5.2.1 Trusted Roles

Management controls for NQC life cycle and secure electronic signature creation devices, key management controls and controls for E-TUGRA management systems and data banks are conducted by "secure staff" having necessary access and control authorization. "Trusted Staff" members are selected from those persons having adequate knowledge of and experience in the issues related to electronic signature technologies, data security and risk management. E-TUGRA Secure Staff definitions are the following:

- Security Officials: Members of "Secure Staff", who have total responsibility for security implementations and additionally have the task and authority of issuing approvals over development, Revocation and suspension of NQC's.
- System Managers: Members of "Secure Staff", who have the task and authority of installing, configuring and having maintenance of E-TUGRA "CSP" secure systems used for NQC applications management, development of NQC's, management of secure electronic signature creation devices and management of Revocation of certificates.
- System operators: Members of "secure staff", who have the task and authority of using E-TUGRA "CSP" secure systems, having system backups and performing backup functions on a daily basis.
- System Auditors: Members of "secure staff", who have the task and authority of ensuring access to and continuity of the audit records and archives of E-TUGRA "CSP" secure systems.

Members of "trusted staff" are selected and assigned by a manager fully authorized in terms of security from persons meeting the criteria under CP 5.3.

5.2.2 Number of Persons Needed for Each Task

E-TUGRA critical operations are generally performed with participation of more than one member of secure staff. Critical operational procedures are the implementations with higher security requirements, which require use of cryptographic devices.

Development, renewal and Revocation operations related to E-TUGRA "CSP" Root and Intermediate Certificates are performed with participation of more than one person having necessary qualifications and powers including at least two members of "secure staff" who are in a position as managers.

5.2.3 Identification and ID Control for Each Task

Persons selected as members of "secure staff" are recorded on the security system in line with the powers assigned to them by registering their ID and biological data. Authority check and task identification are conducted in connection with the operation in question prior to critical operational actions; the operation is validated and entered into records if the check of authority and identification thereof are concluded successfully.

5.2.4 Roles Requiring Separation of Duties

Certain NQC certificate life cycle operations, "CSP" key management operations and related controls are achieved with participation of more than one member of "trusted" staff on the basis of the principle of distinguishing between responsibilities. Thanks to the principle of distinguishing between responsibilities, entire or partial performance of an operation is prevented from being carried out by a single person.

5.3 Staff Controls

5.3.1 Conditions Related to Professional Knowledge, Qualifications and Experience and Clearance by Governmental Authorities

E-TUGRA employment policy has been developed specifically by paying consideration to E-TUGRA "CSP" requirements. The employment policy is classified into two parts: employment of general staff and employment of secure staff. E-TUGRA general staff comprises of those members of staff engaged in marketing, organization and certain administrative tasks, not having any involvement in Trust Center operations.

Recruitment of E-TUGRA general staff is done by a top level manager if he has the opinion that the potential employee possesses the required qualifications and he can keep secrets sticking to confidentiality.

Recruitment of E-TUGRA secure staff is concluded by a top level manager after the presentation by the potential employee of documents evidencing the professional knowledge, qualifications and experience necessary to demonstrate that he can perform his duties and responsibilities satisfactorily as required if the top level manager has a positive opinion about his relevant qualifications. Professional knowledge checks are repeated minimum every 5 years for secure staff.

E-TUGRA founding partners, its managers authorized to represent the legal entity and members of staff employed by it directly or indirectly through outsourcing are required not to have been convicted of the following crimes: a heavy imprisonment sentence or an imprisonment sentence of more than six (6) months regardless of any pardoning thereof or infamous crimes such as simple and complicated embezzlement, extortion, bribery, theft, fraudulency, forgery, breach of trust and fraudulent bankruptcy and conspiracy / plotting in governmental tenders and procurement, money laundering or disclosure of State secrets, tax evasion or participation in it or crimes related to Information Technologies. E-TUGRA also supervises to ensure that employers meet all the processes and controls under 5.3 for any staff of which services are indirectly benefited.

5.3.2 Professional Knowledge Control Procedures

A series of security and identification controls, which involve evaluation of references, checking previous job background, verification of information on training and qualifications and criminal record checks, are conducted about E-TUGRA general staff and secure staff prior to recruitment.

5.3.3 Training Conditions

Before they start performing their tasks, E-TUGRA staff receives necessary legal and technical training on the issues of "CSP" services, certificate life cycle services, professional responsibilities, basic open key platform framework, E-TUGRA security procedures and certificates. E-TUGRA training programs are periodically reviewed and updated as applicable.

5.3.4 Training Frequency and Conditions

E-TUGRA staff is provided with training with updated contents at certain intervals. Training frequency and contents can be changed parallel to the performance analyses conducted on a corporate wide basis. Training is organized in cases of any changes or updates to E-TUGRA operations or software and hardware used or whenever required.

5.3.5 Job Rotation Frequency and Sequence

Not applicable.

5.3.6 Sanctions for Unauthorized Actions

Necessary disciplinary measures are taken by E-TUGRA for those members of staff infringing on the E-TUGRA security and operational policies. E-TUGRA may require those members of staff having such responsibility to indemnify any damages suffered by E-TUGRA or the persons for whom it provides services on ground of such infringements.

Necessary legal proceedings are initiated against the culprits of such actions if unauthorized actions or actions violating the processes are covered by the definitions of crimes under the Electronic Signatures Law, Turkish Criminal Code or other applicable laws.

5.3.7 Independent Contractor Requisites

E-TUGRA can conclude service contracts with independent contractors for performance of "CSP" operations. Service contracts are drawn up such that they are consistent with E-TUGRA security and operational processes.

5.3.8 Documents Furnished to the Staff

E-TUGRA furnish all members of its staff with the documents CPS, CP, TSPS and TSP as well as any specifically Non-Qualified software and hardware operation guides.

5.4 Audits and Recording Procedures 5.4.1 Types of Incidents Recorded

The following records about E-TUGRA "CSP" operational and organizational functions are maintained in an electronic medium and / or on hard copy including definition of an incident, date of occurrence and information on the persons involved in an incident.

- Development, backup, storage, recovery, archiving and destruction of "CSP" keys (data)
- Encryption device periodical management events
- NQC applications, renewal, re-keying and Revocation
- Development and publication of certificates and CRL's
- Successful or unsuccessful attempts to have access to the system
- System failures, hardware failures and other abnormalities
- Firewall and rooter activities
- "CSP" operations center facility visitors entrances / exits

5.4.2 Record Processing Frequency

Audit records are maintained continuously and they are examined at certain intervals provided that this is weekly as a minimum. Audit records are backed up and archived provided that this is weekly as a minimum.

5.4.3 Retention Period for Audit Records

Once processed, audit records are maintained on the system in an accessible manner depending on the data storage capacity. Any information and documents which must be kept according to the applicable legislation are archived as per CP 5.5.2.

5.4.4 Protection of Audit Records

Physical and logical access controls are applied to audit record files in an electronic medium or on hard copy as a precaution against viewing, modification, deletion or access in any manner whatsoever by unauthorized persons and files of audit records are protected that way.

5.4.5 Procedures for Backups of Audit Records

Audit records are periodically backed up in line with the daily and weekly archiving processes.

5.4.6 Audit Data Collection System

During the application stage, audit data on any operations performed in an electronic medium are automatically generated and saved at the level of the network and operating system. Audit data pertaining to the operations performed manually are recorded by E-TUGRA staff manually.

5.4.7 Notification to NQC Holders or Concerned Parties Causing the Incident

When the audit data compilation system records an event, there is no need to inform the persons, corporations or officers on duty, who have caused that event, of the situation.

However, the system may issue an alert to the concerned parties depending on the nature and importance of the event.

5.4.8 Assessment of Security Vulnerabilities

Necessary measures are introduced after establishing any security gaps in the system and processes thereof as a result of routine reviews of audit records.

5.5 Archiving Records

In addition to the audit records specified by CP 5.4, E-TUGRA maintains records on all the communication between NQC applicants and certificate holders, "CSP" and other Parties.

5.5.1 Types of Events Recorded

- Individual and corporate NQC applications, information and documents used as part of applications
- Individual and corporate application contracts, other relevant contracts and documents
- Actions and information related to development, Revocation, suspension and renewal of NQC's (including time of actions and officials doing such actions)
- Contracts and major correspondence made with customers and business associates
- NQC's which have expired
- "CSP" Root and Intermediate Certificates after expiry of the validity periods thereof
- Requests for Revocation, suspension and lifting of suspension and actions for verification of requests and relevant communication information, CRL's
- All CPS, CP, TSPS and TSP documents published by E-TUGRA (all the published versions)

Records can be maintained in an electronic medium or on hard copy provided that they are positioned, stored, protected and reproduced in a correct and full manner.

5.5.2 Archive Retention Period

The records cited by 5.5.1 in line with the provisions of the Regulation and applicable legislation are retained for a period of minimum 20 years.

5.5.3 Protection of Archive

Data archived electronically are protected against viewing, modification, deletion or access in any manner whatsoever by unauthorized persons by making use of appropriate physical and logical access controls. Data manually entered on hard copy are stored in physically protected space accessible by officials only.

5.5.4 Procedures for Backing Up the Archive

E-TUGRA can have backups of any information and documents it deems necessary in or outside the Trust Center on condition that they are subject to the same security level as that of originals.

5.5.5 Conditions for Placing Time Stamps on Records

Date data are contained by NQC's, CRL's, other Revocation data base inputs and any other information and documents considered necessary by E-TUGRA.

5.5.6 Archive Compilation System

Archives are compiled in an electronic medium making use of E-TUGRA management systems or manually under the responsibility of authorized persons.

5.5.7 Procedures for Access To and Verification of Archive Data

The documents, CPS, CP, TSPS and TSP and end user application form models are published in the relevant part of the web site. Confidential documents can be accessed by "secure staff". Information on NQC applications and ID's of NQC Holders is accessible by corporate applicants' officials only to the extent of their own interest and by secure staff, officials in charge of

registration operations. Documents available in the archive will be kept in a readable format throughout their retention period.

5.6 Amendment to Signature Creation - Verification Data (Key)

As specified by the relevant legislation, the validity period of E-TUGRA "CSP" signature creation and verification data will be minimum 10 years. In necessary cases, "CSP" signature creation data can be renewed on security grounds before the expiry of the validity period of "CSP" signature creation data. In such a case, previous keys (signature creation and verification data) are stored in a usable condition until the end of the validity period. NQC's to be created with effect from the amendment to "CSP" signature creation data are signed by new signature creation data. However, to ensure that the previously created NQC's can be verified, accessibility of previous E-TUGRA "CSP" Root Certificates and Sub Certificates in which previous signature creation data are contained is ensured.

5.7 Rescue from Hazards and Disasters

5.7.1 Procedures for Keeping Events and Hazards under Control

In case of occurrence of events of such a nature affecting the security of "CSP" operation, necessary measures are introduced in line with "the Business Continuity and Disaster Recovery Plan" to ensure that the system is restored for resumption of secure operation in the shortest time possible, that the affected parties are informed accordingly and that other measures are put into practice.

5.7.2 Hardware, Software and / or Data Deterioration

In case the hardware, software and necessary data available in the Trust Center suffer failures and deterioration of any kind, the redundant hardware and software are first put into operation. Backups of data lost are operated and/or they are created anew in line with the "Business Continuity and Disaster Recovery Plan". In case of occurrence of irreparable / irreversible failures in the certificate management processes on ground of data that could not be recovered, certificates affected by such failures are immediately destroyed, with relevant parties being informed accordingly.

5.7.3 Damage to "CSP" Signature Creation Data

In case the security of the signature creation data in E-TUGRA "CSP" root certificates is compromised, certificates affected by such a security compromise are immediately destroyed, with relevant parties being informed accordingly via the Web site and emails. New signature creation data are generated for E-TUGRA "CSP" Root Certificates.

5.7.4 Business Continuity after Disaster

Actions and operations are identified against events that may prevent operation in line with E-TUGRA "Business Continuity and Disaster Recovery Plan".

5.8 Halting the Operation of "CSP" or Registration Authority

In case the operations by E-TUGRA "Registration Authority" are halted, all the information and documents in the "Registration Authority" are carried to the Trust Center and/or destructed.

In cases where there is a need to halt "CSP" operations, E-TUGRA exerts all kinds of the necessary efforts in commercial terms in order to inform certificate users, corporate applicants, third Parties and other relevant organizations of this before "CSP" operations are halted.

5.8.1 Discontinuation of Operations by the Telecommunications Agency

According to Article 29 of the Regulation on the Procedures and Principles for Implementation of the Electronic Signatures Law;

In case it establishes as a result of an audit it performs that "CSP" no longer possesses one or several of the conditions in the notification during its continued operations, the Telecommunications Agency grants "CSP" a deadline of up to one (1) month to eliminate such a discrepancy, stopping "CSP" operations during that period. The Telecommunications Agency puts an end to "CSP" operations in case the discrepancy is not eliminated at the end of the deadline granted or in case the offenses listed by Article 18 of the Law are committed for the third time within three (3) years retrospectively from the date when such an offense is first committed.

"CSP", the operation of which is discontinued upon the occurrence of any of the circumstances of discontinuation of operation, can reach agreement with another presently operating "CSP" on the transfer of qualified electronic certificates within fifteen 815) days from the date of the notification of the decision discontinuing its operations. In case of agreement, the Telecommunications Agency decides on the transfer of the QC's developed by the discontinued "CSP" to "CSP" with which agreement is reached. In case of failure to reach an agreement between the discontinued "CSP" and any presently operating "CSP" on the transfer of QC's within fifteen (15) days, the Telecommunications Agency adopts a decision on transfer of such QC's to any other "CSP" on an ex officio basis. "CSP", which takes over QC's, initiates operations for renewal of certificates, completing such operations within one (1) month from the date of the notification of the transfer decision. The Telecommunications Agency can extend an additional deadline of not more than one (1) month if it deems necessary.

"CSP" cannot provide any services related to electronic certificates, time stamps and electronic signatures from the date of the notification by the Telecommunications Agency of the decision on discontinuation of its operations. However, it continues services related to Revocation status records until operations are completed for renewal of certificates.

The discontinued "CSP" transfers documents used in Authentication, relevant directory, archive and Revocation status records, the latter being after the completion of certificate renewal operations, to the "CSP", which takes over QC's, destroying its own signature creation data and their backups.

In case there is no other "CSP" to which QC's can be transferred ex officio, the Telecommunications Agency decides on the Revocation of QC's developed by the discontinued "CSP". The discontinued "CSP" destroys its own signature creation data and their backups after it creates final Revocation status records and it continues Revocation status records service until the expiry of the qualified electronic certificates which expires latest, retaining the archive for a period of minimum twenty (20) years.

The Agency publishes decisions on the transfer of qualified electronic certificates on its Internet page. The discontinued "CSP" informs the holders of qualified electronic certificates of decisions on the transfer by e-mail, also publishing it on its Internet page.

5.8.2 Discontinuation of Operation by "CSP"

According to Article 30 of the Regulation on the Procedures and Principles for Implementation of the Electronic Signatures Law; "CSP" notifies the Agency of the situation at least three (3) months in advance of the planned date of discontinuation of its operations. Once the Agency is notified of its decision to discontinue operation, "CSP" cannot receive any Non-Qualified electronic certificate applications and neither can it develop any new electronic certificates.

"CSP" publishes its decision to discontinue operation on its Internet page at least three (3) months from the date of the planned discontinuation of operation, also informing certificate owners of it by e-mail and placing a notice in three (3) newspapers with largest national circulation thereof.

"CSP" can transfer to any other presently operating "CSP" the Non-Qualified electronic certificates, which will not expire until the date of its continuation of operation and can be served by any other presently operating "CSP" in terms of its use within one (1) month before the date of discontinuation of operation. The discontinued "CSP" informs certificate owners of the transfer by e-mail. In case of transfer of Non-Qualified electronic certificates, the "CSP" taking over the certificates initiates operations for renewal of certificates, completing them in one (1) month. If it deems necessary, the Agency can grant an additional deadline of not more than one (1) month.

The discontinued "CSP" transfers documents used in Authentication, relevant directory, archive and Revocation status records, the latter being after the completion of certificate renewal operations, to the "CSP", which takes over NQC's, destroying its own signature creation data and their backups.

In case of no transfer of Non-Qualified electronic certificates within one (1) month after the date of discontinuation of operation or failure by another presently operating "CSP" to maintain use of such Non-Qualified electronic certificates, the "CSP" intending to discontinue its operation cancels Non-Qualified electronic certificates on the date of discontinuation of operation. The discontinued "CSP" destroys its own signature creation data and their backups after it creates final Revocation status records and it continues Revocation status records service until the expiry of the Non-Qualified electronic certificates which expires latest, retaining the archive for a period of minimum twenty (20) years.

6. Technical Security Controls

6.1. Signature Creation & Verification Data Creation & Setup

6.1.1. Signature Creation and Verification Data Creation

The process of "CSP" (Electronic Certificate Service Provider) digital signature creation and verification data creation is carried out by more than one educated "confident staffs" and relevant officials, using secure systems that ensure the needed security and cryptography for the generated data. Cryptography modules that are used in order to generate digital signing and key pairs for "E-TUGRA" root certificate meets the conditions of FIPS 140-2 level 3. Digital signing and key pair data of "E-TUGRA" root certificate is generated in accordance with the algorithms and standards stated in the "Notification". The activities done during key generation period are recorded and signed together with the date. These records are kept for inspection and monitoring. The data of key pair is generated at secure electronic signature generation tool of "CSP" and cannot take out from there except for the aim of back-up. For keeping the data of key pair in safe condition, all necessary physical and technical safety measures are taken.

The key pair data of "E-TUGRA" root certificate is generated within Republic of Turkey and, in any condition, they cannot take out from these borders. The circulation period of key pair data for 'E-TUGRA' root certificate should not exceed 10 years.

According to "E-TUGRA"'s "CSP" working model, digital signing generation and key pair belonged to "Certificate Owner" will be created by "E-TUGRA" in the places of "ESH" in accordance with algorithms and standards stated in the Article 6 of "Notification". The data of generating signing is created within a secure electronic signature generation tool that, at least, has security standard of EAL+4 according to ISO/IEC 15408 (-1,-2,-3), with software able to give secure access opportunity and by "secure staff". "E-TUGRA" shall not take a copy of signature generating data belong to "Certificate Owner" and/or signature generating data shall not be kept by "E-TUGRA".

6.1.2. NQC Owner Signature Creation Data Delivery

The subscriber private encryption key is supplied to "NQC" (Non-Qualified Electronic Certificate) Owners within secure electronic signature generation tool with "NQC". Minimum "Secure Electronic Signature Generation Tool" and digital signature and key pair data in this tool, and "Secure e-signature pack" with NQC are delivered to NQC Owner against his/her signature and

checking his/her identity card. In addition to this, the access data necessary for using secure electronic signature generation tool is also supplied to NQC Owner through call centre.

6.1.3. Signature Verification Data Delivery to "CSP"

During generating keys, the digital signature data is recorded by "E-TUGRA", because according to "E-TUGRA"'s "CSP" working model, digital signing generation and key pair belonged to "Certificate Owner" will be created by "E-TUGRA" in the places of "ESH" in accordance with algorithms and standards stated in the Article 6
of "Notification".

6.1.4. CSP Signature Verification Data Delivery to Users

An "CSP" certificate (root and sub-root certificates) of "E-TUGRA" is published on the web site of http://www.e-tugra.com.tr . SHA-1 Summary of these certificates is publicly noticed in three national newspapers with the most circulation. In addition to this, "E-TUGRA" digital signature data and "E-TUGRA" root certificate can be provided to the owners of these tools for their usage, loaded on the secure electronic key pair tool supplied by "E-TUGRA".

6.1.5. Signature Creation and Verification Data Size

"E-TUGRA" Intermediate "CSP" digital signing and key pair data is 2048 bit RSA. On the other hand, "NQCs" are created as at least 1024 bit RSA, using digital signature and key pair data.

6.1.6. Key Creation Paramater & Quality Control

Public keys and "NQC" keys belonging to "E-TUGRA" root certificates are created by "secure staff" in the "Security Centre", by ensuring their physical and technical security. Parameters, algorithms and tools used during creation period are in accordance with the requirements stated in the "Notification".

6.1.7. Key Usage Purposes

"NQC" digital signature and key pair data are only used for the purpose of secure signature generation and verification. On the other hand, digital signature generation and verification data for "E-TUGRA" root certificate can be used for the purpose of "NQC" signature, "CRL" (Certificate Revocation List) signature, certificate Revocation situation registration signature, and signature for some information and documents needed for some operations related to "CSP" process. Key usage purposes are indicated in the key usage spaces of certificates.

6.2. Signature Creation Data Protection & Encryption Module System Controls

6.2.1. Encryption Module Standards & Controls

"E-TUGRA" use hardware certified to FIPS 140-2 level 3 to protect signature generation, key protection data generation and signature generation data keeping for root certificate.

Appropriate secure electronic signature generation tools, indicated in the "Notification, are used for the process of private key generation and verification for
"NQCs".

6.2.2. Signature Creation Data (n* m) More than One Person Control

The access to "E-TUGRA" "CSP" signature creation and verification data is only carried out that more than one "secure staffs" perform necessary security and identification procedures.

6.2.3. Signature Creation Data Storage

"E-TUGRA" does not give "CSP" signature creation data into any third parties, even if this is purpose of access official purposes. "E-TUGRA" does not keep the copies of signature creation data belonging to "NQC" owners.

6.2.4. Signature Creation Data Backup

"E-TUGRA" creates backup copies "CSP" signature creation data for protection against disasters and routine purposes. These data are kept as encrypted form in hardware cryptography module and related key storage devices by taking necessary technical and security measures.

6.2.5. Signature Creation Data Archive

Signature creation data related to "E-TUGRA" "CSP" root certificate are not kept for the purpose of archiving. On the other hand, signature verification data are kept for further possible conflicts for 20 years. "E-TUGRA" does not kept private key generation data for "NQC" owners for the purpose of archiving.

6.2.6. Signature Creation Data Cryptography Module Transfer

"E-TUGRA" creates private key generation and verification data for "CSP" root certificates within secure electronic signature generation tool (cryptographic module) belonging to "CSP". "CSP" private key generation data is never taken out from secure electronic signature generation tool belonging to "CSP", except for the purpose of back-up. Transferring private key generation data into another cryptographic module for the purpose of back-up is only carried on by multiple authorized "secure staff" under the appropriate technical and physical measures.

Private key generation data belonging to "NQC" owners is created within secure electronic signature generation tools and it is never taken out from these tools.

6.2.7. Encryption Module Signature Creation Data Storage

Please see "CPS" 6.2.6.

6.2.8. Signature Creation Data Activion Method

"E-TUGRA" can only carry out to activate private key generation data for "CSP" root certificates by multiple authorized "secure staff" under the appropriate technical and physical measures. The activation of private key generation data for "NQC" owners is only carried out by entering activation data into secure electronic signature generation tool.

6.2.9. Signature Creation Data Deactivation Method

"E-TUGRA" keeps private key generation data for "CSP" root certificates as active only during operation and ends the activation after finishing the operation. When the secure electronic signature generation tool belonging to "CSP" is taken out from the reader, private key data is out from the activation.

When the secure electronic signature generation tool of private key data belonging to "NQC" owners' is out from the system or the secure electronic signature generation tool is not worked for a while in connected to the system, its activation is ended.

6.2.10. Signature Creation Data Deletion Method

"E-TUGRA" can only destroy private key generation data for "CSP" root certificates by multiple authorized "secure staff" under the appropriate technical and physical measures, after the circulation period is ended, or for the purpose of security problems. The destroying of private

key data, belonging to "NQC" owners, depends on technical sufficiency of the secure electronic signature generation tool.

6.2.11. Encryption Module Operational Limits

"CSP" secure electronic signature generation tolls of "E-TUGRA" and secure electronic signature generation tools provided to "NQC" owners are complied with the standards stated in the "Notification".

6.3. Key Pair Management Other Aspects

6.3.1. Signature Verification Data Storage

"E-TUGRA" "CSP" root certificates, "NQCs" and public key verification data related to these will be kept at least for 20 years. All necessary measures for ensuring the data complete NQCs are taken during archiving.

6.3.2. Certificate Operational Period & Key Pairs Usage Period

The period of circulation for "NQCs" ends, when "NQC" period is over or revoked. The period of circulation for key pair generation and verification data is the same as the period of "NQCs"; but key pair verification data can be continued to be used for the verification of the signature. The circulation period of "E-TUGRA" "NQCs" can neo exceed 1 year.

"NQC" singing function of key pair generation data for "E-TUGRA" "CSP" root certificate is terminated at a suitable date before the circulation period of the certificate ends. The circulation period of root certificates for "E-TUGRA" "CSP" does not exceed 10 years.

6.4. Activation Data

6.4.1. Activation Data Creation & Setup

Activation data are passwords and access data that "secure staffs" use for the jobs required technical security, and are passwords that "NQC" owners use to access secure electronic signature generation tools.

The activation data for "secure staffs" and "NQC" owners are created by "E-TUGRA" and only delivered to password owners ("secure staffs" and "NQC" owners). The owners of activation

data can alert the activation data with their own controls whenever they want.

6.4.2. Activation Data Protection

After delivering the activation data to "NQC" owners and "secure staffs", the responsibility of protection data secrecy and security belongs to "NQC" owners and "secure staffs".

6.4.3. Other Aspects Regarding Activation Data

The activation data are delivered to their owner in the closed envelopes by just checking identity and against signature. Apart from delivery of secure signature creation device, the activation data are delivered to "NQC" owners by checking identity and against signature.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

All jobs and operations carried out within the process of "E-TUGRA" CSP" are performed in accordance with information security requirements. "E-TUGRA" information security requirements are met by using secure and licensed software and hardware, containing attacking noting systems in the network, controlling access and operation, using identification methods based on information and ownership, distributing limited authorization and duties among "secure staffs", and keeping and backing up all related operations and records.

6.5.2. Computer Security Controls

None related.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

System development controls of "E-TUGRA" certificate life cycle are performed according to "E-TUGRA" quality management procedures and risk reducing methods resulted at TST "17799-2 inspections.

6.6.2. Security Management Controls

"E-TUGRA" carries out routinely inner control procedures in order to perform security management controls for certificate life cycle operations, and these operations are subject to be

audited by independent auditor once per a year in the manner of security management controls, upon ISO/IEC 27001congeniality audits.

6.6.3. Life Cycle Security Controls

Not related.

6.7. Network Security Controls

Key production, certificate life circle and other systems of "E-TUGRA" "Security Centre" has necessary network security infrastructure. In providing network security, hardware such as security walls, collimators and switching devices are structured with necessary configurations. "E-TUGRA" network security management is carried out in accordance with "Network Management Procedures".

In the case that "RAs" transmit the data to the "Security Centre" in electronic environment, they use internet connection whose security is ensured.

6.8. Time Stamping

Time stamping services provided by "E-TUGRA" are independently stated in the documents of Time Stamping Policy ("TSP") and Time Stamping Practice Statement ("TSPS").

7. "NQC", "CRL" and "OCSP" 7.1. "NQC"

Profile

7.1.1. Version Number(s)

"NQCs" of "E-TUGRA" is complied with ITU-TRec X.509V.3 (1997), RFC 3280 and ETSI TS 101 862 standards.

7.1.2. Certificate Extensions

All extensions supported in X.509V.3 (1997) can be used in "E-TUGRA" root certificates and "NQCs". In key usage spaces' extensions of "NQCs", only non-repudiation and digital signature extensions are allowed to be used. On the other hand, in "E-TUGRA" root certificates, only KeyCertSign and CRL sign extensions can be used.

7.1.3. Algorithm Object Identifier (OID)

Object identifiers of used algorithms are identified within "NQC".

7.1.4. Form Names

Name spaces in "NQCs" are complied with the form of ITU X.500 "Distinguished Name".

7.1.5. Name Limitations

Anonymous and nick names cannot be used in "NQCs". In order to ensure that each name is unique, Turkish Republic Identification Card Numbers are used.

7.1.6. Certificate Policy Object Identifier

"NQCs" consists of "CPS" Non-Qualified certificate mark, and for the related "Signature Policy" as optional they include certificate policy object identifier ("OID").

7.1.7. Certificate Policy Extension Limitation Usage

None stipulated.

7.1.8. Certificate Policy Identifier, Written & Meaning Properties

There is a "URL" in certificate Policies extensions, which provides the access into "CPS".

In certificate policies extension, the object identifier that is identified for "CPS" under the object identifier belonging to "E-TUGRA", allocated from "TSE".

7.1.9. Critical Certificate Policy Extensions Meanings

No stipulation.

7.2. "CRL" Profile

"E-TUGRA" arranges "CRLs" complied with RFC 3280. In "CRLs", there is electronic signature made with "E-TUGRA" "CSP" certificate, publishing date of "CRL", publishing date of next "CRL", the serial numbers of revoked "NQCs" and Revocation
date of these "NQCs".

7.2.1. Version Number(s)

"CRLs" are prepared complying with "CRL" format ITU X.509 V.2.

7.2.2. "CRL" and "CRL" Input Additions

In "CRLs", the extensions identified by RFC 3280 are used.

7.3. Online Certificate Status Protocol (OCSP) Profile

"OCSP" is a real-time "NQC" inquiry service.

7.3.1. Version Number(s)

RFC 2560 is supported.

7.3.2. "OCSP" Extensions

RFC 2560 is supported.

8. Compliance Evaluation & Other Measurements

Under statutory legal provisions regarding "Electronic Signature", "E-TUGRA" is subject to be audited by Telekomünikasyon Kurumu for "CSP" services provided by "E-TUGRA" and "CSP" operations carried out by himself. Furthermore, Telekomünikasyon Kurumu audits "E-TUGRA" if it operates complying with legislations and standards at least once in 2 years or not.

"E-TUGRA" is subject to periodic audits for information security in "CSP" processes under ISO/IEC 27001certificate.

Besides the audits mentioned above, "E-TUGRA" continuously performs inner audit processes carried out by his own staffs.

8.1. Evaluation Frequency & Evaluation Status

The frequency of evaluations made by Telekomünikasyon Kurumu shall be at least once per two years, but it is in Corporation's initiative.

Compatibility audits, depended on TST 17799-2, certificate are made every year.

"E-TUGRA" internal audits are made by "E-TUGRA" staffs, when they are considered as necessary.

8.2. Person Making Evaluation Description & Qualifications

The audits made by Telekomünikasyon Kurumu are carried out by Corporation's authorized staffs.

Compatibility audits, depended on ISO/IEC 27001certificate, are made by an authorized auditor.

"E-TUGRA" internal audits are made by authorized "E-TUGRA" "secure staffs".

8.3. Person Making the Inspections Evaluations Relationship with Organization

The methods and principles regarding with the audits made by Telekomünikasyon Kurumu are determined by Corporation.

ISO/IEC 27001certificate is made by an independent audit.

"E-TUGRA" internal audits are made by authorized "E-TUGRA" "secure staffs".

8.4. Topics Covered by Evaluation

In audits by Telekomünikasyon Kurumu, "E-TUGRA"s obligations related to electronic signature under related legislation is audited, if they are carried or not.

In audits related to ISO/IEC 27001certificate, "E-TUGRA" "Secure Centre" operations and "CSP" processes are audited.

8.5. In the Event of Insufficiency the Steps that Will take Place

If any deficiency is identified in inner audits made by "E-TUGRA", these deficiencies are corrected by "E-TUGRA" staffs as soon as possible.

Minor deficiencies identified during ISO/IEC 27001audits are corrected by "E-TUGRA" until next audit period. If the deficiencies are major, the certificate is withdrawn.

In audits made by Telekomünikasyon Kurumu, if "E-TUGRA" does not fulfill his obligations under legislation and related standards, law sanctions and penalties will be applied against "E-TUGRA".

8.6. Evaluation Results Publication & Notification of Concerning Parties

The results of audits made by Telekomünikasyon Kurumu are transmitted to "CSP" through an official notification.

The results of ISO/IEC 27001audits are transmitted to "E-TUGRA" by the audit company.

The results of inner audit made by "E-TUGRA" are transmitted to "E-TUGRA" management and related "secure staffs".

9. Other Commercial & legal Issues

9.1. Fees

9.1.1. Certificate Creation or Renewal Fees

"E-TUGRA" charges fees to "NQC" owners and institutional application owners for certificate creation and renewal. Charges for "NQCs" determined by "E-TUGRA" will be publicly announced through www.e-tugra.com.tr web site.

9.1.2. Certificate Access Fees

"E-TUGRA" does not charge fees for "NQC" access services.

9.1.3. Certificate Revocation or Information Regarding Status Records Access Fees

Revocation or information regarding status related to "E-TUGRA"s "NQCs" are announced to relevant people through "CRLs" and "OCSPs". "E-TUGRA" does not charge fees for "CRLs" and "OCSPs" access.

9.1.4. Fees for Other Services

9.1.4.1. Time Stamping Fees

"E-TUGRA" can charge fees to "NQC" owners and third parties for time stamping services. "E-TUGRA" will publicly announce the information about time stamping fees through www.e-tugra.com.tr web site.

9.1.4.2. Service Fees like Certificate Policy Information

"E-TUGRA" does not charge fees for the access to "CPS", "CAP" (Certificate Application Policies) and other documents open to public. "E-TUGRA" does not allow using documents for other purposes than copying, delivering to the others, altering, processing, inspecting or using in processes related to "NQC.

9.1.5. Refund Policy

The application of "Certificate User" or "Institutional Application Owner" to E-TUGRA is reviewed by using "Application Method" that they chose. If an application is rejected, a notification will be sent to "Certificate User" or "Institutional Application Authority" via e-mail with the secure electronic signature. This notification explains why the application is rejected. Then, within 7 (seven) working days after this notification, the fees paid by "Certificate User" or "Institutional Application Owner" to "CSP" is refund to "Certificate User" or "Institutional Application Owner". Methods and Policies regarding to refunding is publicly announced through web site. If the application of "Certificate User" or "Institutional Application Owner" is rejected depending on deficiency in application documents or on some missing information not to be given, the fees paid to "CSP" will not be refunded and ask to "Certificate User" or "Institutional Application Owner" to complete the documents or missing information within the certain tine period given by "CSP". This request is carried out through a notification with secure electronic signature to the electronic mail address of "Certificate User" or "Institutional Application Owner" by "CSP". "CSP" explains the related methods and Policies to complete deficiencies in the notification. If "Certificate User" or "Institutional Application Owner" completes the identified deficiency complying with these methods and Policies, his/her application will be considered as accepted. If "Certificate User" or "Institutional Application Owner" does not complete the identified deficiency complying with these methods and Policies, his/her application will be considered as rejected, and the fees paid to "CSP" will be refunded to his/her by deducting the expenses made by "CSP". "Certificate User" shall check the "Secure E-Signature Pack" immediately after receiving it for ensuring that all equipments in the pack are complete and working. If "Certificate User" realizes that the equipments that he received in "Secure e-signature Pack" are incomplete or defective, he/she shall inform "CSP" about this situation by calling its call centre within 7 (seven) working days. After "CSP" receive this call, it immediately performs this changing process without any claim for charges. If "Certificate User" sets up the equipments in "Secure e-signature Pack" in wrong way, or "Certificate User" causes any incompleteness or deficiencies related to equipments, or "CSP" has not any obligations about problems, "CSP" has right to charge extra fees to "Certificate User" or "Institutional Application Owner" for solving the problems. "Certificate User" shall set up electronic signature generation tool and check the information within "NQC" installed in the tool immediately after receiving "Secure e-signature Pack". If "Certificate User" realizes that there is a difference between the information in "Certificate Application Form" and the documents in "CPS" that are bases for those information, "Certificate User" or "Institutional Application Owner will immediately ask for NQC Revocation by

calling "CSP" call centre which provides service in 7 (seven) days and 24 (twenty-four) hours. In this case, "Certificate User" or "Institutional Application Owner" will deliver "Certificate Application Form" to "CSP" by completing it according to the methods and Policies indicated in "Application Method". Upon the request by "Certificate User" complied with this form, "CSP" will re-create "NQC" without charging any fees.

9.2. Financial Responsibilities

9.2.1. Insurance Covers (Certificate Liability Insurance)

"CSPs" must arrange mandatory certificate liability insurance under the Article 13 of Electronic Signature Law. Mandatory certificate liability insurance covers the defects, negligence or careless of "CSP" or the staff whose actions are under "CSP" obligations such as;

- Not to perform appropriately his duties related to using secure products and systems of "CSP", carrying out services securely and preventing copying and distortion of certificates,
- To cover wrong information in the certificates, which is caused by "CSP",
- To be faults in the certificates, which the information given by Non-Qualified electronic signature owners during generation certificates was processed incompletely or wrongly by "CSP",
- Not to prepare fully and appropriately certificates according to the contract between "CSP" and "NQC" owners.

The damages, which are caused depending on one or more of followings, are out of insurance cover;

- War, enemy actions, battle (whether the declaration of war has been made or not), revolution, rebellion and any military movements required for those,
- Radiations or radioactivity infection caused by any nuclear fuel or nuclear wastes in the result of nuclear fuel burning or occurred by the reasons considered as such, or military movements required for those,
- Natural disasters such as earthquake, volcano activity, sea earthquake, flood, torrent and water flood, soil creep,

- The problems caused by savings by public authority and not to be raised from "CSP" deficiencies,
- The problems in the communication infrastructure and data processing infrastructure that are not directly under the control of "CSP",
- Using Non-Qualified electronic signature for the illegal purposes by signature owner,
- Transacting with same Non-Qualified electronic certificate that has not been revoked by "CSP" and causes the damages once or more in the date after insurer or policy owner was informed,
- Not to abide to the Policies and technical standards identified by related laws, regulations and notifications subject to activity.

9.2.2. Other Assets

Not relevant.

9.2.3. End User Insurance & Other Guarantee Coverage

Please see "CPS" 9.2.1.

9.3. Commercial Information Privacy

9.3.1. Regarding Private Information

All information and documents considered as private in the scope of information privacy related to "CSP"s technical and operational processes, all kinds of private information and documents related to the business activities of "CSP", "CSP" root and sub-root certificates signature generation data, operational records, information on "NQC" owners considered as "personal data" under the "Law", inspection and assessment records, all kinds of private information and documents regarding to "Secure Centre", and technical security information related to hardware and software is considered as private information.

9.3.2. Information not within the Private Information

"CP", "CPS", Application Forms, the information in the information store, "NQCs" published by "E-TUGRA" in a directory open to the public with the consent of "NQC" owner, "E-TUGRA" root and sub-root certificates, "CRLs" are not considered as private information.

9.3.3. Responsibility of Protecting Private Information

According to the Article 12 of Electronic Signature Law", "CSP";

- Cannot ask any additional information to person asking "NQC" other than necessary information for giving electronic certificate and cannot obtain these information without this person's consent,
- Cannot place the certificate in the environment in which third Parties can access without this person's consent,
- Prevents that the third Parties obtain personal data without written consent of "NQC" asking person,
- Cannot transmit this information into the third Parties and cannot use them for other purposes without "NQC" owner's consent.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

"E-TUGRA" protects the personal information of "NQC" owners according to his obligations under the "Law".

9.4.2. Information Seen as Private

The information that does not include in "NQC" contents and CRLs" and is taken from "NQC" owner during "NQC" application is seen as private information. "E-TUGRA" will not open related "NQC" to the access of public opinion if "NQC" owner does not allow doing this.

9.4.3. Information Regarded as non-private

The information that is published as open to everybody's access in "NQCs" and CRLs" is the information regarded as non-private. "E-TUGRA" will not open related "NQC" to the access of public opinion if "NQC" owner does not allow doing this.

9.4.4. Responsibility of protecting Private Information

"E-TUGRA" staff has the responsibility of protecting the information identified as private information within "CPS". Non-authorized staff cannot access to the private information.

9.4.5. Permission and Usage of Personal Information

Not relevant.

9.4.6. Legal & Managerial Statements Made

"NQC" owners and related parties, in the case that they are obligated to make explanations official authorities, accept that "E-TUGRA" has the authority to explain private/personal

information to official authorities when they are asked by official authorities according to current mandatory legislation provisions.

During the audits made by Telekomünikasyon Kurumu, according to the "Law", "CSPs" must give all kinds of information and documents that they can ask to Corporation's authorized persons.

"NQC" owners and related parties, provided that good faith, accept that "E-TUGRA" has the authority to explain private/personal information in reply to legal, managerial or other legislation processes during the investigation period related to legal and managerial cases such as notice of appearance, investigation documents, mutual written applications, evidence and document requests, if he thinks as necessary.

9.4.7. Other Situations in which Information is Released

Not relevant.

9.5. Intellectual Property Rights

Intellectual property rights of all "NQCs" and root certificates published by "E-TUGRA", certificate Revocation information, "CP", "CPS", Application Forms, all kinds of documents that are published in the information store and generated by "E-TUGRA", all kinds of data bases generated by "E-TUGRA", web sites belonging to "E-TUGRA", and all kinds of documents, visual and aural contents belongs to "E-
TUGRA".

All rights of "NQC" owners and institutional application owners regarding to any trade mark, service mark, service brand, or trade name or title (if any) that belongs to themselves and placed in "NQC" application are reserved.

9.6. Obligations and Liabilities

9.6.1. Obligations & Liabilities of "CSP"

"CSP" must provide its services such as electronic certificate, time stamping and electronic signature in complying with mandatory legislation related to electronic signature. The responsibility regimes of "CSP" are subject to the Article 13 of the "Law" and according to this article, the responsibility of "CSP" against "Certificate Owner" will be determined according to

general provisions. If "CSP" causes any damages for the third parties, because of violating the provisions of the "Law" or the "Regulation" issued by depending on this law, these damages will be compensated by "CSP". If "CSP" staffs cause any damages for the third parties, because of violating the provisions of the "Law" or the "Regulation" issued by depending on this law, these damages will be compensated by "CSP". "CSP" has not any exemption against this responsibility by presenting an exemption proof stated in the Article 55 of Law of Obligations. "CSP" can limit its own responsibility against "NQC" owners and third parties, which means the limitations of "NQC" related to usage and materialistic contents. "CSP", in the case of using without limitations related to materialistic contents and/or usage stated in "NQC", has not any obligation to compensate the damages caused by this usage out of limitations. "CSPs" must arrange mandatory certificate liability insurance under the Article 13 of Electronic Signature Law. Mandatory certificate liability insurance covers the defects, negligence or careless of "CSP" or the staff whose actions are under "CSP" Obligations such as.

9.6.2. Obligations & Liabilities of "RA"

"RA" is responsible for receiving "NQC" applications, determining identify information of "NQC" application owner depending on necessary documents, transmitting necessary information and documents to "E-TUGRA" by taking "NQC" owner, "NQC" renewal, pausing and Revocation requirements.

"E-TUGRA" is exclusively responsible for the correctness of "Identification Information" in "NQCs" against the third Parties. The responsibility regime between "E-TUGRA" and "RAs" that are not directly in its own organizations is determined according to "Registration Unit Service Contract".

9.6.3. "NQC" Owner & Commercial Application Owners Rights & Liabilities

Methods and Policies regarding to refunding is publicly announced through web site. If the application of "Certificate User" or "Institutional Application Owner" is rejected depending on deficiency in application documents or on some missing information not to be given, the fees paid to "CSP" will not be refunded and ask to "Certificate User" or "Institutional Application Owner" to complete the documents or missing information within the certain tine period given by "CSP". This request is carried out through a notification with secure electronic signature to the electronic mail address of "Certificate User" or "Institutional Application Owner" by "CSP". "CSP" explains the related methods and Policies to complete deficiencies in the notification.

If "NQC" owners do not oblige their liabilities mentioned above, the damages of "E-TUGRA", third Parties, institutional application owners and other related parties caused by or to be caused by not obliged to these liabilities will be compensated by "NQC" owners.

Institutional application owner is responsible for identifying the identification information of "NQC" owners in the name of whom he/she is applying according to documents determined by "E-TUGRA, receiving written consents of "NQC" application owners, and transmitting the information and documents determined by "E-TUGRA" to "E-TUGRA" by receiving them from "NQC" application owners.

Institutional application owner is responsible that identification information for "NQC" owners depends on official documents inside the "CPS" and they are correct. If institutional application owners do not oblige their liabilities mentioned above, the damages of "E-TUGRA", third Parties, "NQC" owners and other related parties caused by or to be caused by not obliged to these liabilities are under institutional application owners' responsibility.

9.6.4. Obligations & Liabilities of Third Party

Third parties are responsible for the verification secure electronic signature before carrying out any jobs or operations depending on a secure electronic signature generated regarding to "NQC", and controlling the validation of "NQC". Third parties can meet the requirements of this responsibility by using "secure electronic signature verification tool". At the same time, third parties are obliged to comply with the Obligations stated in the Article 16 of the "Regulation".

If institutional application owners do not oblige their liabilities mentioned above, the damages of "E-TUGRA", third Parties, "NQC" owners and other related parties caused by or to be caused by not obliged to these liabilities are under institutional application owners' responsibility.

9.6.5. Obligations & Liabilities of Others Parties

"E-TUGRA" can enter to a contract with third parties for providing some its services during it continues "CSP"'s operation. The Obligations of these third parties are determined according to service contracts made with them.

9.7. Guarantee Rejection

There are provisions regarding guarantee rejection in Application Forms and Institutional Application Contract.

9.8. Limitations of Obligations of "CSP"

According to the Article 13 of the "Law", "CSP" Obligations can only be restricted with the limitations related to materialistic contents.

9.9. Compensation

If "NQC" owners do not meet the requirements of their Obligations under this CPS and "E-TUGRA", institutional application owners or third parties has any damages caused by this lack of meeting, "NQC" owners are obliged to compensate those damages.

If "NQC" owners do not meet the requirements of their Obligations under this CPS and "E-TUGRA", institutional application owners or third parties has any damages caused by this lack of meeting, "NQC" owners are obliged to compensate those damages.

If "E-TUGRA" does not meet the requirements of his Obligations resulted by the "Law" and related legislation, he is obliged to compensate the damages of "NQC" owners and third parties resulted by this situation.

9.10. Expiration of "CPS"

9.10.1. Validation

"CPS" comes into force when the changes made in "CPS" and new versions of "CPS" are published "E-TUGRA" information store. There is a registration regarding validation dates in the information store while "CPS", the changes in "CPS" and new versions of "CPS" are published. If there is such registration, the validation date is the date stated in the mentioned registration.

9.10.2. Expiration

"CPS"s validation is expired by publishing "CPS" new version.

9.10.3. Event of Expiration

By expiration of "CPS" validation, related parties are now not bound with the provisions of expired "CPS". After the expiration of "CPS", the provisions of new "CPS" will be valid for all parties.

9.11. Personal Notification & Communication between Parties

The communication, telephone calls, web announcement between "E-TUGRA" and "NQC" owners, and Institutional Application Owners and related third parties are carried out by e-mail with secure electronic signature and/or in written form.

9.12. Changes

9.12.1. Changes Procedure

Changes in the "CPS" are carried out by "E-TUGRA" staffs. Changes and/or corrections will be published on "E-TUGRA web site, and in addition to this these changes and/or corrections will be stated in new version of the "CPS" when this version is published.

9.12.2. Notification Mechanism & Period

9.12.2.1. Items that may be Changed without Notification

"E-TUGRA" can carry out "CPS" changes and/or corrections that will not change the rights and Obligations of the related parties in the scope of "CPS" by publishing on web site without prior notification.

9.12.2.2. Items that may Change After Notification

"E-TUGRA" informs about "CPS" changes and/or corrections that will change the rights and Obligations of the related parties in the scope of "CPS" by advice/draft form before some time that is determined according to the importance of changes and/or corrections. "E-TUGRA" transmits advice/draft notifications to "NQC" owners via e-mail, and to other relevant parties via web site announcement. "E-TUGRA" performs the necessary changes according to the comments of related parties on advice/draft document within the period he has determined before, and these changes and/or corrections come into force by publishing in information store.

In the case of the security of "CSP" operation, "E-TUGRA" has the authority to make necessary changes on the "CPS" without any notification or denunciation. In these cases, changes that made come into force after the changes and corrections are published in the information store.

"E-TUGRA" will inform about changes that he made to Telekomünikasyon Kurumu within 7 (seven) days.

9.12.3. Certificate Policy Identifier (OID) or "CPS" Requires Relevant Changes

If "E-TUGRA" publishes a new certificate Policy document for using in a new field of certificate application, certificate Policys identifier belonging to related certificate Policys for "NQCs" that will be used in this certificate field are stated in "NQC" certificate part.

9.13. Resolution of Disputes

In the case of any disputes raised from this "CPS", attorneys of both sides will meet together and try to come to a composition under the Article 35/A of Lawyer Law. If the parties does not come to a composition about the even subject to dispute within 1 (one) month according to method described in this article, the parties will be free to take the event into the court. In any disputes raised from this "CPS", İstanbul (City Centre) Courts and Execution Offices are authorized.

9.14. Applicable Laws

In interpretation of "CPS", "Regulation" and "Notification" have the priority. In performing and interpreting of "CPS", Turkish Law is valid.

9.15. Compliance to Legislation

The "CPS" has prepared in accordance with "Law", "Regulation" and "Notification".

9.16. Conditions

9.16.1. The Agreement as a Whole

Not relevant.

9.16.2. Assignment & Rotation

Not relevant.

9.16.3. Severability

If any part of "CPS" is considered as invalid permanently or temporarily, the other parts that are not influenced by this part are again invalid.

9.16.4. Sanctions

Not relevant.

9.16.5. Compelling Reasons

In the case of occurring compelling reasons, related parties cannot meet the requirements of their obligations raised from "CPS". War, mobilization, terrorist activities, natural disasters (flood, lightning, earthquake) fire, the problems occurred on telecommunication lines and according to correctness law, the changes made in the legislation that will bring a huge managerial an financial troubles to the other party if the performance is required are considered as compelling reasons.

9.16.6. Other Conditions

Not relevant.