1- Translation of related sections of CP/CPS

a) For SSL, verify that the domain referenced in the certificate is owned/controlled by the certificate subscriber.
CP/CPS Section 3.2.2-Determination of Corporate Identity: Determination of Corporate Identity of the public institutions' that request SSL certificates from Kamu SM is done by official correspondence between institutions and domain name that is given in the certificate request is verified through the proper channels(nic.tr).
CP/CPS Sections 3.2.3 / 3.2.5-Determination of Personal Identity / Verification of Authority: The person that requests a SSL certificate from Kamu SM must have authority to request a certificate for the domain name that is used in the certificate request. This authority is verified by official correspondence with the public institution.

b) Verify the email account associated with the email address in the cert is owned by the subscriber, in addition to verification of subscriber’s legal identity.
CP/CPS Sections 3.2.3 / 3.2.5-Determination of Personal Identity / Verification of Authority: To verify the email account associated with the email address in the certificate, email is sent to reach the person for verification. In the email field, email addresses that has the institution's domain name are accepted only. To verify the subscriber's legal identity their national identification number is taken in the application form which is approved by the director of the institution.

c) Verify identity information in code signing certificates is that of subscriber
Currently we do not give code signing certificates.

d) Make sure it’s clear which checks are done for which context (cert usage)
Section 3 of the CP/CPS is for Identification and Authentication. The checks are done by our certificate creation software, which is programmed to work according to policies given in RFC 3647.
Section 3.1.1 Domain Name Types- In the certificates given by Kamu SM, the DN(Distinguished Name) field which holds the subscribers identity information must comply with the “ITU X.500” name types.
Section 3.1.2 Identity information to be recognizable- Identity information that is on the certificate must be meaningful to determine the real or legal entity(name, surname, company name, email address).
Section 3.1.3 Use of nicknames for the subscriber- In the certificate content no nicknames are allowed for the subscriber.
Section 3.1.4 Interpretation of different name forms- In the certificate content name forms other than “ITU X.500” cannot be used.
Section 3.1.5 Uniqueness of identity information- Every certificate given by Kamu SM has distinguishing attributes for the real or legal entities. Same real or legal entity may use the same identity information in certificates but for different entities using same information is not allowed.
Section 3.1.6 Recognition, authentication, and role of trademarks- Applicants who apply for a certificate from Kamu SM may not use names that would harm others' intellectual and industrial property rights. Kamu SM does not verify whether the names used in the certificates are damage to others' intellectual and industrial property rights. If there is a problem with the intellectual and industrial property rights, Kamu SM holds the right to decline the certificate application or to revoke the certificates it has given. Kamu SM does not take mediation actions to solve the intellectual and industrial property rights problems.

2-Explanations on potentially problematic CA practices

a) Long-Lived Domain-Validated SSL certs
We give SSL certificates for 1 year and 3 years.

b) Wildcard DV SSL certs
Wildcard certificates have been given only to public institutions.

c) Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA
We do not issue SSL certificates directly from root. All SSL certificates are issued through our subordinate CA.

d) Allowing external entities to operate subordinate CAs – in this case need to demonstrate that the external entities are required to follow the CPS and are audited as such.

We do not allow external entities to operate on our subordinate CA.

3- Example web site: https://mail.rtuk.org.tr