Key Generation Ceremony Report for

Kamu SM

Reference: AA2025070801

Essen, 2025-07-08

To whom it may concern,

This is to confirm that “TÜV NORD CERT GmbH” has audited a key generation ceremony of “Kamu SM”. The ceremony was followed in its entirety, completed successfully and without non-conformities in accordance with the applicable requirements.

This Key Generation Ceremony Report is registered under the unique identifier number “AA2025070801” and consists of 7 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV NORD CERT GmbH
Business Entity IT
Am TÜV 1
45307 Essen, Germany
E-Mail: info.tncert@tuev-nord.de

With best regards,

Digitally signed by
MATIJA MAČEK
Date: 2025.07.08
15:02:07 +02'00'

Matija Macek
Auditor

This attestation is based on the template version 3.3 as of 2024-10-08, that was approved for use by ACAB-c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- TÜV NORD CERT GmbH, Am TÜV 1, 45307 Essen, Germany, registered under HRB 9976, Amtsgericht Essen, Germany
- Accredited by DAkkS under registration D-ZE-12007-01-12[1] for the certification of trust services according to “DIN EN ISO/IEC 17065:2013” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”.
- Insurance Carrier (BRG section 8.2):
  Allianz Global Corporate & Specialty SE
- Third-party affiliate audit firms involved in the audit:
  None.

Identification and qualification of the audit team

- Number of team members: 1 Auditor
- Academic qualifications of team members:
  All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security.
- Additional competences of team members:
  All team members have knowledge of
  1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days;
  2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;
  3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and
  4) the Conformity Assessment Body's processes.
  Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic.
- Professional training of team members:
  See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in:
  a) knowledge of the CA/TSP standards and other relevant publicly available specifications;
  b) understanding functioning of trust services and information security including network security issues;
  c) understanding of risk assessment and risk management from the business perspective;
  d) technical knowledge of the activity to be audited;
  e) general knowledge of regulatory requirements relevant to TSPs; and

[1] https://www.dakks.de/en/accredited-body.html?id=D-ZE-12007-01-12

f) knowledge of security policies and controls.

- Types of professional experience and practical audit experience:
  The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.
- Additional qualification and experience Lead Auditor:
  On top of what is required for team members (see above), the Lead Auditor
  a) has acted as auditor in at least three complete TSP audits;
  b) has adequate knowledge and attributes to manage the audit process; and
  c) has the competence to communicate effectively, both orally and in writing.
- Special Credentials, Designations, or Certifications:
  All members are qualified and registered assessors within the accredited CAB.
- Auditors code of conduct incl. independence statement:
  Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.

Identification and qualification of the reviewer performing audit quality management

- Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 Reviewer
- The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):
TÜBİTAK BİLGEM KAMU SERTİFİKASYON MERKEZİ (Kamu SM), 41470 Gebze / Kocaeli, Turkey registered under VAT Number: 873 034 1530 (Uluçınar Tax Office)
Type of audit:
☒ Point in time audit of key and certificate generation ceremony
Point in time date:
2025-06-16
Audit location:
41470 Gebze / Kocaeli, Turkey

A key generation script has been prepared in accordance with the normative requirements and with the rules stated in the policy and practice statement documents of the certification service provider. During generation of the keys and certificates, this script has been followed.

In particular:

- The key generation ceremony was performed by nine individuals of the CA Owner acting in Trusted Roles.
- The key generation ceremony was observed by one individual of the Conformity Assessment Body with independence from the CA Owner.
- Principles of multiparty control and split knowledge were observed.
- The CA key pairs were generated in a physically secured environment as described in the CA's CP/CPS.

- The CA key pairs were generated within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CP/CPS.
- CA key pair generation activities were logged.
- Effective controls were maintained to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in its CP/CPS and the Key Generation Script.

The key generation ceremony has been witnessed in person.

No non-conformities have been identified during the audit.

Root 1: TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 2

Standards considered (only with regard to key generation and key protection requirements)

European Standards:
- ETSI EN 319 411-1 V1.4.1 (2023-10)
- ETSI EN 319 401 V3.1.1 (2024-06)

CA Browser Forum Requirements:
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.5

For the Trust Service Provider Conformity Assessment:
- ETSI EN 319 403-1 V2.3.1 (2020-06)
- ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- KAMU SM SSL CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT, version 3.9.0, as of 2025-04-08

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
C=TR, ST=Kocaeli, O=TUBITAK Kamu Sertifikasyon Merkezi, CN=TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 2	EC6431BA9FC13E405DF80ADE58A048136F789A03FDCA4CF5DAA4336AC522225B **SHA-256 fingerprint of Subject Public Key Info** E1CAAAB54EDDB5A47DF96A18CD8B43BF4CE935F3F41AFA3EA2C6EFB8782ABA19	ETSI EN 319 411-1 V1.4.1, OVCP

Table 1: Root-CA 1 in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2025-07-08	Initial attestation

End of the audit attestation letter.