

Standard Audit Attestation for

TÜBİTAK BİLGEM KAMU SM

Reference: ACVPR 776

Granarolo dell'Emilia, 2023-10-26

To whom it may concern,

This is to confirm that Kiwa Cermet Italia S.p.A. has audited the CAs of the TÜBİTAK BİLGEM Kamu SM without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number ACVPR 776 covers a single Root-CA and consists of 6 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Kiwa Cermet Italia S.p.A.
Via Cadriano 23
40057 - Granarolo dell'Emilia (BO) - Italy
E-Mail: info@kiwacermet.it
Phone: +39.051.4593.111

With best regards,



Fabrizio Cirilli
Lead Auditor

Giovanni Balducci
Director of System Certification Division

This attestation is based on the template version 3.1 as of 2023-08-24, 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

- Kiwa Cermet Italia S.p.A. Via Cadriano 23 40057 - Granarolo dell'Emilia (BO) – Italy registered under VAT n. 00627711203
- Accredited by Accredia under registration https://services.accredia.it/ppsearch/accredia_orgmask.jsp?ID_LINK=1733&area=310&PPSEARCH_ORG_SEARCH_MASK_ORG=0014 for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403 V2.2.2 (2015-08)” / “ETSI EN 319 403-1 V2.3.1 (2020-06)”.
- Insurance Carrier (BRG section 8.2):
AIG spa, General Representation for Italy
- Third-party affiliate audit firms involved in the audit:
None.

Identification and qualification of the audit team

- Number of team members: 2
- 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
 - 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 skills or qualifications employed throughout audit:
None.
- 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
- 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 SM, 74 41470 Gebze / Kocaeli, Türkiye registered under VAT n. 873 034 1530 (Uluçınar V.D.)
--	--

Type of audit:	<input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input checked="" type="checkbox"/> Period of time, full audit
Audit period covered for all policies:	2022-09-19 to 2023-09-19
Point in time date:	none, as audit was a period of time audit
Audit dates:	2023-10-16 to 2023-10-24 (remote) 2023-10-19 to 2023-10-20 (on site)
Audit location:	<ul style="list-style-type: none"> • Evaluation activity sites: TÜBİTAK BİLGEM PK. 74, 41470 Gebze / Kocaeli Türkiye • Ankara Office and DR Datacenter: Çamlıca Mahallesi, 408. Cad. No. 136, C Blok 06200 Çankaya / Ankara Türkiye

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

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Baseline Requirements for TLS Server Certificates, version 2.0.1 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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, version 1.0.5, as of 2023-08-09
- Kamu SM SSL Certificate Practice Statement, version 3.6.3, as of 2023-09-04

No major or minor non-conformities have been identified during the audit.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1847193, TÜBİTAK BİLGEM KAMU SM: commonName not in SAN:
https://bugzilla.mozilla.org/show_bug.cgi?id=1847193

The remediation measures taken by TÜBİTAK BİLGEM KAMU SM as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=TR, L=Gebze - Kocaeli, O=Türkiye Bilimsel ve Teknolojik Arastırma Kurumu - TUBITAK, OU=Kamu Sertifikasyon Merkezi - Kamu SM, CN=TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	SHA-256 fingerprint of the certificate: 46EDC3689046D53A453FB3104AB80DCAEC658B2660EA1629DD7E867990648716	ETSI EN 319 411-1 V1.3.1, LCP ETSI EN 319 411-1 V1.3.1, OVCP

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

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
C=TR, L=Gebze - Kocaeli, O=Türkiye Bilimsel ve Teknolojik Arastırma Kurumu - TUBITAK, OU=Kamu Sertifikasyon Merkezi - Kamu SM, CN=TUBITAK Kamu SM SSL Sertifika Hizmet Sağlayicisi - Surum 1	SHA-256 fingerprint of the certificate: BF32DA954571659AAF715C13EE703E3643DFCBAEEEE2D82110CA68EB57CB67CE0	ETSI EN 319 411-1 V1.3.1, LCP ETSI EN 319 411-1 V1.3.1, OVCP

Table 2: Sub-CA's issued by the Root-CA 1 or its Sub-CA's in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2023-10-26	Initial attestation

End of the audit attestation letter.