PC nr. ACVPR 776 **Period-of-time audit Date: from 2020-09-07 to 2020-09-16**

Trust Service Provider (TSP) Organization:

TÜBİTAK-BİLGEM Kamu Sertifikasyon Merkezi (Governmental Certification Center, TÜBİTAK BİLGEM Kamu SM)

Registered office: PK: 74, 41470 Gebze / Kocaeli Türkiye

Sites involved in the services mentioned in the scope and to which the Certification applies:

Addresses	Site Type		TSP services supplied at site ((Refer to the services listed in the scope of certification)
TÜBİTAK BİLGEM PK: 74 41470 Gebze / Kocaeli Türkiye	Main	Primary HSM	Root CA Sub CA
Çamlıca Mahallesi, 408. Cad. No. 136, C Blok 06200 Çankaya / Ankara Türkiye	Secondary	Secondary HSM	Root CA as Disaster recovery site Sub CA as Disaster recovery site

Audit standards and regulations requirements:

- **Regulation (EU) 910/2014 - eIDAS**
- **ETSI EN 319 401 version 2.2.1**
- **ETSI EN 319 411-1 version 1.2.2**
- **ETSI EN 319 411-2 version 2.2.2**
- **CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates version 1.7.1**

Trusted Services (TS)	Laws, Regulations and Standards reference (last editions published at the time of the audit)	
Registration Authority **Certification Authority** **(Digital certificates for websites - SSL)**	**Turkish Electronic Signature Law no. 5070 dated 2004-01-15** **Turkish Personal Data Protection Law no. 6698 dated 2016-04-07** **Regulation (EU) 910/2014 – eIDAS** **ETSI EN 319 401 version 2.2.1** **ETSI EN 319 411-1 version 1.2.2** **ETSI EN 319 411-2 version 2.2.2** **CA/Browser Forum Baseline Requirements version 1.7.1**	☒

Audit type: **Surveillance/Renewal Audit (full audit)**

OBJECTIVES of the Audit: Evaluate the conformity of the certified trust services to the requirements set out in the audit reference documents.

Language used for audit (if different from the language of the auditor and/or the Customer Organization): **English**

Accredited legal entity: **KIWA CERMET ITALIA S.p.A.**
Via Cadriano, 23
40057 - GRANAROLO DELL'EMILIA (BO)
Italia

KIWA CERMET personnel[1]:

Name and Surname	Role
Rutilio Mazza (Kiwa Italy)	Lead Auditor (RGA)
Fabrizio Cirilli (Kiwa Italy)	Training Lead Auditor (AA-RGA)
Gabriele Picchi (Kiwa Italy)	Auditor (AA)
Ufuk Yilmaz (Kiwa Turkey)	Technical Expert (TE)
Emin Beytullah Çamur (Kiwa Turkey)	Witness (SA)

ATTACHED DOCUMENTS to the report and consigned to the Organization:

☐ Audit plan Stage 1 **MOD PO31B**
☒ Detailed Activity plan **MOD PO31P**
☐ Management of NC - **MOD PO 31C**
☒ Checklist EN319 **411**-1
☐ Checklist EN 319 **421**
☒ Other: List of participants, List of internal documents, copies of evidences
☒ Checklist EN319 **411**-2

[1] Indicate, in addition to the members of the Audit Group, also any observers, auditors in training, translators and other roles.

Acceptance of the following KIWA N.V. and KIWA CERMET Italia regulations **Yes ☒** **No ☐** **N/A ☐**

☒ SD.001_E General Terms and Conditions Kiwa N.V. Rev. of 2014-12-08

☒ General Terms and Conditions Kiwa Cermet Italia Rev. of 2017-08-03

☒ PSC 05SF - Regulations for the Certification of Trust Services providers Rev. 3 of 2018-02-26

The Organization declares that it obey and meets the applicable local and international legislative requirements and the requirements for the certification (unless otherwise stated in the report of the present audit) as well as contractual agreements with Kiwa Cermet Italia. The Corporate Manager signatory of this report also declares, with specific reference to the activity of the audit: not to be aware of facts, litigation or legal measures related to the subject of the audit, not to have omitted or falsified information, not to be aware of situations of conflict of interest between the Audit Group and its Organization.

The Head of the Audit Group, aware of civil liability and criminal penalties for false and mendacious declarations declares that:

- have carried out the audit in accordance with the established procedures, including time set and control methodologies;
- not to be aware of conflicts of interest with the Organization under audit in accordance with Kiwa Cermet procedures;
- have carried out a sampling of activities sufficient to determine the conclusions of this audit report.

Granarolo nell'Emilia – Italy, 2020-09-19

Organization's Representative[2]
(Signature and Stamp)

Kiwa Cermet Italia Representative

[redacted]

RESERVED TO Kiwa Cermet Italia - Date: **Signature:**

Remarks:

[2] La presente firma implica accettazione dei contenuti dell'intero rapporto di valutazione comprensivo degli allegati lasciati in copia

INITIAL AND CLOSING MEETING PARTICIPANTS

Abdullah Fahreddin ULUER	Network and Security Specialist
Fatih ÖZCAN	Team Leader of IT System Unit **(System Administrator)**
Fatih ACAR	Team Leader of IT Database Unit **(System Administrator)**
Ömer GÜNEŞ	Sistem Denetçisi **(System Auditor)**
Kaan TEMUR	Team Leader of Electronic Certificate Management Department **(Certificate Issuance Personnel)**
Emrah DURMAZ	Head of Electronic Certificate Services Department
Mesut UĞURLU	Team Leader of Cyber Security Unit **(Security Personnel)**
Caner MAMALI	Cyber Security Specialist **(Security Personnel)**
Necati ALASULU	Team Leader of Information Security Unit **(Security Personnel)**
Nur Betül DEMİREL	Information Security Specialist **(Security Personnel)**
Büşra KARAYEL	Team Leader of Customer Relations Department **(Certificate Enrolment Personnel)**
Ecenur YILDIZ	Customer Relations Specialist **(Certificate Enrolment Personnel)**
Tamer ERGUN	Head of E-Signature Technologies Department
Merve Melis ŞİMŞEK	E-Signature Technologies Specialist

NOTE:
The audit activity was conducted:

- in remote connection (MS-Teams) in accordance with Corona Virus Covid19 dispositions;
- in accordance with sampling criteria and on the basis of the information and the documents consigned by the Organization under audit, in compliance with the rules defined in applicable international reference standards and accreditation regulations.

The absence of non-conformity does not guarantee the total absence of anomalies in the audited areas as referenced at the services/processes/activities verified.

Reference documents of the Organization:

Document list				
Ref.	PUBLIC OR PRIVATE	DOCUMENT NAME	VERSION	REVISION DATE
1	PUBLIC	KAMU SM CERTIFICATE POLICY	1.0.1	16.10.2019
2	PUBLIC	KAMU SM CERTIFICATE PRACTICE STATEMENT	3.3.3	04.09.2020
3	PUBLIC	KAMU SM PKI DISCLOSURE STATEMENT (PRO.01.02)	1	25.10.2019
4	PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) TAAHHÜTNAMESİ (FRM.01.09) **KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SUBSCRIBER AGREEMENT (FRM.01.27)**	13 2	29.07.2020 29.07.2020
5	PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) İPTAL BAŞVURU FORMU (FRM.01.10) **(KAMU SM SECURE SOCKETS LAYER (SSL) REVOCATION REQUEST FORM)**	6	11.05.2020
6	PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) BAŞVURU FORMU (FRM.01.11) **(KAMU SM SECURE SOCKETS LAYER (SSL) APPLICATION FORM)**	14	29.07.2020
7	PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) FAALİYET TAKİP FORMU (FRM.01.12) **(KAMU SM SECURE SOCKETS LAYER (SSL) ACTIVITY TRACKING FORM)**	3	02.05.2019
8	PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) VEKALET FORMU (FRM.01.18) **(KAMU SM SECURE SOCKETS LAYER (SSL) PROCURATORSHIP FORM)**	6	04.09.2020

9	PUBLIC	KAMU SM GÜVENLİ SUNUCU SERTİFİKASI (SSL) SAHİBİ TAAHHÜTNAMESİ (FRM.01.20) **(KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SUBSCRIBER AGREEMENT)**	9	29.07.2020
10	PUBLIC	KAMU SM GÜVENLİ SUNUCU SERTİFİKA (SSL) HİZMETİ YÜKÜMLÜLÜKLERİ (FRM.01.21) **KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SERVICE REPRESENTATIONS AND LIABILITIES (FRM.01.28)**	5 2	17.10.2019 17.10.2019
11	PUBLIC	MÜŞTERİ ŞİKAYET YÖNETİMİ PROSEDÜRÜ (PRO.01.01) **(CUSTOMER COMPLAINT MANAGEMENT PROCEDURE)**	1	24.08.2020
12	PUBLIC	BİLGİ GÜVENLİĞİ POLİTİKASI (POL.03.01) **(INFORMATION SECURITY POLICY)**	16	22.06.2020
13	PRIVATE	SSL TEMİN SÜRECİ (SUR.01.02) **(SSL SUPPLY PROCESS)**	2	02.09.2020
14	PRIVATE	SSL İPTAL SÜRECİ (SUR.01.03) **(SSL REVOCATION PROCESS)**	1	02.09.2020
15	PUBLIC	SONLANDIRMA PLANI (PLN.01.01) **(TERMINATION PLAN)**	2	01.09.2020
16	PRIVATE	ROL VE SORUMLULUKLAR YÖNERGESİ (YON.03.09) **(ROLES AND RESPONSIBILITIES INSTRUCTION)**	32	21.08.2020
17	PRIVATE	ERİŞİM YÖNETİM POLİTİKASI (POL.03.11) **(ACCESS MANAGEMENT POLICY)**	19	27.09.2018
18	PRIVATE	YEDEKLEME YÖNETİM POLİTİKASI (POL.03.13) **(BACKUP MANAGEMENT POLICY)**	14	25.09.2018
19	PRIVATE	ANAHTAR YÖNETİMİ PROSEDÜRÜ (PRO.03.12) **(KEY MANAGEMENT PROCEDURE)**	1	25.09.2018
20	PRIVATE	ANAHTAR ÜRETİMİ VE İMHA FORMU (FRM.01.25) **(KEY CREATION AND EXTERMINATION FORM)**	2	07.09.2020
21	PRIVATE	TEKNİK AÇIKLIK YÖNETİM POLİTİKASI (POL.03.12) **(TECHNICAL VULNERABILITY MANAGEMENT POLICY)**	1	04.07.2018
22	PRIVATE	İŞ SÜREKLİLİĞİ YÖNERGESİ (YON.03.04) **(BUSINESS CONTINUITY PLAN)**	22	15.10.2019
23	PRIVATE	VARLIK YÖNETİM POLİTİKASI (POL.03.07) **(ASSET MANAGEMENT POLICY)**	6	03.07.2018
24	PRIVATE	BİLGİ VARLIKLARI PROSEDÜRÜ (PRO.03.03) **(INFORMATION ASSETS PROCEDURE)**	08	20.02.2020
25	PRIVATE	RİSK YÖNETİM POLİTİKASI (POL.03.06) **(RISK MANAGEMENT POLICY)**	7	21.06.2018
26	PRIVATE	FİZİKSEL VE ÇEVRESEL GÜVENLİK POLİTİKASI (POL.03.16) **(PYHSICAL AND ENVIROMENTAL SECURITY POLICY)**	12	09.07.2018
27	PRIVATE	DİSİPLİN YÖNERGESİ (YON.03.07) **(DISCIPLINARY INSTRUCTION)**	02	13.08.2020
28	PRIVATE	İMHA EDİLEN VARLIK KAYIT FORMU (FRM.03.14) **(DESTROYED ASSET REGISTRATION FORM)**	03	11.07.2018
29	PRIVATE	DEĞİŞİKLİK YÖNETİM PROSEDÜRÜ (PRO.03.09) **(CHANGE MANAGEMENT PROCEDURE)**	14	27.09.2018
30	PRIVATE	SIKILAŞTIRMA PROSEDÜRÜ (PRO.03.05) **(HARDENING PROCEDURE)**	03	28.09.2018
31	PRIVATE	SİSTEM TEMİN, İŞLETİM, BAKIM VE GÜVENLİĞİ PROSEDÜRÜ (PRO.03.08)	07	23.10.2019

		(SYSTEM PROCUREMENT, OPERATION, MAINTENANCE AND SAFETY PROCEDURE)		
32	PRIVATE	BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİM PROSEDÜRÜ (PRO.03.01) **(INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE)**	11	04.08.2020
33	PRIVATE	İŞ SÜREKLİLİĞİ YÖNETİM POLİTİKASI (POL.03.08) (**BUSINESS CONTINUITY MANAGEMENT POLICY)**	07	26.09.2018
34	PRIVATE	GÜVENLİ SUNUCU SERTİFİKASI (SSL) TEMİN SÜRECİ KONTROL LİSTESİ (FRM.01.37) **(SSL SUPPLY PROCESS CHECKLIST)**	01	07.09.2020
5	PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) İPTAL KONTROL LİSTESİ (FRM.01.36) **(SSL REVOCATION CHECKLIST)**	01	07.09.2020

Other references of the Organization:

Distinguished Name and SHA256 fingerprint	
Reference	**Content**
Root CA	CN = TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK L = Gebze - Kocaeli C = TR SHA-256 Fingerprint: 46EDC3689046D53A453FB3104AB80DCAEC658B2660EA1629DD7E867990648716
Sub CA	CN = TUBITAK Kamu SM SSL Sertifika Hizmet Saglayicisi - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK L = Gebze- Kocaeli C = TR SHA-256 Fingerprint: BF32DA954571659AAF715C13EE703E3643DFCBAEEE2D82110CA68EB57CB67CE0

Documentation examined, descriptive of physical environments and infrastructure in scope:

Item	Type
IT Infrastructure	**CMDB and Network Topology documentation and registrations**
Disaster Recovery	**Procedures and instructions and registrations**
Physical and logical security	**Procedures and instructions and registrations**

Outcome of the review of the previous audits findings[3]: ☒ positive ☐ negative (ref. findings:)

Use of the trust mark and the certificate: ☒ Complies ☐ Do not complies (ref. findings:)

Confirmation of the Organization data declared to KIWA CERMET Italia (number of sites and employees):

☒ **Yes** ☐ No (Indicate the changes):

Consistency between the sites and the purpose of the certificate and the information included in the Organization registration certificate

☒ **Yes** ☐ No (Indicate the changes):

[3] To be performed e.g. for verification of transfer audit from another CAB.

Confirmation of the Certificate (Scope, Addresses, Sites):

☒ **Yes** ☐ No (indicate the changes or use specific form attached to the report)

Total number of Category 1 (Major) Non-conformities: 0

Total number of Category 2 (Minor) Non-conformities: 0

Number of Non-conformities still not closed from previous audits: 0

The Organization must conduct an analysis of the root causes of non-conformities and communicate to Kiwa Cermet Italia the treatment and the corrective actions defined to solve the non-conformities within 20 days after the completion of this audit.

The implementation of the corrective actions and the closure of the Non-conformities will be verified in accordance with the PSC 05SF Certification Regulations and under the conditions approved by the Audit Group Manager indicated in the NON-CONFORMITY MANAGEMENT – MOD PO 31C module.

References to the implementation of the security risk analysis:

Internally designed and developed EBA RISK SECURITY MANAGEMENT SYSTEM based on enhanced ISO 31000 specification and ISO/IEC 27001 Annex A controls.

Period of time Audit Date Interval: from 2019-10-25 to 2020-09-16.

On Site Audit Date Interval: from 2020-09-07 to 2020-09-16.

Details of Audit time:

Activities	Expended time (Days)
Document review	**1**
Risk analysis verification	**1**
On site audit	**11**
Reporting	**1**

Audit methodologies adopted:

Activities	Description
Survey methodology	**All processes were submitted to audit with the methodology specified in Kiwa Cermet Italia Regulation for the certification of Trust services PSC 05_SF Rev. 3 2018-02-26** **The audit is a full audit, and the following parts of the criteria were applied: Part 1 (NCP+, OVCP) and Part 2 (Requirements for trust service providers)**
Sampling methodology	**AQL (ISO 2859-1:1999 for acceptability levels 1,00%)**
Performed tests and controls	**On Samples in Registration Authority and Certification Authority:** **Request of new subscriptions (RA) and issues of new certificates (CA)**

Organizational Context and Management Commitment: (also indicate any significant changes and the degree of maturity of the services/processes being certified)

- **High commitment of Management**
- **Very high skill of all personnel involved in scope**
- **Use of first class devices**
- **High quality of internal developed applications both for SSL certificate testing and for general management**
- **Well managed system documentation with recurrent updates and revisions**
- **The improved eBA MS collect all the informations on the system status**

Opportunities for Improvement:

- **none**

Criticalities: (Report any situation that have conditioned the proper conduct of the audit, e.g. not access to staff / locations / information necessary to achieve the audit objectives)

- **No criticalities**

Improvement of Capabilities and Conformity Preservations Guarantees:

- **Management motivations, personnel skills and continuous infrastructure enhancements ensure the maintenance of conformity and improvement of service performance**

Services or activities included in the scope of certification and managed in outsourcing:

- **Kamu SM Site and Datacenter managed by parent Company TÜBİTAK BİLGEM, with mutual formalized agreements**
- **PKI CA Software ESYA developed and maintained by group Company TÜBİTAK BİLGEM UEKAE MA3 with formalized agreement**

The Organization exposes Reserves: ☐ **Yes** [4] ☒ No

Satisfies the conditions for the emission of the certificate of conformity to the applicable standard: ☒ **Yes** ☐ No

We declare that the the audit was performed as a full audit and in OVCP Level

We declare that the Organization subjected to the audit:

☒ **IS COMPLIANT with the rules of the Accreditation scheme** (Accredia Circular of 2017-03-27 prot.: DC2017SSV046), to the requirements of the applicable standards of the ETSI EN 319 Series and to the REGULATION (EU) No 910/2014 of the European Parliament and of the Council stated July, 23th 2014 on electronic identification and trusted services for electronic transactions, in the internal market that revoke the Directive 1999/93/EC, with particular reference to Articles 13, 15, 19, 24, 28, 29, 30 and 32 to 45 and Annexes, where relevant with the services in scope of the certification.

☐ **IS NOT COMPLIANT with the rules of the Accreditation scheme** (Accredia Circular of 2017-03-27 prot.: DC2017SSV046), to the requirements of the applicable standards of the ETSI EN 319 Series and to the REGULATION (EU) No 910/2014 of the European Parliament and of the Council stated July, 23th 2014 on electronic identification and trusted services for electronic transactions, in the internal market that revoke the Directive 1999/93/EC, with particular reference to Articles 13, 15, 19, 24, 28, 29, 30 and 32 to 45 and Annexes, where relevant with the services in scope of the certification. (ref. non conformities in this audit referenced to in the MOD PO 31C modules attached to this report).

DOCUMENTS ATTACHED to this report and consigned to Kiwa Cermet Italia**:**

☒ Audit Program **MOD PO31** ☐ Non Conformity from previous audit nr. 0 of which closed nr. 0

[4] The Organisation must formalize the reserves with formal communication, stamped and signed, to the Representative of Kiwa Cermet Italia