

PC nr. ACVPR 776

Period-of-time audit Date: from 2018/11/08 to 2018/11/16

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

ETSI EN 319 411-1

ETSI EN 319 411-2

ETSI EN 319 412-1/4

CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Trusted Services (TS)	Standards and regulations reference (last editions published at the time of the audit)
Registration Authority Certification Authority (Digital certificates for websites - SSL)	Regulation (EU) 910/2014 – eIDAS ETSI EN 319_401 ETSI EN 319_411-1 ETSI EN 319_411-2 ETSI EN 319_412-1 ETSI EN 319_412-4 CA/Browser Forum Baseline Requirements - 1.6.1.

Audit type: Stage 1 and Stage 2

**OBJECTIVES of the Audit:** Evaluate the conformity of the certified trust services to the requirements set out in the audit reference documents.**Coverage period of the audit:** The previous audit was performed on 8 December 2017 and is valid until 16 November 2018.**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 Italia personnel<sup>1</sup>:**

Name and Surname	Role
Valentino Privato	Audit team responsible (RGA)
Rutilio Mazza	Auditor (A)
Emin Beytullah Çamur (Kiwa Turkey)	Translator (T)
Özgün Okumuş (Kiwa Turkey)	Witness (W)

**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
- ☐ Checklist EN319 **411-2**

<sup>1</sup> 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.

**Gebza, November 16, 2018****Organization's Representative<sup>2</sup>**  
(Signature and Stamp)**Kiwa Cermet Italia Representative****RESERVED TO Kiwa Cermet Italia - Date:****Signature:**

Remarks:

<sup>2</sup> La presente firma implica accettazione dei contenuti dell'intero rapporto di valutazione comprensivo degli allegati lasciati in copia



## Acceptance of the following 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.

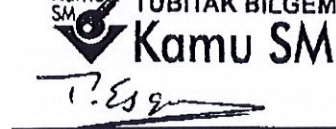
The Head of the Audit Group, aware of civil liability and criminal penalties for false and mendacious declarations declares that:

- 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.

Gebza, November 16, 2018

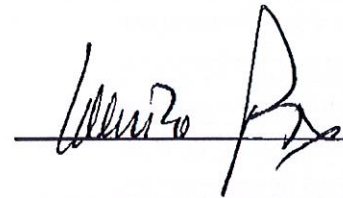
Organization's Representative<sup>2</sup>

(Signature and Stamp)



TUBITAK BİLGEM  
Kamu SM

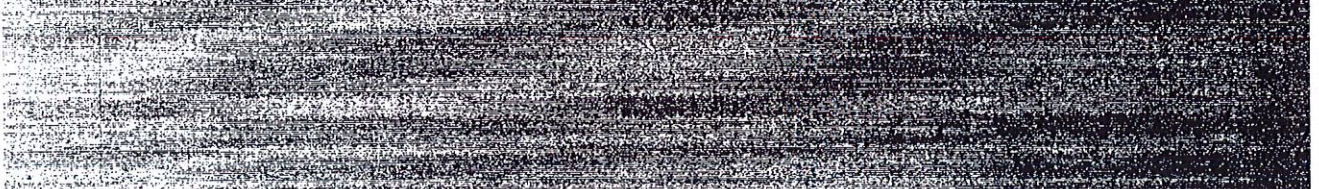
## Kiwa Cermet Italia Representative



RESERVED TO Kiwa Cermet Italia - Date:

Signature:

Remarks:



<sup>2</sup> La presente firma implica accettazione dei contenuti dell'intero rapporto di valutazione comprensivo degli allegati lasciati in copia

**INITIAL AND CLOSING MEETING PARTICIPANTS**

<b>Participants:</b>	
See detailed list attached to the report	

**NOTE:**

The audit activity is conducted 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.	Title
1	Organization documents list attached to the report

**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 = Türkiye Bilimsel ve Teknolojik Arastırma Kurumu - TUBITAK L = Gebze - Kocaeli C = TR SHA-256 Fingerprint: 46EDC3689046D53A453FB3104AB80DCAEC658B2660EA1629DD7E867990648716
Sub CA	CN = TUBITAK Kamu SM SSL Sertifika Hizmet Sağlayıcısı - Surum 1 OU = Kamu Sertifikasyon Merkezi - Kamu SM O = Türkiye Bilimsel ve Teknolojik Arastırma 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<sup>3</sup>:** ☐ positive ☐ negative (ref. findings: ) ☒ **N/A**

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

**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):

**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: 1** (Form TÜBİTAK BİLGEM 2018-11 NCR attached to report)

**Number of Non-conformities still not closed from previous audits: N/A**

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.

<sup>3</sup> To be performed e.g. for verification of transfer audit from another CAB.

**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.

**Details of Audit time:**

Activities	Expended time (Days)
Document review	2
Risk analysis verification	2
On site audit	12
Reporting	2

**Audit methodologies adopted:**

Activities	Description
Survey methodology	<p>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</p> <p>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)</p>
Sampling methodology	AQL (ISO 2859-1:1999 for acceptability levels 1,00%)
Performed tests and controls	<p>On Samples in Registration Authority and Certification Authority:</p> <p>Request of new subscriptions (RA) and issues of new certificates (CA)</p>



**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 apparatus and 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**

**Opportunities for Improvement:**

- **The Objective on System Management Review for OCSP service could be stated at 100%**
- **To Ankara basement infrastructure management could be requested to record the periodic testing on electro generators (weekly test performed but not registered)**
- **In addition to manual shut down procedures to be used during negative or adverse events on critical systems, a procedure for automatic shutdown of the systems could be implemented.**
- **In BCP flow chart representation could be included the communication process used to inform the external parts (Communication instruction YON.03.04\_21)**

**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:**

- **Not applicable: All services are managed by Organization**

The Organization exposes Reserves:

☐ Yes <sup>4</sup>

☒ No

Satisfies the conditions for the emission of the certificate of conformity to the applicable standard: ☒ Yes

☐ No

We declare that 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, 23<sup>th</sup> 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, 23<sup>th</sup> 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

<sup>4</sup> The Organisation must formalize the reserves with formal communication, stamped and signed, to the Representative of Kiwa Cermet Italia



CP no. ACVPR776

Organization Assessed: TÜBİTAK BİLGEM

Audit date: 2018-11-16

<b>No. 1 of 1</b>	
Standard: ETSI EN 319-401	Standard paragraph: 5
Non-conformity: <input type="checkbox"/> Major <input checked="" type="checkbox"/> Minor	
<p>Description: The risk analysis did not explicitly and comprehensively identify the following risk: Non correct identification of the natural person that request the certificate for the subscriber.</p>	
<p>Date: <b>2018-11-14</b> Lead Auditor: (Name/surname and signature) Valentino Privato</p> <p>The Organization commits to communicate to Kiwa Cemet Italia the cause analysis, the treatment and the corrective actions in accordance with the modalities and the timing mentioned in the relevant Certification Regulations applicable to this audit.</p>	
<p>Acceptance by the Management Representative: (Name/surname and signature)</p>	
<p>Non-conformity root cause analysis:</p> <p>Definition of mitigation measures without complete risk assessment</p>	
<p>Non conformity Treatment:</p> <p>To be implemented within 2018-11-14</p>	
<p>Corrective Action (attachments can be provided):</p> <p>Formalization of the risk of non-correct identification of the natural person To be implemented within 2018-11-14</p>	
<p>Date: 2018-11-14 Management Representative: (Name/surname and signature): <u>Tamer Elgun</u></p>	
<p>Treatment and Corrective Action Assessment: <input checked="" type="checkbox"/> Accepted <input type="checkbox"/> Not accepted (Refer to below mentioned notes)</p> <p>Notes:</p> <p>To verify: <input checked="" type="checkbox"/> during this audit <input type="checkbox"/> during supplementary audit <input type="checkbox"/> documental review</p>	
<p>Date: 2018-11-16 Lead Auditor: (Name/surname and signature) Valentino Privato</p>	
<p>Effectiveness assessment and closing of Treatment and Corrective Action: <input checked="" type="checkbox"/> Positive <input type="checkbox"/> Negative (Refer to below mentioned notes)</p> <p>Notes: The NC was handled with an information security incident: number 157 dated 2018/11/14 Verified the risk analysis update. New risk defined as number 198 dated 2018/11/14 in EBA RMT</p>	
<p>Date: 2018-11-16 Lead Auditor: (Name/surname and signature) Valentino Privato</p>	



## KAMU SM SSL CERTIFICATE MANAGEMENT DOCUMENT LIST

PUBLIC OR PRIVATE	DOCUMENT NAME	VERSION	REVISION DATE
PUBLIC	KAMU SM CERTIFICATE POLICY	1.0.0	07.08.2018
PUBLIC	KAMU SM CERTIFICATE PRACTICE STATEMENT	3.3.0	24.10.2018
PUBLIC	KAMU SM PKI DISCLOSURE STATEMENT	0	22.10.2018
PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) TAAHHÜTNAMESİ	10	27.06.2018
	KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SUBSCRIBER AGREEMENT	0	23.10.2018
PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) İPTAL BAŞVURU FORMU (KAMU SM SECURE SOCKETS LAYER (SSL) REVOCATION REQUEST FORM)	4	27.06.2018
PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) BAŞVURU FORMU (KAMU SM SECURE SOCKETS LAYER (SSL) APPLICATION FORM)	10	27.06.2018
PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) FAALİYET TAKİP FORMU (KAMU SM SECURE SOCKETS LAYER (SSL) ACTIVITY TRACKING FORM)	2	27.06.2018
PUBLIC	GÜVENLİ SUNUCU SERTİFİKASI (SSL) VEKALET FORMU (KAMU SM SECURE SOCKETS LAYER (SSL) PROCURATORSHIP FORM)	2	27.06.2018
PUBLIC	KAMU SM GÜVENLİ SUNUCU SERTİFİKASI (SSL) SAHİBİ TAAHHÜTNAMESİ (KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SUBSCRIBER AGREEMENT)	7	27.06.2018
PUBLIC	KAMU SM GÜVENLİ SUNUCU SERTİFİKA (SSL) HİZMETİ YÜKÜMLÜLÜKLERİ	3	22.10.2018
	KAMU SM SECURE SOCKETS LAYER (SSL) CERTIFICATE SERVICE REPRESENTATIONS AND LIABILITIES	0	22.10.2018
PUBLIC	MÜŞTERİ ŞİKAYET YÖNETİMİ PROSEDÜRÜ (CUSTOMER COMPLAINT MANAGEMENT PROCEDURE)	0	18.10.2018
PUBLIC	BİLGİ GÜVENLİĞİ POLİTİKASI (INFORMATION SECURITY POLICY)	15	04.06.2018
PRIVATE	SSL TEMİN SÜRECİ (SSL SUPPLY PROCESS)	0	26.09.2018
PRIVATE	SONLANDIRMA PLANI (TERMINATION PLAN)	0	06.11.2018
PRIVATE	ROL VE SORUMLULUKLAR YÖNERGESİ (ROLES AND RESPONSIBILITIES INSTRUCTION)	30	02.10.2018
PRIVATE	ERİŞİM YÖNETİM POLİTİKASI (ACCESS MANAGEMENT POLICY)	19	27.09.2018
PRIVATE	YEDEKLEME YÖNETİM POLİTİKASI (BACKUP MANAGEMENT POLICY)	14	25.09.2018
PRIVATE	ANAHTAR YÖNETİMİ PROSEDÜRÜ (KEY MANAGEMENT PROCEDURE)	1	25.09.2018
PRIVATE	ANAHTAR ÜRETİMİ VE İMHA FORMU (KEY CREATION AND EXTERMINATION FORM)	0	17.09.2018
PRIVATE	TEKNİK AÇIKLIK YÖNETİM POLİTİKASI (TECHNICAL VULNERABILITY MANAGEMENT POLICY)	1	04.07.2018
PRIVATE	İŞ SÜREKLİLİĞİ YÖNERGESİ (BUSINESS CONTINUITY PLAN)	21	26.09.2018
PRIVATE	VARLIK YÖNETİM POLİTİKASI (ASSET MANAGEMENT POLICY)	6	03.07.2018