To all applicant and accredited Certification and Inspection Bodies for the ISMS scheme or equivalent schemes.

Our ref.: DC2017SSV046 *Milano,* 27/03/2017

Subject: **ACCREDIA Department of Certification and Inspection – Circular N° 8/2017**
Informative Circular regarding the accreditation of certification bodies operating against the requirements of Reg. EU 2014_910 "eIDAS", and against the standard ETSI EN 319_403, for the assessment of Trust Service Providers and the services which they provide, to obtain and maintain the status of "Qualified" by the government agency for Digital Italy" – AgID – (eIDAS scheme),

The present Circular repeals and replaces Circular N° 17/2016 of 19/05/2016

Introduction

Reg. EU 910/2014, known as the eIDAS Regulation [*electronic IDentification Authentication and Signature*], provides for the involvement of accredited CABs according to Reg. EU 765/2008 for TSP (Trust Service Providers) and for services which they provide. This qualified activity is required by the government authorities of all EU countries where TSPs are operative, and they are also notified to the European Commission by the state in question. This state authority (in Italy it is called AgID) shall also perform periodical surveillance activities or activities following the signaling of major problems, concerning Trust Service Providers. These surveillance activities, under normal conditions, are based on on-site verifications, which are carried out twice a year by Certification Bodies (also Conformity Assessment Bodies, or CABs) which are accredited for this scheme.
The necessary condition for a CAB to obtain accreditation is fulfillment of the requirements according to ACCREDIA regulation RG-01 for the accreditation of Certification and Inspection Bodies and ACCREDIA regulation RG-01-03 for the accreditation of Product Certification Bodies.
Following application by the CAB and the verified possession of the minimum requirements of a specific document exam, the accreditation process can begin in accordance with the regulation and in compliance with the normative documents which are applicable for accreditation.

Normative documents

For the accreditation of a CAB to operate in the eIDAS scheme and, consequentially, for it to undertake certification of TSPs, the ETSI (European Telecommunications Standards Institute), in collaboration with EA and with representatives of the interested parties, has developed a specific standard - ETSI EN 319_403, the standard for the accreditation of CABs. This standard is based on UNI CEI EN ISO/IEC 17065:2012, incorporating into it as necessary, such as the qualification of auditors and the CAB's personnel, for operative activities of various types within the scheme.
The other standards are ETSI EN 319_401 (parts 1 and 2) and ETSI EN 319_421 and 422 for the issue of temporary marks (Time Stamping), and ETSI EN 319_412 (parts 1,2,3,4 and 5) for the content of certificates issued by TSPs.
Other ETSI EN standards will be published in the near future to cover the full range of services offered by TSPs operating in Europe.

Sede operativa e amministrativa: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Sede legale: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | Partita IVA - Codice Fiscale 10566361001

THE CERTIFICATION PROCESS	
Certification Bodies possessing the requirements to request extension of accreditation to the eIDAS scheme.	To request accreditation for the eIDAS scheme, a CAB needs to be already accredited for the PRD scheme, against the standard UNI CEI EN ISO/IEC 17065:2012 and for the ISMS scheme against the standard UNI CEI EN ISO/IEC 17021-1:2015 or against another certification scheme for the protection of data considered sufficiently similar to the ISMS scheme by ACCREDIA's Technical Office. Accreditation shall be issued as extension of the PRD scheme, in accordance with ETSI EN 319_403 V2.2.2.
Application for extension	Although the eIDAS scheme regards an area covered by the requirements of Regulation EU 2014/910, the application for extension of accreditation shall be presented by CABs which are entitled to do so, using the forms DA-00 and DA-01, both available on ACCREDIA's website, together with all documents as required by the application.
Certification standard (main references)	ETSI EN 319 401 (in the most recent veriosn) ETSI EN 319 411-2, supported by ETSI EN 319 411-1 ETSI EN 319 421 and 422 ETSI EN 319 412 (1, 2, 3, 4 and 5)
General competences of the CAB's personnel operating in the scheme	The competences of the CAB's personnel operating in the scheme, including personnel undertaking commercial activities and personnel engaged in decision-taking activities, shall conform with the requirements of the standard ETSI EN 319_403, as described in § 6.2.1.2. Decision-taking personnel shall also be acquainted with the certification process according to § 6.2.1.6 of ETSI EN 319_403.
Competence of personnel who review the application for certification	The competences of the CAB's personnel who review application for certification shall be in conformity with the requirements of the standard ETSI EN 319_403, as set out in § 6.2.1.3
Competence of personnel who review the contract	General knowledge of the standards UNI CEI EN ISO/IEC 17065, ETSI EN 319_403 and ETSI EN 319_401 and the specific standards related to the services offered by TSPs.
Competence of the audit team leader and auditors	The competences of the lead auditor and the auditors operating in the eIDAS scheme shall be in conformity with the requirements of the standard ETSI EN 319_403, as set out in § 6.2.1.3, 6.2.1.4 and 6.2.1.8. For the position of lead auditor the CAB shall verify that the lead auditor has adequate knowledge of Reg. (EU) 2014/910 (the eIDAS regulation and competences in conformity with the standard ETSI EN 319_403 § 6.2.1.9.
Overall competence of the audit team	It is possible to include a sector expert among the audit team members. The expert cannot perform alone the audit or any part of it and shall report to the lead auditor throughout. It is the CAB's responsibility to ensure the sectoral competence (IAF sectors and technical areas) of personnel, as defined in ETSI EN 319_403 § 6.2.1.7.
Competence of personnel who review the information gathered during the audit and the audit results	Possession of the specific competences set out in § 6.2.1.4 of the standard ETSI EN 319_403 and participation as auditor in, as a minimum, three complete audits at TSPs.
Competence of decision-making personnel	§ 6.2.1.6 of ETSI EN 319_403.is applicable
Management and	The CAB shall perform full surveillances every two years in

implementation of the audit program, audit times and frequency.	accordance with eIDAS and with the requirements of the standard EN 17065:2012 and ETSI EN 319_403 (§ 7.9), and one partial surveillance in the years in which the complete surveillance is not carried out.
The value and benefits of accreditation	Accreditation issued by ACCREDIA guarantees the conformity of CABs with the requirements of the standard EN 17065:2012 incorporating the requirements of the standard ETSI EN 319_403. Accreditation can be granted for services of Time Stamping [ETSI EN 319 421 and ETSI EN 319 422] and/or of the performance of all services as defined in the standard ETSI EN 319 412 (from § 1 to § 5) and for other services for which the reference standards will be drawn up by EA and/or by the European Commission. Accreditation does not cover and does not permit the certification of services (PSES, REMQ), related to the "preservation of signatures and seals" and to the "delivery of electronic mail". ACCREDIA evaluates the congruity and conformity of the system documentation which is presented (see the list of documents required) both for initial extension to the PRD scheme and when a single CAB presents a specific request.

RULES FOR ACCREDITATION

The requirements of ACCREDIA Regulations RG-01 and RG-01-03 for the granting of accreditation and for extension are applicable.
The accredication certificate does not state the accreditation sectors because the TSPs operate mostly in IAF sector 33 and such wording in the certificate would be redundant.
Witness assessments may be chosen by ACCREDIA on the basis of the services requested by the CAB in order to issue accredited certifications. The following rules apply for accreditation:

PROCESS OF ACCREDITATION/EXTENSION	
CAB <u>not</u> accredited for the standard UNI CEI EN ISO/IEC 17065:2012 – PRD scheme	- The CAB shall present the application for accreditation for the standard UNI CEI EN ISO/IEC 17065:2012 in order to be able to issue certifications of services/processes. - Document review lasting one day. - On-site assessment at the CAB's lasting two days. - Witness assessment at an organization providing services / processes which undergo certification by the CAB against a specific discipline recognized by the interested parties and approved by the ACCREDIA Board in conformity with the requirements of the ACCREDIA procedure PG-13-01.
CAB <u>not</u> accredited for the standard UNI CEI EN ISO/IEC 17021-1:2015 or the ISMS scheme, i.e. according to an accreditation scheme relevant to information security similar to the ISMS scheme by ACCREDIA's Technical Office.	- The CAB shall present the application for accreditation for the ISMS scheme in accordance with the provisions of the specific scheme as shown in ACCREDIA's website.
Accreditation rules for the eIDAS scheme (Reg. EU 2014/910)	
Document review	It is necessary to present to ACCREDIA the system documentation

	showing conformity with the standard ETSI EN 319_403. In certain cases it is possible to accept a single internal regulation produced for the specific scheme. In such cases this regulation shall indicate the CAB's internal documents which are part of the system documentation affected by the requirements of the ETSI standard in question. The regulation shall contain, for every applicable requirement, the applicable modifications, in order to ensure conformity with ETSI EN 319_403.
Evaluation procedure for the eIDAS scheme	The CAB shall produce a system document which describes (also in a concise or graphic way)* the evaluation and decision-taking process for the specific scheme. Note (*) e.g. by means of a flow chart or swim-lane chart etc.
Commercial procedure	The CAB shall produce a system document which includes the existing procedure for the acquisition of contracts, with special attention to the phases of analysis of the TSP and the review of the quote, in order to verify possession of the specific competences to operate in the area of the services required.
Evaluations of the IT system	Regarding use of "cloud" infrastructures, the TSP shall provide evidence of his capacity for real operative control of these services. The CAB shall verify the existence and acceptability of operative controls regarding VA (Vulnerability Assessment) and PT (Penetration Test) processes. These activities shall be done by internal or external laboratories with respect to the TSP, i.e. by internal or external persons to the CAB, whose qualification shall be based on, from June 1, 2017, the standard UNI CEI EN ISO/IEC 17025 and who shall provide evidence forthwith regarding at least: - the clear identification and consistent application of the requirements involved in the methodology of technical evaluation used, preferably in accordance with ISO/IEC 27008; - the formal competences (qualifications, source of issue of such, sector experience) of personnel performing such tests; - the qualification (certification in IT jargon) of the SW used (at least the guarantee that the versions are compatible and updated with respect to their issue by the SOs and the applications of the Holder to be examined) the above validation, where the test laboratory is chosen by the TSP is the responsibility of the TSP and shall be validated as part of the audit process by the CAB. If, however, the laboratory has been chosen by the CAB the qualification rules applied are those set out in the accreditation standard UNI CEI EN ISO/IEC 17065. From June 1, 2018, operators performing PT and VA activities accreditation will become mandatory against the standard UNI CEI EN ISO/IEC 17025:2005.
Audit report	§ 7.4.4 of the standard ETSI EN 319_403 is applicable. The CAB shall prepare and make available a format for the audit report allowing for evidence of the complete evaluation of all the applicable requirements and single controls performed, incorporating in the same report the related ETSI checklists with the validation standards. The CAB's validation process shall cover the services which the TSP declared to AgID. Following the internal review of the CAB, the conformity to the eIDAS Regulation can be deliberated as well as the conformity of the services provided against the ETSI standards and/or other standards specifically identified by EA or by the European Commission for verifying the

	conformity of eIDAS services. In the audit report the CAB shall clearly indicate the conformity status to the accreditation scheme for the eIDAS Regulation 910/2014, in particular as stated in Articles 13, 15, 19, 24, 28, 29, 30 and from 32 to 45 and in the Annexes, where necessary, with the certified services, and also with the standard ETSI EN 319 401, where such conformity occurs. This wording shall also be present in the Certificates of Conformity. The CAB shall adopt a modality for the IT sealing of the report on the basis of which the decision was taken, so as to assure authenticity and integrity for third parties. Subsequently, the report, together with all the documents recording the objective evidence gathered on-site, shall be formally sent to the TSP which, in turn and if necessary, sends it to AgID for the continuation of the process of qualification as QTSP. One modality could be to send it by certified email. The CAB does not have to wait for the decisions of AgID for the purposes of the decision with respect to certification or not of the TSP. The audit report shall give evidence of the verification of all the operative controls in accordance with ETSI EN 319_401, specifying the frequency of monitoring activities by the TSP and the efficacy of such controls (ongoing records and the analysis of them, where possible).
Certificate of Conformity	The certificate of conformity issued by a CAB to a TSP shall contain references to this Circular, the accreditation scheme, and the certificate shall show conformity to Reg. (EU) 910/2014 and to the standard ETSI EN 319 401, without further specifications regarding the services which are the subject of the qualification, which remain the final responsibility of AgID.
Audit timeframe	§ 7.4.2 of the standard ETSI EN 319_403 is applicable. The CAB shall adopt a basic audit times equal to the double time foreseen from a calculation deriving from ISO/IEC 27006:2015, with no possibility of reduction except if there is a valid ISO/IEC 27001:2013 certification, issued under accreditation by the same CAB, that already covering the typical range of activities of the TSP. In such cases there can be a maximum reduction of audit time of 30%. If the scope of certification only partly covers the typical activities of the TSP the maximum time reduction is 10%. For calculating the audit timeframe, for a TSP with up to 25 staff involved in the specific processes which are the subject of the eIDAS evaluation, the first time band of the calculation table for audit times is applied, as set out in ISO/IEC 27001:2013. Stage 1 (ST1) and Stage 2 (ST2) activities, including the review of the system documentation, shall be conducted at the permanent locations of the applicant TSP and they cannot be done consecutively, but with an appropriate time interval for the implementation of the results of the audit. Similarly, the CAB shall prepare an audit plan in line with the evidence gathered during Stage 1. The audit plan shall, with respect to the necessary evaluations of the sampling to be done during Stage 2, be sent to the TSP after the completion of Stage 1. For every service undergoing evaluation two extra days will be added to the time previously fixed. On the date of publication of the present document, the services which can be certified by CABs and therefore accredited are those concerning Time Stamping and the Certification Authorities. Secondary/branch locations submitted to sampling – at least half a day, not including transfer times.

	Locations where there are HSMs in the TSP's infrastructure: at least two days for the verification of the structure and the installation at the first location; at least one additional day for each location where there is an HSM installed and managed similarly to the first one; at least two days if the installation is built by a different structure. This is to permit the verification of the applicable information security requirements (in the mainstream areas, regarding physical, logical and organizational characteristics). The presence of remote signature HSMs in the TSP's infrastructure or at external structures operating within the responsibility of the TSP but not declared, shall always be managed as a major NC. For organizations undertaking exclusively the tasks of a Registration Authority, the audit timeframe may be reduced by as much as 50% with respect to that of a TSP operating the complete processes of eIDAS services. The CAB shall evaluate the applicability of a reduction according to the sampling of the locations where the identification of users takes place, based on sampling in accordance with the requirements of the mandatory document IAF MD 01.
Composition of the audit team	The audit teams operating for each single TSP shall consist of two auditors with eIDAS competence and experts needed for completion of the coverage of all the necessary competences. In the annual surveillances not included in the eIDAS Regulation (therefore, not the renewals every two years), the audit team may consist of one auditor.
Annual surveillances not regulated by Reg. (EU) 2014/910 (eIDAS)	In cases of annual surveillances not foreseen by the eIDAS Regulation but provided for under § 7.9 of the accreditation standards UNI CEI EN ISO/IEC 17065:2012 and ETSI EN 319_403, the report shall be managed in the same way as for the other regulated assessments, apart from specifying in the contractual documents with the QTSPs, that it is not necessary to send the report to AgID unless there is a specific request from the AgID itself. For the calculation of the duration of the non-regulated surveillances shall apply the criteria for assessments of the ISMS scheme, bearing in mind that it will take up at least 1/3 of the time usually needed for initial assessments and for the renewal.
Renewal audit every two years	The two-years renewal audit can have a 20% time reduction on the initial audit, if the same CAB conducts the process. If the TSP changes CAB, the audit shall be performed with 100% of the time of an initial audit. The eventual reduction of 20% of the audit time, permitted in the case indicated above, has no effect in the calculation of the surveillance time.
Changes to the infrastructure of the TSP	CABs shall contractually require the TSP to communicate any changes to their infrastructure or processes. When this occurs, the CABs shall evaluate the impact of such changes, brought by the TSPs, on their infrastructure or on the outsourcing of critical processes for services managed according to the requirements of the eIDAS Regulation. The CABs shall evaluate if such changes also regard the revisions of the TSP Practice Statements and/or of the SOA 27001. If the TSP has not autonomously prepared a risk analysis and subsequent planning process for the management of change, the CAB shall record a major NC. A significant change means a change to the infrastructure network having an impact on the service or information security, as well as changes to security policies and the technical modalities of their application. It could also mean modifications to the organizational set-up of the management system, a variation of the

	SOA or of the TSP Practice Statement, the substitution of an HMS providing for a different level of certification of security of the structure, or the elimination of organizational roles that affect security etc. Factors not considered as significant changes include normal staff turnover, normal maintenance operations involving also the substitution of staff, or the revision of a risk analysis if this does not involve changes in the application of operative controls or in the planning of processes. It is necessary to specify to the TSPs that, in cases of doubt, it is always better to ask the CAB and to record such communication. Failure to communicate changes which have a direct impact on eIDAS services and/or information security infrastructure supporting this service, is to be considered a major NC and shall be treated in a formal evaluation with records on the report, if such changes may cause a breach of security in the period between the application of these changes and the date of the audit being undertaken. The TSP shall actively collaborate with these analyses. In serious cases, given the objective responsibility of the CAB with respect to ACCREDIA and with the AgID, the CAB shall inform ACCREDIA in order to receive specific instructions. Failures of information security which could compromise or could have compromised services shall always be classified as major NCs.
Transfers of certification	Transfers of certification shall be guaranteed only after a review of the entire dossier (previous reports going back at least two years) prepared by the receiving CAB, with an inspection of at least two working days at the TSP's head office and one day at each secondary/branch location where an HSM device is in use. In cases of certification where any NCs have been raised within the last two-year period against the certification requirements, the inspection at the TSP shall have a duration not inferior to the duration of a non-regulated surveillance in order to verify the effectiveness of the corrective actions implemented. The receiving CAB may take over the evaluation activities, in the ambit of validity of the existing certificate, only after it has approved its certification.
Insurance policy	During the validity of the contract and, in particular, during Stage 1, the CAB shall verify the maximum level of civil liability of its policy with respect to its clients. An adequate policy shall be taken out for this level of responsibility, taking into account maximum possible combined losses for an occurrence related to potential disruption of services and the number of clients with a declared transaction value. The CAB shall obtain for itself its insurance or asset cover, which is compatible with the maximum risk level.
Additional evaluations	A CAB certifying a TSP for AgID qualification shall be available for additional evaluations required by AgID, cost met by the TSP, for any further evaluation activities necessary.
Presence of ACCREDIA or of AgID personnel	The CAB shall indicate in its regulation for the eIDAS scheme that, apart from ACCREDIA staff designated to perform evaluations at its location, it also accepts the presence of AgID observers. In the regulation for the eIDAS scheme, which shall be signed with contractual value, by the clients of the TSP, it shall be clearly stated that ACCREDIA and eIDAS observers may intervene as such at all stages and all locations during the audit of conformity to the standards applicable to the scheme.
FAQ and meetings concerning the scope	From June 2016, in the reserved area of ACCREDIA's website for assessors, there is a page for the most frequently asked or most

	significant questions deriving from the work experience gained by CABs' audit teams. ACCREDIA and AgID shall be required, in accordance with a frequency to be agreed between them, to hold meetings for coordination and clarification regarding applicative aspects of the present scheme, which are not clear in the initial phase of accreditation.
TSPs with essential processes for outsourced or fully outsourced services managed in conformity with the eIDAS Regulation.	The CAB shall carry out evaluations at these operators taking into account the fact that the essential processes for services in accordance with the eIDAS Regulation (not support processes) shall be performed by QTSPs. For support processes we mean a process which does not have a direct impact on the service provided in accordance with the eIDAS Regulation. Using outsourcing modalities for the evaluation of TSPs performing such services, the CAB shall evaluate if "outsourcee" activities qualify as QTSPs (a qualification obtained in accordance with the eIDAS Regulation). In such cases of outsourced processes at other QTSPs, the evaluation shall be performed only against ETSI EN 319_401 and the modalities adopted to assure the control of outsourced processes. The same is applicable for full outsourcing process controls. In cases of QTSPs which allocate one or more HSMs at one or more clients, the QTSP shall ensure adequate operative monitoring and control criteria of such structures, ensuring the right to perform audits and authorized access for the CAB's auditors and for AgID and ACCREDIA observers. Outsourcing of essential services (e.g. HSM management, database of CRL withdrawals management, management of the Registration Authority) is not allowed to be performed by operators who are not qualified (non-QTSP)

With kind regards

Director of the Dept. of Certification and Inspection
Dr. Emanuele Riva