CIRCOLARE TECNICA Prot. DC2023OC050 **DATA** Milano, 19-06-2023

A tutti gli Organismi di certificazione accreditati/accreditandi PRD - eIDAS

Alle Associazioni degli Organismi di valutazione della conformità

A tutti gli Ispettori/Esperti del Dipartimento DC

Loro sedi

OGGETTO **Dipartimento Certificazione e Ispezione**

Circolare tecnica DC N° 28/2023 - Disposizioni riguardanti l'aggiornamento dello schema eIDAS a fronte dello sviluppo della normativa tecnica ETSI, della estensione delle attività operative svolte dagli OdC, dell'esperienza maturata nel settore e delle risultanze della vigilanza condotta da AGID e dell'attivazione dei servizio di recapito certificato e QREM.

La presente Circolare annulla e sostituisce la Circolare Tecnica N. 5/2020 Rev.02.

1. PREMESSA

Le norme riportate nel presente documento sono da intendersi tutte nella versione più recente e applicabile, salvo specifiche indicazioni.

2. CONTESTO

La presente circolare è stata predisposta al fine di dare chiare indicazioni agli OdC sia dei requisiti ai quali attenersi ai fini della richiesta e mantenimento dell'Accreditamento nello schema eIDAS, sia per fornire chiare indicazioni normative, per come indicate dall'Autorità Competente, sulle responsabilità e sulle attese nei confronti loro e delle organizzazioni da loro certificate.

I servizi fiduciari eIDAS sono un elemento sostanziale a supporto dello sviluppo del mercato nella UE e nei Paesi che intendono essere nostri partner, pertanto, i servizi fiduciari definiti dal Regolamento eIDAS, così come quelli nazionali, debbono essere considerati strategici per lo sviluppo economico e sociale della stessa UE e del mercato domestico.

A questo fine le infrastrutture fisiche, logiche e organizzative a supporto dei servizi fiduciari eIDAS, per come certificate, debbono garantire non soltanto l'esistenza ed efficacia di tali servizi fiduciari, ma soprattutto la loro affidabilità in termini di continuità operativa, capacità di risposta al mercato e di massima resilienza nei confronti delle possibili minacce e pericoli interni ed esterni, sia rivolti alle stesse infrastrutture, sia rivolti alle dimensioni del ciberspazio nelle quali i relativi servizi fiduciari sono erogati.

SEDE LEGALE
Via Guglielmo Saliceto, 7/9
00161 Roma
T +39 06 8440991
F +39 06 8841199
accredia.it / info@accredia.it
C.F. / P. IVA 10566361001

SEDE OPERATIVA E AMMINISTRATIVA
Via Tonale, 26
20125 Milano
T +39 02 2100961
F +39 02 21009637
milano@accredia.it

3. VALENZA DELL'ACCREDITAMENTO

L'accreditamento rilasciato da ACCREDIA è valido per garantire la conformità degli Organismi di Certificazione (OdC) ai requisiti delle Norme UNI CEI EN ISO/IEC 17065:2012 integrata dalla Norma ETSI EN 319 403-1.

L'accreditamento avverrà per tutti i servizi fiduciari previsti dal Regolamento eIDAS, per i quali l'OdC avrà fatto richiesta e ottenuto il relativo riconoscimento nel Certificato di Accreditamento.

In occasione delle attivazioni di processi di valutazione su nuovi servizi fiduciari non già valutati in sede di verifica iniziale e non ancora riportati nel Certificato di Accreditamento, l'OdC dovrà avvisare con almeno sessanta giorni di anticipo l'ufficio tecnico di ACCREDIA di tale attivazione, al fine di consentire l'analisi di eventuali modifiche documentali e l'effettuazione di specifiche verifiche in accompagnamento.

ACCREDIA valuterà la congruità e conformità della documentazione di sistema che sarà presentata sia in fase di Accreditamento iniziale allo schema eIDAS, sia quando i singoli Organismi di Certificazione presenteranno specifica richiesta di estensione dell'accreditamento a ulteriori servizi fiduciari previsti dal Regolamento in parola.

4. GESTIONE DI RICHIESTE SPECIFICHE DEGLI ORGANISMI

L'accreditamento di prodotto concesso agli OdC è regolato da una specifica convenzione e dai Regolamenti ACCREDIA RG-01, RG-01-03 e RG-09, nonché, per i servizi fiduciari eIDAS, dalla presente Circolare. Eventuali servizi definiti a livello nazionale saranno soggetti a specifiche integrazioni o quanto previsto nella parte restante del presente paragrafo.

Nel caso in cui l'offerta dell'organismo ai TSP dovesse prevedere requisiti aggiuntivi rispetto alla presente circolare è necessario che ogni eccezione e/o ampliamento debba essere valutata con ACCREDIA prima che sia offerta ai clienti degli OdC e resa operativa in modo che possa essere, se del caso, proposta come possibilità a tutti gli OdC accreditati per il medesimo schema, evitando così squilibri sul mercato.

In tal caso saranno fornite comunicazioni specifiche a tutti gli OdC interessati dal medesimo accreditamento come nel caso, ad esempio di estensioni in altri paesi UE e non (apertura diretta del QTSP nel paese, utilizzo di una RA locale o di una CA locale come appoggio ecc.), valutazione prassi operative per i nuovi mercati emergenti (USA e Sud America su tutti), e relativi comportamenti, scopi di certificato che riportino alcune procedure richieste dai mercati europei ed approvate/richieste dalla autorità locali.

5. REGOLE PER L'ACCREDITAMENTO

1	Regole per l'accreditamento	Valgono i prerequisiti previsti dal RG-01 ed RG-01-03 per la concessione dell'accreditamento ed estensione PRD. Le verifiche in accompagnamento possono essere selezionate da ACCREDIA in base ai servizi che l'OdC richiederà di poter certificare sotto accreditamento.
2	Organismi di Certificazione titolati a chiedere l'estensione del proprio	Per richiedere l'accreditamento per lo schema "eIDAS", gli Organismi di Certificazione debbono essere già accreditati per lo schema PRD, a fronte della Norma UNI CEI EN ISO/IEC 17065 e per lo schema SSI, a fronte della Norma

	accreditamento allo schema "eIDAS"	UNI CEI EN ISO/IEC 17021-1 e della norma UNI CEI EN ISO/IEC 27006:2021 L'accreditamento sarà rilasciato come estensione dello schema PRD, con riferimento alla Norma ETSI EN 319 403-1.	
3	Domanda di estensione	La domanda di estensione dell'accreditamento deve essere presentata dagli Organismi di Certificazione titolati a farlo, utilizzando i moduli DA-00 e DA-01, disponibili sul sito web di ACCREDIA, corredati dalla documentazione indicata dai citati moduli e da quella più avanti indicata in questo stesso documento.	
4	Tutte le norme si intendono applicabili per le parti corrispondenti ai servizi erogati dai QTSP oggetto della certificazione	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
		ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
		ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
		ETSI TR 119 411-4	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2 (**da tenere aggiornata rispetto agli standard più recenti. A cura dei CAB)**
		ETSI EN 319 421 e 422	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
		ETSI EN 319 412-xx	Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

		Electronic Signatures and Infrastructures (ESI);
	ETSI EN 319 403-1	Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers
		Electronic Signatures and Infrastructures (ESI);
	ETSI EN TS 119 403-2	Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates
		Electronic Signatures and Infrastructures (ESI);
	ETSI EN TS 119 403-3	Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers
		Electronic Signatures and Infrastructures (ESI);
	ETSI TS 119 511	Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
		Electronic Signatures and Infrastructures (ESI)
	ETSI EN 319 521	Policy and security requirements for Electronic Registered Delivery Service Providers
		Electronic Signatures and Infrastructures (ESI)
	ETSI EN 319 531	Policy and security requirements for Registered Electronic Mail Service Providers
	ETSI EN 319 522-xx	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services;
	ETSI EN 319 532-xx	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services;

		ETSI TS 119 441	Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services
		ETSI EN 319 102-1	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
		ETSI TS 119 612	Electronic Signatures and Infrastructures (ESI); Trusted Lists
		ETSI TS 119 615	Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists
		ETSI TS 119 461	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
		Tutte le norme si intendono applicabili per le parti corrispondenti ai servizi erogati dai QTSP oggetto della certificazione.	
5	Competenze generali del personale degli OdC che opera nello schema	Le competenze del personale degli OdC che opera a vario titolo nello schema, incluso il personale che svolge attività commerciale ed il personale incaricato dell'attività di delibera, debbono essere conformi ai requisiti della Norma ETSI EN 319 403-1 al § 6. Si richiama l'attenzione sulla responsabilità oggettiva dell'OdC circa la gestione della competenza del personale coinvolto nel processo di audit (§6.1.2) con riferimento particolare alle competenze specifiche del riesame della domanda, degli audit, del riesame e della delibera.	

6. ITER DI ACCREDITAMENTO/ESTENSIONE

1	OdC accreditato a fronte della ISO/IEC 17065 e della UNI CEI EN ISO/IEC 17021-1 e ISO/IEC 27006	Presentazione della domanda di estensione dello Accreditamento ai fini eIDAS. • Esame documentale 1 gg/u da remoto. • Verifica ispettiva presso la sede dell'organismo della durata di 2 gg/u. • Accompagnamento di durata variabile, a seconda della articolazione della verifica che l'OdC deve condurre, che sarà valutato di volta in volta dallo ufficio tecnico di ACCREDIA. Gli accompagnamenti dovranno essere in presenza a meno che l'analisi di fattibilità, a cura dell'ufficio tecnico, riveli l'impossibilità di tale scelta.
2	OdC accreditato per lo schema Sistemi di Gestione – SSI, ma non accreditato secondo la Norma UNI CEI EN ISO/IEC 17065:2012 – Schema PRD	L' OdC deve presentare domanda di accreditamento alla ISO/IEC 17065 al fine del rilascio di certificazioni di servizio/processo. • Esame documentale della durata di 1 giornata da remoto. • Verifica ispettiva presso la sede OdC della durata di 4 gg/u e uno o più Accompagnamenti, di durata variabile, a seconda della articolazione delle verifiche che l'OdC deve condurre.
3	OdC accreditato per lo schema PRD, ma non accreditato secondo lo schema SSI	È necessario presentare domanda di accreditamento, per lo schema SSI, secondo le prescrizioni riportate nei regolamenti di ACCREDIA. Una volta ottenuto l'Accreditamento a fronte dello schema SSI, dovranno essere maturati almeno 12 mesi di esperienza operativa nella gestione di certificazioni che coprano servizi assimilabili a quelli dei TSP, prima di poter fare domanda di Accreditamento eIDAS.

7. REGOLE SPECIFICHE DI ACCREDITAMENTO PER LO SCHEMA EIDAS (REGOLAMENTO (UE) N°2014/910)

1	Esame documentale	Devono essere presentati ad ACCREDIA i documenti di sistema che evidenziano la conformità alla Norma ETSI EN 319 403-1. Risulterà accettabile anche un unico regolamento interno prodotto per lo specifico schema, che dovrà indicare quali documenti interni dell'OdC, facenti parte della documentazione di sistema, siano interessati dalle varianti richieste dalla Norma ETSI citata, e per ogni requisito applicabile, quali le modifiche applicabili, per garantire la conformità alla ETSI EN 319 403-1. L'OdC deve produrre un documento di sistema che descriva il processo di valutazione e decisionale per lo specifico schema.

		Le Check List da utilizzare durante gli Audit di Conformità dei QTSP, o aspiranti tali, sono quella allegata ad ETSI TR 119 411-4 oltre a quelle specifiche per gli altri servizi non coperti da tale TR.
2	Riferimenti	Per i documenti di riferimento vedi allegato.
3	Programmazione, Pianificazione ed esecuzione degli Audit da parte degli OdC	L'obiettivo degli OdC è quello di riscontrare, da parte dei TSP, sia la conformità ai requisiti applicabili, derivanti dalle Norme ISO/IEC 27001 e da tutte le Norme ETSI applicabili e ulteriori documenti indicati dalle Autorità Competenti, come nel caso dei servizi QREM, sia quello di riscontrare l'effettiva operatività continuativa dei servizi oggetto di certificazione, ivi compresa la affidabilità e predisposizioni efficaci e testate di continuità operativa e recupero da situazioni di danno catastrofale (cosiddetto Disaster Recovery). L'OdC dovrà assicurare, attraverso gli audit condotti e le analisi dei rapporti, che l'infrastruttura e i servizi erogati siano intrinsecamente sicuri, progettati con criteri orientati alla sicurezza delle informazioni e cybersicurezza e che i servizi fiduciari siano erogati tramite infrastrutture i cui elementi a livello fisico, logico e organizzativo siano tali da consentire il più alto livello di resilienza e capacità di risposta alle possibili minacce, sia interne, sia esterne. L'OdC dovrà garantire che i test di VA-PT siano svolti su "superfici" di attacco credibili e a fronte di una valutazione tecnica documentata e coerente col manuale di sicurezza dello stesso TSP. L'OdC dovrà garantire che i risultati delle analisi di sicurezza (valutazione dei rischi, test di VA e test di PT) trovino una risposta immediata e commisurata al livello delle criticità evidenziate. Inoltre, valgono i seguenti requisiti: 1. durante gli Audit eIDAS, gli Organismi di Certificazione dovranno sincerarsi che per la segnalazione degli incidenti all'Autorità di vigilanza (AgID) sia utilizzata la modulistica prevista dalla stessa (per l'Italia quella presente sul sito di AgID, all'indirizzo QTSP - Notifiche ex art.19 Regolamento eIDAS) ; 2. per la terminazione dei servizi qualificati, dovranno essere adottati i requisiti della Linea Guida di ENISA: "**Guidelines on Termination of Qualified Trust Services",** pubblicata nel Dicembre 2017 Guidelines on Termination of Qualified Trust Services — ENISA (europa.eu); 3. prevedere contrattualmente la necessità di incrementare i tempi di Audit di sorveglianza, al fine di valutare la

		chiusura e l'efficacia di tutte le risultanze di audit registrate negli audit precedenti. Inoltre, dovranno essere valutati i requisiti applicabili a fronte di criteri di campionamento prioritari, che l'OdC definirà sulla base delle analisi dei rapporti di audit precedenti; 4. il Piano di Audit dovrà essere concepito come il "progetto" delle attività da svolgere in campo, tenendo conto dei processi aziendali, delle infrastrutture e dei requisiti di sicurezza e di operatività dei quali deve essere garantita l'esistenza ed efficacia. Di seguito un elenco non esaustivo di tali criteri: a. chiusura NC, se applicabile; b. nuovi servizi e/o variazione dei servizi già erogati, se applicabile (Change management); c. valutazione delle prestazioni dei servizi oggetto di certificazione (efficacia e capacità operativa); d. nuove revisioni degli standard, se applicabile; e. aggiornamenti del contesto, dell'analisi di rischio (a fronte di incidenti, variazioni nell'infrastruttura IT e/o degli applicativi ecc.), dei contratti di outsourcing, del top management; f. esito dei processi di Vulnerability Assessment/Penetration Test, e stato di completamento dei relativi Piani di Correzione; g. segnalazione e gestione degli Incidenti di sicurezza. h. varie applicabili al contesto specifico e ritenute imprescindibili; 5. la pianificazione degli audit in generale, e per quelli di sorveglianza in particolare, deve lasciare evidenza dei razionali adottati per definire il campionamento. Tali registrazioni debbono essere messe a disposizione di ACCREDIA sia durante le verifiche in sede, sia durante le verifiche in accompagnamento; 6. per i servizi di emissione di certificati qualificati legati a schemi internazionali che richiedono audit completi annuali (es. servizi WEB) si applica quanto previsto dalla specifica TS 119 403-2.
4	Elementi aggiuntivi per i servizi di recapito certificato, conservazione e validazione	1. Per i servizi di recapito si applicano le norme ETSI EN 319 521 e, ove applicabile in base alle caratteristiche del servizio fiduciario, ETSI EN 319 531. Eventuali deroghe devono essere approvate per ogni caso specifico da ACCREDIA; 2. le norme ETSI EN 319 522 (tutte le parti) e ETSI EN 319 532 (tutte le parti) sono applicabili secondo il tipo di servizio fornito dal prestatore. Ove il servizio del prestatore abbia **caratteristiche funzionali specifiche non conformi** alle norme ETSI

		EN 319 522/ETSI EN 319 532 in vigore, si applicano le seguenti regole aggiuntive: a. è compito del prestatore fornire tutti i razionali che dimostrino l'equivalenza in termini di requisiti del Regolamento ai fini della valutazione di conformità; b. specifiche indicazioni emesse o approvate da un'autorità nazionale di vigilanza possono costituire elemento valido di cui tener conto per valutare l'equivalenza; c. i razionali con cui è valutata l'equivalenza devono essere documentati e possono essere oggetto di audit da parte di ACCREDIA ai fini della conferma dell'accreditamento dell'organismo; d. il numero di giornate richiesto sarà valutato caso per caso ma non potrà essere inferiore a quello previsto da questa circolare; 3. per i servizi di conservazione di firme e sigilli elettronici qualificati si dovrà utilizzare la specifica ETSI TS 119 511. Tale specifica è applicabile in generale anche alla conservazione dei dati mediante tecnologie basate sulla firma digitale. In caso di richieste di certificazione ulteriori rispetto alla conservazione di firme e sigilli elettronici qualificati e basate sulla TS 119 511 vale quanto indicato al paragrafo 4; 4. per i servizi di validazione di firme e sigilli elettronici qualificati si applica la specifica ETSI TS 119 441 e la norma EN 319 102-1 e – se applicabili in base al tipo di servizio – le specifiche TS 119 102-1 (che aggiorna la EN 319 102-1) e TS 119 102-2. Il servizio deve utilizzare correttamente e validare gli elenchi di fiducia basati sulle specifiche TS 119 612 e TS 119 615 nonché validare correttamente i certificati dei prestatori in esse contenuti; 5. per i servizi di recapito certificato qualificato REM vedasi AGID - Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS n. 910/2014 – Criteri di adozione standard ETSI – REM Policy-IT Versione 1.0 - 11.8.2022 e le ulteriori guide e regolamenti dell'Autorità citata che saranno emessi nel futuro.
5	Procedura commerciale	L'OdC deve produrre un documento di sistema che integri la già esistente procedura di acquisizione dei contratti, con particolare attenzione alle fasi di analisi dei servizi per i quali i TSP possono chiedere la certificazione. Tale documento di sistema deve prevedere anche la fase di riesame dell'offerta, anche per verificare il possesso delle

		specifiche competenze per operare nell'ambito dei servizi richiesti. L'esito di questa analisi dovrà dare evidenza della fattibilità dell'attività da programmare (tempi, competenze degli Auditor e possibile esigenza di Esperti).
6	Valutazioni di robustezza delle infrastrutture "cloud"	In merito all'uso di infrastrutture "cloud", il TSP deve: 1. dare evidenza della capacità di reale "controllo operativo" di tali servizi e della garanzia dell'ubicazione dell'infrastruttura tecnologica di supporto (server fisici a supporto di quelli virtualizzati, infrastrutture di "storage" e di "backup", di trasmissione dei dati, di BC e DR) consentite solo all'interno dell'UE; 2. garantire la trasmissione dei dati in modalità sicura attraverso qualsiasi canale adottato; 3. dare evidenza anche dell'esistenza del diritto contrattuale di svolgere attività di audit interno su tali servizi che preveda la possibilità di accesso anche del personale dell'OdC, di ACCREDIA e dell'Autorità di vigilanza. Vedi punto 4; 4. la certificazione del fornitore di servizi "cloud" rilasciata sotto accreditamento, nel circuito EA/MLA, che copra il perimetro fisico, logico e organizzativo riferiti ai processi del TSP, a fronte della Norma ISO/IEC 27001, corroborata dall'utilizzo della Linea Guida ISO 27017, per il perimetro sottostante la realizzazione dei servizi cloud, comprese le linee di comunicazione punto-punto, sarà considerata una modalità accettabile per considerare il servizio conforme. L'OdC dovrà verificare l'esistenza di una valutazione dei rischi che integri sia il perimetro della infrastruttura tipica del TSP, sia il perimetro costituito dagli elementi di ciberspazio (comunicazione in senso lato) e da quelli del Cloud Service Provider; 5. assicurarsi che le infrastrutture fisiche di elaborazione e memorizzazione dei dati (compresi i backup e altre risorse di BC e DR) risiedano all'interno del territorio dell'UE; 6. la gestione dei dati personali sia conforme ai requisiti del GDPR (Regolamento 679/2016), vuoi che la stessa avvenga tramite l'infrastruttura proprietaria, vuoi che avvenga tramite servizi "cloud".
7	Valutazioni di robustezza del sistema IT e delle terze parti coinvolte nell'erogazione del servizio	**VA/PT** L'OdC verifica l'esistenza e l'accettabilità dei servizi di VA (Vulnerability Assessment) e PT (Penetration Test), garantendo che gli stessi siano estesi a un perimetro di sicurezza, che consenta di dare garanzia di resilienza su tutta l'infrastruttura fisica, logica e organizzativa comunque

correlata o correlabile coi servizi per i quali è richiesta la certificazione.
Ciò significa che non è sufficiente lo svolgimento di un VA-PT sulla superficie rappresentata dalla esposizione delle sole macchine, software e luoghi fisici tramite i quali si offrono i servizi oggetto di certificazione, ma che devono essere ricomprese anche le interfacce verso altre parti dell'infrastruttura connessa, a quella che serve a erogare i servizi oggetto di certificazione.
Inoltre, l'analisi documentata sulla esigenza di VA-PT deve tener conto di tutte le possibili superfici di attacco, ivi comprese le interfacce con le sezioni dell'infrastruttura del TSP deputate ad altri servizi, la gestione degli strati TCP/IP, le API, le librerie interne ed esterne, i SW, in particolare i cosiddetti "open source", gli ambienti cloud etc.
Per i TSP aventi almeno una sede in Italia, i Laboratori incaricati dei controlli operativi relativi ai processi di VA devono essere accreditati secondo la Norma ISO/IEC 17025.
Per i TSP aventi sedi negli altri Paesi della UE i test di VA-PT dovranno essere svolti con laboratori accreditate ove disponibili, ovvero da fornitori che forniscano almeno le seguenti evidenze:

- la chiara individuazione e diligente applicazione dei requisiti inerenti alla metodologia di valutazione tecnica adottata, che richiami, preferibilmente, l'applicazione dei requisiti ISO/IEC 27008;
- la garanzia della specifica competenza formale (quali qualifiche, da chi rilasciate, quale esperienza nel settore) delle Risorse Umane addette a tali test;
- la qualifica (certificazione in gergo IT) dei SW utilizzati (almeno la garanzia che le versioni siano compatibili e aggiornate ai rilasci dei SO e delle applicazioni da analizzare del TSP che svolge servizi di conservazione), nonché costantemente aggiornati con riferimento alle banche dati ufficiali sulle Vulnerabilità note (es. banche dati per singolo elemento di configurazione, curate dagli CSIRT nazionali o altre fonti qualificate come il MITRE (https://cve.mitre.org/cve/).

La valutazione e qualifica del LAB/fornitori è sempre di pertinenza del TSP.
Le evidenze di tale processo di qualifica sono oggetto di valutazione nell'ambito del processo di audit da parte dell'OdC.
Se il TSP avrà delegato l'OdC alla individuazione del Laboratorio di VA-PT, i criteri adottati dall'OdC saranno vagliati in sede di verifica da parte di ACCREDIA.

		L'OdC dovrà richiedere se sia adottato un processo formale e/o una procedura documentata per la gestione del processo di VA/PT e valutarne l'efficacia in termini di: • verifica della comprensione del report della valutazione del laboratorio mediante atto formale; • valutazione dell'impatto delle vulnerabilità riscontrate nel rapporto in relazione ai tempi di remediation; • definizione di un piano di correzione delle risultanze, in funzione del livello di criticità, per come descritto nel rapporto del LAB. L'OdC terrà conto del razionale adottato dal TSP nella pianificazione di risoluzione delle vulnerabilità a fronte delle criticità riscontrate, con riferimento alle esigenze di robustezza e resilienza dell'infrastruttura e di copertura assicurativa in essere. Nel caso in cui le vulnerabilità riscontrate e classificate come critiche non siano prontamente rimosse e/o il piano di correzione risulti inattuato nei tempi previsti, determinando così un potenziale vulnus per la sicurezza delle informazioni, che possano compromettere o che possano aver compromesso i servizi l'OdC deve emettere delle NC Maggiori, riferite sia alla gestione delle carenze riscontrate, sia all'inadeguato impegno (commitment) della Direzione. Contestualmente, l'OdC deve provvedere a iniziare il processo di sospensione del TSP, che – in assenza di azioni di correzione tempestive – dovrà essere portato a termine entro non oltre un mese dalla apertura della stessa NC maggiore.
8	Rapporto di audit	Vale quanto indicato al § 7.4 della ETSI EN 319 403-1 quando applicabile e non in contrasto con la presente circolare, che prevale. I rapporti di audit debbono essere redatti in conformità alla specifica TS 119 403-3. Oltre ai requisiti sopra indicati, l'OdC deve predisporre un formato per il rapporto di audit, che consenta di avere evidenza della completezza e della efficacia nella valutazione di tutti i requisiti applicabili e dei singoli approfondimenti e dei test sui controlli operativi del TSP effettuati, integrando nello stesso rapporto le liste di riscontro ETSI correlate con le Norme di valutazione. Il processo di valutazione dell'OdC deve coprire i servizi che il TSP ha dichiarato all'Autorità di vigilanza con particolare focus sull'efficacia, affidabilità e resilienza alle minacce degli stessi, anche con riferimento alle possibili terze parti utilizzate per l'eventuale "outsourcing" di alcuni dei processi dello stesso TSP. Dopo l'esecuzione del riesame interno allo stesso OdC, può essere deliberata la conformità al Regolamento eIDAS e quella dei servizi erogati a fronte delle Norme ETSI

applicabili e/o di altre Norme specificatamente individuate dall'Autorità di Vigilanza (AgID in Italia) o da EA o dalla Commissione Europea, per la verifica della conformità degli specifici servizi eIDAS (ad es. a seguito di atti di esecuzione della Commissione UE).
Nel rapporto di Audit, l'OdC deve indicare esplicitamente lo stato di conformità al presente schema di accreditamento, al Regolamento 910/2014 "eIDAS", in particolare a quanto riportato agli Articoli 13, 15, 19, 24, 28, 29, 30 e da 32 a 45 e agli Allegati, ove pertinenti con i servizi oggetto di certificazione e alla Norma ETSI EN 319 401, ove tale conformità sia stata riscontrata. Tale dicitura deve essere presente anche nei Certificati di Conformità.
L'OdC dovrà registrare all'interno del rapporto di audit le evidenze che dimostrino la puntuale applicazione delle procedure dichiarate dal TSP nella documentazione di sistema.

<u>Audit interni</u>

L'OdC deve includere nel rapporto di audit del TSP una valutazione degli audit interni che dia evidenza:

- della corretta applicazione della classificazione dei rilievi riscontrati nel corso delle attività di Audit Interno;
- della qualifica degli Auditor Interni e del relativo mantenimento;
- della garanzia di indipendenza degli Auditor Interni, rispetto ai processi valutati;
- della programmazione del ciclo di Audit Interno almeno biennale, sviluppata sulla base delle evidenze emerse dalla valutazione dei rischi dei processi del TSP, quindi basata sull'esigenza di testare i controlli operativi realizzati per mitigare tali rischi. La programmazione dovrà tenere conto delle risultanze degli Audit Interni degli ultimi due anni, dell'esigenza di monitorare l'efficacia di precedenti azioni correttive e di analogo esito della gestione delle risultanze delle verifiche di ACCREDIA e della Vigilanza di AgID;
- dei criteri di campionamento dei processi critici, ad esempio quelli svolti dalle RA tenendo conto della numerosità di tali entità, o per raggruppamento in cluster definiti in base a criteri specifici (es. gestione di QSCD di firma remota per uno specifico cliente), secondo i criteri della norma UNI 2859;
- con riferimento ai processi di identificazione, dovranno essere previsti dei test svolti con tecniche di mistery auditing e dei test di ricostruzione a posteriori dei processi di identificazione, a garanzia della completa affidabilità di questo processo, tenendo ben presente che si tratta del processo a maggior livello di rischio e

di importanza gestito dagli stessi TSP. Nel caso in cui l'attività di audit in incognito non sia fattibile (ad esempio nel caso in cui servizi di firma vengano erogati solo a soggetti dipendenti, del QTSP o del RAO, o facenti parte di associazione di categoria), il QTSP dovrà dimostrare di aver effettuato dei test di ricostruzione a posteriori dei processi di identificazione, dell'affidamento a terze parti di processi critici o che possano rappresentare criticità per la sicurezza delle informazioni e cybersicurezza, in particolare ove sia interessata la sicurezza delle informazioni personali degli utenti – a vario titolo – dei servizi del TSP.

Valutazione dei rischi

L'OdC deve includere nel rapporto di audit del TSP o in un documento a questo collegato una valutazione dall'analisi di rischio del TSP a fronte dei servizi erogati e dei suoi risultati che dia evidenza come minimo:

- di un'analisi di scenario interno ed esterno, con particolare riferimento agli elementi riferibili alle superfici di attacco o che possono interagire con le stesse. A completamento di tale analisi sul contesto esterno e su quello interno, dovrà essere predisposta un'analisi "SWOT", con le relative valutazioni per la gestione dei punti di debolezza e delle minacce;
- l'analisi di scenario esterno dovrà contenere almeno la valutazione delle dinamiche delle minacce che possono impattare sul TSP;
- l'analisi di scenario interno dovrà contenere almeno la valutazione sullo stato delle VA e delle risultanze dei PT, la loro completezza rispetto alle superfici di attacco e le azioni pianificate per la loro gestione;
- la valutazione sull'aggiornamento delle competenze e delle modalità adottate dalla Direzione del TSP per creare consapevolezza tra le Risorse Umane dell'organizzazione a fronte delle esigenze di sicurezza;
- la valutazione dell'accettazione formale del rischio residuo da parte della direzione dello stesso TSP;
- la valutazione dell'adozione da parte del TSP di "best practice" per lo svolgimento della valutazione dei rischi come ad es. la Norma 27005 e, a livello sistemico, la ISO 31000;
- la valutazione delle criticità correlate alle interfacce e dipendenze con gli altri servizi infrastruttura IT – analisi di scenario e modifiche all'infrastruttura ICT – relazione con la 27001);
- la valutazione sulla corretta gestione delle credenziali di accesso ai sistemi;

- la valutazione sulla capacità di gestione degli incidenti, del loro riconoscimento e registrazione (ticketing) e della loro gestione, in particolare nel caso di potenziali "Data Breach", con riferimento alla procedura per la loro gestione;
- la valutazione della definizione di ciclo di sviluppo del SW, della gestione dei cambiamenti (SW compreso), della separazione dagli ambienti di test e di produzione;
- la valutazione della corretta mappatura degli asset del TSP,
- la valutazione della adozione di una procedura per la comunicazione, che tenga conto delle situazioni di emergenza, quali i cosiddetti "data breach";
- la valutazione delle esercitazioni per la verifica dell'efficacia delle soluzioni per la continuità operativa e ripristino dei sistemi dopo eventi catastrofali.

L'OdC deve adottare una modalità per sigillare in via informatica il rapporto sulla base del quale è stata effettuata la delibera, al fine di garantirne autenticità ed integrità nei confronti di terzi (l'uso di sigilli elettronici qualificati intestati all'OdC o di firme elettroniche qualificate intestate a soggetto formalmente incaricato dall'OdC si ritiene adeguato); quindi tale rapporto comprensivo di tutti i documenti di registrazione delle evidenze oggettive prodotti sul campo, deve essere trasmesso formalmente al TSP, che avrà cura di inviarlo tempestivamente all'Autorità di vigilanza di pertinenza del paese, per il prosieguo dell'iter di qualifica come QTSP o del suo mantenimento.

Una ulteriore modalità può essere quella dell'invio tramite PEC, purché l'indirizzo usato per l'invio risulti associato all'OdC nel registro imprese, o servizio di recapito elettronico certificato qualificato intestato all'OdC.

L' OdC non deve attendere le decisioni dell'Autorità di vigilanza ai fini della propria delibera di certificabilità (o meno) del TSP. Vale l'eccezione della certificazione del servizio QREM per QTSP che opera in Italia.

In questo caso l'OdC emetterà e consegnerà al TSP il proprio rapporto e, solo dopo aver ricevuto dall'autorità di vigilanza nazionale AgID l'evidenza dell'esistenza del Rapporto di Prova prodotto dal CNR sulla interoperabilità del servizio, provvederà alla delibera, per l'emissione del proprio certificato.

Ove il TSP adotti modifiche all'infrastruttura utilizzata per erogare il servizio QREM dovrà coordinarsi con AGID per la ripetizione del test di interoperabilità, dando evidenza all'OdC di questa fattispecie.

Il rapporto di audit, tra gli altri, dovrà dare evidenza della verifica eseguita su tutti i controlli operativi previsti dalla

		Norma ETSI EN 319 401, indicando le metriche adottate per il loro monitoraggio continuo da parte del TSP e l'efficacia di tali controlli (registrazioni in continuo e loro analisi, ove possibile). Nei rapporti di Audit saranno considerate accettabili solo le risultanze classificate come NC di tipo Maggiore o Minore, non è ammessa alcuna forma di indicazione per il miglioramento. Il rapporto di Audit dovrà essere integrato, o allegato, con il rapporto predisposto a fronte della Norma ISO/IEC 27001.
9	Certificato di Conformità	Il certificato di conformità rilasciato dagli Organismi di Certificazione ai TSP dovrà riportare: • i riferimenti a questa Circolare, quale schema di Accreditamento; • al Regolamento (UE) 910/2014 e alla Norma ETSI EN 319 401; • la conformità alle Norme relative ai Servizi oggetto di Certificazione e ai Servizi medesimi, compresi i Regolamenti o documenti assimilabili delle Autorità di Vigilanza (AgID in Italia). L'OdC avrà cura di ricordare al TSP di inviare tempestivamente il certificato di conformità e il rapporto di Audit all'Autorità di Vigilanza nazionale. Il certificato di accreditamento non riporta alcun settore IAF di accreditamento.
10	Tempistica per gli Audit	Vale quanto indicato al § 7.4.2 della Norma ETSI EN 319 403-1, considerando che il calcolo secondo l'Allegato B non potrà mai portare a tempi di audit inferiori a quanto richiesto dalla presente Circolare. L'OdC adotta il tempo di Audit di base almeno pari al doppio del tempo previsto dal calcolo derivante dall'applicazione della Norma ISO/IEC 27006, che potrà essere ridotto del 10% , nel caso di esistenza di una certificazione ISO/IEC 27001, rilasciata sotto accreditamento dal medesimo OdC, che copra già il dominio di attività tipiche del TSP e che sia stato condotto da Auditor qualificati eIDAS e per il quale non siano presenti NC per le quali non sia ancora stata gestita la chiusura e le verifica di efficacia. Si evince l'obbligatorietà della certificazione a fronte della 27001 secondo quanto stabilito da AGID Per il calcolo del tempo di audit, ad esempio, per una struttura del TSP fino a 25 dipendenti impegnati negli specifici processi oggetto della valutazione "eIDAS", si dovrà prendere in considerazione la prima fascia della tabella di calcolo del tempo di audit della citata ISO/IEC 27006:2015, raddoppiando tale tempo.

Sopra i 25 dipendenti il calcolo dei giorni uomo segue la tabella B.1 dello standard 27006, sempre raddoppiando i tempi ivi indicati. Il calcolo deve tenere conto anche del personale dei processi affidati all'esterno con le modalità dell'FTE.
Le attività di valutazione della documentazione di sistema possono essere condotte off site con una durata massima di 4 gg/u. L'attività deve concludersi con l'emissione di un rapporto sottoscritto dal cliente.
Il processo di valutazione iniziale non può essere condotto con modalità "back to back" o "incollato" a quello documentale. Il processo di valutazione iniziale dovrà essere condotto lasciando un tempo congruo per il recepimento delle risultanze di verifica.
Allo stesso modo, l'OdC dovrà predisporre un Piano di Audit congruo con le evidenze raccolte durante la fase di esame documentale; lo stesso Piano di Audit, a fronte delle necessarie attività da svolgere durante la fase di campionamento dei processi operativi, dovrà essere inviato al TSP successivamente alla chiusura della fase di esame documentale.
L'audit dovrà essere condotto presso la sede del TSP in presenza.
Per ogni servizio che sarà sottoposto a valutazione dovranno essere applicati 2 gg/u in aggiunta a quanto precedentemente indicato.
Per ogni sede aggiuntiva, rispetto a quella centrale del TSP, debbono essere previsti i seguenti tempi di audit:

- siti secondari sottoposti a campionamento – almeno 0,5 gg/u giornata;
- almeno 2 gg/u per la verifica di architettura e installazione presso il primo sito ove siano presenti dei QSCD (Qualified Secure Signature/Seal Creation Device - Dispositivi di cui all'Allegato II del Regolamento eIDAS);
- almeno 1 gg/u aggiuntivo per ogni sito ove sia presente un QSCD installato e gestito in modo analogo al primo;
- almeno 2 gg/u se l'installazione è avvenuta con un'architettura diversa. Ciò per verificare i requisiti di sicurezza delle informazioni applicabili (nei domini classici di tipo fisico, logico e organizzativo).

Tali tempi non sono comprensivi dei tempi di trasferimento.
Per gli Audit condotti sui servizi REM, il tempo di audit sopra indicato dovrà essere incrementato di almeno 8 (otto) giorni in caso di verifica iniziale o di rinnovo dello specifico servizio REM, e quattro per le sorveglianze.
Ove i servizi siano stati progettati con modalità di "outsourcing", utilizzando i processi di altri QTSP (già

qualificati dalle rispettive Autorità per REM), valgono le regole generali di Accreditamento eIDAS, con due giorni aggiuntivi, sia in fase iniziale, sia in sorveglianza, per l'analisi delle misure adottate dal TSP, per il monitoraggio di tale servizio in outsourcing.
L'emissione del Certificato di Conformità REM in caso di QTSP operante in Italia deve prendere in considerazione l'esistenza del rapporto di conformità (parere positivo di idoneità), per le esigenze di interoperabilità, che sarà rilasciato dal CNR. In tale contesto, in conformità ai requisiti della UNI CEI EN ISO/IEC 17065:2012, il CNR sarà da considerare alla stregua di un LAB che fornisce un Certificato di Conformità valido ai fini della Certificazione di PRD.
Con la pubblicazione della norma ETSI EN 319 403-1, è autorizzata la certificazione di specifici componenti di servizio fiduciario, come ad esempio il servizio di Registration Authority.
È evidente in ogni caso che un componente di un servizio fiduciario inserito in una trusted list deve dare evidenza di avere le caratteristiche che non mettano in dubbio l'affidabilità del servizio.
I componenti **HW** di un servizio trusted quindi debbono essere certificati secondo le normative stabilite a livello comunitario o nazionale, es. in Italia a fronte dei requisiti introdotti dal DPCM 30 ottobre 2003.
Le componenti **SW** di un servizio fiduciario (ove non soggette a certificazione ex. DPCM sopracitato), ovvero le componenti di analogo servizio di carattere organizzativo, debbono essere chiaramente identificate, sottoposte a valutazione sia in sede di ST1, sia in sede di ST2 e della successiva sorveglianza, per monitorarne la costante validità, per come stabilita contrattualmente e operativamente tra i due TSP che stipulano l'accordo di outsourcing. Se tali componenti sono operate da terze parti esterne, debbono essere già oggetto di certificazione del servizio del quale fanno parte, e di continua valutazione (comprese le necessarie sorveglianze) da parte di un altro OdC accreditato eIDAS, per il medesimo servizio, senza che siano vigenti rilievi che possano compromettere la fiducia sulle stesse. L'OdC richiederà al TSP, che intende avvalersi di tali componenti, l'evidenza delle pertinenti informazioni. Diversamente, tali componenti debbono essere sottoposte ad audit da parte dello OdC che svolge il processo di valutazione del TSP interessato.
Nell'utilizzo di componenti esterne, per la creazione di un servizio fiduciario, il TSP deve tener conto del livello di garanzia (assicurativa) che il TSP che esercisce la

		componente (o gruppo di componenti) riconosce ai fruitori dei propri servizi, salvo altro accordo contrattuale o altra copertura assicurativa garantita dal TSP, con chiaro riferimento all'uso di tali componenti. Gli OdC richiederanno ad ACCREDIA un parere scritto di fattibilità per ogni fattispecie di questo tipo che vorranno certificare, con riferimento allo specifico TSP/QTSP. Il numero di giornate allocato a tale processo di valutazione in campo deve essere congruente con la complessità del componente in questione e non essere inferiore a 2 (due) giornate. Per la compilazione dei rapporti di audit, stante il tempo di audit calcolato secondo i criteri sopra indicati, deve essere prevista l'allocazione del 10% di tale tempo in modalità "off-site", che sarà a disposizione del Lead Auditor, per la chiusura delle check-list applicabili. Tale allocazione di tempo "off-site" sarà quantificata con un minimo di un giorno e un massimo di due giorni di tempo di audit. Tale tempo di audit dovrà essere oggetto di fatturazione ai QTSP (o TSP in fase di certificazione iniziale).
11	Tempistica per il full outsourcing	Nel caso una CA richieda una estensione ad un altro servizio non compreso nel certificato è necessario prevedere: • 2 gg/u per la valutazione degli aspetti di sistema pertinenti al servizio che si intende certificare. Lo stesso tempo deve essere conteggiato nel caso si aggiungano più servizi nella stessa domanda; • 2 gg/u per ogni servizio che si intende aggiungere (affidabilità e sicurezza) Ove un QTSP operi con dei servizi in outsourcing allocati ad altri QTSP, il tempo di audit previsto per le attività di monitoraggio di tali "outsourcee" e per gli specifici servizi dati in outsourcing, deve essere eliso dal calcolo del tempo di audit complessivo. Esempio di **Full outsourcing** Nel caso di un QTSP (con 15 addetti), certificato ISO 27001 con identico OdC, in full outsourcing per un servizio di TIME STAMPING. il calcolo deve prevedere: – 10,00 gg/u per addetti 15 (inferiori a 25, quindi giorni della prima fascia della 27001); – 1,00 gg/u ossia il 10 % riduzione società certificata ISO 27001 (prevista estensione al perimetro servizi fiduciari prima di audit eIDAS solo se lo scopo della 27001 è orientato al full outsourcing) Sub totale = 9 gg/u – -2,70 gg/u ossia il 30 % riduzione per full outsourcing Sub totale = 6,30 gg/u + 2,00 gg/u giorni per marca temporale

		Totale 8,3 → 8,5 gg/u con riduzione 27001; 9 gg/u senza riduzione 27001.
12	Composizione dei Gruppi di Audit	I Gruppi di Audit chiamati a operare per ogni singolo TSP debbono essere composti da 2 (due) Auditor competenti eIDAS e dagli eventuali ESP necessari per completare la copertura delle competenze richieste al Gruppo di Audit. Nelle sorveglianze annuali che esulano dal Regolamento eIDAS (quindi, non i rinnovi biennali), il GdA può essere composto da un solo Auditor. Nel caso il piano di audit preveda che il gruppo di audit operi come un unicum (parti dell'Audit nelle quali i due membri del Team operano assieme) deve essere previsto un tempo di audit aggiuntivo a fronte di un razionale che affronti l'esigenza di ottimizzare il conseguimento degli obiettivi dello stesso Audit.
13	Sorveglianze annuali non regolamentate dal Regolamento (UE) n°2014/910 (eIDAS)	Nel caso delle sorveglianze annuali non previste dal Regolamento eIDAS, ma previste comunque al § 7.9 delle Norme di accreditamento UNI CEI EN 17065:2012 ed ETSI EN 319 403, il relativo rapporto deve essere gestito come nel caso degli audit regolamentati, salvo specificare nella documentazione contrattuale con i QTSP che non è richiesto l'invio all'Autorità di vigilanza, se non dietro specifica richiesta della stessa. Per il calcolo della durata degli audit di sorveglianza, dovrà essere allocato almeno 1/3 del tempo normalmente allocato nelle verifiche iniziale e di rinnovo biennale, aumentando tale durata in funzione delle attività aggiuntive da svolgere per verificare l'efficacia di eventuali azioni correttive derivanti dalle precedenti verifiche o dalle attività di VA-PT.
14	Verifiche di rinnovo biennali	**Cambio dell'ODC** Ove il TSP cambi OdC, la verifica di rinnovo deve essere condotta con il 100% del tempo di una verifica iniziale.
15	Modifiche all'infrastruttura/configurazione dei processi del TSP	**Modifiche alle proprie infrastrutture o configurazione dei processi** Gli OdC devono richiedere contrattualmente ai TSP di comunicare le eventuali modifiche alle proprie infrastrutture o alla configurazione dei processi (ETSI EN 319 403 §7.10). Ove tale situazione si realizzi, gli stessi OdC devono valutare l'impatto di tali modifiche apportate dai TSP alla propria infrastruttura o all'allocazione all'esterno di processi critici per i servizi gestiti a fronte dei requisiti del Regolamento "eIDAS", basando il proprio giudizio anche sulla valutazione dei rischi che il TSP avrà condotto a fronte del cambiamento. Gli OdC valutano se tali modifiche debbano riguardare anche le revisioni dei "TSP Practice Statements" e/o dello

"Statement of Applicability" (dichiarazione di applicabilità) previsto dalla 27001.
Ove il TSP non abbia già provveduto autonomamente, a fronte di una valutazione dei rischi e successivo processo di pianificazione del processo di corretta gestione del "Change Management", l'OdC registrerà una NC maggiore.
Per modifica significativa si deve intendere:

- una variazione di configurazione dell'infrastruttura di rete che abbia impatto sul servizio o sulla sicurezza delle informazioni;
- modifiche delle politiche di sicurezza e delle modalità tecniche per la loro applicazione;
- modifiche agli assetti organizzativi del sistema di gestione;
- una variazione del SOA o del TSP Practice Statement,
- la sostituzione di un QSCD che preveda un diverso livello di certificazione di sicurezza dell'apparato;
- l'eliminazione di posizioni organizzative che hanno impatto sulla sicurezza etc.

Non sono da considerare modifiche significative:

- il normale turnover del personale;
- le normali operazioni di manutenzione che prevedano anche sostituzione di componenti;
- le revisioni delle valutazioni dei rischi, ove non comportino variazioni nell'applicazione dei controlli operativi o nella progettazione dei processi.

NOTA 1
Nel dubbio il TSP è meglio chieda all'OdC e lasci traccia di tale comunicazione.
La mancata comunicazione di modifiche che abbiano un impatto diretto sui servizi "eIDAS" e/o sulla sicurezza delle informazioni dell'infrastruttura a supporto di tali servizi, è da considerare come NC
Maggiore con adeguata registrazione sul rapporto di verifica, se tali modifiche possano aver creato delle brecce di sicurezza nel periodo intercorrente dalla applicazione di tali modifiche sino alla data dell'audit in corso.
Il TSP dovrà collaborare attivamente a tale analisi.
In casi gravi, vista la responsabilità oggettiva dell'OdC nei confronti di ACCREDIA e dell'Autorità di vigilanza, lo stesso OdC dovrà fare una specifica segnalazione ad ACCREDIA per ricevere specifiche istruzioni di vigilanza.
Carenze inerenti alla sicurezza delle informazioni, che possano compromettere o che possano aver compromesso i servizi debbono essere sempre classificate come NC Maggiori.
NOTA 2
Nel caso di modifiche sostanziali ai servizi QREM, il TSP fornirà l'OdC anche l'evidenza del nuovo Rapporto di Prova per

		l'interoperabilità, con esito positivo, ai fini della continua validità del Certificato di Conformità.
16	Trasferimenti della certificazione	I trasferimenti delle certificazioni debbono essere garantiti solo dopo un riesame dell'intera pratica (precedenti rapporti di almeno un biennio) fatta dall'OdC subentrante, con un sopralluogo di almeno due giorni lavorativi presso la sede centrale del TSP e di un giorno (un solo Auditor) presso ogni sede secondaria ove viene gestito un QSCD. Solo ad esito positivo di tale attività, avendo riscontrato l'assenza di NC aperte e non gestite, l'OdC potrà deliberare il trasferimento. Nel caso di certificazioni ove siano state registrate delle non conformità nell'ultimo biennio a fronte dei requisiti di certificazione, il sopralluogo presso il TSP deve essere di durata non inferiore al tempo di una sorveglianza, anche al fine di verificare l'efficacia delle azioni correttive adottate dal QTSP. L'OdC subentrante può farsi carico delle attività di valutazione, nell'ambito della validità del certificato già esistente e valido, solo dopo aver deliberato la propria certificazione. L'attività di trasferimento non può essere effettuata contestualmente alle attività di sorveglianza o di rinnovo
17	Polizza assicurativa / Capacità risarcitoria	L'OdC, durante la fase contrattuale e, in particolare, durante la fase 1, deve verificare il livello di responsabilità civile massimo assunto dal TSP nei confronti dei propri clienti. A questo livello di responsabilità deve corrispondere una adeguata polizza assicurativa che consideri il massimo livello di perdite cumulabile per un determinato evento legato ai disservizi potenziali e al numero di clienti con il valore di transazioni dichiarato. L'OdC chiederà evidenza dell'invio dei documenti assicurativi attestanti la copertura assicurativa in corso di validità all'Autorità di Vigilanza (AgID). L'OdC dovrà prevedere per sé medesimo una copertura assicurativa o di tipo patrimoniale, che possa essere compatibile con tale livello massimo di danno atteso.
18	Verifiche aggiuntive	L'OdC che certifica un TSP ai fini della qualificazione eIDAS, deve rendersi disponibile ad effettuare eventuali verifiche aggiuntive richieste dall'Autorità di vigilanza, a titolo oneroso verso il TSP, per gli approfondimenti richiesti.
19	Presenza di ACCREDIA o dell'Autorità di vigilanza	L'OdC deve indicare nel proprio Regolamento per lo schema "eIDAS", che i QTSP (o TSP in certificazione iniziale) debbono garantire l'accettazione degli Ispettori di ACCREDIA durante le diverse fasi di audit svolte dal personale dello stesso TSP/QTSP.

		La mancata accettazione di questo requisito impedisce la prosecuzione di qualsiasi attività inerente allo schema eIDAS. Inoltre, nel Regolamento del TSP/QTSP per lo schema "eIDAS", che deve essere sottoscritto a livello contrattuale dai TSP/QTSP clienti, deve essere chiaramente indicata la possibilità per gli Osservatori di ACCREDIA e dell'Autorità di vigilanza di poter intervenire in tutte le fasi e in tutti i siti e gli ambienti lavorativi, in qualità di osservatori, durante gli audit di conformità alle Norme applicabili allo schema.
20	FAQ e riunioni di scopo	Con cadenza da decidere di comune accordo tra gli OdC accreditati, ACCREDIA e le Autorità di sorveglianza, potranno essere convocate delle riunioni di coordinamento e di chiarimento sugli aspetti applicativi.
21	TSP con processi essenziali per i servizi gestiti in conformità al Regolamento "eIDAS", gestiti in regime di "outsourcing" o "full outsourcing"	L'OdC deve effettuare la verifica presso tali operatori (outsourcee) tenendo conto del fatto che i processi essenziali alla realizzazione dei servizi gestiti a fronte del Regolamento "eIDAS" (non i processi di supporto) debbono essere comunque svolti da un QTSP. Per processo di supporto si deve intendere un processo che non abbia impatto diretto sul servizio erogato a fronte del Regolamento "eIDAS" (es. l'addestramento dei neoassunti, l'amministrazione, la gestione delle Risorse Umane). Nel valutare i servizi dei TSP che sono stati allocati all'esterno, con modalità di "outsourcing", l'OdC deve verificare che tali prestatori "outsourcee" siano qualificati come QTSP (qualifica ottenuta a fronte del Regolamento "eIDAS"). In tale caso, la verifica condotta dall'OdC sul TSP/QTSP sarà riconducibile, per i servizi dati in outsourcing, all'applicazione della ETSI EN 319 401 e alle modalità adottate per garantire il mantenimento sotto controllo di tali processi in "outsourcing". Per gli eventuali altri servizi gestiti internamente dal TSP/QTSP, varranno le regole indicate nella presente Circolare. In generale l'OdC deve valutare come gli operatori gestiscano le terze parti a partire dalle attività più critiche, quali le Registration Authority (RA), per le quali deve essere data evidenza del controllo attraverso procedure di affidamento del sottoprocesso condivise e sottoscritte contrattualmente che prevedano almeno la possibilità di condurre audit (anche in incognito -mistery auditor interni-), l'impegno alla gestione ed alla comunicazione degli incidenti anche a fronte della legislazione applicabile (es: data breach ex GDPR), gestione di KPI condivisi).

		Full outsourcing Ciò vale anche per l'erogazione dei processi QTSP in modalità "**full outsourcing".** Nel caso di QTSP che allocano sotto la propria responsabilità uno o più QSCD presso uno o più Clienti, il QTSP deve garantire degli adeguati criteri di monitoraggio e controllo operativo di tali apparati, facendosi garantire il diritto di audit e l'autorizzazione di accesso per gli Auditor dell'OdC e per gli Osservatori dell'Autorità di vigilanza e di ACCREDIA. Non è ammesso l'outsourcing di servizi essenziali (es.: gestione degli QSCD; gestione dei database delle revoche CRL; gestione delle Registration Authority (RA) **verso operatori non qualificati (non QTSP).** In ogni caso, ove questo non fosse possibile, il TSP deve dare evidenza che questi fornitori sono valutati ed allineati ai requisiti di sicurezza ed affidabilità definiti ed applicati all'interno del TSP stesso. **Requisito comune ad "outsourcing" e "full outsourcing**" Il TSP/QTSP dovrà mantenere un elenco aggiornato delle terze parti alle quali ha delegato in tutto o in parte lo svolgimento dei propri processi, con particolare riferimento (sezione specifica dell'elenco) ai processi che impattano direttamente sui servizi eIDAS. Di tali processi dovrà essere predisposta una mappatura, la descrizione di come lo "outsourcer" li governa, delle modalità adottate per il monitoraggio, compreso il diritto di auditing senza restrizioni. Nel rapporto di audit l'OdC dovrà dare evidenza dell'efficacia del controllo dei processi del TSP affidati all'esterno in special modo per i processi di identificazione ed autenticazione. *NOTA.* La gestione in ambito fisico extra UE è consentita solo per quelle parti di processo che non impattino sulla sicurezza ed affidabilità del servizio (customer satisfaction, help desk ecc.)

L'occasione è gradita per porgere cordiali saluti.

Dott. Emanuele Riva

Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da:
EMANUELE RIVA
Data: 19/06/2023 16:41:31

ALLEGATO

Per la Programmazione, Pianificazione ed esecuzione degli Audit si debbono considerare come documenti di riferimento le seguenti Linee Guida, nelle corrispondenti versioni applicabili:

1 Assessment of Standards related to eIDAS – Dicembre 2018
https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

2 eIDAS: Overview on the implementation and uptake of Trust Services – Gennaio 2018
https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services

3 Recommendations for QTSPs based on Standards - Technical guidelines on trust services – Dicembre 2017
https://www.enisa.europa.eu/publications/reccomendations-for-qtsps-based-on-standards/

4 Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services – Dicembre 2017
https://op.europa.eu/en/publication-detail/-/publication/d94bbe97-3e5a-11ea-ba6e-01aa75ed71a1/language-en/format-PDF

5 Guidelines on Initiation of Qualified Trust Services - Technical guidelines on trust services – Dicembre 2017
https://www.enisa.europa.eu/publications/tsp-initiation

6 Conformity assessment of Trust Service Providers - Technical guidelines on trust services – Dicembre 2017
https://op.europa.eu/en/publication-detail/-/publication/c7669925-3e5a-11ea-ba6e-01aa75ed71a1/language-en/format-PDF/source-search

7 Security framework for Trust Service Providers - Technical guidelines on trust services – Dicembre 2017
https://www.enisa.europa.eu/publications/tsp-security

8 Security guidelines on the appropriate use of qualified electronic signatures - Giugno 2017
https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures

9 Security guidelines on the appropriate use of qualified electronic seals – Giugno 2017
https://op.europa.eu/en/publication-detail/-/publication/90d99ddb-d3de-11e6-ad7c-01aa75ed71a1/language-en/format-PDF/source-search

10 Security guidelines on the appropriate use of qualified electronic time stamps – Giugno 2017
https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures

11 Security guidelines on the appropriate use of qualified website authentication certificates - Giugno 2017
https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-website-authentication-certificates

12 Security guidelines on the appropriate use of qualified electronic registered delivery services – Giugno 2017
https://op.europa.eu/en/publication-detail/-/publication/25a740dd-d3dd-11e6-ad7c-01aa75ed71a1/language-en/format-PDF

13 Regolamenti e Circolari mandatorie emesse da AgID, per gli specifici servizi.

NOTA
Le Linee Guida, in ipertesto, facenti riferimento a requisiti di legge, devono essere applicate in modo mandatorio.