Prot. DC2020SPM032 Milano, 16/03/2020

A tutti gli Organismi di Certificazione accreditati e accreditandi per gli schemi Eidas e ISO 27001

Oggetto: **Dipartimento DC - Circolare Tecnica N. 5/2020 Rev.02**

La presente Circolare per l'Accreditamento a fronte del Regolamento Europeo 910/2014 (eIDAS) sostituisce, integrandola, la precedente Circolare N° 8/2017.
Le Norme riportate nel presente documento sono da intendersi tutte nella versione più recente e applicabile, salvo specifiche indicazioni.
La data di entrata in vigore di futuri aggiornamenti alle norme che sono citate in questo documento o di altre norme applicabili allo schema sarà formalizzata ai CAB tramite il sito "SLACK", che viene reso operativo per gli aggiornamenti e per le FAQ. Le date di entrata in vigore dei documenti citati saranno comunicate ai QTSP da parte dei CAB in base allo specifico requisito del Regolamento di Certificazione, inerente l'aggiornamento normativo.
Gli organismi già accreditati in base alla circolare 8/2017 devono presentare ad Accredia entro il 30 Aprile 2020 i propri documenti di sistema aggiornati come necessario; approvati tali documenti potranno operare su tutti i servizi fiduciari eIDAS.

ITER DI CERTIFICAZIONE	
Organismi di Certificazione titolati a chiedere l'estensione del proprio accreditamento allo schema "eIDAS"	Per richiedere l'accreditamento per lo schema "eIDAS", gli Organismi di Certificazione debbono essere già accreditati per lo schema PRD, secondo la Norma UNI CEI EN ISO/IEC 17065 e per lo schema SSI, secondo la Norma UNI CEI EN ISO/IEC 17021-1. L'accreditamento sarà rilasciato come estensione dello schema PRD, con riferimento alla Norma ETSI EN 319 403 V2.2.2 sino all'entrata in vigore della ETSI EN 319 403-1 V2.3.0 che è in fase di approvazione.
Domanda di estensione	Pur se lo schema "eIDAS" riguarda un ambito coperto dai requisiti del Regolamento UE 2014/910, la domanda di estensione dell'accreditamento deve essere presentata dagli Organismi di Certificazione titolati a farlo, utilizzando i moduli DA e DA-01, diponibili sul sito web di ACCREDIA, corredati dalla documentazione più avanti indicata in questo stesso documento.
Norma di certificazione (riferimenti principali)	ETSI EN 319 401 ETSI EN 319 411-2, supportata dalla ETSI EN 319 411-1 ETSI TR 119 411-4 (la lista di riscontro, che è parte integrante della serie EN 319 411 e che sarà mandatoria a partire dal giorno 01 Maggio 2020, rendendo obsolete le precedenti). ETSI EN 319 421 e 422 ETSI EN 319 412 (parti 1, 2, 3, 4 e 5) ETSI EN TS 119 403-2 per certificati qualificati legati a schemi internazionali che richiedono audit annuali.

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

	ETSI EN TS 119 403-3 per la redazione dei report a far data dal 30 Aprile 2020. ETSI EN 319 521 e ETSI EN 319 531 ETSI EN 319 522 e ETSI EN 319 532 (tutte le parti di entrambe) ETSI TS 119 511 ETSI TS 119 441 ed ETSI EN 319 102-1 ETSI TS 119 612 e ETSI TS 119 615 Tutte le norme si intendono applicabili per le parti corrispondenti ai servizi erogati dai QTSP oggetto della certificazione.
Competenze generali del personale del CAB che opera nello schema	Le competenze del personale del CAB 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 al § 6.
Gestione e attuazione del programma di audit, tempi di verifica e periodicità	Il CAB deve svolgere sia le sorveglianze complete biennali previste dal Regolamento eIDAS sia, in conformità ai requisiti della Norme UNI CEI EN 17065:2012 ed ETSI EN 319_403 (§ 7.9), una sorveglianza parziale, negli anni di mancata copertura delle sorveglianze regolamentate.
Valenza dell'accreditamento	L'accreditamento rilasciato da ACCREDIA è valido per garantire la conformità degli Organismi di Certificazione ai requisiti delle Norme UNI CEI EN ISO/IEC 17065:2012, per come integrata dalla Norma ETSI EN 319 403. L'accreditamento avverrà per tutti i servizi previsti dal Regolamento eIDAS. In occasione delle attivazioni di processi di valutazione su nuovi servizi non già valutati in sede di verifica iniziale, il CAB dovrà avvisare con almeno trenta 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 (vedi elenco dei documenti richiesti) sia in fase di estensione iniziale allo schema PRD, sia quando i singoli Organismi di Certificazione presenteranno specifica richiesta.

Note

1. Dalla data di pubblicazione della presente comunicazione, è reso disponibile il sito web SLACK al Canale #corso eIDAS (https://accredia.slack.com/?redir=%2Fgantry%2Fclient) ove sono presenti due aree di interesse per gli Organismi di Certificazione: l'area chiamata "materiale del corso", nella quale sono presenti tutti i file di riferimento del corso tenuto in data 09-13 Settembre 2019 e un'area chiamata "eIDAS" ove potranno essere registrate domande che richiedono risposte ragionate e ponderate al fine di garantire l'uniformità di approccio nello schema. Prima di registrare domande specifiche, si richiede di verificare se non siano già state registrate in precedenza e abbiano ottenuto già una risposta. La summa di tali domande, costituirà, nel tempo un database di "FAQ" per lo schema eIDAS.
2. Gli Organismi di Certificazione sono tenuti a monitorare nel tempo il sito di AgID, in particolare https://www.agid.gov.it/it/agenzia/vigilanza e in particolare gli Avvisi e le Linee guida emanate da AgID pubblicate su https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata.
3. Gli Organismi di Certificazione sono tenuti a monitorare nel tempo il sito di ETSI per verificare la pubblicazione di aggiornamenti delle norme o di nuove norme applicabili. Come regola generale si utilizza l'ultima versione disponibile delle norme, indipendentemente da quanto risulta in vigore all'emissione delle circolari Accredia. Per l'uso di nuove norme o specifiche si tiene conto dei tempi ragionevolmente necessari per la loro implementazione da parte dei prestatori, fermo restando che non è consentito l'uso di norme e specifiche ritirate o dichiarate "historical" da ETSI senza specifica autorizzazione di Accredia.
4. Gli Organismi di Certificazione sono tenuti a monitorare periodicamente i contenuti del sito "SLACK", per avere notizia degli aggiornamenti ivi registrati.
5. Tutti i requisiti relativi alla Norma ETSI EN 319 403 V.2.2.2. sono sostituiti dagli analoghi requisiti della Norma ETSI EN 319 403-1 non appena la stessa entrerà in vigore, fatto salvo il tempo che verrà concesso per la transizione.

REGOLE PER L' ACCREDITAMENTO

Valgono i prerequisiti previsti dal RG-01 ed RG-01-03 per la concessione dell'accreditamento ed estensione.

Il certificato di accreditamento non riporta settori di accreditamento, atteso il fatto che i TSP operano essenzialmente nel settore EA 33 e tale dicitura nel certificato sarebbe pleonastica.

Le verifiche in accompagnamento possono essere scelte da ACCREDIA in base ai servizi che il CAB richiederà di poter certificare sotto accreditamento. Per l'accreditamento valgono le seguenti regole:

ITER DI ACCREDITAMENTO/ESTENSIONE	
L'Organismo di Certificazione non accreditato secondo la Norma UNI CEI EN ISO/IEC 17065:2012 – Schema PRD	- 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 - Verifica ispettiva presso la sede dell'Organismo di certificazione della durata di 2 giornate - Verifica in accompagnamento presso un'organizzazione che eroga servizi / processi sottoposti a certificazione da parte dell'Organismo di Certificazione a fronte di uno specifico disciplinare riconosciuto dalle Parti Interessate e approvato dal Direttivo di ACCREDIA in conformità ai requisiti della procedura di ACCREDIA PG 13-1
L'Organismo di Certificazione non accreditato secondo la Norma UNI CEI EN ISO/IEC 17021-1:2015 per lo schema SSI, ovvero secondo uno schema di accreditamento inerente la sicurezza delle informazioni, giudicato affine allo schema SSI dall'Ufficio Tecnico di ACCREDIA.	- Deve presentare domanda di accreditamento e/o estensione, per lo schema SSI, secondo le prescrizioni tipiche dello specifico schema, che sono indicate sul sito web di ACCREDIA.
Regole specifiche di accreditamento per lo schema eIDAS (Regolamento (UE) n°2014/910)	

Esame documentale	Devono essere presentati ad ACCREDIA i documenti di sistema che evidenziano la conformità alla Norma ETSI EN 319 403. Nella fattispecie, risulterà accettabile anche un unico regolamento interno prodotto per lo specifico schema. In questo caso, tale Regolamento dovrà indicare quali documenti interni dell'Organismo di Certificazione, facenti parte della documentazione di sistema, sono interessati dalle varianti richieste dalla Norma ETSI citata. Il Regolamento dovrà riportare, per ogni requisito applicabile, quali modifiche debbono essere considerate applicabili, per garantire la conformità alla citata ETSI EN 319 403. L'Organismo di Certificazione 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. Nei rapporti di Audit non saranno consentite registrazioni inerenti suggerimenti per il miglioramento (commenti, raccomandazioni, spunti di miglioramento etc.) del sistema di gestione o dei servizi, saranno considerate accettabili solo le risultanze classificate come NC di tipo Maggiore o Minore.
Programmazione, Pianificazione ed esecuzione degli Audit da parte dei CAB	Per la Programmazione, Pianificazione ed esecuzione degli Audit si debbono considerare come documenti di riferimento le seguenti Linee Guida, nelle corrispondenti versioni applicabili: • Assessment of Standards related to eIDAS – Dicembre 2018 • eIDAS: Overview on the implementation and uptake of Trust Services – Gennaio 2018 • Recommendations for QTSPs based on Standards - Technical guidelines on trust services – Dicembre 2017 • Guidelines on Supervision of Qualified Trust Services - Technical guidelines on trust services – Dicembre 2017 • Guidelines on Initiation of Qualified Trust Services - Technical guidelines on trust services – Dicembre 2017 • Conformity assessment of Trust Service Providers - Technical guidelines on trust services – Dicembre 2017 • Security framework for Trust Service Providers - Technical guidelines on trust services – Dicembre 2017 • Security guidelines on the appropriate use of qualified electronic signatures - Giugno 2017 • Security guidelines on the appropriate use of qualified electronic seals – Giugno 2017 • Security guidelines on the appropriate use of qualified electronic time stamps – Giugno 2017 • Security guidelines on the appropriate use of qualified website authentication certificates - Giugno 2017 • Security guidelines on the appropriate use of qualified

	electronic registered delivery services – Giugno 2017 • Auditing Framework for TSPs – Aprile 2015 Si precisa che le Linee Guida che fanno riferimento a requisiti di legge devono essere applicate in modo mandatorio. 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 https://www.enisa.europa.eu/publications/tsp-termination. 3. Stante l'impossibilità, correlata con i tempi di Audit di sorveglianza, di valutare tutti i requisiti applicabili con uguale approfondimento, gli organismi devono prevedere che le sorveglianze periodiche siano pianificate a fronte di criteri di campionamento prioritari. Di seguito un elenco non esaustivo di tali criteri: a. Chiusura rilievi, se applicabile. b. Nuovi servizi e/o variazione dei servizi già erogati, se applicabile (Change management). c. Nuove revisioni degli standard, se applicabile. d. 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. e. Attività di Vulnerability Assessment/Penetration Test, e relativi Remediation Plan f. Segnalazione e gestione degli Incidenti di sicurezza. g. Varie applicabili al contesto specifico e ritenute imprescindibili. 4. 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. 5. 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.
Elementi aggiuntivi per i servizi di recapito, 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. 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. 2. Per i servizi di conservazione di firme e sigilli elettronici qualificati si dovrà utilizzare la specifica ETSI TS 119 511. 3. 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.
Procedura commerciale	L'Organismo di Certificazione deve produrre un documento di sistema che integri la già esistente procedura di acquisizione dei contratti, con particolare attenzione alle fasi di analisi delle esigenze del TSP e di riesame dell'offerta, anche per verificare il possesso delle specifiche competenze per operare nell'ambito dei servizi richiesti.
Valutazioni di robustezza delle infrastrutture "cloud".	In merito all'uso di infrastrutture "cloud", il TSP deve dare evidenza della capacità di reale "controllo operativo" di tali servizi e della garanzia dell'ubicazione dell'infrastruttura tecnologica di supporto (server, storage e infrastrutture di trasmissione dei dati, come VPN) all'interno dell'UE. Deve essere sempre garantita la trasmissione dei dati di conservazione in modalità sicura attraverso qualsiasi canale adottato. Il TSP deve 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 del CAB e dell'Autorità di vigilanza. L'esistenza di una certificazione del fornitore di servizi "cloud" rilasciata sotto accreditamento 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. Le infrastrutture fisiche di elaborazione e memorizzazione dei dati debbono risiedere all'interno del territorio dell'UE. La gestione dei

	dati dovrà essere conforme ai requisiti del GDPR (Regolamento 679/2016), vuoi che la stessa avvenga tramite l'infrastruttura proprietaria, vuoi che avvenga tramite servizi "cloud".
Valutazioni di robustezza del sistema IT	L'Organismo di Certificazione verifica l'esistenza e l'accettabilità dei controlli operativi relativi ai processi di VA (Vulnerability Assessment) e PT (Penetration Test). Gli stessi possono essere svolti da strutture interne o esterne al TSP, ovvero da strutture interne o esterne agli stessi Organismi di Certificazione. L'organizzazione interna di questi Laboratori deve essere basata sulla Norma ISO/IEC 17025 e, sin da subito, devono fornire evidenza almeno: - della chiara individuazione e diligente applicazione dei requisiti inerenti alla metodologia di valutazione tecnica adottata, che richiami, preferibilmente, l'applicazione dei requisiti ISO/IEC 27008; a) della competenza formale (quali qualifiche, da chi rilasciate, quale esperienza nel settore) delle Risorse Umane addette a tali test; - della 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). La valutazione di cui sopra, ove il Laboratorio di test sia scelto dal TSP è di pertinenza dello stesso TSP e sarà oggetto di valutazione nell'ambito del processo di audit da parte dell'Organismo di Certificazione. Diversamente, se il Laboratorio sarà stato scelto dall'Organismo di Certificazione, si applicheranno le regole di qualifica previste dalla Norma di accreditamento 17025. Le date entro le quali debbono essere adottati i servizi di LAB accreditati per VA e, successivamente, anche per PT saranno oggetto di comunicazioni specifiche.
Rapporto di Audit	Vale quanto indicato al § 7.4.4 della Norma ETSI EN 319 403 e al § 7.4.5 della ETSI EN 319 403-1 quando applicabile. Dal 30 Aprile 2020 i rapporti di audit debbono essere redatti in conformità alla specifica TS 119 403-3. Oltre ai requisiti sopra indicati, l'Organismo di Certificazione deve predisporre un formato per il rapporto di audit, che consenta di avere evidenza della completezza nella valutazione di tutti i requisiti applicabili e dei singoli controlli effettuati, integrando nello stesso rapporto le liste di riscontro ETSI correlate con le Norme di valutazione. Il processo di valutazione dell'Organismo di Certificazione deve coprire i servizi che il TSP ha dichiarato all'Autorità di vigilanza. Dopo l'esecuzione del riesame interno allo stesso Organismo di Certificazione, 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 da EA o dalla Commissione Europea, per la verifica della conformità degli

	specifici servizi eIDAS. Nel rapporto di Audit, l'Organismo di Certificazione 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'Organismo di Certificazione 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 o firme elettroniche qualificate 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 (AgID), per il prosieguo dell'iter di qualifica come QTSP o del suo mantenimento. Una modalità può essere quella dell'invio tramite PEC o servizio di recapito elettronico certificato qualificato. L'Organismo di Certificazione non deve attendere le decisioni dell'Autorità di vigilanza ai fini della propria delibera di certificabilità (o meno) del TSP. Il rapporto di audit 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).
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, e dovrà indicare la conformità al Regolamento (UE) 910/2014 e alla Norma ETSI EN 319 401, alle Norme relative ai Servizi oggetto di Certificazione e ai Servizi medesimi. Il CAB avrà cura di ricordare al TSP di inviare tempestivamente il certificato di conformità e il rapporto di Audit all'Autorità di Vigilanza (AgID).
Tempistica per gli Audit	Vale quanto indicato al § 7.4.2 della Norma ETSI EN 319 403 e analogo paragrafo della ETSI EN 319 403-1, compreso quanto indicato nell'Annesso B, non appena in vigore. L'Organismo di Certificazione adotta il tempo di Audit di base pari al doppio del tempo previsto dal calcolo derivante dall'applicazione della Norma ISO/IEC 27006, senza possibilità di riduzioni, se non nel caso di esistenza di una certificazione ISO/IEC 27001, rilasciata sotto accreditamento dal medesimo Organismo di Certificazione, che copra già il dominio di attività tipiche del TSP e che sia stato svolto da Auditor qualificati eIDAS. In tal caso, potrà essere adottata una riduzione massima del 30% del tempo di Audit precedentemente indicato. Per il calcolo del tempo di audit, si specifica che per una struttura del TSP fino a 25 dipendenti impegnati negli specifici processi relativi ai 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 27001:2013. Le attività di fase 1 (ST1) e di fase 2 (ST2), ivi compresa la fase di valutazione della documentazione di sistema, dovranno essere condotte presso i siti pertinenti del richiedente TSP e non possono essere svolte con modalità consecutive, bensì 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 ST1; lo stesso Piano di Audit, a fronte delle necessarie valutazioni sul campionamento da svolgere durante la fase di ST2, dovrà essere inviato al TSP successivamente alla chiusura della fase di ST1. Per ogni servizio che sarà sottoposto a valutazione dovranno essere applicati 2 gg-uomo 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 mezza giornata non comprensiva dei tempi di trasferimento. Siti ove siano presenti dei QSCD (Qualified Secure Signature/Seal Creation Device - Dispositivi di cui all'Allegato II del Regolamento eIDAS): almeno due giorni per la verifica di architettura e installazione presso il primo sito, almeno un giorno aggiuntivo per ogni sito ove sia presente un QSCD installato e gestito in modo analogo al primo, almeno due giorni 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. La presenza nell'infrastruttura del TSP di QSCD in servizio per la creazione di firme o sigilli qualificati, installati in rete o presso strutture esterne che operano sotto la responsabilità del TSP, ma non dichiarati, deve essere sempre gestita come NC Maggiore. Si sottolinea che la configurazione e gestione degli QSCD deve essere sempre sotto la diretta responsabilità del QTSP inclusa la fase di dismissione sicura degli stessi. Eventuali configurazioni che prevedano QSCD in strutture non sotto la responsabilità del QTSP dovranno essere sempre gestite come NC Maggiori. Per le organizzazioni che svolgono esclusivamente la funzione di "Registration Authority", il tempo di audit può essere ridotto di un terzo, rispetto a quello di un TSP che opera integralmente i processi tipici dei servizi "eIDAS". Questo requisito decadrà con l'approvazione e l'adozione della ETSI EN 319 403-1, per come di seguito indicato. Con la pubblicazione ed entrata in vigore della norma ETSI EN 319 403-1, in sostituzione della ETSI EN 319 403, è autorizzata la certificazione di specifici componenti di servizio fiduciario. 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). Ove un QTSP operi con dei servizi in outsourcing allocati ad altri QTSP, il tempo di audit previsto per le attività di monitoraggio degli "outsourcee" deve essere eliso dal calcolo del tempo di audit globale. Ciò, perché tali "outsourcee" sono già oggetto di audit per lo schema eIDAS.
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.
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 delle sorveglianze non regolamentate, si applicano i criteri tipici delle verifiche dello schema SSI, tenendo conto che dovrà essere allocato almeno 1/3 del tempo normalmente allocato nelle verifiche iniziale e di rinnovo biennale.
Verifiche di rinnovo biennali	Le verifiche di rinnovo biennali possono godere di una riduzione del 20% del tempo di audit calcolato per la verifica inziale, ove tale processo sia condotto dallo stesso Organismo di Certificazione. Ove il TSP cambi Organismo di Certificazione, la verifica biennale deve essere condotta con il 100% del tempo di una verifica inziale. L'eventuale riduzione del 20% del tempo di audit, consentita nel caso sopra indicato, non ha effetto nel calcolo del tempo delle sorveglianze.
Modifiche all'infrastruttura del TSP	Gli OdC devono richiedere contrattualmente ai TSP di comunicare le eventuali modifiche alle proprie infrastrutture o configurazione dei processi. Quindi, 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". Gli stessi 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'Organismo di Certificazione 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, così come modifiche delle politiche di sicurezza e delle modalità tecniche per la loro applicazione, ma anche le 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. Invece, non sono da considerare modifiche significative il normale turnover del personale, le normali operazioni di manutenzione che prevedano anche sostituzione di componenti, altrettanto non sono modifiche significative le revisioni delle valutazione dei rischi, ove non comportino variazioni nell'applicazione dei controlli operativi o nella progettazione dei processi. Occorre specificare ai TSP che nel dubbio è sempre meglio chiedere all'OdC e lasciare 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 e come tale va trattata, valutando in modo formale, quindi 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'Organismo di Certificazione nei confronti di ACCREDIA e dell'Autorità di vigilanza, lo stesso Organismo di Certificazione dovrà fare una specifica segnalazione ad ACCREDIA per ricevere specifiche istruzioni di vigilanza. Carenze inerenti la sicurezza delle informazioni, che possano compromettere o che possano aver compromesso i servizi debbono essere sempre classificate come NC Maggiori.
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'Organismo di Certificazione 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. 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 non regolamentata, al fine di verificare l'efficacia delle azioni correttive adottate. L'Organismo di Certificazione 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.
Polizza assicurativa / Capacità risarcitoria	L'Organismo di Certificazione, durante la fase contrattuale e, in particolare, durante la fase di 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'Organismo di Certificazione chiederà evidenza dell'invio dei documenti assicurativi attestanti la copertura assicurativa in corso di validità all'Autorità di Vigilanza (AgID). L'Organismo di Certificazione dovrà prevedere per sé medesimo una copertura assicurativa o di tipo patrimoniale, che possa essere compatibile con tale livello massimo di danno atteso.
Verifiche aggiuntive	L'Organismo di Certificazione 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.
Presenza di ACCREDIA o dell'Autorità di vigilanza	L'Organismo di Certificazione 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 QTSP. La mancata accettazione di questo requisito impedisce la prosecuzione di qualsiasi attività inerente lo schema eIDAS. Inoltre, nel Regolamento per lo schema "eIDAS", che deve essere sottoscritto a livello contrattuale dai TSP 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.
FAQ e riunioni di scopo	A partire dal mese di marzo 2020 è resa disponibile la piattaforma SLACK che contiente documenti e un'area FAQ per lo specifico schema eIDAS Con cadenza da decidere di comune accordo tra gli Organismi di Certificazione accreditati, ACCREDIA e AgID saranno convocate delle riunioni di coordinamento e di chiarimento sugli aspetti applicativi del presente schema che non possono trovare indicazione nella fase iniziale di accreditamento.
TSP con processi essenziali per i servizi gestiti in conformità al Regolamento "eIDAS", gestiti in regime di "outsourcing" o "full outsourcing" .	L'Organismo di Certificazione deve effettuare la verifica presso tali operatori tenendo conto del fatto che i processi essenziali alla realizzazione dei servizi gestiti a fronte del Regolamento "eIDAS" (non 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". Nel valutare i servizi dei TSP che sono stati allocati all'esterno, con modalità di "outsourcing", l'Organismo di Certificazione deve verificare che tali prestatori "outsourcee" siano qualificati come QTSP (qualifica ottenuta a fronte del Regolamento "eIDAS").In tale caso (processi in outsourcing presso altri QTSP), la verifica sarà riconducibile all'applicazione della sola ETSI EN 319 401 e alle modalità adottate per garantire il controllo dei processi in "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'Organismo di Certificazione 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).

Ci è gradita l'occasione per porgerVi cordiali saluti.

Dott. Emanuele Riva
Direttore Dipartimento
Certificazione e Ispezione