A tutti gli Organismi di Certificazione e Ispezione accreditati e accreditandi per lo schema SSI o schemi equivalenti

Loro sedi

Ns. rif.: DC2017SSV046 *Milano,* 27/03/2017

Oggetto: **Dipartimento Certificazione e Ispezione Accredia - Circolare N° 8/2017**
Informativa in merito all'accreditamento degli Organismi di Certificazione operanti a fronte dei requisiti del Regolamento UE 2014_910 "eIDAS" e della Norma ETSI EN 319_403, per la valutazione dei Prestatori di servizi fiduciari e dei servizi da essi forniti, al fine di ottenere o confermare lo status di "Qualificato" da parte dell'Agenzia Governativa AgID (schema eIDAS)

Annulla e sostituisce la Circolare N° 17/2016 del 19/05/2016

Introduzione
Il Regolamento UE 910/2014, noto come Regolamento eIDAS [*electronic IDentification Authentication and Signature*], prevede espressamente il coinvolgimento di CAB accreditati secondo il Regolamento UE 765/2008, per la qualifica degli operatori di servizi fiduciari (TSP o Trust Service Providers) e dei servizi fiduciari da essi prestati. Tale attività di qualifica è demandata alle autorità governative di ogni singolo Paese UE, ove queste siano esistenti e interessate, nonché notificate alla Commissione Europea dal proprio Paese. Tali autorità governative (in Italia AGID), sono chiamate anche allo svolgimento di attività di vigilanza periodiche o a seguito di segnalazioni di gravi problemi, proprio sui Prestatori di servizi fiduciari. Tale sorveglianza, in condizioni normali, si basa su specifiche verifiche biennali, da eseguire in campo, da parte degli Organismi di Certificazione - OdC (o anche Conformity Assessment Body – CAB) accreditati per questo schema.
Condizione perché un OdC possa essere accreditato è il possesso dei requisiti di cui al Regolamento ACCREDIA RG-01 per l'accreditamento degli Organismi di Certificazione e di Ispezione e al Regolamento ACCREDIA RG-01-03 per l'accreditamento degli Organismi di Certificazione del Prodotto.
Dietro richiesta dei CAB interessati e accertato il possesso dei requisiti minimi a fronte di uno specifico esame documentale, si darà avvio all'iter di accreditamento con la conduzione delle attività di verifica come previste nei Regolamenti di cui sopra e in conformità alle norme/documenti applicabili all'accreditamento.

Contesto Normativo
Per l'esigenza dell'accreditamento dei CAB interessati ad operare nello schema eIDAS e, in cascata, per lo svolgimento dei processi di certificazione dei TSP [*Trust Service Provider*], sono state elaborate delle specifiche Norme da parte dell'ETSI, in collaborazione con EA e con i rappresentanti delle parti interessate. Si tratta della Norma ETSI EN 319_403, che è la Norma per l'accreditamento dei CAB. Tale Norma si basa sulla UNI CEI EN ISO/IEC 17065:2012, integrandola ove ritenuto necessario, come nel caso della qualifica degli Auditor e del restante Personale dei CAB destinati a operare a vario titolo nello schema.
Le altre Norme sono la ETSI EN 319_401 destinata a disciplinare l'organizzazione e la sicurezza delle informazioni dei TSP; la ETSI EN 411 (parti 1 e parte 2) e la ETSI EN 319_421 e 422 per l'emissione di marche temporali (Time Stamping), e la ETSI EN 319_412 (parti 1,2,3,4 e 5) per il contenuto dei certificati emessi dai TSP.
Altre specifiche Norme ETSI EN saranno pubblicate nell'immediato futuro per coprire tutto il ventaglio dei servizi offerti dai TSP operanti a livello Europeo.

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

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 17065:2012 e per lo schema SSI, secondo la Norma UNI CEI EN ISO/IEC 17021-1:2015 o per altro schema di certificazione per la protezione dei dati, ritenuto assimilabile allo schema SSI da parte dell'Ufficio Tecnico di ACCREDIA. L'accreditamento sarà rilasciato come estensione dello schema PRD, con riferimento alla Norma ETSI EN 319_403 V2.2.2.
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 dovrà 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 (nella versione più recente) ETSI EN 319 411-2, supportata dalla ETSI EN 319 411-1 ETSI EN 319 421 e 422 ETSI EN 319 412 (1, 2, 3, 4 e 5)
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, per come indicati al § 6.2.1.2. Il personale che delibera deve inoltre conoscere il processo di certificazione come previsto al § 6.2.1.6 di ETSI EN 319_403.
Competenza del personale che riesamina la domanda di certificazione	Le competenze del personale del CAB che riesamina la domanda di certificazione debbono essere conformi ai requisiti della Norma ETSI EN 319_403, per come indicati al § 6.2.1.3
Competenza della funzione che riesamina il contratto	Avere conoscenza generale sulle Norme UNI CEI EN ISO/IEC 17065, ETSI EN 319_403 ed ETSI EN 319_401 e sulle specifiche Norme relative ai servizi offerti dal TSP.
Criteri di competenza del RGVI e degli auditor	Le competenze dei Lead Auditor e degli Auditor che operano nello schema eIDAS debbono essere conformi ai requisiti della Norma ETSI EN 319_403, per come indicati ai §§ 6.2.1.3, 6.2.1.4 e 6.2.1.8. Per la qualifica degli RGVI, gli Organismi di Certificazione dovranno verificare che gli stessi abbiano una sufficiente padronanza del Regolamento (UE) n°2014/910 (Regolamento eIDAS) e competenze conformi ai requisiti della Norma ETSI EN 319_403 § 6.2.1.9.
Competenza del Gruppo di audit nel suo insieme	È possibile integrare le competenze del gruppo di audit con un esperto del settore. L'esperto non può condurre da solo la verifica o parte di essa ed in ogni momento risponde al RGVI. Spetta all'Organismo di Certificazione garantire la competenza settoriale (settori IAF/aree tecniche) del personale, secondo quanto indicato dalla ETSI EN 319_403 al § 6.2.1.7.
Competenza del personale che riesamina le informazioni raccolte in fase di audit ed i risultati dell'audit	Avere le specifiche competenze indicate al § 6.2.1.4 della norma ETSI EN 319_403 ed aver partecipato come auditor ad almeno tre audit completi presso TSP.
Competenza della funzione di delibera	Vale quanto indicato al § 6.2.1.6 della ETSI EN 319_403.

Gestione e attuazione del programma di audit, tempi di verifica e periodicità	Il CAB dovrà svolgere le sorveglianze complete biennali previste dal Regolamento eIDAS e, in conformità ai requisiti delle 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 della Norma UNI CEI EN ISO/IEC 17065:2012, come integrata dalla Norma ETSI EN 319_403. L'accreditamento avverrà per dei servizi di marcatura temporale [ETSI EN 319 421 ed ETSI EN 319 422] e/o di realizzazione di tutti i servizi previsti dalla Norma ETSI EN 319 412 (da 1 a 5) e di altri servizi le cui Norme di riferimento saranno individuate da EA e/o dalla Commissione Europea. L'Accreditamento non copre e non consente la certificazione dei servizi (PSES, REMQ), relativi alla "conservazione di firme e sigilli" ed alla "consegna di posta elettronica". 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.

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	
Organismo di Certificazione non accreditato secondo la Norma UNI CEI EN ISO/IEC 17065:2012 – Schema PRD	- Deve presentare domanda di accreditamento alla norma UNI CEI EN ISO/IEC 17065:2012 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 dal parte dell'Organismo di Certificazione a fronte di uno specifico disciplinare riconosciuto dalle Parti Interessate e approvato dal Consiglio Direttivo di ACCREDIA in conformità ai requisiti della procedura di ACCREDIA PG-13-01.
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	Dovranno 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.
Procedura di valutazione per lo schema eIDAS	L'Organismo di Certificazione dovrà produrre un documento di sistema che descriva, anche in modo sintetico e/o grafico* il processo di valutazione e decisionale per lo specifico schema. Nota (*) ad esempio tramite diagrammi di flusso o swim-lane chart etc.
Procedura commerciale	L'Organismo di Certificazione dovrà 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, per verificare il possesso delle specifiche competenze per operare nell'ambito dei servizi richiesti.
Valutazioni di robustezza del sistema IT	In merito all'uso di infrastrutture "cloud", il TSP dovrà dare evidenza della capacità di reale "controllo operativo" di tali servizi. L'Organismo di Certificazione verificherà l'esistenza e l'accettabilità dei controlli operativi relativi ai processi di VA (Vulnerability Assessment) e PT (Penetration Test). Gli stessi dovranno essere svolti da Laboratori interni o esterni al TSP, ovvero da strutture interne o esterne agli stessi Organismi di Certificazione, la cui qualificazione deve essere basata, a partire dal 01 Giugno 2017, sulla Norma UNI CEI EN ISO/IEC 17025 e che, sin da subito, forniscano evidenza almeno: - della chiara individuazione e diligente applicazione dei requisiti inerenti la metodologia di valutazione tecnica adottata, che richiami, preferibilmente, l'applicazione dei requisiti della norma ISO/IEC 27008; - della competenza formale (quali qualifiche, da chi rilasciate, quale esperienza nel settore) delle Risorse Umane addette a tali test; e - 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). 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 UNI CEI EN ISO/IEC 17065. Dal 01 Giugno 2018, gli Operatori che effettueranno tali attività di PT e VA dovranno essere accreditati secondo la norma UNI CEI EN ISO/IEC 17025:2005.
Rapporto di Audit	Vale quanto indicato al § 7.4.4 della Norma ETSI EN 319_403. L'Organismo di Certificazione dovrà 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 dovrà coprire i servizi che il TSP ha dichiarato ad AgID. Dopo l'esecuzione del riesame interno allo stesso Organismo di Certificazione, potrà 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 dovrà indicare esplicitamente lo stato di conformità al presente schema di accreditamento, per il 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 sarà presente anche nei Certificati di Conformità. L'Organismo di Certificazione dovrà 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; quindi tale rapporto comprensivo di tutti i documenti di registrazione delle evidenze oggettive prodotte sul campo, dovrà essere trasmesso formalmente al TSP, che avrà cura, se del caso, di inviarlo ad AgID, per il prosieguo dell'iter di qualifica come QTSP. Una modalità può essere quella dell'invio tramite PEC. L'Organismo di Certificazione non dovrà attendere le decisioni di AgID 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, senza ulteriori specificazioni sui servizi oggetto di qualifica, che rimarranno nella responsabilità finale di AgID.
Tempistica per gli Audit	Vale quanto indicato al § 7.4.2 della Norma ETSI EN 319_403. L'Organismo di Certificazione adotterà un tempo di Audit di base pari al doppio del tempo previsto dal calcolo derivante dall'applicazione della Norma ISO/IEC 27006:2015, senza possibilità di riduzioni, se non nel caso di esistenza di una certificazione ISO/IEC 27001:2013, rilasciata sotto accreditamento dal medesimo Organismo di Certificazione, che copra già il dominio di attività tipiche del TSP. In tal caso, potrà essere adottata una riduzione massima del 30% del tempo di Audit precedentemente indicato. Ove lo scopo di certificazione copra solo parzialmente le attività tipiche del TSP, la riduzione massima consentita sarà del 10%. 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. Nella fattispecie, alla data di pubblicazione di questo documento, i servizi che possono essere oggetto di certificazione da parte degli OdC e, conseguentemente oggetto di accreditamento, sono quelli inerenti le Marche Temporali e le Certification Authority. Per ogni sede aggiuntiva, rispetto a quella centrale del TSP, dovranno 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 degli HSM: 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 HSM 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 HSM di firma remota installati in rete o presso strutture esterne che operano sotto la responsabilità del TSP, ma non dichiarati, dovrà essere sempre gestita come NC Maggiore. Per le organizzazioni che svolgono esclusivamente la funzione di "Registration Authority", il tempo di audit potrà essere ridotto sino al 50%, rispetto a quello di un TSP che opera integralmente i processi tipici dei servizi "eIDAS". L'OdC valuterà l'applicabilità di tale riduzione in funzione del campionamento dei siti ove avvengono le identificazioni degli utenti, sulla base del campionamento che dovrà rispondere ai requisiti del documento mandatorio IAF MD 01.
Composizione dei Gruppi di Audit	I Gruppi di Audit chiamati a operare per ogni singolo TSP dovranno 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 potrà 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 ISO/IEC 17065:2012 ed ETSI EN 319_403, il relativo rapporto dovrà essere gestito come nel caso degli audit regolamentati, salvo specificare nella documentazione contrattuale con i QTSP che non è richiesto l'invio ad AgID, se non dietro specifica richiesta della stessa Agenzia. Per il calcolo della durata delle sorveglianze non regolamentate, si applicheranno 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 potranno 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 dovrà 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 valuteranno se tali modifiche debbano riguardare anche le revisioni dei "TSP Practice Statements" e/o del SOA 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 HMS 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 della 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 di AgID, 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 dovranno 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 presso ogni sede secondaria ove viene gestito un dispositivo HSM. 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 dovrà 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 potrà farsi carico delle attività di valutazione, nell'ambito della validità del certificato già esistente e valido, solo dopo che avrà deliberato la propria certificazione.
Polizza assicurativa	L'Organismo di Certificazione, durante la fase contrattuale e, in particolare, durante la fase di stage 1, dovrà verificare il livello di responsabilità civile massimo assunto dal TSP nei confronti del propri clienti. A questo livello di responsabilità dovrà 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 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 qualifica di AgID, deve rendersi disponibile ad effettuare eventuali verifiche aggiuntive richieste dalla stessa Agenzia, a titolo oneroso verso il TSP, per gli approfondimenti richiesti.
Presenza di ACCREDIA o di AgID	L'Organismo di Certificazione deve indicare nel proprio Regolamento per lo schema "eIDAS", che oltre al personale di ACCREDIA, designato allo svolgimento delle verifiche presso la propria sede, accetta anche la presenza di Osservatori di AgID. Inoltre, nel Regolamento per lo schema "eIDAS", che dovrà essere sottoscritto a livello contrattuale dai TSP clienti, dovrà essere chiaramente indicata la possibilità per gli Osservatori di ACCREDIA e di AgID 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 Giugno 2016, nell'area riservata agli Ispettori del sito web di ACCREDIA è presente una pagina destinata a ospitare le domande più frequenti o più significative derivanti dall'esperienza maturata in campo dai Gruppi di Audit degli Organismi di Certificazione accreditati. Altrettanto, 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 effettuerà 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 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 verificherà 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 uno o più HSM 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 di AgID e di ACCREDIA. Non è ammesso l'outsourcing di servizi essenziali (es.: gestione degli HSM; gestione dei database delle revoche CRL; gestione delle Registration Authority RA) verso operatori non qualificati (non QTSP).

Cordiali saluti.

Il Direttore di Dipartimento
Dr. Emanuele Riva