REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

Indice Revisioni

0	2016-05-23	**Prima emissione**
1	2016-09-30	*Aggiornamenti in corsivo ai §5.2.3 e §5.8.1 in relazione agli esiti dell'esame documentale ACCREDIA.*
2	2016-12-16	Aggiornamenti per integrazione con erogazione servizi SPID e Conservazione
3	2017-02-28	Aggiornamenti per nuova circolare Accredia n. 05/2017 del 27-02-2017
4	2017-04-11	Aggiornamenti per nuova circolare Accredia n. 08/2017 del 27-03-2017
5	2017-09-04	Revisione Generale.
6	2019-02-26	Aggiornato §4.4.4. data di partenza obbligo accreditamento laboratori VA 01-06-2019
7	2019-09-13	Eliminato §4.9.3 Opportunità di Miglioramento (OdM), le anomalie sono solo NC Maggiore e NC Minore; Modificata data al §4.4.4 scadenza portata al 01/06/2020.

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

1 OGGETTO E CAMPO DI APPLICAZIONE

Il presente documento costituisce il Regolamento relativo agli schemi per la certificazione dei Servizi del Regolamento **eIDAS** "electronic IDentification Authentication and Signature", dello **SPID** "Sistema Pubblico di Identità Digitale", della **Conservazione dei documenti informatici** e quindi descrive le condizioni e le procedure applicate da DNG GL Business Assurance Italia S.r.l. (in seguito DNV GL) per la certificazione, operati da organizzazioni che realizzano prodotti e/o erogano servizi TSP.

Il Regolamento eIDAS (UE) (n. 910/2014):

a) Fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro;
b) Stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche, e
c) Istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

Il presente documento definisce condizioni e procedure supplementari rispetto a quanto già definito nei:

- "REGOLAMENTO GENERALE PER LA CERTIFICAZIONE DI PRODOTTI, PROCESSI E SERVIZI (PRD)" e nel
- "REGOLAMENTO GENERALE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE AZIENDALE (MSC)".

2 TERMINI E DEFINIZIONI

Servizio fiduciario:
un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: *creazione, verifica e convalida dei certificati relativi a tali servizi*;

Prestatore di servizi fiduciari:
una persona fisica o giuridica che presta uno o più servizi fiduciari

Prestatore di servizi fiduciari qualificato:
un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato

eIDAS:
electronic IDentification Authentication and Signature.

SPID:
Sistema Pubblico per la gestione dell'Identita' Digitale

CONSERVATORI:
Conservatori di documenti digitali

TSP:
operatori di servizi fiduciari **Trust Service Provider**.

QTSP:

operatori di servizi fiduciari **Qualified Trust Service Provider**.

Scopo:
l'ambito di riferimento in cui opera il/i servizio/i fiduciario/i di TSP, ossia le caratteristiche di business (servizi, attività), l'assetto organizzativo (ruoli, responsabilità) i siti coinvolti, le risorse (assets), le tecnologie e i confini e le relazioni con processi e sistemi informatici esterni.

Scopo di certificazione:
il paragrafo riportato sul certificato che descrive le attività sottoposte a certificazione (elenco servizi fiduciari) . In generale si tratta di un breve periodo.

Organizzazione:
in questo documento, si intende con questo termine l'Organizzazione oggetto dell'audit o *auditee*.

3 SERVIZI IN CERTIFICAZIONE

I servizi che vanno in certificazione e che quindi richiedono un "Conformity assessment" sono:

1. **I servizi "eIDAS - electronic IDentification Authentication and Signature" che sono**:

   - *creazione, verifica e convalida di sigilli elettronici*
   - *validazioni temporali elettroniche e certificati relativi a tali servizi*
   - *servizi elettronici di recapito certificato e certificati relativi a tali servizi*
   - *creazione, verifica e convalida di certificati di autenticazione di siti web*
   - *conservazione di firme, sigilli o certificati elettronici relativi a tali servizi*
   - *creazione, verifica e convalida di firme elettroniche e certificati relativi a tali servizi*

2. **I servizi "SPID - Sistema Pubblico per la gestione dell'Identita' Digitale";**

3. **I servizi dei "Conservatori di documenti digitali";**

4 DOCUMENTI DI RIFERIMENTO

Le norme e i documenti di riferimento per la certificazione e registrazione dei servizi TSP sono i seguenti:

ZSEIT-10-RG-020 (I)	REGOLAMENTO GENERALE PER LA CERTIFICAZIONE DI PRODOTTI, PROCESSI E SERVIZI (PRD)
ZEOIT-10-RG-002 (I)	REGOLAMENTO GENERALE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE AZIENDALE (MSC)
ISO/IEC 27001:	"Information technology - Security techniques - Information security management systems - Requirements"

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

ISO/IEC 27002:	“Information technology - Security techniques - Code of practice for information security management systems”
ISO/IEC 27005:	“Information technology — Security techniques — Information security risk management”
ISO/IEC 27006:	“Information technology - Security techniques – Requirements for bodies providing audit and certification of information security management systems”
ISO/IEC 27008:	“Information technology — Security techniques — Guidelines for auditors on information security controls”
ISO/IEC 17065:	"Conformity assessment -- Requirements for bodies certifying products, processes and services".
ISO/IEC 17000:	"Conformity assessment -- Vocabulary and general principles".
ISO/IEC 15408:	"Information technology -- Security techniques -- Evaluation criteria for IT security".
ISO 2859-1:1999:	“Sampling procedures for inspection by attributes – Part 1: sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection”
ETSI EN 319 401:	"Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures".
ETSI EN 319 403:	“Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing 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 for Trust Service Providers issuing certificates".
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 qualified certificates".

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

ETSI EN 319 412-1:	" Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
ETSI EN 319 412-2:	“Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons”.
ETSI EN 319 412-3:	“Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons”.
ETSI EN 319 412-4:	“Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates”.
ETSI EN 319 412-5:	“Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements”. (Qualified certificate statements)
ETSI EN 319 421:	"Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services".
ETSI EN 319 422:	"Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
ETSI TR 101 533-1:	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management
ETSI TR 101 533-2:	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors
ETSI TS 102 573:	Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects
Circolare N.35/2016 ACCREDIA	Schema di accreditamento degli Organismi di Certificazione, per il processo di certificazione degli operatori SPID, secondo le disposizioni dell'Agenzia per l'Italia Digitale
Circolare N.5/2017 ACCREDIA	Schema di accreditamento degli Organismi di certificazione, per il processo di certificazione dei Conservatori a Norma, secondo le disposizioni dell'Agenzia per l'Italia Digitale.

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

Circolare N.8/2017 ACCREDIA	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).
Circolare tecnica n° 02/2019 ACCREDIA	Comunicazione Tecnica sugli schemi di Accreditamento PRD eIDAS, Conservatori a norma e SPID
Regolamento eIADS	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.
Regolamento (UE) 2016/679	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
DECRETO DEL PRESIDENTE DELLA REPUBBLICA 28 dicembre 2000, n. 445	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
D.Lgs. CAD – Codice dell'Amministrazione Digitale. Decreto legislativo 26 agosto 2016 n. 179	recante "Modifiche e integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche".

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

SPID - Sistema Pubblico per la gestione dell'Identita' Digitale	• ISO/IEC 29115:2013 “Entity authentication assurance program”; • Regolamento di attuazione UE 2015/1502; • DPCM24/10/2014 “Definizione delle caratteristiche del sistema pubblico per la gestione dell'identita' digitale di cittadini e imprese (SPID), nonche' dei tempi e delle modalita' di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376)”; • ISO 14721: 2012 (OASIS) “Space data and information transfer systems — Open archival information system (OAIS) — Reference model”; • UNI 11386:2010 “Supporto all’Interoperabilità nella conservazione e nel Recupero degli Oggetti digitali (SInCRO)”; • ISO 15836:2009 “Information and documentation — The Dublin Core metadata element set”;

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

Conservatori di documenti digitali	• DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 3 dicembre 2013 “Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell’amministrazione digitale di cui al decreto legislativo n. 82 del 2005.”; • DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 novembre 2014 “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis , 23 -ter , 40, comma 1, 41, e 71, comma 1, del Codice dell’amministrazione digitale di cui al decreto legislativo n. 82 del 2005.”; • CIRCOLARE N. 65 del 10 aprile 2014 “Modalità per l’accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.”; • ISO/IEC 29115:2013 “Entity authentication assurance program”; • Regolamento di attuazione UE 2015/1502; • AGID “ACCREDITAMENTO DEI SOGGETTI PUBBLICI E PRIVATI CHE SVOLGONO ATTIVITÀ DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI. REQUISITI DI QUALITÀ E SICUREZZA PER L’ACCREDITAMENTO E LA VIGILANZA” v.1.1; • ISO 14721: 2012 (OASIS) “Space data and information transfer systems — Open archival information system (OAIS) — Reference model”; • ISO 16363:2012 “Space data and information transfer systems — Audit and certification of trustworthy digital repositories”; • ISO 16919:2014 “Space data and information transfer systems — Requirements for bodies providing audit and certification of candidate trustworthy digital repositories; • ISO 15836:2009 “Information and documentation — The Dublin Core metadata element set”; • UNI 11386:2010 “Supporto all’Interoperabilità nella conservazione e nel Recupero degli Oggetti digitali (SInCRO)”;

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

4.1 REGOLE PARTICOLARI – CERTIFICAZIONE IN ACCORDO ALLE NORME DI RIFERIMENTO

Per i servizi **eIDAS e SPID**, l'Organizzazione deve avere un Sistema di Gestione in accordo ai requisiti della normativa di riferimento per la certificazione dei servizi fiduciari del TSP la ETSI EN 319 401 "*Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures*".

4.2 Referente per DNV GL

Lo standard di riferimento per la certificazione dei servizi fiduciari del TSP non richiede la nomina di un rappresentante della Direzione. Ciononostante, l'Organizzazione deve indicare la persona al suo interno come referente per DNV GL e con la necessaria autorità per garantire l'esecuzione dell'audit.
In particolare, deve garantire l'accesso alla documentazione, a tutte le aree comprese nello scopo del servizio fiduciario del TSP, alle registrazioni che danno garanzia della corretta applicazione del servizio TSP, al personale compreso nello scopo del servizio fiduciario del TSP.

4.3 Audit

I paragrafi che seguono specificano i requisiti aggiuntivi rispetto a quanto già indicato dal "REGOLAMENTO GENERALE PER LA CERTIFICAZIONE DI PRODOTTI, PROCESSI E SERVIZI (PRD)" e nel "REGOLAMENTO GENERALE PER LA CERTIFICAZIONE DI SISTEMI DI GESTIONE AZIENDALE (MSC)".

4.3.1 Audit della documentazione di sistema (**Stage 1**)

Viene verificato che l'Organizzazione abbia sviluppato una documentazione di sistema conforme ai requisiti delle norme di riferimento.

Oltre alla documentazione sono analizzati il/i servizio/i fiduciario/i in ambito TSP e in particolare la progettazione dei servizio/i.

Nel corso della valutazione della documentazione verrà definito lo "Scopo di certificazione" (paragrafo 4.4), che potrà essere modificato anche negli audit successivi.

Altre considerazioni in merito alla documentazione sono riportate nel paragrafo 4.3.

Al termine della valutazione della documentazione, che DNV GL svolge presso l'Organizzazione, il Lead Auditor illustra le eventuali anomalie riscontrate rispetto ai requisiti dello standard.

4.3.2 Audit preliminare (**Stage 1**)

Viene valutata la capacità del Sistema di fornire una giustificata fiducia a mantenersi conforme ai requisiti relativi alla erogazione del/i servizio/i fiduciario/i stabiliti dall'organizzazione.
Tra questi requisiti devono essere inclusi quelli legislativi e normativi applicabili e gli accordi con i clienti eventualmente sottoscritti dall'Organizzazione.

A tal scopo, nel corso dell'audit preliminare sono analizzate le caratteristiche dei siti, dei processi, delle attività e dei servizi, dei sistemi e delle reti informatiche incluse nello scopo del servizio fiduciario del TSP al fine di valutare l'adeguatezza, la completezza e l'affidabilità del processo e dei report di valutazione e trattamento del rischio, incluso il piano di trattamento del rischio con le politiche e gli obiettivi dell'Organizzazione relativi alla sicurezza.

Ci si assicura inoltre che tutte le interfacce con i servizi o le attività che non sono incluse completamente all'interno dello scopo del servizio fiduciario del TSP siano correttamente affrontate dai processi di valutazione e trattamento del rischio.

L'Organizzazione deve altresì dimostrare di avere attivi i controlli di sicurezza richiesti a livello legislativo, regolamentare e contrattuale.

In questa fase, è esaminato il processo di gestione degli incidenti e il processo di gestione della continuità operativa per quanto pertinente lo scopo del servizio fiduciario del TSP.

Al termine della valutazione preliminare, che DNV GL svolge presso l'Organizzazione, il Lead Auditor illustra gli eventuali rilievi (Non Conformità) riscontrati, stabilisce se l'Organizzazione è pronta per l'Audit Iniziale e, in tal caso, prepara un piano per tale audit.

Nota: E' possibile condurre congiuntamente l'audit della documentazione e l'audit preliminare (dipende dal grado di maturità del sistema, dichiarato dal cliente).

4.3.3 Audit Iniziale (**Stage 2**)

Gli obiettivi della fase di Stage 2 sono:

- confermare che il servizio fiduciario del TSP aderisce alle sue politiche, gli obiettivi e le procedure; e
- confermare che i servizi fiduciari implementati sono conformi ai requisiti dei criteri di audit Applicabili e rispettano le politiche applicabile, gli obiettivi e le procedure.

Durante questa fase saranno verificate in relazione ai servizi fiduciari del TSP:

a) L'applicazione dei requisiti del servizio TSP;
b) Il servizio TSP riguardo i processi e le procedure Organizzative;

c) Il servizio TSP riguardo i processi e le procedure Tecniche;
d) sia correttamente implementato un sistema della sicurezza delle informazioni per i servizi TSP compresa la protezione della rete;
e) i device relativi al servizio TSP (sistemi affidabili), quali moduli di crittografia (HSM);
f) la sicurezza fisica dei siti TSP;
g) Analisi Checklist AgID;

Inoltre, ci si assicura che tutte le interfacce con i servizi fiduciari o le attività che non sono incluse completamente all'interno dello scopo del servizio TSP siano correttamente presidiate con opportuni controlli di sicurezza.

Le altre aree di attenzione sono le seguenti:

- Gestione degli Asset;
- Gestione dei supporti rimovibili e fissi;
- Controllo degli accessi;
- Controlli Crittografici;
- Sicurezza fisica e ambientale;
- Sicurezza delle attività operative;
- Sicurezza della rete (interna e dalle minacce esterne);
- Gestione degli incidenti;
- Raccolta [e conservazione] delle evidenze della gestione come TSP;
- Gestione della continuità operativa;
- Interruzione delle attività del TSP e piano relativo;
- Compliance;

In caso di assenza di Non Conformità maggiori, il rapporto viene inviato dal Gruppo di Audit al DNV GL per valutazione tecnica (**Technical Review**).

DNV GL può approvare, ma anche negare la certificazione, comunicando all'Organizzazione le ragioni di tale decisione.

Dopo l'approvazione del rapporto del Gruppo di audit, per come eventualmente integrato a fronte delle decisioni del DNV GL, DNV GL provvede alla firma digitale con marca temporale dello stesso rapporto e ad inviarlo via PEC all'Organizzazione affinchè **quest'ultima possa inviarlo a AGID per il proseguo dell'iter di accreditamento pubblico come operatore a norma**.

4.3.4 Frequenza degli audit / Audit periodici (P1)

La validità del certificato è di **2 (due) anni**. Quindi al termine della validità del certificato va svolto un audit di rinnovo della certificazione.

Nel corso del primo anno di certificazione va svolta un'attività di audit periodico (P1) entro 12 mesi dall'ultima attività di Stage 2.

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

Lo schema prevede:

1) STAGE 1 + STAGE 2
2) P1
3) RC (Rinnovo)
4) P1
5) RC (Rinnovo)
6) P1
7) RC (Rinnovo)
8) P1
9) RC (Rinnovo)
10) P1
11) E cosi via.

Nel caso dello schema dei CONSERVATORI, non essendo previste norme di sistema, l'audit iniziale non prevede la suddivisione in Stage 1 + Stage 2, ma una unica attività di audit.

Per semplicità, manterremo la suddivisione in DI+IA, ma le attività saranno erogate in maniera continuativa e il rapporto sarà unico.

Le seguenti attività fanno parte della verifica di sorveglianza (P1) per **eIDAS e SPID**:

- revisione delle azioni intraprese sulla non conformità identificate durante il precedente audit;
- Revisione della strategia di campionamento multi-sito, se il campionamento è stato applicato nel precedente audit;
- Revisione delle eventuali modifiche di documentazione e il funzionamento del servizio TSP;
- Revisione degli audit interni e riesame della direzione;
- il trattamento dei reclami;
- uso dei marchi e/o di qualsiasi altro riferimento alla valutazione di conformità; e
- analisi delle dichiarazioni pubbliche sul servizio TSP (ad esempio materiale promozionale, sito web);
- Valutazione punti aperti delle Checklist.

Nel caso dei **Conservatori** la verifica di sorveglianza (P1) sarà limitata all'accertamento dell'applicazione dei requisiti individuati della Lista di Riscontro predisposta da AgID.
Inoltre, l'Organismo di Certificazione prenderà atto in tutte le verifiche, dell'esito delle valutazioni a fronte della Norma UNI CEI EN ISO/IEC 27001:2017.

In caso di assenza di Non Conformità maggiori, il rapporto viene inviato dal Gruppo di Audit al DNV GL per valutazione tecnica (**Technical Review**).

Dopo l'approvazione del rapporto del Gruppo di audit, per come eventualmente integrato a fronte delle decisioni del DNV GL, DNV GL provvede alla firma digitale con marca temporale dello stesso rapporto e ad inviarlo via PEC all'Organizzazione.

In questo caso non è richiesto che l'Organizzazione che la stessa ne invii copia a AGID, se non dietro esplicità richiesta di quest'ultima, in quanto autorità di vigilanza.

4.4 Documentazione

La documentazione fa riferimento:

- Per i servizi **eIDAS e SPID** quanto previsto nella **ETSI EN 319 401** Electronic Signatures and Infrastructures (ETSI); General Policy Requirements for Trust Service Providers;

- Per il servizio di **Conservazione** quanto previsto **all'Art. 24 del Regolamento UE 2014/910 eIDAS "**Requirements for qualified trust service providers";

4.4.1 Perimetro in certificazione

Lo Scopo (distinto dallo "Scopo di certificazione" trattato nel successivo 4.4) deve essere descritto in modo da dare all'auditor tutti gli elementi per comprendere i servizi previsti in perimetro:

- personale e struttura organizzativa;
- attività;
- dati e informazioni;
- infrastrutture;
- siti;
- sistemi informatici;
- reti informatiche;
- fornitori utilizzati.

Vanno anche evidenziate le loro interrelazioni e interfacce con elementi non compresi nello scopo. Tra questi, vanno anche segnalati elementi che utilizzano i medesimi siti e infrastruttura informatica.

4.4.2 Processo di valutazione del rischio (Risk Assessment)

Per i servizi **eIDAS e SPID.**

L'Organizzazione deve aver stabilito un processo di valutazione del rischio che:
- Sia sistematico;
- Consideri tutti i rischi, al corretto livello di dettaglio;
- Garantisca risultati comparabili e riproducibili;
- Garantisca il mantenimento nel tempo dei suoi risultati.

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

4.4.3 Conformità legislativa

DNV GL verifica che l'Organizzazione abbia stabilito e mantenga un efficace processo per identificare ed avere accesso ai requisiti normativi relativi ai servizi in scopo.

Si ricorda che un audit di certificazione non è un audit di conformità legale.

4.4.4 Valutazione di robustezza dei sistemi di Information Technology (IT)

In merito all'uso di infrastrutture "cloud", l'operatore SPID dovrà dare evidenza della capacità di reale "controllo operativo" di tali servizi e della adesione alle eventuali indicazioni di AgID in merito all'ubicazione dei server fisici e sui repository [sistemi di memorizzazione] nei quali avviene l'archiviazione dei dati/informazioni inerenti l'identificazione delle Persone Fisiche e Giuridiche.

I controli operativi, riferiti alla norma ISO/IEC 27001 (versione applicabile), referiti ai processi di **VA** (Vulnerability Assessment) e **PT** (Penetration Test), dovranno essere svolte da strutture interne o esterne all'Organizzazione, ovvero da strutture interne o esterne al DNV GL, la cui qualifica deve essere basata, a partire dal **01 Giugno 2017**, sulla norma ISO/IEC 17065 (versione applicabile) 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 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 siano compatibili e aggiornate ai rilasci dei S.O. e delle applicazioni da analizzare dell'Organizzazione);

La valutazione di cui sopra, ove il Laboratorio dei Test sia scelto dall'Organizzazione è di pertinenza della stessa e sarà ogetto di valutazione nell'ambito del processo di audit da parte di DNV GL. Diversamente se il laboratorio sarà scelto da DNV GL, si applicheranno le regole di qualifica previste dalla norma di accreditamento ISO/IEC 17065 (versione applicabile).

A partire dal 01 Giugno 2020 tali Laboratori, da chiunque scelti, dovranno essere accreditati secondo la Norma ISO/IEC 17025.

4.5 Scopo di certificazione

In questo paragrafo, si intende con “scopo di certificazione” *la frase riportata* sul certificato che descrive le attività sottoposte a certificazione.

Lo scopo di certificazione deve indicare le tipologie di processi (attività svolte) e i servizi offerti dall’Organizzazione.

Si raccomanda di utilizzare la terminologia proposta da organismi quali AgID (Agenzia per l'Italia Digitale).

4.6 Outsourcing

TSP con servizi essenziali ai fini **eIDAS**, in regime di "outsourcing" o "full outsourcing".

Va effettuata la verifica presso tali operatori tenendo conto del fatto che i servizi critici debbono essere comunque svolti da QTSP.

In tale caso (servizi 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 del DNV GL 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).

Nel caso dei **Conservatori,** come previsto dalla circolare n. 65 di AgID:

Il conservatore può affidare ad altro conservatore accreditato le attività a supporto del processo di conservazione limitatamente a quelle che riguardano le infrastrutture per la memorizzazione, trasmissione ed elaborazione dei dati.

In questo caso è importante analizzare come vengano gestiti i rapporti con il fornitore.

4.7 Multisito

L'approccio multisito viene considerato possibile, ove le Organizzazioni che lo richiedono operino, nei diversi siti, con processi assimilabili.

Il campionamento dovrà prevedere sempre la valutazione dell'efficacia dei controlli di sicurezza e delle responsabilità della Direzione, più un campione di siti, che consenta, in un periodo ragionevole e comunque prima del rinnovo della certificazione, la copertura di tutta la Organizzazione.

Le non-conformità (di cui al paragrafo 4.8), comunque classificate, rilevate nei vari siti, dovranno essere oggetto di un processo di miglioramento applicato a tutti i siti dell'Organizzazione.

L' eventuale persistenza di una Non Conformità maggiore, comporta il ritiro della certificazione a tutta l'Organizzazione e non solamente al singolo sito.

Si applica il documento IAF MD01 per certificazione multi-site.

4.7.1 Siti condivisi

Nel caso in cui l'Organizzazione condivida il proprio sito e la gestione delle infrastrutture con altre entità, essa:

- Deve avere identificato nel documento di Scopo dei servizi tale situazione e considerarla nell'ambito della valutazione e del trattamento del rischio;
- Deve aver identificato le proprie interfacce per la gestione del sito e delle infrastrutture con le altre identità;
- Deve dimostrare di esercitare un adeguato livello di controllo, sul sito e sulle infrastrutture, anche in ottica di miglioramento.

4.8 Elenco dei reclami e incidenti

L'Organizzazione deve tenere aggiornato e rendere disponibile **un elenco dei "reclami" e degli "incidenti"** e di come sono stati opportunamente gestiti collegabili alla erogazione dei servizi fiduciari in perimetro.

4.9 Classificazione delle non-conformità

In aggiunta a quanto già indicato dal "Regolamento Generale per la Certificazione di Sistemi di Gestione Aziendale (MSC)" valgono le seguenti definizioni.

4.9.1 **NC di categoria 1 (Maggiore)**

- Il mancato rispetto degli obblighi di legge;
- Il mancato rispetto di requisiti contrattuali eventualmente concordati con partner o clienti relativamente;
- La palese evidenza di un immediato rischio per le informazioni o un'anomalia nelle procedure che possono causare un significativo rischio per la sicurezza;
- Nessuna evidenza oggettiva disponibile in relazione alla gestione degli incidenti o la mancanza di una pianificazione e attuazione di controlli di continuità operativa;
- La non esecuzione di un ciclo completo di audit interni precedenti l'audit iniziale e di rinnovo del certificato svolti nel biennio precedente secondo un programma di audit coerente con i requisiti della norma di riferimento.
- Per i servizi **eIDAS e SPID**:
    - La non esecuzione di un Risk Assessment completo;
    - La mancata applicazione o efficacia di uno o più controlli operativi, previsti dal "Trust Service Practice Statement", se non rilevata e già oggetto di specifica azione correttiva;
    - La mancata periodica rivisitazione e revisione della valutazione dei rischi;
- Nel caso di servizi **SPID**, la non corretta applicazione dei requisiti relativi al Regolamento di attuazione UE 2015/1502;
- Per il servizio di **Conservazione**:
    - la certificazione a fronte della Norma UNI CEI EN ISO/IEC 27001, che può essere condotta da un qualsivoglia Organismo di Certificazione, purché accreditato a fronte del Regolamento (UE) 765/2008, lo scopo di certificazione non comprende i servizi di conservazione a norma;
    - Qualunque altra risultanza di verifica, riferita a scostamenti dall'efficace adempimento ai requisiti previsti dalla Check List di AgID, se tali Non Conformità risultino potenzialmente in grado di inficiare il processo di conservazione o l'integrità, disponibilità e riservatezza delle informazioni soggette a conservazione, la stessa risultanza dovrà essere classificata come Non Conformità maggiore.
- La mancata preventiva comunicazione al DNV GL, per le opportune valutazioni, delle modifiche sostanziali:
    - che impattano sulla sicurezza;
    - variazioni significative sull'architettura dei prodotti/sistemi IT utilizzati per l'erogazione del servizio;

- variazioni geografiche dei sistemi IT utilizzati per l'erogazione del servizio;

- La mancata gestione / chiusura di una o più NC minori;
- Il mancato svolgimento di attività di Vulnerability Assessment (VA) e Penetration Test (PT);

In caso di NC maggiori le Organizzazioni, già in possesso di accreditamento da parte di AGID, devono prevedere di inviare una risposta immediata a DNV GL entro **5 (cinque) gg** lavorativi, con l'indicazione dei provvedimenti adottati per tamponare la/le criticità incontrate.

Nel caso dei **Conservatori**, per le NC maggiori registrate in vigenza dell'Accreditamento rilasciato da AgID, DNV GL deve segnalare tale evento alla stessa Agenzia, inviando direttamente una copia del Rapporto di Verifica, con le modalità di firma e invio utilizzate per l'invio dello stesso rapporto all'Organizzazione.

Entro i successivi **5 (cinque) gg** lavorativi, per **eIDAS e SPID**, mentre **15 (quindici) gg** lavorativi per i **Conservatori**, dovrà essere definita l'analisi delle cause e la pianificazione delle azioni necessarie per eliminarle e/o mitigarle in modo da avere come risultato un rischio di disservizio / non conformità valutato accettabile.

DNV GL valuterà le azioni proposte, darà una sua valutazione e pianificherà una verifica di Follow UP per la verifica della chiusura e dell'efficacia delle azioni proposte e accettate entro e non oltre **90 (novanta) gg** dall'ultima data di audit.

Per i servizi **eIDAS e SPID**:

Se nel processo di valutazione (iniziale, rinnovo, sorveglianza), **dovessero emergere della NC maggiori riferibili anche alla norma ISO/IEC 27001 (versione applicabile)** si dovrà effettuare una verifica su tale norma, con un tempo minimo, aggiuntivo, assimilabile a una sorveglianza, per verificare la robustezza sistemica e tecnica, tenendo conto delle sinergie/interazioni con la norma ETSI EN 319 401.

4.9.2 NC di categoria 2 (Minore)

Una Organizzazione TSP può essere certificata con non conformità in sospeso, a condizione che questa non influenzi la capacità del TSP di soddisfare il servizio previsto.

In caso di NC minori le Organizzazioni, già in possesso di accreditamento da parte di AgID, devono prevedere di inviare una risposta a DNV GL entro **10 (dieci) gg** lavorativi, con la definizione dell'analisi delle cause e la pianificazione delle azioni necessarie per eliminarle e/o mitigarle in modo da avere come risultato un rischio di disservizio / non conformità valutato accettabile.

DNV GL valuterà le azioni proposte, darà una sua valutazione e la valutazione della chiusura e dell'efficacia delle azioni proposte e accettate sarà effettuata durante la successiva attività di audit (sorveglianza o rinnovo).

Questa decisione alla certificazione è subordinata alla realizzazione di azioni correttive **entro 90 (novanta) gg** dopo la conclusione della verifica (a seconda del tipo e della criticità della/e correzione/i).

L'Organizzazione è obbligata al termine dei tempi per la gestione delle Azioni Correttive a inviare a DNV GL evidenze della gestione / chiusura delle stesse per una desk review prima della verifica successiva.

4.10 Sospensione o Revoca della Certificazione

Non Conformità maggiori che pregiudicano il corretto svolgimento dei servizi fiduciari possono portare alla sospensione o anche alla revoca della certificazione.

DNV GL comunicherà a ACCREDIA la sospensione o revoca della certificazione.

L'Organizzazione è responsabile della comunicazione a AgID delle sospensione o revoca della certificazione.

4.11 Trasferimenti della certificazione

I trasferimenti delle certificazioni dovranno essere garantiti solo dopo un riesame dell'intera pratica (precedenti rapporti di almeno un biennio) fatta da DNV GL subentrante, con un sopralluogo presso la sede centrale del TSP e 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.

DNV GL subentrante potrà farsi carico delle attività di valutazione, nell'ambito della validità del certificato già esistente.

4.12Polizza assicurativa

Durante la fase contrattuale e, in particolare, durante la fase di **STAGE 1**, dovrà essere verificato il livello di responsabilità civile massimo assunto dal **TSP** nei confronti del propri clienti.
A questo livello di responsabilità dovrà corrispondere un'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.

REGOLAMENTO PARTICOLARE PER LA CERTIFICAZIONE DEI SERVIZI eIDAS, SPID e CONSERVATORI

4.13 Registri delle organizzazioni certificate

Dopo l'approvazione del Rapporto del Gruppo di Audit, per come eventualmente integrato a fronte delle decisioni del Technical Reviewer, DNV GL provvede alla firma digitale con marca temporale dello stesso rapporto e ad inviarlo via PEC all'Organizzazione, affinché quest'ultima possa inviarlo ad AgID per il prosieguo dell'iter di accreditamento pubblico.

L'Organizzazione deve inviare a AgID tutta la documentazione relativa alle attività di audit al fine di ottenere l'accreditamento tramite PEC.
AgID pubblicherà sul suo sito l'elenco dei QTSP (Qualified Trust Service Provider) e delle organizzazione ACCREDITATE.

Si chiarisce che la qualifica di TSP, QTSP dell'Organizzazione è una responsabilità di AgID (Agenzia per l'Italia Digitale) e non del DNV GL e l'emissione del Certificato di Conformità non presuppone l'automaticità della stessa qualifica.

4.14 Uso del marchio di certificazione

L'Organizzazione, una volta certificata, deve richiedere a AgID il marchio di certificazione come QTSP per i servizi eIDAS.

Per i servizi eIDAS, SPID e Conservatori le organizzazioni accreditate saranno inserite da AGID in in apposito elenco pubblicato sul loro stesso sito.

Per le certificazioni SPID e Conservatori, non sono previsti specifici marchi di certificazione.