AGID | Agenzia per l'Italia Digitale

Vigilanza sui *servizi fiduciari qualificati, PEC, SpID, conservazione a norma*

(art. 14-bis, c2.i del Codice dell'Amministrazione Digitale)

Rapporto di riepilogo

gennaio-dicembre 2021

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Presidenza del Consiglio dei Ministri

Indice

1 PREFAZIONE

La presente relazione illustra le attività di vigilanza svolte nel 2021 dall'Agenzia per l'Italia Digitale ("AgID") ai sensi dell'art. 14-bis, comma 2, lettera i) del Codice dell'Amministrazione Digitale (CAD)[1].

L'esercizio delle funzioni di vigilanza in materia di identificazione elettronica *e trusted services* è volto a prevenire irregolarità, malfunzionamenti o disservizi nei processi di erogazione, verificando che i soggetti vigilati operino nel rispetto di regole e requisiti definiti e mutuamente riconosciuti tra agli Stati Membri dell'Unione Europea con l'obiettivo di rafforzare la fiducia dei cittadini nelle transazioni on line e favorire lo sviluppo dell'economia digitale[2]; mira altresì ad accertare presunte violazioni da cui possono derivare utilizzi impropri o a scopo fraudolento di tali servizi, esponendo l'utente al rischio di falsificazioni o di furti di dati.

Per tali finalità, l'Agenzia, nel suo ruolo di autorità di vigilanza, svolge **accertamenti di tipo ispettivo** e promuove **verifiche in via preventiva**, in un'ottica di miglioramento continuo dei processi per la qualità e la sicurezza dei servizi.

I poteri di vigilanza trovano fondamento in un **quadro regolatorio** costituito da norme comunitarie e nazionali e vedono coinvolti una rete di ***stakeholder*** - gli utenti[3], le istituzioni e gli stessi operatori ai quali si applicano le funzioni di vigilanza - ciascuno con diversi profili di interesse e di aspettative per le specifiche componenti dei servizi, che ne influenzano lo sviluppo e l'evoluzione.

La vigilanza consente di acquisire elementi per individuare e pianificare gli interventi correttivi ed evolutivi, sia dal punto di vista delle specifiche modalità realizzative di interesse dei gestori, sia per quanto riguarda gli aggiornamenti del quadro normativo a cura degli enti regolatori, sia con rifermento alle responsabilità degli utenti nell'utilizzo consapevole e secondo specifica dei servizi fruiti. L'Agenzia, con la presente relazione, rende conto annualmente delle attività svolte, informando gli *stakeholder* e il pubblico dei temi più rilevanti trattati nell'anno trascorso, dei problemi riscontrati e dei principali risultati relativi alle componenti dei servizi oggetto di esame.

---

[1] L'art. 14-bis, comma 2, lettera i) del decreto legislativo 7 marzo 2005, n. 82, s.m.i. recante il Codice dell'Amministrazione Digitale (CAD) prevede che AgID svolga «[…] *vigilanza sui servizi fiduciari ai sensi dell'articolo 17del regolamento UE 910/2014 ("Regolamento eIDAS") in qualità di organismo a tal fine designato, sui gestori di posta elettronica certificata, sui soggetti di cui all'articolo 34, comma 1-bis, lettera b), nonché' sui soggetti, pubblici e privati, che partecipano a SPID di cui all'articolo 64; nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'articolo 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza*».

[2] Il Regolamento (UE) n. 910/2014 (eIDAS, electronic IDentification Authentication and Signature), in vigore dal 1 luglio 2016, *mira a rafforzare la fiducia nelle transazioni elettroniche enel mercato interno, fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche*.

[3] Gli utenti dei servizi vigilati ai sensi dell'art. 14-bis, comma 2, lettera i) del CAD (servizi fiduciari qualificati tra i quali ad esempio i servizi di firma digitale, PEC, conservazione e SpID) sono persone fisiche e persone giuridiche (cittadini, imprese, pubbliche amministrazioni).

La relazione è giunta alla sua quinta edizione. La pandemia da Covid-19 e le iniziative governative correlate hanno dato nuovo impulso allo sviluppo dei servizi *on line*, favorendo anche la diffusione e l'utilizzo dei servizi quali la firma digitale e l'identà digitale che, proprio perché abilitanti le transazioni on line con le pubbliche amministrazioni, hanno fatto registrare un incremento considerevole dei volumi, con **oltre 29 milioni di certificati qualificati di firma attivi e 27 milioni di identità digitali SpID gestite**[4]**,** valori questi ultimi che risultano raddoppiati rispetto al 2020 e quintuplicati rispetto al 2019. Nel caso dei servizi SPID, l'aumento esponenziale delle identità gestite nel 2021 è stato determinato anche dall'entrata in vigore delle disposizioni[5] che obbligano le pubbliche amministrazioni a rendere accessibili i servizi *on line* mediante SpID, Carta di Identità Elettronica (CIE) e Carta Nazionale dei Servizi (CNS).

Il 2021 ha visto importanti progressi nelle attività gestite da AgID per l'attuazione del **nuovo quadro normativo di riferimento per la PEC**[6] **e per i servizi di conservazione a norma**. Nel caso della PEC, con l'emissione (a giugno 2021), del documento "REM SERVICES – Criteri di adozione degli standard ETSI – Policy IT" e il conseguente avvio del percorso di standardizzazione[7], sono stati completati i lavori del gruppo istituito da AgID (a settembre 2019) per l'aggiornamento delle regole tecniche e l'evoluzione della PEC verso il nuovo servizio di recapito certificato qualificato ("REM") conforme al Regolamento eIDAS. Per i servizi di conservazione, è stato adottato il Regolamento[8] previsto all'art. 34, comma 1-bis, del CAD, che definisce i nuovi criteri per la fornitura del servizio di conservazione dei documenti informatici, nonché i requisiti (generali, di qualità, di sicurezza e di organizzazione) necessari per la fornitura del servizio.

---

[4] Dati al 31 dicembre 2021.

[5] Dal 1 ottobre 2021 i servizi pubblici digitali sono accessibili con SPID, Carta d'Identità Elettronica (CIE) e Carta Nazionale dei Servizi (CNS), in sostituzione dell'accesso mediante credenziali proprietarie delle singole amministrazioni. L'iniziativa è stata avviata con la Legge 11 settembre 2020, n.120, che ha reso efficaci le disposizioni del decreto "Semplificazione e innovazione digitale".

[6] L'art. 8 del decreto legge n. 135 del 14 dicembre 2018, s.m.i. ha introdotto disposizioni per l'adeguamento del servizio PEC ai requisiti del Regolamento eiDAS, prevedendo in particolare che "*sentita l'Agenzia per l'Italia Digitale e il Garante per la protezione dei dati personali, sono adottate le misure necessarie a garantire la conformità dei servizi di posta elettronica certifica-ta (PEC), di cui agli articoli 29 e 48 del decreto legislativo n. 82 del 7 marzo 2005, al regola-mento (UE) n. 910 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. A far data dall'entrata in vigore del suindicato DPCM, l'articolo 48 del decreto legislativo n. 82 del 2005 è abrogato*".

[7] Il gruppo di lavoro, coordinato da AgID, si è orientato verso l'implementazione del modello REM (servizio di recapito certificato qualificato) basato sugli standard ETSI. Dall'analisi è stata avviata una interlocuzione con il Comitato ESI che, a seguito di successive sessioni di lavoro, ha portato a integrare gli standard ETSI REM giungendo (28 gennaio 2021 alla definizione della REM Baseline (contenente gli elementi di interoperabilità essenziali al dialogo tra provider) approvata in forma di draft dal Comitato ESI. Tale Baseline è stata sottoposta, su iniziativa di ETSI, a Plug test, a seguito dei quali ETSI ha deciso di completare il set di standard REM con un nuovo documento – il Draft ETSI EN 319 532-4 (V1.1.7).

[8] Il Regolamento, adottato con Determinazione n. 455/2021, integra quanto già definito nell'ambito delle Linee guida sulla formazione, gestione e conservazione del documento informatico, emesse a settembre 2020. Il Regolamento è in vigore il 1° gennaio 2022, data a partire dalla quale è abrogata la Circolare AgID n. 65/2014.

In considerazione degli sviluppi *in itinere* per la PEC e per i servizi di conservazione a norma, i **22 procedimenti di verifica** avviati nel corso del 2021 hanno riguardato principalmente i gestori di identità digitale SpID (10 procedimenti) e i prestatori di servizi fiduciari qualificati (9 procedimenti). L'allentamento delle restrizioni sugli spostamenti in ambito nazionale in determinati periodi dell'anno, ha consentito sia la conduzione di **verifiche ispettive da remoto** (16 su 22)**,** che l'esecuzione di **ispezioni *on site*** (6 su 22)**,** in entrambi i casi con l'apporto di competenze specialistiche dal Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza[9], dal Cert-AgID[10] e da auditor specializzati di organismi di certificazione per gli aspetti prevalentemente metodologici.

Parallelamente alla conduzione dei procedimenti di verifica, nel 2021 sono proseguite le attività per la realizzazione della sistema informatico di supporto all'espletamento delle funzioni di vigilanza[11] e sono state rilasciate le prime **funzioni per la raccolta e la gestione dei dati strutturati**[12] dai soggetti vigilati. In tale ambito è stata avviata l'acquisizione delle notifiche di incidenti/malfunzionamenti con tali nuove modalità -che indipendentemente dalla tipologia di servizio, prevedono un metodo uniforme di classificazione e gestione degli eventi impattanti la regolarità del servizio - con emissione delle istruzioni operative ad uso dei gestori. Per i dati relativi ai servizi erogati, sono state pubblicate le *Linee guida per l'invio dei dati periodici relativi ai servizi fiduciari e ai servizi PEC* (marzo 2021)[13] e sono stati completati i documenti tecnici[14] per la raccolta dei dati SpID attraverso interfacce applicative. Dopo una fase di adeguamento e di avviamento da parte dei gestori, è prevista l'attivazione a regime delle nuove modalità nel secondo semestre 2022.

A gennaio 2021 è entrata in vigore una nuova versione del **Regolamento di vigilanza**[15], emessa per recepire le modifiche all'art. 14 bis, comma 2, lett. i) del CAD (e articoli correlati) introdotte dal decreto-legge 16 luglio 2020, n. 76 s.m.i.

Alle attività sopra accennate sono dedicate specifiche sezioni della relazione; nella sezione introduttiva si richiamano le informazioni di contesto sulla vigilanza, evidenziando eventuali modifiche intervenute rispetto al 2020.

---

[9] La collaborazione ricade nell'ambito dell'accordo stipulato a novembre 2018 (https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/03/06/agid-guardia-finanza-danno-il-ad-azioni-congiunte-rafforzare-fiducia-nelleconomia).

[10] (https://cert-agid.gov.it). Il Cert-AgID è la struttura di AgID che da maggio 2020, a seguito dell'entrata in vigore delle "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano" (DPCM 8 agosto 2019), ha sostituito il CERT-PA. Fornisce supporto su tutti i temi riguardanti trasversalmente gli aspetti di sicurezza informatica relativi ai progetti a cui AgID partecipa in maniera diretta o indiretta.

[11] Piattaforma https://trustservices.agid.gov.it/.

[12] Dati relativi alle notifiche di incidenti/malfunzionamenti; dati periodici di riepilogo sui servizi; dati relativi all'anagrafica dei soggetti vigilati.

[13] Determinazione n. 259/2021

[14] Documenti tecnici pubblicati sul sito AgID (https://www.agid.gov.it/it/agenzia/vigilanza): Documenti che definiscono le modalità per la raccolta dei dati attraverso piattaforma informatica (Documento Tecnico Acquisizione Dati e allegati; Specifiche dei formati e dei tracciati dei dati relativi ai servizi SpID).

[15] Determinazione n. 74/2021 del 19/01/2021. A gennaio 2022 (Determinazione n. 1/2022 del 12/01/2022) è stata adottata una successiva versione, per recepire le modifiche introdotte dall'art.. 27, comma 1, lettera d) del decreto legge n. 152/2021.

I risultati delle verifiche sono esposti in forma anonima ed in modalità aggregata.

I dati si riferiscono al 31/12/2021.

2 LE FUNZIONI DI VIGILANZA SVOLTE DA AGID

2.1 Richiami relativi al quadro normativo

Le funzioni di vigilanza svolte da AgID trovano fondamento in un contesto di regole nazionali e comunitarie. In base al Codice dell'Amministrazione Digitale (CAD)[16], AgID svolge funzioni di vigilanza sui *prestatori di servizi fiduciari qualificati*, sui *gestori di posta elettronica certificata*, sui *conservatori di documenti informatici* (soggetti di cui all'art. 34, comma 1 bis del CAD, che svolgono attività di conservazione di documenti informatici per le pubbliche amministrazioni) e sui *soggetti pubblici e privati che partecipano a SpID di cui all'art. 64*, tra i quali i *gestori di identità digitale SPID*. Nell'esercizio di tale funzione l'Agenzia può irrogare per le violazioni accertate a carico dei soggetti vigilati le sanzioni amministrative di cui all'art. 32-bis in relazione alla gravità della violazione accertata e all'entità del danno provocato all'utenza.

Al regime di identificazione elettronica SPID e ai servizi fiduciari qualificati, si applica la disciplina del Regolamento UE 910/2014 (Regolamento eIDAS). Con riferimento, in particolare ai servizi fiduciari qualificati, AgID è l'organismo di vigilanza designato in Italia, con gli specifici compiti previsti dal Regolamento[17].

In virtù delle previsioni dell'art. 29 del CAD, l'obbligo di soddisfare i requisiti indicati nell'art. 24 del Regolamento eIDAS per i prestatori di servizi fiduciari qualificati si estende anche ai soggetti che intendono operare come gestori PEC.

Nel 2021 le funzioni di vigilanza sui soggetti qualificati o accreditati ai sensi del CAD hanno riguardato 19 prestatori di servizi fiduciari qualificati ("QTSP") (3 cessati nel corso del 2021), 19 gestori di posta elettronica certificata accreditati e 9 gestori di identità digitale SpID. Nel caso dei conservatori, nel corso del 2021 è stato adottato il Regolamento[18] che definisce i nuovi criteri per la fornitura del servizio di conservazione dei documenti informatici e specifica i requisiti generali, di qualità, di sicurezza e di organizzazione necessari per la fornitura del servizio. Il Regolamento integra quanto già definito nell'ambito delle Linee guida sulla formazione, gestione e conservazione del documento informatico, emanate a settembre 2020, ed è entrato in vigore il 1° gennaio 2022, data a partire dalla quale è abrogata la Circolare AgID n. 65/2014.

[16] art. 14-bis, comma2, lettera i)

[17] Il ruolo ed i compiti di un Organismo di vigilanza sonoindicati nell'art. 17 del Regolamento (UE) N.910/2014. Sono previste inoltre attività di collaborazione ed assistenza reciproca tra gli Organismi di vigilanza dei diversi Stati Membri

[18] Determinazione n. 455/2021

2.2 Le regole e le modalità di esecuzione

Le modalità di esecuzione della vigilanza e di esercizio dei poteri sanzionatori previsti dalle norme sono oggetto di un Regolamento[19], adottato nella prima versione a giugno 2018. A fine 2020 è stata completata una seconda stesura, per tenere conto delle modifiche normative intervenute e delle esperienze maturate a distanza di oltre due anni dalla prima emissione. La nuova versione è entrata in vigore a febbraio 2021.

I procedimenti di verifica gestiti nel 2021 fanno riferimento alla versione del Regolamento adottata nel 2018.

Il Regolamento richiama i principi generali della vigilanza: da un lato è volta ad accertare violazioni o irregolarità; dall'altro, è volta a favorire l'adozione di azioni preventive e di miglioramento continuo dei processi di erogazione dei servizi.

Le verifiche possono essere condotte su base documentale o prevedere anche l'esecuzione di verifiche ispettive, on site o da remoto; tale ultima modalità è stata quella più frequentemente seguita nel 2021 a causa delle restrizioni legate all'emergenza sanitaria.

Un procedimento di verifica può essere avviato a seguito di una segnalazione o nell'ambito di un programma di audit predisposto periodicamente, tipicamente con frequenza quadrimestrale, sulla base di indici di rischio[20]; nel 2021 la programmazione periodica ha dato priorità alle verifiche sui servizi erogati dai QTSP e dai gestori SPID con un'utenza più ampia, vista l'accresciuta rilevanza di tali servizi nel particolare periodo, dimostrata anche dall'aumento dei volumi, come si rileva al § 3.

I procedimenti di verifica si concludono in un tempo massimo di centottanta giorni, fatti salvi eventuali termini di sospensione, e possono portare alla formulazione di rilievi, distinti rispettivamente in 'Non Conformità[21]' e 'Osservazioni[22]'. Tutti i rilievi e le azioni conseguenti definite dai gestori sono oggetto di monitoraggio nell'ambito delle verifiche svolte d'ufficio e sono tenute sotto controllo fino alla completa attuazione, anche a procedimento concluso.

---

[19] https://www.agid.gov.it/it/agenzia/vigilanza - "Regolamento recante le modalità per la vigilanza e per l'esercizio del potere sanzionatorio ai sensi dell'art.32-bis del d.lgs. 7 marzo 2005, n.82 e successive modificazioni", adottato con Determinazione n. 191/2019 del 5 giugno 2019.

[20] L'indice di rischio relativo ad un gestore è previsto che sia valorizzato sulla base di alcune caratteristiche (dimensioni e tipologia di servizi e utenti; soluzioni tecnologiche adottate; segnalazioni pervenute; partner che gestiscono specifiche componenti del servizio; verifiche precedenti; analisi di tipo predittivo).

[21] Non Conformità: è una irregolarità o violazione accertata rispetto alle norme di riferimento (CAD, Regolamento eIDAS e norme attuative o correlate), classificata secondo tre livelli di gravità crescente: 'Lieve', 'Media', 'Grave'. Ciascuna Non Conformità richiede azioni correttive da adottare entro tempi massimi stabiliti.

[22] Osservazione: è una raccomandazione o spunto per il miglioramento; ha l'obiettivo di invogliare i gestori a riesaminare i processi e ad adottare in via continuativa azioni volte ad adeguare l'offerta di servizi alle potenzialità offerte dalle evoluzoni tecnologiche in itinere, a migliorare la qualità erogata, nonché a prevenire situazioni di degrado.

2.3 Le parti interessate (*stakeholder*)

Le funzioni di vigilanza vedono coinvolti a diverso titolo più organizzazioni esterne.

- **Istituzioni nazionali**: organizzazioni preposte alla definizione degli obiettivi e degli indirizzi strategici che l'Agenzia deve mettere in atto; organizzazioni alle quali compete dotare AgID, in quanto Organismo di vigilanza designato in Italia ai sensi dell'art. 17, comma 2 del Regolamento eIDAS, dei poteri e delle risorse adeguate per l'esercizio dei compiti previsti; altre organizzazioni nazionali direttamente coinvolte nei processi primari della vigilanza[23]
- **Soggetti vigilati:** soggetti ai quali si applicano le funzioni di vigilanza. Si veda il § 3.
- **Utenti**: persone fisiche (cittadini) o giuridiche (imprese e pubbliche amministrazioni) che usufruiscono dei servizi erogati dai soggetti vigilati.
- **Istituzioni internazionali**: enti regolatori o di standardizzazione; principali organizzazioni europee che operano ai fini dell'attuazione del Regolamento eIDAS, tra i quali:
    - la Commissione Europea, competente per l'emanazione degli atti di esecuzione, o alla quale fanno riferimento i procedimenti di notifica. È anche l'istituzione alla quale AgiD, in quanto organismo di vigilanza designato, deve annualmente riferire, in attuazione delle previsioni di cui al punto (40) ed all'art. 17, comma 6, del Regolamento eIDAS;
    - ENISA (Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione), soggetto destinatario delle notifiche di violazioni alla sicurezza da parte di AgID, in attuazione delle previsioni di cui al punto (39) ed all'art. 19 del Regolamento eIDAS;
    - FESA (*Forum of European Supervisory Authorities for trust service providers*), associazione degli Organismi di vigilanza europei previsti all'art. 17 del Regolamento eIDAS, avente lo scopo di supportare e migliorare la cooperazione e l'assistenza reciproca, secondo quanto previsto dallo stesso Regolamento eIDAS. Sono svolti periodici incontri - di regola semestrali - per consentire la condivisione e lo scambio di informazioni e di buone pratiche.
    - Organismi di vigilanza degli altri Stati Membri. Con tali organismi sono previsti dal Regolamento eIDAS rapporti di collaborazione ed assistenza reciproca, nonché l'invio delle notifiche di incidenti di sicurezza e perdita di integrità dei dati ricevute dai QTSP nazionali che abbiano impatto su altri Stati Membri.

[23] Ad esempio, il Garante, che, con proprio personale può prendere parte alle attività ispettive presso i gestori SpID, o ACCREDIA, l'ente nazionale per l'accreditamento degli organismi di certificazione, con il quale AgID collabora ai fini della definizione degli schemi di accreditamento per le valutazioni di conformità di parte terza nell'ambito dei servizi vigilati.

3 TASSONOMIA DEI SOGGETTI VIGILATI

Nel corso del 2021 le funzioni di vigilanzahanno riguardato principalmente tre tipologie di soggetti, alle quali si fa riferimento nel presente rapporto: i gestori di identità digitale SpID ("IdP"), i prestatori di servizi fiduciari qualificati ("QTSP") e i gestori PEC. Si tratta di soggetti qualificati o accreditati da AgID ed iscritti in elenchi pubblici[24].

Per l'altra categoria di soggetti ai quali si applicano le funzioni di vigilanza previste all'art. 14-bis, comma 2, lettera i) del CAD, i conservatori di documenti informatici, a partire dal 1 gennaio 2022 è prevista l'iscrizione su una piattaforma dedicata[25], all'interno della quale il conservatore attesta, mediante un'autocertificazione, il possesso dei requisiti di qualità, sicurezza e organizzazione, condizione necessaria per l'erogazione di servizi di conservazione per conto della Pubblica Amministrazione. La piattaforma nel corso del 2021 era in fase di realizzazione.

Per le tre categorie sopra richiamate, per le quali nel 2021 sono state svolte attività di vigilanza, nei paragrafi che seguono si presentano in forma anonima ed in modalità aggregate le principali caratteristiche[26], evidenziando le modifiche rispetto alla situazione relativa al 2020.

[24] Elenco dei prestatori di servizi fiduciari attivi in Italia (https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia);

Elenco dei gestori PEC accreditati (https://www.agid.gov.it/it/piattaforme/posta-elettronica-certificata/elenco-gestori-pec);

Elenco degli Identy Provider accreditati (https://www.agid.gov.it/it/piattaforme/SpID/identity-provider-accreditati)

[25] Marketplace dei servizi di conservazione

[26] Le caratteristiche che riguardano la numerosità e la tipologia di utenti; la rete dei partner tecnologici; i volumi gestiti concorrono a valorizzare indici di rischiio, che sono esaminati ai fini della programmazione delle verifiche periodiche.

3.1 Prestatori di servizi fiduciari qualificati (QTSP)

Nel 2021 non sono stati qualificati nuovi prestatori di servizi fiduciari, mentre **tre prestatori qualificati hanno cessato la loro attività.**

Al 31/12/2021 risultano iscritti nell'elenco dei prestatori di servizi fiduciari qualificati attivi in Italia 19 soggetti, qualificati per uno o più servizi fiduciari (servizi di firma, sigillo, marche temporali e certificati qualificati per siti web).

Si rilevano per i soggetti iscritti nell'elenco dei QTSP le seguenti caratteristiche:

- **servizi erogati e volumi gestiti**: come si rileva dalla *Trusted list* italiana[27], tutti i QTSP sono qualificati per i servizi di firma, ad eccezione di 1 soggetto che è qualificato solo per il servizio di validazione temporale; 3 QTSP sono qualificati per le quattro tipologie di servizi. 4 QTSP coprono il 93% dei certificati qualificati per firma remota, 4 QTSP, coprono oltre l'83% delle marche temporali qualificate;**caratteristiche dell'utenza**: 9 QTSP operano solo per una clientela predefinita e limitata (interna al gestore stesso o limitata ad una rete specifica di utenze, come ad esempio la rete dei dottori commercialisti, la rete dei notai, la rete dei tabaccai); 13 gestori rilasciano firme sigilli certificati o marche sia a clientela business che a persone fisiche (cittadini);
- **soluzioni tecnologiche e partner**: per l'erogazione del servizio, alcuni QTSP si appoggiano all'infrastruttura software di un altro QTSP. Per alcuni gestori sono esternalizzate le attività di identificazione e gestione del processo di servizio nei confronti dei richiedenti.

Nel grafico che segue si riporta un estratto dell'andamento dei volumi dei servizi di firma e marca temporale al 31/12/2021, che costituiscono l'offerta di servizi più consistente per questa tipologia di soggetti vigilati.

[27] Si consulti EU Trust Services Dashboard

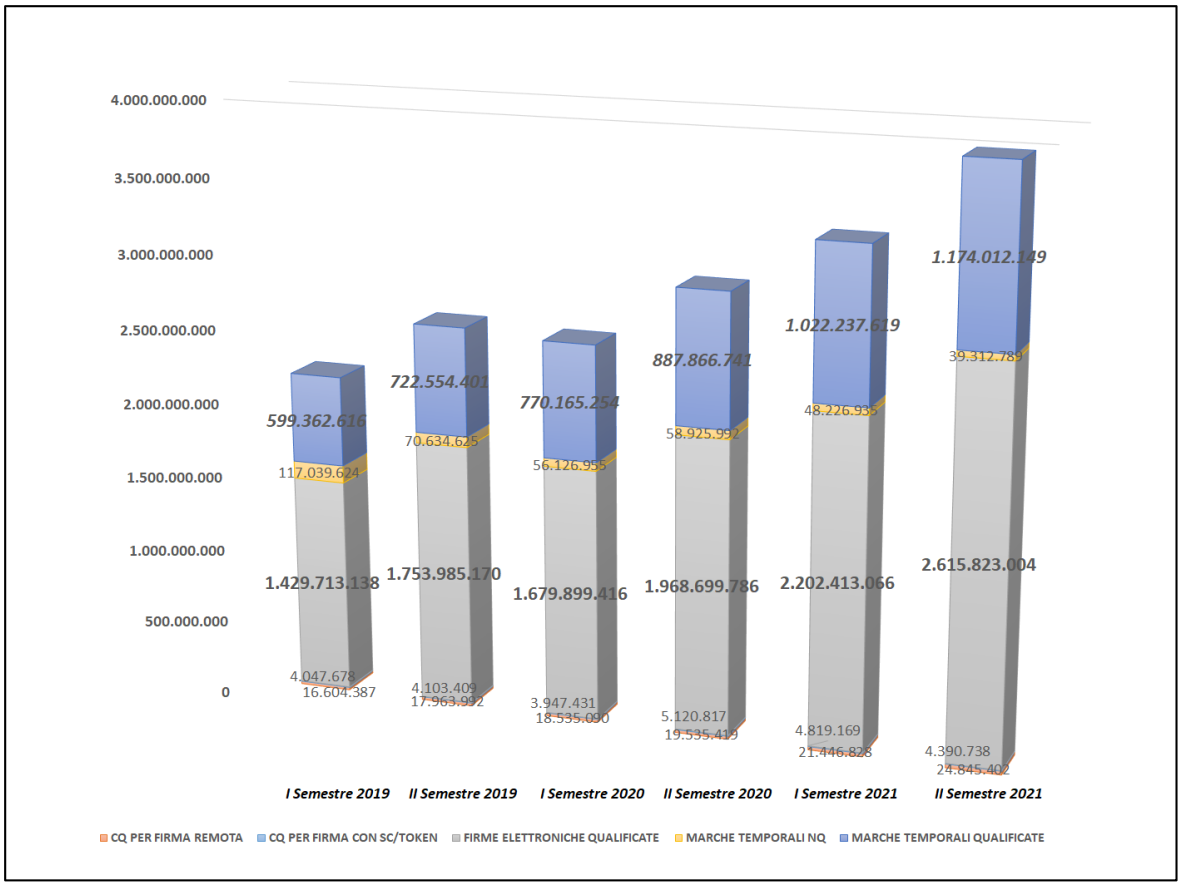

Fig. 3.1 —Andamento servizi di firma e marca temporale [gennaio-dicembre 2021, dati aggregati per semestre]

Da dicembre 2020 si nota un andamento in crescita fino a dicembre 2021 del 25% per le firme elettroniche qualificate e di oltre il 26% delle marche temporali qualificate.

3.3 Gestori PEC

Al 31/12/2021 risultano iscritti nell'elenco dei gestori PEC accreditati 19 oggetti. Un nuovo gestore è stato iscritto nel corso del 2021.

Si rilevano per i 19 soggetti iscritti nell'elenco dei gestori PEC le seguenti caratteristiche:

- **volumi gestiti:** 1 solo gestore copre circa l'80% dei domini e il 60% delle caselle; 2 gestori insieme coprono l'85% circa delle caselle totali;
- **caratteristiche dell'utenza**: a parte alcuni gestori, per lo più i soggetti pubblici, che gestiscono ciascuno domini e caselle di una clientela predefinita e limitata ad una rete specifica di utenze per una percentuale inferiore all'1%, gli altri soggetti e soprattutto quelli a cui fanno riferimento i volumi più rilevanti, gestiscono domini e caselle sia per clientela business che per persone fisiche (cittadini);
- **soluzioni tecnologiche e partner:** per l'erogazione del servizio, alcuni gestori PEC si appoggiano all'infrastruttura software di altro gestore. Più gestori distribuiscono il servizio attraverso una rete di partner commerciali ramificata sul territorio.

Nei grafici che seguono si riporta un estratto dell'andamento al 31/12/2021 dei volumi di domini, caselle PEC e messaggi scambiati, indicatori che confermano l'importanza dei numeri di questo servizio (totale annuo di 2.498.131.944 messaggi complessivamente scambiati nel 2021, rispetto al totale di 2.258.047.494 registrato nel 2020).

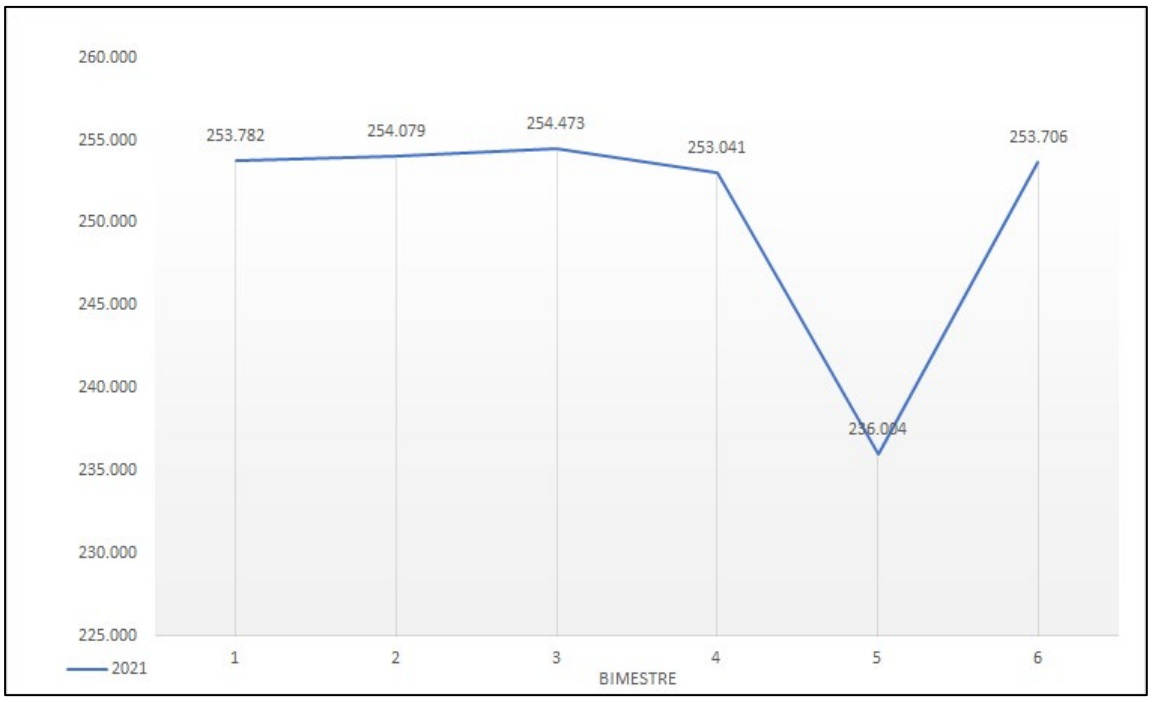

Fig. 3.2 - Andamento domini PEC nel 2021 (dati aggregati per bimestre)

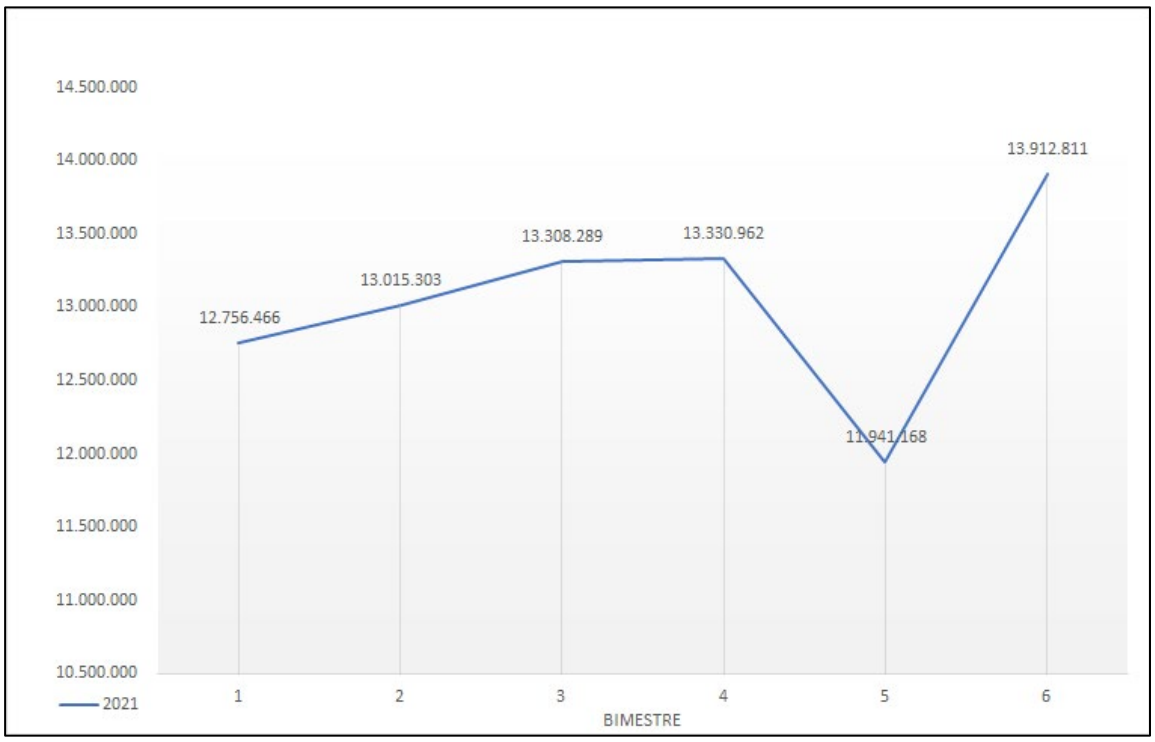

Fig. 3.3 - Andamento caselle PEC nel 2021 (dati aggregati per bimestre)

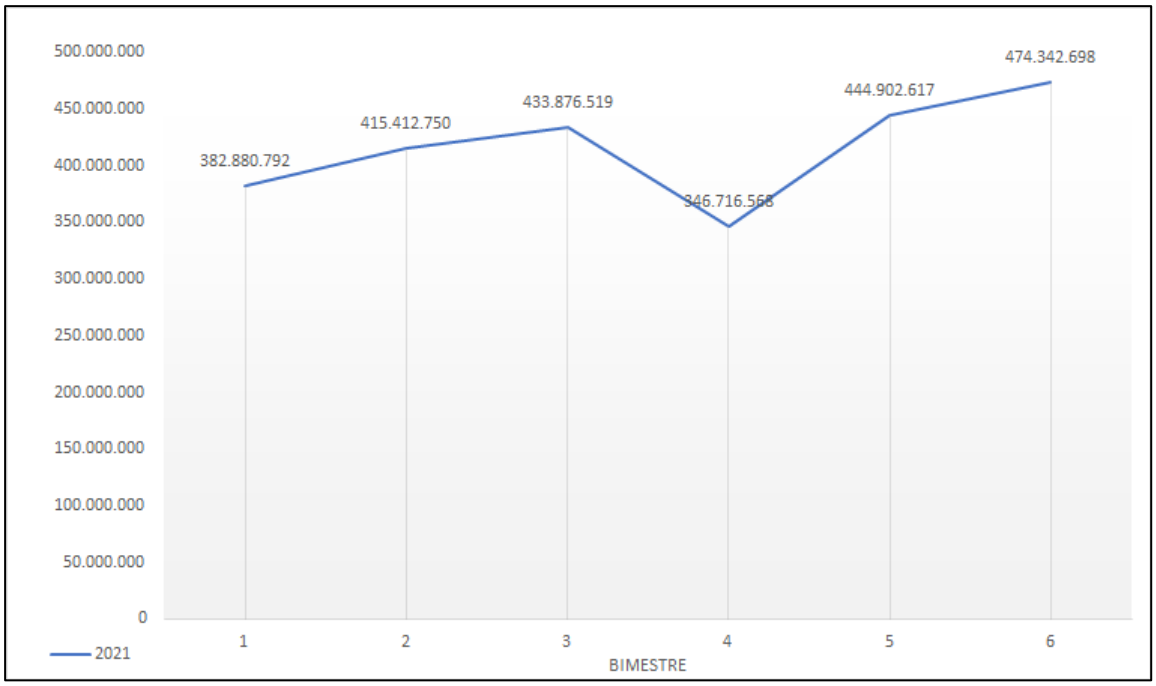

Fig. 3.4 - Andamento messaggi PEC nel 2021 (dati aggregati per bimestre)

3.5 Identity Provider SPID (IdP)

Nel 2021 sono state **rilasciate oltre 11.700.000 di identità**, per un totale di identità gestite al 31/12/2020 dai 9 IdP di oltre 27.000.000; un IdP ne gestisce circa l'82%, come si rileva dal grafico seguente.

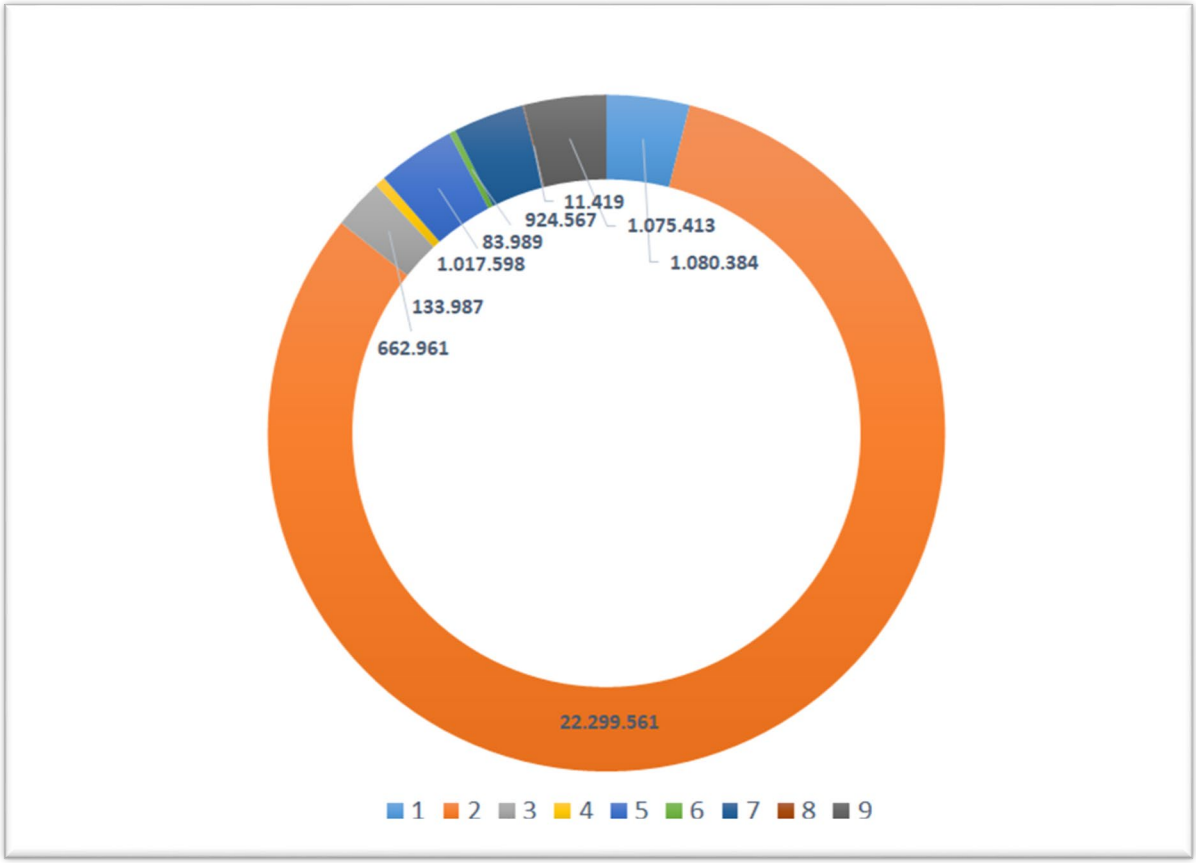

Fig. 3.7- Identità gestite per IdP a fine dicembre 2021

Come si rileva nel grafico che segue, **il totale delle identità a fine 2021 è quasi il doppio del valore registrato a fine 2020** ed è pari a cinque volte circa il valore registrato a fine 2019.

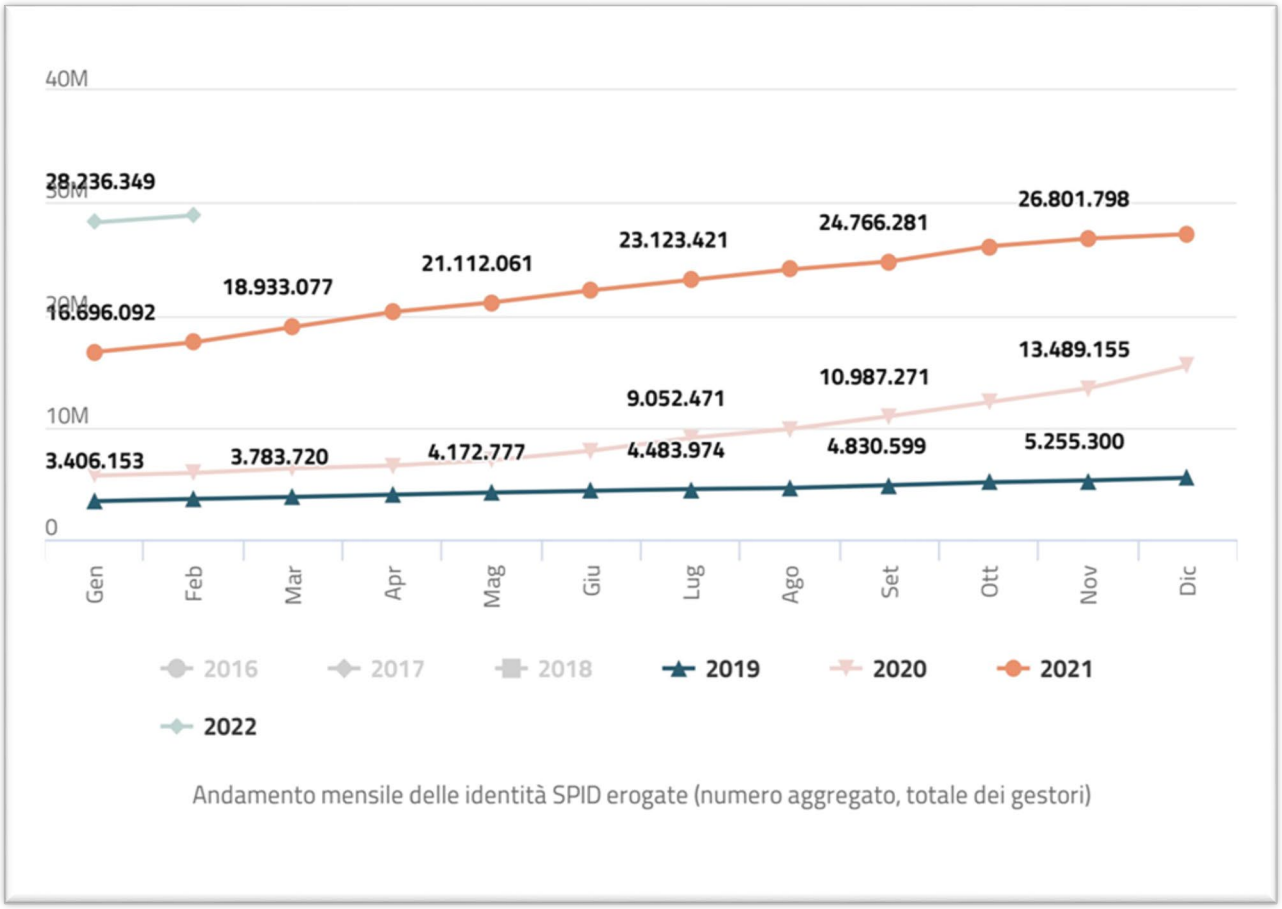

Fig. 3.8- Andamento delle identità gestite nel triennio 2019- 2021

Nel 2021 per tutti gli IdP si è registrato un considerevole aumento dei volumi di identità gestite rispetto al 2020. L'incremento considerevole rispetto al 2020 è stato certamente determinato anche dalle numerose iniziative legate al periodo Covid, che hanno richiesto l'accesso con SPID su diversi portali di pubbliche amministrazioni (bonus; transazioni con le pubbliche amministrazioni in modalità on line; ecc.), nonché dall'introduzione dell'obbligo di utilizzo dello SpID (e della CIE) come metodo per l'accesso ai servizi on line delle pubbliche amministrazioni.

Dalle relazioni annuali di riepilogo[28] fornite dai gestori, si rileva che i servizi più acceduti attraverso SpID riguardano servizi INPS (previdenza nazionale) (http://www.inps.it), Agenzia delle Entrate (https://SpID.agenziaentrate.gov.it); servizi comunali (pagamenti tasse/tributi); App IO (es. Green Pass); servizi regionali (es. prestazioni sanitarie; pagamenti bollo auto); bonus e cashback di Stato (https://access.mef.gov.it/oam/fed; https://app-backend.io.italia.it; https://SpID.18app.ita-

[28] La Convenzione che ciascun IdP stipula con AgID ai sensi dell'art. 10, comma 2 del DPCM 24 ottobre 2014 prevede che entro il 31 marzo di ciascun anno, il gestore predispone una relazione sui risultati conseguiti nel precedente esercizio; la relazione fornisce dati di riepilogo sui servizi, con indicatori di tipo quantitativo e qualitativo, con riferimento ad esempio ai volumi gestiti (identità rilasciate/revocate; richieste di assistenza attraverso il *Custome Care*), alle modalità di utilizzo del servizio (servizi più frequentemente acceduti), ai livelli di servizio eogati e ai risultati di periodiche valutazione degli utenti sulla qualità del servizio (indagini di *Customer Satisfaction*).

lia.it; https://SpID.cartadeldocente.istruzione.it); Camere di commercio (https://SpID.infocamere.it)); Istituzioni scolastiche/MIUR (https://SpID.pubblica.istruzione.it); pagamenti (https://pagopa.gov.it); servizi INAIL (prevenzione).

Ulteriori indicatori riferiti al servizio SPID sono disponibili nell'apposita sezione del portale di avanzamento digitale (https://avanzamentodigitale.italia.it/it/progetto/SpID).

4 PROCEDIMENTI DI VERIFICA NEL 2021

Le attività svolte nel 2021 hanno dovuto tenere conto, come nel 2020, delle esigenze e delle priorità connesse alla nota situazione di emergenza sanitaria, aspetti che hanno condizionato la pianificazione e la modalità di conduzione delle verifiche sui soggetti vigilati.

L'allentamento delle restrizioni sugli spostamenti in ambito nazionale ha consentito l'esecuzione di verifiche ispettive anche in presenza, unitamente alla conduzione di ispezioni da remoto. Come nell'anno precedente, anche nel 2021 le verifiche hanno visto l'apporto di competenze specialistiche dal Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza (nell'ambito dell'accordo stipulato a novembre 2018[29], in fase di rinnovo a fine 2021), dal Cert-AgID (https://cert-agid.gov.it) per gli aspetti principalmente legati alle misure di sicurezza e da *auditor* degli organismi di certificazione aggiudicatari della la procedura[30] che ha portato nel 2019 alla stipula di due contratti rispettivamente con Rina Services SpA e Bureau Veritas Italia SpA.

4.1 Riepilogo delle verifiche

Nel corso del 2021 sono stati attivati **22 procedimenti di verifica,** dei quali 6 a seguito di segnalazione esterna e 16 nell'ambito di verifiche programmate. Inoltre 6 verifiche sono state svolte in presenza le altre 16 da remoto.

Le verifiche che hanno comportato un maggior impegno sono certamente quelle condotte da remoto. La conduzione degli audit a distanza ha comportato delle limitazioni per l'esecuzione di alcuni controlli, che sono significativi solo se eseguiti in presenza, come per esempio i controlli relativi alle misure di sicurezza fisica implementate nei CED. È stato invece possibile analizzare senza limitazioni rilevanti le componenti di servizio che riguardano ad esempio gli aspetti di processo e di gestione dei sistemi.

Come si rileva dal grafico, i 22 procedimenti hanno riguardato i QTSP (9), i gestori SPID (10), e i gestori PEC (3)

[29] https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/03/06/agid-guardia-finanza-danno-il-ad-azioni-congiunte-rafforzare-fiducia-nelleconomia.

[30] RDO n. 2042442 in due lotti per l'acquisizione di servizi di supporto alle attività ispettive. I due contratti sono stati attivati a settembre 2019.

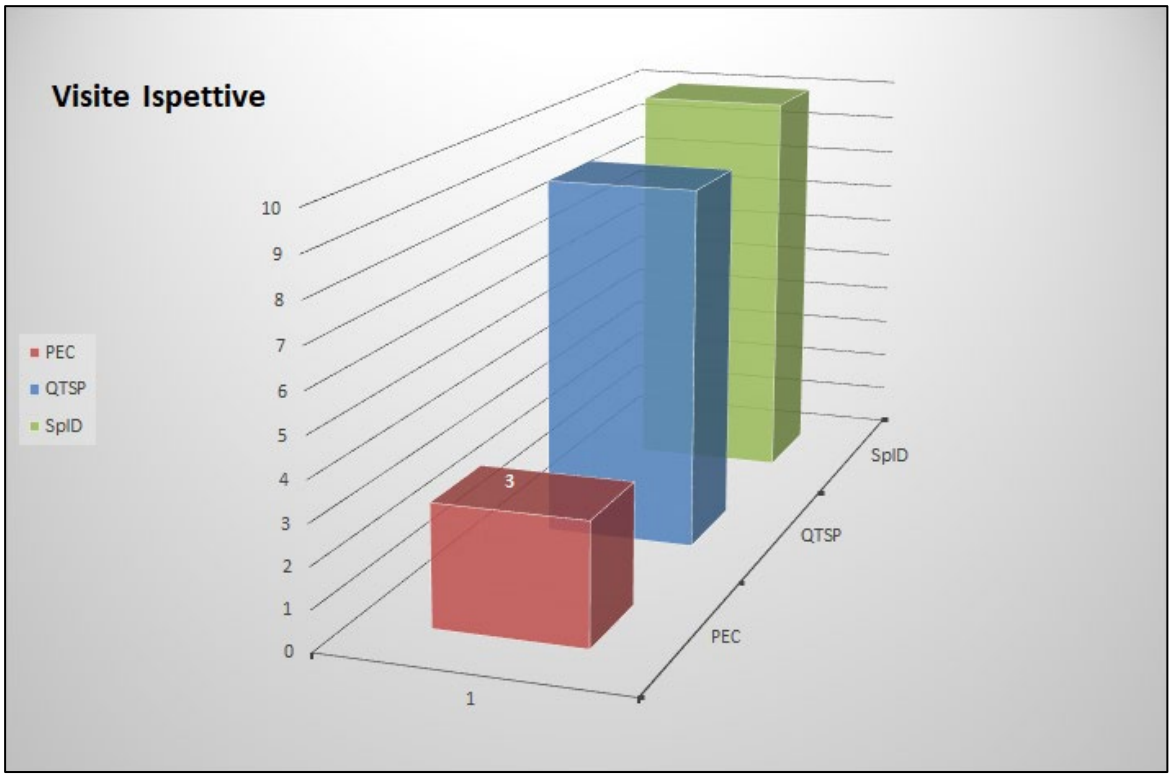

Fig. 4.1 —-Procedimenti di verifica avviati nel 2021

Per i 9 procedimenti in ambito QTSP, 2 procedimenti sono stati avviati su segnalazione. I 9 QTSP ispezionati, in riferimento ai volumi, coprono il 25% dei certificati qualificati per firma con SC/Token, il 25% dei certificati di firma remota, quasi il 40% delle firme elettroniche qualificate ed il 50% circa delle marche temporali qualificate; con riferimento, invece, alle caratteristiche dell'utenza, 4 QTSP rilasciano firme solo ad una clientela predefinita e limitata ad una rete specifica di utenza; gli altri 5 QTSP rilasciano firme, sigilli, certificati e marche temporali sia a clientela business che a persone fisiche.

Per i 3 procedimenti in ambito PEC, 1 procedimento è stato avviato su segnalazione.

I 10 procedimenti in ambito SPID hanno riguardato tutti i gestori (più procedimenti per un gestore); 3 sono stati avviati su segnalazione.

Le verifiche complessivamente svolte per le quattro tipologie di soggetti vigilati hanno portato:

- in 1 caso alla cessazione dell'attività per scelta del gestore, comunicata in fase di di ispezione;
- in 3 casi (2 riuniti) all'attivazione della fase sanzionatoria in entrambi i casi il procedimento era stato avviato su segnalazione.

4.2 Verifiche di *seconda parte* e componenti di servizio

Diversamente dalle verifiche di "terza parte" svolte dagli organismi di certificazione accreditati dall'ente nazionale di accreditamento, finalizzate a certificare la conformità di un sistema di gestione

ad una norma o ad uno standard internazionale, le verifiche svolte da AgID ai fini della vigilanza si configurano come verifiche di "seconda parte" e sono in genere diverse l'una dall'altra e limitate ad aspetti specifici ("componenti del servizio"), in relazione agli obiettivi di ciascuna verifica (verifica conseguente ad una segnalazione, o disposta a fronte di un evento negativo come per esempio un attacco informatico, o da programmazione).

Al fine di rendere comparabili i risultati ed in considerazione del fatto che le quattro tipologie di servizi, pur nelle diverse modalità realizzative, includono componenti analoghe, si è adottata una classificazione che prevede una nomenclatura standard per quelle comuni alle quattro tipologie di servizi vigilati. A titolo di esempio, sono comuni a tutti i servizi le seguenti componenti:

a) Organizzazione
b) Documentazione di riscontro
c) Politiche, procedure e misure di sicurezza
d) Infrastruttura per l'erogazione del servizio
e) Gestione del processo
f) Analisi dei rischi e VA/PT(Vulnerability Assessment e Penetration Test)
g) Gestione delle terze parti
h) Gestione e segnalazione di incidenti, malfunzionamenti e interruzioni di servizio
i) Piano di cessazione
j) Report periodici

A titolo di esempio:

- la componente "Organizzazione", fa riferimento all'insieme dei requisiti di ciascun servizio (QTS, PEC, SPID), inerenti l'organizzazione, le procedure e il personale);
- la componente "Documentazione di riscontro", riguarda la documentazione (Manuale operativo, Piano di sicurezza, ecc.) prevista ai fini della qualificazione o dell'accreditamento;
- la componente "Gestione del processo" riguarda l'insieme delle attività che attengono al processo specifico (QTS, PEC, SPID) in tutto il ciclo di vita del servizio (dall'avvio alla cessazione per singolo utente o azienda).

Le verifiche condotte nell'ambito dei 12 procedimenti hanno preso in esame alcune componenti, non necessariamente le stesse per le quattro tipologie di servizio. Alle componenti esaminate si riferiscono i rilievi indicati nel paragrafo che segue.

4.3 Riepilogo dei rilievi

Complessivamente sono stati formulati 139 **rilievi**, distinti in 98 "Non Conformità" e 41 "Osservazioni"; quasi il 45% dei rilievi ha riguardato i QTSP, il 48% è relativo ai gestori SPID e il resto ai gestori PEC.

Fig. 4.1- Totale dei rilievi e distribuzione per servizio

Tali dati si riferiscono alla totalità dei procedimenti sopra indicati, con esclusione di un procedimento per il quale il gestore ha comunicato la cessazione e nell'ambito del quale non sono stati quindi formulati rilievi.

Classificazione Rilievi	PEC	QTSP	SPID	Totale complessivo
Grave	2	4	4	10
Lieve	1	19	18	38
Media	4	26	20	50
OSSERVAZIONE	2	14	25	41
Totale complessivo	**9**	**63**	**67**	**139**

Tab.4.2 – Classificazione dei rilievi per servizio

La tabella che segue riporta in media sul singolo procedimento la numerosità dei rilievi per servizio divisi tra Non Conformità e Osservazioni.

Media Rilievi per Servizio	# Medio Non Conformità	# MEDIO Osservazioni
PEC	**2,33**	**0,67**
QTSP	**5,44**	**1,56**
SPID	**4,1**	**2,8**
Media complessiva	**4,41**	**2**

Tab. 4.3 – Media rilievi per procedimento secondo il Servizio

I rilievi sono stati formulati rispetto alle componenti di servizio esaminate nell'ambito dei procedimenti.

Le tabelle che seguono mostrano la distribuzione dei rilievi per servizio e per le specifiche componenti del servizio a cui sono riferiti.

Campo di Applicazione NC	Grave	Lieve	Media	OSSERVAZIONE	Totale complessivo
Gestione terze parti	2	6	7	9	24
Analisi dei rischi e VA/PT	1	5	9	5	20
Gestione del processo	4	2	9	6	21
Documentazione di riscontro		9	2	5	16
Formazione		1	4	7	12
Politiche e procedure di sicurezza	1	4	5	1	11
Piano di Cessazione		6		1	7
Organizzazione, ruoli e responsabilità		2	2	3	7
Gestione degli incidenti	2	1	2	1	6
log			4		4
Asset e change management		1	2		3
Piano della sicurezza			1		1
Conservazione dei dati sensibili		1			1
Commercializzazione dei Servizi				1	1
Infrastruttura per l'erogazione del servizio			2	2	4
Gestione e segnalazione di incidenti, malfunzionamenti e interruzioni di servizio			1		1
Totale complessivo	**10**	**38**	**50**	**41**	**139**

Tab.4.4 - Distribuzione dei rilievi per classificazione e componenti di servizio

Campo di Applicazione NC	PEC	QTSP	SPID	Totale complessivo
Gestione terze parti		8	16	24
Analisi dei rischi e VA/PT	1	9	10	20
Gestione del processo	3	11	7	21
Documentazione di riscontro		9	7	16
Formazione		5	7	12
Politiche e procedure di sicurezza	2	3	6	11
Piano di Cessazione	1	4	2	7
Organizzazione, ruoli e responsabilità		6	1	7
Gestione degli incidenti		3	3	6
Gestione dei log		1	3	4
Asset e change management		2	1	3
Piano della sicurezza			1	1
Gestione e segnalazione di incidenti, malfunzionamenti e interruzioni di servizio	1			1
Conservazione dei dati sensibili			1	1
Commercializzazione dei Servizi		1		1
Infrastruttura per l'erogazione del servizio 1		1	2	4
Totale complessivo	**9**	**63**	**67**	**139**

Tab.4.5 - Distribuzione dei rilievi per servizio e componenti

4.4 Analisi dei rilievi più ricorrenti

Il presente paragrafo è dedicato ad una breve analisi delle tipologie dei rilievi formulti per le componenti di servizio esaminate nell'ambito dei 21 procedimenti a cui sono riferiti.

Come si vede dalle Tab.4.4 e Tab.4.5, alle prime cinque linee di servizio fa riferimento oltre il 65% dei rilievi complessivamente riscontrati. In particolare alle tre componenti **Gestione delle terze parti**, **Analisi dei rischi e VA/PT**, **Gestione del processo** fa capo il maggior numero di rilievi.

La **Gestione delle Terze Parti** riguarda il complesso delle attività che i gestori devono svolgere per assicurare che, in caso di affidamento ad organizzazioni esterne di specifiche componenti di servizio[31], i subcontraenti siano dotati delle competenze, dell'affidabilità, dell'esperienza e delle qualifiche necessarie e che abbiano ricevuto una formazione adeguata in materia di norme di sicurezza e di protezione dei dati personali e in relazione agli obblighi ed alle procedure che devono essere seguiti nell'erogazione del servizio. I rilievi formulati per tale componente riguardano in gran parte l'assenza di piani di audit o la loro mancata/inadeguata esecuzione.

Permane per i gestori la tendenza ad assumere generalmente sufficiente la presenza di obblighi contrattuali per valutare che una terza parte operi nel rispetto delle procedure definite per l'erogazione del servizio, senza che siano svolti specifici controlli, pianificati tenendo conto anche di criteri di rischio in relazione alla componente di servizio oggetto di affidamento. Per quanto riguarda in particolare il processo delegato alla terza parte che riguarda l'identificazione dei richiedenti ai fini del rilascio di un'identità SpID o di un certificato qualificato di firma digitale, si è rilevato che gli incaricati alla registrazione o gli operatori di Regitration Authority non hanno piena consapevolezza delle responsabilità che derivano dall'esercizio di quel ruolo; in taluni casi non hanno a disposizione procedure formalizzate e liste di controlli da prendere a riferimento al fine di limitare il più possibile l'iniziativa personale ad esempio sulla possibilità di accettare o meno un documento di riconoscimento esibito dal richiedente. Più in generale, la formazione risulta limitata alla normativa e all'uso degli applicativi messi a disposizione dei gestori.

Per la componente di servizio **Analisi dei rischi e VA/PT,** i rilievi ripropongono alcune tematiche già evidenziate in occasione delle verifiche relative al 2020, anche se in linea generale si è rilevato un maggior livello di attenzione alla gestione degli aspetti che riguardano le misure di prevenzione, come appunto la conduzione di attività periodiche di Vulnerability Assessment e Penetration Test.

I gestori eseguono con periodicità più o meno definite questi controlli di sicurezza; talvolta gli esiti di un VA/PT sono sottovalutati, determinando una reazione non sempre adeguata, spesso ac-

[31] Attività per le quali i gestori qualificati o accreditati si avvalgono di organizzazioni esterne sono ad esempio le attività di identificazione e registrazione dei richiedenti un'identità SpID o un certificato di firma digitale, che vengono svolte da operatori ("Registration Authority Operator" o "RAO") incaricati da soggetti terzi che svolgono il ruolo di "Registration Autority". Altre attività per le quali i soggetti vigilati si avvalgono tipicamente di organizzazioni esterne, riguardano la predisposizione e la gestione delle componenti infrastrutturali e applicative utilizzate per l'erogazione del servizi ("partner tecnici").

compagnata da ulteriori aspetti che compromettono un efficace trattamento delle vulnerabilità riscontrate: problemi di natura organizzativa; mancato o incompleto tracciamento delle azioni di risoluzione; non corretta valutazione dei livelli di gravità in funzione del rischio e, in alcuni casi, assenza totale di azioni di trattamento. Talvolta, soprattutto nei casi in cui il gestore è una realtà di piccole dimensioni, l'azione di VA/PT viene limitata al solo ambito di servizio pur se l'infrastruttura tecnologica è utilizzata anche per altri servizi, riducendone così l'efficacia.

La **Gestione del processo,** presenta differenze legate alla differente natura del servizio, anche se per i servizi di firma digitale e di identità digitale SpID alcuni aspetti del processo sono simili. I rilievi hanno interessato (tra i vari temi), le modalità di raccolta documentali dei richiedenti il servizio, la mancanza di verifiche di congruenza tra la documentazione acquisita e i dati inseriti a sistema, il mancato controllo che gli incaricati al riconoscimento venissero scelti tra coloro già formati sugli aggiornamenti relativi alle procedure utilizzate per l'identificazione dei richiedenti.

5 SEGNALAZIONI DI INCIDENTI E MALFUNZIONAMENTI

I soggetti vigilati sono tenuti a segnalare ad AgID e, quando ne ricorrano le circostanze[32] alle altre autorità preposte, gli incidenti di sicurezza o gli eventi che si configurino come malfunzionamenti o interruzioni di servizio.

Nel corso del 2021 sono stati notificati complessivamente **43 incidenti o malfunzionamenti**, che hanno interessato le quattro tipologie di servizi.

La figura che segue mostra il totale degli eventi di cui è stata data notifica nel corso delle settimane dell'anno.

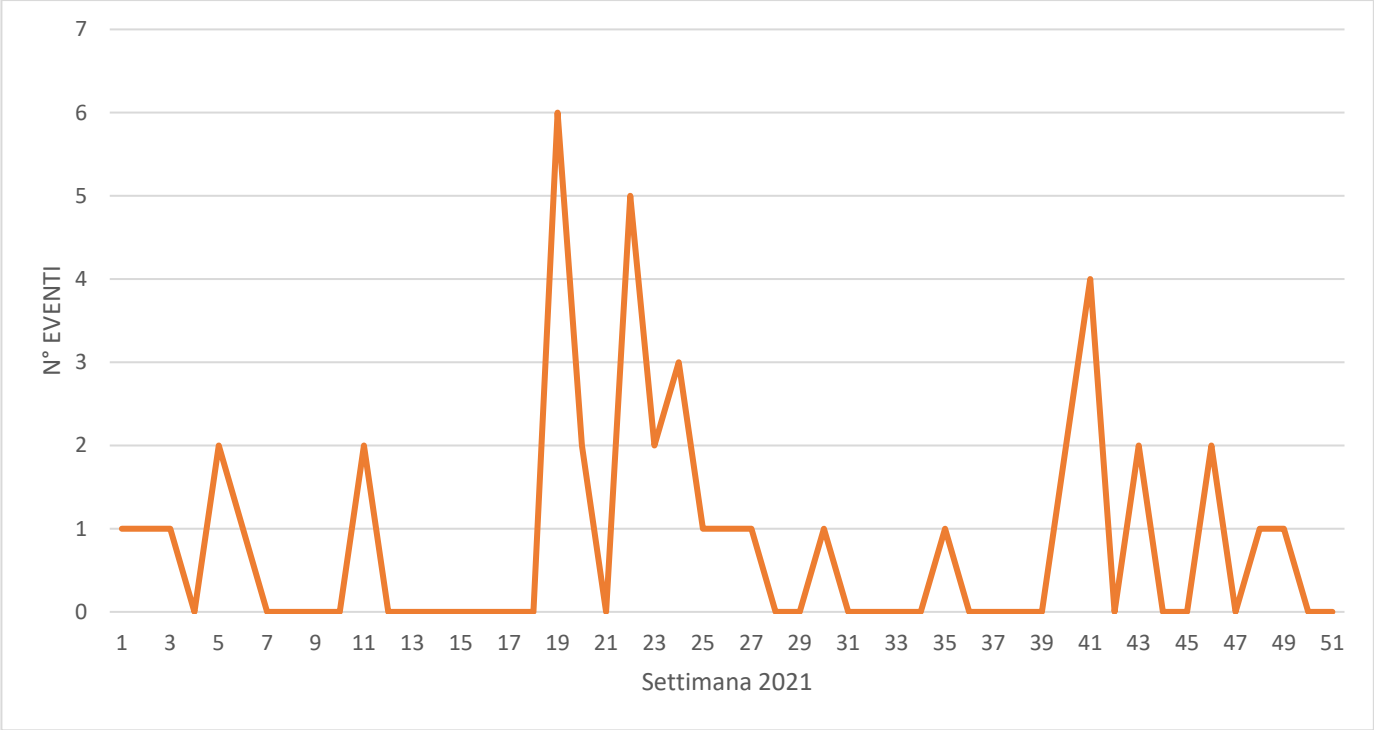

Fig. 5-1 – ***Incidenti e malfunzionamenti segnalati nel corso del 2021***

La tabella che segue riassume i totali per servizio.

	Conservatore	PEC	QTSP	SPID	Totale complessivo
Notifiche per servizio	**1**	**10**	**16**	**16**	**43**

Tab.5.2– Notifiche per servizio

[32] Per esempio nel caso di violazioni di dati personali, i gestori sono tenuti ad effettuare le notifiche al Garante per la protezione dei dati personali.

Nella figura successiva è stata eseguita una valutazione della distribuzione dei tempi di rientro, (vale a dire della durata del disservizio). In particolare dal grafico è possibile rilevare la numerosità degli eventi rientrati rispetto al tempo trascorso dall'inizio del disservizio. Le etichette mostrano l'ora e il totale di eventi risolti in quell'ora[33].

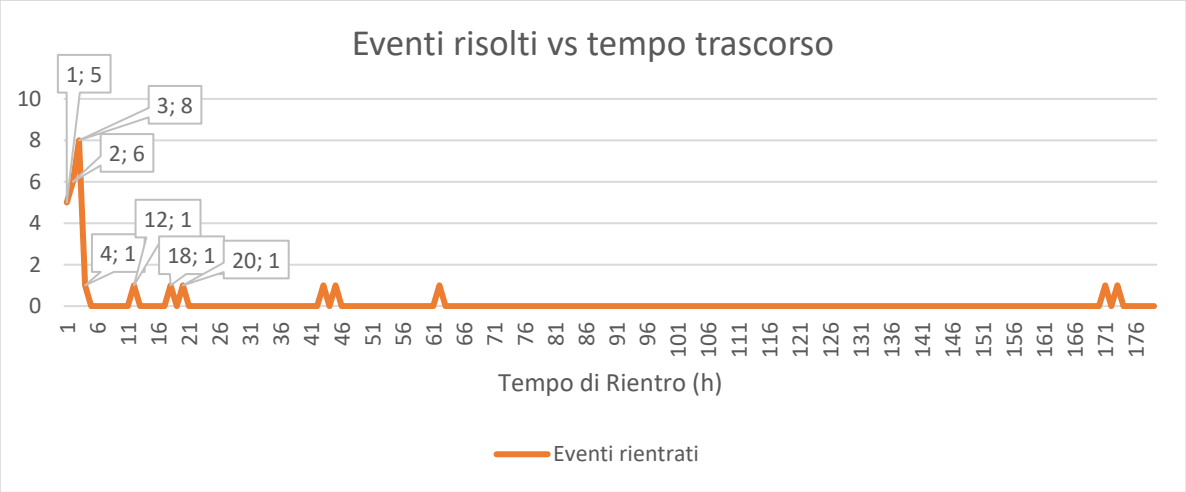

Fig. 5.2 – Distribuzione degli eventi rispetto alla durata del disservizio nel corso del 2021

Da questa ultima considerazione segue il grafico successivo, nel quale è stata eseguita una valutazione del tasso di rientro dei malfunzionamenti.

Nella figura in particolare viene mostrata la percentuale di eventi rientrati rispetto al tempo trascorso dall'inizio dell'evento notificato. SI ricorda che l'evento può essere un disservizio, un malfunzionamento un'attività di manutenzione programmata ovvero anche un incidente di sicurezza.

Nel grafico sono evidenziati alcuni punti di riferimento indicati con le etichette da cui si desume che ad esempio nelle prime 4 ore più dei tre quarti degli eventi riscontrati dai gestori è stato risolto. Inoltre il punto relativo alle 5 ore mostra che quasi l'80% degli eventi è stato risolto in questo tempo.

[33] Ad esempio, per comprendere quanti eventi sono stati risolti nelle prime 4 ore occorre sommare il dato con etichetta da 1 a 4 (intervallo orario), in questo caso 20.

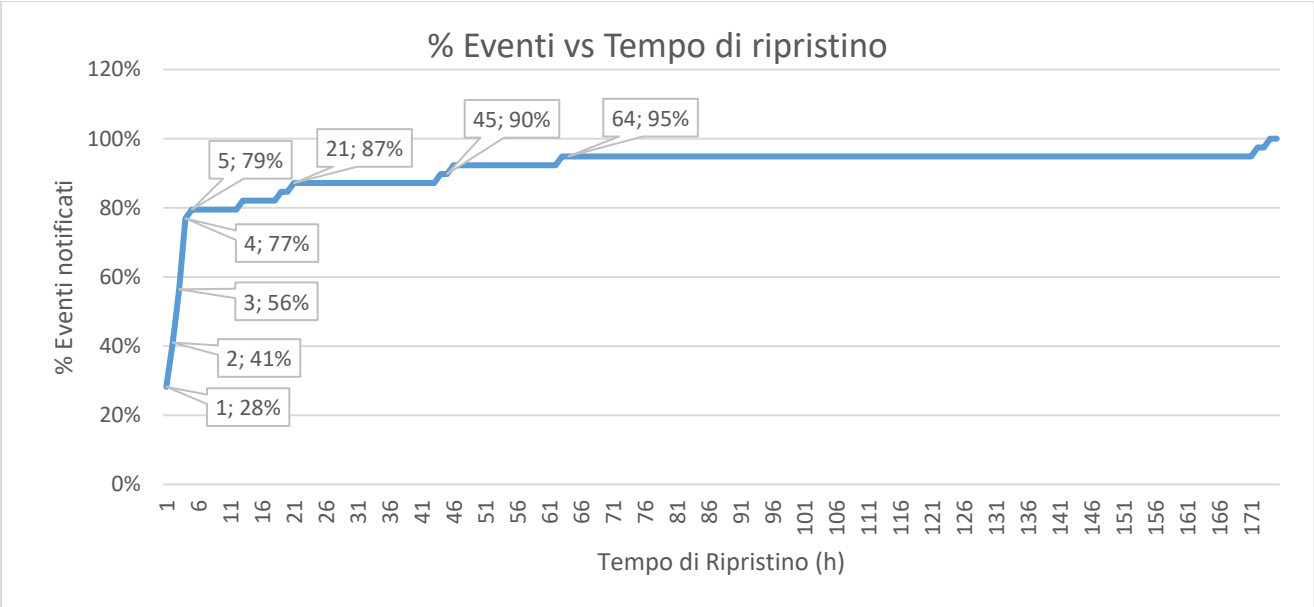

Fig. 5.3 – Tasso di ripristino rispetto alla durata nel corso del 2021

6 SEGNALAZIONI DAGLI UTENTI E RICHIESTE DA ALTRE AUTORITA'

Il Regolamento di vigilanza prevede che gli utenti o i soggetti interessati possono segnalare ad AgID presunte violazioni normative o irregolarità da parte dei gestori.

La nota di segnalazione da utente deve indicare almeno:

a. i recapiti completi del soggetto che effettua la segnalazione;
b. la descrizione della presunta violazione o irregolarità, il gestore coinvolto, i fatti e le circostanze all'origine della segnalazione, il periodo al quale la presunta violazione o irregolarità sarebbe riferita;
c. la documentazione, se disponibile, a sostegno della presunzione di violazione normativa o irregolarità.

Le segnalazioni che non siano archiviate per irricevibilità o per inammissibilità possono comportare l'avvio di un procedimento di verifica.

Nel 2021 sono state gestite **24 segnalazioni utente**, delle quali 6 hanno dato luogo all'avvio di procedimenti di verifica; le rimanenti sono state risolte attraverso interlocuzioni con l'utente o con il gestore. Sono state inoltre gestite circa 30 segnalazioni provenienti da altri enti, tipicamente relative a richieste di dati/informazioni per utilizzo dei servizi (principalmente SpID e firma digitale) a scopo asseritamente fraudolento.

7 LE ATTIVITÀ IN AMBITO EUROPEO

Per quanto riguarda la vigilanza sui prestatori di servizi fiduciari qualificati, AgID, in quanto organismo designato in Italia ai sensi del Regolamento eIDAS, è coinvolta in un insieme di attività che da un lato riguardano la cura di adempimenti previsti dal Regolamento stesso, dall'altro rientrano nelle attività di collaborazione ed assistenza reciproca o sono volte a favorire lo scambio di best practice tra gli organismi di vigilanza dei diversi Stati Membri.

Annualmente, entro il 31 marzo di ogni anno, AgID trasmette alla Commissione una relazione sulle principalti attività di vigilanza svolte sia ai fini della qualificazione di nuovi TSP (prestatori di servizi fiduciari) che sui prestatori già qualificati. È parte integrante della relazione annuale, una sintesi delle notifiche di violazioni su incidenti di sicurezza o perdite di integrità ricevute dai QTSP ai sensi dell'art. 19 del Regolamento eIDAS.

Per dare attuazione a tali obblighi di notifica relativi all'art. 19 del Regolamento eIDAS, è stato costituito un tavolo di lavoro, art. 19 Expert Group, coordinato da ENISA[34], Agenzia dell'Unione Europea per la Cybersecurity che si occupa di coordinare le modalità per le rendicontazioni di tali eventi tra i diversi organismi di vigilanza degli Stati Membri, per adottare pratiche comuni di classificazione e gestione. ENISA annualmente pubblica un report[35] che riepiloga, in forma anonima e con dati aggregati, gli incidenti notificati dai diversi Stati membri, al fine di creare una conoscenza comune dei punti deboli riscontrati e delle vulnerabilità più ricorrenti.

Il quadro per la segnalazione degli incidenti ai sensi dell'articolo 19 è stato preparato da ENISA in consultazione con i membri del gruppo di esperti e rivisto anche dal settore privato e dal Forum delle autorità europee di vigilanza per le firme elettroniche (FESA) L'ENISA ha sviluppato uno strumento in linea (CIRAS-T), ad uso degli organismi di vigilanza degli Stati Membri, per facilitare la procedura di notifica degli incidenti con impatto transfrontaliero.

L'art. 19 Expert Group si riunisce periodicamente, in genere con frequenza semestrale, agendo tramite scambi di email e documentazione, anche al fine di trovare soluzioni tecniche o metodologiche per affrontare temi di comune interesse quali integrazione con nuove tecnologie, response a nuovi business case o esigenze di mercato anche locali, strumenti di validazione di soluzioni e verifica della conformità delle stesse. L'esito di questi incontri è, ove non secretato per ragioni di sicurezza e riservatezza, disponibile sul portale europeo in numerose sezioni interne. Nel corso del 2021, a causa delle restrizioni dovute all'emergenza Covid, i due incontri si sono svolti da remoto, in modalità videoconferenza.

[34] L'ENISA, Agenzia dell'Unione europea per la cibersicurezza, è un centro di competenze in materia di sicurezza informatica in Europa. Aiuta l'UE e i paesi membri dell'UE a essere meglio attrezzati e preparati a prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione. Rif. https://www.enisa.europa.eu/about-enisa.

[35] Il 27 luglio 2022 è stato pubblicato da ENISA il reposrt Trust Services Security Incidents 2021, in cui sono presentati in forma aggregata i dati relativi agli eventi notificati nel 2021 dagli Stati Membri ai sensi dell'art. 19 del Regolamento eIDAS.

Sempre in ambito QTSP, il team AgID è parte attiva del citato Forum of European Supervisory Authorities for trust service providers (FESA), con lo scopo di coordinarsi nelle attività di vigilanza, nelle metodologie e nell'assistenza reciproca con gli organismi di vigilanza degli altri Stati Membri.

8 LE SANZIONI

Il CAD[36] definisce i casi per i quali possono essere irrogate sanzioni amministrative.

Nel 2021 **per 3 procedimenti,** avviati a seguito di segnalazioni, **è stata attivata la fase sanzionatoria,** dei quali due (riuniti) in ambito SpID e l'altro in ambito QTSP. A dicembre 2021 le attività istruttorie risultavano ancora in corso.

Le irregolarità riscontrate hanno riguardato in linea di massima:

- l'adozione di sistemi e pratiche operative e gestionali non sempre in grado di contrastare richieste di identità digitale o certificati di firma per utilizzi impropri del servizio;
- le modalità definite per l'identificazione dei richiedenti un'identità digitale o un certificato di firma attraverso terze parti e la mancanza di adeguati controlli da parte del gestore, in grado di rilevare e contrastare tempestivamente anomalie o comportamenti difformi dalle procedure previste.

Nel corso del 2021 **si è concluso 1 procedimento avviato a fine 2020,** a seguito della positiva verifica che le irregolarità accertate fossero state correttamente indirizzate e dell'avvenuto pagaento in oblazione di circa 160.000,00 euro.

Tali risorse saranno destinate a rafforzare le iniziative già intraprese, rivolte ai soggetti vigilati, volte a migliorare la capacità di prevenzione degli stessi gestori.

[36] Art. 32-bis

9 AZIONI SCATURITE DALLE VERIFICHE E PROSSIME ATTIVITÀ

I procedimenti di verifica comportano l'adozione da parte dei gestori di azioni correttive o di miglioramento.

Quando nel corso di un procedimento sono rilevate criticità che possono riguardare più soggetti vigilati, sono richiesti specifici controlli o avviate iniziative che coinvolgono tutti i gestori.

Per quanto riguarda i prestatori di servizi fiduciari qualificati e gli IdP SpID, principalmente interessati dai procedimenti avviati nel 2021, sono stati richiesti interventi volti a migliorare i controlli e a centralizzare i sistemi per la registrazione dei dati dei titolari, al fine di rilevare tempestivamente anomalie nei processi di identificazione e registrazione dei dati dei richiedenti un'identità SpID o una firma digitale svolti attraverso terze parti (Registration Authority ("RA")[37] e Registration Authority Operator ("RAO")[38].

Come già avvenuto nel corso del 2020, le iniziative sono volte a contrastare **fenomeni sempre più frequenti di furti di identità,** o di utilizzo dei servizi di firma e SpID a scopo fraudolento, che anche nel 2021 si sono rivelati numerosi. I furti di identità sono perpetrati per operazioni specifiche (es. accesso ai bonus di iniziativa governativa[39]; accensione di conti correnti on-line; richieste di finanziamenti o di prestiti; accessi abusivi a prestazioni di tipo pensionistico).

Un'identità SPID e una firma digitale basata su un certificato qualificato sono entrambi strumenti di identificazione ed hanno uguale rilevanza negli scenari di utilizzo sopra richiamati: una firma digitale può essere ottenuta anche utilizzando lo SpID come sistema di riconoscimento e, viceversa, è possibile ottenere un'identità digitale disponendo di una firma digitale. È necessario che l'utente sia sensibilizzato nell'utilizzo consapevole e responsabile di tali sistemi, adottando comportamenti[40] che ostacolino utilizzi impropri di tali servizi. Per quel che riguarda i gestori, è necessaria un'accurata gestione delle anagrafiche dei titolari[41] e degli operatori addetti al riconoscimento dei richiedenti, con l'abilitazione di controlli incrociati sui sistemi di registrazione in uso, nel caso in cui il gestore sia prestatore di più servizi. Parallelamente, è necessario che le terze parti e gli incaricati al riconoscimento che operano per conto dei gestori acquisiscano sempre maggiore consapevolezza sulle responsabilità civili e penali nelle quali incorrono in caso di violazione degli obblighi previsti

[37] Registration Authority: soggetti cui un gestore, nel suo ruolo di Certification Authority o di Identity Provider accreditato, conferisce specifico mandato con rappresentanza con il quale affida lo svolgimento di una o più attività proprie del processo di registrazione, come ad esempio: l'identificazione del richiedente; la registrazione dei dati; l'inoltro dei dati ai sistemi del gestore; la raccolta della richiesta del certificato qualificato o dell'identità digitale

[38] Operatore di Registrazione. Persona fisica che, per conto del gestore (IdP SpID o QTSP), svolge le attività di identificazione/registrazione dei richiedenti un'identità SpID o una firma digitale, nell'ambito di un mandato conferito dal gestore e dalla RA. Il RAO è tenuto ad operare secondo le procedure operative definite dal gestore e può essere abilitato solo dopo aver ricevuto adeguata formazione sulle procedure da seguire, sugli obblighi e sulle responsabilità civili e penali in cui incorre in caso di violazione delle procedure previste.

[39] Ad esempio.: bonus vacanze; bonus 18app, carta del docente.

[40] Ad esempio assicurare la custodia del dispositivo di firma; non rivelare a terzi le credenziali di acceso; utilizzare personalmente i sistemi di cui è titolare;

[41] Ad esempio assicurando, in fase di registrazione, che i dati di contatto (e-mail; cellulare) siano riferibili ad un unico titolare o che non siano presenti similitudini tra dati riferiti a diversi titolari.

per il rilascio dell'identità digitale e dei certificati qualificati di firma digitale, risultando in particolare necessaria l'adozione di ogni misura idonea per l'identificazione certa del richiedente.

I risultati delle attività di vigilanza e le esperienze maturate sul campo sono messe a disposizione delle unità organizzative di AgID preposte alla revisione delle regole ed all'emanazione delle Linee Guida previste dal CAD. Gli impegni futuri sono certamente orientati a consolidare e migliorare sempre più gli strumenti disponibili ad AgID per costruire conoscenza e pianificare le verifiche a partire dai dati. In tale ottica, nel 2021 sono proseguite le attività per il consolidamento del sistema informatico di supporto all'espletamento delle funzioni di vigilanza (piattaforma https://trustservices.agid.gov.it/) e sono state rilasciate le prime funzioni per la raccolta e la gestione dei dati strutturati da parte dei soggetti vigilati. A tal fine sono state attivate le utenze dei gestori per l'accesso alla piattaforma ed è stata avviata l'acquisizione delle notifiche di incidenti/malfunzionamenti con tali nuove modalità, prendendo a riferimento, per le indicazioni ai gestori e per la revisione delle procedure in uso, le indicazioni ENISA per la gestione degli eventi impattanti la regolarità dei servizi in riferimento ai regimi di identificazione elettronica e ai servizi fiduciari qualificati.

Per gli ulteriori dati relativi ai servizi erogati, sono state pubblicate le *Linee guida per l'invio dei dati periodici relativi ai servizi fiduciari e ai servizi PEC* (marzo 2021)[42] e sono stati completati i documenti tecnici[43] per la raccolta dei dati SpID attraverso interfacce applicative. Dopo una fase di adeguamento e di avviamento da parte dei gestori, è prevista l'attivazione a regime delle nuove modalità nel secondo semestre 2022.

[42] Determinazione n. 259/2021

[43] Documenti tecnici pubblicati sul sito AgID (https://www.agid.gov.it/it/agenzia/vigilanza): Documenti che definiscono le modalità per la raccolta dei dati attraverso piattaforma informatica (Documento Tecnico Acquisizione Dati e allegati; Specifiche dei formati e dei tracciati dei dati relativi ai servizi SpID).

10 APPENDICE

12.1 Glossario

AgID - Agenzia per l'Italia Digitale

CAD - Codice dell'Amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82 s.m.i.)

IdP – Identity Provider. Gestore dell'identità digitale SPID

NC - Non Conformità. Irregolarità classificata secondo tre livelli di gravità crescente (Lieve, Media, Grave), che richiede azioni correttive entro tempi massimi stabiliti

QTS - Qualified Trust Services - Servizi fiduciari qualificati - servizi elettronici, normalmente forniti a pagamento, che soddisfano un insieme di requisiti validi su tutto il territorio dell'Unione europea (requisiti stabiliti dal Regolamento eIDAS) fornendo agli utenti mutue garanzie di sicurezza e qualità. I più diffusi servizi fiduciari qualificati in Italia sono i servizi di firma digitale.

QTSP - Qualified Trust Service Provider - Prestatore di servizi fiduciari qualificati - Soggetti qualificati per l'erogazione di uno o più servizi fiduciari qualificati (QTS) e sui quali AgID esercita le funzioni di vigilanza

SPID - Sistema Pubblico di Identità Digitale

12.1 Riferimenti normativi

Decreto Legislativo 7 marzo 2005, n.82 s.m.i — Codice dell'Amministrazione Digitale ("CAD")

Regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 ("eIDAS"), in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

Regolamento recante le modalità per la vigilanza e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 7 marzo 2005, n. 82 e successive modificazioni