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 2023

AGID | Agenzia per l'Italia Digitale

Indice

1 PREFAZIONE

La presente relazione illustra le attività di vigilanza svolte nel 2023 dall'Agenzia per l'Italia Digitale ("AgID") ai sensi dell'art. 14-*bis*, comma 2, lettera i) del Codice dell'Amministrazione Digitale (CAD)[1].

Le funzioni di vigilanza si riferiscono ai principali fornitori di servizi quali la firma elettronica, l'identità digitale e la posta elettronica certificata, essenziali per garantire transazioni digitali sicure tra pubbliche amministrazioni, imprese e cittadini, e favorire lo sviluppo dell'economia digitale. **Obiettivo della vigilanza** è verificare che i soggetti vigilati operino nel rispetto di regole comuni tra gli Stati Membri dell'Unione Europea[2], prevenendo irregolarità, accertando eventuali violazioni e promuovendo il miglioramento continuo dei servizi, al fine di rafforzare la fiducia dei cittadini nelle transazioni *online*.

I poteri di vigilanza si basano su un **quadro regolatorio** che comprende norme comunitarie e nazionali, coinvolgendo una rete di *stakeholder* – utenti[3], istituzioni e operatori – ognuno con profili di interesse e aspettative diverse per le specifiche componenti dei servizi, che influenzano il loro sviluppo e la loro evoluzione. Con la presente relazione, giunta alla settima edizione**,** l'Agenzia rende conto annualmente delle attività svolte e dei temi più rilevanti trattati nell'anno trascorso.

Nel 2023 le funzioni di vigilanza hanno riguardato 20 prestatori di servizi fiduciari qualificati, per oltre 32 milioni di certificati qualificati di firma, 19 gestori di posta elettronica certificata accreditati, per circa 16 milioni di caselle PEC e 13 gestori di identità digitale, per 37 milioni di identità digitali SPID[4]. Tali soggetti **comprendono i principali operatori economici** che offrono servizi e soluzioni sul mercato nazionale ed internazionale.

Sono destinatari delle funzioni di vigilanza ai sensi dell'art. 14-*bis* del CAD gli ulteriori soggetti pubblici e privati che partecipano a SPID, tra i quali i fornitori dei servizi ("Service Provider" o "SP") e i soggetti di cui all'art. 34, comma 1-*bis* del CAD, che erogano servizi di conservazione ("Conservatori"). Dal 1° gennaio 2022, data in cui è stata avviata l'iscrizione al *Marketplace dei servizi di conservazione*[5], risultano iscritti 68 Conservatori (dato riferito al 31/12/2023).

---

[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 17 del 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 e nel 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).

[4] I dati relativi ai volumi gestiti per SPID, firme digitali e PEC si riferiscono al 31 dicembre 2023.

[5] https://conservatoriqualificati.agid.gov.it/

Nel 2023 sono stati avviati **20 procedimenti di verifica** ed eseguite **17 ispezioni**, svolte con l'apporto delle competenze specialistiche dell'*Area Vigilanza e Monitoraggio* dell'Agenzia, del personale del *Cert-AgID* e del *Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza*.

Sono, inoltre, proseguite le attività per l'attuazione del nuovo quadro normativo di riferimento per l'evoluzione della PEC verso il nuovo servizio di recapito certificato qualificato conforme al Regolamento eIDAS[6]. Pertanto, i procedimenti di verifica hanno riguardato prevalentemente i gestori di identità digitale SPID e i prestatori di servizi fiduciari qualificati che erogano servizi di firma digitale. Sono stati, inoltre, avviati anche i **primi procedimenti nei confronti di 2 *Service Provider* SPID,** che sono stati selezionati sulla base di un questionario somministrato nel corso dell'anno precedente, volto a rilevare il livello di conformità agli obblighi previsti per i fornitori di servizi in ambito SPID.

Quanto alle attività di raccolta e gestione dei dati strutturati trasmessi dai soggetti vigilati tramite il sistema informatico[7], nel 2023 sono stati notificati dai gestori oltre **120 eventi** relativi a incidenti, malfunzionamenti o notifiche di interventi di manutenzione programmata. Sono state, altresì, oggetto di trattazione **137 segnalazioni** (relative a **oltre 500 utenze**), di cui **96 richieste** relative all'acquisizione di informazioni nell'ambito di indagini di polizia giudiziaria per utilizzo dei servizi a scopo asseritamente fraudolento (principalmente SPID e firma digitale), e **41 segnalazioni da parte di utenti** (c.d. segnalazioni utente).

Le attività di verifica hanno stimolato i gestori a implementare significative misure per migliorare la sicurezza e contrastare i tentativi di frode ai danni degli utenti. **Di particolare importanza è stata, in tale contesto, la costante e sinergica collaborazione con il CERT-AgID**, che ha svolto un ruolo fondamentale nel limitare la diffusione di contenuti dannosi e garantire una maggiore sicurezza per gli utenti finali.

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

[6] L'art. 8 del decreto legge n. 135 del 14 dicembre 2018 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 certificata (PEC), di cui agli articoli 29 e 48 del decreto legislativo n. 82 del 7 marzo 2005, al regolamento (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] Piattaforma TrustServices.

2 LE FUNZIONI DI VIGILANZA SVOLTE DA AGID

2.1 RICHIAMI RELATIVI AL QUADRO NORMATIVO

Le funzioni di vigilanza dell'Agenzia per l'Italia Digitale (d'ora innanzi Agenzia o AgID) trovano fondamento – come già evidenziato – in normative nazionali e comunitarie, tra queste il Codice dell'Amministrazione Digitale (CAD)[8]. L'Agenzia esercita vigilanza su prestatori di servizi fiduciari qualificati, gestori di posta elettronica certificata e conservatori di documenti informatici, oltre a soggetti coinvolti nel sistema SPID. In caso di violazioni, AgID può irrogare sanzioni amministrative in base alla gravità della violazione e al danno causato, ai sensi dell'art. 32-*bis* del CAD.

Al regime di identificazione elettronica SPID e ai servizi fiduciari qualificati si applica la disciplina del Regolamento UE 910/2014 (Regolamento eIDAS[9]). Con particolare riferimento ai servizi fiduciari qualificati, AgID è l'organismo di vigilanza designato in Italia[10]. L'art. 29 del CAD estende, inoltre, i requisiti del Regolamento eIDAS anche ai gestori PEC.

Infine, la Direttiva (UE) 2022/2555 ("Direttiva NIS 2"), entrata in vigore il 17 gennaio 2023, include i servizi fiduciari nel suo campo di applicazione e prevede modifiche ai requisiti di sicurezza e agli obblighi di notifica delle violazioni di sicurezza previsti dal Regolamento eIDAS a partire dal 18 ottobre 2024[11].

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 descritte nel "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" (d'ora innanzi Regolamento)[12].

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

---

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

[9] Il 20 maggio 2024 è entrato il vigore il Regolamento (UE) 2024/1183 del Parlamento Europeo e del Consiglio ("eIDAS 2"), che ha apportato sostanziali modifiche al Regolamento (UE) 910/2014.

[10] Il ruolo ed i compiti di un organismo di vigilanza sono indicati nell'art. 17 del Regolamento (UE) n.910/2014. Sono previste inoltre attività di collaborazione e assistenza reciproca tra gli organismi di vigilanza dei diversi Stati Membri.

[11] La Direttiva (UE) 2022/2555, recepita con il Decreto Legislativo 4 settembre 2024, n. 138, richiede un coordinamento con la disciplina eIDAS 2 per le previsioni relative ai requisiti di sicurezza dei prestatori di servizi fiduciari.

[12] 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. A gennaio 2022 (Determinazione n. 1/2022 del 12/01/2022) è stata adottata una nuova versione per recepire le modifiche introdotte dall'art. 27, comma 1, lettera d) del decreto legge n. 152/2021, successivamente modificata con Determinazione N. 270/2022 del 18/10/2022.

Le verifiche possono essere condotte su base documentale o prevedere l'esecuzione di ispezioni, *on site* o da remoto; la modalità *on site* è stata quella più frequentemente utilizzata nel 2023.

Diversamente dagli *audit* di "terza parte" svolti dagli organismi di certificazione accreditati dall'ente nazionale di accreditamento, finalizzati a certificare la conformità di un sistema di gestione a una norma o a uno standard internazionale, le verifiche svolte da AgID ai fini della vigilanza si configurano come *audit* di "seconda parte", secondo la definizione contenuta nella norma tecnica di riferimento ISO 19011. Tali *audit* sono in genere diversi l'uno dall'altro e limitati ad aspetti specifici ("componenti del servizio"), in relazione agli obiettivi di ciascuna verifica.

Un procedimento di verifica può essere avviato a seguito di una segnalazione o nell'ambito di un programma di *audit* predisposto periodicamente, secondo di indici di rischio valorizzati sulla base delle dimensioni e tipologia di servizi e utenti, delle soluzioni tecnologiche adottate, delle segnalazioni pervenute, dei partner che gestiscono specifiche componenti del servizio, delle verifiche precedenti e, non da ultimo, da analisi di tipo predittivo. Nel 2023, in considerazione delle attività *in itinere* per i servizi PEC e di conservazione ai fini dell'attuazione del nuovo quadro normativo, la programmazione periodica ha dato priorità alle verifiche sui servizi erogati dai prestatori di servizi fiduciari qualificati e dai gestori SPID con un'utenza più ampia, vista anche l'accresciuta rilevanza di tali servizi, accompagnata da un aumento delle segnalazioni.

La fase di verifica dei procedimenti di vigilanza si conclude in un tempo massimo di centottanta giorni, fatti salvi gli eventuali termini di sospensione previsti dal Regolamento, e può portare alla formulazione di rilievi, distinti rispettivamente in 'Non Conformità' e 'Osservazioni'[13]. Tutti i rilievi e le conseguenti azioni definite dai gestori sono oggetto di monitoraggio continuativo, sia nell'ambito di successive verifiche che a procedimento concluso, fino alla completa attuazione.

2.3 LE PARTI INTERESSATE (*STAKEHOLDER*)

Le funzioni di vigilanza vedono coinvolti, a diverso titolo, le seguenti entità:

- **enti nazionali,** con riferimento sia a quelli preposti alla definizione degli obiettivi e degli indirizzi strategici che l'Agenzia deve mettere in atto[14], sia a quelli direttamente coinvolti nei processi

[13] La 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. L'Osservazione è una raccomandazione o spunto per il miglioramento, con l'obiettivo di stimolare i gestori a riesaminare i processi e ad adottare in via continuativa azioni volte a adeguare l'offerta di servizi alle potenzialità offerte dalle evoluzioni tecnologiche *in itinere*, a migliorare la qualità erogata, nonché a prevenire situazioni di degrado.

[14] Si fa riferimento all'autorità governativa che esercita i poteri di indirizzo e vigilanza sull'Agenzia, attualmente attribuiti al Sottosegretario di Stato con delega all'innovazione.

primari della vigilanza[15];

- **soggetti vigilati**: soggetti ai quali si applicano le funzioni di vigilanza (vds. Cap. 3);
- **utenti**: persone fisiche o giuridiche (imprese e pubbliche amministrazioni) che usufruiscono dei servizi erogati dai soggetti vigilati;
- **Istituzioni internazionali**: enti regolatori o di standardizzazione e 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 e alla quale fanno riferimento i procedimenti di notifica;
    - 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;
    - FESA (*Forum of European Supervisory Authorities for trust service providers*), gruppo di lavoro con rappresentanti degli Organismi di vigilanza europei, avente lo scopo di supportare e migliorare la cooperazione e l'assistenza reciproca;
    - ECATS (*European Competent Authorities for Trust Services*) gruppo di lavoro con rappresentanti degli Organismi di vigilanza europei, con il compito di favorire l'attuazione dell'art. 19 del Regolamento eIDAS;
    - Organismi di vigilanza degli altri Stati Membri, con i quali sono previsti rapporti di collaborazione e assistenza reciproca, oltre a essere i destinatari delle notifiche di incidenti di sicurezza e perdita di integrità dei dati ricevute dai prestatori di servizi fiduciari qualificati-QTSP[16] nazionali che abbiano impatto su altri Stati Membri.

[15] Tra le altre, il Garante per la protezione dei dati personali, che può prendere parte alle attività ispettive presso i gestori SPID, o anche 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.

[16] *Qualified Trust Service Provider.*

3 TASSONOMIA DEI SOGGETTI VIGILATI

Le funzioni di vigilanza ai sensi dell'art 14-*bis* del CAD sono state esercitate, alla data del 31/12/2023, nei confronti di: **20 prestatori di servizi fiduciari qualificati** (di cui 1 risulta cessato nel 2023); **19 gestori di posta elettronica certificata accreditati** (di cui 2 risultano cessati nel 2023); **13 gestori di identità digitale SPID** (di cui 1 risulta cessato nel 2023); **68 conservatori** (ovvero i soggetti di cui all'art. 34, comma 1-*bis* del CAD, che erogano servizi di conservazione); ulteriori soggetti pubblici e privati che partecipano a SPID, tra i quali i **fornitori dei servizi** ("Service Provider" o "SP"). Tutti i soggetti menzionati sono qualificati o accreditati da AgID e iscritti in elenchi pubblici[17].

Ai fini della programmazione periodica delle verifiche, si valorizzano i menzionati indici di rischio (vds. Cap. 2.2) che richiedono la collezione di dati strutturati relativi ai servizi vigilati, il cui formato è definito da specifici tracciati[18]. Per la raccolta dei dati si utilizza un'apposita piattaforma, che consente ai soggetti vigilati l'interazione applicativa tramite API ("Application Programming Interface"). I dati raccolti vengono utilizzati per analisi statistiche e per la gestione degli indici di rischio. A tal fine sono rilevanti le dimensioni e tipologia di servizi erogati. Nei paragrafi che seguono si presentano le principali caratteristiche, in forma anonima ed in modalità aggregate, evidenziando le modifiche rispetto alla situazione relativa al 2022.

Per i Service Provider si rimanda al Cap. 5.

3.1 PRESTATORI DI SERVIZI FIDUCIARI QUALIFICATI (QTSP)

Nel 2023 è stato qualificato un nuovo prestatore di servizi fiduciari, mentre un prestatore è cessato. Al 31/12/2023 risultano pertanto iscritti nell'elenco dei prestatori di servizi fiduciari qualificati attivi in Italia, 20 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 evidenziato dalla *Trusted list* italiana[19], tutti i QTSP sono qualificati per i servizi di firma, ad eccezione di 1 soggetto che è qualificato solo per il servizio

[17] Si tratta di soggetti qualificati o accreditati da AgID e iscritti sei seguenti elenchi pubblici: 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 Identity Provider accreditati (https://www.agid.gov.it/it/piattaforme/SpID/identity-provider-accreditati); elenco dei Conservatori iscritti al Marketplace (https://conservatoriqualificati.agid.gov.it/?page_id=276); lista dei Fornitori di Servizi aderenti a SPID (https://www.spid.gov.it/open-data-spid/).

[18] Come previsto dalla Determinazione Direttoriale n.259/2021, di emanazione delle "*Linee Guida per la normalizzazione dei dati statistici dei servizi erogati dai Gestori PEC, dai Conservatori e dai Prestatori di servizi fiduciari qualificati*", unitamente al documento tecnico integrativo "*Tracciato record dei dati statistici dei servizi erogati dai Gestori PEC, Conservatori e dai Prestatori di servizi fiduciari qualificati*" e ai documenti relativi ai tracciati per l'invio dei dati SPID.

[19] Si consulti EU Trust Services Dashboard

di validazione temporale; 3 QTSP sono qualificati per le quattro tipologie di servizi; 13 QTSP rilasciano Marche Temporali qualificate (eIDAS) e, di questi, 2 QTSP ne rilasciano circa il 70%; 16 QTSP emettono certificati qualificati per firma remota e, di questi, 4 QTSP ha staccato il 60% delle firme elettroniche qualificate remote nel 2023;

- **caratteristiche dell'utenza**: 7 QTSP non operano sul mercato, bensì 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);
- **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.

Nei grafici che seguono si riporta un estratto dell'andamento dei volumi dei servizi di firma e marca temporale al 31/12/2023, che costituiscono l'offerta di servizi più consistente per questa tipologia di soggetti vigilati.

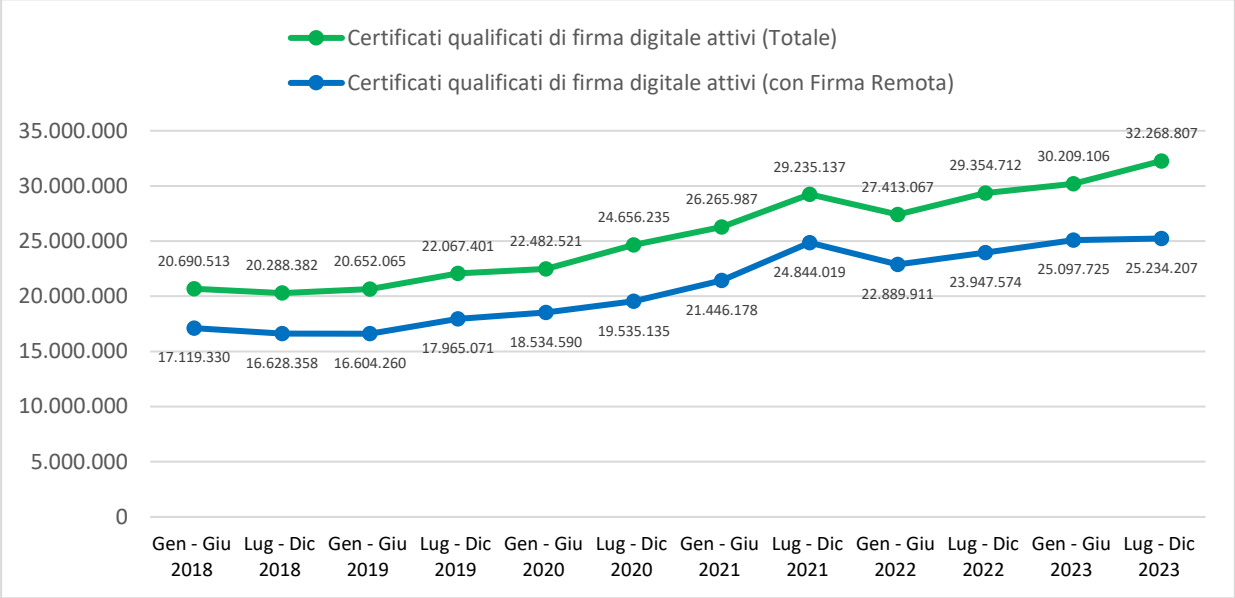

Fig. 1 - Certificati di firma digitale attivi (dati aggregati per semestre)

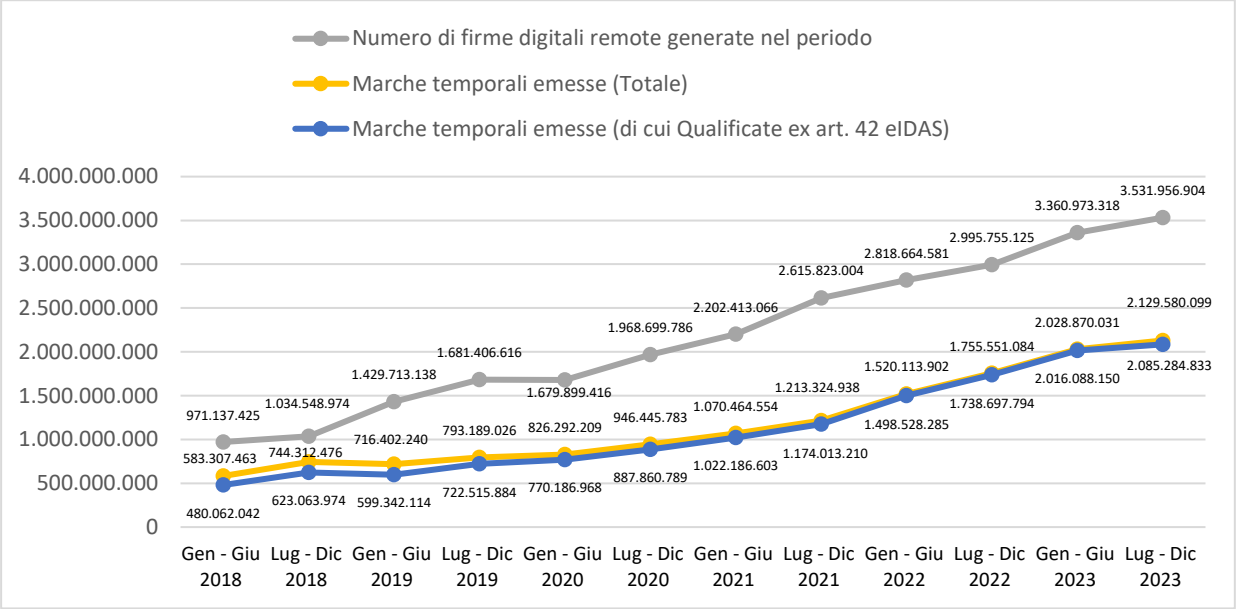

Fig. 2 - Firme digitali remote generate e marche temporali emesse (dati aggregati per semestre)

3.2 GESTORI PEC

Al 31/12/2023 risultano iscritti nell'elenco dei gestori PEC accreditati 18 soggetti (dei 19 originari, 2 hanno cessato l'attività, ma al contempo ne è stato accreditato 1 nuovo nel corso dell'anno).

Di seguito, i dati caratterizzanti dei soggetti iscritti nell'elenco dei gestori PEC:

- **volumi gestiti**: 1 solo gestore copre circa l'80% dei domini e il 60% delle caselle; 2 gestori insieme coprono il 75% circa delle caselle totali;
- **caratteristiche dell'utenza**: a parte alcuni gestori – segnatamente soggetti pubblici –, che gestiscono domini e caselle di una clientela predefinita e limitata ad una rete specifica di utenze per una percentuale inferiore all'1%, gli altri soggetti, 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. Diversi gestori distribuiscono il servizio attraverso una rete di partner commerciali ramificata sul territorio.

Per quanto riguarda i volumi di domini, caselle PEC e messaggi, dai grafici che seguono si rileva un totale annuo di quasi 2,5 miliardi di messaggi complessivamente scambiati, circa 262.000 domini registrati, 16 milioni di caselle attive e con picchi di oltre 840 milioni di messaggi scambiati a bimestre.

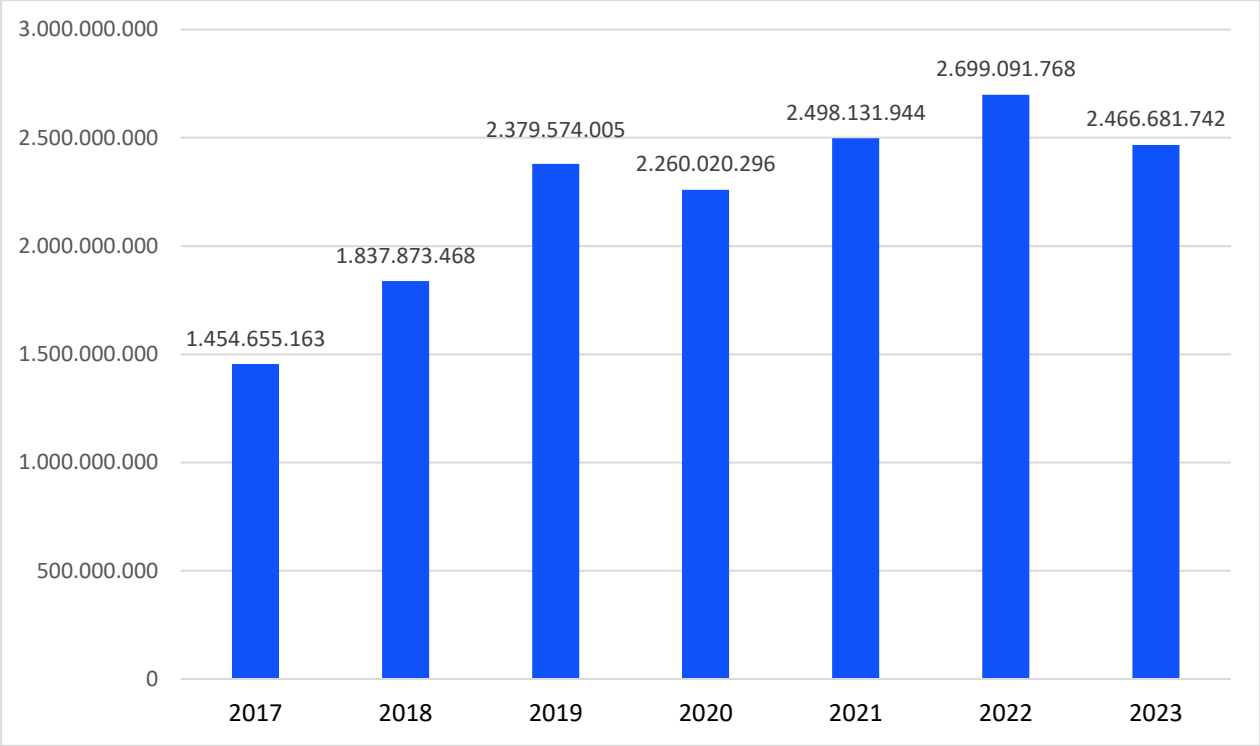

Fig. 3 - Messaggi PEC scambiati dal 2017 al 2023

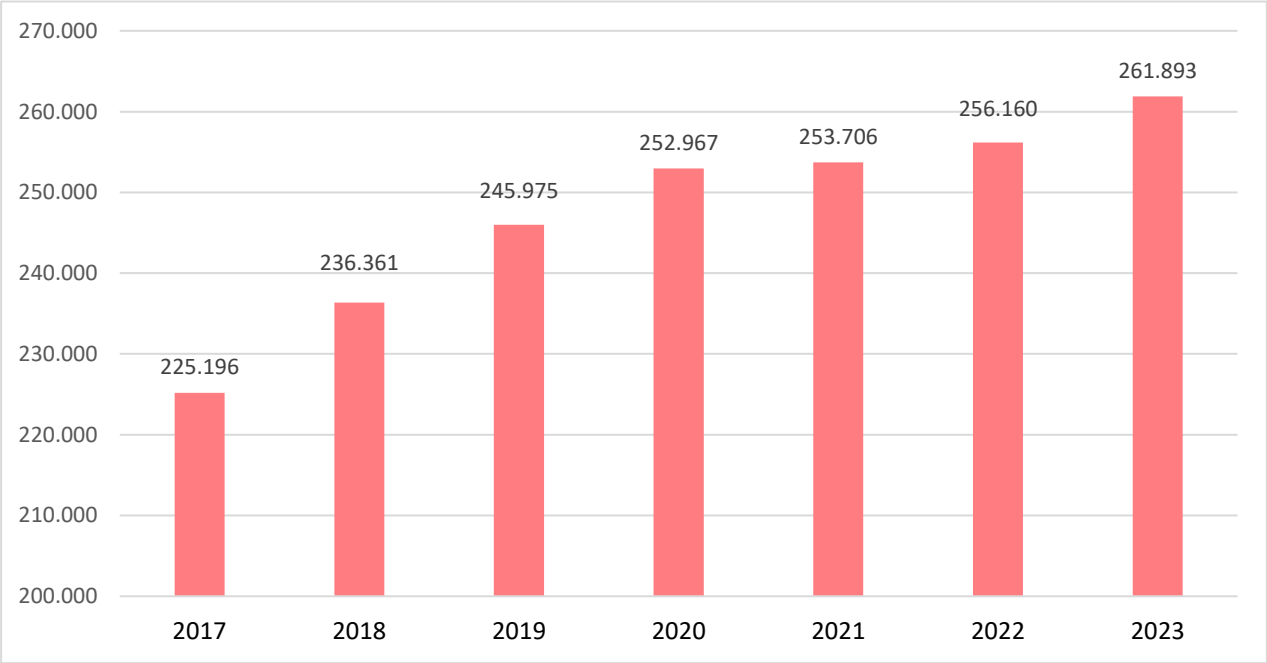

Fig. 4 - Domini PEC attivi dal 2017 al 2023

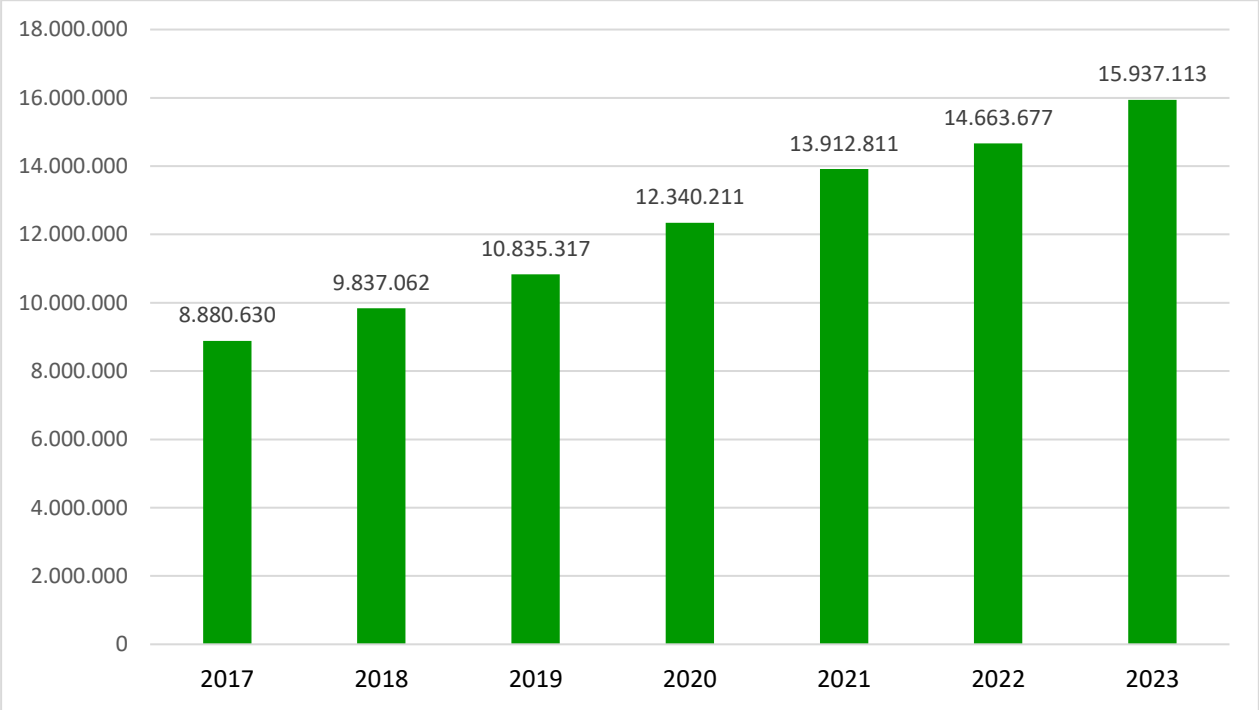

Fig. 5 - Caselle PEC attive dal 2017 al 2023

3.3 IDENTITY PROVIDER SPID (IDP)

Al 31/12/2023 risultano attivi 12 Identity Provider (1 gestore è cessato) e sono state emesse oltre 3 milioni di identità digitali, per un totale di quasi 37 milioni di identità digitali dal 2017 (circa 5,5 milioni ad inizio 2020).

Come si rileva nel grafico che segue, **il totale delle identità a fine 2023** è ben oltre il doppio del valore registrato a fine 2020.

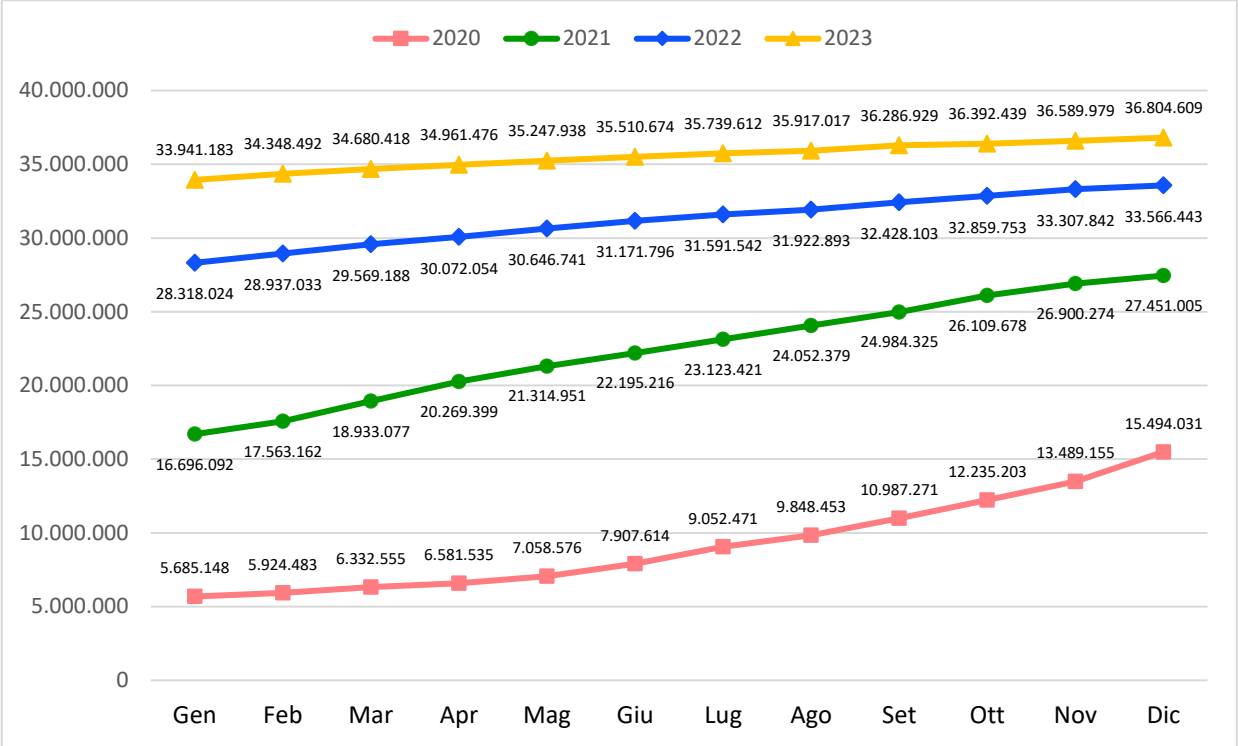

Fig. 6 - Identità gestite nel periodo 2020 – 2023

Complessivamente, a fine 2023 si è registrato un aumento di circa il 10% dei volumi di identità gestite rispetto al 2022.

Le amministrazioni pubbliche che forniscono servizi tramite SPID sono circa 16.000 (circa 3.500 ad inizio 2020), e tra queste hanno aderito a SPID oltre il 95% dei comuni italiani. Il numero complessivo di autenticazioni ai servizi on-line tramite SPID è stato di 1.073.422.405, in lieve aumento rispetto al 2022.

Dalle relazioni annuali di riepilogo fornite dai gestori[20], si rileva che i servizi cui si è registrato l'accesso attraverso SPID hanno riguardato: INPS (http://www.inps.it); Agenzia delle Entrate (https://spid.agenziaentrate.gov.it); istituzioni scolastiche (https://spid.pubblica.istruzione.it); pagamenti (https://pagopa.gov.it); App IO (https://app-backend.io.italia.it/); servizi comunali (pagamenti tasse/tributi); servizi regionali (es. prestazioni sanitarie; pagamenti bollo auto); servizi per l'accesso a bonus governativi (https://spid.18app.italia.it; https://spid.cartadeldocente.istruzione.it). Come indicato da alcuni gestori, nel 2023 è aumentata la percentuale di clienti che ha utilizzato SPID per accedere all'app IO e che ha effettuato l'accesso al fascicolo sanitario elettronico. Ulteriori indicatori riferiti al servizio SPID sono disponibili nell'apposita sezione del portale di avanzamento digitale (https://avanzamentodigitale.italia.it/it/progetto/spid).

[20] 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 predisponga 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 *Customer Care*), alle modalità di utilizzo del servizio (servizi più frequentemente acceduti), ai livelli di servizio erogati e ai risultati di periodiche valutazioni degli utenti sulla qualità del servizio (indagini di *Customer Satisfaction*).

4 PROCEDIMENTI DI VERIFICA NEL 2023

Le verifiche svolte nel 2023 hanno riguardato prevalentemente i gestori di identità digitale SPID e i prestatori di servizi fiduciari qualificati e, come per gli anni precedenti, sono state condotte con l'apporto di competenze specialistiche dell'*Area Vigilanza e Monitoraggio* dell'Agenzia, dal personale del *Cert-AgID*[21] e del *Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza*[22].

Sono state avviate anche ispezioni nei confronti dei Service Provider SPID, volte a rilevare il livello di conformità agli obblighi previsti dal DPCM 24 ottobre 2014 e alla Convenzione stipulata con AgID, e nei confronti dei Conservatori, relativamente ai requisiti per l'erogazione del servizio di conservazione[23].

4.1 RIEPILOGO DELLE VERIFICHE

Nel corso del 2023 sono stati attivati **20 procedimenti di verifica** (1 dei quali riunito in un procedimento avviato nel 2022, e altri 2 riuniti in un procedimento avviato nel 2024), di cui 3 avviati a seguito di segnalazioni e richieste nell'ambito di indagini di polizia giudiziaria e 17 nell'ambito di verifiche programmate. Le ispezioni condotte nei 17 procedimenti oggetto di programmazione hanno, comunque, preso in esame anche le segnalazioni pervenute per il soggetto ispezionato, elemento che peraltro concorre alla valorizzazione del menzionato indice di rischio[24].

È importante evidenziare che i procedimenti di verifica possono scaturire, altresì, dall'attività istruttoria avviata a seguito di richieste da parte dell'autorità giudiziaria o da segnalazioni effettuate dagli utenti, eventualmente riunite in un unico procedimento qualora relative a uno stesso gestore o a più servizi erogati dallo stesso gestore (ad esempio SPID e firme digitali). Tutte le richieste provenienti dall'autorità giudiziaria e le segnalazioni utente non manifestamente infondate danno luogo a un'istruttoria, nell'ambito della quale si acquisiscono dai gestori coinvolti gli elementi necessari che, ove ne ricorrano i presupposti, possono portare all'avvio di un procedimento di verifica. Possono essere trattate nell'ambito di uno stesso procedimento le richieste e le segnalazioni pervenute anche in tempi diversi e relative a uno stesso gestore o a più servizi erogati dallo stesso gestore (ad esempio SPID e firme digitali). Nel 2023 le richieste e le segnalazioni sono state in gran parte relative a situazioni per le quali i gestori interessati avevano già in corso azioni per la relativa risoluzione; un numero rilevante di segnalazioni utente, inoltre, è stato risolto attraverso interlocuzioni

[21] https://cert-agid.gov.it

[22] 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) e rinnovato a marzo 2022.

[23] Allegato A al Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici, adottato con determina n. 455/2021.

[24] Si veda Cap. 2.2.

con l'utente o con il gestore, riguardando richieste di informazioni sul servizio o asseriti malfunzionamenti.

Per i 20 procedimenti avviati sono state svolte complessivamente 17 ispezioni (per una corretta lettura del dato si evidenzia che per due procedimenti avviati a fine 2023, l'ispezione è stata svolta nel 2024, mentre due procedimenti sono stati riuniti e ne è scaturita un'unica ispezione). Delle 17 ispezioni, 15 sono state condotte presso le sedi dei gestori, 2 ispezioni relative ai Service Provider SPID sono state svolte da remoto.

Come si rileva dal grafico che segue, i 20 procedimenti hanno riguardato le seguenti tipologie di soggetti vigilati: i QTSP (9); i gestori di identità SPID (7); i gestori PEC (1); i fornitori di servizi SPID (2); i Conservatori (1).

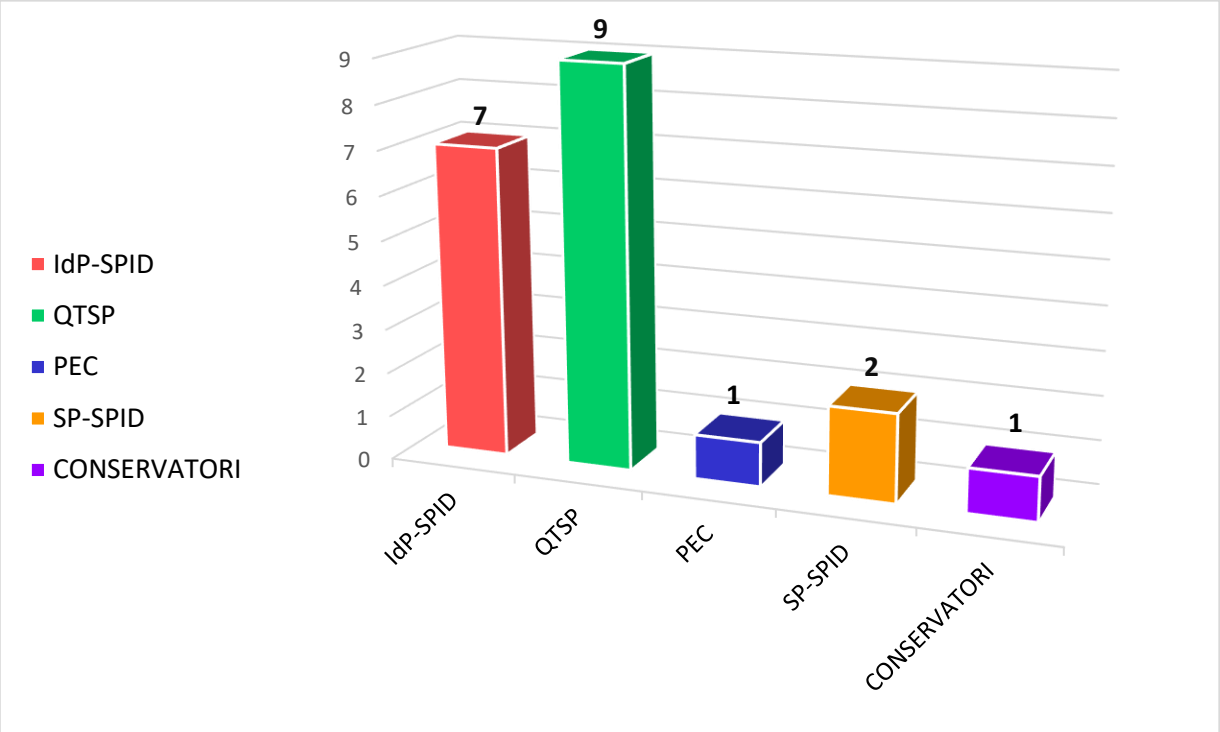

Fig. 7 - Procedimenti di verifica avviati nel 2023 suddivisi per ambito

Le verifiche 2023 hanno portato in 3 casi all'attivazione della fase sanzionatoria. È stata, inoltre, conclusa l'istruttoria per 4 procedimenti sanzionatori avviati nel 2022 (2 riuniti).

Per l'attività sanzionatoria si rimanda al Cap. 9.

Le verifiche condotte nell'ambito dei 20 procedimenti hanno preso in esame alcune componenti, non necessariamente le stesse per le varie tipologie di servizio.

Alle componenti esaminate si riferiscono i rilievi indicati nel paragrafo che segue.

4.2 RIEPILOGO DEI RILIEVI

Il grafico che segue mostra che complessivamente sono stati formulati 99 rilievi, distinti in 61 "Non Conformità" e 38 "Osservazioni"; circa il 41% dei rilievi ha riguardato i gestori SPID, circa il 47% dei rilievi ha riguardato i QTSP, il restante 12% l'insieme di gestori PEC, Conservatori e SP-SPID.

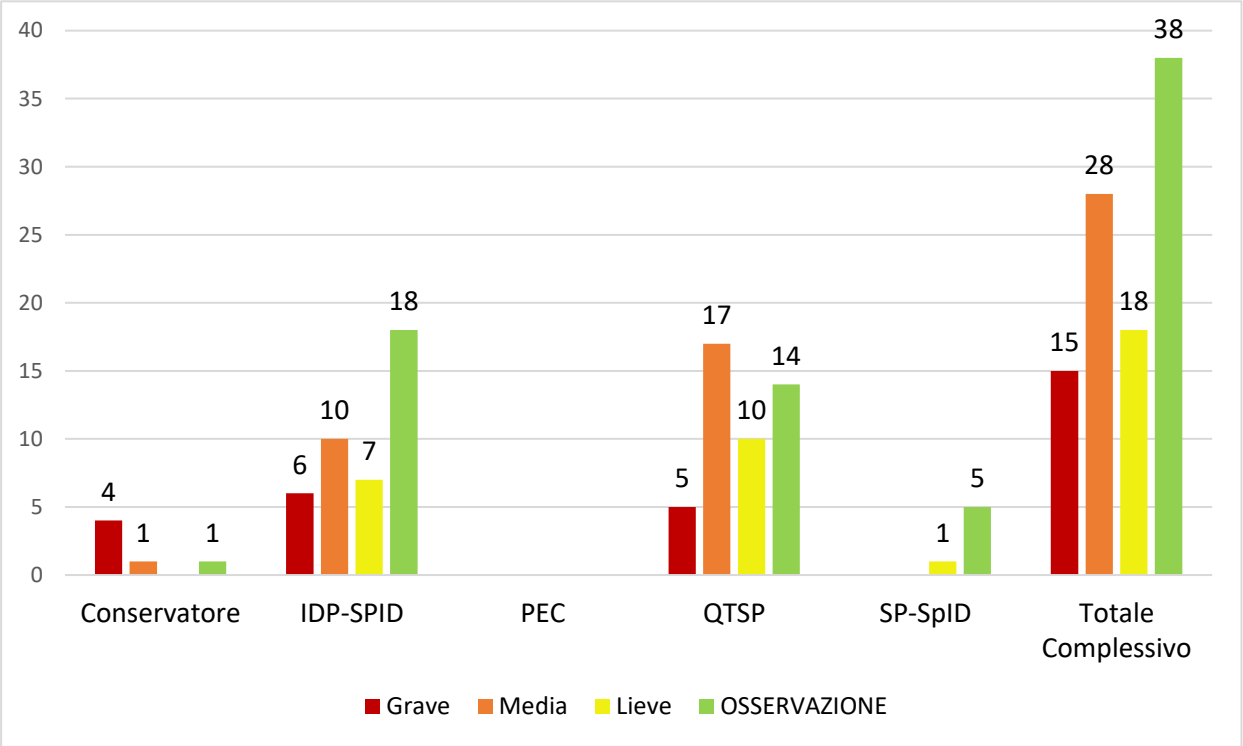

Fig. 8 - Totale dei rilievi e distribuzione per servizio per l'anno 2023

Tali dati si riferiscono a 18 dei 20 dei procedimenti sopra indicati (2 procedimenti sono stati successivamente riuniti in un unico procedimento avviato nel 2024).

Tutti i procedimenti hanno comportato l'adozione di azioni correttive o di miglioramento, che sono oggetto di monitoraggio nell'ambito delle verifiche d'ufficio.

Le verifiche hanno portato in 3 casi all'attivazione della fase sanzionatoria, dei quali 2 in ambito SPID, e 1 in ambito conservazione documentale.

Classificazione Rilievi	Conservatore	IDP-SPID	PEC	QTSP	SP-SPID	Totale complessivo
Grave	4	6	-	5	-	15
Lieve	-	7	-	10	1	18
Media	1	10	-	17	-	28
OSSERVAZIONE	1	18	-	14	5	38
Totale complessivo	**6**	**41**	**0**	**46**	**6**	**99**

Tab. 1 - Classificazione dei rilievi per servizio

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

4.3 ANALISI DEI RILIEVI

L'analisi dei rilievi formulati nell'ambito dei procedimenti di verifica consente di evidenziare se vi siano situazioni critiche più ricorrenti.

Le componenti di servizio a cui fa riferimento il maggior numero di rilievi (un rilievo può riguardare più componenti di servizio) riguardano la Gestione delle terze parti, la Gestione del processo, la Formazione e la componente di Analisi rischi e VA/PT relativa alle misure per la prevenzione degli incidenti di sicurezza.

Le prime tre componenti sono strettamente correlate ai fini della corretta erogazione dei servizi all'utente finale.

La **Gestione delle Terze Parti**, in particolare, 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, i subcontraenti siano dotati delle competenze, dell'affidabilità, dell'esperienza e delle qualifiche necessarie, e che abbiano ricevuto una formazione adeguata sugli obblighi e le procedure che devono essere seguiti nell'erogazione del servizio[25]. La terza parte può operare solo nell'ambito di un accordo contrattuale con il gestore che, in ogni caso, rimane il responsabile dell'erogazione del servizio all'utente finale. I rilievi formulati per tale componente sono conseguenza di un non sempre adeguato governo da parte del gestore dell'accordo contrattuale, con controlli non tempestivi o condotti in modo inefficace.

Più in generale, in riferimento alla **Gestione del processo**, i rilievi riguardano in gran parte procedure e strumenti che il gestore rende disponibili agli operatori preposti all'identificazione dei richiedenti un'identità digitale o un certificato di firma digitale, non sempre in grado di limitare errori o comportamenti difformi dalle procedure previste.

La **Formazione** è spesso limitata a nozioni di base sulla normativa e sull'uso degli applicativi messi a disposizione dei gestori.

[25] 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 servizio ("partner tecnici").

5 SERVICE PROVIDER SPID

In riferimento al potenziamento delle funzioni di vigilanza esercitate da AgID ai sensi dell'art. 14-*bis* del CAD, nel 2023 sono state effettuate le prime visite ispettive da remoto nell'ambito di 2 procedimenti nei confronti dei fornitori di servizi SPID ("SP"). I procedimenti sono stati avviati sulla base dei risultati del questionario somministrato ai SP durante l'anno precedente attraverso la piattaforma informatica TrustServices, selezionando i soggetti con il più alto numero di risposte negative.

A seguito dell'attività ispettiva sono emersi complessivamente **6 rilievi**, di cui 1 "Non Conformità Lieve" e 5 "Osservazioni", che hanno comportato, da parte dei fornitori di servizi, la produzione di un piano di rientro e/o di miglioramento da attuare attraverso azioni correttive.

6 NOTIFICHE DI INCIDENTI E MALFUNZIONAMENTI

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

Con riferimento agli obblighi di notifica di incidenti e malfunzionamenti da parte dei soggetti vigilati, nel 2023 sono stati notificati complessivamente **120 eventi relativi a incidenti, malfunzionamenti o indisponibilità** per attività di manutenzione relativi ai servizi PEC (4), SPID (82) e servizi fiduciari (34).

Sono stati oggetto di notifica principalmente eventi relativi a indisponibilità (anche per attività di manutenzione), ed eventi con impatto su confidenzialità, integrità o autenticità.

Le notifiche sono inoltrate ad AgID e gestite attraverso la piattaforma informatica TrustServices.

Di seguito alcuni grafici riassuntivi.

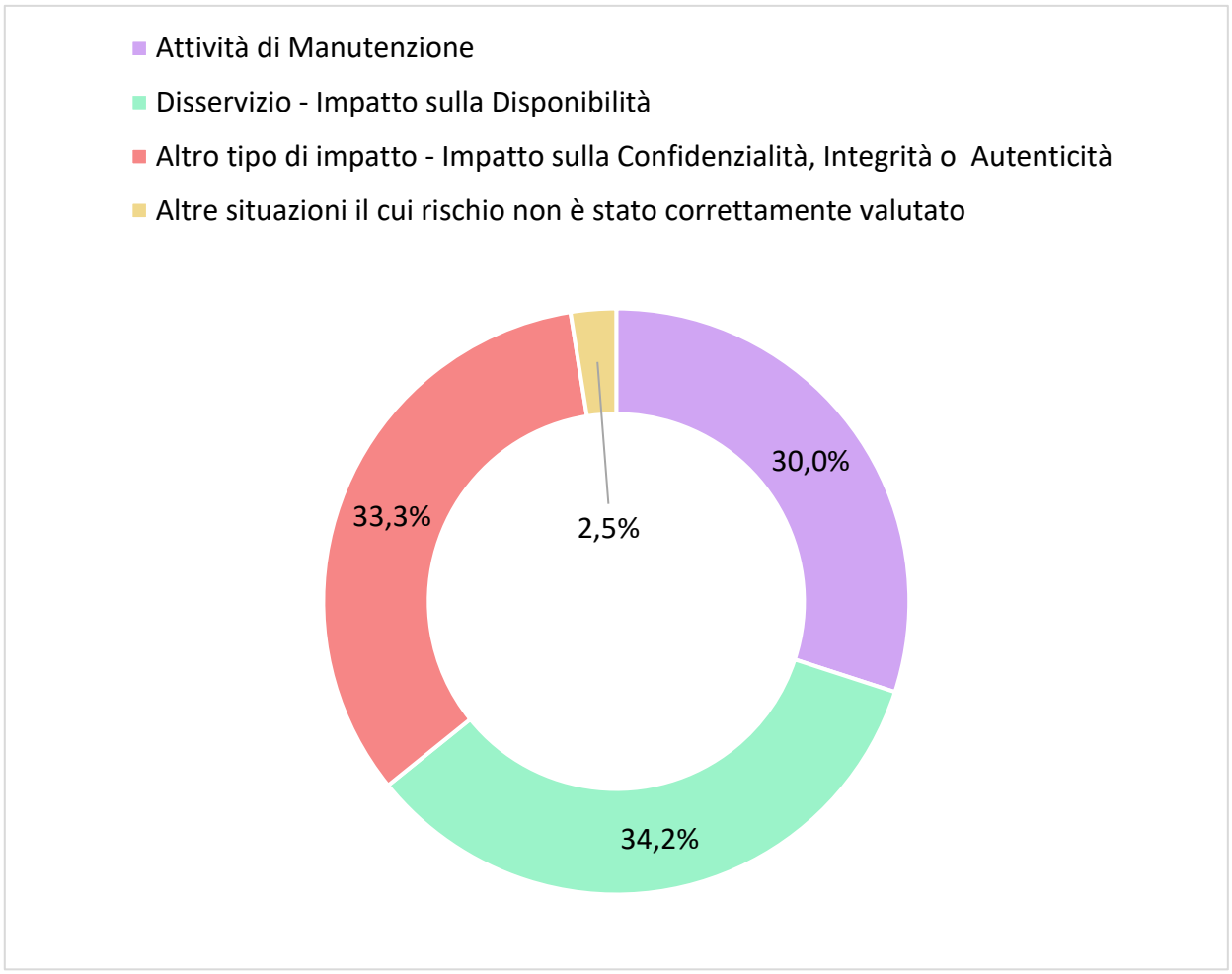

Fig. 9 - Distribuzione percentuale delle notifiche 2023 per tipologia

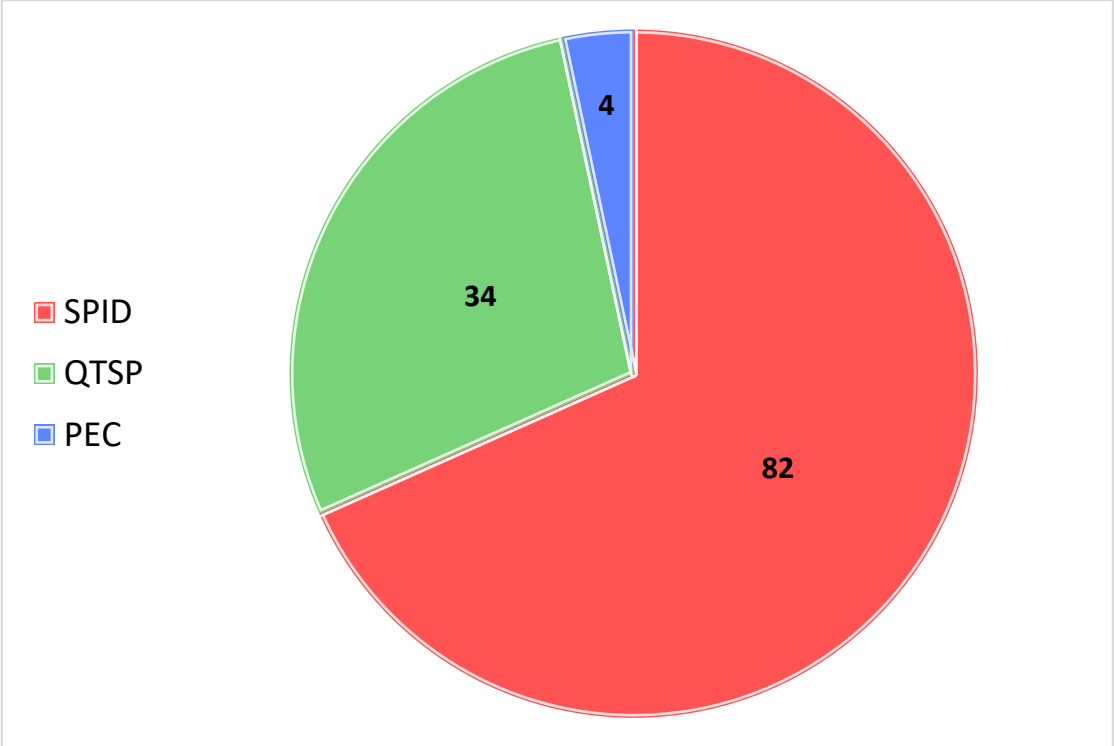

Fig. 10 - Notifiche 2023 suddivise per servizio

7 SEGNALAZIONI DAGLI UTENTI E RICHIESTE DA ALTRE AUTORITÀ

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, eventualmente disponibile, a sostegno della presunzione di violazione normativa o irregolarità.

Ad AgID, inoltre, sono indirizzate richieste che riguardano l'acquisizione di informazioni nell'ambito di indagini di polizia giudiziaria.

Al fine di riscontrare efficacemente sia le segnalazioni e che le sopra menzionate richieste di informazioni, si fa riferimento alla classificazione implementata attraverso la piattaforma informatica TrustServices. Tale sistema, che si interfaccia con il protocollo AgID, permette una gestione semplificata delle comunicazioni da e verso i soggetti vigilati, ai quali viene fornito l'accesso tramite utenze configurate attraverso apposita procedura.

Nel 2023 sono state gestite **137 segnalazioni** (relative a oltre 500 utenze), di cui **96 richieste su presunte irregolarità** o utilizzo dei servizi a scopo asseritamente fraudolento (principalmente SPID e firma digitale) e **41 segnalazioni utente**.

Il numero di segnalazioni che ogni anno arrivano ad AgID è in **forte crescita**, come si evidenzia dai grafici di seguito riportati, verosimilmente a causa della sempre maggiore centralità che rivestono per i cittadini il sistema SPID di identità digitale e i servizi fiduciari di firma. Nell'ultimo anno tale crescita è stata ulteriormente accentuata dalla maggiore attenzione posta dai media nei riguardi del fenomeno dei furti di identità digitali.

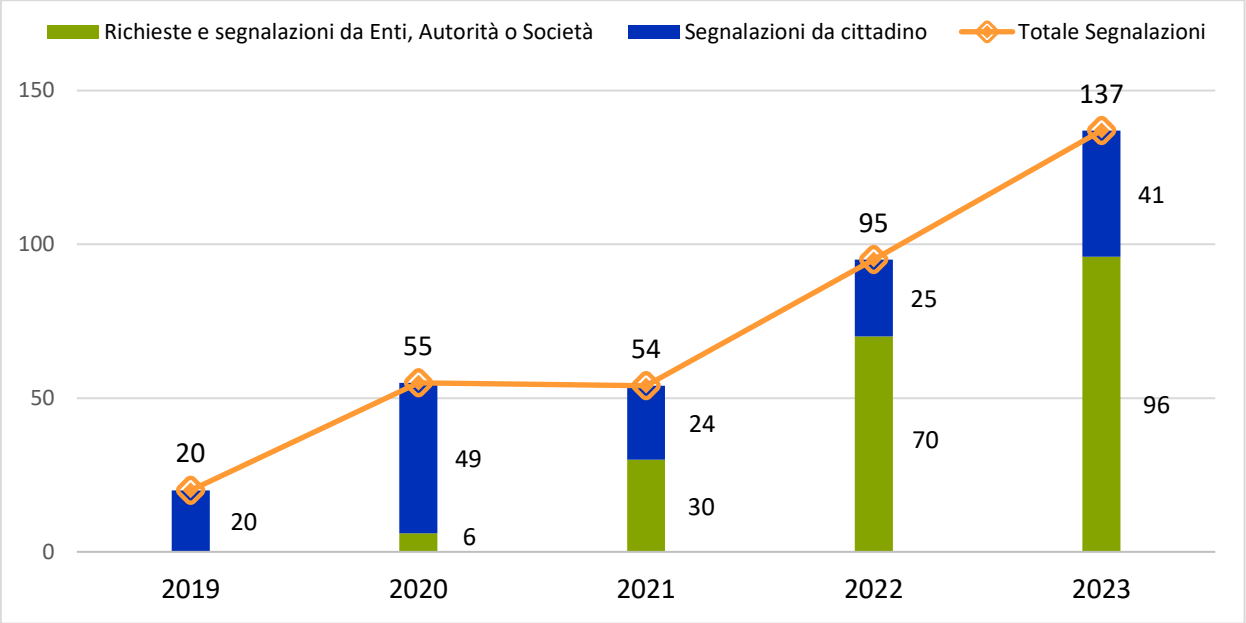

Fig. 11 - Andamento del numero di segnalazioni pervenute ad AgID dal 2019 al 2023

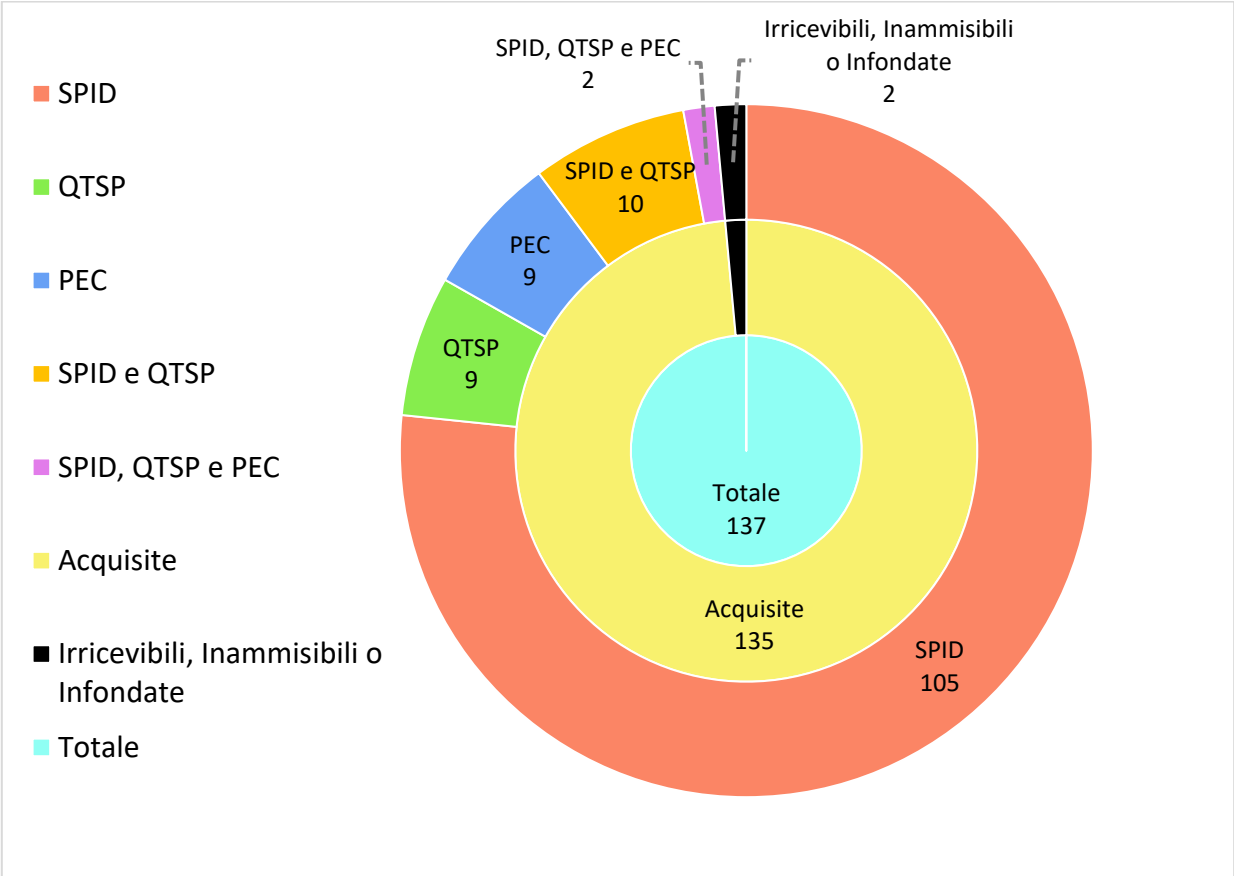

Fig. 12 - Classificazione delle segnalazioni 2023 per servizio coinvolto

8 LE ATTIVITÀ IN AMBITO EUROPEO

Per quanto riguarda la vigilanza sui prestatori di servizi fiduciari qualificati, AgID, in qualità di 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 e assistenza reciproca o sono volte a favorire lo scambio di *best practice* tra gli organismi di vigilanza dei diversi Stati Membri.

Entro il 31 marzo di ogni anno AgID trasmette alla Commissione una relazione sulle principali attività di vigilanza svolte sia ai fini della qualificazione di nuovi TSP (prestatori di servizi fiduciari) che sui prestatori già qualificati (QTSP). 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 agli obblighi di notifica ex art. 19 del Regolamento eIDAS, è stato costituito il gruppo di lavoro ECATS (*European Competent Authorities for Trust Services* – in precedenza *Article 19 Expert Group*), composto dai rappresentanti degli Organismi di vigilanza europei previsti all'art. 17 del Regolamento eIDAS. Coordina il gruppo di lavoro ENISA, l'Agenzia dell'Unione Europea per la Cybersecurity (https://www.enisa.europa.eu/about-enisa), con riferimento, tra l'altro, alle modalità per le rendicontazioni di tali eventi tra i diversi organismi di vigilanza degli Stati Membri, al fine di adottare pratiche comuni di classificazione e gestione. ENISA pubblica annualmente un *report* che riepiloga, in forma anonima e con dati aggregati, gli incidenti notificati dai diversi Stati membri, con lo scopo di creare una conoscenza comune dei punti deboli riscontrati e delle vulnerabilità più ricorrenti[26].

Il quadro per la segnalazione degli incidenti ai sensi del più volte citato 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). ENISA ha sviluppato uno strumento in linea, ad uso degli organismi di vigilanza degli Stati Membri, per facilitare la procedura di notifica degli incidenti con impatto transfrontaliero.

ECATS si riunisce con frequenza semestrale, ma agisce anche attraverso altre forme di interlocuzione 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, 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.

[26] Il 22 febbraio 2024 è stato pubblicato da ENISA il report Trust Services Security Incidents 2022, 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 analoghi organismi degli altri Stati Membri.

9 LE SANZIONI

Il CAD, all'art. 32-*bis*, definisce i casi per i quali possono essere irrogate sanzioni amministrative.

Le verifiche effettuate nel 2023 hanno portato, in **3 casi**, all'attivazione della **fase sanzionatoria**, dei quali 2 in ambito SPID e 1 in ambito conservazione documentale.

Le irregolarità riscontrate hanno riguardato in linea di massima:

- l'impiego di personale non sempre adeguatamente formato e aggiornato sulle specifiche tematiche;
- l'adozione di sistemi e pratiche operative e gestionali non sempre in grado di contrastare o limitare comportamenti non conformi alle procedure stabilite, o richieste di identità digitale o certificati di firma per utilizzi impropri del servizio;
- l'assenza o l'inefficacia di controlli sistematici sulle terze parti per prevenire comportamenti non conformi alle procedure previste e per rilevare prontamente eventuali livelli di disponibilità e sicurezza dei sistemi non in linea con gli accordi contrattuali.

Nel corso del 2023 è stata, inoltre, **conclusa l'istruttoria per 4 procedimenti sanzionatori avviati nel 2022** (2 riuniti), con pagamento in misura ridotta di sanzioni amministrative per un totale di 480.000,00 euro.

10 AZIONI SCATURITE DALLE VERIFICHE

Le verifiche sui soggetti vigilati, effettuate tramite ispezioni dirette e controlli documentali continui, forniscono gli elementi necessari per individuare e pianificare interventi correttivi e di miglioramento. Questi interventi riguardano sia le modalità di erogazione del servizio da parte del soggetto vigilato, sia gli aggiornamenti normativi da parte degli enti regolatori, sia le responsabilità degli utenti nell'uso consapevole e conforme dei servizi. Ai fini delle attività istruttorie, vengono preliminarmente esaminati i documenti di riscontro nell'ultima versione comunicata ad AgID (Manuale Operativo, Guida Utente, Piano della Sicurezza), nonché le informazioni disponibili relative a notifiche di incidenti/malfunzionamenti, dati periodici di riepilogo, azioni del piano di rientro relativo al precedente procedimento.

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, in riferimento a uno o più servizi, sono **richiesti specifici controlli o avviate iniziative indirizzate a tutti i gestori** che vedono attivamente coinvolte le diverse unità organizzative AgID.

Ne sono un esempio i risultati riportati nel report annuale del CERT-AgID, che confermano l'impatto positivo delle iniziative di contrasto avviate negli anni precedenti, mirate a ridurre gli effetti negativi delle campagne malware diffuse tramite Posta Elettronica Certificata. La **collaborazione costante e sinergica tra il CERT-AgID e i gestori PEC** è stata cruciale nel limitare la diffusione di contenuti dannosi e nel garantire maggiore sicurezza per gli utenti finali.

Numerosi interventi sono stati adottati, inoltre, dai soggetti vigilati nel corso del 2023 in relazione alle situazioni rilevate attraverso le segnalazioni utente e le richieste nell'ambito di indagini di polizia giudiziaria (vds. Cap. 7). Per quanto riguarda i prestatori di servizi fiduciari qualificati e i gestori SPID principalmente coinvolti nelle segnalazioni e nei procedimenti avviati nel 2023, sono stati richiesti interventi mirati a sistematizzare e documentare le procedure e gli strumenti utilizzati dagli operatori incaricati dell'identificazione dei richiedenti. L'obiettivo è garantire un controllo adeguato sul loro operato, in particolare per l'emissione di identità digitali e firme digitali, al fine di individuare tempestivamente errori umani e anomalie nei processi di identificazione e registrazione dei dati, sia effettuati direttamente, sia tramite terze parti (*Registration Authority*-RA[27] e *Registration Authority Operator* -RAO[28]).

[27] *Registration Authority*: soggetto 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

[28] *Registration Authority Operator*-RAO: 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.

Tali iniziative, in continuità con quanto già avviato negli anni precedenti, sono volte a contrastare **fenomeni sempre più frequenti di furti di identità**, o di utilizzo dei servizi a scopo fraudolento, numerosi anche nel 2023, seppur perpetrati con rinnovate modalità. I furti di identità continuano a registrarsi per operazioni specifiche (es. accesso ai *bonus* di iniziativa governativa quali *bonus* vacanze, *bonus* 18app, carta del docente; 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 strumenti di identificazione e 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 sull'utilizzo consapevole e responsabile di tali sistemi, adottando comportamenti che ostacolino utilizzi impropri di tali servizi, ad esempio assicurando la custodia del dispositivo di firma, non rivelando a terzi le credenziali di acceso, utilizzando personalmente i sistemi di cui è titolare. Per quel che riguarda i gestori, è necessaria un'accurata gestione delle anagrafiche dei titolari (ad esempio assicurando, in fase di registrazione, che i dati di contatto come e-mail e cellulare siano riferibili ad un unico titolare o che non siano presenti similitudini tra dati riferiti a diversi titolari) 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 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.

Per gli impegni futuri, proseguono le iniziative già avviate negli anni precedenti volte a consolidare e migliorare sempre più gli strumenti disponibili ad AgID per costruire conoscenza e pianificare le verifiche a partire dai dati.

11 APPENDICE

11.1GLOSSARIO

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.

SP – *Service Provider*- Fornitore di servizi cui accedere tramite autenticazione SPID.

SPID – Sistema Pubblico di Identità Digitale.

VA - *Vulnerability Assessment*: Processo sistematico volto a identificare, classificare e valutare le vulnerabilità presenti in un sistema informatico, una rete o un'applicazione, al fine di mitigare i rischi di sicurezza.

PT - *Penetration Test*: Attività simulata di attacco informatico, condotta da esperti, che mira a sfruttare le vulnerabilità individuate per valutare il livello di sicurezza e la resilienza del sistema a potenziali intrusioni reali.

11.2RIFERIMENTI 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