Riepilogo dati 2022

Vigilanza sui servizi fiduciari qualificati, PEC, SPID, conservazione a norma

AGID | Agenzia per l'Italia Digitale

Indice

1 PREFAZIONE 3

2 LE FUNZIONI DI VIGILANZA SVOLTE DA AGID 6

2.1 RICHIAMI RELATIVI AL QUADRO NORMATIVO 6
2.2 LE REGOLE E LE MODALITÀ DI ESECUZIONE 7
2.3 LE PARTI INTERESSATE (*STAKEHOLDER*) 8

3 TASSONOMIA DEI SOGGETTI VIGILATI 10

3.1 PRESTATORI DI SERVIZI FIDUCIARI QUALIFICATI (QTSP) 10
3.2 GESTORI PEC 13
3.3 IDENTITY PROVIDER SPID (IDP) 14

4 PROCEDIMENTI DI VERIFICA NEL 2022 17

4.1 RIEPILOGO DELLE VERIFICHE 17
4.2 VERIFICHE DI SECONDA PARTE E COMPONENTI DI SERVIZIO 18
4.3 RIEPILOGO DEI RILIEVI 18
4.4 ANALISI DEI RILIEVI 19

5 SERVICE PROVIDER SPID 21

6 NOTIFICHE DI INCIDENTI E MALFUNZIONAMENTI 22

7 SEGNALAZIONI DAGLI UTENTI E RICHIESTE DA ALTRE AUTORITÀ 23

8 LE ATTIVITÀ IN AMBITO EUROPEO 24

9 LE SANZIONI 26

10 AZIONI SCATURITE DALLE VERIFICHE 27

11 APPENDICE 29

11.1 GLOSSARIO 29
11.2 RIFERIMENTI NORMATIVI 29

1 PREFAZIONE

La presente relazione illustra le attività di vigilanza svolte nel 2022 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 riguardano i principali prestatori dei *digital trust services*, servizi quali la firma elettronica qualificata, l'identità digitale e la posta elettronica certificata, che abilitano le transazioni digitali in sicurezza tra le pubbliche amministrazioni, le imprese ed i cittadini, favorendo lo sviluppo di servizi *on line*.

Obiettivo della vigilanza è da un lato **prevenire irregolarità 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 allo scopo di **rafforzare la fiducia dei cittadini nelle transazioni on line** e favorire lo sviluppo dell'economia digitale[2]; dall'altro la vigilanza mira 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. L'impegno costante dell'Agenzia, nel ruolo di autorità di vigilanza, è **stimolare i soggetti vigilati al miglioramento continuo dei processi di erogazione,** in modo sostenibile per il sistema dei *digital trust services*, secondo livelli di qualità e sicurezza coerenti tra i diversi operatori, sfruttando le opportunità offerte dalla continua evoluzione tecnologica e assicurando la conformità alle indicazioni del quadro normativo europeo.

Per tali finalità, l'Agenzia svolge **accertamenti di tipo ispettivo,** allo scopo di verificare irregolarità che danno luogo all'irrogazione di sanzioni e richiedono azioni correttive; promuove inoltre **verifiche in via preventiva**, richiedendo ai soggetti vigilati azioni di miglioramento. La vigilanza consente infatti di rilevare elementi per individuare e pianificare 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.

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[2], le istituzioni e gli stessi

[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*.

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 relazione è giunta alla sua sesta edizione. Nel 2022 le funzioni di vigilanza hanno riguardato 20 prestatori di servizi fiduciari qualificati con **oltre 29 milioni di certificati qualificati di firma**, 18 gestori di posta elettronica certificata accreditati con oltre **15 milioni di caselle PEC** e 10 gestori di identità digitale SPID per circa **33 milioni di identità digitali SPID**[3]**.** Tali soggetti **includono 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"). Per questi ultimi, il 1° gennaio 2022 è entrato in vigore il Regolamento[4] che definisce i nuovi criteri per la fornitura del servizio e specifica i requisiti generali, di qualità, di sicurezza e di organizzazione necessari per la fornitura del servizio. Da tale data è stata avviata l'iscrizione al *Marketplace dei servizi di conservazione*[5] e nel corso del 2022 sono stati iscritti 56 Conservatori.

Nel 2022 sono proseguite le attività gestite 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].

In considerazione degli sviluppi in itinere per la conservazione e la PEC e del **volume crescente di segnalazioni** per asseriti utilizzi impropri dei servizi di firma e di identità digiltale, i **12 procedimenti di verifica** avviati 2022 hanno riguardato prevalentemente i gestori di identità digitale SPID e i prestatori di servizi fiduciari qualificati. Al fini del potenziamento delle funzioni di vigilanza, nel 2022 sono state avviate anche **specifiche verifiche sui Service Provider SPID**, coinvolgendo in particolare 18 Regioni, nel ruolo di SP SPID, in un *assessment* volto a rilevare il livello di conformità agli obblighi previsti dal DPCM 24 ottobre 2014 e alla Convenzione stipulata con AgID.

In riferimento ai 12 procedimenti di verifica, sono state eseguite **14 verifiche ispettive**, delle quali 11 *on site*, presso le sedi dei gestori, 3 da remoto, con l'apporto di competenze specialistiche dal

---

[3] I dati relativi ai volumi gestiti per SPID e firme digitalisi siriferiscono al 31 dicembre 2022; per le caselle PEC si riferiscono al 30 giugno 2022.

[4] 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.

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

[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*".

Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza[7] e dal personale del ***Cert-AgID***[8].

In linea con gli obiettivi programmati, nel 2022 sono proseguite le attività per il rilascio delle funzioni per la raccolta e la gestione dei **dati strutturati** da parte dei soggetti vigilati attraverso il sistema informatico[9]. A tal fine è stata avviata a regime l'acquisizione da parte dei soggetti vigilati delle notifiche di incidenti, malfunzionamenti e interruzioni di servizio con tali nuove modalità e la gestione delle segnalazioni e richieste relative ai servizi vigilati. Sono state gestite nel 2022 circa **70 notifiche** di eventi pervenute dai gestori e 95 segnalazioni, di cui **70 richieste relative a oltre 500 utenze** oggetto di indagini su presunto utilizzo dei servizi (principalmente SPID e firma digitale) a scopo asseritamente fraudolento e **25 segnalazioni utente**. Tali segnalazioni hanno dato luogo a 9 dei 12 procedimenti di verifica avviati nel 2022.

Le verifiche svolte, sia in occasione delle attività ispettive che in via continuativa in sinergia con il Cert-AgID, hanno portato i gestori ad adottare importanti azioni per elevare le misure di sicurezza e contrastare i tentativi di frode perpetrate a danno degli utenti. **Di particolare rilievo la collaborazione continua e sinergica dei gestori PEC con il CERT-AgID**, che ha rivestito un ruolo fondamentale nel limitare la diffusione di contenuti dannosi e nell'assicurare una maggior sicurezza degli utenti finali. L'impiego della piattaforma MISP[10] per la condivisione degli Indicatori di Compromissione (IoC) con i gestori PEC ha agevolato le attività di contrasto alle minacce informatiche. Altrettanto efficacemente **sono stati respinti vari attacchi DDoS diretti ai gestori SPID** durante il periodo di tensione nel conflitto Russia-Ucraina, confermando così l'efficacia e la flessibilità delle misure di sicurezza adottate.

Con riferimento al sistema informatico, è stata implementata una nuova sezione interamente dedicata alla progettazione e alla somministrazione alle diverse categorie di soggetti vigilati di questionari di autovalutazione. Tale funzione consente di acquisire preliminarmente elementi per pianificare verifiche verso i soggetti vigilati.

Attraverso il sistema informatico, nel 2022, a seguito del completamento dei documenti tecnici di specifica dell'infrastruttura di raccolta e dei tracciati dati, è stata **avviata l'acquisizione dei dati periodici** relativi al servizio SPID attraverso interfacce applicative.

Alle attività sopra accennate sono dedicate specifiche sezioni della relazione; nella sezione introduttiva si richiamano le informazioni di contesto sulla vigilanza, evidenziando le modifiche intervenute rispetto al 2021.

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

I dati si riferiscono al 31/12/2022.

---

[7] 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.

[8] (https://cert-agid.gov.it)

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

[10] Malware Information Sharing Platform

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)[11], 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 e i Service Provider*. 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[12].

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.

Le principali novità del 2022 sul quadro normativo di riferimento per la vigilanza riguardano proprio il Regolamento eIDAS. A dicembre 2022 è stata infatti pubblicata la Direttiva (UE) 2022/2555 ("Direttiva NIS 2"). La nuova disciplina, che entra in vigore il 17 gennaio 2023 e dovrà essere recepita dagli Stati membri entro il 17 ottobre 2024, include nel campo di applicazione anche i servizi forniti da prestatori di servizi di fiducia e preve a decorrere dal 18 ottobre 2024 la soppressione dell'articolo 19 del Regolamento eIDAS, inerente i requisiti di sicurezza e gli obblighi di notifica all'organismo di vigilanza delle violazioni di sicurezza che abbiano un impatto significativo sui servizi fiduciari prestati.

Ulteriori novità introdotte nel 2022 riguardano il servizio SPID. L'Agenzia per l'Italia Digitale ha adottato[13] le Linee guida operative per il rilascio dell'identità digitale in favore dei minori d'età e la fruizione dei servizi online. Il rilascio di SPID a minori (nella fascia di età da 5 a 14 anni) e il suo utilizzo per l'accesso ai servizi online sono consentiti, in prima applicazione per un periodo sperimentale sino al 30 giugno 2023, per la sola fruizione dei servizi in rete erogati dagli istituti scolastici di ogni ordine e grado.

---

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

[12] 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 ed assistenza reciproca tra gli Organismi di vigilanza dei diversi Stati Membri

[13] Determinazione n.51/2022 del 3/03/2022.

Per quanto riguarda la PEC, a maggio 2022, nell'ambito dei lavori del tavolo istituito da AgID con i gestori PEC e Uninfo, è stato approvato da ETSI lo standard EN 319 532-4 V1.2.1 (REM (Registered Electronic Mail) Baseline). A seguito della pubblicazione del Draft il gruppo di lavoro ha pubblicato il documento "REM SERVICES - Criteri di adozione degli standard ETSI - Policy IT"- nella versione 1.2. Con determinazione n. 233 del 9 agosto 2022 AGID ha pubblicato le relative Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS n. 910/2014 - Criteri di adozione standard ETSI - REMPolicy-IT 1.0.

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 ai sensi dell'e per l'esercizio del potere sanzionatorio ai sensi dell'art.32-bis del d.lgs. 7 marzo 2005, n.82 e successive modificazioni"[14].

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; la modalità *on site* è stata quella più frequentemente utilizzata nel 2022.

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[15]; nel 2022, 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 QTSP 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 eventuali termini di sospensione, e può portare alla formulazione di rilievi, distinti

[14] 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.

[15] 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).

rispettivamente in 'Non Conformità[16]' e 'Osservazioni[17]'. 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.

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 all'esercizio dei compiti previsti; altre organizzazioni nazionali direttamente coinvolte nei processi primari della vigilanza[18].
- **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*), gruppo di lavoro con rappresentanti 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;
    - ECATS (*European Competent Authorities for Trust Services* – in precedenza *Article 19 Expert Group)*, gruppo di lavoro con rappresentanti degli Organismi di vigilanza europei

[16] 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.

[17] 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.

[18] 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.

previsti all'art. 17 del Regolamento eIDAS con il compito di favorire l'attuazione dell'art. 19 del Regolamento eIDAS;

- 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.

3 TASSONOMIA DEI SOGGETTI VIGILATI

Le funzioni di vigilanza ai sensi dell'art 14-bis dei CAD riguardano **20 prestatori di servizi fiduciari qualificati** ("QTSP") (1 nuovo prestatore qualificato nel 2022), **18 gestori di posta elettronica certificata accreditati** (1 prestatore cessato nel 2022), **10 gestori di identità digitale SPID** (1 nuovo gestore accreditato nel 2022) e gli ulteriori soggetti pubblici e privati che partecipano a SPID, tra i quali i fornitori dei servizi ("Service Provider" o "SP"); si applicano inoltre ai soggetti di cui all'art. 34, comma 1 bis del CAD, che erogano servizi di conservazione. Per questi ultimi, il 1° gennaio 2022 è entrato in vigore il Regolamento che definisce i nuovi criteri per la fornitura del servizio e specifica i requisiti generali, di qualità, di sicurezza e di organizzazione necessari per la fornitura del servizio. Da tale data è stata avviata l'iscrizione al Marketplace dei servizi di conservazione e nel corso del 2022 sono stati iscritti 56 soggetti.

Nel corso del 2022 i procedimenti di verifica hanno riguardato i gestori di identità digitale SPID, 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[19].

Nei paragrafi che seguono si presentano in forma anonima ed in modalità aggregate le principali caratteristiche, evidenziando le modifiche rispetto alla situazione relativa al 2021.

3.1 PRESTATORI DI SERVIZI FIDUCIARI QUALIFICATI (QTSP)

Nel 2022 è stato qualificato 1 nuovo prestatore di servizi fiduciari.

Al 31/12/2022 risultano 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 si rileva dalla *Trusted list* italiana[20], 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 circa il 93% dei certificati qualificati per firma remota; 4 QTSP coprono oltre l'88% 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

[19] 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)

[20] Si consulti EU Trust Services Dashboard

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 31/12/2022, che costituiscono l'offerta di servizi più consistente per questa tipologia di soggetti vigilati.

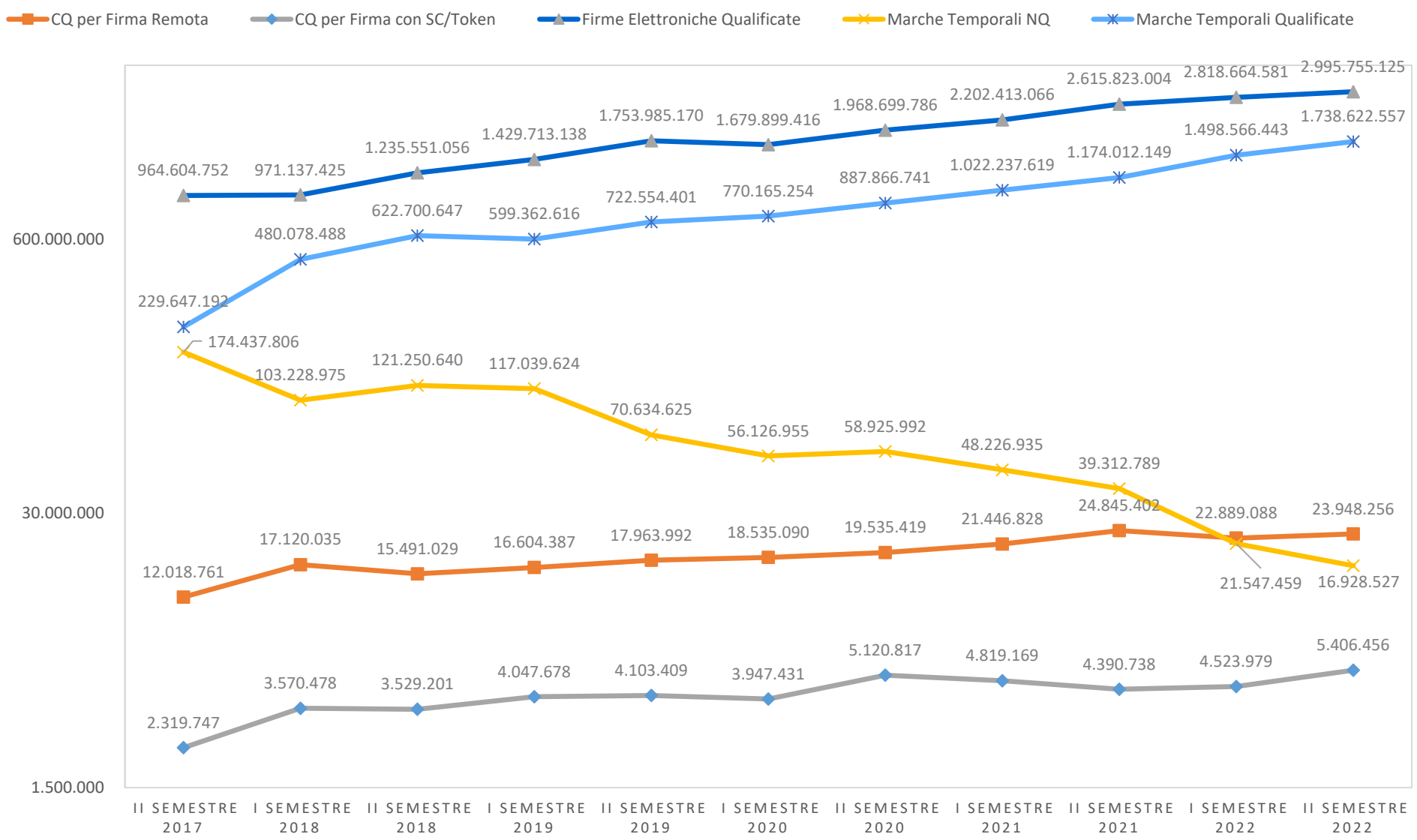

Fig. 1 - Andamento servizi di firma e marca temporale [gennaio-dicembre 2022, dati aggregati per semestre]

3.2 GESTORI PEC

Al 31/12/2022 risultano iscritti nell'elenco dei gestori PEC accreditati 18 soggetti. Non sono stati accreditati nuovi gestori nel corso del 2022, mentre 1 gestore ha cessato l'attività.

Si rilevano per i 18 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.

Per quanto riguarda i volumi di domini, caselle PEC e messaggi si rileva dai grafici che seguono un totale annuo di quasi 3 miliardi di messaggi complessivamente scambiati nel 2022, rispetto al totale di 2.498.131.944 registrato nel 2021, circa 256.000 domini registrati, 15 milioni di caselle attive e con picchi di oltre 550 milioni di messaggi scambiati a bimestre).

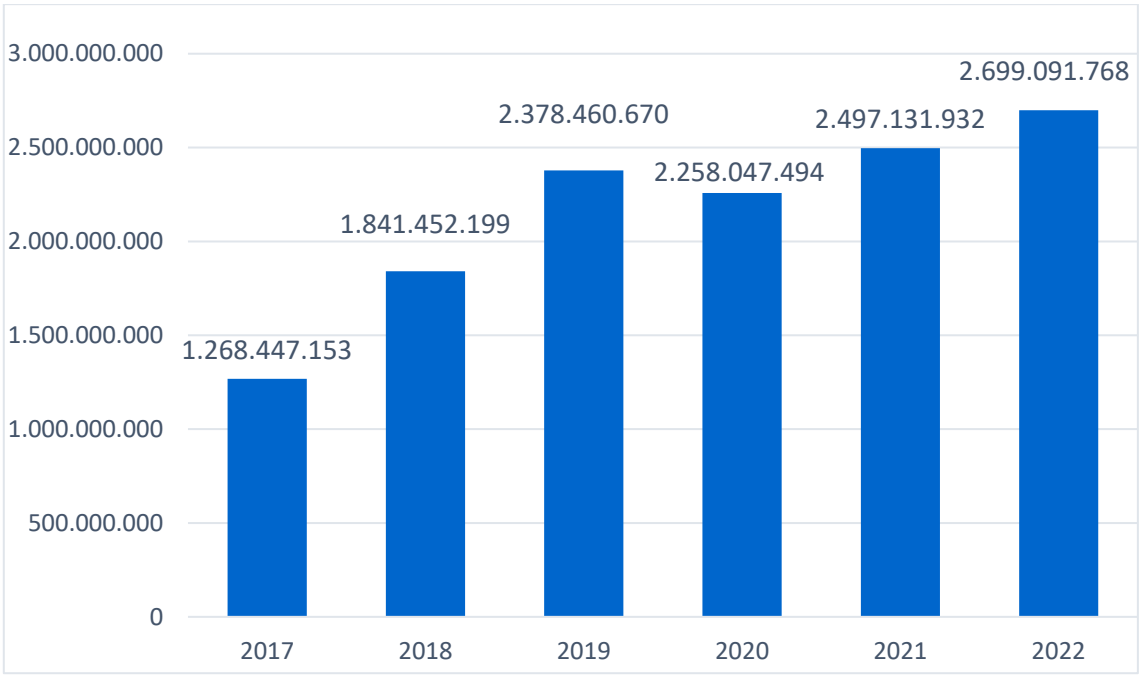

Fig. 2 - Messaggi PEC scambiati dal 2017 al 2022

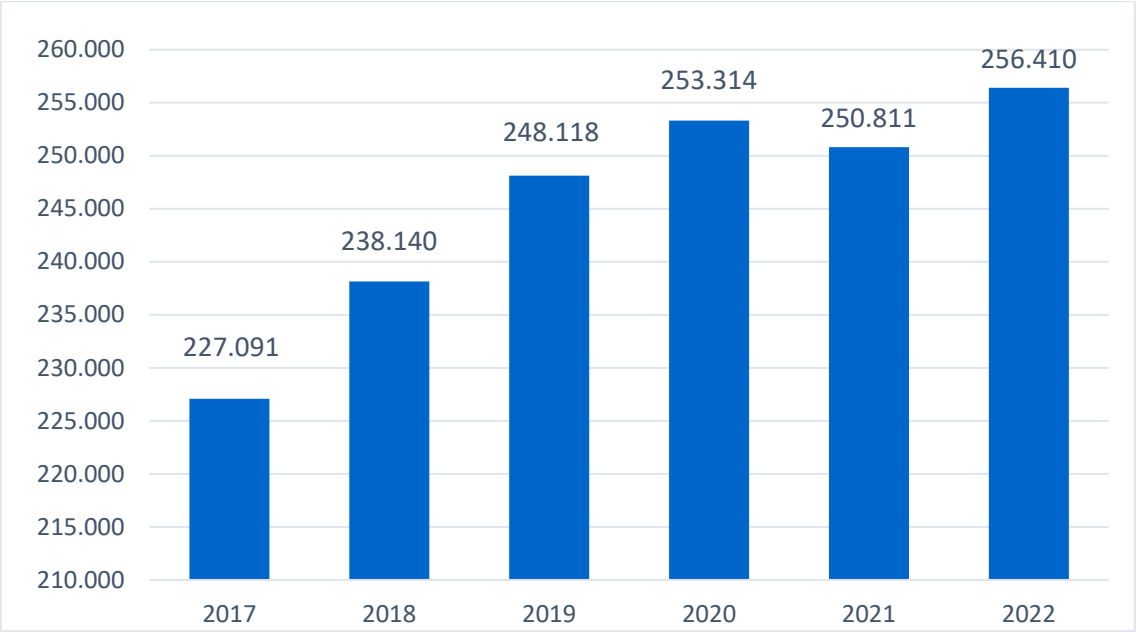

Fig. 3 - Domini PEC attivi dal 2017 al 2022

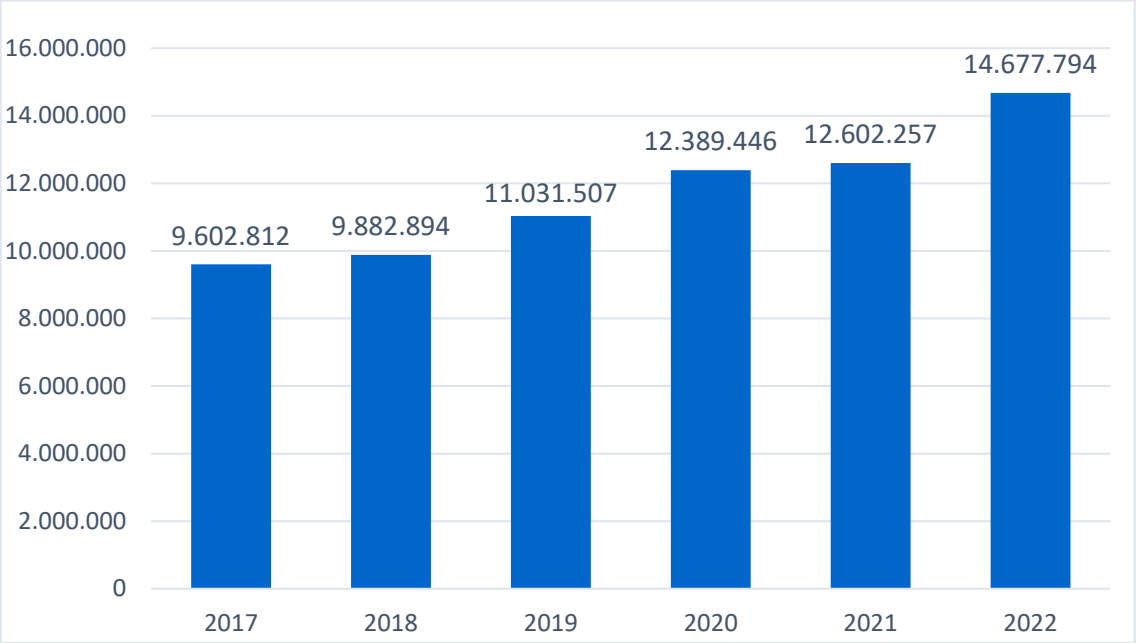

Fig. 4 - Caselle PEC attive dal 2017 al 2022

3.3 IDENTITY PROVIDER SPID (IDP)

Nel 2022 sono risultati attivi 10 Identity Provider (un nuovo IdP attivato nel corso dell'anno) e sono state emesse oltre 6 milioni di identità digitali, per un totale di oltre 33 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 2022** è ben oltre il doppio del valore registrato nel triennio 2020-2022.

Fig. 5 - Andamento delle identità gestite nel triennio 2020 - 2022

Per tutti gli IdP nel 2022 si è registrato un aumento dei volumi di identità gestite rispetto al 2021.

Le amministrazioni pubbliche che forniscono servizi tramite SPID sono 12.624 (circa3.500 ad inizio 2020) e, tra queste, hanno aderito a SPID oltre il 95% dei comuni italiani. 153 invece gli enti privati. Il numero complessivo di autenticazioni ai servizi on-line tramite SPID ha superato quota 1 miliardo, pari a circa il doppio del numero di autenticazioni registrato nell'intero 2021.

Dalle relazioni annuali di riepilogo[21] fornite dai gestori si rileva che i servizi più acceduti attraverso SPID riguardano 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 2022 è aumentata la percentuale di clienti che ha utilizzato SPID per accedere ai

[21] 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*).

Servizi INPS e che ha effettuato l'accesso al fascicolo sanitario. È più che raddoppiato rispetto al 2021 il numero di accessi ai servizi in rete effettuato mediante SPID.

Con riferimento alle campagne periodiche di Customer Satisfaction, e in particolare alle valutazioni sul livello di soddisfazione complessiva, passaparola e utilità del servizio, i gestori hanno confermato nelle relazioni annuali valori in crescita rispetto agli anni precedenti per i principali indicatori, soprattutto in riferimento agli indicatori di *performance*. Il servizio è ritenuto soddisfacente e molto utile dalla maggior parte degli utenti e aumenta la quota di clienti propensi a raccomandarlo. I principali motivi di insoddisfazione riguardano principalmente la complessità del processo in fase di attivazione, l'assistenza e la gestione delle password.

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 2022

Le verifiche svolte nel 2022 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 dal Nucleo di Prevenzione delle Frodi Tecnologiche della Guardia di Finanza[22] e dal personale del Cert-AgID[23].

Al fini del potenziamento delle funzioni di vigilanza, sono state avviate anche specifiche verifiche sui Service Provider SPID, in un *assessment* volto a rilevare il livello di conformità agli obblighi previsti dal DPCM 24 ottobre 2014 e alla Convenzione stipulata con AgID.

4.1 RIEPILOGO DELLE VERIFICHE

Nel corso del 2022, sono stati attivati **12 procedimenti di verifica** (2 riuniti; 1 riunito in un procedimento avviato nel 2023), dei quali 9 a seguito di segnalazioni o richieste nell'ambito di indagini di polizia giudiziaria e 3 nell'ambito di verifiche programmate. Per i 12 procedimenti sono state svolte complessivamente svolte 14 verifiche ispettive, delle quali 11 in presenza, presso le sedi dei gestori, 3 da remoto (due procedimenti hanno previsto più verifiche).

Come si rileva dal grafico che segue, i 12 procedimenti hanno riguardato le tre tipologie di soggetti vigilati: i QTSP (3); i gestori SPID (8); i gestori PEC (1).

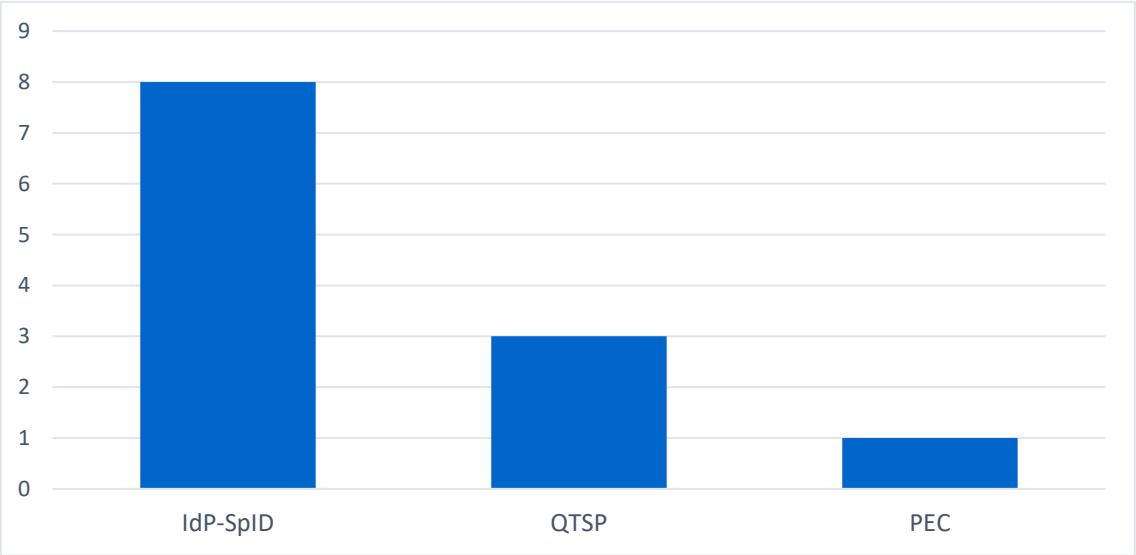

Fig. 6 - Procedimenti di verifica avviati nel 2022

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

Le verifiche 2022 hanno portato in 4 casi (2 riuniti) all'attivazione della fase sanzionatoria; è stata inoltre conclusa l'istruttoria per 3 procedimenti avviati nel 2021, di cui 2 riuniti in fase sanzionatoria. Per l'attività sanzionatoria si rimanda al § 8.

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 a una norma o a uno standard internazionale, le verifiche svolte da AgID ai fini della vigilanza si configurano come verifiche di "seconda parte", 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).

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

Il grafico che segue mostra che complessivamente sono stati formulati 68 rilievi, distinti in 35 "Non Conformità" e 33 "Osservazioni"; circa il 65% dei rilievi ha riguardato i gestori SPID, circa il 29% dei rilievi ha riguardato i QTSP, il restante 6% i gestori PEC.

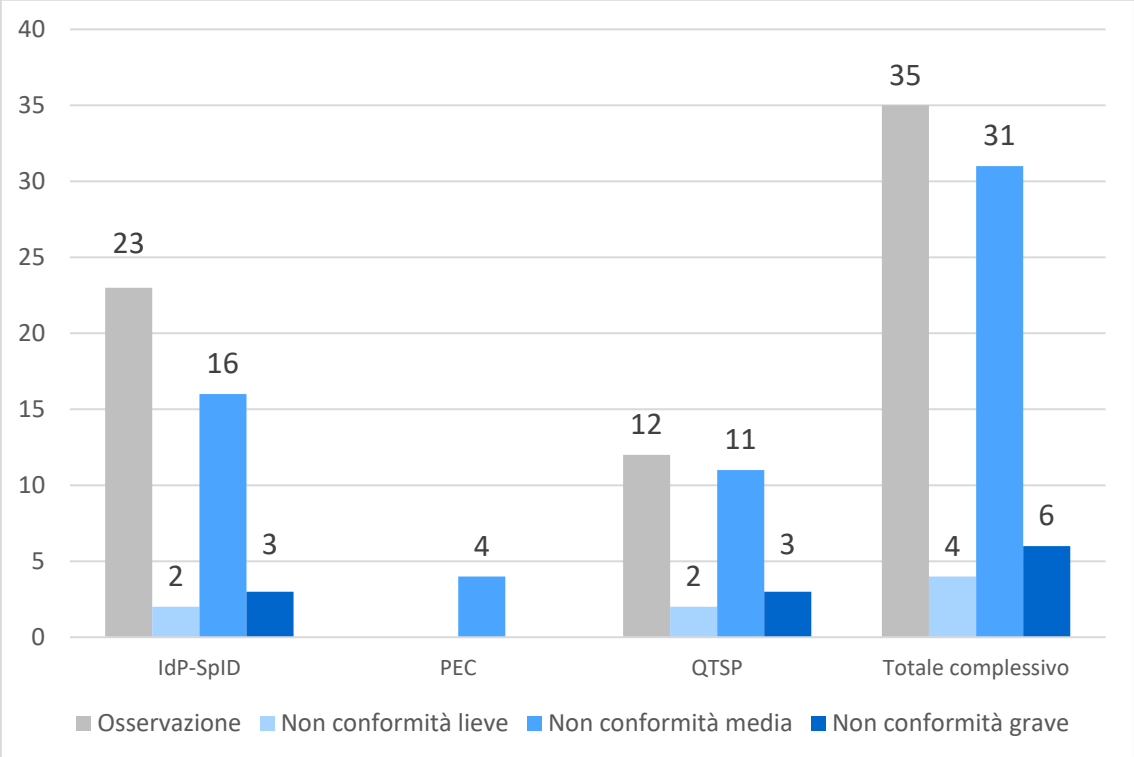

Fig. 7 - Totale dei rilievi e distribuzione per servizio per l'anno 2022

Tali dati si riferiscono alla totalità dei procedimenti sopra indicati.

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 2022 hanno portato in 4 casi (2 riuniti) all'attivazione della fase sanzionatoria.

Classificazione Rilievi	PEC	QTSP	SPID	Totale complessivo
Grave	-	-	3	3
Lieve	-	2	2	4
Media	4	8	16	28
OSSERVAZIONE	-	10	23	33
Totale complessivo	**4**	**20**	**44**	**68**

Tab. 1 – Classificazione dei rilievi per servizio

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

4.4 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[24] a cui fa riferimento il maggior numero di rilievi riguardano la Gestione del processo, la Gestione delle terze parti, 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** 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[25], 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. La terza parte può operare solo nell'ambito di un adeguato accordo contrattuale con il gestore, che in ogni caso è responsabile dell'erogazione

[24] Un rilievo può riguardare più componenti di servizio.

[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 servizi ("partner tecnici").

del servizio all'utente finale. I rilievi formulati per tale componente riguardano la mancanza di tempestivi controlli e, pur in presenza di piani di audit, l'incompleta o inefficace gestione dei risultati degli audit svolti sulle terze parti.

Più in generale, in riferimento alla **Gestione del processo**, i rilievi riguardano in gran parte procedure e strumenti in uso agli operatori incaricati all'identificazione dei richiedenti un'identità digitale o un certificato di firma digitale, non sempre in grado di rilevare e contrastare tempestivamente errori degli stessi operatori, comportamenti difformi dalle procedure definite dal gestore o tentativi di contraffazione di documenti in fase di richiesta del servizio.

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

5 SERVICE PROVIDER SPID

In riferimento al potenziamento delle funzioni di vigilanza esercitate da AgID ai sensi dell'art. 14-bis del CAD, nel 2022 sono state avviate verifiche sui fornitori di servizi SPID ("SP"). L'attività è stata condotta attraverso la somministrazione su piattaforma informatica (https://trustservices.agid.gov.it/) di una lista di controllo, con quesiti informativi formulati sulla base degli obblighi[26] a carico del soggetto che opera come fornitore di servizi SPID, previsti dal DPCM 24 ottobre 2014 e alla Convenzione stipulata con AgID.

La verifica è stata condotta per 18 Regioni nel ruolo di SP SPID. Le domande sono state formulate prevedendo risposte chiuse[27] in riferimento agli specifici; i risultati ottenuti sono riassunti in forma anonima e in modalità aggregata nel grafico che segue.

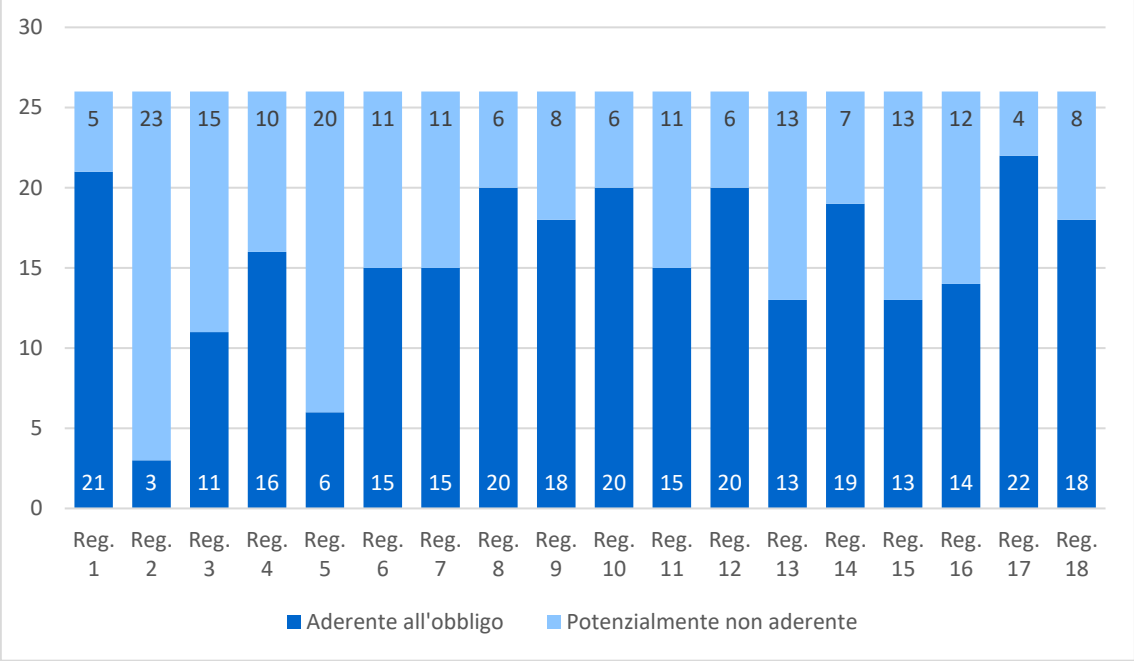

Fig. 8 - Esiti della rilevazione condotta su SP

Dal grafico si rileva che almeno in 3 casi (Regioni individuate dai codici 2, 3 e 5) ci sono situazioni con più del 50% di risposte negative, che si possono configurare come potenzialmente critiche e richiedono azioni da parte del SP.

[26] Tali obblighi, previsti agli artt. 13 e 14 del o DPCM 24 ottobre 2014 e all'art. 2 dello schema di Convenzione, riguardano, a titolo di esempio: la comunicazione ad AgID, l'aggiornamento continuo dell'elenco dei servizi qualificati erogati in rete e le informazioni tecniche richieste da AgID per consentire la fruizione degli stessi previa autenticazione SPID; la conservazione delle informazioni necessarie a imputare, alle singole identità digitali, le operazioni effettuate sui sistemi tramite SPID; le notifiche ad AgID in caso di rilevazione di usi anomali di identità digitali; ecc.

[27] Risposte possibili: "SI" in caso di piena conformità al requisito indirizzato dal quesito; "NO" in caso di parziale adempimento o potenziale non conformità

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 2022 sono stati notificati complessivamente **71 eventi relativi a incidenti, malfunzionamenti** o indisponibilità per attività di manutenzione relativi ai servizi PEC (12), SPID (34) e servizi fiduciari (25).

Dal 1° marzo 2022 le notifiche sono state inoltrate ad AgID e gestite attraverso il portale di vigilanza (piattaforma https://trustservices.agid.gov.it/).

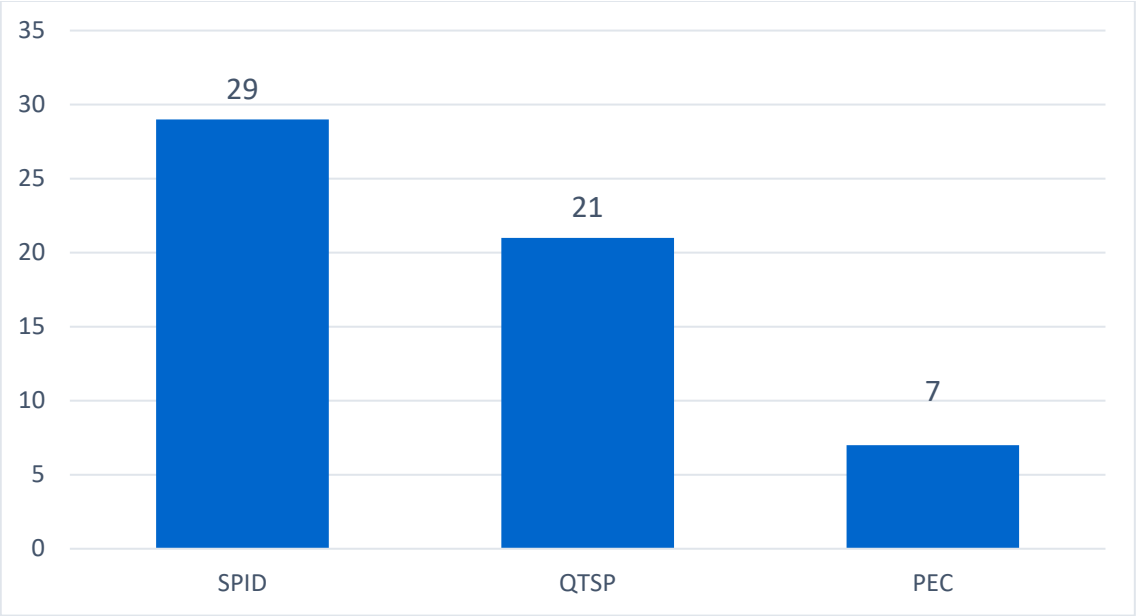

Fig. 9 - Notifiche 2022 per tipologia di servizio

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

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, 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.

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

Nel 2022 sono state gestite circa **95 segnalazioni**, di cui 70 richieste (relative a oltre 500 utenze) su presunte irregolarità o utilizzo dei servizi (principalmente SPID e firma digitale) a scopo asseritamente fraudolento e 25 segnalazioni utente. Tali segnalazioni hanno dato luogo a 9 dei 12 procedimenti di verifica avviati nel 2022.

8 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 principali 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 il gruppo di lavoro ECATS (*European Competent Authorities for Trust Services* – in precedenza *Article 19 Expert Group*) con rappresentanti degli Organismi di vigilanza europei previsti all'art. 17 del Regolamento eIDAS con il compito di favorire l'attuazione dell'art. 19 del Regolamento eIDAS coordinato da ENISA[28], 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[29] 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), 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 e-mail 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.

[28] 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.

[29] 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.

9 LE SANZIONI

Il CAD[30] definisce i casi per i quali possono essere irrogate sanzioni amministrative.

Nel 2022 **per 4 procedimenti** avviati a seguito di segnalazioni, **è stata attivata la fase sanzionatoria**, dei quali tre in ambito SPID (due riuniti) e uno in ambito servizi fiduciari qualificati. A dicembre 2022 le attività istruttorie risultavano ancora in corso.

Le irregolarità riscontrate hanno riguardato in linea di massima:

- l'utilizzo di personale addetto alle attività di identificazione dei richiedenti un'identità digitale o un certificato di firma non sempre adeguatamente formato ed aggiornato in riferimento alle tematiche specifiche del riconoscimento e alle procedure da seguire;
- l'adozione di sistemi e pratiche operative e gestionali non sempre in grado di bloccare errori degli operatori, comportamenti difformi dalle specifiche procedure, o di contrastare richieste di identità digitale o certificati di firma per utilizzi impropri del servizio;
- la mancanza di sistematici controlli sulle terze parti, in grado di rilevare e contrastare tempestivamente anomalie o comportamenti difformi dalle procedure previste.

Nel corso del 2022 **sono stati conclusi 3 procedimenti (riuniti) avviati nel 2021 ed attivi in fase sanzionatoria**, a seguito dell'avvenuto pagamento in misura ridotta di circa 400.000,00 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.

[30] Art. 32-bis

10 AZIONI SCATURITE DALLE VERIFICHE

Le verifiche svolte sui soggetti vigilati, sia attraverso le ispezioni sul campo che in via continuativa, su base documentale, consentono di disporre di elementi per individuare e pianificare interventi correttivi ed evolutivi, sia dal punto di vista delle specifiche modalità realizzative del servizio da parte del soggetto vigilato, sia per quanto riguarda gli aggiornamenti al quadro normativo da parte degli enti regolatori, sia con rifermento alle responsabilità degli utenti nell'utilizzo consapevole e secondo specifica dei servizi fruiti.

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**, anche per il tramite delle associazioni di categoria, che vedono attivamente coinvolte le diverse unità organizzative AgID.

A titolo di esempio si richiamano i risultati riportati nel report annuale del CERT-AgID, che evidenziano senza dubbi l'impatto positivo delle iniziative di contrasto, avviate negli anni precedenti, volte a ridurre gli effetti negativi delle campagne malware veicolate tramite account di Posta Elettronica Certificata. La **collaborazione continua e sinergica tra il CERT-AgID e i gestori PEC** ha rivestito un ruolo fondamentale nel limitare la diffusione di contenuti dannosi e nell'assicurare una maggior sicurezza degli utenti finali. In particolare, l'impiego della piattaforma MISP[31] per la **condivisione degli Indicatori di Compromissione (IoC) con i gestori PEC** ha agevolato le attività di contrasto alle minacce informatiche. Altrettanto efficacemente sono stati **respinti vari attacchi DDoS diretti ai gestori SPID** durante il periodo di tensione nel conflitto Russia-Ucraina, confermando così l'efficacia e la flessibilità delle misure di sicurezza adottate."

Numerosi interventi sono stati adottati inoltre dai soggetti vigilati nel corso del 2022 in relazione alle situazioni rilevate attraverso le segnalazioni utente e le richieste nell'ambito di indagini di polizia giudiziaria (cfr. § 6). Per quanto riguarda i prestatori di servizi fiduciari qualificati e i gestori SPID principalmente interessati dalle segnalazioni e dai procedimenti avviati nel 2022, sono stati richiesti interventi principalmente volti a sistematizzare e documentare le procedure e gli strumenti in uso agli operatori addetti all'identificazione dei richiedenti e i controlli da svolgere sul relativo operato ai fini dell'emissione di un'identità digitale o di una firma digitale, al fine di rilevare tempestivamente errori umani, anomalie nei processi di identificazione e registrazione dei dati dei richiedenti svolti direttamente o attraverso terze parti (Registration Authority ("RA")[32] e Registration Authority Operator ("RAO")[33]. Tali iniziative, in continuità con quanto già avviato negli anni precedenti,

[31] Malware Information Sharing Platform

[32] 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

[33] 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

sono volte a contrastare **fenomeni sempre più frequenti di furti di identità,** o di utilizzo dei servizi a scopo fraudolento, che anche nel 2022 si sono rivelati numerosi, seppur perpetrati con rinnovate modalità. I furti di identità continuano a registrarsi per operazioni specifiche (es. accesso ai bonus di iniziativa governativa[34]; 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[35] che ostacolino utilizzi impropri di tali servizi. Per quel che riguarda i gestori, è necessaria un'accurata gestione delle anagrafiche dei titolari[36] 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. In tale ottica, nel 2022 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 ulteriori funzioni per la raccolta e la gestione dei dati strutturati da parte dei soggetti vigilati.

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.

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

[35] 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;

[36] 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.

11 APPENDICE

11.1 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

SP - Service Providere. Fornitore di servizi cui accedere tramite autenticazione SPID.

SPID - Sistema Pubblico di Identità Digitale

11.2 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.