Manuale Operativo **PosteID**

Sistema Pubblico di Identità Digitale

REDATTO DA	Pagamenti, Mobile e Digital
VERIFICATO DA	Chief Operating Office, Mercato Privati, Posta, Comunicazione e Logistica, Corporate Affairs, Risorse Umane e Organizzazione
APPROVATO DA	Pagamenti, Mobile e Digital

INDICE

1 INTRODUZIONE AL DOCUMENTO 5

1.1 STORIA DELLE MODIFICHE 5

1.2 LISTA DI DISTRIBUZIONE 7

1.3 SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO 7

1.4 RIFERIMENTI NORMATIVI, STANDARD TECNICI E DEFINIZIONI 7

1.4.1 Riferimenti normativi 7

1.4.2 Standard tecnici 8

1.5 DEFINIZIONI 9

1.6 ACRONIMI E ABBREVIAZIONI 10

2 GENERALITÀ 13

2.1 IDENTIFICAZIONE DEL DOCUMENTO 13

2.2 DATI IDENTIFICATIVI DEL GESTORE 13

2.3 RESPONSABILITÀ DEL MANUALE OPERATIVO 14

2.3.1 Correlazione Manuale operativo Poste – Regolamento Accreditamento 14

2.3.2 Aggiornamento del Manuale Operativo e notifica ad AgID 15

2.3.3 Sito del servizio, pubblicazione e conformità del Manuale Operativo 15

3 PREMESSA 16

4 DESCRIZIONE DEL SERVIZIO SPID 17

4.1 CARATTERISTICHE GENERALI DEL SERVIZIO 17

4.2 DEFINIZIONE APPLICATIVA DELLE COMPONENTI DEL SERVIZIO POSTEID 19

4.2.1 Modello logico-applicativo del servizio PosteID 19

5 MODALITÀ DI RICHIESTA DEL SERVIZIO 22

5.1 REGISTRAZIONE IDENTITÀ POSTEID PER CLIENTI POSTE ITALIANE GIÀ IDENTIFICATI "A VISTA" E DOTATI DI STRUMENTI DI IDENTIFICAZIONE ONLINE RILASCIATI DA POSTE 23

5.2 REGISTRAZIONE IDENTITÀ POSTEID PER UTENTI CHE NON DISPONGONO DI STRUMENTI DI IDENTIFICAZIONE ONLINE RILASCIATI DA POSTE ITALIANE 24

5.2.1 Registrazione/Adesione per clienti con Firma Digitale o Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica 25

5.2.1.1 Registrazione/Adesione per clienti con Firma Digitale 25

5.2.1.2 Registrazione/Adesione per clienti con Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica 26

5.2.2 Registrazione/Adesione per clienti senza strumento di identificazione online 26

5.2.2.1 Identificazione presso gli uffici postali abilitati 27

5.2.2.2 Identificazione a domicilio mediante un portalettere 28

5.2.3 Registrazione/Adesione per titolari di strumenti di identificazione informatica preesistenti a SPID rilasciati da Enti Terzi autorizzati da AgID ad operare come GIP 29
5.3 REGISTRAZIONE AL SERVIZIO POSTEID EFFETTUATA DA UN SOGGETTO TUTORE O AMMINISTRATORE DI SOSTEGNO PER I NATI NEL 1998 E 1999 30
5.4 ANAGRAFICA UTENTE 31
5.5 RILASCIO CREDENZIALI 32
5.5.1 Conservazione delle evidenze 33
6 STRUMENTI DI AUTENTICAZIONE 34
6.1 TIPOLOGIA DI STRUMENTI DI AUTENTICAZIONE POSTEID 34
6.1.1 Strumenti di primo livello SPID 34
6.1.2 Strumenti di secondo livello SPID 34
6.1.2.1 Ulteriori strumenti di secondo livello SPID 35
6.2 UTILIZZO DEGLI STRUMENTI DI AUTENTICAZIONE POSTEID 35
6.3 AMBITI DI UTILIZZO DI POSTEID 38
6.4 MESSAGGI DI ANOMALIA 38
7 GESTIONE DEL CICLO DI VITA DELL'IDENTITÀ DIGITALE 41
7.1 SOSPENSIONE 41
7.1.1 Sospensione immediata tramite il servizio web 41
7.1.2 Sospensione immediata tramite il servizio Interactive Voice Response 41
7.2 REVOCA 42
7.2.1 Richiesta di revoca in seguito a sospensione immediata 42
7.2.1.1 Riattivazione delle credenziali sospese 44
7.2.2 Richiesta di revoca credenziali e recesso dal servizio PosteID 44
7.2.3 Revoca o sospensione dell'Identità Digitale su iniziativa del Gestore 45
7.3 BLOCCO TEMPORANEO DEL PROFILO 46
8 RAPPORTI CON GLI UTENTI 47
9 CONDIZIONI DI FORNITURA 48
10 OBBLIGHI E RESPONSABILITÀ 49
10.1 OBBLIGHI DEL GESTORE 49
10.2 OBBLIGHI DELL'UTENTE 52
10.3 RESPONSABILITÀ 53
11 ESCLUSIONI E LIMITAZIONI DI RESPONSABILITÀ 54
12 LIVELLI DI SERVIZIO 56
13 SICUREZZA DEL SERVIZIO POSTEID 58
13.1 CONSERVAZIONE EVIDENZE PER IL RILASCIO DELL'IDENTITÀ DIGITALE 58

13.2 TRACCIATURA DEGLI ACCESSI AL SERVIZIO DI AUTENTICAZIONE 59
13.3 REPERIMENTO E PRESENTAZIONE DELLE INFORMAZIONI DI LOG 60
13.4 MISURE ANTICONTRAFFAZIONE 61
13.4.1 Misure per il primo livello SPID con sistemi di autenticazione a 1 fattore 61
13.4.2 Misure per il secondo livello SPID con sistemi di autenticazione a 2 fattori 61
13.4.2.1 App PosteID 62
13.4.2.2 Codice di verifica SMS - OTP PosteID[1] 62
13.5 SISTEMA DI MONITORAGGIO 63
13.5.1 Presidi di Sicurezza 64
14 MODALITÀ DI PROTEZIONE DEI DATI DEI TITOLARI 65
14.1 AMBITO DEL TRATTAMENTO DEI DATI PERSONALI 65
14.1.1 Accesso ai dati 65
14.2 SICUREZZA DEI DATI 65

1 Introduzione al documento

1.1 Storia delle modifiche

Data	Versione	Descrizione modifiche	Codifica
14/09/2015	1.0	Prima versione	DTO_SPID_PI_004_v1.0
30/11/2015	1.1	- Aggiornamento lista acronimi e abbreviazioni - Inserimento premesse - Inserimento CIE come strumento di identificazione (§ 5; 13.1) - Dettagliato processo di certificazione del cellulare e della e-mail (§ 4.2.1; 5) - Aggiornato dettaglio messaggi di anomalia (§ 6.4) - Inserita premessa ad Obblighi e Responsabilità (§ 10) - Aggiornati livelli di servizio (§ 12) - Aggiornate evidenze conservate nell'identificazione a vista (§ 13.1) - Integrato monitoraggio sull'utilizzo delle credenziali (§ 13.5)	DTO_SPID_PI_004_v1.1
09/12/2015	1.2	- Aggiornato descrizione Strumenti di autenticazione (§ 6) - Aggiornato Obblighi e responsabilità (§ 10)	DTO_SPID_PI_004_v1.2
15/12/2015	1.3	- Eliminazione riferimenti identità pregresse (§ vari)	DTO_SPID_PI_004_v1.3
19/02/2016	1.4	- Reintroduzione riferimenti identità pregresse (§ vari) - Aggiornamento durata contratto (§ 9) - Aggiornamento livelli di sicurezza (§ vari) - Aggiornamento sezione dati anagrafici (§ 2.3)	DTO_SPID_PI_004_v1.4
29/02/2016	1.5	- Inseriti maggiori dettagli sul processo di autenticazione con il livello 2 SPID (§ vari)	DTO_SPID_PI_004_v1.5
28/04/2016	1.6	- Inseriti ulteriori dettagli sul processo di pre-registrazione online (§ vari)	DTO_SPID_PI_004_V1.6
06/06/2016	1.7	- Inseriti dettagli sul processo di autorizzazione mediante fingerprint con l'app PosteID (§ vari)	DTO_SPID_PI_004_V1.7

06/06/2016	1.7.1	- Modifiche alla procedura di identificazione mediante firma digitale	DTO_SPID_PI_004_V1.7.1
06/06/2016	1.8	- Inseriti dettagli sull'identificazione a domicilio mediante portalettere (§ vari)	DTO_SPID_PI_004_V1.8
08/06/2016	1.8.1	- Modifiche alla procedura di identificazione mediante firma digitale	DTO_SPID_PI_004_V1.8.1
20/10/2016	1.8.2	- Aggiornato il processo di richiesta dell'identità digitale per utenti non dotati di strumenti di identificazione online (attivazione dopo l'identificazione "de visu") (§ vari) - Inseriti i dettagli sulla sospensione dell'identità digitale alla scadenza del documento di riconoscimento dell'utente (§ vari)	DTO_SPID_PI_004_V1.8.2
25/11/2016	1.8.3	- Semplificazione scenari di registrazione a PosteID, in ambiente web e su mobile (§5.1, §5.2.1) - Funzionalità di modifica dei dati di pre-registrazione per i clienti che richiedono l'identificazione in Ufficio Postale (§5.2.2.1)	DTO_SPID_PI_004_V1.8.3
20/12/2016	1.8.4	- Aggiornato il processo di richiesta dell'identità digitale (§5)	DTO_SPID_PI_004_V1.8.4
31/01/2017	1.8.5	- Dettagliato il processo di richiesta dell'identità digitale ad opera di un tutore/amministratore di sostegno che opera in nome e per conto del soggetto tutelato nato tra il 1998 ed il 1999 (§vari)	DTO_SPID_PI_004_v1.8.5
07/03/2017	1.8.6	- Inserito riferimento al trattamento dei dati sensibili nello scenario di richiesta dell'identità digitale ad opera di un tutore/amministratore di sostegno (§5.3)	DTO_SPID_PI_004_v1.8.6
02/05/2017	1.8.7	- Descrizione nuova modalità di autenticazione di livello 2 SPID da App PosteID tramite QR code (§6.2)	DTO_SPID_PI_004_v1.8.7
31/07/2017	1.8.8	- Aggiornamento strutture organizzative di riferimento e correzione refusi	DTO_SPID_PI_004_v1.8.8
31/10/2017	1.8.9	- Introduzione supporto all'impronta facciale (Face ID)	DTO_SPID_PI_004_v1.8.9
13/11/2017	1.9	- Aggiornamento §6.2 e §13.4.2 relativamente alle notifiche di "tentato accesso" in fase di primo utilizzo degli strumenti di Livello 2 SPID	DTO_SPID_PI_004_v1.9
26/03/2018	2.0	- Descrizione modalità di registrazione tramite identità pre-esistenti di Enti Terzi	DTO_SPID_PI_004_v2.0

		autorizzati da AgID - Aggiornamento sugli strumenti di autenticazione di Livello 2 SPID resi disponibili ai clienti del Servizio	
18/05/2018	2.1	- Introduzione riferimenti al Regolamento 2016/679/UE (GDPR) - Aggiornamento pagina posteid.poste.it	DTO_SPID_PI_004_v2.1

1.2 Lista di distribuzione

Lista di distribuzione
Agenzia per l'Italia Digitale
Documento pubblico disponibile sul portale del servizio di Poste Italiane https://posteid.poste.it

1.3 Scopo e campo di applicazione del documento

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate da Poste Italiane nella conduzione del servizio di Identità Digitale aderente al Sistema Pubblico per la gestione dell'Identità Digitale.

Il contenuto del presente Manuale è conforme al DPCM 24 ottobre 2014 ed alla regolamentazione emanata da AgID in attuazione dell'articolo 4 del citato DPCM.

Il presente manuale rappresenta una integrazione di dettaglio alla informativa fornita ai titolari del servizio ai sensi del Regolamento 2016/679/UE (Regolamento europeo in materia di protezione dei dati personali).

1.4 Riferimenti normativi, standard tecnici e definizioni

1.4.1 Riferimenti normativi

DLgs 82/2005	Decreto Legislativo 7 marzo 2005, n° 82 -Codice dell'amministrazione digitale.
DPCM 24/10/2014	Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese

Regolamento AgID per l'Accreditamento	Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di gestione dei servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete di cui all'articolo 64, comma 2-ter, del decreto legislativo 7 marzo 2005, n. 82.
Regolamento AgID per l'utilizzo sistemi di identificazione informatica preesistenti	Procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM 24 ottobre 2014.
Modalità attuative SPID	Sistema Pubblico per la Gestione dell'identità Digitale – Modalità Attuative
Regole Tecniche SPID	SPID – REGOLE TECNICHE

Riferimenti normativi, Regolamenti e Regole tecniche

1.4.2 Standard tecnici

ISO-IEC 18014	Time-stamping
ISO-IEC 19790:2012	Security requirements for cryptographic modules
ISO-IEC 24760-1	A framework for identity management -- Part 1: Terminology and concept
ISO-IEC 27001	Information security management
ISO-IEC 29003	Identity proofing
ISO-IEC 29100	Basic privacy requirements
ISO-IEC 29115:2013	Entity authentication assurance framework
ITU-T X.1254	Entity Authentication Framework
ITU-T Recommendation X.1252 (2010)	Baseline identity management terms and definitions
FIPS PUB 140-2	Security requirements for cryptographic modules

Standard tecnici

1.5 Definizioni

Gestore dell'Identità Digitale	La persona giuridica accreditata allo SPID che, in qualità di gestore di servizio pubblico, previa identificazione certa dell'utente, assegna, rende disponibili e gestisce gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Il Gestore fornisce i servizi necessari a gestire l'attribuzione dell'identità digitale agli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti. Nel presente documento il termine è utilizzato per identificare Poste Italiane nell'esecuzione delle attività di Gestore dell'identità digitale.
Gestore degli attributi qualificati	Soggetto accreditato ai sensi dell'art. 16 del DPCM 24 ottobre 2014 che ha il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
Fornitore di servizi	Il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita.
AgID	Agenzia per l'Italia Digitale che gestisce l'accreditamento e la vigilanza per il Sistema Pubblico di Identità Digitale.
Utente	Persona fisica, titolare di una identità digitale SPID, che utilizza i servizi erogati in rete, da un Fornitore di servizi, previa identificazione informatica. L'utente con riferimento all'acquisizione di servizi di Poste Italiane, nel presente Manuale, è anche richiamato come Cliente.
Gestore di Identità Pregresse	Ente Terzo, pubblico o privato, che ha richiesto il riconoscimento delle identità pregresse ed è stato autorizzato da AgID sulla base delle modalità attuative pubblicate dall'Agenzia ed in coerenza con quanto previsto dal *Regolamento recante le procedure per consentire ai Gestori dell'Identità Digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM 24 ottobre 2014.*

Attori del Sistema Pubblico per l'Identità Digitale

Attributo	Informazione o qualità di un utente utilizzata per rappresentare la sua identità, il suo stato, la sua forma giuridica o altra caratteristica peculiari.
Attributi identificativi	Nome, cognome, luogo e data di nascita, sesso, nonché il codice fiscale e gli estremi del documento d'identità utilizzato ai fini dell'identificazione.
Attributi secondari	Il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni.
Autenticazione informatica	Verifica effettuata dal gestore dell'identità digitale, su richiesta del Fornitore di servizi, della validità delle credenziali di accesso dell'utente, al fine di convalidarne l'identificazione informatica.
Codice identificativo	Il particolare attributo assegnato dal gestore dell'identità digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID.

Credenziali di accesso	Attributi di cui l'utente si avvale, per accedere in modo sicuro, tramite autenticazione informatica, ai servizi erogati in rete dai Fornitori di servizi che aderiscono allo SPID.
Identificazione informatica	Validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.
Identità digitale	Rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità previste dalla normativa vigente.
Impronta Digitale (fingerprint)	Sistema di riconoscimento biometrico che, tramite strumenti informatici, ha la funzionalità e lo scopo di identificare una persona sulla base di una o più caratteristiche biologiche e/o comportamentali (biometria), confrontandole con i dati, precedentemente acquisiti e presenti nel database del sistema, tramite degli algoritmi e di sensori di acquisizione dei dati in input. L'impronta digitale utilizza tracce lasciate dai dermatoglifi.
Impronta Facciale (Face ID)	Sistema di riconoscimento biometrico che, tramite strumenti informatici, ha la funzionalità e lo scopo di identificare una persona sulla base di una o più caratteristiche biologiche e/o comportamentali (biometria), confrontandole con i dati, precedentemente acquisiti e presenti nel database del sistema, tramite degli algoritmi e di sensori di acquisizione dei dati in input. L'impronta facciale utilizza la fisionomia del volto.
Revoca dell'identità digitale	Disattivazione definitiva dell'identità digitale.
Registrazione	Insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione previsti dal DPCM 24 ottobre 2014 e dai suoi regolamenti attuativi, è attribuita un'identità digitale a un utente, previa raccolta, verifica e certificazione degli attributi da parte del gestore dell'identità digitale, garantendo l'assegnazione e la consegna delle credenziali di accesso prescelte in modalità sicura.
Sospensione dell'identità digitale	Disattivazione temporanea dell'identità digitale.
SPID	Sistema Pubblico di Identità Digitale, istituito ai sensi dell'art. 64 del Codice dell'Amministrazione Digitale, per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese.

Termini ricorrenti

1.6 Acronimi e abbreviazioni

Nome Utente	AccountID utilizzato dall'utente per l'identificazione univoca all'interno del dominio del Gestore dell'Identità Digitale.
Android	Sistema operativo per dispositivi mobili quali smartphone e tablet, sviluppato dalla società Google
App	Applicazione software per smartphone.
Captcha	Codice per domanda e risposta, allo scopo di determinare se l'utente è una persona oppure una applicazione

CC.I.AA.	Camere di commercio, industria, artigianato e agricoltura
CGS	Condizioni Generali del Servizio.
CIE	Carta di Identità Elettronica
CNS	Carta Nazionale dei Servizi.
D.Lgs.	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri. Se non ulteriormente specificato, all'interno del presente Manuale Operativo ci si riferisce al DPCM 24 ottobre 2014 "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese."
HSM	Hardware Security Module – Dispositivo Sicuro per la conservazione e l'uso delle chiavi crittografiche associate ai certificati elettronici
IdP	Identity Provider – Gestore dell'Identità Digitale come indicato nelle definizioni.
iOS	Sistema operativo sviluppato dalla società Apple per smartphone e tablet della stessa società.
ISO/IEC DIS 29115	Standard individuato dal DPCM 24 ottobre 2014 per la definizione dei liveli di sicurezza degli strumenti di autenticazione informatica
IVR	Interactive Voice Response (IVR): sistema capace di recitare informazioni ad un chiamante che interagisce tramite tastiera telefonica.
MISE	Ministero dello Sviluppo Economico
NIST	National Institute of Standards and Technology - Agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie
OTP	One Time Password – Codice a bruciatura, utilizzabile una sola volta ed in un determinato periodo temporale.
PCR	Personal Card Reader (lettore BancoPosta) in dotazione agli utenti BancoPosta OnLine e BancoPosta Click per l'autenticazione ai servizi online e l'autorizzazione delle transazioni tramite la carta Postamat.
PEC	Posta Elettronica Certificata
Penetration test	Processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato.
PIN	Personal Identification Number - Numero di Identificazione Personale, sequenza di caratteri usata per verificare che la persona che utilizza un dispositivo sia effettivamente autorizzata a compiere quella operazione in quanto proprietaria del dispositivo stesso.
PP.AA.	Pubbliche Amministrazioni.

RPO	Recovery Point Objective - Rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza. Di conseguenza fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.
RTO	Recovery Time Objective - Tempo necessario per il pieno recupero dell'operatività di un sistema, a seguito della sua indisponibilità a causa di guasto improvviso.
TS-CNS	Tessera Sanitaria-Carta Nazionale dei Servizi.
SAML	Security Assertion Markup Language - Protocollo per lo scambio di autenticazione e autorizzazione dei dati attraverso il quale colloquiano il Gestore dell'Identità, il Fornitore di Servizi o il Gestore degli attributi qualificati.
SMS	Short Message Service - Breve messaggio di testo inviato da un telefono cellulare o da un sistema ad un altro.
SP	Service Provider - Il Fornitore di servizi, come indicato nelle definizioni.
S.m.i.	Successive modifiche ed integrazioni. Viene aggiunto ad un riferimento normativo per contemplarne i cambiamenti e le evoluzioni susseguitesi nel corso del tempo.
WiFi	La tecnologia ed i relativi dispositivi che consentono a terminali di collegarsi tra loro attraverso una rete locale in modalità wireless, senza fili.
GIP	Gestore di Identità Pregresse

Acronimi e abbreviazioni

2 Generalità

2.1 Identificazione del documento

Questo documento è denominato “Manuale Operativo”, ed è identificato attraverso il numero di versione presente in calce ad ogni pagina e il nome “Manuale Operativo PosteID – Sistema Pubblico di Identità Digitale” e consultabile, per via telematica, sul sito del Gestore Poste Italiane S.p.A. all’indirizzo *https://posteid.poste.it.*

2.2 Dati identificativi del Gestore

Poste Italiane S.p.A. è il Gestore aderente a SPID che opera in conformità alle Regole Tecniche ed ai Regolamenti AgID, in aderenza a quanto prescritto dal Codice dell’Amministrazione Digitale di cui al D.Lgs 82/2005 e s.m.i. e dal DPCM 24 ottobre 2014.

In questo documento si usa il termine Gestore per indicare Poste Italiane nel ruolo di Gestore dell’Identità Digitale.

Denominazione e Ragione Sociale	POSTE ITALIANE S.p.A.
Rappresentante Legale	Matteo Del Fante
Sede Legale	Viale Europa, 190 - 00144 ROMA
Telefono	0039 06 59581
Sede Operativa	Viale Europa, 175 - 00144 ROMA
Telefono	0039 06 59581
Indirizzo Internet del Gestore	http://www.poste.it
Indirizzo Internet del servizio SPID	https://posteid.poste.it

Dati identificativi del Gestore

2.3 Responsabilità del Manuale Operativo

Poste Italiane è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.

Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo e alla persona di seguito indicata.

RESPONSABILE DEL MANUALE OPERATIVO	
NOME	Roberto
COGNOME	Palumbo
TELEFONO	06 59581
EMAIL	responsabilemanualeposteid@posteitaliane.it

Dati identificativi del Responsabile del Manuale Operativo

2.3.1 Correlazione Manuale operativo Poste – Regolamento Accreditamento

Contenuto Regolamento accreditamento	Riferimento manuale operativo
Dati identificativi del gestore	§ 2.2
Dati identificativi della versione del manuale	§ 2.1
Responsabile del Manuale Operativo	§ 2.3
Descrizione delle architetture, applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche	§ 4
Descrizione delle architetture dei sistemi di autenticazione e delle credenziali	§4; § 6
Descrizione dei codici e dei formati dei messaggi di anomalia sia relativi ai protocolli che ai dispositivi di autenticazione utilizzati	§ 6.4
Livelli di servizio garantiti per le diverse fasi della registrazione e della gestione del ciclo di vita delle identità	§ 12
Livelli di servizio garantiti per le diverse fasi del processo di autenticazione	§ 12
Descrizione dei contenuti delle tracciature degli accessi al servizio di autenticazione e delle modalità di acquisizione ai fini dell'opponibilità a terzi	§ 13.2
Guida utente del servizio	Allegato "Guida Utente PosteID"
Descrizione dei processi e delle procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali	§ 5
Descrizione dei metodi di gestione dei rapporti con gli utenti	§ 8
Descrizione generale delle misure anti-contraffazione	§ 13.4

Contenuto Regolamento accreditamento	Riferimento manuale operativo
Descrizione generale del sistema di monitoraggio	§ 13.5
Definizione degli obblighi del Gestore e dei titolari dell'identità digitale	§ 10
Indirizzo (o indirizzi) del sito web del gestore ove è resa direttamente disponibile la descrizione del servizio in lingua italiana e lingua inglese	§ 2.3.3
Descrizione delle modalità disponibili agli utenti per richiedere la revoca e sospensione dell'identità digitale	§ 7

Tabella – Contenuto del Manuale Operativo e riferimenti al Regolamento per l'accreditamento

2.3.2 Aggiornamento del Manuale Operativo e notifica ad AgID

Il Gestore si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche organizzative alle procedure derivanti da norme di legge, regolamenti e miglioramenti dei processi di rilascio, utilizzo e gestione delle identità digitali.

Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni.

Ogni variazione al presente Manuale Operativo sarà sottoposta ad AgID per la preventiva approvazione e sarà pubblicata e resa operativa solo a seguito di tale approvazione.

2.3.3 Sito del servizio, pubblicazione e conformità del Manuale Operativo

Questo documento è pubblicato in formato elettronico presso il sito web del Gestore all'indirizzo:

https://posteid.poste.it

I contenuti del presente Manuale Operativo sono pienamente rispondenti alla normativa relativa all'Identità Digitale, con particolare riferimento al DPCM 24 ottobre 2014 ed ai Regolamenti attuativi emanati dall'AgID in attuazione dell'articolo 4 del DPCM.

All'indirizzo https://posteid.poste.it è disponibile la descrizione del servizio.

3 Premessa

PosteID è l'Identità Digitale che Poste Italiane mette a disposizione dei Cittadini per consentire:

- l'accesso ai servizi in rete della Pubblica Amministrazione e dei soggetti privati aderenti al Servizio Pubblico per la gestione dell'identità digitale SPID;
- l'accesso ai servizi che Poste Italiane offre privatamente ai suoi clienti.

4 Descrizione del servizio SPID

4.1 Caratteristiche generali del servizio

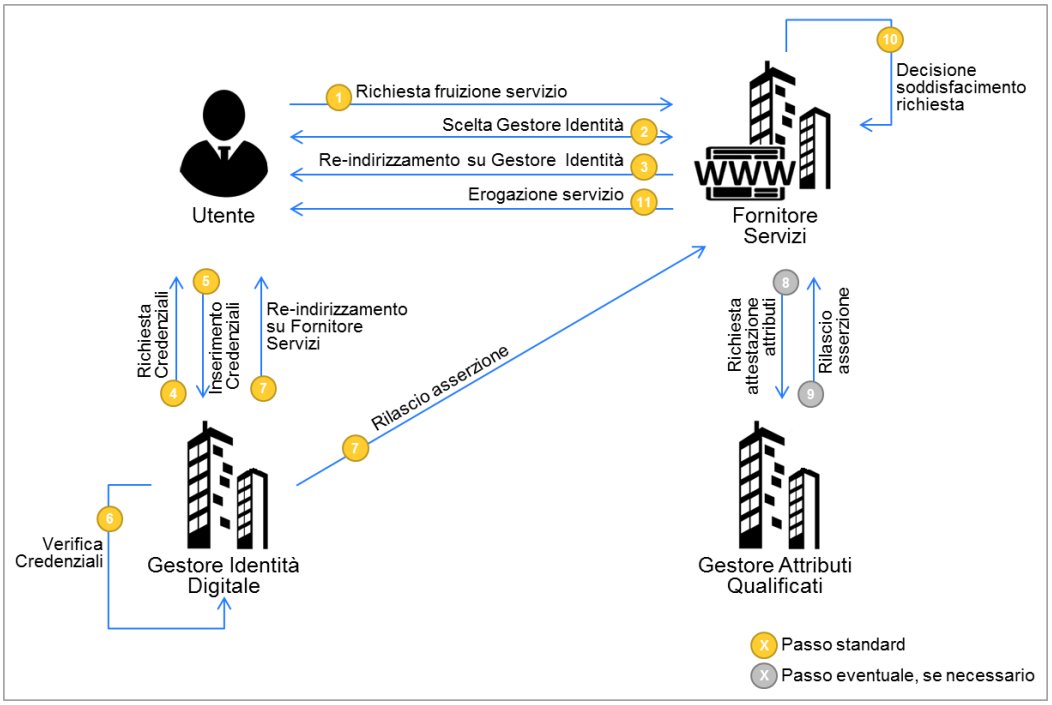
Il Sistema Pubblico di Identità Digitale (SPID) è definito dall'articolo 64 del Codice per l'Amministrazione Digitale per l'accesso ai dati ed ai servizi online erogati dalle Pubbliche Amministrazioni e dai Fornitori di servizi privati.

Al Sistema partecipano i seguenti attori:

- Gestori dell'Identità Digitale;
- Gestori di Attributi Qualificati (ad es: Ordini e collegi professionali, CC.I.AA., MISE, ecc.);
- Fornitori di Servizi (ad es: PP.AA., Gestori di Pubblici Servizi, Imprese, …);
- Agenzia per l'Italia Digitale;
- Utenti.

Il Sistema mette in relazione i suddetti attori per le attività necessarie alla richiesta e fruizione di un servizio online, erogato da un Fornitore di servizi a seguito della richiesta da parte di un utente ed, eventualmente, anche a seguito dell'accertamento di ruoli e qualifiche presso i Gestori degli attributi qualificati.

Il quadro delle interazioni è schematizzato nella figura che segue.



Interazioni tra gli Attori del sistema Pubblico per l'Identità Digitale

1 **Richiesta fruizione servizio**: l'utente, sul sito del Fornitore di Servizi, chiede accesso a funzionalità per le quali è necessaria l'autenticazione informatica del richiedente.

2 **Scelta Gestore Identità**: l'utente, sul sito del Fornitore di servizi, seleziona il proprio Gestore

dell'identità.

3 **Re-indirizzamento su Gestore Identità**: l'utente viene re-diretto sul sito del Gestore dell'identità con la richiesta di autenticazione, il livello di sicurezza SPID necessario ed il set di dati richiesti.

4 **Richiesta credenziali**: il Gestore dell'identità richiede all'utente l'inserimento delle proprie credenziali SPID in aderenza al livello di sicurezza necessario.

5 **Inserimento credenziali**: l'utente inserisce le proprie credenziali in funzione della richiesta del Gestore dell'identità.

6 **Verifica credenziali**: il Gestore dell'identità verifica la correttezza delle credenziali inserite dall'utente.

7 **Re-indirizzamento su Fornitore di servizi e rilascio asserzione per il Fornitore di servizi**: il Gestore dell'identità restituisce al Fornitore di servizi l'esito del processo di autenticazione ed i dati richiesti.

8 **Eventuale richiesta attestazione specifici attributi qualificati**: è un processo opzionale che non coinvolge il Gestore dell'identità. Mira, nei casi previsti, alla raccolta di attributi qualificati dell'utente eventualmente necessari ai fini della fruizione di specifici servizi, presso i soggetti che li detengono.

9 **Eventuale rilascio attestazione specifici attributi qualificati**: nei casi previsti, il Gestore di attributi qualificati restituisce gli attributi richiesti (ad esempio possesso di qualifiche, iscrizioni ad ordini professionali, ecc.).

10 **Autorizzazione all'accesso ai servizi**: Il Fornitore di servizi ha a disposizione l'evidenza del processo di autenticazione e gli eventuali attributi qualificati necessari per l'accesso ai servizi e, in caso di esito positivo, ne autorizza la fruizione.

Le credenziali SPID, utilizzate dall'utente, devono essere coerenti con il livello di sicurezza richiesto dal Fornitore dei Servizi affinché l'utente possa usufruire del particolare servizio scelto.

Esistono, infatti, tre differenti livelli di sicurezza delle credenziali SPID che possono essere richiesti dal Fornitore dei Servizi, in funzione del servizio/dati ai quali si richiede l'accesso.

- **Primo livello**: (corrispondente al Level of Assurance 2 dello standard ISO/IEC DIS 29115) prevede un sistema di autenticazione informatica ad un solo fattore, come ad esempio la password; in genere viene utilizzato nei casi in cui il rischio derivi da un utilizzo indebito dell'identità digitale, con un basso impatto per le attività del cittadino/impresa/amministrazione.
- **Secondo livello**: (corrispondente al Level of Assurance 3 dello standard ISO/IEC DIS 29115) prevede un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi che possono subire un danno consistente da un utilizzo indebito dell' identità digitale.

- **Terzo livello**: (corrispondente al Level of Assurance 4 dello standard ISO/IEC DIS 29115) prevede un sistema di autenticazione informatica basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi sicuri che soddisfano i requisiti dell' Allegato 3 della Direttiva 1999/93/CE; questo è il livello di garanzia più elevato, solitamente associato a quei servizi che possono subire un serio e grave danno per cause imputabili ad abusi di identità.

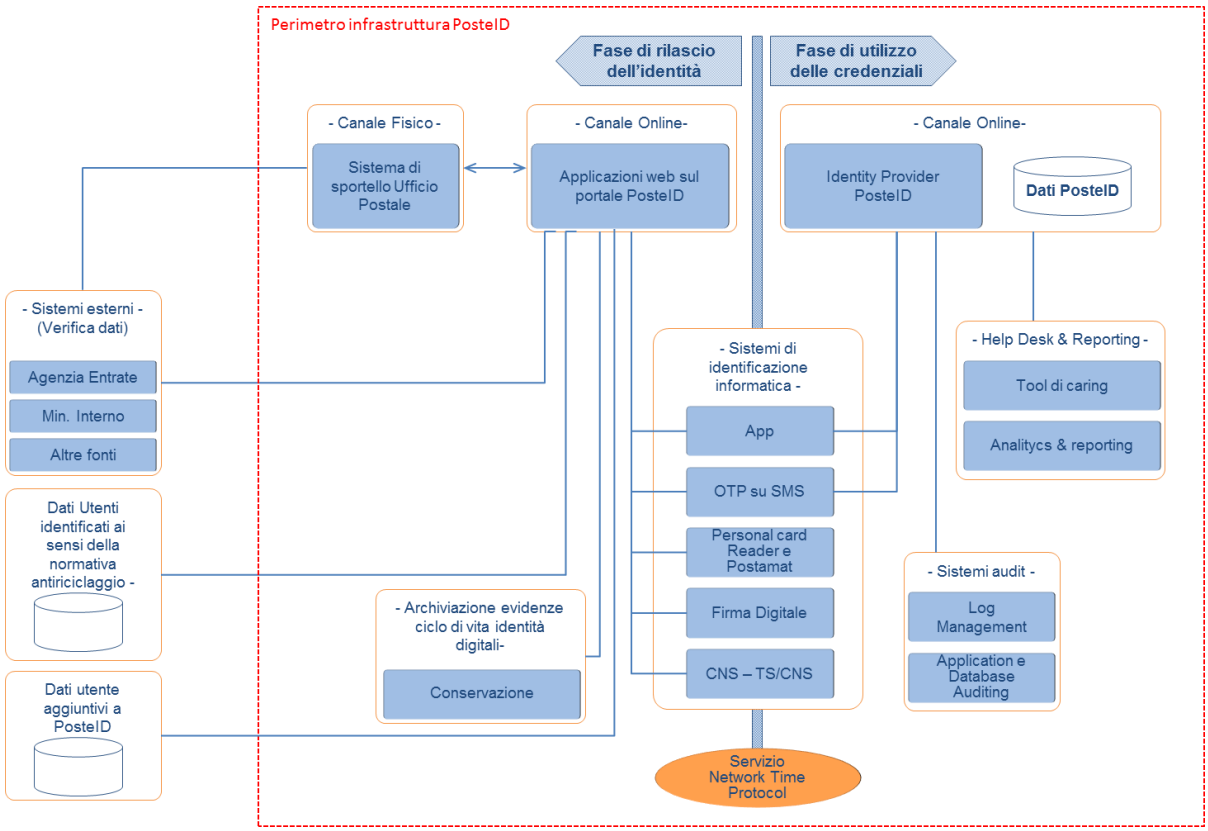
I Fornitori di servizi pubblici/privati attribuiscono i livelli di sicurezza necessari per l'accesso ai propri servizi.

4.2 Definizione applicativa delle componenti del servizio PosteID

PosteID, nella nuova versione resa disponibile dopo l'accreditamento presso AgID, è la soluzione di Poste Italiane per il rilascio delle identità digitali previste dal Sistema Pubblico per l'Identità Digitale (SPID).

4.2.1 Modello logico-applicativo del servizio PosteID

Di seguito viene riportato lo schema logico-applicativo del servizio PosteID con evidenziazione delle fase di emissione dell'Identità Digitale e rilascio delle credenziali e della fase di utilizzo delle credenziali per l'accesso ai servizi.



Modello logico-applicativo del servizio PosteID

Di seguito viene riportata una sintetica descrizione dei sottosistemi che compongono l'infrastruttura.

- **Canale online per la richiesta del servizio** - Il portale web per il rilascio dell'identità digitale PosteID e per la gestione delle relative credenziali. Il portale permette di gestire sia la fase di rilascio che di gestione del ciclo di vita dell'identità digitale. In particolare sono disponibili le funzioni di richiesta dell'identità digitale ed accettazione delle Condizioni Generali del Servizio, modifica degli attributi e di gestione delle credenziali.
- **Canale fisico** – portalettere a domicilio oppure Ufficio Postale utilizzati per l'identificazione e certificazione del telefono cellulare degli utenti che non dispongono di strumenti di identificazione online.
- **Sistemi esterni contenenti basi dati utenti già identificati ai sensi della normativa antiriciclaggio** – rappresenta le basi dati degli utenti precedentemente identificati con certezza da Poste Italiane, nel rispetto della normativa antiriciclaggio.
- **Sistemi esterni per la verifica dati** – Si tratta dei sistemi che permettono la verifica o l'acquisizione dei dati identificativi del richiedente e che sono interrogati al fine di validarne la correttezza e completezza.
- **Sistemi di identificazione informatica** – Rappresentano i sistemi per l'identificazione informatica per il rilascio dell'Identità Digitale o, per gli strumenti descritti al paragrafo 6.1 "Tipologia di strumenti di autenticazione PosteID", i sistemi richiamati nella fase di autenticazione per l'accesso ai servizi erogati online dai Fornitori di servizi.
- **Sistemi di conservazione delle evidenze del rilascio dell'identità digitale ed della gestione del ciclo di vita** – Sistemi per la conservazione delle evidenze connesse al rilascio dell'identità, all'accettazione delle Condizioni Generali del Servizio ed alla gestione del ciclo di vita dell'identità digitale; tali sistemi permettono la conservazione e l'esibizione delle evidenze, per 20 anni dalla data di scadenza o revoca dell'identità stessa.
- **Sistema di gestione delle richieste di autenticazione** - Modulo IDP (Identity Provider) che permette di porre in relazione i sistemi di identità con i Fornitori di servizi, attraverso la generazione di asserzioni SAML 2.0. Viene interrogato al momento della richiesta di autenticazione sul portale del Fornitore di servizi da parte dell'utente.
- **Sistema di supporto all'help desk ed alle attività di reporting** – Tool a supporto dell'assistenza clienti, finalizzati a mettere l'operatore in condizione di gestire direttamente ed in fase di prima interazione il maggior numero possibile di richieste di assistenza relative al servizio PosteID.
- **Sistemi di Audit** – Strumenti a supporto della gestione dei log delle transazioni ed al monitoraggio delle applicazioni e dei sistemi che gestiscono i dati.
- **Basi dati aggiuntive a PosteID** – Poste Italiane richiede, previa acquisizione del consenso da parte del cliente ed al fine di migliorare l'esperienza d'uso dei servizi, dati aggiuntivi (quali indirizzo di residenza e indirizzo di recapito) che il cliente fornisce su base volontaria. Tali dati

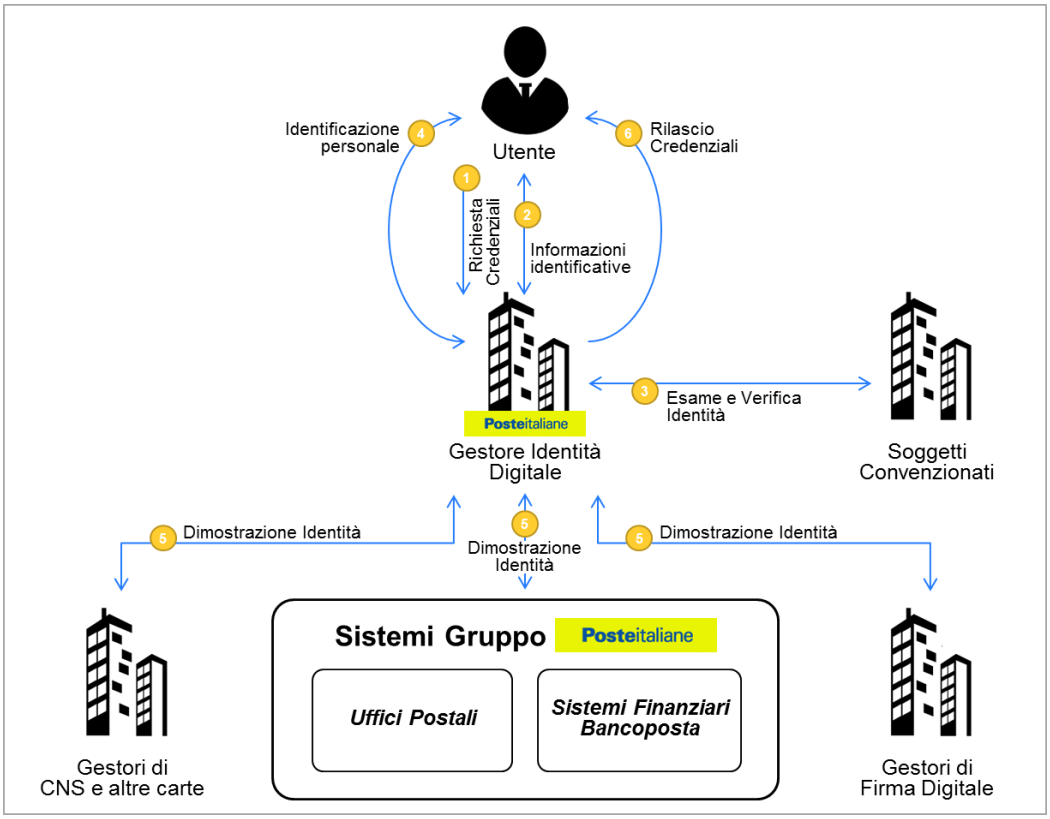
sono memorizzati su basi dati distinte da quelle dedicate al servizio PosteID**.**

- **Servizio Network Time Protocol** – Modulo servizio che garantisce la distribuzione ai sistemi di un riferimento temporale affidabile.

Nella fase di rilascio dell'Identità Digitale, le componenti applicative del Servizio procedono alla certificazione della disponibilità del numero di telefono cellulare e della email da parte del richiedente, attraverso l'invio di un codice di verifica SMS - OTP che viene inserito dall'utente nelle maschere di conferma.

5 Modalità di richiesta del servizio

In questa sezione è descritto il processo di richiesta e creazione dell'Identità Digitale PosteID.



Schema dei flussi di attivazione dell'Identità Digitale PosteID

Le modalità di verifica dell'identità per il rilascio delle credenziali PosteID sono le seguenti:

- identificazione informatica e registrazione identità PosteID:
  - identificazione informatica per clienti che hanno già una identità digitale PosteID attiva con strumenti di secondo livello di tipo SMS su cellulare certificato o APP (clienti che hanno eseguito il processo di attivazione delle funzionalità "Sicurezza web Postepay" o i servizi dispositivi Risparmio Postale Online);
  - strumenti di identificazione informatica preesistenti rilasciati da BancoPosta (clienti con lettore Bancoposta e carta Postamat);
  - strumenti di identificazione informatica preesistenti rilasciati da Enti Terzi autorizzati da AgID ad operare come Gestori di Identità Pregresse (GIP);
  - Firma Digitale, Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica;
- richiesta di PosteID on line ed identificazione "a vista" con associazione del cellulare presso lo sportello di Poste oppure a domicilio mediante portalettere. A completamento

dell'identificazione, i possessori di smartphone/tablet scaricano l'app PosteID che supporta la generazione delle credenziali mentre ai possessori di cellulare viene inviata una conferma di attivazione del servizio.

- richiesta di PosteID on line ad opera di un tutore/amministratore di sostegno che opera in nome e per conto del soggetto tutelata nato tra il 1998 ed il 1999, con identificazione mediante la verifica dei dati anagrafici del titolare inseriti sul portale e della copia del suo codice fiscale e documento di riconoscimento caricati all'atto della richiesta.

Il Titolare dell'Identità Digitale potrà utilizzare PosteID nell'ambito del Sistema Pubblico d'Identità Digitale, dei Servizi Finanziari di Poste Italiane o di altri servizi di Poste stessa.

Nella fase di rilascio dell'Identità Digitale, per le diverse modalità riportate nei paragrafi che seguono, le componenti applicative del Servizio procedono alla **certificazione della disponibilità**:

- del **numero di telefono cellulare**, attraverso l'invio di un codice di verifica SMS - OTP che viene inserito dall'utente nelle maschera di conferma;
- della **email del richiedente**, attraverso l'invio di un codice OTP che viene inserito dall'utente nella maschera di conferma oppure attraverso l'invio sulla email indicata di un link (token) che l'utente dovrà cliccare.

5.1 Registrazione Identità PosteID per clienti Poste Italiane già identificati "a vista" e dotati di strumenti di identificazione online rilasciati da Poste

In questo caso il cliente è stato già identificato "a vista", preliminarmente al rilascio degli strumenti di identificazione informatica, mediante esibizione del documento di identità e del codice fiscale, dei quali è stata effettuata una copia conservata da Poste Italiane nel fascicolo utente. L'autenticità e la congruenza di tali documenti è stata verificata da Poste Italiane presso le relative banche dati.

Il cliente si registra al servizio PosteID conforme alla normativa SPID, per il rilascio dell'Identità Digitale, attraverso le azioni riportate di seguito.

Identificazione

Il cliente che si identifica con SMS sul cellulare certificato o lettore BancoPosta:

- inserisce il proprio Nome Utente e la password poste.it per semplificare la raccolta dei dati necessari e si identifica online con gli strumenti in suo possesso (lettore BancoPosta con Postamat oppure password e OTP; in alternativa può utilizzare la Firma Digitale o la Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica), con le modalità operative riportate nella Guida Utente.

Nel caso l'utente effettui l'identificazione tramite SMS sul cellulare certificato, il sistema richiede l'inserimento del numero e della data di scadenza del documento ad esso associato nel momento

di rilascio da parte di Poste.

Conferma dati, verifica contatti e configurazione del servizio

L'utente:

- inserisce come proprio Nome Utente un indirizzo email valido, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo 5 "Modalità di richiesta del servizio";
- sceglie una password, rispondente ai requisiti descritti nel paragrafo 13.4 "Misure anticontraffazione";
- indica o conferma il numero di cellulare, il cui possesso viene certificato mediante l'invio di un SMS con una One Time Password che deve essere digitata nella maschera di inserimento dati. NB: se l'utente ha effettuato l'identificazione tramite SMS sul cellulare certificato, il numero di cellulare viene riproposto automaticamente, con possibilità per l'utente di modificarlo;
- verifica, ed eventualmente aggiorna, i propri dati identificativi già presenti nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- viene informato che l'identità digitale PosteID consente di accedere a tutti i servizi del Sistema Pubblico di Identità Digitale con livello di sicurezza fino a SPID L2, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6..

Accettazione condizioni generali del servizio

L'utente accetta le Condizioni Generali del Servizio, anche ai sensi degli artt. 1341 e 1342 cc, e fornisce i consensi relativi alla privacy barrando gli appositi campi.

A seguito della conferma da parte del cliente, attraverso l'inserimento della password, Poste Italiane provvede all'attivazione dell'Identità Digitale e delle credenziali associate.

5.2 Registrazione Identità PosteID per utenti che non dispongono di strumenti di identificazione online rilasciati da Poste Italiane

In questo scenario, sono previsti tre differenti processi:

- Registrazione/Adesione per clienti con Firma Digitale o Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica;
- Registrazione/Adesione per clienti senza strumento di identificazione online;
- Registrazione/Adesione per titolari di strumenti di identificazione informatica preesistenti a SPID rilasciati da Enti Terzi autorizzati da AgID ad operare come GIP.

5.2.1 Registrazione/Adesione per clienti con Firma Digitale o Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica

L'utente, collegandosi al portale PosteID, viene guidato nel processo di registrazione per i nuovi utenti. Questo prevede i seguenti passaggi:

Identificazione

L'utente si identifica attraverso lo strumento di identificazione online (Firma Digitale o Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica). Nel caso di utenti che dispongono di Firma Digitale, l'identificazione viene eseguita alla conclusione della procedura di registrazione, attraverso la firma del modulo di richiesta di adesione.

NB: *Se l'utente sceglie di registrarsi a PosteID accedendo al sito https://posteid.poste.it tramite il browser dello smartphone o del tablet (modalità responsive), l'identificazione "Firma Digitale" e "Carta Nazionale dei Servizi o Carta di Identità Elettronica" non saranno disponibili, poiché l'utilizzo di tali strumenti non è fruibile con le apparecchiature mobili.*

5.2.1.1 Registrazione/Adesione per clienti con Firma Digitale

Inserimento/conferma dei dati

L'utente:

- inserisce i propri attributi identificativi (esclusi gli estremi del documento di identità) nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- inserisce come proprio Nome Utente un indirizzo email valido, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo 5 "Modalità di richiesta del servizio";
- sceglie una password, rispondente ai requisiti descritti nel paragrafo 13.4 "Misure anticontraffazione";
- sceglie se già presente (nel caso sia comunque un cliente censito di Poste Italiane) o indica il numero di cellulare, il cui possesso viene certificato mediante l'invio di un SMS con una One Time Password che deve essere digitata nella maschera di inserimento dati;
- inserisce gli estremi del documento di identità ed i propri attributi secondari nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- viene informato che l'identità digitale PosteID consente di accedere a tutti i servizi del Sistema Pubblico di Identità Digitale con livello di sicurezza fino a SPID L2, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6.

Accettazione condizioni generali del servizio

Dopo aver accettato le Condizioni Generali del Servizio, anche ai sensi degli artt. 1341 e 1342 cc, e fornito i consensi relativi alla privacy barrando gli appositi campi, l'utente procede alla conferma della

richiesta.

L'utente completa la registrazione effettuando il download del modulo di richiesta di adesione, sottoscrivendolo digitalmente e ricaricandolo sul portale;

Il sistema procede con l'attivazione delle credenziali.

5.2.1.2 Registrazione/Adesione per clienti con Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica

Inserimento/conferma dei dati

L'utente:

- inserisce come proprio Nome Utente un indirizzo email valido, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo 5 "Modalità di richiesta del servizio";
- sceglie una password, rispondente ai requisiti descritti nel paragrafo 13.4 "Misure anticontraffazione";
- indica o conferma il numero di cellulare, il cui possesso viene certificato mediante l'invio di un SMS con una One Time Password che deve essere digitata nella maschera di inserimento dati. NB: se l'utente ha effettuato l'identificazione tramite SMS sul cellulare certificato, il numero di cellulare viene riproposto automaticamente, con possibilità per l'utente di modificarlo;
- inserisce i propri dati identificativi già presenti nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- viene informato che l'identità digitale PosteID consente di accedere a tutti i servizi del Sistema Pubblico di Identità Digitale con livello di sicurezza fino a SPID L2, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6.

Accettazione condizioni generali del servizio

Dopo aver accettato le Condizioni Generali del Servizio, anche ai sensi degli artt. 1341 e 1342 cc, e fornito i consensi relativi alla privacy barrando gli appositi campi, l'utente procede alla conferma della richiesta.

L'utente ripete la procedura di controllo effettuata in fase di identificazione.

Il sistema procede con l'attivazione delle credenziali.

5.2.2 Registrazione/Adesione per clienti senza strumento di identificazione online

L'utente, collegandosi al portale PosteID, viene guidato nel processo di registrazione per i nuovi utenti che prevede l'identificazione e certificazione del numero cellulare negli uffici postali abilitati oppure a domicilio mediante portalettere.

5.2.2.1 Identificazione presso gli uffici postali abilitati

Durante il processo di identificazione in ufficio postale l'utente:

- inserisce i propri attributi identificativi (esclusi gli estremi del documento di identità) nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- inserisce come proprio Nome Utente un indirizzo email valido, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo 5 "Modalità di richiesta del servizio";
- sceglie una password, rispondente ai requisiti descritti nel paragrafo 13.4 "Misure anticontraffazione";
- sceglie se già presente (nel caso sia comunque un cliente censito di Poste Italiane) o indica il numero di cellulare, il cui possesso viene certificato mediante l'invio di un SMS con una One Time Password che deve essere digitata nella maschera di inserimento dati;
- inserisce gli estremi del documento di identità ed i propri attributi secondari nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- viene informato che l'identità digitale PosteID consente di accedere a tutti i servizi del Sistema Pubblico di Identità Digitale con livello di sicurezza fino a SPID L2, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6;
- sceglie di essere identificato in un ufficio postale abilitato effettuando l'upload fronte-retro a colori del documento d'identificazione e del codice fiscale. In questo caso, potrà completare l'identificazione "a vista" con associazione del numero cellulare presso un qualsiasi ufficio postale. In alternativa, nel caso in cui fosse impossibilitato alla scansione del documento, può comunque completare la registrazione identificandosi "a vista" con associazione del numero di cellulare presso un ufficio postale dotato di sala consulenza (ricercabile attraverso apposita funzionalità presente online), nel quale un operatore effettuerà la scansione di documento e codice fiscale per suo conto.

Accettazione condizioni generali del servizio

L'utente accetta le condizioni generali del servizio ma, ai fini del perfezionamento di detta accettazione, dovrà seguire l'identificazione dell'utente stesso presso l'Ufficio Postale (cfr. *"Identificazione a Vista presso l'ufficio postale abilitato"*).

Identificazione a Vista presso l'ufficio postale abilitato

L'identificazione a vista viene eseguita:

- presso gli sportelli degli Uffici Postali abilitati al servizio, nel caso in cui l'utente, in fase di pre-registrazione, abbia effettuato l'upload dei documenti di riconoscimento, oppure
- presso la sala consulenza degli Uffici Postali, nel caso in cui all'utente non sia stato possibile caricare la scansione del documento in fase di pre-registrazione.

In entrambi gli scenari, l'operatore, verifica le informazioni di base dell'anagrafica utente

(precedentemente inserite dall'Utente stesso durante la richiesta di registrazione online), esegue l'identificazione a vista del richiedente e certifica l'associazione del numero di telefono cellulare, precedentemente verificato con le modalità indicate al paragrafo 5 "Modalità di richiesta del servizio", chiedendo al soggetto di confermare che il numero di cellulare inserito a sistema sia corretto.

Nel caso di identificazione in sala consulenza, inoltre, l'operatore scansiona codice fiscale e documento d'identità per la conservazione delle evidenze.

Al termine della procedura di identificazione, il sistema invierà un SMS di conferma del buon esito delle verifiche "de visu". A seguire il sistema invierà una e-mail per comunicare l'avvenuta attivazione dell'identità digitale.

Se l'utente avesse commesso un errore di digitazione dei propri dati in fase di pre-registrazione, può accedere al sito PosteID con il nome utente e la password che aveva scelto e procedere alla modifica dei dati errati o all'annullamento della sua richiesta, prima di recarsi nuovamente in Ufficio Postale per completare l'identificazione.

5.2.2.2 Identificazione a domicilio mediante un portalettere

Durante il processo di registrazione con richiesta di identificazione a domicilio mediante portalettere, l'utente:

- inserisce i propri attributi identificativi (esclusi gli estremi del documento di identità) nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- inserisce come proprio Nome Utente un indirizzo email valido, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo 5 "Modalità di richiesta del servizio";
- sceglie una password, rispondente ai requisiti descritti nel paragrafo 13.4 "Misure anticontraffazione";
- sceglie se già presente (nel caso sia comunque un cliente censito di Poste Italiane) o indica il numero di cellulare, il cui possesso viene certificato mediante l'invio di un SMS con una One Time Password che deve essere inserita sulla maschera di inserimento dati;
- inserisce gli estremi del documento di identità ed i propri attributi secondari nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- viene informato che l'identità digitale PosteID consente di accedere a tutti i servizi del Sistema Pubblico di Identità Digitale con livello di sicurezza fino a SPID L2, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6;
- sceglie di essere identificato a domicilio mediante un portalettere.

Accettazione condizioni generali del servizio

L' utente accetta le condizioni contrattuali e le clausole vessatorie del servizio di identificazione a domicilio visualizzando le condizioni generali del servizio di identità digitale. Ai fine del perfezionamento di dette accettazioni, dovrà seguire l'identificazione a domicilio ad opera di un portalettere (cfr. "*Identificazione a domicilio mediante portalettere*") .

Identificazione a domicilio mediante portalettere

L'utente viene contattato a domicilio da un portalettere. Dopo le verifiche preventive legate all'identità dell'utente, consistenti nella verifica dell'identità dell'utente previa presentazione da parte dell'utente di un documento di identità in corso di validità nonché del codice fiscale, l'operatore richiede la copia fronte retro del codice fiscale e del documento del cliente. A valle delle verifiche preliminari sui dati forniti richiede la sottoscrizione del modulo di richiesta dell'identità digitale, consegnato in busta chiusa, prodotto all'atto della pre-registrazione per confermare l'accettazione della pratica. L'utente effettua il pagamento del servizio di identificazione a domicilio in contrassegno direttamente con il portalettere tramite contanti e/o carta. Il portalettere acquisisce la documentazione ricevuta che verrà successivamente scansionata per la conservazione delle evidenze. Al termine della procedura di identificazione e certificazione del cellulare, il sistema invierà un SMS di conferma del buon esito delle verifiche "de visu". A seguire il sistema invierà una e-mail per comunicare l'avvenuta attivazione dell'identità digitale.

Laddove l'utente non dovesse essere presente, è previsto il rilascio di un avviso e la possibilità di prendere un secondo appuntamento entro 5 giorni dalla visita.

5.2.3 Registrazione/Adesione per titolari di strumenti di identificazione informatica preesistenti a SPID rilasciati da Enti Terzi autorizzati da AgID ad operare come GIP

Poste Italiane di tempo in tempo potrà predisporre procedure di registrazione/adesione a PosteID abilitato a SPID sulla base di specifiche autorizzazioni ricevute da AgID relativamente al riutilizzo di strumenti di identificazione informatica preesistenti a SPID rilasciati da Enti Terzi. Gli Enti Terzi autorizzati si qualificano come Gestori di Identità Pregresse (GIP).

Tali procedure di registrazione prevedono due momenti:

- Il titolare dello strumento di identificazione informatica preesistente richiede sul sito dell'Ente Terzo di poter avviare la procedura di adesione all'Identità Digitale di Poste Italiane. Le modalità di richiesta sono specifiche per il singolo GIP e prevedono che il titolare effettui un'operazione di identificazione informatica con credenziali con livello di sicurezza almeno analogo al livello SPID 2 (LoA3), e che l'esito positivo dell'identificazione forte abiliti l'Ente Terzo a trasferire i dati anagrafici (almeno nome, cognome e codice fiscale) e gli attributi del titolare in suo possesso;
- Il richiedente viene re-indirizzato sul sito del servizio PosteID abilitato a SPID, dove:

- sceglie il nome utente e la password della propria identità digitale,
- compila o completa i propri dati anagrafici e attributi necessari alla registrazione,
- consulta ed accetta le Condizioni Generali del Servizio ed esprime i consensi al trattamento dei dati personali.

Relativamente ai passi della procedura di registrazione previsti sul sito del servizio PosteID abilitato a SPID, le fasi di "Conferma dati, verifica contatti e configurazione del servizio" e "Accettazione condizioni generali del servizio" sono analoghe a quanto previsto per i clienti di Poste Italiane già identificati "a vista" e dotati di strumenti di identificazione online rilasciati da Poste (cfr. capitolo 5.1).

5.3 Registrazione al servizio PosteID effettuata da un soggetto tutore o amministratore di sostegno per i nati nel 1998 e 1999

L'identità digitale PosteID per persone fisiche può essere richiesta anche da parte di un tutore o amministratore di sostegno (in seguito "rappresentante") per i nati degli anni 1998 e 1999 (in seguito "rappresentati"). Tale identità potrà essere utilizzata solo su specifici servizi che saranno via via identificati e comunicati da AgID sul sito www.spid.gov.it.

Al fine di avviare la richiesta per conto di un rappresentato, il soggetto rappresentante deve essere dotato di un'identità digitale PosteID attiva.

La procedura di richiesta e attivazione prevede i seguenti passaggi:

1. Avvio richiesta;
2. Compilazione richiesta Identità Digitale;
3. Accettazione del contratto e manifestazione del consenso al trattamento dei dati sensibili;
4. Verifica documentazione da parte di Poste Italiane;
5. Attivazione Identità Digitale.

Avvio richiesta

Il soggetto rappresentante si collega al sito https://posteid.poste.it e si identifica accedendo alla propria area personale selezionando il link "ACCEDI".

Nella propria area personale seleziona l'apposito link "Richiesta Identità Digitale per soggetto rappresentato" per avviare la procedura di richiesta.

Compilazione richiesta

Il rappresentante:

- inserisce come Nome Utente un indirizzo email valido, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo 5 "Modalità di richiesta del servizio";

- sceglie una password, rispondente ai requisiti descritti nel paragrafo 13.4 “Misure anticontraffazione”;
- sceglie se già presente (nel caso sia comunque un cliente censito di Poste Italiane) o indica il numero di cellulare, il cui possesso viene certificato mediante l’invio di un SMS con una One Time Password che deve essere inserita sulla maschera di inserimento dati;
- inserisce gli estremi del documento di identità e gli attributi secondari del soggetto rappresentato nel form di richiesta, come riportati nel paragrafo 5.4 “Anagrafica utente”; Carica:
    - copia digitale del fronte del documento d’identità e del codice fiscale del soggetto rappresentato;
    - copia digitale del retro del documento d’identità e del codice fiscale del soggetto rappresentato;
    - copia digitale della documentazione che attesta la titolarità del rappresentante ad effettuare la richiesta dell’identità digitale per conto del rappresentato;
- viene informato che l’identità digitale PosteID consente di accedere a tutti i servizi del Sistema Pubblico di Identità Digitale con livello di sicurezza fino a SPID L2, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6.

Accettazione del contratto e manifestazione del consenso al trattamento dei dati sensibili

Ai sensi del Regolamento 2016/679/UE (Regolamento europeo in materia di protezione dei dati personali) e s.m.i. (trattamento dei dati sensibili), dell’art. 65.1 lett. b) del CAD (istanze presentate per via telematica) e dell’art. 21.1 del CAD (utilizzo della Firma Elettronica), il soggetto rappresentante il tutelato/beneficiario sottoscrive l’accettazione della proposta contrattuale di Poste inerente il Servizio e manifesta il consenso al trattamento dei dati sensibili apponendo una firma elettronica tramite autenticazione PosteID abilitato a SPID basata su credenziali di Livello 2 SPID.

Verifica documentazione da parte di Poste Italiane

La pratica viene assegnata ad un operatore di backoffice di Poste Italiane che, dopo aver verificato la correttezza dei dati, la completezza della documentazione e la titolarità della domanda, fornisce una conferma per l’avvio del provisioning tecnico e, quindi, dell’attivazione dell’Identità Digitale e delle relative credenziali.

Qualora la pratica presenti anomalie, Poste Italiane contatterà il richiedente che potrà modificare o annullare la richiesta, così come descritto nella guida utente.

5.4 Anagrafica utente

L’anagrafica dell’utente è composta dai dati riportati di seguito.

Attributi identificativi

I campi sono precompilati con i dati già in possesso, se già clienti di Poste Italiane o derivanti dallo specifico strumento di identificazione utilizzato:

- nome (obbligatorio);
- cognome (obbligatorio);
- sesso (obbligatorio);
- data e luogo di nascita (obbligatorio);
- codice fiscale (obbligatorio);
- estremi documento di identità (obbligatorio); nel caso la registrazione si riferisca a soggetti già clienti di Poste Italiane, il documento è quello fornito in fase di identificazione a vista. Qualora il documento non fosse più valido, verrà richiesto al cliente di aggiornarne gli estremi. Fermo restando ciò, i processi di Poste Italiane prevedono che i clienti dei servizi BancoPosta, sulla base dei requisiti normativi dell'adeguata verifica, siano periodicamente richiamati a sportello per fornire dati e copia di documenti di identità in corso di validità.

Attributi secondari

I campi sono precompilati con i dati già in possesso, se già clienti di Poste Italiane:

- numero di cellulare certificato (obbligatorio);
- indirizzo di posta elettronica di contatto (obbligatorio);
- indirizzo di domicilio;
- numero di telefonia fissa;
- indirizzo di domicilio digitale.

Poste Italiane può associare al fine di migliorare l'esperienza d'uso, i dati aggiuntivi riportati di seguito:

- indirizzo di residenza;
- domicilio di recapito.

I dati aggiuntivi sono associati all'identità digitale ma non utilizzati nel contesto di erogazione dei servizi SPID.

5.5 Rilascio Credenziali

Il rilascio delle credenziali prevede, a valle del completamento della richiesta dell'Identità Digitale PosteID, l'attivazione delle credenziali e la conservazione delle evidenze.

Il processo di attivazione delle credenziali termina con l'invio all'utente di una comunicazione via

email di avvenuta attivazione del servizio e comunicazione del codice di sospensione immediata, nei casi previsti.

Nel caso di credenziali PosteID di primo livello l'utente può da subito utilizzare la propria identità digitale.[1]

Qualora l'utente abbia scelto le credenziali PosteID di secondo livello basate su app, visualizza le indicazioni per il download e la configurazione dell'app e procede con i passi operativi riportati nella Guida Utente

5.5.1 Conservazione delle evidenze

La conservazione delle evidenze prevede l'archiviazione della documentazione comprovante la corretta attribuzione dell'Identità Digitale al richiedente.

Il sistema invia in conservazione il fascicolo di richiesta dell'identità digitale, contenente le evidenze, i documenti e i dati utilizzati per l'associazione e la verifica degli attributi. Il dettaglio dei dati conservati è riportato al paragrafo 13.1 "Conservazione evidenze per il rilascio dell'Identità Digitale".

6 Strumenti di autenticazione

6.1 Tipologia di strumenti di autenticazione PosteID

In questo paragrafo sono descritti gli strumenti realizzati dal Gestore ed autorizzati da AgID in aderenza ai livelli di sicurezza SPID previsti dal DPCM 24 ottobre 2014.

Livello di Sicurezza SPID	Utenti PosteID che utilizzano app	Utenti PosteID che non utilizzano app
Primo livello (LoA2)	Password	
Secondo livello (LoA3)	App e codice personale	Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato[1]
Terzo livello (LoA4)	*Soluzioni non ancora disponibili*	

Livelli di sicurezza SPID e strumenti PosteID

La descrizione di dettaglio degli strumenti è riportata nella Guida Utente e sul sito https://posteid.poste.it.

Le misure di sicurezza e anticontraffazione adottate sono riportate al paragrafo 13 “Sicurezza del servizio PosteID”.

6.1.1 Strumenti di primo livello SPID

Lo strumento di primo livello messo a disposizione dal Gestore è la password utente conforme ai requisiti previsti da AgID e riportati al paragrafo 13.4.1 “Misure per il primo livello SPID con sistemi di autenticazione a 1 fattore”.

6.1.2 Strumenti di secondo livello SPID

L’app PosteID è lo strumento di autenticazione LoA3 messo a disposizione dal Gestore per gli utenti che dispongono di uno smartphone/tablet.

La soluzione implementa un meccanismo di autenticazione a due fattori basati sul possesso del dispositivo mobile a cui è associato un certificato e la conoscenza del codice personale.

Tale soluzione nasce dall’esperienza maturata dal Gestore sul canale mobile e si basa sull’associazione dell’identità digitale allo smartphone/tablet dell’utente. Il dispositivo mobile diventa così lo strumento che abilita l’utente all’utilizzo dell’Identità Digitale. L’utente dispone di un codice

[1] Per l’effettiva disponibilità dello strumento di autenticazione “Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato” si rimanda a quanto è disciplinato nelle Condizioni Generali del Servizio “PosteID abilitato a SPID”.

personale definito in fase di installazione dell'app.

Processo di attivazione della credenziali PosteID di secondo livello con app

Il processo di attivazione dello strumento prevede che l'utente esegua i seguenti passi:

- download e installazione dell'app sul proprio dispositivo mobile;
- login sull'app con le proprie credenziali Nome Utente/password;
- scelta del codice personale che abilita all'utilizzo delle credenziali
- ricezione sul numero di telefono certificato di un sms con il codice di attivazione;
- inserimento e verifica del codice di attivazione sull'app.

6.1.2.1 Ulteriori strumenti di secondo livello SPID

Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato[12]

La soluzione PosteID con codice di verifica SMS - OTP si basa sull'utilizzo di un dispositivo mobile, in grado di ricevere SMS e implementa una "autenticazione a due fattori" completamente software. Tale soluzione si basa sull'associazione della password e del numero telefonico certificato del cellulare dell'utente.

Il cliente riceve sul numero di telefono certificato un SMS - OTP che utilizza come secondo fattore di autenticazione, in associazione alla password, per l'accesso ai servizi che richiedono il secondo livello di sicurezza, come previsto dal DPCM 24 ottobre 2014.

6.2 Utilizzo degli strumenti di autenticazione PosteID

- L'utente richiede l'accesso ad un servizio collegandosi telematicamente al sito del Fornitore di servizi (ad esempio la Pubblica Amministrazione) dove indica il proprio Gestore dell'Identità.
- Il Fornitore di servizi rimanda il soggetto titolare dell'identità digitale verso il Gestore dell'identità digitale, richiedendone l'autenticazione con uno specifico livello di sicurezza

[2] Per l'effettiva disponibilità dello strumento di autenticazione "Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato" si rimanda a quanto è disciplinato nelle Condizioni Generali del Servizio "PosteID abilitato a SPID".

SPID.

- Il Gestore dell'identità digitale verifica l'identità del soggetto sulla base delle credenziali esibite.

Per favorire l'usabilità, a seguito dell'inserimento del Nome Utente e della password, il sistema riconosce l'utente e propone l'utilizzo dello strumento con livello di sicurezza adeguato. In ogni caso, viene lasciata la possibilità di richiedere l'utilizzo di strumenti di livello superiore.

Autenticazione con sistemi di autenticazione a 1 fattore

Utente con Password
L'utente inserisce il proprio Nome Utente e la propria password nella maschera di autenticazione visualizzata dal Gestore.

Autenticazione PosteID con sistemi di autenticazione a 2 fattori

Utente con app PosteID	Utente con SMS - OTP PosteID[3]
Modalità 1 di avvio dell'autenticazione: L'utente inserisce il proprio Nome Utente e password sulla maschera web di login e riceve una notifica sul proprio smartphone tramite l'app PosteID. *Modalità 2 di avvio dell'autenticazione*: L'utente apre l'APP PosteID e fotografa il QR code visualizzato sulla maschera web di login. *Per entrambe le modalità di avvio dell'autenticazione*: L'utente inserisce il proprio codice personale sull'APP. Al termine della prima autorizzazione andata a buon fine, l'utente può associare la propria impronta digitale (cosiddetta "fingerprint") oppure la sua impronta facciale (cosiddetta "Face ID") al codice personale - definito in fase di installazione dell'app sull'apparato mobile di cui ha la disponibilità - per evitarne la digitazione nelle fasi in	L'utente inserisce il proprio Nome Utente e la propria password nella maschera di autenticazione visualizzata dal Gestore. Riceve un codice di verifica SMS a bruciatura (OTP) sul numero di telefono cellulare "certificato" in fase di adesione. L'utente inserisce il codice OTP ricevuto. • **NB**: nel solo caso di primo utilizzo di un nuovo PC/Browser, il sistema invia all'utente una notifica di "tentativo di accesso" ad un servizio sulla sua e-mail di contatto, invitando l'utente a contattare l'Assistenza Clienti nel caso in cui non si riconoscesse nella richiesta di autenticazione.

[3] Per l'effettiva disponibilità dello strumento di autenticazione "Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato" si rimanda a quanto è disciplinato nelle Condizioni Generali del Servizio "PosteID abilitato a SPID".

cui ciò viene richiesto dal servizio PosteID abilitato a SPID.
Di seguito il dettaglio della versione minima dei sistemi operativi che supportano le diverse modalità, in particolare:

- Per quanto concerne l'mpronta digitale:
  a) iOS 9 o superiore e lettore d'impronta (es. iPhone 5s o versioni più recenti, iPad Pro, iPad Air 2 oppure iPad mini 3 o versioni più recenti);
  b) Android 6.0 (Marshmallow) o superiore e lettore di impronta.
- Per quanto concerne l'impronta facciale, iOS 11 o superiore e sensore di riconoscimento della fisionomia del volto (es. iPhone X o versioni più recenti).

E' vietato all'utente associare al codice personale l'impronta digitale o l'impronta facciale di un soggetto terzo.

L'utente può, in qualunque momento, disabilitare l'eventuale associazione dell'impronta digitale o dell'impronta facciale al codice personale tramite le funzionalità previste dall'apparato mobile in uso.

Poste non effettua alcun trattamento dei dati personali biometrici, relativi all'impronta digitale o all'impronta facciale, che vengono acquisiti dall'apparato mobile utilizzato dall'utente, e pertanto non può essere ritenuta responsabile di eventuali danni materiali o immateriali, diretti o indiretti, derivanti dal non corretto utilizzo da parte dell'utente o da eventuali compromissioni del sensore di rilevamento e dei relativi servizi di gestione dell'apparato mobile (es. furto o usurpazione d'identità).

Per quanto attiene termini e modalità di trattamento dei suddetti dati biometrici da parte dei produttori del sistema operativo (Apple, Android) e dell'apparato mobile si rinvia alla loro informativa privacy.

Per motivi di sicurezza, Poste si riserva di disattivare in qualsiasi momento la funzionalità di associazione dell'impronta digitale o dell'impronta facciale al codice personale e di ripristinare il normale funzionamento tramite immissione del codice PosteID.

- **NB**: nel solo caso di primo utilizzo dell'APP su un nuovo smartphone, il sistema invia all'utente una notifica di "tentativo di accesso" ad un servizio sulla sua e-mail di contatto, invitando l'utente a contattare l'Assistenza Clienti nel caso in cui non si riconoscesse nella richiesta di autenticazione.

- In caso di esito positivo, il Gestore nel rispetto di quanto previsto dalle regole tecniche e dalle

modalità attuative di SPID emette a favore del Fornitore di servizi una certificazione di autenticazione e rimanda l'utente verso il Fornitore di servizi.

- Il Fornitore di servizi avendo conferma dell'identità dell'utente e delle informazioni necessarie, autorizza la fruizione del servizio richiesto. (per particolari tipologie di servizi il Fornitore può provvedere alla verifica presso i Gestori di attributi qualificati in relazione al possesso di specifiche qualifiche o poteri).

6.3 Ambiti di utilizzo di PosteID

PosteID è utilizzato sia per l'accesso e la sicurezza dei servizi che Poste Italiane eroga ai propri clienti che come soluzione di autenticazione accreditata nell'ambito del Sistema Pubblico per l'Identità Digitale.

6.4 Messaggi di anomalia

Nella fase di autenticazione possono essere riscontrate le tipologie di errore riportate di seguito.

Scenario	Dettaglio Errore	Azioni e notifica all'utente	Errore SAML
Autenticazione corretta	n.a.	L'utente viene autenticato e rediretto verso il SP	urn:oasis:names:tc:SAML:2.0:status:Success
Indisponibilità sistema	n.a.	Viene mostrato un errore generico sul sito dell'IDP	n/a
Errore generico (parametro mancante)	Parametri obbligatori: SAMLRequest SigAlg Signature Parametri non obbligatori: RelayState	Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 417 per facilitare l'assistenza	n/a
Errore generico (parametro mancante)	Parametri obbligatori: SAMLRequest Parametri non obbligatori: RelayState	Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 417 per facilitare l'assistenza	n/a
Errore generico (parametro mancante)	Verifica della presenza nella AuthnRequest dei seguenti attributi/nodi: Issuer: identificativo SP ID: necessario per la SAMLresponse "InResponseTo"	Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 417 per facilitare l'assistenza	n/a

Scenario	Dettaglio Errore	Azioni e notifica all'utente	Errore SAML
Binding su metodo HTTP errato	invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell'identity	Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 405 per facilitare l'assistenza	n/a
Binding su metodo HTTP errato	invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity	Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 405 per facilitare l'assistenza	n/a
SP non riconosciuto	Dati SP non presenti nel AuthnRequest	Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 403 per facilitare l'assistenza	n/a
AuthnRequest non firmata		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 403 per facilitare l'assistenza	n/a
AuthnRequest con firma non corretta		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 403 per facilitare l'assistenza	n/a
AuthnRequest con firma corretta e certificato non trustato su IDP		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 403 per facilitare l'assistenza	n/a
AuthnRequest con firma corretta e certificato scaduto		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione sul sito dell'IdP. Viene fornita una pagina HTML con status code 200 e riportante il codice di errore 403 per facilitare l'assistenza	n/a
RequestAuthnContext con livello di autenticazione non esistente	Auth livello richiesto diverso da: urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3	Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Responder SubStatus:NoAuthnContext
mancata validità temporale dell'asserzione		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester SubStatus:RequestDenied

Scenario	Dettaglio Errore	Azioni e notifica all'utente	Errore SAML
Utente nega il consenso all'invio di dati al SP		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Responder SubStatus:RequestDenied
Autenticazione fallita (superato numero X tentativi)		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Responder SubStatus:AuthnFailed
Identità senza il livello richiesto		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Responder SubStatus:AuthnFailed
versione saml diversa dalla 2.0		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch
versione saml non specificata		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester SubStatus:RequestUnsupported
IssueInstant non presente		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester SubStatus:RequestUnsupported
protocol binding non specificato nella request		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester SubStatus:RequestUnsupported
destination non specificata nella request		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester SubStatus:RequestUnsupported
attributo isPassive non settato a false		Viene mostrata una pagina informativa di carattere generale relativa alla fallita autenticazione. L'utente non viene re-diretto verso il Fornitore di servizi che ha richiesto l'autenticazione.	urn:oasis:names:tc:SAML:2.0:status:Requester SubStatus:NoPassive

Tipologia di errori

7 Gestione del ciclo di vita dell'identità digitale

7.1 Sospensione

Nel caso in cui l'utente debba sospendere le proprie credenziali, potrà richiederne in qualunque momento (servizio accessibile H24 7 giorni su 7) la sospensione immediata.

La sospensione può essere richiesta dall'utente sia sul portale web PosteID all'indirizzo https://posteid.poste.it, che tramite Interactive Voice Response (IVR) del Servizio Clienti del Gestore.

In caso l'utente ritenga, poi, di voler revocare le proprie credenziali, dopo aver effettuato la sospensione potrà avviare la richiesta di revoca delle credenziali PosteID.

La sospensione delle credenziali potrà avvenire anche ad opera del Gestore alla scadenza del documento di riconoscimento rilasciato dal cliente all'atto della registrazione. In questo caso il titolare dell'Identità Digitale dovrà aggiornare il proprio documento di riconoscimento accedendo alla propria area personale sul sito www.posteid.poste.it.

7.1.1 Sospensione immediata tramite il servizio web

Per effettuare la richiesta l'utente deve:

- inserire il proprio Nome Utente;
- inserire il codice di sospensione immediata ricevuto in fase di attivazione delle credenziali PosteID;
- inserire il codice di controllo intelligente "captcha";
- scegliere da menù a tendina la motivazione della richiesta di sospensione (furto o smarrimento delle credenziali o dello strumento di autenticazione associato - sospetto utilizzo abusivo o fraudolento da parte di un soggetto terzo - esigenze personali);
- confermare la richiesta.

Il sistema verifica la validità del codice fornito: in caso positivo, presenta un messaggio di sospensione avvenuta con successo, le credenziali sono poste in stato "sospese" e viene inviata una comunicazione di avvenuta sospensione (completa delle istruzioni per procedere alla revoca delle credenziali ovvero alla ri-attivazione delle stesse) all'indirizzo email verificato in fase di adesione al servizio; in caso negativo, verrà presentato un messaggio di errore nella richiesta di sospensione e la possibilità di procedere con un ulteriore tentativo.

La richiesta di sospensione ha una durata di 30 giorni. In tale periodo l'utente che voglia procedere alla revoca delle credenziali deve formalizzare la richiesta come descritto nel paragrafo 7.2.1 "Richiesta di revoca in seguito a sospensione immediata".

7.1.2 Sospensione immediata tramite il servizio Interactive Voice Response

La richiesta di sospensione immediata mediante Interactive Voice Response (IVR) è avviata

dall'utente tramite telefonata al Servizio Clienti, (con chiamata ai numero verde gratuito 803 160 oppure da rete mobile al numero 199.100.160, selezione *servizi internet\servizio PosteID\Sospensione immediata credenziali PosteID*). Interagendo con il servizio IVR, l'utente deve:

- seguire il percorso per selezionare il servizio corrispondente alla richiesta di sospensione;
- scegliere se sta chiamando dal numero certificato PosteID o da altro numero di telefono;
- digitare il proprio numero di telefono certificato PosteID, in caso stia chiamando da altro numero di telefono,
- digitare il codice di sospensione immediata.

Il sistema verifica la validità del codice fornito.

In caso negativo, il servizio IVR comunicherà l'errore nella richiesta di sospensione e la possibilità di procedere con un altro tentativo di digitazione del codice di sospensione.

In caso positivo, invece, il servizio IVR richiederà all'utente di scegliere la motivazione della richiesta di sospensione, digitando il numero corrispondente alla stessa (furto o smarrimento delle credenziali o dello strumento di autenticazione associato - sospetto utilizzo abusivo o fraudolento da parte di un soggetto terzo - esigenze personali).

Il sistema, a questo punto, comunica la sospensione avvenuta con successo; le credenziali sono poste in stato "sospese" e viene inviata una comunicazione di avvenuta sospensione (completa delle istruzioni per procedere con la revoca delle credenziali ovvero alla ri-attivazione delle stesse) all'indirizzo email (indirizzo certificato in fase di adesione al servizio).

Come nel caso di sospensione da portale, la richiesta di sospensione tramite servizio IVR ha una durata di 30 giorni. In tale periodo l'utente che voglia procedere alla revoca delle credenziali deve formalizzare la richiesta come descritto nel paragrafo 7.2.1 "Richiesta di revoca in seguito a sospensione immediata".

7.2 Revoca

7.2.1 Richiesta di revoca in seguito a sospensione immediata

La sospensione immediata ha una durata di 30 giorni; durante tale periodo, l'utente deve far pervenire al Gestore la richiesta di revoca delle credenziali con le modalità riportate nel seguito:

- compilare il modulo di richiesta di revoca delle credenziali e firmarlo;
- effettuare la denuncia di smarrimento ovvero utilizzo abusivo/ fraudolento da parte di soggetto terzo (per gli stessi fatti per cui ha richiesto la sospensione);
- far pervenire a Poste Italiane la richiesta, corredata da copia del proprio documento di identità.

La trasmissione a Poste Italiane può essere effettuata tramite i seguenti canali alternativi:

- posta elettronica certificata (PEC) con allegata la documentazione firmata digitalmente;
- email inviata da casella verificata in fase di adesione al servizio con allegata la documentazione (firmata digitalmente o con firma autografa).

L'operatore di Poste Italiane, ricevuta la richiesta di revoca, verifica:

- la completezza della documentazione;
- la consistenza della documentazione (compilata correttamente, documento di identità allegato corrispondente al titolare delle credenziali di identità digitale che si intendono revocare);
- che esista una precedente richiesta di sospensione per la stessa identità;
- nei casi previsti, la validità/conformità della denuncia (la motivazione deve essere coerente con quanto dichiarato in fase di richiesta di sospensione);
- la provenienza della documentazione, verificando:
  - che l'indirizzo email del mittente sia corrispondente all'indirizzo email verificata in fase di adesione al servizio,

  oppure

  - che i dati del titolare della Firma Digitale corrispondano ai dati del titolare dell'Identità Digitale.

In caso anche solo una delle verifiche suddette dia esito negativo, l'operatore contatta tempestivamente l'utente al fine di definire la problematica e l'eventuale soluzione.

Nel caso tutte le verifiche diano esito positivo, viene inviato all'utente un SMS al numero di cellulare certificato contenente la conferma della presa in carico della richiesta di revoca e l'identificativo della richiesta stessa.

Dopo 72 ore dall'invio dell'SMS le credenziali vengono revocate definitivamente.

Qualora l'utente riceva l'SMS senza che abbia fatto alcuna richiesta di revoca deve contattare il Servizio Clienti (vedi capitolo 8 "Rapporti con gli utenti" per numeri o orari), entro 72 ore dalla ricezione dell'SMS, per bloccare il processo di revoca specificando l'identificativo della richiesta riportato sull'SMS.

Al completamento di tale processo, l'utente riceve presso l'indirizzo email di contatto una conferma di avvenuta revoca delle singole credenziali o dell'Identità Digitale, completa di data e motivazione.

Diversamente, decorsi 20 giorni senza che sia pervenuta la documentazione di richiesta di revoca, il sistema genera una comunicazione verso l'utente per ricordargli la prossima scadenza della richiesta di sospensione.

Al termine dei 30 giorni dalla richiesta di sospensione, senza che sia pervenuta alcuna richiesta di revoca, le credenziali sospese sono automaticamente riattivate e l'utente riceve una comunicazione di avvenuta riattivazione.

In ogni caso, per garantire il rispetto dei tempi previsti, l'utente è tenuto ad inviare la documentazione di revoca almeno 5 giorni lavorativi prima che siano trascorsi i 30 giorni dalla sospensione immediata.

7.2.1.1 Riattivazione delle credenziali sospese

Nel caso in cui l'utente ritenga di voler ri-attivare le proprie credenziali, può farne richiesta dal portale PosteID, nella sezione dedicata alla gestione delle credenziali.

L'utente individua la credenziale da ri-attivare ed effettua la richiesta; il sistema invia un codice di verifica SMS - OTP al numero di cellulare certificato dell'utente, che:

- inserisce l'OTP sulla maschera presentata dal portale;
- sceglie dal menù a tendina la motivazione della richiesta di ri-attivazione (ritrovamento, errata sospensione automatica da parte del sistema, altro);
- conferma l'operazione.

Il sistema verifica la validità del codice di verifica OTP fornito e:

- in caso negativo, viene presentato un messaggio di errore nella richiesta di ri-attivazione e la possibilità di procedere con un altro tentativo (massimo 5 tentativi).
- in caso positivo, viene presentato un messaggio di verifica avvenuta con successo e il sistema invia all'utente via SMS il nuovo codice di sospensione immediata. Il portale presenta il pulsante per confermare l'avvenuta ricezione del codice e la richiesta di ri-attivazione delle credenziali.
- contestualmente, le credenziali sono poste in stato "attive" e viene inviata una comunicazione di avvenuta ri-attivazione all'indirizzo email (indirizzo certificato in fase di adesione al servizio).

7.2.2 Richiesta di revoca credenziali e recesso dal servizio PosteID

Nel caso in cui l'utente ritenga di revocare alcune credenziali in possesso ovvero recedere completamente dal servizio PosteID, deve effettuare il processo di revoca o il recesso sul portale del Gestore Poste Italiane.

L'utente deve:

- compilare e firmare il modulo di richiesta;
- far pervenire a Poste Italiane la documentazione, corredata da copia del proprio documento di identità.

L'inoltro della documentazione a Poste Italiane può essere effettuato tramite i seguenti canali alternativi. In particolare:

- posta elettronica certificata (PEC) con allegata la documentazione firmata digitalmente;
- email inviata da casella verificata in fase di adesione al servizio con allegata la documentazione (firmata digitalmente o con firma autografa).

L'operatore, ricevuta la richiesta di revoca, verifica:

- la completezza della documentazione necessaria;
- la consistenza della documentazione (compilata correttamente, documento di identità allegato corrispondente al titolare dell'identità digitale che si intende revocare);
- la provenienza della documentazione, verificando:
  - che l'indirizzo email del mittente sia corrispondente all'indirizzo email verificata in fase di adesione al servizio,

  oppure

  - che i dati del titolare della Firma Digitale corrispondano ai dati del titolare dell'Identità Digitale.

In caso anche solo una delle verifiche suddette dia esito negativo, l'operatore contatta tempestivamente l'utente al fine di definire la problematica e l'eventuale soluzione.

In caso tutte le verifiche diano esito positivo, viene inviato all'utente un SMS al numero di cellulare certificato contenente la conferma della presa in carico della richiesta di revoca e l'identificativo della richiesta stessa.

Dopo 72 ore dall' invio dell'SMS le credenziali vengono revocate definitivamente.

Qualora l'utente riceva l'SMS senza che abbia fatto alcuna richiesta di revoca deve contattare il Servizio Clienti (vedi capitolo 8 "Rapporti con gli utenti"), entro 72 ore dalla ricezione dell'SMS, per bloccare il processo di revoca specificando l'identificativo richiesta riportato sull'SMS.

A fronte dell'avvenuto processo di revoca, l'utente riceve all'indirizzo email di contatto una conferma di avvenuta revoca delle singole credenziali o dell'Identità Digitale, completa di data e motivazione.

I tutori/amministratori di sostegno dovranno richiedere la revoca dell'identità del soggetto tutelato una volta decaduto il proprio ruolo.

7.2.3 Revoca o sospensione dell'Identità Digitale su iniziativa del Gestore

Poste Italiane in qualità di Gestore dell'identità provvede alla revoca di una Identità nei seguenti casi:

- mancato utilizzo dell'identità per un periodo continuativo superiore ai 24 mesi;

- decesso della persona fisica a cui era associata l'identità accertato tramite il collegamento alle banche dati messe a disposizione tramite le convenzioni AgID o a seguito di comunicazione ufficiale – opportunamente verificata - da parte degli eredi oppure di una delle autorità competenti;
- scadenza del contratto relativo alla specifica Identità;
- scadenza del documento connesso all'Identità - in questo caso il Gestore provvede ad effettuare solo la sospensione della Identità e non la revoca della stessa.

Nei casi in cui la sospensione o revoca sono relativi ad eventi temporali pianificabili, il Gestore fornisce comunicazione al cliente (sugli attributi secondari indicati dal cliente) almeno 90 giorni prima e poi 30, 10 ed 1 giorno prima, specificando la causa e la data di sospensione o revoca dell'Identità.

7.3 Blocco temporaneo del profilo

Tramite apposita funzionalità presente nell'area di postlogin sul sito https://posteid.poste.it, il titolare di PosteID abilitato a SPID può effettuare un blocco temporaneo della propria identità digitale. Abilitando questa funzione il titolare può sospendere, con un'unica operazione e per il tempo che ritenga necessario, l'utilizzo di tutte le sue credenziali di accesso ai servizi offerti dai fornitori di servizi pubblici e privati aderenti a SPID. Il blocco può essere attivato e disattivato solo in selfcare dal titolare, previa autenticazione di accesso all'area riservata di gestione del proprio profilo, tramite il pulsante "ACCEDI" sul sito https://posteid.poste.it. Il blocco temporaneo non si applica agli accessi alle digital properties di Poste Italiane.

8 Rapporti con gli utenti

Poste Italiane mette a disposizione dei propri utenti un servizio di Call Center con operatore disponibile dalle 8:00 alle 20:00, dal lunedì al sabato (festivi esclusi), accessibile da rete fissa al numero verde gratuito 803 160 oppure da rete mobile al numero 199.100.160 (il costo della chiamata è legato al piano tariffario dell'operatore utilizzato).

Ogni comunicazione dell'utente relativa al servizio PosteID, concernente osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo, può essere inviata al seguente indirizzo:

Poste Italiane S.p.A.
Responsabile del Manuale Operativo PosteID
Viale Europa 175
00144 Roma
Email: responsabilemanualeposteid@posteitaliane.it

9 Condizioni di fornitura

Il servizio PosteID ha una durata di anni 2.

In assenza di disdetta da parte del Titolare, ai sensi di quanto previsto nelle Condizioni Generali del Servizio PosteID abilitato a SPID, la data di scadenza è tacitamente rinnovata di anno in anno fintantoché il Servizio sarà reso a titolo gratuito. Successivamente alla scadenza, non sarà più possibile eseguire il rinnovo e l'utente dovrà procedere con una nuova richiesta di Identità Digitale.

Il Gestore potrà sospendere temporaneamente il Servizio, fermo restando gli obblighi di legge, per procedere alla manutenzione di impianti ed altre apparecchiature necessarie all'esecuzione del servizio stesso, dandone comunicazione con avviso pubblicato sul sito https://posteid.poste.it, con un preavviso di 1 (uno) giorno.

Il Gestore potrà sospendere il Servizio anche in caso di violazione da parte dell'utente degli obblighi posti a suo carico in base a quanto previsto dal Manuale Operativo o dallo specifico accordo contrattuale oppure per ragioni di sicurezza, dandone comunicazione al Titolare tramite e-mail, fatta salva ogni eventuale azione di rivalsa nei riguardi del responsabile delle violazioni.

Nel caso in cui l'esecuzione del servizio fosse ritardata, impedita od ostacolata da cause di forza maggiore, l'esecuzione medesima si intenderà sospesa per un periodo equivalente alla durata della causa di *forza maggiore*.

Per **"forza maggiore"** si intende qualsiasi circostanza al di fuori del ragionevole controllo del Gestore e, pertanto, in via esemplificativa e non esaustiva, si riferisce ad atti di pubbliche autorità, guerre, rivoluzioni, insurrezioni o disordini civili, scioperi, serrate o altre vertenze sindacali, blocchi od embarghi, interruzioni nella fornitura di energia elettrica, inondazioni, disastri naturali, epidemie ed altre circostanze che esulino dal controllo del Gestore.

10 Obblighi e responsabilità

Sulla base della normativa vigente, nel presente paragrafo sono sinteticamente riassunti:

- gli obblighi che il Gestore SPID Poste Italiane assume in relazione alla propria attività;
- gli obblighi che il Titolare dell'identità digitale SPID assume in relazione alla richiesta e all'utilizzo dell'Identità Digitale rilasciata dal Gestore, con indicazione dei rispettivi riferimenti normativi.

Nella documentazione contrattuale del servizio che il Gestore sottoporrà all'Utente nell'ambito delle operazioni necessarie per il rilascio dell'Identità Digitale, sono indicati gli ulteriori elementi di natura contrattuale derivanti dal rapporto di erogazione del servizio. La documentazione contrattuale, unitamente alle sue successive versioni, sarà resa disponibile nel sito internet del Gestore.

10.1 Obblighi del Gestore

Descrizione obblighi del Gestore
Rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta
Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale
Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione *de visu*
Conservare copia del log della transazione nei casi di identificazione tramite documenti digitali di identità, identificazione informatica tramite altra identità digitale SPID o altra identificazione informatica autorizzata
Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso si identificazione tramite firma digitale
Verifica degli attributi identificativi del richiedente
Consegnare in modalità sicura le credenziali di accesso all'utente
Conservare la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale
Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale
Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al Regolamento 2016/679/UE.
Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione
Effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso
Revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica

Descrizione obblighi del Gestore
Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente
Verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata)
Fornire all'utente che l'ha inviata conferma della ricezione della richiesta di sospensione
Sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni ed informarne il richiedente.
Comunicare all'utente l'approssimarsi della scadenza del proprio documento di riconoscimento chiedendone l'aggiornamento. Sospendere l'identità digitale alla scadenza del documento di riconoscimento dell'utente.
Rispristinare o revocare l'identità digitale sospesa, nei casi previsti
Revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione
Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale
Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso
Effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta
Effettuare con cadenza almeno annuale un'analisi dei rischi
Definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID
Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato
Condurre con cadenza almeno semestrale il *Penetration Test*
Garantire la continuità operativa dei servizi afferenti allo SPID
Effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna
Garantire la gestione sicura delle componenti riservate delle identità digitali assicurando non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata
Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa
Sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti
Informare tempestivamente l'AGID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali
Adeguare i propri sistemi a seguito dell'aggiornamento della normativa

Descrizione obblighi del Gestore
Inviare all'AGID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici.
In caso intendesse cessare la propria attività, comunicarlo all'AGID "e ai titolari" almeno 30 giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali rilasciate
In caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e ne conserva le informazioni
In caso di cessazione dell'attività, scaduti i 30 giorni, revocare le identità digitali rilasciate e per le quali non si è avuto subentro
Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi
Se richiesto dall'utente, segnalargli via email o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso.
Notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale
Nel caso l'identità digitale risulti non attiva per un periodo superiore a 24 mesi o il contratto sia scaduto, revocarla e informarne l'utente via posta elettronica e numero di telefono mobile
In caso di decesso del titolare (persona fisica) o di estinzione della persona giuridica, revocare previo accertamento l'identità digitale
Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.
Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione.
Nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale.
Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.
In caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.
Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa.
All'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta

Descrizione obblighi del Gestore
In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID
Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, adottando idonee misure di sicurezza (ai sensi del Regolamento 2016/679/UE) ed utilizzando meccanismi di cifratura.

10.2 Obblighi dell'Utente

Descrizione obblighi del Titolare dell'Identità Digitale
Esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione
Si obbliga all'uso esclusivamente personale delle credenziali connesse all'Identità Digitale
Si obbliga a non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti. A tale proposito, si precisa che l'utente è tenuto ad adottare tutte le misure tecniche e organizzative idonee ad evitare danni a terzi
Si obbliga a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine
deve garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi
L'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private
Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite
Fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci
Accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze
Informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati
Mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi: • se persona fisica: estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale, • se persona giuridica: indirizzo sede legale, codice fiscale o P.IVA, rappresentante legale della società, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale

Descrizione obblighi del Titolare dell'Identità Digitale
Conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i rischi seguenti: • divulgazione, rivelazione e manomissione • furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale • accertarsi dell'autenticità del fornitore di servizi o del gestore dell'identità digitale quando viene richiesto di utilizzare l'identità digitale
Attenersi alle indicazioni fornite dal Gestore in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele che da adottare per la conservazione e protezione delle credenziali.
In caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali.
In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali.

10.3 Responsabilità

Il Gestore è responsabile verso l'utente per l'adempimento di tutti gli obblighi derivanti dall'espletamento delle attività richieste dalla normativa vigente in materia di Sistema Pubblico di Identità Digitale. In particolare, nello svolgimento della sua attività:

- Attribuisce l'Identità Digitale e rilascia le credenziali connesse attenendosi alle Regole Tecniche emanate dall'AGID.
- Si attiene alle misure di sicurezza previste ai sensi del Regolamento 2016/679/UE (Regolamento europeo in materia di protezione dei dati personali) e s.m.i. nonché alle indicazioni fornite nell'informativa pubblicata sul sito https:\\posteid.poste.it.
- Procede alla sospensione o revoca delle credenziali in caso di richiesta avanzata dall'utente per perdita del possesso o compromissione della segretezza, per provvedimento dell'AGID o su propria iniziativa per acquisizione della conoscenza di cause limitative della capacità dell'utente, per sospetti di abusi o falsificazioni.
- Garantisce i profili di sicurezza delle soluzioni rese via via disponibili, riservandosi di effettuare comunque modifiche tecnico/organizzative ai servizi, ai fini del continuo aggiornamento alle best practices del settore in termini di usabilità e sicurezza. Per tale ragione, gli strumenti di autenticazione di volta in volta disponibili potranno subire modifiche nel corso del tempo o anche essere disattivati.

11 Esclusioni e limitazioni di responsabilità

L'utente è responsabile della correttezza e completezza dei dati necessari per l'attivazione del servizio di Identità Digitale PosteID.

- L'utente assume qualsivoglia responsabilità, in ordine all'utilizzo improprio delle credenziali associate all'Identità Digitale o all'utilizzo delle stesse con forme e modalità difformi dalla normativa vigente e dal Manuale Operativo del Gestore, impegnandosi ad esonerare il Gestore da qualsiasi pretesa o azione da parte di terzi.
- Il Gestore non sarà responsabile per la mancata o non corretta esecuzione degli obblighi su di lui incombenti, in tutti i casi in cui il mancato o non corretto adempimento sia dovuto a cause ad esso non imputabili, quali, a titolo meramente esemplificativo: caso fortuito, forza maggiore, calamità naturali, eventi bellici, furti, interventi dell'autorità.
- Il Gestore non assume alcuna responsabilità per ogni abuso conseguente alla veridicità di tutti i dati comunicati in occasione della richiesta di rilascio dell'Identità Digitale, alla mancata comunicazione da parte dell'utente di ogni variazione intervenuta, con particolare riguardo ai dati che hanno determinato l'attribuzione dell'Identità Digitale ed il rilascio delle credenziali.
- Il Gestore non assume alcuna responsabilità circa il corretto funzionamento e la sicurezza dei dispositivi, hardware e software, utilizzati dall'utente, sul regolare funzionamento di linee elettriche, telefoniche nazionali e/o internazionali.
- Il Gestore è estraneo al rapporto tra l'utente medesimo ed il Fornitore di Servizi, essendo detto rapporto disciplinato esclusivamente dalle relative condizioni contrattuali adottate in assoluta autonomia dal Fornitore di servizi medesimo ed essendo, pertanto, il Gestore estraneo ad ogni eventuale connessa controversia potesse insorgere tra gli stessi. Altresì il Gestore non garantisce in alcun modo l'utente dal rischio di eventuali truffe o da altre eventuali evenienze negative legate al rapporto con il Fornitore di Servizi.

Il Gestore ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi mediante polizza assicurativa delle Responsabilità Civili professionali per l'attività di Gestore di identità del Sistema Pubblico per l'Identità Digitale, stipulata per la copertura dei rischi derivanti da tale attività e dei danni causati a terzi.

Massimale per singolo sinistro	**Massimale per annualità assicurativa dipendente dal numero di identità digitali rilasciate**			
€ 150.000	fino a 100.000 identità	fino 1 milione di identità	fino a 3 milioni di identità	oltre 3 milioni di identità digitali
	7,5 milioni di euro	10 milioni di euro	13 milioni di euro	15 milioni di euro

Requisiti Polizza Assicurativa previsti dal Regolamento di accreditamento

12 Livelli di servizio

Codice	Indicatore di qualità	Modalità funzionamento	Valore limite
IQ-01	Disponibilità del sotto-servizio di registrazione identità	*Erogazione automatica*	>= 99,0%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-02	Tempo di risposta del sotto-servizio di registrazione identità		<= 24h (ore lavorative)
IQ-03	Disponibilità del sotto-servizio di gestione rilascio credenziali	*Erogazione automatica*	>= 99,0%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-04	Tempo di rilascio credenziali		<= 5 giorni lavorativi
IQ-05	Tempo riattivazione delle credenziali		<= 2 giorni lavorativi
IQ-06	Disponibilità del sotto-servizio di sospensione e revoca delle credenziali		>= 99,0%
			Singolo evento di indisponibilità < =6 ore
IQ-07	Tempo di sospensione delle credenziali		< =30 minuti
IQ-08	Tempo di revoca delle credenziali		<= 5 giorni lavorativi
IQ-09	Disponibilità del sotto-servizio di rinnovo e sostituzione delle credenziali	*Erogazione automatica*	>= 99,0%
		Erogazione in presenza	>= 98,0%
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		<= 5 giorni lavorativi
IQ-11	Disponibilità del sotto-servizio di autenticazione		>= 99,0%
			Singolo evento indisponibilità <= 4 ore
IQ-12	Tempo di risposta del sotto-servizio di autenticazione		Tempo di risposta <=3 sec almeno nel 95,0% delle richieste
IQ-13	RPO (*) sotto-servizio registrazione e rilascio delle identità		1 ora
IQ-14	RTO (*) sotto-servizio registrazione e rilascio		8 ore

Codice	Indicatore di qualità	Modalità funzionamento	Valore limite
	delle identità		
IQ-15	RPO (*) sotto-servizio di sospensione e revoca delle credenziali		1 ora
IQ-16	RTO (*) sotto-servizio di sospensione e revoca delle credenziali		8 ore
IQ-17	RPO (*) sotto-servizio di Autenticazione		1 ora
IQ-18	RTO (*) sotto-servizio di Autenticazione		8 ore

***RPO** (*) si intende **Recovery Point Objective** - Rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza. Di conseguenza fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.*

***RTO** (*) si intende **Recovery Time Objective** - Tempo necessario per il pieno recupero dell'operatività di un sistema, a seguito della sua indisponibilità a causa di guasto improvviso.*

13 Sicurezza del servizio PosteID

13.1 Conservazione evidenze per il rilascio dell'Identità Digitale

Al fine di poter documentare la corretta attribuzione di una Identità Digitale PosteID, saranno archiviate nel sistema di conservazione (per una durata pari ad anni venti decorrenti dalla scadenza o dalla revoca dell'identità digitale) le seguenti informazioni, in funzione della modalità di identificazione utilizzata dall'utente.

Modalità di richiesta	Evidenze sottoposte a conservazione
Identificazione "a vista"	Modulo di richiesta del servizio(*) con CGS e consensi privacy. Copia dei documenti utilizzati per l'identificazione (documento di identità e tessera sanitaria/codice fiscale). Log di conferma della richiesta di adesione. Log verifiche effettuate. Identificativo operatore che ha eseguito l'identificazione a vista
Identificazione tramite Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica	Modulo di richiesta del servizio(*) con CGS e consensi privacy. Log del processo di identificazione tramite Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica. Log verifiche effettuate.
Identificazione tramite Firma Digitale	Modulo di richiesta di adesione, firmato digitalmente. Modulo di adesione con CGS e consensi privacy (*). Log verifiche effettuate.
Identificazione mediante strumenti Poste Italiane preesistenti allo SPID	Modulo di richiesta del servizio(*) con CGS e consensi privacy. Log del processo di identificazione tramite strumenti Poste Italiane preesistenti allo SPID. Log verifiche effettuate.
Richiesta da parte di un soggetto rappresentante dotato di Identità Digitale PosteID	Log del processo di identificazione del soggetto rappresentante tramite Identità Digitale PosteID. Modulo di richiesta del servizio(*) con CGS e consensi privacy. Copia dei documenti del soggetto rappresentato (documento di identità e tessera sanitaria/codice fiscale). Copia del documento che attesta la titolarità del

Modalità di richiesta	Evidenze sottoposte a conservazione
	rappresentante ad effettuare la richiesta. Log verifiche effettuate. Identificativo operatore che ha eseguito la verifica della documentazione in backoffice.

(*) I moduli di richiesta del servizio riportano il riferimento alla versione delle Condizioni Generali del Servizio applicabili.

Per quanto riguarda le evidenze relative alla gestione del ciclo di vita dell'identità digitale saranno conservati:

- i log relativi alla modifica di attributi;
- i log relativi alla modifica delle credenziali;
- i documenti e i dati comprovanti la ricezione di un avviso e l'eventuale verifica (qualora lo stesso avviso non sia stato ricevuto da uno dei soggetti da AgID convenzionati) del decesso di un titolare di identità digitale;
- i log per ciascuna richiesta di sospensione credenziali effettuata tramite l'utilizzo del codice di sospensione immediata in dotazione al titolare dell'identità Digitale;
- copia di tutta la documentazione inviata dall'utente per la richiesta di revoca di una identità (modulo di richiesta di revoca sottoscritto, copia del documento di identità, copia della denuncia presentata all'autorità giudiziaria, dove presente).

13.2 Tracciatura degli accessi al servizio di autenticazione

Il Gestore, in aderenza alle Regole Tecniche emanate in attuazione dell'art. 4 del DPCM 24 ottobre 2014, mantiene il *Registro delle transazioni* contenente tracciati delle richieste di autenticazione gestite negli ultimi 24 mesi.

Le registrazioni garantiscono il collegamento per ogni transazione tra codice identificativo dell'Identità Digitale, richiesta di autenticazione generata dal Fornitore di servizi e relativa risposta generata dal Gestore in seguito all'autenticazione dell'utente, mediante le credenziali fornite in fase di rilascio dell'Identità Digitale.

Il Gestore assicura il mantenimento delle tracciature nel rispetto del Codice della Privacy, garantendone l'accesso esclusivamente al personale incaricato.

Per garantire l'integrità dei dati di tracciatura, ad essi viene apposto una marca temporale e una firma elettronica da parte del servizio di gestione dei log delle transazioni.

In particolare per ogni richiesta di autenticazione vengono registrati i seguenti dati:

- codice Identificativo dell'identità digitale attribuito al momento del rilascio dell'identità stessa;

- richiesta di autenticazione, conforme ai protocolli definiti dalle Regole tecniche emessa dal Fornitore di Servizi;
- asserzione di risposta alla richiesta di autenticazione emessa dal Gestore dell'Identità;
- codice identificativo della richiesta di autenticazione emessa dal Fornitore di servizi;
- data e ora della richiesta di autenticazione emessa dal Fornitore di servizi;
- fornitore di servizi che ha sottoposto la richiesta;
- codice identificativo della risposta fornita dal Gestore dell'Identità;
- data e ora della risposta fornita dal Gestore dell'Identità;
- gestore dell'identità che ha fornito la risposta;
- codice identificativo della asserzione di risposta alla richiesta di autenticazione, emessa dal Gestore dell'Identità;
- soggetto che si è autenticato;
- indirizzo univoco Gestore identità.

13.3 Reperimento e presentazione delle informazioni di log

L'AgID, l'utente o in generale i soggetti aventi diritto possono richiedere di ricevere le informazioni inerenti le transazioni, inviando un apposito modulo di richiesta compilato e sottoscritto, corredato di copia del documento di identità, tramite uno dei seguenti canali (in aderenza al DPCM 24 ottobre 2014):

- scansione e invio tramite posta elettronica certificata;
- firma digitale e invio tramite comune posta elettronica;
- invio tramite FAX.

Il modulo disponibile sul sito *https://posteid.poste.it* riporta gli indirizzi di posta o i numeri fi fax a cui vanno inoltrate le richieste.

L'operatore, verifica l'autenticità della richiesta:

- completezza della documentazione necessaria;
- consistenza della documentazione (compilata correttamente, firmata, documento di identità allegato corrispondente al soggetto avente diritto);
- eventuale provenienza della documentazione (indirizzo PEC intestato al soggetto richiedente, in caso di ricezione via PEC);
- eventuale Firma Digitale apposta sul modulo di richiesta (firma intestata al soggetto richiedente).

Il Gestore, effettuate le suddette verifiche, prende in carico la richiesta, che viene così inviata ai sistemi ai fini della sua elaborazione.

I sistemi effettueranno le operazioni necessarie per l'estrazione ed esibizione delle evidenze richieste. In particolare:

- recupero delle evidenze, raggruppando i log per periodo temporale;
- formazione del documento di attestazione delle evidenze;
- trasmissione da parte del Gestore del documento di attestazione.

L'utente, titolare dell'identità, può effettuare la richiesta anche direttamente sul portale web del servizio PosteID.

L'utente può inoltre impostare la funzionalità di comunicazione ad ogni utilizzo delle credenziali.

13.4 Misure anticontraffazione

13.4.1 Misure per il primo livello SPID con sistemi di autenticazione a 1 fattore

Le credenziali di primo livello sono rappresentate dalla password. Le misure previste sono riportate di seguito:

- lunghezza minima di otto caratteri;
- uso di caratteri maiuscoli e minuscoli;
- inclusione di uno o più caratteri numerici;
- non deve contenere più di due caratteri identici consecutivi;
- inclusione di almeno un carattere speciale ad es #, $,% ecc.

La password non deve contenere formati comuni quali, ad esempio, codice fiscale, patente auto, sigle documenti, date, includere nomi, Nome Utente, ecc.

Le password hanno una durata massima pari a 180 giorni e non possono essere riusate, o avere elementi di similitudine, prima di cinque variazioni e comunque non prima di 15 mesi;

13.4.2 Misure per il secondo livello SPID con sistemi di autenticazione a 2 fattori

Per rafforzare l'utilizzo delle credenziali di secondo livello SPID, il sistema notificherà sulla e-mail di contatto scelta dall'utente un "tentativo di accesso" ad un servizio online tramite l'identità, nei seguenti due scenari:

- a seguito di una richiesta di autenticazione tramite app PosteID seguente ad un'installazione dell'app su un nuovo smartphone;
- a seguito di una richiesta di autenticazione, tramite OTP via SMS, da una postazione (PC e Browser) mai utilizzata in passato.[1]

13.4.2.1 App PosteID

Il servizio genera un certificato digitale che viene salvato sul dispositivo dell'utente insieme con la sua chiave privata, in un "ambiente controllato" dell'app PosteID.

L'ambiente controllato è costituito da un'area di memoria sicura a disposizione dell'applicazione, che ne rende i dati e l'esecuzione del codice inaccessibili alle altre applicazioni.

Oltre alle soluzioni di sicurezza offerte in forma nativa dalle piattaforme Android e iOS, l'app PosteID implementa ulteriori meccanismi di protezione del certificato e della chiave privata associata.

All'interno dell'ambiente controllato l'app PosteID crea un "contenitore per la chiave privata" protetto da due meccanismi:

- **Blocco del dispositivo**: al momento della prima installazione del certificato viene generato una "impronta" del dispositivo, combinandone secondo uno specifico algoritmo proprietario alcuni parametri caratteristici (a titolo esemplificativo codice identificativo univoco della scheda WiFi, nome modello dispositivo, numero dispositivo, risoluzione, velocità del processore, ecc.).

  L'"impronta" del dispositivo viene utilizzata come chiave di accesso al "contenitore per la chiave privata", non è salvata sul dispositivo ne' sui server centrali ma viene calcolata ogni volta dall'applicazione.

  Con queste modalità è possibile collegare univocamente il certificato digitale al dispositivo di prima installazione, impedendo che uno stesso certificato possa essere copiato e utilizzato su un dispositivo differente.

- "**Cryptographic camouflage**": la chiave prima di essere salvata nel "contenitore per la chiave privata" viene crittografata con il codice personale, scelto dall'utente e protetta con la tecnologia Cryptographic Camouflage.

  La tecnologia Cryptographic Camouflage, certificata dal NIST (National Institute of Standard and Technology), consente di proteggere la chiave privata contro attacchi informatici di tipo "brute force" basati sul tentativo di decifrarla generando tutte le possibili password fino ad identificare quella corretta.

  La tecnologia Cryptographic Camouflage fa sì che si ottenga un risultato formalmente corretto anche decifrando la chiave privata con una password errata. In questo modo l'unica possibilità per un attaccante di verificarne la correttezza è di utilizzarla tentando di accedere attraverso un processo di autenticazione. Implementando opportuni controlli sul numero di tentavi di inserimento di una password errata, le probabilità che un attaccante riesca a decifrare la chiave privata con un attacco "brute force" sono drasticamente ridotte.

13.4.2.2 Codice di verifica SMS - OTP PosteID[1]

In questo caso le credenziali sono rappresentate dalla password come già descritta al paragrafo

13.4.1 “Misure per il primo livello SPID con sistemi di autenticazione a 1 fattore” e da un codice di verifica a bruciatura (One Time Password – OTP) utilizzabile una sola volta nel periodo di tempo prestabilito.

L’utilizzo del codice di verifica OTP in aggiunta alla password annulla la vulnerabilità legata agli attacchi con replica, garantendo che il codice – anche se intercettato - non potrà più essere riutilizzato per eseguire una autenticazione, in quanto valido solo per il determinato periodo temporale per il quale è stato emesso.

Il codice di verifica OTP è generato dal sistema OTP Generator che utilizza uno specifico algoritmo di sicurezza ed è inviato all’utente sul numero di cellulare certificato. Il codice di verifica SMS - OTP associato univocamente all’utente, una volta generato non è più utilizzabile al di fuori della specifica sessione temporale.

13.5 Sistema di Monitoraggio

Il monitoraggio implementato sui sistemi è orientato a verificare:

- lo stato di efficienza in termini di performance, occupazione di spazi fisici e logici, temperatura ambientale;
- la disponibilità dei sistemi (check di raggiungibilità, controlli sulle connessione attive, ecc.);
- l’esecuzione ed il corretto funzionamento delle applicazioni;
- la sistematica e corretta sincronizzazione dei sistemi con la fonte oraria di riferimento;
- l’assenza di tentativi di accesso non autorizzato;
- che i livelli di servizio siano effettivamente rispettati;
- che i processi di conservazione dei log e delle evidenze siano correttamente eseguiti.

Qualora nel corso delle operazioni di verifica e monitoraggio, il team di gestione rilevi anomalie nel funzionamento del servizio, sono attivate le analisi al fine di comprenderne cause e conseguenze nonché determinare le azioni da intraprendere. Gli eventi significativi che hanno impatto sul servizio sono notificati alla Service Control Room del Gestore dell’Identità Digitale. I cambiamenti di stato dell’evento vengono monitorati e notificati agli attori interessati.

Poste Italiane si avvale di gruppi specialistici per il monitoraggio della sicurezza dei Sistemi informativi che erogano il servizio PosteID.

In particolare sono svolte attività di rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica per mezzo della continua osservazione dell’infrastruttura gestita.

I suddetti eventi/allarmi sono rilevati attraverso piattaforme di Intrusion Prevention atte a difendere applicazioni e dati critici da attacchi avanzati e piattaforme di “Security Information and Event Management” per la raccolta degli eventi di Sicurezza.

Le consolle di monitoraggio sono configurate per il controllo continuo e la produzione di allarmi e

report di sicurezza per le diverse tipologie di controlli effettuati. Con cadenza settimanale è prodotta la reportistica degli eventi verificatisi, al fine di valutare l'efficacia dei controlli attuati.

La struttura Tutela Aziendale Fraud - Management al fine della prevenzione e gestione delle frodi sul canale internet, detiene una soluzione di Adaptive Authentication denominata "Fraud DNA", basata su tecnologia RSA che, in maniera automatica, delinea uno scoring di rischio della sessione di autenticazione al sito "poste.it". Tale score è computato in funzione del riconoscimento del finger print della sessione (caratteristiche tecniche del dispositivo utilizzato: IP, configurazione dei parametri di rete, S.O., browser, …) rispetto al comportamento tipico del cliente archiviato nella kwnoledge base di Poste Italiane. Inoltre è stato integrato nell'infrastruttura Fraud DNA un servizio antimalware fraud detection volto alla rilevazione dell'eventuale presenza di codice malevolo sulla postazione del cliente.

Il sistema cataloga in real time gli accessi ai siti di Poste ma è impostato in modalità "invisible" lato cliente in modo da consentire comunque l'accesso del cliente anche in caso di rilevazione "High Risk". Le attività di monitoraggio ed analisi eseguite successivamente analizzando gli scoring a più alto rischio concretizzano eventualmente il blocco degli account confermati compromessi.

13.5.1 Presidi di Sicurezza

Il Gestore si avvale di gruppi specialistici per il monitoraggio della sicurezza dei sistemi informativi che erogano il servizio PosteID.

L'infrastruttura di sicurezza è costituita dall'insieme dei sistemi e degli apparati adibiti alla protezione dell'ambiente tecnologico ed applicativo dedicato al servizio PosteID, nonché dai meccanismi di protezione dei dati transitano o risiedono sui sistemi.

Sono svolte attività di rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica per mezzo della continua osservazione dell'infrastruttura gestita. I suddetti eventi/allarmi sono visualizzati principalmente attraverso specifiche console di monitoraggio.

Ciascuna console è configurata per monitorare eventi diversi e produrre allarmi e report in funzione della tipologia dei controlli effettuati. Con cadenza settimanale è prodotta la reportistica degli eventi verificatisi al fine di valutare l'efficacia dei controlli attuati.

Le attività di monitoraggio delle componenti di sicurezza attraverso il controllo e l'analisi dei report viene utilizzata anche ai fini della prevenzione degli incidenti di sicurezza. Gli eventi riscontrati sono classificati in funzione della loro gravità e degli impatti che possono avere sugli asset; in relazione a tale classificazione, sono identificate le contromisure idonee a gestire l'evento. Quando dall'evento scaturisce un danno, sono svolte le attività necessarie ad accertare e valutare il danno subito nonché a definire il piano di ripristino.

14 Modalità di protezione dei dati dei titolari

La normativa di riferimento in materia di trattamento dei dati personali è il Regolamento europeo in materia di protezione dei dati personali (Regolamento 2016/679/UE).

Le figure a cui sono attribuiti specifici ruoli e responsabilità nel trattamento dei dati personali sono:

- **Titolare**: Poste Italiane S.p.A., rappresentata dai soggetti indicati nello Statuto (Presidente e Amministratore Delegato); sono Contitolari i Responsabili pro-tempore delle funzioni organizzative di primo livello.
- **Responsabile**: con riferimento ai dati di clienti e fornitori le strutture che riferiscono direttamente ai primi livelli organizzativi (Contitolari), nella persona dei Responsabili pro-tempore.
- **Incaricato**: sono i dipendenti di Poste Italiane e le figure assimilate ex D.Lgs. 276/2003 addetti/e materialmente al trattamento dei dati personali.

Il Titolare è il soggetto cui compete la scelta in ordine alle finalità e modalità del trattamento.

Per ognuna delle strutture di primo livello di Poste Italiane S.p.A. sono individuate le tipologie dei dati trattati e le operazioni di trattamento consentite; l'individuazione è effettuata a livello di funzioni all'interno della singola struttura.

14.1 Ambito del trattamento dei dati personali

Il Gestore delle identità digitali, ai sensi del Regolamento 2016/679/UE, dà al richiedente informativa sui soggetti che effettuano il trattamento dei dati forniti dal richiedente stesso, attraverso quali modalità e per quali finalità questo viene operato, allo scopo di ottenere per tale trattamento espresso assenso.

Il Gestore dell'identità, autentica l'utente ed emette l'asserzione verso il Fornitore di servizi nel rispetto di quanto previsto dalle Regole Tecniche, dalle Modalità Attuative e, più in generale, nel rispetto del Regolamento 2016/679/UE.

14.1.1 Accesso ai dati

Ai dati possono avere accesso solo i dipendenti a ciò autorizzati. La designazione è effettuata anche per categoria, sulla base delle medesime mansioni ricoperte all'interno di una stessa unità organizzativa.

14.2 Sicurezza dei dati

Come previsto dalle norme, il Titolare adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento delle risorse hardware su cui sono registrati e dei locali ove vengono custoditi;
- l'accesso non autorizzato ai dati stessi;
- modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

- l'integrità dei dati, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;
- la disponibilità dei dati, da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi;
- la confidenzialità/riservatezza dei dati, da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

*****QUESTA È L'ULTIMA PAGINA DEL DOCUMENTO*****