Manuale Operativo **PosteID abilitato a SPID**

Sistema Pubblico di Identità Digitale

REDATTO DA: Digital Technology Operations

INDICE

1 INTRODUZIONE AL DOCUMENTO 6

1.1 STORIA DELLE MODIFICHE 6

1.2 LISTA DI DISTRIBUZIONE 9

1.3 SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO 10

1.4 RIFERIMENTI NORMATIVI, STANDARD TECNICI E DEFINIZIONI 10

1.4.1 Riferimenti normativi 10

1.4.2 Standard tecnici 11

1.5 DEFINIZIONI 11

1.6 ACRONIMI E ABBREVIAZIONI 14

2 GENERALITÀ 17

2.1 IDENTIFICAZIONE DEL DOCUMENTO 17

2.2 DATI IDENTIFICATIVI DEL GESTORE 17

2.3 RESPONSABILITÀ DEL MANUALE OPERATIVO 18

2.3.1 Correlazione Manuale operativo Poste Italiane – Regolamento Accreditamento 18

2.3.2 Aggiornamento del Manuale Operativo e notifica ad AgID 19

2.3.3 Sito del servizio, pubblicazione e conformità del Manuale Operativo 19

3 PREMESSA 20

4 DESCRIZIONE DEL SERVIZIO SPID 21

4.1 CARATTERISTICHE GENERALI DEL SERVIZIO 21

4.2 DEFINIZIONE APPLICATIVA DELLE COMPONENTI DEL SERVIZIO POSTEID 23

4.2.1 Modello logico-applicativo del servizio PosteID 23

5 MODALITÀ DI RICHIESTA DEL SERVIZIO POSTEID ABILITATO A SPID PER USO PERSONALE (SPID TIPO 1) E PROFESSIONALE PER PERSONA FISICA (SPID TIPO 3) 26

5.1 REGISTRAZIONE IDENTITÀ POSTEID PER CLIENTI POSTE ITALIANE GIÀ IDENTIFICATI E DOTATI DI STRUMENTI DI IDENTIFICAZIONE ONLINE RILASCIATI DA POSTE ITALIANE 28

5.2 REGISTRAZIONE IDENTITÀ POSTEID PER UTENTI CHE NON DISPONGONO DI STRUMENTI DI IDENTIFICAZIONE ONLINE RILASCIATI DA POSTE ITALIANE 29

5.2.1 Adesione per clienti con Firma Digitale, Carta Nazionale dei Servizi (CNS) attiva o Carta di Identità Elettronica attiva (CIE 2.0, versione non-contactless con lettore, e CIE 3.0 con PIN associato) 29

5.2.2 Adesione per clienti senza strumento di identificazione online 33

5.2.3 Adesione per titolari di strumenti di identificazione informatica preesistenti a SPID rilasciati da Enti Terzi autorizzati da AgID ad operare come GIP 44

5.3 REGISTRAZIONE AL SERVIZIO POSTEID EFFETTUATA DA UN SOGGETTO TUTORE O AMMINISTRATORE DI SOSTEGNO PER I NATI NEL

1998-2004 45
5.4 ANAGRAFICA UTENTE 46
5.5 DOCUMENTI AMMESSI PER L'IDENTIFICAZIONE 48
5.6 RILASCIO CREDENZIALI 53
5.6.1 Credenziali SPID 1 53
5.6.2 Credenziali SPID 2 53
5.6.3 Credenziali SPID 3 54
5.6.4 Conservazione delle evidenze 55
6 AUTENTICAZIONE AI SERVIZI SPID 56
6.1 TIPOLOGIA DI STRUMENTI DI AUTENTICAZIONE POSTEID 56
6.1.1 Strumenti SPID 1 (primo livello SPID) 56
6.1.2 Strumenti SPID 2 (secondo livello SPID) 56
6.1.3 Strumenti SPID 3 (terzo livello SPID) 60
6.2 UTILIZZO DEGLI STRUMENTI DI AUTENTICAZIONE POSTEID 60
6.3 INTERROGAZIONE DEGLI ATTRIBUTI QUALIFICATI DEL TITOLARE DELL'IDENTITÀ DIGITALE 65
6.3.1 Modello Public 65
6.3.2 Modello Protected 66
6.3.3 Modello Private 67
6.4 PROCEDURE DI AGGIORNAMENTO E RECUPERO DELLA PASSWORD 68
6.4.1 Aggiornamento password 69
6.4.2 Recupero della password dimenticata da web e da dispositivo mobile 69
6.4.3 Recupero della password dimenticata tramite Call Center 70
6.4.4 Cambio password obbligatorio a scadenza 71
6.4.5 Procedura in caso di perdita dei fattori di sicurezza utili ad assicurare la titolarità del richiedente ad effettuarne il recupero 71
6.5 AMBITI DI UTILIZZO DI POSTEID 72
6.6 MESSAGGI DI ANOMALIA 72
7 GESTIONE DEL CICLO DI VITA DELL'IDENTITÀ DIGITALE 75
7.1 PAGAMENTO DEL CORRISPETTIVO PERIODICO PER L'UTILIZZO DELLA FUNZIONALITÀ DI AUTENTICAZIONE SUL CIRCUITO SPID 75
7.1.1 Rinnovo da casa, tramite accesso all'area personale del titolare 75
7.1.2 Rinnovo da casa, senza accesso all'area personale del titolare 76
7.1.3 Rinnovo in Ufficio Postale 76
7.2 SOSPENSIONE 77
7.2.1 Sospensione immediata tramite il servizio web 77
7.2.2 Sospensione immediata tramite il servizio Interactive Voice Response 77
7.2.3 Riattivazione delle credenziali sospese 78
7.3 REVOCA 79

7.3.1 Richiesta di revoca credenziali e recesso dal servizio PosteID ... 79
7.3.2 Revoca o sospensione dell'identità digitale su iniziativa del Gestore ... 80
7.4 BLOCCO TEMPORANEO DEL PROFILO ... 80
7.5 RICHIESTA DI DISASSOCIAZIONE DEL NUMERO DI CELLULARE DA ALTRA IDENTITÀ DIGITALE ... 81
8 IDENTITÀ DIGITALE PER TITOLARI MINORENNI (SPID TIPO 1) ... 83
8.1 RICHIESTA DI RILASCIO SPID IN FAVORE DI UN MINORE ... 83
8.2 ATTIVITÀ IN CAPO AL MINORE ... 85
8.3 SINTESI DELLA DOCUMENTAZIONE DA PRESENTARE IN UFFICIO POSTALE ... 88
8.4 UTILIZZO DELL'IDENTITÀ DEL MINORE ... 89
8.4.1 Autenticazione da parte del minore ... 89
8.4.2 Autorizzazione del Genitore richiedente all'accesso ai servizi aderenti a SPID ... 90
8.4.3 Effetti della cessazione dell'identità digitale del Genitore richiedente ... 91
8.4.4 Conservazione dei log di accesso ... 91
8.5 CICLO DI VITA DELL'IDENTITÀ DEL MINORE ... 91
8.5.1 Sospensione e riattivazione ... 91
8.5.2 Revoca ... 92
8.5.3 Compimento del 18esimo anno di età ... 92
8.6 ASSISTENZA CLIENTI PER IL MINORE ... 93
9 ABILITAZIONE DELL'IDENTITÀ DIGITALE ALL'USO PROFESSIONALE PER PERSONE FISICHE (SPID TIPO 3) ... 94
9.1 RICHIESTA ... 94
9.1.1 Identificazione ... 94
9.1.2 Indicazione attributi relativi all'uso professionale, verifica contatti e configurazione del servizio ... 94
9.1.3 Presa visione delle condizioni generali del servizio e dell'informativa privacy ... 96
9.1.4 Pagamento del servizio ... 96
9.1.5 Conservazione delle evidenze ... 96
9.2 UTILIZZO E CICLO DI VITA DELL'ABILITAZIONE ALL'USO PROFESSIONALE ... 97
9.3 RINNOVO USO PROFESSIONALE ... 98
9.4 RECESSO ANTICIPATO DALL'ABILITAZIONE DELL'USO PROFESSIONALE ... 99
10 MODALITÀ DI RICHIESTA DEL SERVIZIO DI IDENTITÀ DIGITALE SPID AD USO PROFESSIONALE PER PERSONA GIURIDICA (SPID TIPO 4) ... 101
10.1 RICHIESTA DEL SERVIZIO E ATTIVAZIONE DELLE ID SPID AD USO PROFESSIONALE PER PERSONA GIURIDICA ... 102
10.1.1 Registrazione dell'organizzazione e del Rappresentante legale richiedente ... 102
10.1.2 Identificazione del Rappresentante legale richiedente ... 103
10.1.3 Attivazione del servizio e identificazione del Referente di governo e del Referente di gestione ... 104
10.1.4 Funzionalità a disposizione del Referente di governo per il censimento di nuovi utenti ... 105
10.1.5 Funzionalità a disposizione degli utenti per l'identificazione senza operatore ... 106
10.1.6 Funzionalità a disposizione del Referente di gestione per l'identificazione con operatore di nuovi utenti

107
10.1.7 Conservazione delle evidenze ... 108
10.2 UTILIZZO E CICLO DI VITA DELL'ID SPID AD USO PROFESSIONALE PER PERSONA GIURIDICA ... 108
10.2.1 Operatività dell'Utilizzatore finale ... 108
10.2.2 Operatività del Referente di governo sulle ID associate all'organizzazione ... 109
10.3 RINNOVO DEL SERVIZIO DI ID SPID AD USO PROFESSIONALE PER PERSONA GIURIDICA ... 109
10.4 RECESSO ANTICIPATO DAL SERVIZIO DI ID SPID AD USO PROFESSIONALE PER PERSONA GIURIDICA ... 110
11 RAPPORTI CON GLI UTENTI ... 112
12 CONDIZIONI DI FORNITURA ... 113
13 OBBLIGHI E RESPONSABILITÀ ... 115
13.1 OBBLIGHI DEL GESTORE ... 115
13.2 OBBLIGHI DELL'UTENTE ... 118
13.3 RESPONSABILITÀ ... 119
14 ESCLUSIONI E LIMITAZIONI DI RESPONSABILITÀ ... 120
15 LIVELLI DI SERVIZIO ... 121
16 SICUREZZA DEL SERVIZIO POSTEID ABILITATO A SPID ... 124
16.1 CONSERVAZIONE EVIDENZE PER IL RILASCIO DELL'IDENTITÀ DIGITALE ... 124
16.2 TRACCIATURA DEGLI ACCESSI AL SERVIZIO DI AUTENTICAZIONE ... 127
16.3 REPERIMENTO E PRESENTAZIONE DELLE INFORMAZIONI DI LOG ... 128
16.4 MISURE ANTICONTRAFFAZIONE ... 128
16.4.1 Misure per SPID 1 (primo livello SPID) ... 128
16.4.2 Misure per SPID 2 (secondo livello SPID) ... 129
16.4.3 Misure per SPID 3 (terzo livello SPID) ... 131
16.5 SISTEMA DI MONITORAGGIO ... 131
16.5.1 Presidi di Sicurezza ... 133
17 MODALITÀ DI PROTEZIONE DEI DATI DEI TITOLARI ... 134
17.1 AMBITO DEL TRATTAMENTO DEI DATI PERSONALI ... 134
17.1.1 Accesso ai dati ... 134
17.2 SICUREZZA DEI DATI ... 135

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 (§ 13) - Aggiornati livelli di servizio (§ 15) - Aggiornate evidenze conservate nell'identificazione a vista (§ 16.1) - Integrato monitoraggio sull'utilizzo delle credenziali (§ 16.5)	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 §16.4.2 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 autorizzati da AgID - Aggiornamento sugli strumenti di autenticazione di Livello 2 SPID resi disponibili ai clienti del Servizio	DTO_SPID_PI_004_v2.0
18/05/2018	2.1	- Introduzione riferimenti al Regolamento 2016/679/UE (GDPR) - Aggiornamento pagina posteid.poste.it	DTO_SPID_PI_004_v2.1
30/09/2018	2.2	- Estensione della procedura di richiesta dell'identità digitale ad opera di un tutore/amministratore di sostegno ai nati negli anni 2000 e 2001 - Descrizione procedura di adesione in ufficio postale	DTO_SPID_PI_004_v2.2
09/11/2018	2.3	- Descrizione soluzione SPID 3	DTO_SPID_PI_004_v2.3
10/12/2018	2.4	- Aggiornamento nominativo del Responsabile del Manuale Operativo - Descrizione procedura di identificazione tramite documento elettronico	DTO_SPID_PI_004_v2.4
18/01/2019	2.5	- Aggiornamento sugli strumenti di autenticazione di Livello 2 SPID resi disponibili ai clienti del Servizio	DTO_SPID_PI_004_v2.5
21/02/2019	2.6	- Aggiornamento numero telefonico di assistenza	DTO_SPID_PI_004_v2.6
29/10/2019	2.7	- Chiarimento modalità di utilizzo delle credenziali di sicurezza	DTO_SPID_PI_004_v2.7

22/11/2019	2.8	- Descrizione procedura di identificazione tramite CIE 3.0 con PIN	DTO_SPID_PI_004_v2.8
19/12/2019	2.9	- Modifiche alle condizioni di fornitura	DTO_SPID_PI_004_v2.9
18/03/2020	3.0	- Estensione procedure di identificazione con documento elettronico a dispositivi mobili iOS - Introduzione procedura di identificazione tramite R.A.O. pubblico	DTO_SPID_PI_004_v3.0
29/10/2020	3.1	- Introduzione procedura di identificazione da remoto con bonifico - Descrizione procedura di disassociazione del numero di cellulare in fase di registrazione	DTO_SPID_PI_004_v3.1
27/11/2020	3.2	- Chiarimenti disponibilità credenziali SPID 2	DTO_SPID_PI_004_v3.2
12/03/2021	3.3	- Descrizione ulteriore modalità di utilizzo della credenziale SPID 2 App (§6 e §16.4.2)	DTO_SPID_PI_004_v3.3
30/06/2021	3.4	- Descrizione funzionalità di abilitazione dell'ID all'uso professionale per persone fisiche (§8)	DTO_SPID_PI_004_v3.4
23/11/2021	3.5	- Disabilitazione della modalità di identificazione tramite Lettore Bancoposta (§5) - Modalità di richiesta del servizio attraverso funzionalità opzionali aggiuntive (§5) - Descrizione dell'utilizzo del c.d. deeplink in scenario di login su browser mobile (§6.1.2) - Procedura in caso di perdita di tutti i fattori di sicurezza utili ad assicurare la titolarità del richiedente ad effettuarne il recupero (§6.4.5)	DTO_SPID_PI_004_v3.5
21/02/2022	3.6	- Aggiornamento numero di assistenza telefonica	DTO_SPID_PI_004_v3.6
27/06/2022	3.7	- Identità Digitale per titolari minorenni (§8)	DTO_SPID_PI_004_v3.7
21/07/2022	3.8	- Capability OpenID Connect (§6.2)	DTO_SPID_PI_004_v3.8
11/10/2022	3.9	- Aggiornamento definizioni - Prospetto documenti ammessi per l'identificazione (§5.5) - Descrizione modelli di interrogazione dei Gestori di attributi qualificati (§6.3)	DTO_SPID_PI_004_v3.9
15/05/2023	4.0	- Aggiornamento procedura di recupero della password (reset) (§6.4.2 e §6.4.3)	DTO_SPID_PI_004_v4.0
28/06/2023	4.1	- Requisiti minimi tecnici per l'installazione e l'utilizzo dell'app PosteID (§1.5)	DTO_SPID_PI_004_v4.1
18/10/2023	4.2	- Aggiornamento funzionalità per gestione delle app installate (§6.1.2) - Aggiornamento con descrizione della procedura di rinnovo del certificato SPID 3 (§6.1.3) - Aggiornamento procedura di recupero della password (reset) (§6.4.2) - Estensione fattispecie di revoca (§7.2.1) - Aggiornamenti sulle comunicazioni all'utente connesse all'utilizzo dell'ID (§16.4)	DTO_SPID_PI_004_v4.2
03/11/2023	4.3	- App e dispositivi associati all'ID (§6.1.2)	DTO_SPID_PI_004_v4.3

30/11/2023	4.4	- Sospensione temporanea identificazioni tramite CNS (§5.2.1.2)	DTO_SPID_PI_004_v4.4
26/02/2024	4.5	- Aggiornamento procedura di revoca (§7.2.1) - Aggiornamento procedure di utilizzo dell'abilitazione all'uso professionale per persone fisiche (§9.2)	DTO_SPID_PI_004_v4.5
08/04/2024	4.6	- Aggiornamento controlli in fase di identificazione tramite identità preesistenti di Poste Italiane (§5.1) e tramite firma digitale (§5.2.1)	DTO_SPID_PI_004_v4.6
31/07/2024	4.7	- Innalzamento versione minima iOS da 11 a 12 - Descrizione del servizio di identità digitale SPID ad uso professionale per persona giuridica (SPID Tipo 4) (§10)	DTO_SPID_PI_004_v4.7
16/10/2024	4.8	- Aggiornamento lista documenti ammessi per l'identificazione (§5.5) - Aggiornamento Livelli di Servizio (§15)	DTO_SPID_PI_004_v4.8
18/04/2025	4.9	- Innalzamento versione minima iOS da 12 a 13 - Aggiornamento lista documenti ammessi per l'identificazione (§5.5)	DTO_SPID_PI_004_v4.9
09/07/2025	5.0	- Innalzamento versione minima iOS da 13 a 14 - Innalzamento versione minima Android da 4.4 a 5 - Correzione refuso (§5.1) - Correzione refuso (§15)	DTO_SPID_PI_004_v5.0
14/11/2025	5.1	- Innalzamento versione minima Android da 5 a 8 - Descrizione introduzione corrispettivo periodico per l'utilizzo della funzionalità di autenticazione sul circuito SPID (§7.1 e §12) - Aggiunta indicazioni puntuali (§8 e §15)	DTO_SPID_PI_004_v5.1
27/01/2026	5.2	- Controlli "unfair use" su app PosteID (§6.1.2)	DTO_SPID_PI_004_v5.2
08/05/2026	5.3	- Innalzamento versione minima sistemi operativi mobili (§1.5) - Aggiunta indicazioni puntuali su fonti autoritative (cfr. §1.5 e §5) - Aggiornamento su modalità di richiesta rafforzata con bonifico (cfr. §5.2.2.5) - Aggiornamento su ammissibilità della carta di identità cartacea (cfr. §5.5) - Correzione refusi e allineamenti con Guida Utente (cfr. §7.3)	DTO_SPID_PI_004_v5.3

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 di 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

Codice dell'Amministrazione Digitale	Il Codice dell'Amministrazione Digitale (CAD) è un testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza 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 o Gestore di attributi	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 (GIP)	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.*
R.A.O.	Registration Authority Office. Ente Terzo, pubblico o privato, è stato autorizzato da AgID ad effettuare identificazioni de-visu a norma SPID.
Fonti autoritative	Sistemi pubblici di riscontro di dati, messi a disposizione del Gestore d'Identità tramite AgID, per la verifica delle informazioni fornite dal cittadino in fase di richiesta dell'identità digitale o in fase di gestione del ciclo di vita del profilo SPID. In particolare: Agenzia delle Entrate, SCIPAFI, Anagrafe Nazionale della Popolazione Residente (ANPR).

Attori del Sistema Pubblico di 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.

App PosteID	Applicazione mobile, utilizzabile dal titolare di Identità Digitale PosteID abilitato a SPID per effettuare autenticazioni di livello SPID 2 e SPID 3 e per consultare i propri dati di registrazione, previa installazione su smartphone / tablet compatibili e associazione dell'app alla propria identità digitale. Di seguito i requisiti minimi dei dispositivi mobili (smartphone / tablet) - per l'installazione e l'utilizzo dell'app PosteID: Android 9.0 o superiore, iOS 16 o superiore; - per quanto concerne l'utilizzo dell'impronta digitale: Android 9.0 o superiore e lettore di impronta, iOS 16 o superiore e lettore d'impronta; - per quanto concerne l'utilizzo dell'impronta facciale: Android 9.0 o superiore e sensore di riconoscimento della fisionomia del volto, iOS 16 o superiore e sensore di riconoscimento della fisionomia del volto; - funzione NFC, per la lettura dei documenti elettronici.
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.
SPID Tipo 1	Identità digitale SPID ad uso personale, destinata all'utente che accede a servizi per il cittadino e che attesta i propri attributi identificativi e di contatto personali.
SPID Tipo 3	Identità digitale SPID ad uso professionale per persona fisica, destinata all'utente che accede a servizi di tipo professionale e che attesta attributi identificativi e di contatto professionali collegati alla propria attività.

SPID Tipo 4	Identità digitale SPID ad uso professionale per persona giuridica, destinata al rappresentante, dipendente o collaboratore di un'organizzazione che accede a servizi di tipo professionale e che attesta attributi identificativi e di contatto collegati ad un'organizzazione.
Referente di governo	"Utente di governo" descritto nella LL.GG. AgID relative all'ID SPID Tipo 4
Referente di gestione	"Utente di gestione" descritto nella LL.GG. AgID relative all'ID SPID Tipo 4
Documento di riconoscimento	Documento di identità (carta d'identità o passaporto o patente), rilasciato da un'Autorità Italiana, che abbia una validità residua di almeno 1 mese.
Documento di riconoscimento elettronico	Documento dotato di un microchip all'interno del quale sono contenute le informazioni personali del titolare (dati anagrafici, foto, et al.). Ad es. Carta d'Identità Elettronica (CIE) e Passaporto Elettronico, rilasciati da un'Autorità Italiana.
Documento di attestazione del codice fiscale	Tessera o certificato che attestano il codice fiscale del cittadino. Per conoscere la lista di documenti ammissibili per l'attestazione del codice fiscale ai sensi dei regolamenti SPID, fare riferimento alla tabella presente al §5.5
Area riservata o area personale	Area di post-login sul sito https://posteid.poste.it all'interno della quale il cliente può gestire il ciclo di vita della propria identità digitale SPID, può richiedere l'abilitazione di nuove funzionalità o servizi a valore aggiunto e può gestire il controllo parentale sull'attività di minori a sé collegati.
Minore o minorenne	Soggetto che non ha compiuto 18 anni di età. NB: ai fini del rilascio dell'identità digitale SPID, è ammessa la richiesta per i minori con almeno 5 anni di età.
Genitore richiedente o Genitore	Il soggetto che esercita la responsabilità genitoriale sul minore e che chiede il rilascio di SPID in favore di quest'ultimo.
Genitore non richiedente o Secondo genitore	Altro soggetto che esercita la responsabilità genitoriale sul minore.

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. Il formato dell'AccountID è un indirizzo e-mail valido, la cui esistenza e disponibilità sono verificate dal servizio. NB: tale indirizzo e-mail può essere sostituito nel tempo con altro indirizzo e-mail, ma rimane legato al primo utilizzatore che l'ha verificato sul servizio (tramite codice fiscale). In caso quindi di sostituzione volontaria oppure a seguito di una revoca dell'identità e successiva richiesta di nuova identità, un indirizzo già utilizzato può essere ri-utilizzato solo dal cittadino (codice fiscale) che per primo l'ha verificato sul servizio

Android	Sistema operativo per dispositivi mobili quali smartphone e tablet, sviluppato dalla società Google
App	Applicazione software per smartphone/tablet
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 e Condizioni Economiche
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 livelli 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
MRZ	Machine Readable Zone (MRZ) è un codice alfa-numerico contenente una sequenza di caratteri su più righe. Tale sequenza può essere letta da appositi lettori al fine di agevolare la lettura dei dati contenuti all'interno del documento elettronico
NFC	Tecnologia che fornisce connettività senza fili bidirezionale a corto raggio (fino a un massimo di 10 cm)
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
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
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
SP	Service Provider - Il Fornitore di servizi, come indicato nelle definizioni
SPID 1 **SPID 2** **SPID 3**	Livelli di sicurezza regolati all'interno del Sistema Pubblico di Identità Digitale e corrispondenti, rispettivamente a EU LoA2, EU LoA3, EU LoA4 dello standard ISO/IEC DIS 29115
TS-CNS	Tessera Sanitaria-Carta Nazionale dei Servizi
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	Marco
COGNOME	De Iacovo
TELEFONO	06 59581
E-MAIL	responsabilemanualeposteid@posteitaliane.it

Dati identificativi del Responsabile del Manuale Operativo

2.3.1 Correlazione Manuale operativo Poste Italiane – 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	§ 6.6
Livelli di servizio garantiti per le diverse fasi della registrazione e della gestione del ciclo di vita delle identità	§ 15
Livelli di servizio garantiti per le diverse fasi del processo di autenticazione	§ 15
Descrizione dei contenuti delle tracciature degli accessi al servizio di autenticazione e delle modalità di acquisizione ai fini dell'opponibilità a terzi	§ 16.2
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; § 8; § 9; § 10
Descrizione dei metodi di gestione dei rapporti con gli utenti	§ 11
Descrizione generale delle misure anti-contraffazione	§ 16.4

Contenuto Regolamento accreditamento	Riferimento manuale operativo
Descrizione generale del sistema di monitoraggio	§ 16.5
Definizione degli obblighi del Gestore e dei titolari dell'identità digitale	§ 13
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 di 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

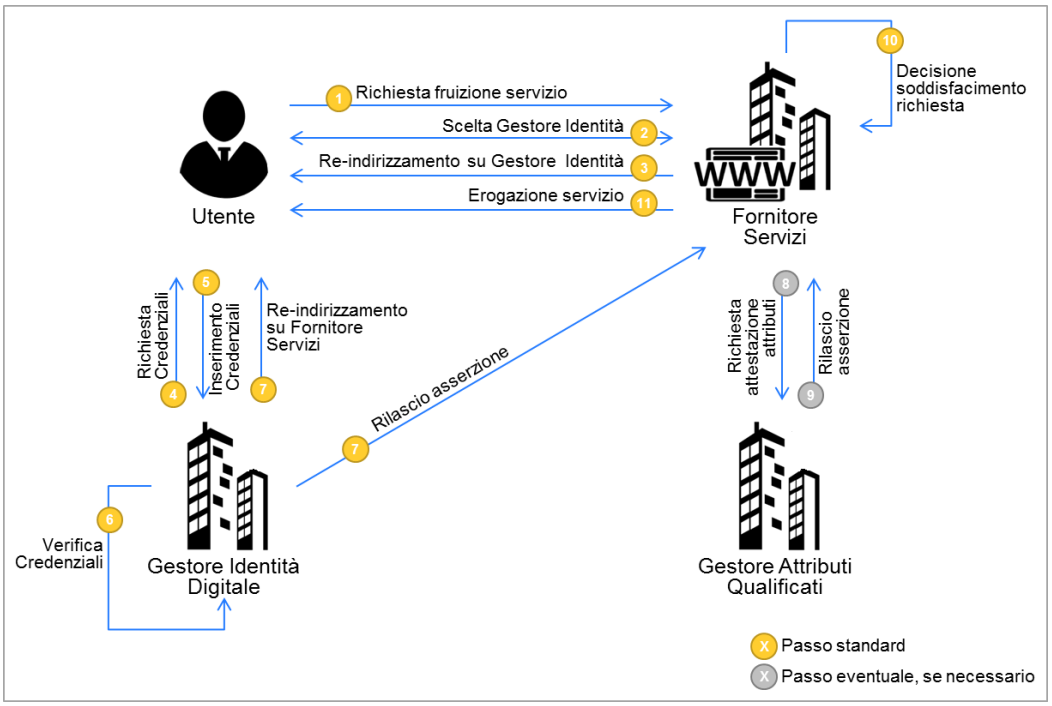
Il Sistema Pubblico di Identità Digitale (SPID) è definito dall'articolo 64 del Codice per l'Amministrazione Digitale per l'accesso ai dati ed ai servizi online erogati dalle Pubbliche Amministrazioni e dai Fornitori di servizi privati.

Al Sistema partecipano i seguenti attori:

- Gestori dell'Identità Digitale;
- Gestori di Attributi Qualificati (ad es: Ordini e collegi professionali, CC.I.AA., etc.);
- 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 di 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 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.

- **SPID 1 (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.
- **SPID 2 (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.

- **SPID 3 (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.

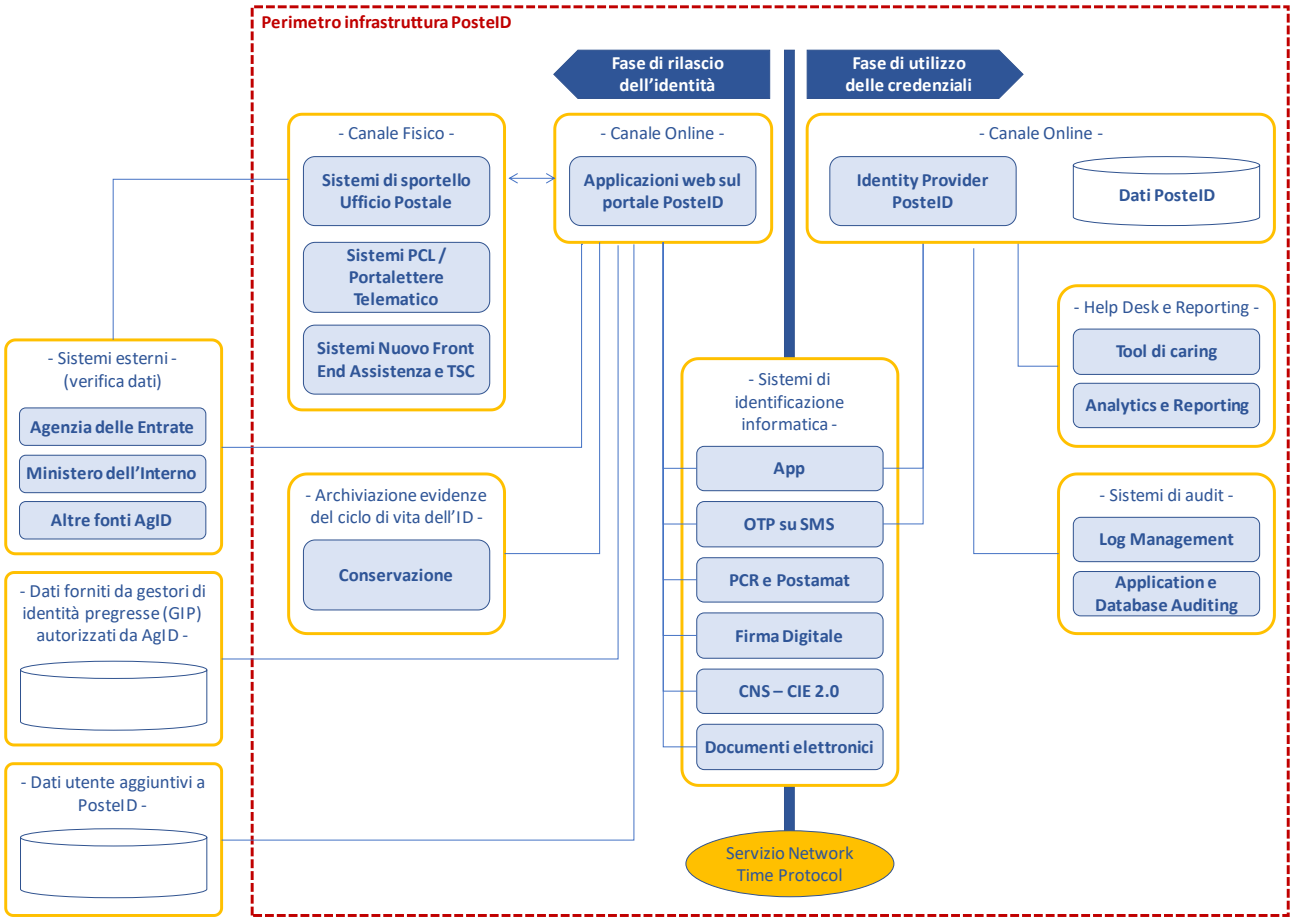
I Fornitori di servizi pubblici/privati attribuiscono i livelli di sicurezza necessari per l'accesso ai propri servizi.

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 di 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 e Condizioni Economiche, 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 e Condizioni Economiche 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 o conformi alle regole tecniche/linee guida via via emesse dall'Agenzia per l'Italia Digitale. 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

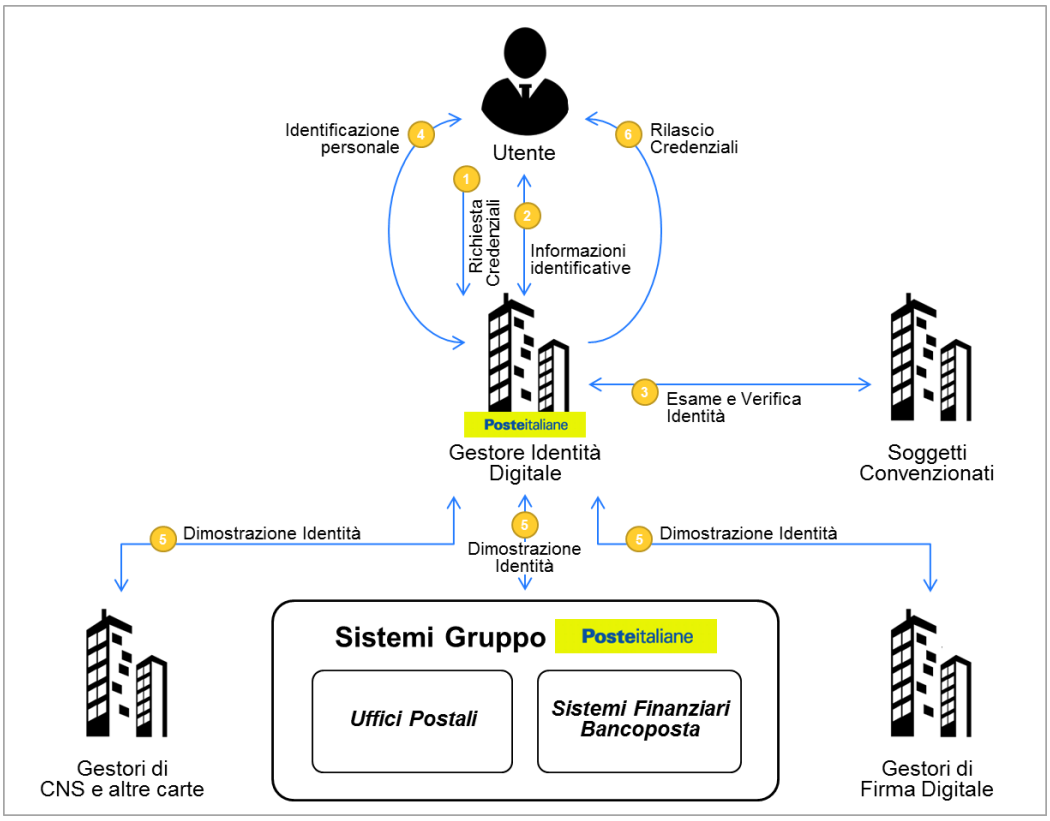
monitoraggio delle applicazioni e dei sistemi che gestiscono i dati.

- **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 e-mail 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 PosteID abilitato a SPID per uso personale (SPID Tipo 1) e professionale per persona fisica (SPID Tipo 3)

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)[1];

[1] La modalità di identificazione tramite "Lettore Bancoposta" è stata disabilitata nel mese di dicembre 2021

  - 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 (CNS) attiva oppure Carta di Identità Elettronica attiva (CIE 2.0, versione non-contactless con lettore);
- identificazione "a vista":
  - con richiesta online dell'identità digitale e riconoscimento "de-visu" in ufficio postale;
  - con richiesta dell'identità digitale e contestuale riconoscimento "de-visu" in ufficio postale, e successiva finalizzazione online dell'adesione;
  - con richiesta online dell'identità digitale e riconoscimento "de-visu" a domicilio mediante portalettere;
  - con richiesta dell'identità digitale via App PosteID, tramite lettura di un documento elettronico e successiva verifica da parte di operatori di back-office;
  - con richiesta dell'identità digitale via App PosteID, tramite presentazione di documenti di riconoscimento, disposizione di un bonifico e successiva verifica da parte di operatori di back-office;
  - con richiesta dell'identità digitale e contestuale identificazione effettuata presso uno sportello della Pubblica Amministrazione accreditato come Registration Authority Office (R.A.O.) e successivo completamento online della registrazione.
- richiesta di PosteID online ad opera di un tutore/amministratore di sostegno che opera in nome e per conto del soggetto tutelata nato tra il 1998 ed il 2004, con identificazione mediante la verifica dei dati anagrafici del titolare inseriti sul portale e della copia della sua tessera sanitaria/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 e dei servizi di Poste Italiane abilitati.

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 nella maschera di conferma;
- della **e-mail del richiedente**, attraverso l'invio di un codice OTP che viene inserito dall'utente nella maschera di conferma oppure attraverso l'invio sulla e-mail indicata di un link (token) che l'utente dovrà cliccare.

Prima del rilascio dell'identità digitale a una persona fisica, sono verificati i dati identificativi del richiedente, ivi inclusi ove disponibili, il domicilio digitale o altro indirizzo di contatto, mediante consultazione dei dati disponibili presso l'ANPR di cui all'articolo 62 del D.lgs. 82/2005. Tali verifiche

sono svolte anche successivamente al rilascio dell'identità digitale, con cadenza almeno annuale, anche ai fini della verifica dell'esistenza in vita.

Ai sensi di quanto previsto nelle Condizioni Generali del Servizio e Condizioni Economiche, alcune modalità di verifica dell'identità per il rilascio dell'identità digitale PosteID abilitato a SPID possono essere a pagamento. L'avvenuto pagamento, nei casi previsti, è condizione necessaria affinché Poste Italiane possa procedere con la successiva attivazione del servizio e all'abilitazione all'operatività sul circuito SPID.

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

In questo caso il cliente è stato già identificato, preliminarmente al rilascio degli strumenti di identificazione informatica, mediante esibizione del documento di identità. 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[2]:

- 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, la Carta Nazionale dei Servizi (CNS) attiva oppure la Carta di Identità Elettronica attiva, in versione non-contactless con lettore), 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 Italiane.

NB: Poste Italiane si riserva di applicare eventuali ulteriori controlli sui dati che, in specifici scenari, potrebbero inibire l'utilizzo di questa modalità. Il richiedente avrà comunque la possibilità di selezionare una modalità alternativa di identificazione tra quelle tempo per tempo disponibili.

[2] La modalità di identificazione tramite "Lettore Bancoposta" è stata disabilitata nel mese di dicembre 2021

Conferma dati, verifica contatti e configurazione del servizio

L'utente:

- inserisce come proprio Nome Utente un indirizzo e-mail 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 15.4 "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 3, 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 e Condizioni Economiche, 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 Adesione per clienti con Firma Digitale, Carta Nazionale dei Servizi (CNS) attiva

o Carta di Identità Elettronica attiva (CIE 2.0, versione non-contactless con lettore, e CIE 3.0 con PIN associato)

L'utente, collegandosi al portale PosteID (https://posteid.poste.it), viene guidato nella scelta di una delle procedure di registrazione online disponibili, sulla base dello strumento di identificazione in suo possesso. Di seguito i passaggi previsti per i singoli strumenti.

5.2.1.1 Adesione per clienti con Firma Digitale

Identificazione

L'utente si identifica online attraverso lo strumento Firma Digitale. L'identificazione viene eseguita alla conclusione della procedura di registrazione, attraverso la firma del modulo di richiesta di adesione.

NB1: Poste Italiane si riserva di applicare eventuali ulteriori controlli sui dati che, in specifici scenari, potrebbero inibire l'utilizzo di questa modalità. Il richiedente avrà comunque la possibilità di selezionare una modalità alternativa di identificazione tra quelle tempo per tempo disponibili.

NB2: *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" non sarà disponibile, poiché l'utilizzo di tale strumento non è fruibile con le apparecchiature mobili.*

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 e-mail 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 15.4 "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 3, 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 e Condizioni Economiche, 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 Adesione per clienti con Carta Nazionale dei Servizi (CNS) attiva o Carta di Identità Elettronica attiva (CIE 2.0, versione non-contactless) [*MODALITA' TEMPORANEAMENTE SOSPESA*]

Identificazione

L'utente si identifica online attraverso lo strumento Carta Nazionale dei Servizi (o Tessera Sanitaria-Carta Nazionale dei Servizi) oppure Carta di Identità Elettronica attiva (CIE 2.0, versione non-contactless con lettore).

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 "Carta Nazionale dei Servizi o Carta d'Identità Elettronica" non sarà disponibile, poiché l'utilizzo di tali strumenti non è fruibile con le apparecchiature mobili.*

Inserimento/conferma dei dati

L'utente:

- inserisce come proprio Nome Utente un indirizzo e-mail 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 15.4 "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 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 3, 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 e Condizioni Economiche, 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.

5.2.1.3 Adesione per clienti con Carta di Identità Elettronica (CIE 3.0) in possesso del PIN associato

Identificazione

L'utente che dispone di:

- una Carta di Identità Elettronica (CIE 3.0, versione contactless),
- PIN associato alla CIE 3.0[3],
- uno smartphone/tablet con tecnologia NFC attiva,

può scegliere di avviare la propria adesione dall'App PosteID, dopo averla scaricata sul proprio dispositivo mobile dallo store Google Play o da Apple Appstore. NB: *la modalità di seguito descritta non è disponibile per smartphone / tablet con sistema operativo iOS in versione inferiore a 13 e non abilitati all'utilizzo di NFC*.

L'utente seleziona sull'App PosteID la procedura di adesione mediante documento elettronico e seguendo passo dopo passo la procedura guidata:

- sceglie se utilizzare la propria Carta di Identità Elettronica o il proprio Passaporto Elettronico;
- sceglie di utilizzare la Carta di Identità Elettronica con digitazione del PIN;
- digita il PIN sulla maschera in App;
- avvicina il documento elettronico al dispositivo mobile, per attivare la lettura, tramite tecnologia NFC, dei dati contenuti nella memoria elettronica del chip. La lettura prevede l'acquisizione di un certificato di autenticazione, sul quale vengono effettuate le opportune verifiche di autenticità e validità sulle fonti autoritative[4];
- sceglie se proseguire la procedura di registrazione sul dispositivo mobile oppure se collegarsi

[3] In caso di smarrimento del PIN sarà necessario richiederne la ristampa presso il Comune di emissione della CIE. In caso di blocco per numero di tentativi errati consecutivi, sarà necessario utilizzare il codice PUK consegnato al momento dell'emissione della CIE, oppure in caso di smarrimento dello stesso richiederne la ristampa presso il Comune di emissione della carta di identità elettronica.

[4] Nell'ambito del processo di registrazione, tramite la lettura del microchip del documento elettronico, il sistema verifica sulla "certificate revocation list" pubblicata dall'Autorità emittente la validità della firma tecnica e l'eventuale presenza del certificato associato alla firma nella lista di revoca, impedendo l'attivazione dell'Identità nel caso in cui fossero rilevate delle anomalie.

da un computer, utilizzando un codice temporaneo, valido per 30 minuti, che dovrà digitare su apposita pagina del sito https://posteid.poste.it.

Scelta credenziali e compilazione attributi secondari

Proseguendo sulle pagine di registrazione, indifferentemente da dispositivo mobile o da computer, l'utente:

- inserisce come proprio Nome Utente un indirizzo e-mail 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 15.4 "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;
- verifica i propri dati identificativi già presenti nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- inserisce 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 3, 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 e Condizioni Economiche, 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 ad avviare i controlli sulle fonti autoritative, il cui superamento è necessario per all'attivazione dell'Identità Digitale e delle credenziali associate.

5.2.2 Adesione per clienti senza strumento di identificazione online

L'utente, collegandosi al portale PosteID (https://posteid.poste.it), viene guidato nella scelta di una delle procedure di registrazione con identificazione "a vista" disponibili. L'utente può effettuare l'identificazione e certificazione del numero cellulare negli uffici postali abilitati oppure a domicilio mediante portalettere. Di seguito i passaggi previsti nelle diverse modalità.

5.2.2.1 Richiesta online e successiva identificazione in ufficio postale

Pre-registrazione

L'utente che non dispone di strumenti di identificazione online e sceglie di avviare la propria adesione sul sito https://posteid.poste.it :

- 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 e-mail 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 15.4 "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 3, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6;
- sceglie di essere identificato in un ufficio postale portando con sé documento di riconoscimento inserito a sistema e tessera sanitaria/codice fiscale, richiedendo all'operatore di effettuare la loro scansione.

Accettazione condizioni generali del servizio

L'utente accetta le Condizioni Generali del Servizio e Condizioni Economiche 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"*).

Identificazione a vista presso l'ufficio postale

L'identificazione a vista viene eseguita presso gli sportelli degli uffici postali.

L'operatore verifica le informazioni precedentemente inserite dall'utente durante la pre-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.

Al termine della procedura di identificazione, il sistema invierà un SMS di conferma del buon esito delle verifiche "a vista". 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 Richiesta in ufficio postale e identificazione contestuale

Creazione pratica e identificazione a vista presso l'ufficio postale

L'utente che non dispone di strumenti di identificazione online e sceglie di avviare la propria adesione presso un ufficio postale:

- richiede all'operatore di creare una pratica di registrazione, comunicando il proprio codice fiscale. Se il codice fiscale è presente nell'anagrafica dei clienti di Poste Italiane, gli attributi identificativi del richiedente (inclusi gli estremi del documento di identità), gli attributi secondari e gli attributi di contatto vengono recuperati in automatico sulla pratica (cfr. paragrafo 5.4 "Anagrafica utente"). Se il codice fiscale non è presente nell'anagrafica dei clienti di Poste Italiane, l'operatore digita tutti i dati su indicazione dell'utente ed effettua la scansione di documento di riconoscimento e tessera sanitaria/codice fiscale, dopo averli verificati in originale;
- comunica e conferma all'operatore un indirizzo e-mail valido, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo successivo;
- comunica e conferma all'operatore il proprio numero di cellulare, la cui esistenza e disponibilità sono verificate dal servizio, con le modalità indicate al paragrafo successivo;
- riceve dall'operatore una ricevuta contenente i principali dati della pratica e un'informativa breve sul trattamento dei dati raccolti. La ricevuta indica il numero di giorni di validità della pratica, superati i quali tutti i dati vengono cancellati dai sistemi di Poste Italiane.

Certificazione di e-mail e cellulare e scelta delle credenziali dell'identità digitale

Completata la richiesta in ufficio postale, comprensiva dell'identificazione a vista, l'utente:

- riceve un SMS contenente una password temporanea, da utilizzare per certificare il possesso del numero di cellulare, e una welcome e-mail, contenente un link utile a certificare il possesso dell'indirizzo e-mail. Cliccando sul link il richiedente avvia la procedura di finalizzazione dell'adesione al servizio di identità digitale, il cui primo step prevede la visualizzazione di una pagina web sulla quale inserire la password temporanea e successivamente digitare la propria password;
- visualizza una pagina di riepilogo dei dati di adesione recuperati dalla pratica in ufficio postale e conferma la correttezza delle informazioni. Nel caso in cui il richiedente verifichi che i propri attributi identificativi non sono correttamente riportati, può annullare la richiesta e tornare in

ufficio postale per effettuare nuovamente l'identificazione;

Accettazione condizioni generali del servizio

L'utente accetta le Condizioni Generali del Servizio e Condizioni Economiche, 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.

5.2.2.3 Richiesta online e successiva identificazione a domicilio mediante un portalettere

Pre-registrazione

Durante il processo di pre-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 e-mail 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 15.4 "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 3, 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 e Condizioni Economiche 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[5]

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 della tessera sanitaria/codice fiscale, l'operatore richiede la copia fronte retro della tessera sanitaria/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. 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.

5.2.2.4 Richiesta da parte di clienti con Carta di Identità Elettronica (CIE 3.0) o Passaporto Elettronico

Identificazione

L'utente che dispone di:

- una Carta di Identità Elettronica (CIE 3.0, versione contactless) o di Passaporto Elettronico (emesso dopo il 2006),
- uno smartphone/tablet con tecnologia NFC attiva,

può scegliere di avviare la propria adesione dall'App PosteID, dopo averla scaricata sul proprio dispositivo mobile dallo store Google Play o da Apple Appstore. NB: *la modalità di seguito descritta non è disponibile per smartphone / tablet con sistema operativo iOS in versione inferiore a 13 e non abilitati all'utilizzo di NFC*.

L'utente seleziona sull'App PosteID la procedura di adesione mediante documento elettronico e seguendo passo dopo passo la procedura guidata:

- sceglie se utilizzare la propria Carta di Identità Elettronica o il proprio Passaporto Elettronico;
- inquadra con la fotocamera il documento elettronico sulle facce o pagine su cui sono presenti la propria foto ed i dati identificativi e i codici funzionali all'espletamento del processo (cfr.

[5] Modalità di richiesta attualmente sospesa

codice MRZ);

- avvicina il documento elettronico al dispositivo mobile, per attivare la lettura, tramite tecnologia NFC, dei dati contenuti nella memoria elettronica del chip. La lettura prevede l'estrazione dei dati identificativi del titolare del documento, della foto elettronica salvata nella memoria del chip e della firma tecnica dello stesso documento, utile a verificarne l'autenticità e la validità sulle fonti autoritative[6];
- effettua una breve ripresa audio-video (c.a. 5 secondi in risoluzione 320 x 240 px), tramite l'APP PosteID, leggendo uno specifico testo richiesto dall'App stessa;
- scatta in diretta, tramite l'APP PosteID, una propria foto (c.d. "selfie") tenendo il documento aperto e visibile sotto il proprio mento;
- inquadra e fotografa il fronte ed il retro della propria tessera sanitaria;
- sceglie se proseguire la procedura di registrazione sul dispositivo mobile oppure se collegarsi da un computer, utilizzando un codice temporaneo, valido per 30 minuti, che dovrà digitare su apposita pagina del sito https://posteid.poste.it.

Scelta credenziali e compilazione attributi secondari

Proseguendo sulle pagine di registrazione, indifferentemente da dispositivo mobile o da computer, l'utente:

- inserisce come proprio Nome Utente un indirizzo e-mail 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 15.4 "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;
- verifica i propri dati identificativi già presenti nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- inserisce 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 3, tramite gli

[6] Nell'ambito del processo di registrazione, tramite la lettura del microchip del documento elettronico, il sistema verifica sulla "certificate revocation list" pubblicata dall'Autorità emittente la validità della firma tecnica e l'eventuale presenza del certificato associato alla firma nella lista di revoca, impedendo l'attivazione dell'Identità nel caso in cui fossero rilevate delle anomalie.

strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6.

Accettazione condizioni generali del servizio

L'utente accetta le Condizioni Generali del Servizio e Condizioni Economiche, 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 ad avviare i controlli di back-office, il cui superamento è necessario per all'attivazione dell'Identità Digitale e delle credenziali associate.

Controlli di back-office

Operatori delle strutture di back-office di Poste Italiane ricevono la pratica di richiesta di attivazione dell'identità digitale creata dall'utente ed effettuano i seguenti controlli:

- corrispondenza tra i dati riportati sulle fotografie del documento elettronico, raccolte durante la procedura guidata all'interno dell'App PosteID, ed i dati identificativi estratti dalla memoria elettronica del documento stesso e registrati sulla pratica;
- corrispondenza tra il volto ritratto nella fotografia elettronica estratta dal documento e quello ritratto nel "selfie" effettuato in diretta tramite la fotocamera del dispositivo mobile;
- verifica che il soggetto ritratto nel breve video sia lo stesso ritratto nella foto estratta dal chip del documento e che il video ritragga una scena reale contraddistinta da "liveness";
- verifica che il soggetto ritratto nel breve video pronunci la frase richiesta dall'App PosteID in fase di identificazione;
- corrispondenza tra i dati riportati sulle fotografie della tessera sanitaria/codice fiscale raccolte durante la procedura guidata all'interno dell'App PosteID ed i dati identificativi registrati sulla pratica, in particolare il codice fiscale dell'utente.

Se i controlli sono tutti superati con esito positivo, l'operatore di back-office certifica l'identificazione del richiedente. A seguito di questa certificazione, vengono effettuati ulteriori controlli sulle fonti autoritative disponibili e, una volta superati con successo, Poste Italiane provvede all'attivazione dell'Identità Digitale e delle credenziali associate. N.B.: al fine di mitigare ulteriormente il rischio di utilizzo di documenti furtati/smarriti, il controllo sulla fonte autoritativa messa a disposizione dal Ministero dell'Interno sarà effettuata con un ritardo di almeno 36 ore rispetto al momento di creazione della pratica.

5.2.2.5 Richiesta da parte di clienti titolari di conto corrente italiano con operatività online [*MODALITA' PROGRESSIVAMENTE SOSPESA A PARTIRE DA LUGLIO 2026*]

Identificazione

L'utente che dispone di:

- un conto corrente italiano a sé intestato o cointestato, su cui sia in grado di operare la disposizione di un bonifico,
- uno smartphone/tablet,

può scegliere di avviare la propria adesione dall'App PosteID, dopo averla scaricata sul proprio dispositivo mobile dallo store Google Play o da Apple Appstore.

L'utente seleziona sull'App PosteID la procedura di adesione mediante bonifico:

- sceglie se utilizzare la propria Carta di Identità elettronica o il proprio Passaporto Elettronico come documento di riconoscimento;
- inquadra con la fotocamera il documento sulle facce o pagine su cui sono presenti la propria foto ed i dati identificativi (fronte e retro per la carta di identità, pagina con la foto per il passaporto);
- effettua una breve ripresa audio-video (c.a. 5 secondi in risoluzione 320 x 240 px), tramite l'APP PosteID, leggendo uno specifico testo richiesto dall'APP stessa;
- scatta in diretta, tramite l'APP PosteID, una propria foto (c.d. "selfie") tenendo il documento aperto e visibile sotto il proprio mento;
- inquadra e fotografa il fronte ed il retro della propria tessera sanitaria;
- sceglie se proseguire la procedura di registrazione sul dispositivo mobile oppure se collegarsi da un computer, utilizzando un codice temporaneo, valido per 30 minuti, che dovrà digitare su apposita pagina del sito https://posteid.poste.it.

Scelta credenziali e compilazione attributi secondari

Proseguendo sulle pagine di registrazione, indifferentemente da dispositivo mobile o da computer, l'utente:

- inserisce come proprio Nome Utente un indirizzo e-mail 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 15.4 "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;
- verifica i propri dati identificativi già presenti nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- inserisce 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 3, 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 e Condizioni Economiche, anche ai sensi degli artt. 1341 e 1342 cc, e fornisce i consensi relativi alla privacy barrando gli appositi campi e confermando tutto attraverso l'inserimento della password precedentemente scelta.

Disposizione del bonifico

Superato lo step precedente, viene visualizzata una pagina che fornisce all'utente le indicazioni per disporre un bonifico verso un conto corrente di Poste Italiane (intestatario, IBAN, importo e specifica causale da riportare), informando altresì l'utente che analoghe informazioni saranno inviate con una e-mail riepilogativa a completamento della procedura di richiesta. Solo se il bonifico viene accreditato entro 10 giorni dal completamento della richiesta, Poste Italiane, previa verifica delle condizioni sopra riportate, in particolare relativamente al disponente e al contenuto del campo "causale", provvede ad avviare i controlli di back-office, il cui superamento è necessario per l'attivazione dell'Identità Digitale e delle credenziali associate. NB: l'importo del bonifico disposto verso Poste Italiane viene restituito al richiedente con un bonifico di pari importo disposto da Poste Italiane. Non vengono restituiti eventuali costi applicati dalla banca del richiedente per la disposizione dell'operazione di bonifico. L'importo previsto per il bonifico è 1 €.

Controlli di back-office

Operatori delle strutture di back-office di Poste Italiane ricevono la pratica di richiesta di attivazione dell'identità digitale creata dall'utente ed effettuano i seguenti controlli:

- corrispondenza tra i dati riportati sulle fotografie del documento di riconoscimento ed i dati identificativi registrati sulla pratica;
- corrispondenza tra il volto presente nella fotografia del documento e quello ritratto nel "selfie" effettuato in diretta tramite la fotocamera del dispositivo mobile;
- verifica che il soggetto ritratto nel breve video sia lo stesso ritratto nella foto del documento e che il video ritragga una scena reale contraddistinta da "liveness";
- verifica che il soggetto ritratto nel breve video pronunci la frase richiesta dall'App PosteID in fase di identificazione;
- corrispondenza tra i dati riportati sulle fotografie della tessera sanitaria/codice fiscale raccolte durante la procedura guidata all'interno dell'App PosteID ed i dati identificativi registrati sulla pratica, in particolare il codice fiscale dell'utente;
- corrispondenza tra disponente del bonifico e dati presenti nel campo "causale" e dati registrati sulla pratica.

Se i controlli sono tutti superati con esito positivo, l'operatore di back-office certifica l'identificazione

del richiedente. A seguito di questa certificazione, vengono effettuati ulteriori controlli sulle fonti autoritative disponibili e, una volta superati con successo, Poste Italiane provvede all'attivazione dell'Identità Digitale e delle credenziali associate. N.B.: al fine di mitigare ulteriormente il rischio di utilizzo di documenti furtati/smarriti, il controllo sulla fonte autoritativa messa a disposizione dal Ministero dell'Interno sarà effettuata con un ritardo di almeno 36 ore rispetto al momento di creazione della pratica.

5.2.2.6 Richiesta presso uno sportello della Pubblica Amministrazione (R.A.O.)

L'utente che non dispone di strumenti di identificazione online e sceglie di avviare la propria adesione presso uno sportello della Pubblica Amministrazione accreditato come R.A.O.. Sono previste due modalità di richiesta e successiva identificazione:

1. **Richiesta a sportello senza scelta del Gestore di Identità, con utilizzo di un pacchetto di attivazione (token R.A.O.)**. Il cittadino:

- richiede al funzionario pubblico di creare una pratica di registrazione, effettuando un'identificazione de-visu secondo le procedure previste dal R.A.O.;
- comunica e conferma al funzionario un indirizzo e-mail valido;
- comunica e conferma al funzionario il proprio numero di cellulare;
- riceve sull'indirizzo e-mail appena comunicato un *pacchetto di attivazione* (file criptato, c.d. token R.A.O.), contenente i propri dati di identificazione, da conservare ed utilizzare successivamente sul sito https://posteid.poste.it per il completamento della registrazione;
- riceve sul numero di cellulare appena comunicato un SMS con una password temporanea (c.d. *codice di attivazione*), da conservare ed utilizzare sul sito https://posteid.poste.it per il completamento della registrazione.

NB: l'identificazione tramite R.A.O: ha una validità di 10 giorni, passati i quali il *pacchetto di attivazione* ed il *codice di attivazione* non sono più utilizzabili per il completamento della registrazione.

L'utente a questo punto può collegarsi sul sito https://posteid.poste.it e, dopo aver selezionato la modalità di **Identificazione tramite Sportello Pubblico** - "*Non ho indicato nessun Gestore*":

- inserisce negli appositi campi il proprio codice fiscale;
- effettua l'upload del file criptato precedentemente ricevuto sulla propria e-mail;
- digita il *codice di attivazione* precedentemente ricevuto via sms sul proprio numero di cellulare.

Il sistema verifica che il file criptato sia stato creato da meno di 10 giorni, che si riferisca al codice fiscale indicato e che il *codice di attivazione* ne decripti il contenuto. In caso di esito negativo di almeno una delle verifiche, la procedura si blocca e all'utente è richiesto di procedere con una nuova

identificazione presso uno sportello R.A.O..

2. **Richiesta a sportello con scelta del Gestore di Identità**. Il cittadino:

- richiede al funzionario pubblico di creare una pratica di registrazione, effettuando un'identificazione de-visu secondo le procedure previste dal R.A.O.;
- comunica e conferma al funzionario un indirizzo e-mail valido;
- comunica e conferma al funzionario il proprio numero di cellulare;
- comunica al funzionario il Gestore di Identità a cui intende rivolgere la richiesta di rilascio dell'identità digitale SPID;
- riceve sul numero di cellulare appena comunicato un SMS con una password temporanea (c.d. *codice di attivazione*), da conservare ed utilizzare sul sito https://posteid.poste.it per il completamento della registrazione.

NB: l'identificazione tramite R.A.O: ha una validità di 10 giorni, passati i quali il *codice di attivazione* non è più utilizzabile per il completamento della registrazione.

L'utente a questo punto può collegarsi sul sito https://posteid.poste.it e, dopo aver selezionato la modalità di **Identificazione tramite Sportello Pubblico** - "*Ho scelto Poste Italiane*":

- inserisce negli appositi campi il proprio codice fiscale;
- digita il *codice di attivazione* precedentemente ricevuto via sms sul proprio numero di cellulare.

Il sistema verifica che un R.A.O. abbia inviato a Poste Italiane un token creato da meno di 10 giorni, che si riferisca al codice fiscale indicato e che il *codice di attivazione* ne decripti il contenuto. In caso di esito negativo di almeno una delle verifiche, la procedura si blocca e all'utente è richiesto di procedere con una nuova identificazione presso uno sportello R.A.O.

Per entrambe le modalità, in caso di esito positivo dei controlli, il sistema avvia la procedura di completamento della registrazione, e l'utente effettua i seguenti passi:

- conferma come proprio Nome Utente l'indirizzo e-mail comunicato allo sportello R.A.O. o ne indica uno nuovo. L'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 15.4 "Misure anticontraffazione";
- conferma il numero di cellulare comunicato allo sportello R.A.O. o ne indica uno nuovo. Il possesso viene certificato mediante l'invio di un SMS con una One Time Password che deve essere digitata nella maschera di inserimento dati;
- conferma, integra o modifica gli attributi del proprio profilo, 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 3, tramite gli strumenti di autenticazione previsti dal Servizio, descritti dettagliatamente al capitolo 6;

- conferma di voler finalizzare l'adesione al servizio di identità digitale.

Accettazione condizioni generali del servizio

Dopo aver accettato le Condizioni Generali del Servizio e Condizioni Economiche, 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.

Il sistema procede con l'attivazione delle credenziali.

5.2.3 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 e Condizioni Economiche 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 Italiane (cfr. capitolo 5.1).

5.3 Registrazione al servizio PosteID effettuata da un soggetto tutore o amministratore di sostegno per i nati nel 1998-2004

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 1998-2004 (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" ed inserendo le proprie credenziali.

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 e-mail 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 15.4 "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 della tessera sanitaria/codice fiscale del soggetto rappresentato;
  - copia digitale del retro del documento d'identità e del la tessera sanitaria/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 3, 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 Italiane inerente al 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 back-office 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)[7];
- 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 raccogliere, al fine di migliorare l'esperienza d'uso, i dati aggiuntivi riportati di seguito:

- indirizzo di residenza;
- indirizzo di recapito.

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

[7] Nella selezione della Provincia si richiede di indicare la Provincia a cui appartiene il Comune di nascita al momento dell'identificazione del richiedente.

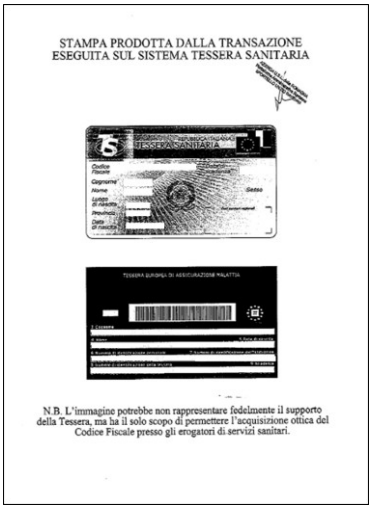
5.5 Documenti ammessi per l'identificazione

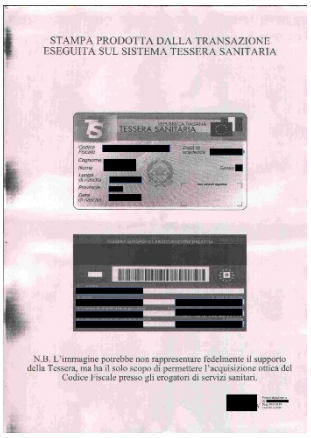
Di seguito i documenti, rilasciati da un'Autorità italiana, autorizzati da AgID per l'identificazione:

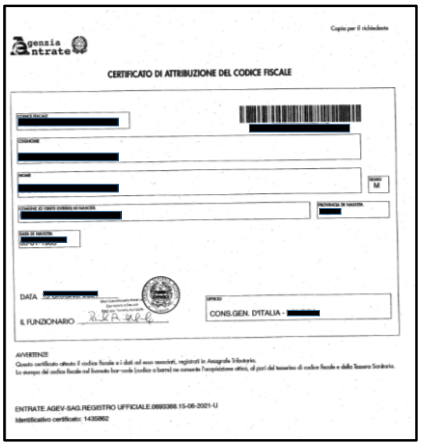
Documento di riconoscimento	
• Carta di identità elettronica (CIE)[8] • Passaporto[9] • Patente (*non utilizzabile nelle procedure di richiesta da App PosteID*)	
Documento attestante il Codice Fiscale **(cfr. combinato disposto determinazione AgID 505/2020 e Avvisi AgID n. 7 25/10/2017 e n. 17 del 18/2/2020)**	
Tessera Sanitaria plastificata ***N.B.:*** *E' accettabile anche la Tessera Sanitaria plastificata rilasciata dal MEF con il retro invalidato dall'apposizione di asterischi.*	
Copia provvisoria della Tessera Sanitaria	

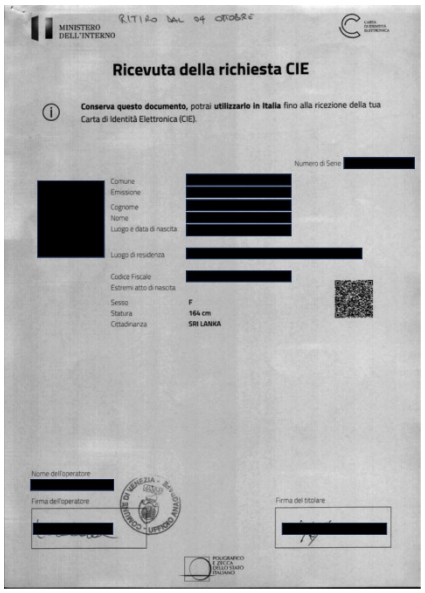
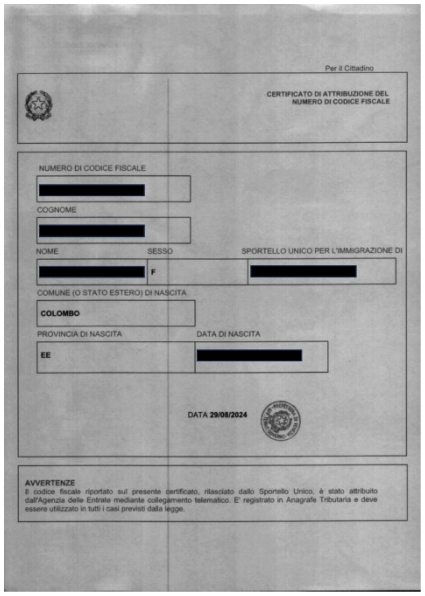
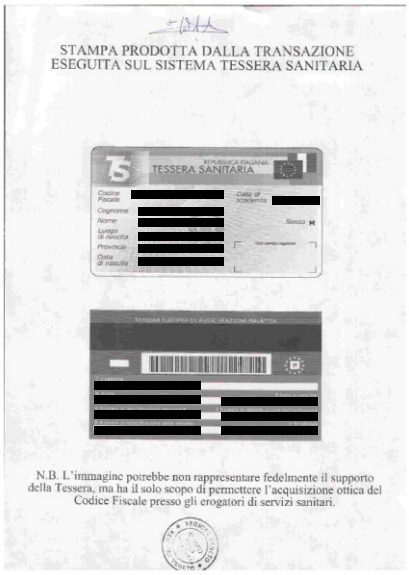
[8] Dal 3 agosto 2026, in ottemperanza a quanto previsto dal Regolamento europeo n. 1208 del 12 giugno 2025, la carta di identità cartacea non è più considerato un documento valido ai fini dell'identificazione del cittadino

[9] Tra le tipologie di passaporto è ammissibile anche il *Documento di viaggio per Rifugiati (Convenzione del 28 luglio 1951)*

Copia provvisoria della Tessera Sanitaria firmata digitalmente dal sistema TS	
Certificato provvisorio Tessera Sanitaria con timbro della ASL	
Stampa prodotta dalla transazione eseguita sul sistema Tessera Sanitaria con timbro della ASL	

Stampa prodotta dalla transazione eseguita sul sistema Tessera Sanitaria firmata digitalmente	
Codice Fiscale plastificato rilasciato da Agenzia delle Entrate ***(per cittadino non avente diritto alla tessera sanitaria)***	
Certificato di attribuzione del Codice Fiscale cartaceo rilasciato da Agenzia delle Entrate ***(per cittadino non avente diritto alla tessera sanitaria)***	
Certificato di attribuzione del Codice Fiscale cartaceo rilasciato da Agenzia delle Entrate con timbro originale ***(per cittadino non avente diritto alla tessera sanitaria)***	

Certificato di attribuzione del Codice Fiscale cartaceo rilasciato da Agenzia delle Entrate ai <u>residenti all'estero</u> con timbro originale dell'Ufficio Consolare ***(per cittadino non avente diritto alla tessera sanitaria)*** ***N.B.:*** *E' accettabile anche il documento ricevuto via email dal Consolato Italiano all'estero.*	 Copia per il richiedente CERTIFICATO DI ATTRIBUZIONE DEL CODICE FISCALE [redacted] SESSO M DATA [redacted] IL FUNZIONARIO UFFICIO CONS.GEN. D'ITALIA - [redacted] AVVERTENZE ENTRATE.AGEV-SAG.REGISTRO UFFICIALE.0693369.15-06-2021-U Identificativo certificato: 1430882
Certificato di attribuzione del Codice Fiscale cartaceo rilasciato da Agenzia delle Entrate ai <u>residenti all'estero</u> con timbro originale dell'Ambasciata Italia ***(per cittadino non avente diritto alla tessera sanitaria)*** ***N.B.:*** *E' accettabile anche il documento ricevuto via email dall'Ambasciata Italiana all'estero.*	 Copia per il richiedente CERTIFICATO DI ATTRIBUZIONE DEL CODICE FISCALE [redacted] SESSO F COMUNE DI NASCITA ROMA PROVINCIA DI NASCITA RM DATA [redacted] IL FUNZIONARIO UFFICIO AMBASCIATA D'ITALIA - CITTA DEL MESSICO AVVERTENZE ENTRATE.AGEV-SAG.REGISTRO UFFICIALE.1908754.10-10-2024-U Identificativo certificato: 6749575
Certificato di attribuzione del Codice Fiscale cartaceo rilasciato da Agenzia delle Entrate contenente il QR Code e l'indicazione della verifica di corrispondenza con il documento originale sul sito di ADE	 CERTIFICATO DI ATTRIBUZIONE DEL CODICE FISCALE

Certificato di attribuzione del codice fiscale cartaceo con timbro della prefettura	 MINISTERO DELL'INTERNO RITIRO DAL 04 OTTOBRE **Ricevuta della richiesta CIE** **Conserva questo documento,** potrai **utilizzarlo in Italia** fino alla ricezione della tua Carta di Identità Elettronica (CIE). Numero di Serie [redacted] Comune Emissione [redacted] Cognome [redacted] Nome [redacted] Luogo e data di nascita [redacted] Luogo di residenza [redacted] Codice Fiscale [redacted] Estremi atto di nascita Sesso F Statura 164 cm Cittadinanza SRI LANKA Nome dell'operatore [redacted] Firma dell'operatore [redacted] Firma del titolare [redacted]  Per il Cittadino CERTIFICATO DI ATTRIBUZIONE DEL NUMERO DI CODICE FISCALE NUMERO DI CODICE FISCALE [redacted] COGNOME [redacted] NOME [redacted] SESSO F SPORTELLO UNICO PER L'IMMIGRAZIONE DI [redacted] COMUNE (O STATO ESTERO) DI NASCITA COLOMBO PROVINCIA DI NASCITA EE DATA DI NASCITA [redacted] DATA 29/08/2024 AVVERTENZE Il codice fiscale riportato sul presente certificato, rilasciato dallo Sportello Unico, è stato attribuito dall'Agenzia delle Entrate mediante collegamento telematico. E' registrato in Anagrafe Tributaria e deve essere utilizzato in tutti i casi previsti dalla legge.
Stampa prodotta dalla transazione eseguita sul sistema tessera sanitaria con timbro della regione	 STAMPA PRODOTTA DALLA TRANSAZIONE ESEGUITA SUL SISTEMA TESSERA SANITARIA REPUBBLICA ITALIANA TESSERA SANITARIA Codice Fiscale [redacted] Data di scadenza [redacted] Cognome [redacted] Nome [redacted] Sesso M Luogo di nascita [redacted] Provincia [redacted] Data di nascita [redacted] N.B. L'immagine potrebbe non rappresentare fedelmente il supporto della Tessera, ma ha il solo scopo di permettere l'acquisizione ottica del Codice Fiscale presso gli erogatori di servizi sanitari.

Il richiedente dovrà essere in possesso ed esibire, nelle procedure di identificazione de-visu, un documento di entrambe le tipologie sopra descritte.

5.6 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 dell'identità digitale termina con l'invio all'utente di una conferma via e-mail di avvenuta attivazione del servizio "PosteID abilitato a SPID" e comunicazione del codice di sospensione immediata, nei casi previsti.

5.6.1 Credenziali SPID 1

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

5.6.2 Credenziali SPID 2

Nella fase di richiesta e attivazione dell'Identità digitale, l'Utente è chiamato sempre (in aggiunta alla scelta della password che costituisce la Credenziale di Livello 1 SPID) a comunicare, quale Attributo secondario, un numero di telefono mobile, verificato da Poste Italiane, che rappresenta il secondo fattore di sicurezza per il Livello 2 SPID. L'utilizzo di tale Credenziale è sempre possibile per l'accesso all'area riservata di gestione dell'Identità digitale su https://posteid.poste.it.

Relativamente alle credenziali PosteID di secondo livello basate su app, l'utente, prima di poter utilizzare la propria identità digitale, dovrà seguire le indicazioni per il download e procedere con i passi operativi riportati nella Guida Utente per la configurazione e attivazione dell'app stessa.

L'utente può inoltre richiedere l'abilitazione per l'accesso ai servizi del circuito SPID, della credenziale di secondo livello basata su codice di verifica OTP inviato tramite SMS sul telefono mobile certificato, con le modalità di utilizzo descritte di seguito e nella Guida Utente e con le eventuali limitazioni in termini di numero di accessi eseguibili con tali credenziali come riportate nelle Condizioni Generali del Servizio e Condizioni Economiche e sul sito posteid.poste.it.

Al fine di garantire il più alto grado di resilienza del sistema e la maggiore efficacia degli strumenti di autenticazione, potrà essere resa disponibile, in forma temporanea e in determinate circostanze, a tutti gli Utenti la possibilità di utilizzare, senza alcun aggravio, la credenziale di autenticazione basata su password e OTP inviato tramite SMS, dandone evidenza all'Utente in fase di autenticazione.

Inoltre, limitatamente ai titolari di identità SPID Tipo 4 è disponibile la credenziale di secondo livello basata su codice di verifica OTP inviato tramite e-mail sull'indirizzo di contatto certificato, con le modalità di utilizzo descritte di seguito e nella Guida Utente. Tale credenziale è abilitata in

automatico al momento dell'attivazione dell'identità SPID Tipo 4.

5.6.3 Credenziali SPID 3

Le credenziali PosteID di terzo livello possono essere ottenute solo dopo l'attivazione dell'identità digitale. Il titolare di identità digitale deve entrare nella propria area riservata, collegandosi al sito https://posteid.poste.it, cliccando su ACCEDI e seguendo le procedure di login con credenziali SPID 2. Dopo aver effettuato l'accesso, nella sezione "Il tuo profilo SPID" il cliente visualizza un box da cui è possibile avviare la richiesta di SPID 3. Cliccando sul box si apre una pagina che descrive le caratteristiche della credenziale di livello 3 e richiede l'input del "codice di attivazione SPID 3" (codice numerico di 6 caratteri). Tale codice è ottenuto dal richiedente con modalità diverse a seconda della procedura di identificazione utilizzata dal richiedente e della data di adesione al servizio PosteID:

a. titolare di identità digitale che si è identificato tramite:
   - Firma Digitale,
   - Carta Nazionale dei Servizi (CNS) attiva,
   - Carta di Identità Elettronica attiva (CIE 3.0, con utilizzo del PIN in App PosteID),
   - Carta di Identità Elettronica attiva (CIE 2.0, versione non-contactless con lettore),
   - riconoscimento "de-visu" in ufficio postale oppure a domicilio con portalettere,
   - riconoscimento presso uno sportello della Pubblica Amministrazione (R.A.O.).

   Tale cliente riceve il "codice di attivazione SPID 3" via SMS sul numero di cellulare associato alla propria identità digitale, contestualmente all'e-mail di conferma dell'attivazione dell'identità digitale.

b. titolare di identità digitale che si è identificato tramite:
   - strumenti di identificazione rilasciati da Poste Italiane autorizzati da AgID,
   - strumenti di identificazione informatica preesistenti a SPID rilasciati da Enti Terzi autorizzati da AgID ad operare come GIP,
   - Passaporto Elettronico o Carta di Identità Elettronica (CIE 3.0, senza utilizzo del PIN in App PosteID),
   - documento di riconoscimento e bonifico, tramite app PosteID.

   Tale cliente riceve il "codice di attivazione SPID 3" via SMS sul numero di cellulare associato alla propria identità digitale, a fronte di una specifica identificazione effettuata presso un ufficio postale. Il cliente deve quindi recarsi in un qualunque ufficio postale e richiedere all'operatore di sportello il rilascio del "codice di attivazione SPID 3", previa presentazione di un documento di riconoscimento (carta d'identità, patente o passaporto) e della propria tessera sanitaria/codice fiscale, entrambi in originale e in corso di validità, per permettere la verifica dell'identità in presenza. Superata con successo questa verifica, l'operatore autorizza a sistema l'invio via SMS del "codice di attivazione SPID 3".

c. titolare di identità digitale che ha aderito al servizio PosteID abilitato a SPID prima del 17 dicembre 2018: tale cliente riceve il "codice di attivazione SPID 3" con le stesse modalità previste per il cliente descritto al caso b., a prescindere dalla procedura di identificazione utilizzata in fase di adesione al servizio di identità digitale.

Dopo aver effettuato l'input del "codice di attivazione SPID 3", il cliente può prendere visione della documentazione relativa alla soluzione SPID 3 e successivamente deve scegliere il "PIN SPID 3" (codice numerico di 8 caratteri), digitandolo una prima volta e confermandolo una seconda[10], per finalizzare la procedura di richiesta di SPID 3.

Una volta completata con successo la procedura, il sistema presenta una pagina di conferma dell'esito e il cliente riceve via SMS un nuovo "codice di attivazione SPID 3", da conservare e utilizzare nel caso in futuro sia necessario sostituire il "PIN SPID 3" dimenticato[11].

Le credenziali SPID 3 sono basate sull'App PosteID e il cliente, prima di poterle utilizzare, dovrà seguire le indicazioni per il download e procedere con i passi operativi riportati nella Guida Utente per la configurazione e attivazione dell'app stessa.

5.6.4 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 16.1 "Conservazione evidenze per il rilascio dell'Identità Digitale".

[10] Il "PIN SPID 3" dovrà essere digitato sull'App PosteID dal cliente ogni volta che un Fornitore di servizi richiederà un'autenticazione di livello 3 SPID. Dovrà quindi essere conservato con cura dal cliente, non essendo recuperabile dagli operatori di assistenza telefonica nel caso venga dimenticato.

[11] Nel caso il cliente dimentichi il proprio "PIN SPID 3", può utilizzare l'ultimo "codice di attivazione SPID 3" ricevuto via SMS per richiedere nuovamente uno SPID 3. È necessario che clicchi sulla voce "Richiedi nuovo PIN" nel box presente nella sezione "Il tuo profilo SPID". La procedura risulta analoga ad una prima richiesta e determina la revoca automatica del vecchio certificato prima della creazione del nuovo.

6 Autenticazione ai servizi SPID

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
SPID 1 Primo livello (LoA2)	Password	
SPID 2 Secondo livello (LoA3)	App + codice PosteID *oppure* Password + PIN temporaneo (OTP) tramite App	Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato[12] *oppure* Password e codice di verifica OTP inviato tramite e-mail sull'indirizzo di contatto certificato *(applicabile solo a SPID tipo 4)*
SPID 3 Terzo livello (LoA4)	App + codice PosteID + PIN SPID 3	*Non disponibile*

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 16 "Sicurezza del servizio PosteID".

6.1.1 Strumenti SPID 1 (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 16.4.1 "Misure per SPID 1 (primo livello SPID)".

6.1.2 Strumenti SPID 2 (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 si basa sulla disponibilità da parte dell'utente di un dispositivo mobile su cui è stata

[12] Per aggiornamenti sull'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 e Condizioni Economiche "PosteID abilitato a SPID".

attivata l'App PosteID, mediante preliminare verifica dell'identità dell'utente. L'attivazione dell'App PosteID si completa con la generazione di un certificato e di un codice di sblocco, il codice PosteID.

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 del codice PosteID, un codice personale definito in fase di installazione dell'App.

Processo di attivazione delle 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;
- ricezione, sul numero di telefono certificato, di un sms con il codice di attivazione;
- inserimento e verifica del codice di attivazione sull'App;
- scelta del codice PosteID che abilita l'autorizzazione in app.

La soluzione SPID 2 su App PosteID implementa un meccanismo di autenticazione a due fattori basati sul possesso del dispositivo mobile che prevede tre modalità di interazione da parte del titolare dell'Identità Digitale SPID associata:

1. il cliente inserisce nome utente e password dell'identità digitale sulla maschera di login al servizio e sceglie di ricevere una push notification in app. l'App PosteID viene risvegliata dalla push notification e il cliente digita il codice PosteID per autorizzare l'autenticazione. La digitazione del codice PosteID è sostituibile con l'utilizzo dell'impronta digitale o dell'impronta facciale, fattori biometrici di inerenza, qualora lo smartphone/tablet posseduto dall'utente metta a disposizione queste funzionalità. In questo caso l'App si configura come un generatore di token di autenticazione multifattore;
2. il cliente, tramite l'App PosteID, inquadra il QR code che appare sulla maschera di login al servizio e digita il codice PosteID per autorizzare l'autenticazione. La digitazione del codice PosteID è sostituibile con l'utilizzo dell'impronta digitale o dell'impronta facciale, fattori biometrici di inerenza, qualora lo smartphone/tablet posseduto dall'utente metta a disposizione queste funzionalità. Anche in questo caso l'App si configura come un generatore di token di autenticazione multifattore. NB: nel solo scenario di utilizzo del servizio su browser mobile, alla visualizzazione del QR code si può sostituire la

visualizzazione di uno speciale link (c.d. deeplink) che permette all'utente di risvegliare l'App PosteID (se installata e attivata sul device) con le stesse modalità del QR code, permettendo poi la digitazione del codice PosteID (o l'utilizzo di un fattore biometrico) per autorizzare l'autenticazione;

3. il cliente inserisce nome utente e password dell'identità digitale sulla maschera di login al servizio e sceglie di generare un PIN temporaneo (OTP) in app. La maschera di login si mette in attesa della digitazione del PIN temporaneo (OTP) che il cliente genera, mediante bottone dedicato, sull'App PosteID, dopo averla aperta. L'inserimento sulla maschera di login del PIN temporaneo (OTP) autorizza l'autenticazione. In questo caso l'App si configura come un generatore esplicito di One Time Password che si va ad aggiungere alla password già digitata per consentire l'autenticazione di secondo livello di sicurezza SPID.

L'utente può verificare la lista di dispositivi su cui è installata l'app PosteID:

- dal menu dell'app stessa, sezione "Impostazioni",
- da apposita sezione presente nell'area personale su https://posteid.poste.it,

ed eventualmente procedere alla disassociazione dell'app da uno specifico dispositivo.

È possibile associare due sole istanze dell'app PosteID all'identità digitale di un titolare. Se il cliente prova ad enrollare una terza istanza dell'applicazione su un nuovo dispositivo viene bloccato e deve procedere alla disassociazione di una delle due app attive prima di enrollare la nuova.

NB: Poste Italiane adotta attività di monitoraggio volte a garantire che l'Identità Digitale in App PosteID venga utilizzata in modo conforme ai criteri di sicurezza e ai modelli d'uso previsti. Nel corso di tali verifiche, qualora emergano configurazioni o comportamenti non coerenti con tali criteri, l'associazione o l'utilizzo dell'App PosteID su uno specifico dispositivo può essere temporaneamente regolato, al fine di preservare l'integrità del servizio. Nell'area riservata post login sul sito posteid.poste.it, nel menu "Funzionalità Avanzate", è prevista la funzionalità "Sblocca dispositivo" a disposizione del titolare dell'Identità Digitale per gestire in autonomia la richiesta di sblocco del dispositivo in suo possesso, qualora siano rispettati i criteri di sicurezza richiesti.

6.1.2.1 Ulteriori strumenti di secondo livello SPID

6.1.2.1.1 Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato[13]

La soluzione PosteID con codice di verifica SMS - OTP si basa sull'utilizzo di un dispositivo mobile,

[13] Per aggiornamenti sull'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 e Condizioni Economiche "PosteID abilitato a SPID".

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.

Al fine di consentire l’accesso ai servizi anche ai Clienti impossibilitati ad utilizzare l’App PosteID, dal giorno 01/03/2019, l’accesso tramite credenziale SPID 2 basata su SMS sarà garantito con una limitazione degli accessi, secondo quanto disciplinato nelle Condizioni Generali del Servizio e Condizioni Economiche “PosteID abilitato a SPID”. La limitazione si applica per trimestri solari, calcolati a partire dalle seguenti date: 1 gennaio, 1 aprile, 1 luglio, 1 ottobre, di ogni anno. Gli accessi tramite OTP via SMS saranno utilizzabili nell’arco del trimestre di riferimento fino ad esaurimento, e torneranno disponibili a partire dal primo giorno del trimestre successivo, con la stessa modalità di utilizzo. Gli accessi non utilizzati entro l’ultimo giorno del singolo trimestre non saranno trasferiti nei trimestri successivi, ma si perderanno, non saranno quindi cumulabili. L’utente che attiva la credenziale di accesso tramite OTP via SMS in un qualsiasi giorno di un trimestre, potrà utilizzare tutti gli accessi disponibili entro l’ultimo giorno dello stesso trimestre. Il limite sugli accessi non si applica quando l’utente entra nella propria area personale su https://posteid.poste.it per gestire il suo profilo SPID.

6.1.2.1.2 Password e codice di verifica OTP inviato tramite e-mail sull’indirizzo di contatto certificato (limitato ai titolari di identità SPID Tipo 4)

La soluzione PosteID con codice di verifica OTP inviato tramite e-mail sull’indirizzo di contatto certificato associato all’identità SPID Tipo 4 è prevista da AgID con Determina 316/2021. L’abilitazione all’utilizzo è automatica, dal momento in cui l’identità SPID Tipo 4 è attiva.

Lo strumento prevede i seguenti step di utilizzo:

- l’utente digita e conferma il suo nome utente e la sua password sulla maschera di autenticazione,
- nel caso in cui i dati siano corretti e il servizio richieda il secondo livello di sicurezza, come previsto dal DPCM 24 ottobre 2014, l’utente selezione tale modalità tra quelle tempo per tempo disponibili e abilitate,
- l’utente riceve sull’indirizzo e-mail associato alla propria identità un codice temporaneo a bruciatura (OTP) e lo digita sulla pagina per l’accesso,
- nel caso i dati siano corretti, il sistema invitata l’utente a digitare due caratteri presenti nel codice del documento di riconoscimento associato alla sua identità digitale SPID Tipo 4. Il

sistema indica all'utente la loro posizione all'interno del numero. La posizione scelta dal sistema è casuale,

- l'utente digita sulla pagina per l'accesso i due caratteri richiesti e, nel caso i dati siano corretti, visualizza la pagina di autorizzazione al passaggio dei dati al Fornitore di servizi SPID, per completare l'autenticazione.

6.1.3 Strumenti SPID 3 (terzo livello SPID)

La soluzione PosteID di terzo livello si basa sull'utilizzo di un certificato digitale, la cui chiave privata viene memorizzata su un dispositivo di sicurezza Hardware Security Module (HSM) conforme alla normativa vigente e certificato, al fine di garantirne la riservatezza.

In fase di utilizzo è richiesta sia l'autenticazione tramite app, digitando il codice PosteID, che l'inserimento del "PIN SPID 3" per lo sblocco del certificato. La digitazione del codice PosteID può essere sostituita con l'utilizzo dell'impronta digitale (fingerprint) o dell'impronta facciale (Face ID) qualora lo smartphone/tablet posseduto dall'utente metta a disposizione queste funzionalità. Il "PIN SPID 3" deve essere digitato ad ogni utilizzo.

In fase di autorizzazione dell'accesso SPID 3, qualora la stessa avvenga a partire dal 90esimo giorno antecedente la scadenza del certificato digitale o dopo la scadenza dello stesso, l'app PosteID, dopo la verifica di tutti i fattori di sicurezza, informa l'utente che proseguendo il certificato sarà rinnovato:

- se l'utente nega l'autorizzazione, il certificato non viene rinnovato e l'autenticazione si conclude con esito negativo;
- se l'utente conferma l'autorizzazione, il sistema provvede al rinnovo del certificato e l'autenticazione si conclude con esito positivo. Il nuovo certificato ha durata pari a 3 anni.

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 SPID.
- Il Gestore dell'identità digitale verifica l'identità del soggetto sulla base delle credenziali esibite.
- Eventualmente, su input del Fornitore di servizi, il Gestore dell'identità digitale richiede al titolare dell'ID se intende autorizzare puntualmente il Fornitore di servizi a consultare gli

attributi qualificati riferibili al titolare stesso e messi a disposizione da specifici Gestori di attributi.

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.

Con specifiche Linee Guida, AgID ha introdotto le cosiddette "sessioni lunghe revocabili" da utilizzare nell'ambito delle applicazioni mobili, per migliorare l'esperienza di fruizione dei servizi da parte dell'utente. Le sessioni lunghe revocabili sono possibili in caso di utilizzo del protocollo OpenID Connect da parte del Fornitore di Servizi e permettono di mantenere attivo solo il livello base di autenticazione (SPID 1) per un massimo di 30 giorni, entro i quali il Fornitore di Servizi richiedere gli attributi dell'utente un numero illimitato di volte. Allo scadere dei 30 giorni sarà necessario rieseguire l'autenticazione completa.

Le sessioni lunghe revocabili di autenticazione possono essere instaurate solo previa autorizzazione dell'utente a valle della procedura di autenticazione.

L'autorizzazione alla gestione di una sessione lunga revocabile avviene sulla pagina che, dopo la verifica con esito positivo dell'identità dell'utente, mostra la lista di attributi richiesti dal Fornitore di Servizi per poter erogare il servizio. L'autorizzazione avviene mediante apposizione di un flag (opt-in) con cui l'utente stesso acconsente a mantenere la sessione aperta per un massimo di 30 giorni. In questo periodo il Fornitore di Servizi può accedere ai dati dell'identità digitale dell'utente e garantisce all'utente stesso di poter accedere ai suoi servizi mobili senza utilizzare ogni volta le credenziali PosteID abilitato a SPID, ma un PIN locale oppure un fattore biometrico.

La mancata autorizzazione all'apertura di una sessione lunga revocabile non invalida il buon esito dell'autenticazione effettuata dall'utente per il servizio.

Le sessioni lunghe revocabili possono essere revocate in ogni momento, prima della scadenza massima di 30 giorni, utilizzando un'apposita funzionalità messa a disposizione nell'area riservata del servizio PosteID abilitato a SPID. Accedendo al tab "Gestione Sessioni", l'utente può visualizzare le sessioni lunghe revocabili attive ed effettuare un logout puntuale o massivo per revocarle.

La sessione lunga è annullata anche a fronte di un logout esplicito dell'utente sull'app mobile del Fornitore di Servizi (funzionalità a carico del Fornitore di Servizi stesso).

Autenticazione PosteID con sistemi di autenticazione a 2 fattori

Utente con App PosteID	Utente con SMS - OTP PosteID[14]
Modalità 1 di avvio dell'autenticazione: **PASSWORD + PUSH IN APP + CODICE POSTEID** L'utente inserisce il proprio Nome Utente e password sulla maschera web di login e riceve una notifica sul proprio smartphone/tablet tramite l'App PosteID. *Modalità 2 di avvio dell'autenticazione*: **QR CODE + CODICE POSTEID** L'utente apre l'App PosteID e fotografa il QR code visualizzato sulla maschera web di login. NB: nello scenario di login tramite browser mobile, al QR code si può sostituire uno speciale link (c.d. deeplink) per risvegliare l'App PosteID (se installata e attivata sullo stesso device). *Per le Modalità 1 e Modalità 2 di avvio dell'autenticazione*: L'utente inserisce il proprio codice PosteID 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	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.

[14] Per aggiornamenti sull'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 e Condizioni Economiche "PosteID abilitato a SPID".

codice PosteID - definito in fase di installazione dell'App sull'apparato mobile di cui ha la disponibilità - per evitarne la digitazione nelle fasi in cui ciò viene richiesto dal servizio PosteID abilitato a SPID. E' vietato all'utente associare al codice PosteID 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 PosteID tramite le funzionalità previste dall'apparato mobile in uso. Poste Italiane 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 Italiane si riserva di disattivare in qualsiasi momento la funzionalità di associazione dell'impronta digitale o dell'impronta facciale al codice PosteID 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. *Modalità 3 di avvio dell'autenticazione*: **PASSWORD + PIN TEMPORANEO (OTP) generato in App** L'utente inserisce il proprio Nome Utente e password sulla maschera web di login, apre l'App PosteID e richiede, tramite apposito bottone, la generazione di un OTP da digitare sulla maschera di login al servizio.	

Autenticazione PosteID con sistemi di autenticazione di livello 3

Utente con App PosteID
Modalità 1 di avvio dell'autenticazione: **PASSWORD + PUSH IN APP + CODICE POSTEID + PIN SPID 3** L'utente inserisce il proprio Nome Utente e password sulla maschera web di login e riceve una notifica sul proprio smartphone/tablet tramite l'App PosteID. *Modalità 2 di avvio dell'autenticazione*: **QR CODE + CODICE POSTEID + PIN SPID 3** 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*: 1. L'utente inserisce il proprio codice PosteID 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 PosteID - definito in fase di installazione dell'App sull'apparato mobile di cui ha la disponibilità - per evitarne la digitazione nelle fasi in cui ciò viene richiesto dal servizio PosteID abilitato a SPID. E' vietato all'utente associare al codice PosteID 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 PosteID tramite le funzionalità previste dall'apparato mobile in uso. Poste Italiane 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 Italiane si riserva di disattivare in qualsiasi momento la funzionalità di associazione dell'impronta digitale o dell'impronta facciale al codice PosteID e di ripristinare il normale funzionamento tramite immissione del codice PosteID. 2. L'utente inserisce il proprio "PIN SPID 3" sull'App. la digitazione del "PIN SPID 3" non può essere sostituita dall'associazione dell'impronta digitale (cosiddetta "fingerprint") oppure dell'impronta facciale (cosiddetta "Face ID") dell'utente. Il PIN si disabilita automaticamente dopo 5 tentativi errati in fase di inserimento. **NB**: nel solo caso di primo utilizzo dell'App su un nuovo smartphone/tablet, 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, previa autorizzazione da parte dell'utente, può provvedere alla verifica presso i Gestori di attributi qualificati in relazione al possesso di specifiche qualifiche o poteri.

6.3 Interrogazione degli attributi qualificati del titolare dell'identità digitale

I regolamenti SPID prevedono che i Fornitori di servizi possano accedere ai dati messi a disposizione dai Gestori di attributi accreditati, secondo differenti modelli che possono prevedere o meno un'autorizzazione esplicita da parte del titolare dell'identità digitale.

In particolare, i modelli definiti da AgID sono i seguenti:

1. Public

- **Ambito:** richiesta di **attributi pubblicamente disponibili** (es. domicilio digitale, iscrizione albo)
- **Modalità:** il Fornitore di servizi può richiedere gli attributi **senza alcuna autorizzazione** da parte dell'utente

2. Protected

- **Ambito:** richiesta di **attributi non di pubblico dominio** che necessitano di specifiche autorizzazioni.
- **Modalità:** il **Fornitore di servizi è convenzionato con il Gestore di attributi** e l'utente deve **esprimere il consenso** sulle maschere di autenticazione del Gestore di identità in fase di accesso al servizio

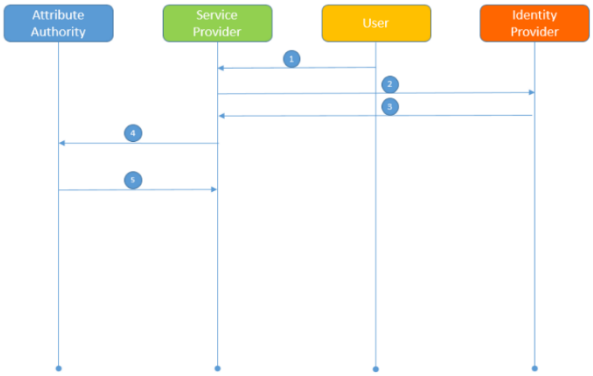
3. Private

- **Ambito:** richiesta di **attributi riservati o con richieste di accesso continuativo**
- **Modalità:** l'utente è chiamato ad eseguire una **seconda autenticazione presso il portale online del Gestore di attributi** per autorizzare il passaggio dei dati

6.3.1 Modello Public

Il modello "Public" è basato sull'accesso ad attributi qualificati pubblici. È caratterizzato dal fatto che il dato riferito all'attributo qualificato è open, di pubblico dominio o liberamente accessibile. In tal caso il Fornitore di servizi può richiedere l'accesso al dato al Gestore di attributi senza necessità di acquisire l'autorizzazione dell'utente.

La mimica di autenticazione del modello Public è la seguente:



1. L'utente chiede l'accesso a un servizio del Fornitore di servizi per la cui fruizione è richiesta l'acquisizione di uno o più attributi qualificati e seleziona il proprio Gestore di identità.

2. Il Fornitore di servizi trasferisce l'utente sulle maschere di autenticazione del Gestore di identità.

3. Il Gestore di identità esegue la procedura di autenticazione, chiede all'utente l'assenso alla trasmissione dei propri dati e invia la risposta di autenticazione al Fornitore di servizi.

4. Il Fornitore di servizi invia la richiesta al Gestore di attributi

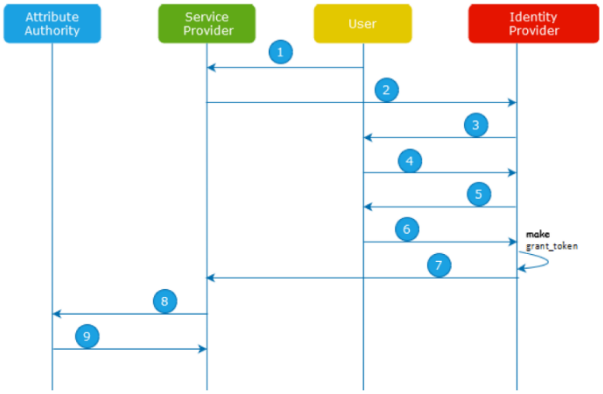
5. Il Gestore di attributi riscontra direttamente il Fornitore di servizi mediante attestazione degli attributi richiesti.

Nel modello "Public" il Gestore di identità non ha alcun ruolo specifico.

6.3.2 Modello Protected

Il modello "Protected" è basato sull'accesso ad attributi qualificati protetti, non pubblici. È caratterizzato dal fatto che il dato riferito all'attributo qualificato non è liberamente accessibile e prevede che il Fornitore di servizi abbia sottoscritto una specifica convenzione con il Gestore di attributi. In tal caso il Fornitore di servizi deve richiedere la preventiva autorizzazione dell'utente per l'accesso al dato e trasferire al Gestore di attributi l'assenso dell'utente stesso.

La mimica di autenticazione del modello "Protected" è la seguente:



1. L'utente chiede l'accesso a un servizio del Fornitore di servizi per la cui fruizione è richiesta l'acquisizione di uno o più attributi qualificati e seleziona il proprio Gestore di identità.

2. Il Fornitore di servizi, una volta individuata una lista di attributi qualificati con i relativi Gestori di attributi, trasferisce l'utente sulle maschere di autenticazione del Gestore di identità e, nella richiesta di autorizzazione, dichiara i Gestori di attributi che potrebbe potenzialmente interrogare ai fini dell'erogazione dei servizi resi.

3. Il Gestore di identità, nell'eseguire la procedura di autenticazione, mostra all'utente la lista di Gestori di attributi indicati dal Fornitore di servizi.

4. L'utente seleziona i Gestori di attributi per i quali autorizza l'interrogazione da parte del Fornitore di servizi.

5. Il Gestore di identità, durante la medesima procedura di autenticazione, chiede all'utente l'assenso alla trasmissione dei propri dati al Fornitore di servizi e all'interrogazione da parte del Fornitore di servizi dei Gestori di attributi selezionati.

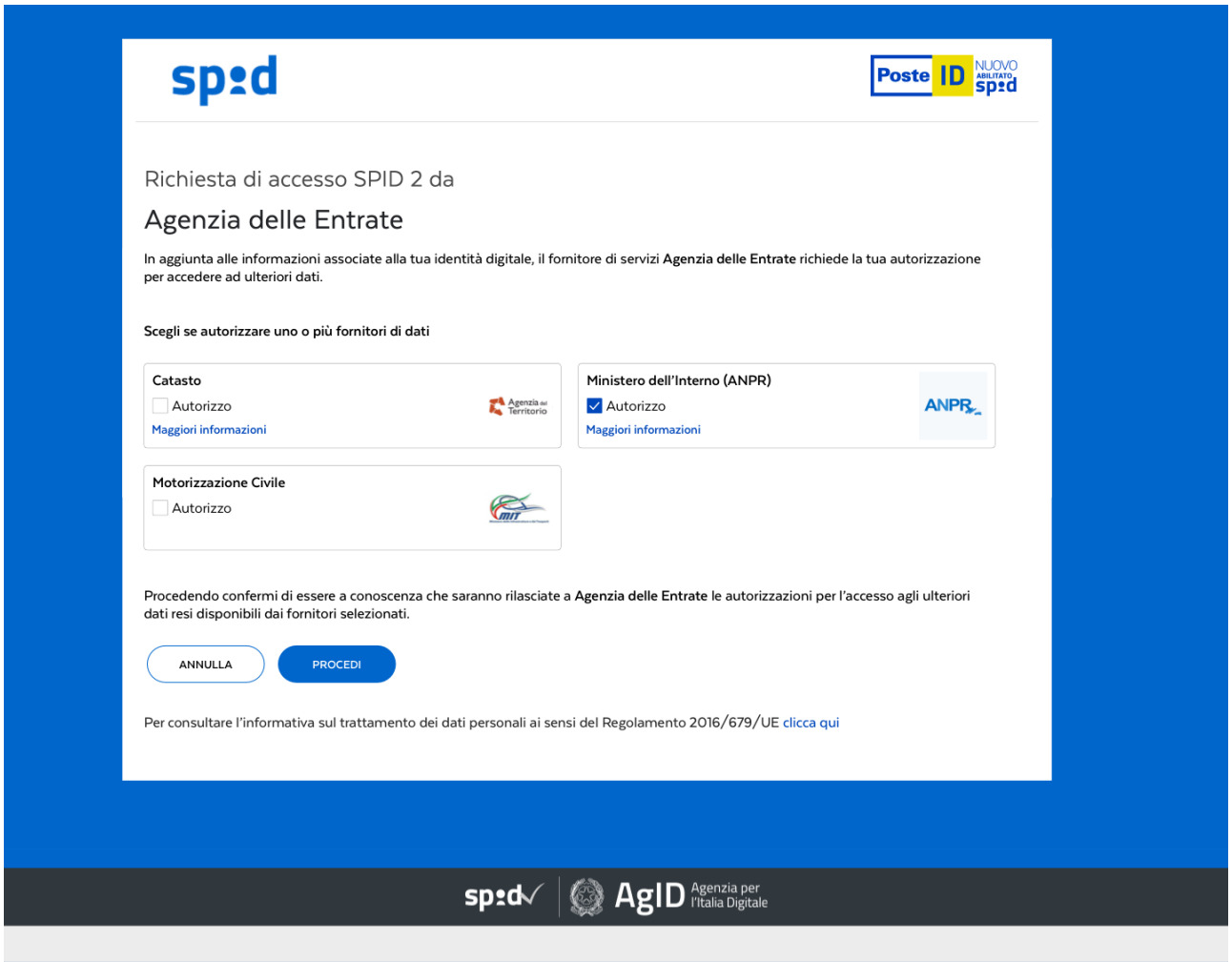
6. L'utente restituisce il proprio assenso.

7. Il Gestore di identità genera un token di concessione (grant_token) per ognuno dei Gestori di attributi selezionati e reindirizza l'utente sul Fornitore di servizi con la risposta (response) contenente il token di concessione.

8. Il Fornitore di servizi invia il token di concessione (grant_token) ai Gestori di attributi.

9. I Gestori di attributi, sulla base del token di concessione (grant_token) e dei controlli specifici derivanti dalla convenzione stipulata con il Fornitore di servizi, fornisce a quest'ultimo un'autorizzazione per recuperare gli attributi qualificati.

Di seguito un esempio della maschera di autorizzazione descritta al punto 4:



Maschera di autorizzazione dell'interrogazione dei Gestori di attributi (puramente esemplificativa)

Poste Italiane, che implementa il profilo Protected in qualità di Gestore di identità:

1. acquisisce dall'utente un singolo assenso per ogni Gestore di attributi visualizzato sulla maschera di autorizzazione dell'interrogazione;
2. trasmette tale assenso al Fornitore di servizi in forma di "grant token";
3. implementa un "token introspection endpoint" per permettere ai soggetti interessati di verificare i "grant token" emessi.

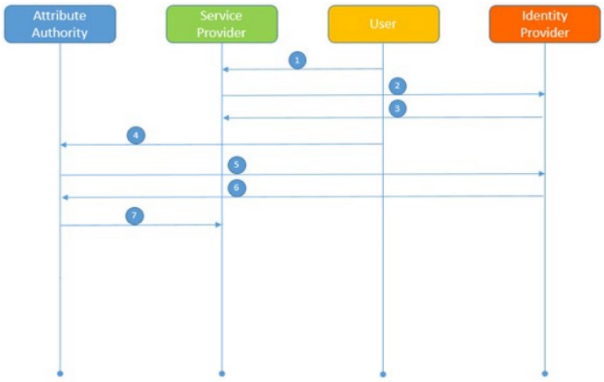
6.3.3 Modello Private

Il modello "Private" è basato sull'accesso ad attributi qualificati privati. È caratterizzato dal fatto che il dato riferito all'attributo qualificato non è liberamente accessibile e prevede che il Fornitore di servizi abbia sottoscritto una specifica convenzione con il Gestore di attributi. In tal caso il Fornitore di servizi deve richiedere la preventiva autorizzazione dell'utente per l'accesso al dato e successivamente il Gestore di attributi deve procedere ad una seconda autenticazione dell'utente sul proprio portale per raccogliere direttamente l'assenso dell'utente stesso.

Tale modello si applica sempre nei casi di richiesta continuativa di attributi qualificati. La richiesta è

continuativa quando il Fornitore di servizi può ottenere da parte del Gestore di attributi più attestazioni “asincrone” del/i medesimo/i attributo/i qualificato/i all’interno di una finestra temporale - non superiore a un periodo ininterrotto di 12 mesi - reciprocamente concordata tra Fornitore di servizi, Gestore di attributi e utente. E’ necessario richiedere all’utente un assenso esplicito (che interviene mediante autenticazione dell’utente interessato anche presso il Gestore di attributi mediante il proprio Gestore di identità). L’utente può anche negare l’assenso, convertire la richiesta continuativa in una richiesta puntuale o ridurre ulteriormente la durata temporale a un periodo inferiore di propria scelta. Tutta questa gestione è in carico al Gestore di attributi.

La mimica di autenticazione del modello “Private” è la seguente:



1. L’utente chiede l’accesso a un servizio del Fornitore di servizi per la cui fruizione è necessaria l’acquisizione di uno o più attributi qualificati e seleziona il proprio Gestore di identità.

2. Il Fornitore di servizi trasferisce l’utente sulle maschere di autenticazione del Gestore di identità.

3. Il Gestore di identità esegue la procedura di autenticazione e invia la risposta di autenticazione al Fornitore di servizi.

4. Il Fornitore di servizi invia al Gestore di attributi la richiesta di attributi qualificati dell’utente, reinoltrando l’utente stesso sul portale del Gestore di attributi.

5. Il Gestore di attributi trasferisce nuovamente l’utente sulle maschere di autenticazione del suo Gestore di identità (NB: esiste una procedura semplificata, chiamata IdP hinting, che evita all’utente di procedere con la scelta del Gestore di identità, in quanto viene richiamato lo stesso utilizzato per l’autenticazione al Fornitore di servizi).

6. Il Gestore di identità esegue la procedura di autenticazione e invia la risposta di autenticazione al Gestore di attributi.

7. Il Gestore di attributi fornisce al Fornitore di servizi un’autorizzazione per recuperare gli attributi qualificati; il Fornitore di servizi invia la richiesta al Gestore di attributi per recuperare gli attributi qualificati; il Gestore di attributi riscontra direttamente il Fornitore di servizi mediante attestazione degli attributi richiesti.

Nel modello “Private” il Gestore di identità non ha alcun ruolo specifico, in virtù del fatto che il Gestore di attributi si presenta al Gestore di identità con le modalità di un Fornitore di servizi.

6.4 Procedure di aggiornamento e recupero della password

La password dell’identità digitale viene creata dall’utente in fase di richiesta del servizio “PosteID abilitato a SPID” ed è conforme ai requisiti previsti da AgID e riportati al paragrafo 16.4.1 “Misure per SPID 1 (primo livello SPID)”. Ha una durata massima di 180 giorni e:

- nel periodo di validità può essere aggiornata dal titolare o recuperata in caso venga dimenticata (c.d. *reset*),
- quando l’utente inserisce la password, ne viene controllata la data di scadenza e se risulta superato il periodo di validità deve essere obbligatoriamente aggiornata (c.d. *cambio password obbligatorio*).

6.4.1 Aggiornamento password

L'aggiornamento della password su iniziativa dell'utente avviene mediante apposita funzionalità dall'area di gestione del profilo del titolare dell'identità (post-login) sul sito https://posteid.poste.it.

Una volta selezionata la voce "Cambia password", è richiesto di

- digitare la password che l'utente utilizza per accedere ai servizi e che vuole modificare,
- digitare la nuova password, che l'utente vuole utilizzare da quel momento in avanti,
- ri-digitare una seconda volta la nuova password, per confermarla.

Se tutti i requisiti formali sono rispettati, il sistema comunica all'utente che l'aggiornamento è avvenuto con successo e che da quel momento in poi può utilizzare la nuova password scelta.

Nel caso in cui uno più requisiti formali non siano rispettati, il sistema mostra un messaggio di errore ed invita l'utente a verificare di aver soddisfatto tutti i criteri di sicurezza elencati sulla pagina.

6.4.2 Recupero della password dimenticata da web e da dispositivo mobile

Se l'utente dimentica la password associata alla propria identità digitale può effettuare la procedura di recupero da tutte le pagine in cui sia presente il link "*Hai dimenticato il nome utente o la password?*". Tale link è presente in particolare:

- sulla pagina del servizio https://posteid.poste.it, sotto il pulsante ACCEDI;
- sulle maschere di accesso ai servizi, sotto i campi "*nome utente*" e "*password*".

Dopo che l'utente ha cliccato sul link, si apre una pagina che richiede di scegliere tra il recupero del "*nome utente*" ed il recupero della "*password*". Una volta selezionata la voce "*Voglio effettuare il reset della password*":

- l'utente visualizza una pagina informativa che lo invita a chiamare il numero dedicato automatico 06.4526.3893[15] dal telefono cellulare associato alla sua identità digitale e seguire le indicazioni della voce guida;
- una volta chiamato il numero 06.4526.3893, l'utente viene automaticamente riconosciuto dal sistema e viene informato che proseguendo la telefonata avvierà la procedura di recupero della password;
- se l'utente abbandonata la telefonata, la procedura si interrompe e la password non viene resettata. Se l'utente prosegue con la chiamata, viene informato che il sistema invierà una e-mail all'indirizzo di posta elettronica associato alla sua identità digitale, con specifiche indicazioni e il link per scegliere la sua nuova password. La chiamata viene abbattuta senza

[15] Interactive Voice Response (IVR), senza operatore

interazione;

- al click del link il sistema apre una pagina web che mostra un campo dove digitare la nuova password, che l'utente vuole utilizzare da quel momento in avanti, e un campo dove ri-digitare una seconda volta la nuova password, per confermarla.

Se tutti i requisiti formali sono rispettati, il sistema comunica all'utente che l'aggiornamento è avvenuto con successo e che da quel momento in poi può utilizzare la nuova password scelta.

Nel caso in cui uno più requisiti formali non siano rispettati, il sistema mostra un messaggio di errore ed invita l'utente a verificare di aver soddisfatto tutti i criteri di sicurezza elencati sulla pagina.

NB: per soddisfare specifiche esigenze da parte dell'utente, è prevista la possibilità di attivare, tramite link dedicato indicato nelle FAQ del Servizio o richiedibile al servizio di Assistenza Clienti, anche la seguente modalità alternativa di recupero della password. Il sistema visualizzerà una pagina su cui:

- è richiesto all'utente di digitare il proprio nome utente, digitare il codice di controllo intelligente "captcha" che appare sullo schermo e cliccare su PROSEGUI;
- il sistema invia un messaggio all'e-mail certificata del titolare dell'identità. Il messaggio contiene un link da cliccare;
- al click del link il sistema invia via SMS un codice temporaneo sul cellulare certificato del titolare dell'identità e apre una pagina web che mostra un campo dove digitare il codice ricevuto via SMS;
- se il codice digitato risulta corretto, il sistema mostra la pagina dove
    - digitare la nuova password, che l'utente vuole utilizzare da quel momento in avanti,
    - ri-digitare una seconda volta la nuova password, per confermarla.

Se tutti i requisiti formali sono rispettati, il sistema comunica all'utente che l'aggiornamento è avvenuto con successo e che da quel momento in poi può utilizzare la nuova password scelta.

Nel caso in cui uno più requisiti formali non siano rispettati, il sistema mostra un messaggio di errore ed invita l'utente a verificare di aver soddisfatto tutti i criteri di sicurezza elencati sulla pagina.

Tale seconda modalità potrà essere attivata per tutti gli utenti in specifici casi di disservizio prolungato sul servizio dedicato automatico.

6.4.3 Recupero della password dimenticata tramite Call Center

Se l'utente dimentica la password, in alternativa alla procedura di recupero via web e dispositivo mobile, può effettuare la procedura di reset automatico chiamando il Call Center di Poste Italiane, al numero 06.977.977.77, con il numero di cellulare associato alla propria identità digitale. Seguendo le indicazioni della voce automatica:

- l'utente seleziona l'opzione di recupero della password,

- il sistema informa l'utente che premendo un apposito numero sulla tastiera del cellulare potrà recuperare la propria password. Alla pressione del numero, il sistema invia un messaggio all'e-mail certificata del titolare dell'identità. Il messaggio contiene un link da cliccare;
- al click del link il sistema apre una pagina web dove
    - digitare la nuova password, che l'utente vuole utilizzare da quel momento in avanti,
    - ri-digitare una seconda volta la nuova password, per confermarla.

Se tutti i requisiti formali sono rispettati, il sistema comunica all'utente che l'aggiornamento è avvenuto con successo e che da quel momento in poi può utilizzare la nuova password scelta.

Nel caso in cui uno più requisiti formali non siano rispettati, il sistema mostra un messaggio di errore ed invita l'utente a verificare di aver soddisfatto tutti i criteri di sicurezza elencati sulla pagina.

6.4.4 Cambio password obbligatorio a scadenza

Superato il periodo di validità di 180 giorni, la password dell'identità digitale deve essere obbligatoriamente aggiornata. In fase di utilizzo dell'identità, quando l'utente inserisce la password, il sistema ne controlla la validità e se ne rileva l'avvenuta scadenza, mostra all'utente un messaggio che lo informa della necessità di aggiornare la propria password. L'aggiornamento avviene tramite l'apertura di una pagina dedicata, sia web che da App, su cui all'utente è richiesto di:

- digitare l'ultima password che l'utente utilizzava per accedere ai servizi e che è scaduta;
- digitare la nuova password, che l'utente vuole utilizzare da quel momento in avanti;
- ri-digitare una seconda volta la nuova password, per confermarla.

Se tutti i requisiti formali sono rispettati, il sistema comunica all'utente che l'aggiornamento è avvenuto con successo e che da quel momento in poi può utilizzare la nuova password scelta.

Nel caso in cui uno più requisiti formali non siano rispettati, il sistema mostra un messaggio di errore ed invita l'utente a verificare di aver soddisfatto tutti i criteri di sicurezza elencati sulla pagina.

6.4.5 Procedura in caso di perdita dei fattori di sicurezza utili ad assicurare la titolarità del richiedente ad effettuarne il recupero

Nel caso in cui l'utente in un certo momento non ricordi la password e abbia necessità di recuperarla, è necessario che sia in possesso del numero di cellulare e dell'e-mail di contatto associati alla sua identità digitale, utili a dimostrare la sua titolarità al recupero della password stessa.

Qualora non abbia più disponibilità dei suddetti fattori, potrà comunque accedere in autonomia alle funzionalità di gestione del proprio profilo digitale dal sito https://posteid.poste.it tramite l'app PosteID e aggiornare il numero di cellulare e/o l'e-mail di contatto. Prerequisito è che l'app PosteID sia installata e attivata sul proprio device e che l'utente ricordi il codice PosteID ad essa associato.

Diversamente non sarà possibile effettuare il recupero delle credenziali, mancando gli elementi di sicurezza necessari ad assicurare la titolarità del richiedente ad effettuare il suddetto recupero.

NB: in quest'ultimo caso, per poter utilizzare nuovamente il Servizio sarà necessario che l'utente proceda alla revoca della propria identità e ad una successiva adesione ex novo.

6.5 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 di Identità Digitale.

6.6 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
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	n/a

Scenario	Dettaglio Errore	Azioni e notifica all'utente	Errore SAML
		per facilitare l'assistenza	
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 Pagamento del corrispettivo periodico per l'utilizzo della funzionalità di autenticazione sul circuito SPID

L'accesso ai servizi che espongono il logo SPID prevede il pagamento di un corrispettivo annuale a partire dalla scadenza del primo anno dall'attivazione dell'identità digitale.

Il cliente che non appartiene ad una delle categorie per cui è prevista l'esenzione dal pagamento[16] può richiedere il rinnovo della funzionalità di accesso da casa, visitando il portale del Servizio all'indirizzo https://posteid.poste.it, oppure recarsi in Ufficio Postale. Può rinnovare la funzionalità di accesso per sé stesso oppure per un soggetto terzo che necessita di supporto. La richiesta di rinnovo può essere presentata nei trenta giorni precedenti alla data di scadenza. A seguito del buon esito del pagamento del corrispettivo, la funzionalità viene rinnovata di un anno, a partire dal giorno successivo alla scadenza in essere, senza alcuna interruzione dell'accesso ai servizi che espongono il pulsante "ENTRA CON SPID".

In caso di mancato pagamento entro la data di scadenza prevista, l'identità digitale continuerà a restare attiva ma verrà inibito l'accesso ai servizi SPID. L'utente potrà in qualsiasi momento rinnovare la funzionalità procedendo al pagamento del corrispettivo previsto. A seguito del buon esito del pagamento il servizio verrà automaticamente riattivato per un anno a partire dalla data di avvenuto pagamento e il titolare potrà riprendere il regolare accesso ai servizi SPID.

Il titolare dell'identità digitale può conoscere la data di scadenza della funzionalità di accesso accedendo alla sua area personale dal portale del Servizio https://posteid.poste.it oppure entrando nell'App PosteID associata alla sua ID. In ogni caso da trenta giorni prima della scadenza il titolare sarà informato della possibilità e delle modalità per procedere al rinnovo, tramite comunicazioni sull'indirizzo e-mail associato alla sua identità digitale.

È possibile consultare tutti i dettagli sui termini di servizio sulla pagina https://www.poste.it/posteid, dove sono disponibili le condizioni generali e le condizioni economiche vigenti, sulle pagine informative collegate e sul portale del Servizio https://posteid.poste.it.

7.1.1 Rinnovo da casa, tramite accesso all'area personale del titolare

Il titolare può richiedere il rinnovo della funzionalità di accesso ai servizi SPID per la sua identità digitale accedendo all'area personale disponibile all'indirizzo https://posteid.poste.it. Nella sezione "SPID ad uso personale" è possibile verificare la data di scadenza del rinnovo e procedere al rinnovo

[16] Le categorie di clienti esentati dal pagamento sono indicate sulle pagine informative del servizio (https://www.poste.it/posteid)

tramite il link “Rinnova ora”. Il titolare può utilizzare un codice promozionale, se in suo possesso, e procedere online al pagamento del corrispettivo previsto mediante una propria carta di pagamento. A seguito del buon esito dell’operazione il servizio verrà rinnovato di un anno, in accordo a quanto indicato in precedenza, e sarà possibile richiedere l’invio della fattura indicando l’indirizzo di fatturazione. Al termine della procedura il titolare riceverà all’indirizzo e-mail associato alla sua identità digitale una comunicazione di conferma dell’avvenuto rinnovo.

7.1.2 Rinnovo da casa, senza accesso all’area personale del titolare

È possibile richiedere il rinnovo della funzionalità di accesso dal portale del Servizio https://posteid.poste.it anche senza accedere all’area personale. In questo caso la richiesta può essere presentata per sé stesso oppure per un soggetto terzo che necessita di supporto. Dovrà essere indicato il codice fiscale del titolare dell’identità digitale e l’indirizzo e-mail utilizzato come nome utente della stessa identità per cui si vuole procedere al rinnovo. Per confermare la correttezza dei dati indicati, sarà inviato all’indirizzo e-mail un codice di verifica che il titolare dovrà eventualmente fornire all’utente che lo sta supportando per essere digitato in pagina. Completata questa verifica, il richiedente potrà procedere con il pagamento previsto mediante una carta di pagamento. Se l’utente dispone di un codice promozionale, può indicarlo subito prima di effettuare il pagamento. A seguito del buon esito dell’operazione, la funzionalità di accesso verrà rinnovata di un anno, in accordo a quanto indicato in precedenza, e sarà possibile richiedere l’invio della fattura indicando l’indirizzo di fatturazione del titolare dell’identità digitale. Al termine della procedura verrà inviata una comunicazione di conferma dell’avvenuto rinnovo all’indirizzo e-mail associato all’identità digitale per la quale è stato richiesto il rinnovo dell’accesso ai servizi SPID.

7.1.3 Rinnovo in Ufficio Postale

È possibile procedere al rinnovo della funzionalità di accesso in un qualunque Ufficio Postale. La richiesta può essere presentata per sé stesso oppure per un soggetto terzo che necessita di supporto. In entrambi i casi dovrà essere comunicato all’operatore di sportello il solo codice fiscale associato all’identità digitale per la quale si vuole richiedere il rinnovo della funzionalità di accesso ai servizi che espongono il logo SPID.

Durante la procedura a sportello l’utente può pagare il corrispettivo previsto in contanti oppure mediante una carta di pagamento. Completata la richiesta in Ufficio Postale la funzionalità di accesso ai servizi SPID verrà automaticamente rinnovata di un anno, in accordo a quanto indicato in precedenza, e verrà inviata una comunicazione di conferma dell’avvenuto rinnovo all’indirizzo e-mail associato all’identità digitale per la quale è stata presentata la richiesta.

7.2 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 a seguito della 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 https://posteid.poste.it.

7.2.1 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 e-mail 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.

7.2.2 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 al numero 06.977.977.77, selezione *2-3 (Se hai già una Identità Digitale PosteID abilitato a SPID \ Se vuoi sospendere le tue credenziali*).

Interagendo con il servizio IVR, l'utente deve seguire il percorso per selezionare il servizio corrispondente alla richiesta di sospensione:

- se sta chiamando dal numero certificato PosteID, può digitare direttamente il codice di sospensione immediata;
- se sta chiamando da altro numero di telefono, deve digitare il proprio numero di telefono certificato PosteID e successivamente 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 e-mail (indirizzo certificato in fase di adesione al servizio).

7.2.3 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 e-mail (indirizzo certificato in fase di adesione al servizio).

7.3 Revoca

7.3.1 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 / recesso a partire dal portale del Gestore Poste Italiane.

L’utente deve:

- compilare e firmare il modulo di richiesta, disponibile nell’area di gestione del profilo del titolare dell’identità (post-login) o nella sezione “RICHIEDI ASSISTENZA” (pre-login) selezionando “Modulo di richiesta di revoca dell’Identità Digitale di clienti maggiorenni o minorenni con almeno quattordici anni”, sul sito https://posteid.poste.it;
- far pervenire a Poste Italiane la documentazione, corredata da copia del proprio documento di identità.

L’inoltro della documentazione a Poste Italiane per la richiesta di revoca può essere effettuato tramite i seguenti canali alternativi. In particolare:

- posta elettronica certificata (PEC) con allegata la documentazione firmata digitalmente;
- e-mail 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 e-mail del mittente sia corrispondente all’indirizzo e-mail verificato 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 via e-mail al fine di definire la problematica e l'eventuale soluzione.

In caso tutte le verifiche diano esito positivo, l'identità viene posta in uno stato di sospensione e viene inviato all'utente un SMS al numero di cellulare certificato contenente la conferma della presa in carico della richiesta di revoca. La richiesta di revoca non è annullabile.

Entro 5 giorni dall'invio dell'SMS le credenziali vengono revocate definitivamente.

A fronte dell'avvenuto processo di revoca, l'utente riceve all'indirizzo e-mail di contatto una conferma di avvenuta revoca 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.

NB: nel caso in cui la richiesta di revoca pervenisse da un'Autorità Giudiziaria (direttamente o per il tramite di AgID), Poste Italiane provvederà ad effettuare direttamente la revoca senza l'invio di SMS al numero di cellulare del titolare dell'identità.

7.3.2 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, tramite presentazione del certificato di morte;
- 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.

7.4 Blocco temporaneo del profilo

Tramite apposita funzionalità presente nell'area di gestione del profilo del titolare dell'identità (post-login) 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.

7.5 Richiesta di disassociazione del numero di cellulare da altra identità digitale

Si è potuto verificare che vi sono diversi casi in cui i richiedenti l'identità digitale si vedono rifiutare dal Gestore dell'identità digitale l'indicazione del numero di cellulare da associare alla propria identità, in quanto già associato ad altro utente. I casi più frequenti sono riconducibili alla riassegnazione di numeri di telefono da parte dei gestori di telefonia mobile a seguito della scadenza della SIM, altri al precedente utilizzo del medesimo numero da parte di un familiare/affine per ottenere l'identità digitale. Peraltro, vi potrebbero essere casi nei quali il cellulare sia stato sottratto, anche temporaneamente, al legittimo proprietario ed utilizzato per ottenere l'identità digitale SPID.

Per sanare le situazioni di cui sopra, il richiedente può contattare il servizio di Assistenza Clienti al numero 06.977.977.77 e richiedere la verifica sul fatto che il numero di cellulare risulti già associato ad altra identità digitale PosteID abilitato a SPID, e che pertanto sia un cellulare indisponibile.

L'operatore non fornirà informazioni sull'attuale titolare dell'identità digitale a cui il numero sia associato, ma offrirà supporto ad una disassociazione in self-care nel caso in cui il richiedente abbia contezza dell'identità dell'attuale assegnatario. Nel caso in cui il richiedente non abbia contezza dell'identità dell'attuale assegnatario, l'operatore dell'Assistenza Clienti comunicherà al richiedente come scaricare dal sito il modulo da compilare per la richiesta di disassociazione. Tale modulo deve essere compilato dal richiedente, fornendo i propri dati anagrafici, l'indicazione del numero di cellulare di cui si richiede la disassociazione, un indirizzo e-mail valido e attivo e copia del documento di riconoscimento (carta di identità o passaporto, in corso di validità) e inviato all'indirizzo e-mail indicato nel modulo stesso.

Ricevuto il modulo e appurata l'indisponibilità del numero, l'Assistenza Clienti invia all'indirizzo e-mail indicato dal richiedente nel modulo una comunicazione contenente un codice pratica che il richiedente dovrà fornire all'operatore di Poste Italiane che lo contatterà telefonicamente nelle successive 36 ore. In occasione di tale contatto telefonico l'operatore verifica che a rispondere sia il richiedente e che questo sia in possesso del codice pratica inviato via e-mail. Se queste verifiche hanno esito negativo, la pratica viene annullata. Se le verifiche hanno esito positivo, l'Assistenza Clienti invia una comunicazione all'attuale assegnatario, sull'indirizzo e-mail di contatto associato alla sua identità digitale, informandolo che Poste Italiane procederà alla revoca della sua identità digitale, a meno che non proceda in self alla sostituzione del numero di cellulare con un altro numero effettivamente in suo possesso, mediante accesso all'area riservata sul sito https://posteid.poste.it tramite autenticazione con l'app PosteID.

Il numero di cellulare indicato dal richiedente viene liberato e l'Assistenza clienti comunica al richiedente che da quel momento è possibile procedere alla registrazione al servizio con quel numero. L'identità dell'attuale assegnatario viene posta in stato sospeso e viene revocata se dopo 15 giorni non è stato effettuato un aggiornamento in self del numero, secondo le modalità sopra riportate.

8 Identità Digitale per titolari minorenni (SPID Tipo 1)

Con l'introduzione dell'identità digitale dei minori, attraverso l'emanazione delle Linee Guida dedicate da parte dell'AgID, il circuito SPID mira a garantire il raggiungimento dei seguenti obiettivi:

1. consentire ai minori di acquisire la propria identità digitale, previa richiesta autorizzativa da parte di chi esercita la responsabilità genitoriale;
2. consentire al minore di fruire autonomamente di servizi online mediante la propria identità digitale, ferma restando, nei casi previsti, la possibilità di autorizzazione e verifica da parte del Genitore richiedente;
3. consentire ai fornitori di servizi in rete la possibilità di definire criteri di accesso in funzione dell'età dell'utente.

Il servizio PosteID abilitato a SPID rende disponibile una modalità di rilascio e gestione dell'identità digitale per i minori, in coerenza con le Linee Guida AgID.

In considerazione della sensibilità del servizio e al fine di eseguire gli specifici controlli previsti per l'attivazione dell'identità dei minori, in fase di prima applicazione delle suddette Linee Guida, nelle more della disponibilità di fonti dati per l'esecuzione automatica delle verifiche, Poste Italiane procederà ad effettuare la verifica dell'identità del minore stesso presso la capillare rete degli Uffici Postali, fermi restando i corrispettivi associati a tale modalità di identificazione come riportati sulle Condizioni Generali del Servizio e Condizioni Economiche e sul sito del servizio stesso.

8.1 Richiesta di rilascio SPID in favore di un minore

La richiesta di attivazione di un'identità digitale SPID per minore può essere avviata dal Genitore richiedente se già titolare di un'identità digitale PosteID abilitato a SPID attiva.

Il Genitore richiedente potrà creare la pratica di richiesta dell'identità digitale del minore dalla sua area riservata del Servizio, sul sito https://posteid.poste.it, accedendo alla scheda "ID minore" e seguendo le indicazioni.

Il primo step in carico al Genitore richiedente prevede l'indicazione dei dati anagrafici del minore, precisamente di:

- codice fiscale,
- nome e cognome,
- data di nascita.

Il minore deve aver compiuto almeno 5 anni di età.

Successivamente il Genitore richiedente deve dichiarare:

- ai sensi dell'art. 46 del DPR 445/2000, di essere il titolare della responsabilità genitoriale del minore per il quale sta chiedendo il rilascio dell'Identità Digitale;

- con quale ruolo sta operando, scegliendo tra "**genitore**" e "**altro titolo**" (ad es. tutore):
  - **nel caso in cui selezioni "genitore"**, viene informato che se sul documento del minore non è presente il suo nome e cognome dovrà consegnare in ufficio postale un certificato di stato di famiglia con rapporti di parentela in cui siano contemporaneamente riportati il suo nome e quello del minore;
  - **nel caso in cui selezioni "altro titolo"**, viene informato che dovrà presentare in ufficio postale il decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina a tutore o l'affidamento del minore;
- ai sensi dell'art. 47 del DPR 445/2000:
  - **se non esiste un secondo soggetto che ha responsabilità genitoriale sul minore**, di poter operare in autonomia. Il Genitore richiedente viene inoltre informato che dovrà presentare in ufficio postale il certificato di morte del Secondo genitore oppure un eventuale provvedimento del tribunale oppure l'estratto di nascita del minore con indicazioni di maternità/paternità;
  - **se esiste un secondo soggetto che ha responsabilità genitoriale sul minore** (di seguito "Genitore non richiedente"), di aver ricevuto l'autorizzazione alla gestione dell'identità del minore da parte del Genitore non richiedente. Il Genitore richiedente viene inoltre informato che dovrà presentare in ufficio postale il documento di riconoscimento in originale in corso di validità del Genitore non richiedente. In questo caso è richiesto di **indicare anche il nome e cognome del Genitore non richiedente**.
- di accettare di ricevere le notifiche per autorizzare il minore all'accesso ai servizi che richiedono l'approvazione del Genitore richiedente.

Il secondo step in carico al Genitore richiedente prevede la dichiarazione di:

- presa visione dell'informativa privacy del Servizio[17], disponibile in consultazione e download dalla stessa pagina del sito,
- accettazione delle Condizioni Generali del Servizio e Condizioni Economiche,

con conferma tramite inserimento della password associata alla sua identità digitale.

La procedura di creazione della pratica di richiesta si conclude con una pagina di esito su cui viene visualizzato un **codice di verifica, generato e associato univocamente alla richiesta per il minore indicato dal Genitore richiedente**. Il codice di verifica viene anche inviato via e-mail sull'indirizzo di contatto del Genitore richiedente. Tale codice di verifica dovrà essere consegnato

[17] L'informativa privacy del Servizio include una specifica appendice denominata "Sintesi esplicativa per soggetti minori", che descrive dettagliatamente le caratteristiche del trattamento e i correlati diritti, a beneficio del genitore e del minore

dal Genitore richiedente al minore, per permettere a quest'ultimo di avviare l'effettiva richiesta di rilascio dell'identità digitale per sè stesso.

Un Genitore richiedente può eseguire la procedura descritta in precedenza per richiedere il rilascio dello SPID di Poste Italiane per eventuali ulteriori minori di cui è titolare della responsabilità genitoriale. Ogni minore, una volta attivata la relativa identità digitale, sarà gestito dal Genitore richiedente con le modalità e nei limiti del controllo parentale descritti nei paragrafi successivi.

8.2 Attività in capo al minore

Una volta **ricevuto il codice di verifica dal Genitore richiedente**, il minore sul sito https://posteid.poste.it, accede tramite il tasto REGISTRATI e seleziona l'opzione "Identificazione in ufficio postale".

Pre-registrazione online

Il minore indica i suoi dati anagrafici, come riportati nel paragrafo 5.4 "Anagrafica utente", ma a differenza di un richiedente maggiorenne, alla digitazione della data di nascita **il sistema attiva il campo obbligatorio "codice di verifica", all'interno del quale il minore dovrà digitare il codice ricevuto dal Genitore richiedente** a valle della creazione della pratica di richiesta. Solo in caso di corrispondenza tra i dati anagrafici appena inseriti dal minore e del codice di verifica con l'analoga combinazione di dati precedentemente indicati dal Genitore richiedente, il sistema permette al minore di proseguire il percorso di rilascio dell'identità digitale.

Nessun dato viene acquisito dai sistemi di Poste Italiane prima che il controllo al punto precedente dia esito positivo. In caso di discordanza tra i dati, viene visualizzato un errore bloccante e la procedura non può andare avanti.

Solo a seguito del controllo del corretto abbinamento tra dati anagrafici del minore e codice di verifica fornitogli dal Genitore richiedente, il minore può proseguire con i successivi step:

- inserisce come proprio Nome Utente un indirizzo e-mail 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 15.4 "Misure anticontraffazione";
- sceglie se rilasciare un proprio numero di telefono cellulare, il cui possesso viene verificato mediante l'invio di un SMS con una One Time Password che deve essere digitata nella maschera di inserimento dati. Nel caso il minore non sia in possesso di un numero di cellulare, al fine di garantire specifiche funzionalità (alert di sicurezza, procedure di recupero delle credenziali, configurazione dell'app di autenticazione, processi di sospensione/revoca, processi di assistenza per ragioni di sicurezza), verrà associato all'ID del minore il numero di

cellulare del Genitore richiedente. NB: nel caso di associazione del numero di cellulare del Genitore richiedente sarà inibito al minore l'utilizzo della credenziale "Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato", descritta al §6.1.2.1; nel caso in cui il Genitore richiedente aggiorni il suo numero di cellulare, l'aggiornamento si riflette automaticamente sull'associazione dello stesso numero all'identità del minore.

- inserisce gli estremi del documento di identità;
- rilascia un indirizzo di domicilio, necessario per l'eventuale richiesta di emissione di una fattura da parte Poste Italiane, ma, essendo un attributo facoltativo nel circuito SPID, sceglie se l'indirizzo possa essere messo a disposizione o meno dei Fornitori di servizi che ne facciano richiesta; eventualmente completa la compilazione dei propri attributi secondari nel form di richiesta, come riportati nel paragrafo 5.4 "Anagrafica utente";
- viene informato che sarà identificato in un ufficio postale.

Per concludere la procedura online il minore, al fine di confermare la pratica, inserisce la password appena scelta e associata alla sua identità digitale. Qualora il minore abbia compiuto i 14 anni dovrà altresì preliminarmente prendere visione delle Condizioni Generali del Servizio e Condizioni Economiche e dell'informativa privacy del Servizio, entrambe disponibili in consultazione e download dalla stessa pagina del sito.

La procedura si conclude con una pagina di esito su cui vengono visualizzate le informazioni utili prima di recarsi in ufficio postale e di completare la procedura di rilascio dell'identità digitale per il minore stesso. Il minore viene informato che al momento dell'identificazione è necessaria la presenza in ufficio postale anche del Genitore richiedente e che andranno esibiti i documenti di riconoscimento del minore e del Genitore richiedente, in originale ed in corso di validità, per l'identificazione. In caso di esistenza di un Secondo genitore, andrà esibito in ufficio postale anche il documento di riconoscimento, in originale ed in corso di validità, del Secondo genitore indicato dal Genitore richiedente durante la creazione della pratica online. Prima di recarsi in ufficio postale è necessario attendere un'e-mail di conferma del buon esito della pre-registrazione e prenotare un appuntamento per l'identificazione SPID. Il buon esito della pre-registrazione viene anche inviato via e-mail sull'indirizzo di contatto del Genitore richiedente.

Identificazione a vista presso l'ufficio postale

L'identificazione a vista viene eseguita presso gli sportelli degli uffici postali.

Il minore deve essere sempre accompagnato dal Genitore richiedente.

Il minore deve presentare all'operatore dell'ufficio postale il documento di riconoscimento indicato in fase di pre-registrazione online e su cui sia stampato il nome e cognome del Genitore richiedente. Nel caso in cui il documento di riconoscimento del minore non riporti il nome e il cognome del Genitore richiedente, in coerenza con quanto previsto nelle Linee Guida emanate dall'AgID, dovrà

essere fornito un “certificato di stato di famiglia con rapporti di parentela” oppure, nei casi previsti, il “decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina del tutore o l’affidamento del minore” sempre per verificare l’esercizio della responsabilità genitoriale in capo al soggetto che ha avviato la richiesta dell’identità digitale per il minore. Sul “certificato di stato di famiglia con rapporti di parentela” o sul “decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina del tutore o l’affidamento del minore” dovranno essere contemporaneamente presenti il nome del Genitore richiedente e del minore.

In entrambi gli scenari, l’operatore verifica le informazioni precedentemente inserite durante la pre-registrazione online, esegue l’identificazione a vista del minore 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 minore di confermare che il numero di cellulare inserito a sistema sia corretto.

L’operatore:

- verifica che sul documento di riconoscimento del minore o sul certificato di stato di famiglia con rapporti di parentela oppure, nei casi previsti, nel decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina del tutore o l’affidamento del minore siano stampati e leggibili il nome ed il cognome del Genitore richiedente,
- riporta a sistema gli estremi del documento (tipo e numero) di riconoscimento presentato dal Genitore richiedente in originale e in corso di validità.

In caso di non presenza del nome e cognome del Genitore richiedente sul documento del minore o sul “certificato di stato di famiglia con rapporti di parentela” oppure sul “decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina del tutore o l’affidamento del minore” o in caso di mancata corrispondenza, la procedura viene interrotta e non può essere finalizzata l’identificazione. Il Genitore richiedente deve essere sempre presente come accompagnatore del minore.

L’eventuale “certificato di stato di famiglia con rapporti di parentela” oppure “decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina del tutore o l’affidamento del minore” sono acquisiti ed associati alla richiesta di rilascio dell’identità digitale.

Il Genitore richiedente presenta all’operatore dell’ufficio postale un documento di identità in originale e in corso di validità dell’eventuale Secondo genitore o copia di un documento che attesti la dichiarazione di essere l’unico esercente la responsabilità genitoriale (es. stato di morte dell’altro genitore, nomina in qualità di tutore, ecc.), l’operatore verifica l’assenza di eventuali incongruenze e acquisisce copia della documentazione presentata.

Al termine della procedura di identificazione, il sistema invierà una e-mail per comunicare l'avvenuta attivazione dell'identità digitale, sia sull’indirizzo di contatto del minore che su quello del Genitore richiedente.

Se il minore 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 pratica, prima di recarsi nuovamente in ufficio postale con il Genitore richiedente per completare l'identificazione.

8.3 Sintesi della documentazione da presentare in ufficio postale

Di seguito una vista di sintesi della documentazione di cui il Genitore richiedente e il minore devono essere in possesso e che deve essere presentata in ufficio postale per l'identificazione dei soggetti e la raccolta delle evidenze:

#	Ruolo del "Genitore richiedente"	Esistenza del "Secondo genitore"	Documentazione da presentare in ufficio postale
1	Genitore	Esiste un secondo soggetto che ha responsabilità genitoriale sul minore	• un documento in corso di validità attestante il codice fiscale del minore • un documento di riconoscimento in originale in corso di validità del minore (carta di identità o passaporto) • se sul documento del minore non è riportato il nome e cognome del Genitore richiedente, il certificato di stato di famiglia con rapporti di parentela in cui siano riportati contemporaneamente il nome del Genitore richiedente e quello del minore • un documento di riconoscimento in originale in corso di validità del Genitore richiedente (carta di identità, patente o passaporto) • un documento di riconoscimento in originale in corso di validità del Secondo genitore (carta di identità, patente o passaporto)
2	Genitore	Non esiste un secondo soggetto che ha responsabilità genitoriale sul minore	• un documento in corso di validità attestante il codice fiscale del minore • un documento di riconoscimento in originale in corso di validità del minore (carta di identità o passaporto) • se sul documento del minore non è riportato il nome e cognome del Genitore richiedente, il certificato di stato di famiglia con rapporti di parentela in cui siano riportati contemporaneamente il nome del Genitore richiedente e quello del minore • un documento di riconoscimento in originale in corso di validità del Genitore richiedente (carta di identità, patente o passaporto) • un certificato di morte del Secondo genitore oppure un eventuale provvedimento del tribunale oppure l'estratto di nascita del minore con indicazioni di maternità/paternità
3	Altro titolo	Esiste un secondo soggetto che ha responsabilità genitoriale sul minore	• un documento in corso di validità attestante il codice fiscale del minore • un documento di riconoscimento in originale in corso di validità del minore (carta di identità o passaporto) • il decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina a tutore o l'affidamento del minore • un documento di riconoscimento in originale in corso di validità del soggetto che esercita la responsabilità genitoriale sul minore e che chiede il rilascio di SPID in favore di quest'ultimo con titolo diverso da quello di genitore (carta di identità, patente o passaporto) • un documento di riconoscimento in originale in corso di validità del Secondo genitore (carta di identità, patente o passaporto)
4	Altro titolo	Non esiste un secondo soggetto che ha responsabilità	• un documento in corso di validità attestante il codice fiscale del minore • un documento di riconoscimento in originale in corso di validità

#	Ruolo del "Genitore richiedente"	Esistenza del "Secondo genitore"	Documentazione da presentare in ufficio postale
		genitoriale sul minore	del minore (carta di identità o passaporto) • il decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina a tutore o l'affidamento del minore • un documento di riconoscimento in originale in corso di validità del soggetto che esercita la responsabilità genitoriale sul minore e che chiede il rilascio di SPID in favore di quest'ultimo con titolo diverso da quello di genitore (carta di identità, patente o passaporto)

8.4 Utilizzo dell'identità del minore

Come da obiettivo del Circuito, è essenziale consentire al minore di utilizzare la propria identità digitale SPID autonomamente, ferma restando la possibilità di controllo da parte del Genitore richiedente, nei termini e nei casi previsti dalle Linee Guida emanate dall'AgID.

I Fornitori di servizi SPID, oltre a definire il livello di sicurezza minimo necessario per l'accesso, a massima tutela dei minori:

- definiscono quale sia l'età minima e l'età massima richiesta al titolare dell'identità digitale per poter fruire dei servizi online offerti;
- indicano se il servizio che offrono richieda o meno la preventiva autorizzazione del Genitore richiedente all'accesso del minore;
- mettono a disposizione del minore / Genitore richiedente un'informativa sul trattamento applicato ai dati del minore stesso sulle proprie pagine del servizio.

8.4.1 Autenticazione da parte del minore

Al momento dell'accesso il titolare minorenne deve disporre di uno degli strumenti descritti al capitolo 6 "Autenticazione" compatibile con il livello di sicurezza minimo richiesto dal Fornitore di servizi SPID. Una volta avviata l'autenticazione, il sistema:

- verifica che il minore abbia un'età compresa nei limiti richiesti dal Fornitore di servizi SPID. Se l'età non è compatibile con i limiti definiti dal Fornitore di servizi, comunica al minore che non è possibile proseguire con l'accesso.

  Se l'età è compatibile con i limiti:
- verifica se il Fornitore di servizi preveda l'autorizzazione preventiva del Genitore richiedente all'accesso del minore. **Se non è prevista un'autorizzazione preventiva** (*Procedura A* delle Linee Guida), il minore visualizza la lista di dati richiesti dal Fornitore di servizi e, dopo aver acconsentito al passaggio dei suoi dati, accede al servizio SPID. **Se è prevista l'autorizzazione preventiva** (*Procedura B* delle Linee Guida), il sistema visualizza una prima maschera che informa il minore della necessità di sottoporre al Genitore richiedente la

richiesta di autorizzazione all'accesso e richiede al minore se vuole procedere alla notifica della richiesta di autorizzazione verso il Genitore richiedente. Se il minore decide di non procedere, la procedura di autenticazione si interrompe. Se decide di inviare la notifica al Genitore richiedente, il minore viene informato che il Genitore richiedente ha 24 ore per approvare la richiesta e che solo dopo tale approvazione sarà possibile accedere al servizio SPID oggetto della richiesta;

- invia una e-mail al Genitore richiedente, per informarlo che è il minore ha richiesto l'approvazione per l'accesso ad uno specifico servizio SPID e che è necessario entrare nell'area personale della propria identità digitale per gestire la richiesta.

8.4.2 Autorizzazione del Genitore richiedente all'accesso ai servizi aderenti a SPID

Una volta ricevuta la notifica della richiesta di approvazione all'accesso ad un servizio SPID da parte del minore, il Genitore richiedente entra nell'area personale della propria identità digitale per gestire la richiesta. Nella scheda "ID Minore" visualizza la lista di minori collegati alla propria utenza e, tramite la funzione "Gestisci", può selezionare l'identità del minore sulla quale agire il controllo parentale. Nella pagina che si apre, il Genitore richiedente può visualizzare la lista di Fornitori di servizi (Service Provider) per i quali è stata richiesta l'approvazione all'accesso da parte del minore.

In caso di nuova richiesta, il Genitore richiedente visualizza il nome del Fornitore di servizi, lo stato "da approvare" e la data di notifica da parte del minore. Se decide di non approvare la richiesta, è sufficiente lasciar trascorrere 24 ore senza nessuna azione e la richiesta viene cancellata. In questo caso il minore riceve un'e-mail che lo informa della mancata approvazione della richiesta. Se decide invece di approvare la richiesta, il Genitore richiedente, tramite la funzione "Approva", entra in una maschera di dettaglio che contiene i seguenti campi:

- Service Provider: nome del Fornitore di servizi, in sola lettura,
- Data e ora di accesso: data e ora di richiesta dell'approvazione, in sola lettura,
- Data fine validità: campo nel quale il Genitore richiedente indica il numero di giorni (da 1 a 365) per i quali il minore è autorizzato all'accesso senza ulteriori azioni richieste al Genitore richiedente,
- Dati del minore richiesti dal Service Provider: lista degli attributi dell'identità digitale del minore richiesti dal Fornitore di servizi per poter erogare il servizio al minore stesso, in sola lettura.

Il Genitore richiedente, tramite appositi tasti, può rifiutare esplicitamente di autorizzare il minore all'accesso. In questo caso il minore riceve un'e-mail che lo informa della mancata approvazione della richiesta. Oppure può approvare l'accesso, nei limiti da lui definiti in pagina. In questo caso il minore riceve un'e-mail che lo informa della avvenuta approvazione della richiesta e della possibilità di fruire del servizio specifico, previa sua autenticazione.

Sulla pagina di gestione delle autorizzazioni viene visualizzato lo stato aggiornato della richiesta e

vengono rese disponibili al Genitore richiedente le funzioni “sospendi” e “revoca”, per inibire temporaneamente o revocare l’autorizzazione all’accesso del minore.

Dopo l’e-mail di conferma dell’autorizzazione, il minore può accedere al servizio previo superamento dei controlli descritti al §8.3.1 e acconsentendo al passaggio dei suoi dati al Fornitore di servizi.

NB: non è mai previsto il mantenimento della sessione di autenticazione del minore, neppure a livello SPID 1.

8.4.3 Effetti della cessazione dell’identità digitale del Genitore richiedente

In caso di cessazione per qualunque motivo dell’identità digitale del Genitore richiedente:

- tutte le autorizzazioni all’accesso concesse al minore decadono, ed il minore può continuare ad utilizzare i soli servizi che non richiedono la preventiva autorizzazione del Genitore richiedente stesso;
- se il minore ha dichiarato di non essere in possesso di un numero di cellulare ed è stato associato alla sua identità il numero di cellulare del Genitore richiedente, l’utilizzo dell’identità viene sospeso fino a che il minore sostituisce il numero del Genitore richiedente con un nuovo numero, con modalità e criteri standard del servizio.

8.4.4 Conservazione dei log di accesso

I log di accesso relativi all’utilizzo dell’identità digitale da parte del minore sono conservati ai sensi della normativa SPID e con le modalità descritte al successivo capitolo 16.

8.5 Ciclo di vita dell’identità del minore

La gestione dell’identità digitale del minore prevede che specifiche azioni siano riservate al Genitore richiedente, nell’ottica del controllo parentale, fino al compimento del 14esimo anno di età del minore, per poi essere agite direttamente dal minore stesso.

In particolare, la sospensione temporanea delle credenziali / dell’identità, la richiesta di revoca e la richiesta degli official log vengono gestite in esclusiva dal Genitore richiedente per il minore con meno di 14 anni. Al compimento del 14esimo anno, il minore può gestire anche in autonomia queste operazioni.

Per i titolari minorenni, Poste Italiane non prevede la raccolta dei consensi al trattamento dei dati per eventuali finalità commerciali.

8.5.1 Sospensione e riattivazione

Il minore con almeno 14 anni potrà procedere in autonomia alla sospensione e alla riattivazione delle proprie credenziali con le modalità descritte ai paragrafi §7.1.1, §7.1.3 e, solo se ha associato un proprio numero di cellulare, §7.1.2.

Il Genitore richiedente potrà gestire la sospensione e riattivazione delle credenziali del minore dalla propria area personale sul sito https://posteid.poste.it, entrando nella scheda "ID Minore", utilizzando la funzionalità "Gestisci" per il minore interessato e successivamente utilizzando l'azione "Sospendi". In ogni momento il Genitore richiedente, dalla stessa pagina, potrà riattivare le credenziali, annullando la sospensione. L'esito delle operazioni vene comunicato via e-mail al Genitore richiedente.

8.5.2 Revoca

8.5.2.1 Richiesta di revoca da parte del minore con almeno 14 anni

Il minore con almeno 14 anni potrà richiedere la revoca della propria identità digitale con le modalità descritte al §7.2.1. È sempre applicabile la procedura descritta al §7.2.2.

8.5.2.2 Richiesta di revoca da parte del Genitore richiedente

Il Genitore richiedente potrà richiedere la revoca dell'identità digitale del minore con le modalità descritte al §7.2.1 (selezionando "Modulo di richiesta di revoca dell'Identità Digitale di un minorenne da parte del Genitore richiedente che ha autorizzato il rilascio dell'Identità del minore" nella sezione "RICHIEDI ASSISTENZA") oppure potrà richiedere la revoca dalla propria area personale sul sito https://posteid.poste.it entrando nella scheda "ID Minore", utilizzando la funzionalità "Gestisci" per il minore interessato e successivamente utilizzando l'azione "Revoca". A completamento delle operazioni di revoca dell'identità, il Genitore richiedente riceve una comunicazione via e-mail con l'esito della revoca.

8.5.2.3 Richiesta di revoca da parte del Secondo genitore

La richiesta di revoca dell'identità del minore può essere indirizzata a Poste Italiane anche dal Secondo genitore, che non ha richiesto il rilascio dell'identità del minore stesso. A tale scopo il Secondo genitore può utilizzare le modalità previste al §7.2.1, selezionando "Modulo di richiesta di revoca dell'Identità Digitale di un minorenne da parte del genitore che non ha richiesto il rilascio dell'Identità del minore" nella sezione "RICHIEDI ASSISTENZA" del sito https://posteid.poste.it e seguendo le istruzioni riportate.

8.5.3 Compimento del 18esimo anno di età

Al compimento del 18esimo anno di età il titolare dell'identità digitale viene informato via e-mail che da quel momento è rimosso qualunque controllo parentale sulla sua ID e che, se non ha interesse a mantenere attivo il servizio PosteID abilitato a SPID, ha la facoltà di recedere dallo stesso tramite la procedura di richiesta di revoca. Se invece intende mantenere attivo il servizio, alla prima autenticazione dovrà fornire esplicita autorizzazione, in assenza della quale sarà inibito l'utilizzo dell'ID per l'accesso ai servizi del Circuito SPID. In caso di mancato utilizzo dell'identità per 24 mesi, questa viene automaticamente revocata, come previsto dai regolamenti SPID.

Nel caso in cui il minore in fase di registrazione abbia dichiarato di non disporre di un numero di cellulare e sia stato associato alla sua identità digitale il numero di cellulare del Genitore richiedente, per continuare ad utilizzare la sua identità dovrà associare un proprio numero di cellulare e seguire la procedura di verifica del possesso dello stesso numero. A seguito di questa operazione, sarà possibile al neomaggiorenne l'attivazione e l'utilizzo della credenziale "Password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato", descritta al §6.1.2.1.

Al neomaggiorenne sarà richiesto di manifestare i propri consensi privacy ai fini commerciali prima di proseguire con l'utilizzo del Servizio.

8.6 Assistenza clienti per il minore

In caso di chiamata al Call Center di Poste Italiane, il Genitore richiedente, opportunamente identificato, può richiedere:

- informazioni sullo stato della pratica di richiesta di attivazione dell'identità digitale del minore che ha lui stesso avviato;
- informazioni sullo stato dell'identità digitale associata al minore / ai minori sui quali agisce il controllo parentale;
- assistenza sull'utilizzo dell'identità del minore.

Il minore con almeno 14 anni di età può operare in autonomia sui canali di assistenza di Poste Italiane, opportunamente identificato, con le modalità in essere.

9 Abilitazione dell'identità digitale all'uso professionale per persone fisiche (SPID Tipo 3)

Il circuito SPID prevede che i Fornitori di Servizi abbiano la facoltà di richiedere all'utente l'utilizzo di un'identità digitale SPID abilitata all'uso professionale per persone fisiche per la fruizione dei servizi erogati. Ogni servizio può quindi essere configurato dal Fornitore di Servizi per essere accessibile in modalità "uso personale" e/o in modalità "uso professionale". Tale caratteristica viene specificata in fase di accesso al singolo servizio.

Il cittadino o professionista già titolare della soluzione PosteID abilitato a SPID può abilitare la propria identità digitale di Poste Italiane all'uso professionale per persone fisiche con una procedura completamente online.

Entrando nell'area riservata della sua Identità Digitale dal sito https://posteid.poste.it, tramite tasto ACCEDI, il cliente potrà visualizzare la scheda "Uso professionale dell'Identità". Cliccando sulla scheda indicata, avrà la possibilità di richiedere l'abilitazione dell'uso professionale, se non lo ha già attivato sulla propria identità, oppure di visualizzare e gestire gli attributi specifici del suo profilo professionale.

Di seguito sono riportate le funzionalità di richiesta dell'uso professionale per persone fisiche e di gestione del ciclo di vita dell'abilitazione e degli attributi specifici del profilo professionale.

9.1 Richiesta

9.1.1 Identificazione

L'identificazione certa del richiedente ai fini dell'abilitazione dell'uso professionale per persone fisiche è garantita dal soddisfacimento dei seguenti prerequisiti:

- l'utente deve essere titolare di un'identità digitale PosteID abilitato a SPID attiva, ottenuta con le modalità descritte nel capitolo 5 Modalità di richiesta del servizio.
- l'utente deve accedere alla propria area riservata sul sito https://posteid.poste.it tramite autenticazione SPID 2, con le modalità operative descritte nel capitolo 6.2 Utilizzo degli strumenti di autenticazione PosteID.

9.1.2 Indicazione attributi relativi all'uso professionale, verifica contatti e configurazione del servizio

In fase di richiesta di abilitazione dell'uso professionale per persone fisiche l'utente deve indicare gli attributi specifici da associare al profilo che dovrà essere utilizzato sui servizi che richiedono un uso dell'identità digitale diverso da quello personale. È facoltà esclusiva del Fornitore di Servizi richiedere

all'utente l'utilizzo di un'identità digitale SPID abilitata all'uso professionale piuttosto che un'identità abilitata all'uso personale.

Il profilo dell'utente associato all'uso professionale dell'identità digitale SPID di Poste Italiane è composto dai dati riportati di seguito.

Attributi identificativi associati alla persona fisica

L'anagrafica del cliente è condivisa con i dati dell'identità digitale PosteID abilitato a SPID ad uso personale attiva.

Attributi specifici per l'uso professionale per persona fisica

Di seguito gli attributi che qualificano il profilo professionale del cliente:

Attributi di contatto:

- Numero di cellulare professionale (obbligatorio). Viene precompilato dal sistema con la proposta del numero di cellulare di contatto del profilo dell'identità ad uso personale ed è modificabile;
- E-mail professionale (obbligatorio). Viene precompilato dal sistema con la proposta dell'e-mail di contatto del profilo dell'identità ad uso personale ed è modificabile;
- Indirizzo di domicilio professionale (obbligatorio). Viene precompilato dal sistema con la proposta dell'indirizzo di domicilio del profilo dell'identità ad uso personale ed è modificabile;
- Indirizzo PEC (facoltativo).

Nel caso l'utente modifichi il numero di cellulare professionale e/o l'e-mail professionale proposti, dopo l'indicazione dei nuovi valori, il sistema procederà all'invio di un codice OTP rispettivamente via SMS e via messaggio di posta elettronica, per la dimostrazione del possesso e certificazione.

Attributi funzionali alla fatturazione del canone del servizio[18]:

- Partita IVA (facoltativo);
- Ragione sociale associata alla Partita IVA (obbligatorio solo se indicata una Partita IVA).
- Forma Giuridica (obbligatorio solo se indicata una Partita IVA).
- Codice Destinatario (obbligatorio solo se indicata una Partita IVA).

[18] Se il cliente non indica una Partita IVA, la fattura emessa viene intestata al codice fiscale del cliente

9.1.3 Presa visione delle condizioni generali del servizio e dell'informativa privacy

Per completare la richiesta di abilitazione dell'uso professionale dell'identità digitale, l'utente prende visione delle Condizioni Generali del Servizio e Condizioni Economiche e dell'informativa privacy.

A seguito della conferma da parte del cliente, attraverso il click sul tasto PROSEGUI, Poste Italiane avvia le attività di provisioning delle funzionalità.

Completato il provisioning tecnico, Poste Italiane invia una e-mail all'indirizzo di contatto del cliente per confermare il buon esito della richiesta e comunicare che è possibile procedere al pagamento per completare l'abilitazione dell'uso professionale sull'identità e poter cominciare ad accedere ai servizi che lo richiedono.

9.1.4 Pagamento del servizio

Dopo aver ricevuto l'e-mail di buon esito della richiesta di abilitazione dell'uso professionale, nella sua area riservata, nella apposita scheda, il cliente troverà tutti i dati inseriti in fase di richiesta, non editabili, la richiesta in stato "Da Attivare" e una data entro cui effettuare il pagamento per completare l'abilitazione[19]. Procedendo con il pagamento, il cliente potrà scegliere l'offerta di suo interesse tra quelle disponibili. Prezzo e durata della sottoscrizione saranno descritte in fase di selezione dell'offerta.

Solo dopo il buon esito del pagamento e la ricezione da parte del cliente di una e-mail di conferma, le funzionalità legate all'abilitazione dell'uso professionale dell'identità diventano effettivamente disponibili sul circuito SPID.

Nel periodo che va dall'istante in cui il cliente effettua con successo il pagamento fino alla ricezione dell'e-mail di conferma, la richiesta del cliente passa nello stato "In Attivazione".

In caso di problemi in fase di provisioning tecnico o di pagamento, il cliente viene informato sulle pagine del servizio della necessità di procedere ad una nuova richiesta.

9.1.5 Conservazione delle evidenze

Con l'attivazione delle funzionalità legate all'uso professionale dell'identità si procede all'invio in conservazione delle evidenze prodotte e raccolte nelle diverse fasi di richiesta dell'abilitazione da parte del cliente e provisioning tecnico.

Il sistema invia in conservazione il fascicolo di richiesta, contenente le evidenze, i dati utilizzati per

[19] Superata la data di entro cui effettuare il pagamento, la richiesta decade e risulta necessaria una richiesta ex novo.

l'associazione e la verifica degli attributi. Il dettaglio dei dati conservati è riportato al paragrafo 16.1 Conservazione evidenze per il rilascio dell'Identità Digitale.

Ad ogni aggiornamento degli attributi o in caso di eventi rilevanti nel ciclo di vita dell'identità digitale, le evidenze delle operazioni vengono inviate in conservazione e rese disponibili al cliente su richiesta.

9.2 Utilizzo e ciclo di vita dell'abilitazione all'uso professionale

Una volta abilitata l'identità all'uso professionale per persona fisica, il cliente potrà accedere ai servizi SPID che lo richiedono utilizzando le stesse credenziali SPID 1 e gli stessi ulteriori fattori / modalità di autenticazione SPID 2 / SPID 3 associati all'uso personale. Per i dettagli si faccia riferimento al capitolo 6 Autenticazione.

Le evoluzioni delle funzionalità e dei processi legati alle credenziali ed alle modalità di autenticazione saranno comuni all'uso personale ed all'uso professionale per persona fisica dell'identità del cliente.

In fase di accesso ai servizi che richiedono l'uso professionale per persona fisica, il cliente, dopo aver effettuato correttamente le operazioni di autenticazione, visualizzerà la lista degli attributi richiesti dal Fornitore di Servizi. Tali attributi, eventualmente in aggiunta a quelli anagrafici comuni, saranno recuperati dal profilo che il cliente ha specificato per l'uso professionale dell'identità. Sui servizi che richiedono l'uso professionale saranno quindi spendibili gli attributi elencati al paragrafo 9.1.2 Indicazione attributi relativi all'uso professionale, verifica contatti e configurazione del servizio.

I suddetti attributi possono essere modificati / aggiornati dal cliente nel corso del ciclo di vita dell'abilitazione all'uso professionale, con le stesse modalità di verifica del possesso e certificazione dei dati previste in fase di primo input. In particolare:

Attributi di contatto:

- Numero di cellulare professionale: modificabile, previa verifica del possesso tramite OTP via SMS;
- E-mail professionale: modificabile, previa verifica del possesso tramite OTP via e-mail;
- Indirizzo di domicilio professionale: modificabile, con normalizzazione dei dati dichiarati e responsabilità del cliente sulla effettiva correttezza;
- Indirizzo PEC: modificabile, con responsabilità del cliente sulla effettiva correttezza.

Attributi funzionali alla fatturazione del canone del servizio[20]:

[20] Se il cliente non indica una Partita IVA, la fattura emessa viene intestata al codice fiscale del cliente

- Partita IVA: modificabile, con controllo sull'esistenza e corrispondenza con la Ragione sociale, con responsabilità del cliente sulla effettiva correttezza;
- Ragione sociale associata alla Partita IVA: modificabile, con controllo di corrispondenza con la Partita IVA, con responsabilità del cliente sulla effettiva correttezza;
- Forma Giuridica: modificabile, con responsabilità del cliente sulla effettiva correttezza;
- Codice Destinatario: modificabile, con responsabilità del cliente sulla effettiva correttezza.

NB: la modifica degli attributi di fatturazione ha effetto sulla fattura emessa successivamente alla modifica stessa, ma non implica la ri-emissione di fattura. È responsabilità del cliente verificare la correttezza dei dati di fatturazione prima dell'emissione della fattura.

In fase di accesso ad un servizio abilitato sia ad un'identità SPID Tipo 1 (uso personale) che di SPID Tipo 3 (uso professionale per persona fisica), sulla pagina di autorizzazione al passaggio degli attributi al Fornitore di Servizi il cliente può optare tra gli attributi associati al suo profilo di "uso personale" (cfr. §5.4) e gli attributi associati al suo profilo di "uso professionale per persona fisica" (cfr. §9.1.2), tramite selezione dello specifico flag visualizzato.

9.3 Rinnovo uso professionale

L'offerta scelta e sottoscritta dal cliente ha una specifica durata e in prossimità della scadenza il sistema prevede dei messaggi di reminder via e-mail per informare il titolare della possibilità di rinnovare la sottoscrizione, scegliendo tra le offerte disponibili in quel momento, per mantenere attiva l'abilitazione dell'uso professionale per persona fisica sulla sua identità digitale PosteID abilitato a SPID. Tali messaggi invitano il cliente ad avviare la procedura di rinnovo dell'abilitazione dall'area riservata del titolare dell'identità digitale, previa autenticazione di livello SPID 2 al sito https://posteid.poste.it, tramite pulsante ACCEDI. Nella scheda "Uso Professionale dell'Identità" dell'area riservata sarà disponibile il pulsante RINNOVA, che, una volta cliccato, permetterà al cliente di selezionare l'offerta di suo interesse tra quelle disponibili e procedere al pagamento dell'importo associato all'offerta. Il rinnovo potrà essere effettuato prima della scadenza dell'offerta sottoscritta ed entro i 30 giorni successivi alla stessa scadenza. Nei 30 giorni successivi alla scadenza l'abilitazione viene sospesa, in attesa di rinnovo, mentre superati i 30 giorni l'abilitazione all'uso professionale viene disattivata, e il cliente viene informato sulle pagine del servizio della necessità di procedere ad una nuova richiesta per poter abilitare nuovamente l'uso professionale per persona fisica.

Prima di procedere al rinnovo, il cliente può modificare gli attributi di fatturazione, per permettere l'emissione della fattura con i riferimenti più aggiornati. Una volta completata con successo la procedura di rinnovo, una eventuale modifica dei dati avrà effetto sulla fattura emessa a seguito di un futuro rinnovo.

La procedura di rinnovo può essere avviata in momenti diversi del ciclo di vita dell'abilitazione all'uso professionale. Di seguito i dettagli per le diverse fattispecie.

Rinnovo prima della scadenza dell'offerta sottoscritta

Se l'utente decide di procedere al rinnovo prima della scadenza dell'offerta precedentemente sottoscritta, potrà selezionare una delle offerte al momento disponibili ed effettuare il pagamento con le modalità e gli strumenti abilitati. La data di validità del rinnovo e di decorrenza della durata della nuova offerta sottoscritta corrisponderà con il giorno successivo alla scadenza dell'offerta ancora in essere. Il cliente riceverà apposita comunicazione sulle pagine del servizio e/o via e-mail con la conferma sull'avvenuto rinnovo e l'aggiornamento delle date di validità dell'abilitazione dell'uso professionale.

Nel caso in cui le procedure di rinnovo / pagamento abbiano esito negativo, il cliente viene informato sulle pagine del servizio della necessità di procedere nuovamente al rinnovo entro i termini generali di validità dell'offerta ancora attiva.

Rinnovo dopo la scadenza dell'offerta sottoscritta, entro 30 giorni

Se l'utente procede al rinnovo dopo la scadenza dell'offerta precedentemente sottoscritta ed entro 30 giorni dalla scadenza stessa, potrà selezionare una delle offerte al momento disponibili ed effettuare il pagamento con le modalità e gli strumenti abilitati. La data di validità del rinnovo e di decorrenza della durata della nuova offerta sottoscritta corrisponderà con l'istante in cui il pagamento viene perfezionato grazie all'incasso dell'importo del costo del servizio, rinnovando contestualmente l'uso professionale dell'identità digitale. Il cliente riceverà apposita comunicazione sulle pagine del servizio e/o via e-mail con la conferma sull'avvenuto rinnovo e l'aggiornamento delle date di validità dell'abilitazione dell'uso professionale.

Nel tempo che intercorre tra la data di scadenza dell'offerta precedentemente sottoscritta e i successivi 30 giorni, l'uso professionale viene disabilitato con gli attributi ad esso associati non modificabili.

Nel caso in cui le procedure di rinnovo / pagamento abbiano esito negativo, il cliente viene informato sulle pagine del servizio della necessità di procedere nuovamente al rinnovo entro i 30 giorni successivi alla scadenza, per non incorrere nella disattivazione dell'abilitazione all'uso professionale.

9.4 Recesso anticipato dall'abilitazione dell'uso professionale

Nel caso in cui il cliente ritenga di voler recedere dall'abilitazione all'uso professionale associato alla sua identità digitale prima della naturale scadenza dell'offerta sottoscritta, dovrà accedere alla propria area riservata sul sito https://posteid.poste.it, previa autenticazione di livello SPID 2, tramite pulsante ACCEDI. Nella scheda "Uso professionale dell'Identità" dell'area riservata sarà disponibile

un link alla funzionalità di recesso anticipato. Avviata la procedura di recesso, previa conferma della volontà di disabilitare l'uso professionale, il cliente tornerà ad utilizzare la propria identità digitale PosteID abilitato a SPID solo ad uso personale, disattivando il profilo professionale ed eliminando dalla basedati gli attributi specifici.

Nel caso di recesso anticipato non è previsto nessun rimborso per la quota parte di offerta sottoscritta e non goduta.

A fronte dell'avvenuto richiesta di recesso anticipato, l'utente riceverà all'indirizzo e-mail di contatto dell'Identità Digitale una conferma di avvenuta disabilitazione.

Qualora l'utente riceva la e-mail senza che abbia fatto alcuna richiesta di recesso, deve contattare il Servizio Clienti (vedi capitolo 11 Rapporti con gli utenti) per ricevere adeguato supporto.

Qualora l'utente voglia procedere alla revoca del servizio, ma non ricordi le credenziali per accedere all'area riservata, può recuperarle dalle pagine del sito https://posteid.poste.it.

Qualora sia effettuata la revoca del servizio di Identità Digitale PosteID abilitato a SPID, come descritto al paragrafo 7.3 Revoca, automaticamente verrà effettuata anche la disabilitazione dell'uso professionale dell'identità. Non è previsto in nessun caso il mantenimento dell'uso professionale dell'identità a seguito di revoca del servizio PosteID abilitato a SPID.

10 Modalità di richiesta del servizio di identità digitale SPID ad uso professionale per persona giuridica (SPID Tipo 4)

Il circuito SPID prevede che i Fornitori di Servizi abbiano la facoltà di richiedere all'utente l'utilizzo di un'identità digitale SPID abilitata all'uso professionale per persone giuridiche (SPID Tipo 4) per la fruizione dei servizi destinati ad una organizzazione. Ogni servizio può quindi essere configurato dal Fornitore di Servizi per essere accessibile in modalità "uso personale" e/o in modalità "uso professionale". Tale caratteristica viene specificata in fase di accesso al singolo servizio.

Il Rappresentante Legale di un'organizzazione può richiedere l'abilitazione di identità digitali associate a rappresentanti, dipendenti o collaboratori dell'organizzazione stessa, utilizzabili per la fruizione di servizi destinati direttamente ed esclusivamente all'organizzazione. Tale richiesta può essere effettuata mediante una procedura completamente online.

La procedura può essere avviata sito https://posteid.poste.it/organizzazione, tramite tasto ACCEDI.

Il servizio di identità digitale SPID ad uso professionale per persona giuridica prevede diversi ruoli:

- **Rappresentante legale dell'organizzazione**: è la persona che, dotata di opportuni poteri, richiede l'attivazione del servizio, sottoscrive il contratto con Poste Italiane, indica e gestisce i Referenti di governo, i Referenti di gestione ed eventualmente anche gli Utilizzatori finali. Potrà intervenire sul ciclo di vita delle identità dei suddetti soggetti, anche richiedendone la revoca. Viene dotato di identità digitale SPID ad uso professionale per persona giuridica, con la quale può operare per conto dell'organizzazione stessa sui servizi abilitati.
- **Referente di governo**: una o più persone incaricate a sistema dal Rappresentante legale (o da altro Referente di governo) di indicare e gestire altri Referenti di governo, i Referenti di gestione e gli Utilizzatori finali che verranno dotati di identità digitale SPID ad uso professionale per persona giuridica. Potrà intervenire sul ciclo di vita delle suddette identità, anche richiedendone la revoca. In nessun caso può ricoprire anche il ruolo di Referente di gestione; viene dotato di identità digitale SPID Tipo 4 per operare per conto dell'organizzazione stessa sui servizi abilitati.
- **Referente di gestione**: una o più persone incaricate a sistema dal Rappresentante legale (o da un Referente di governo) di effettuare l'identificazione a vista dei Referenti di governo, di altri Referenti di gestione e degli Utilizzatori finali prima di mettere a loro disposizione l'identità digitale SPID ad uso professionale per persona giuridica. In nessun caso può ricoprire il ruolo di Referente di governo; viene dotato di identità digitale SPID Tipo 4 per operare per conto dell'organizzazione stessa sui servizi abilitati.
- **Utilizzatore finale**: è un rappresentante, dipendente o collaboratore dell'organizzazione che viene dotato di identità digitale SPID ad uso professionale per persona giuridica, previa identificazione a vista effettuata dal Referente di gestione o tramite altre modalità rese tempo per tempo disponibili nell'ambito del servizio, con la quale può operare con l'identità

che riporta sia i dati dell'utilizzatore che dell'Organizzazione.

L'attivazione del servizio di identità digitale SPID Tipo 4 prevede tre fasi:

1. **richiesta da parte del Rappresentante legale dell'organizzazione**: vengono indicati i dati della persona giuridica e del rappresentante legale stesso (compresa la scelta di credenziali SPID), viene fornito il numero di identità SPID Tipo 4 richieste, viene sottoscritto il contratto di servizio, vengono manifestati i consensi privacy commerciali e, previa verifica dell'identità e del titolo del richiedente nonché dei dati dell'organizzazione, viene effettuato il pagamento del corrispettivo annuale del servizio. Una volta attivato il contratto di servizio, il Rappresentante legale può indicare a sistema i dati anagrafici e di contatto dei Referenti di governo e/o dei Referenti di gestione dell'organizzazione.
2. **indicazione degli Utilizzatori finali**: il Rappresentante legale dell'organizzazione e/o il Referente di governo dell'organizzazione, previo accesso all'area riservata in post-login, inseriscono a sistema la lista di Utilizzatori finali a cui associare le identità digitali SPID ad uso professionale per persona giuridica.
3. **rilascio delle identità digitali SPID ad uso professionale per persona giuridica**: gli Utilizzatori finali si registrano e scelgono le proprie credenziali SPID Tipo 4, che saranno abilitate ad operare solo a seguito della verifica dell'identità effettuata tramite il Referente di gestione o le altre modalità rese tempo per tempo disponibili nell'ambito del servizio.

Di seguito sono riportate le funzionalità di richiesta dell'uso professionale per persone giuridiche e di gestione del ciclo di vita dell'abilitazione e degli attributi specifici del profilo professionale.

10.1 Richiesta del servizio e attivazione delle ID SPID ad uso professionale per persona giuridica

Per avviare la richiesta il Rappresentante legale di un'organizzazione si collega al sito https://posteid.poste.it/organizzazione e procede tramite tasto REGISTRATI SUBITO.

10.1.1 Registrazione dell'organizzazione e del Rappresentante legale richiedente

Dopo aver selezionato "Sì, sono il Rappresentante legale" e cliccato sul tasto PROSEGUI, viene visualizzata l'opzione di registrazione ex novo in alternativa all'avvio della procedura di subentro ad un Rappresentante legale di un'organizzazione già attiva. Dopo aver selezionato "Sì, devo attivare per la prima volta l'ID dell'organizzazione" e cliccato sul tasto PROSEGUI, viene visualizzata una pagina con l'indicazione dei dati e dei documenti necessari per procedere con la richiesta, ivi inclusa la disponibilità di una firma digitale personale del Rappresentante legale stesso. Cliccando sul tasto PROSEGUI viene avviata la procedura di registrazione, che prevede l'indicazione di:

- dati dell'organizzazione,
- dati di contatto e indirizzo della sede legale,
- numero di identità SPID Tipo 4 richieste, per ottenere un preventivo del canone periodico corrispondente,
- dati amministrativi dell'organizzazione,
- dati anagrafici del Rappresentante legale richiedente,
- dati del documento di riconoscimento del Rappresentante legale richiedente,
- dati di contatto e indirizzo di domicilio professionale.

Dopo il completamento della compilazione dei suddetti dati, il sistema propone una pagina di riepilogo, per permettere al richiedente una verifica ulteriore della correttezza delle informazioni.

Proseguendo, il Rappresentante legale imposta i fattori di sicurezza della propria identità digitale ad uso professionale per persona giuridica:

- e-mail professionale, da utilizzare come nome utente, il cui possesso viene controllato contestualmente tramite invio e verifica di un codice OTP,
- numero di cellulare professionale, da utilizzare come nome utente, il cui possesso viene controllato contestualmente tramite invio e verifica di un codice OTP,
- password,

inoltre visualizza e accetta le Condizioni Generali del Servizio e Condizioni Economiche, prende visione delle istruzioni operative per l'attivazione dell'identità digitale ad uso professionale per persona giuridica, prende visione dell'informativa privacy del servizio e manifesta i consensi privacy commerciali per l'organizzazione.

La fase si conclude con una thank-you-page, che informa il richiedente che dovrà attendere un'e-mail di conferma per poter procedere all'identificazione. Il sistema invia l'e-mail solo dopo aver effettuato controlli sull'anagrafica e sui dati del documento del richiedente, mediante interrogazione delle fonti autoritative disponibili.

10.1.2 Identificazione del Rappresentante legale richiedente

Quando il Rappresentante legale richiedente riceve l'e-mail di conferma del buon esito dei controlli preliminari, si collega al sito https://posteid.poste.it/organizzazione e procede tramite tasto ACCEDI.

Il sistema visualizza una pagina di riepilogo dei dati della pratica e avvia l'identificazione del richiedente. L'identità del Rappresentante legale richiedente viene verificata in maniera certa tramite apposizione e controllo informatico di una firma digitale a lui intestata. Il sistema genera un modulo di riepilogo .pdf dei dati della registrazione, che il Rappresentante legale richiedente deve scaricare dalla pagina MODULO DI ADESIONE. Una volta scaricato il file .pdf, su questo deve essere apposta la firma digitale e successivamente il file .pdf firmato deve essere ricaricato sulla medesima pagina

MODULO DI ADESIONE. Il sistema verifica la validità della firma digitale, l'assenza di revoca o sospensione della stessa sulla Certificate Revocation List, la corrispondenza tra il CF del titolare della firma e il CF del Rappresentante legale richiedente.

Superati i controlli della firma digitale, la pratica completa viene inviata ad una struttura di back-office di Poste Italiane, che verifica, mediante l'interrogazione di fonti autoritative disponibili:

- l'esistenza dell'organizzazione e la correttezza dei dati registrati.
- la titolarità del richiedente a rappresentare l'organizzazione.

Il buon esito delle verifiche viene comunicato al Rappresentante legale richiedente tramite e-mail, con l'invito a concludere l'attivazione del servizio con il pagamento del corrispettivo specifico. A seguito del buon esito del pagamento viene attivato il servizio e, contestualmente, l'ID uso professionale dell'Organizzazione del Rappresentante Legale.

10.1.3 Attivazione del servizio e identificazione del Referente di governo e del Referente di gestione

Quando il Rappresentante legale richiedente riceve l'e-mail di conferma del buon esito dei controlli di registrazione, si collega al sito https://posteid.poste.it/organizzazione e procede tramite tasto ACCEDI. A fronte di un'autenticazione di livello SPID 2 con le credenziali in suo possesso, viene visualizzata l'area di post-login del Servizio.

Il Rappresentante legale può procedere al censimento di due utenti con un ruolo specifico nel servizio: Referente di governo e Referente di gestione. Non è obbligatorio assegnare entrambi i ruoli, ma non è possibile centralizzare i ruoli e le rispettive responsabilità di processo e le funzionalità agite sul servizio. Non è possibile che un unico utente abbia entrambi i ruoli a sistema, poiché questi sono unici e alternativi. Inoltre il Rappresentante legale può indicare direttamente una lista di Utilizzatori finali. Per ogni ruolo vanno indicati: dati anagrafici (CF), dati di contatto (e-mail professionale) e ruolo (Referente di governo, Referente di gestione o Utilizzatore finale).

Gli utenti ricevono un'e-mail contenente un codice alfanumerico personale e l'indicazione di collegarsi al sito https://posteid.poste.it/organizzazione e procedere tramite tasto REGISTRATI SUBITO. Dopo aver selezionato "No, non sono il Rappresentante legale" e cliccato sul tasto PROSEGUI, viene avviata la procedura di registrazione e identificazione. Il primo step consiste nell'inserimento dei rispettivi:

- dati anagrafici,
- dati del documento di riconoscimento,
- indirizzo di domicilio professionale.
- codice personale di verifica ricevuto via e-mail.

Il sistema verifica la corrispondenza dei dati e del codice con quanto censito dal Rappresentante legale e inviato via e-mail. In caso di esito negativo del controllo, la procedura viene interrotta. In caso di esito positivo del controllo, il sistema propone una pagina di riepilogo, per permettere agli utenti una verifica ulteriore della correttezza delle informazioni inserite

Proseguendo, gli utenti scelgono i fattori di sicurezza della propria identità digitale ad uso professionale per persona giuridica:

- e-mail professionale, da utilizzare come nome utente, il cui possesso viene controllato contestualmente tramite invio e verifica di un codice OTP,
- numero di cellulare professionale, da utilizzare come nome utente, il cui possesso viene controllato contestualmente tramite invio e verifica di un codice OTP,
- password,

prendono visione delle istruzioni operative per l'attivazione dell'identità digitale SPID Tipo 4 e confermano la richiesta di attivazione tramite tasto PROSEGUI.

Il sistema avvia lo step di identificazione forte degli utenti. Gli utenti possono scegliere la modalità di identificazione:

- «Voglio utilizzare la mia identità personale»: l'utente può utilizzare un'identità digitale PosteID abilitato a SPID per l'identificazione, tramite autenticazione di livello SPID 2. È escluso l'utilizzo di identità digitali SPID diverse da quella rilasciata da Poste Italiane.
- «Voglio utilizzare la mia firma Digitale»: l'utente può utilizzare una firma digitale di cui è titolare, con una procedura che prevede che il sistema generi un modulo di riepilogo dei dati in formato .pdf, che l'utente scarica in locale e sul quale appone la sua firma digitale, prima di ricaricare il file .pdf firmato. I controlli applicati sono i medesimi descritti per l'identificazione del Rappresentante legale.
- «Voglio procedere all'identificazione tramite il Referente di gestione»: l'utente dovrà essere identificato dal Referente di gestione, dovrà fornire nelle mani dello stesso il codice personale di verifica ricevuto via e-mail e il proprio documento di riconoscimento (lo stesso indicato in fase di registrazione, scegliendo tra carta di identità, passaporto o patente emessi da autorità italiana in corso di validità).

A seguito del buon esito dello step di identificazione, le credenziali degli utenti diventano attive e li abilitano ad accedere al post-login del servizio, per espletare i compiti previsti dai rispettivi ruoli, tramite specifiche funzionalità di sistema.

In caso di fallimento della fase di identificazione o di mancata identificazione nei 30 giorni successivi alla registrazione dell'utente, la registrazione viene annullata e cancellati i dati.

10.1.4 Funzionalità a disposizione del Referente di governo per il censimento di nuovi

utenti

Quando il Referente di governo riceve l'e-mail di conferma del buon esito dell'attivazione delle sue credenziali, si collega al sito https://posteid.poste.it/organizzazione e procede tramite tasto ACCEDI.

A fronte di un'autenticazione di livello SPID 2 con le credenziali in suo possesso, viene visualizzata l'area di post-login del Servizio.

Il sistema presenta una sezione in cui sono visualizzabili e modificabili i suoi dati di registrazione e una sezione in cui il Referente di governo può effettuare il censimento di altri Referenti di governo, dei Referenti di gestione e degli Utilizzatori finali da abilitare all'identità digitale SPID ad uso professionale per persona giuridica.

Il censimento prevede l'indicazione per ogni utente di dati anagrafici (CF) e dati di contatto (e-mail professionale) ed è propedeutico alla fase di registrazione e identificazione degli stessi.

Una volta completato il censimento, il Referente di governo conferma i dati e il sistema invia all'utente censito un'e-mail contenente un codice alfanumerico personale e l'indicazione di collegarsi al sito https://posteid.poste.it/organizzazione.

10.1.5 Funzionalità a disposizione degli utenti per l'identificazione senza operatore

Quando un utente non sceglie l'opzione «Voglio procedere all'identificazione tramite il Referente di gestione» in fase di registrazione, il Referente di gestione non viene coinvolto e l'identificazione avviene contestualmente alla registrazione secondo due modalità:

- L'utente seleziona «Voglio utilizzare la mia identità personale» e clicca sul tasto PROSEGUI. L'utente viene reindirizzato sulla pagina di login SPID del servizio PosteID abilitato a SPID, con richiesta di effettuare un'autenticazione di livello SPID 2. Procedendo con le modalità e gli strumenti di tempo in tempo resi disponibili dal servizio SPID di Poste Italiane, l'utente completa la procedura di autenticazione, che richiede il passaggio degli attributi nome, cognome e codice fiscale e, in caso il sistema verifichi la corrispondenza dei dati di registrazione con gli attributi suddetti, conclude l'identificazione con esito positivo, procedendo alla conservazione dell'asserzione di autenticazione. In caso il sistema non verifichi la corrispondenza dei dati di registrazione con gli attributi suddetti, conclude l'identificazione con esito negativo, informando l'utente e permettendo allo stesso di scegliere una modalità alternativa di identificazione tra quelle disponibili. È sempre escluso l'utilizzo di identità digitali SPID diverse da quella rilasciata da Poste Italiane.
- L'utente seleziona «Voglio utilizzare la mia firma Digitale» e clicca sul tasto PROSEGUI. L'utente viene reindirizzato su una pagina che prevede una funzionalità di download in locale di un modulo .pdf contenente il riepilogo dei dati di registrazione dell'utente. L'utente deve apporre una firma digitale di cui è titolare sul suddetto modulo e poi utilizzare la

funzionalità di upload del file .pdf firmato. Il sistema applica i medesimi controlli descritti per l'identificazione del Rappresentante legale. In caso il sistema verifichi il corretto superamento dei controlli, conclude l'identificazione con esito positivo, procedendo alla conservazione del modulo firmato. In caso il sistema non verifichi il corretto superamento dei controlli, conclude l'identificazione con esito negativo, informando l'utente e permettendo allo stesso di scegliere una modalità alternativa di identificazione tra quelle disponibili.

A valle del buon esito dei controlli di sistema, l'identità digitale SPID Tipo 4 viene attivata per l'utente identificato, con contestuale invio allo stesso di un'e-mail di conferma.

10.1.6 Funzionalità a disposizione del Referente di gestione per l'identificazione con operatore di nuovi utenti

Quando un utente sceglie l'opzione «Voglio procedere all'identificazione tramite il Referente di gestione» in fase di registrazione, il Referente di gestione collegandosi alla sua area di post-login del Servizio, a fronte di un'autenticazione di livello SPID 2 con le credenziali in suo possesso, visualizza la richiesta di identificazione.

Il sistema presenta una sezione in cui il Referente di gestione ha a disposizione le funzionalità a supporto dello step di identificazione degli utenti registrati. Il Referente di gestione visualizza nome, cognome e codice fiscale di ogni utente da identificare e può selezionare l'utente per cui effettuare l'identificazione.

Per l'utente selezionato, l'identificazione richiede che il Referente di gestione:

- riceva dalle mani dell'utente il codice di verifica personale utilizzato in fase di registrazione e lo digiti a sistema per avviare la procedura. Solo nel caso in cui il sistema verifichi la corrispondenza tra codice fiscale e codice di verifica personale, l'identificazione può proseguire;
- riceva dalle mani dell'utente il documento di riconoscimento censito in fase di registrazione (carta di identità, passaporto o patente) e digiti a sistema il numero del documento e la scadenza riportati sullo stesso. Solo nel caso in cui il sistema verifichi la corrispondenza tra dati del documento censiti dall'utente in fase di registrazione e dati del documento censiti dal Referente di gestione in fase di identificazione, l'identificazione può proseguire;
- identifichi l'utente, verificando la corrispondenza tra lo stesso e quando riportato sul documento di riconoscimento in termini di fotografia e dati;
- effettui a sistema l'upload della copia per immagine del documento di riconoscimento e del documento attestante il codice fiscale dell'utente.

Al termine di questi passaggi, il Referente di gestione conferma il buon esito dell'identificazione e completa la procedura di attivazione dell'utente. A valle del buon esito dei controlli di sistema, si

procede con l'invio in conservazione della documentazione raccolta e l'identità digitale SPID Tipo 4 viene attivata per l'utente identificato, con contestuale invio allo stesso di un'e-mail di conferma.

10.1.7 Conservazione delle evidenze

Con l'attivazione dell'identità digitale SPID Tipo 4 si procede all'invio in conservazione delle evidenze prodotte e raccolte nelle diverse fasi di richiesta dell'abilitazione da parte dell'utente e provisioning tecnico.

Il sistema invia in conservazione il fascicolo di richiesta, contenente le evidenze, i dati utilizzati per l'associazione e la verifica degli attributi. Il dettaglio dei dati conservati è riportato al paragrafo 16.1 Conservazione evidenze per il rilascio dell'Identità Digitale.

Ad ogni aggiornamento degli attributi o in caso di eventi rilevanti nel ciclo di vita dell'identità digitale, le evidenze delle operazioni vengono inviate in conservazione e rese disponibili all'utente su richiesta.

10.2 Utilizzo e ciclo di vita dell'ID SPID ad uso professionale per persona giuridica

10.2.1 Operatività dell'Utilizzatore finale

Una volta attivata l'identità SPID Tipo 4, l'utente potrà accedere ai servizi SPID che lo richiedono utilizzando le credenziali SPID 1 ("password") e le credenziali SPID 2 compatibili ("password e codice di verifica OTP inviato tramite SMS sul telefono mobile certificato" oppure "password e codice di verifica OTP inviato tramite e-mail sull'indirizzo di contatto certificato"). Per i dettagli si faccia riferimento al capitolo 6 Autenticazione.

In fase di accesso ai servizi che richiedono lo SPID Tipo 4, l'utente, dopo aver effettuato correttamente le operazioni di autenticazione, visualizzerà la lista degli attributi richiesti dal Fornitore di Servizi. Tali attributi, eventualmente in aggiunta a quelli anagrafici comuni, saranno recuperati dal profilo che l'utente ha specificato per l'uso professionale per persona giuridica. Sui servizi che richiedono lo SPID Tipo 4 saranno quindi spendibili gli attributi descritti al paragrafo 10.1 Richiesta del servizio e attivazione delle ID SPID ad uso professionale per persona giuridica.

I suddetti attributi possono essere modificati / aggiornati dall'utente nel corso del ciclo di vita della propria ID SPID ad uso professionale per persona giuridica, con le stesse modalità di verifica del possesso e certificazione dei dati previste in fase di primo input. In particolare:

<u>Attributi di contatto</u>:

- Numero di cellulare professionale: modificabile, previa verifica del possesso tramite OTP via SMS;

- E-mail professionale: modificabile, previa verifica del possesso tramite OTP via e-mail;
- Indirizzo di domicilio professionale: modificabile, con normalizzazione dei dati dichiarati e responsabilità del cliente sulla effettiva correttezza;
- Indirizzo PEC: modificabile, con responsabilità del cliente sulla effettiva correttezza.

Nel caso in cui l'Utilizzatore finale voglia disattivare l'ID a sé associata, per qualunque motivo, deve rivolgersi al Rappresentante legale o ad un Referente di Governo della propria organizzazione, che procederà alla sospensione e/o alla revoca dell'ID.

10.2.2 Operatività del Referente di governo sulle ID associate all'organizzazione

Il Referente di governo ha a disposizione nella sua area di post-login una dashboard che permette di:

- visualizzare l'elenco di utenti associati all'organizzazione, con qualsiasi ruolo (Referenti di governo, Referenti di gestione, Utilizzatori finali),
- visualizzare per ognuno lo stato dell'ID associata (richiesta, attiva, sospesa, revocata),
- aggiornare lo stato della singola ID associata, ad esclusione dello stato di prima attivazione, che può essere determinato esclusivamente dal superamento con esito positivo di una procedura di identificazione,
- indicare i dati di un nuovo soggetto per il quale viene avviata la procedura di richiesta dell'ID SPID Tipo 4 collegata all'organizzazione.

10.3 Rinnovo del servizio di ID SPID ad uso professionale per persona giuridica

Con l'approssimarsi della data di scadenza del contratto di servizio stipulato tra Poste Italiane e l'organizzazione, il sistema prevede dei messaggi di reminder via e-mail per informare il Rappresentante legale della possibilità di rinnovare il servizio, previo pagamento del corrispettivo previsto. Il rinnovo potrà essere effettuato prima della scadenza dell'offerta sottoscritta ed entro i 30 giorni successivi alla stessa scadenza. Nei 30 giorni successivi alla scadenza il funzionamento delle ID viene sospeso, in attesa di rinnovo, mentre superati i 30 giorni le ID vengono disattivate, e il Rappresentante legale dell'organizzazione viene informato via e-mail della necessità di procedere ad una nuova richiesta per poter attivare nuovamente il servizio di ID SPID ad uso professionale per persona giuridica.

La procedura di rinnovo può essere avviata in momenti diversi del ciclo di vita dell'abilitazione all'uso professionale. Di seguito i dettagli per le diverse fattispecie.

Rinnovo prima della scadenza dell'offerta sottoscritta

Se l'utente decide di procedere al rinnovo prima della scadenza dell'offerta precedentemente sottoscritta, previo pagamento del corrispettivo previsto, la data di validità del rinnovo e di decorrenza della durata della nuova offerta sottoscritta corrisponderà con il giorno successivo alla scadenza dell'offerta ancora in essere. Il Rappresentante legale riceverà apposita comunicazione sulle pagine del servizio e/o via e-mail con la conferma sull'avvenuto rinnovo e l'aggiornamento delle date di validità del contratto di servizio.

Nel caso in cui le procedure di rinnovo / pagamento abbiano esito negativo, il Rappresentante legale viene informato sulle pagine del servizio della necessità di procedere nuovamente al rinnovo entro i termini generali di validità dell'offerta ancora attiva.

Rinnovo dopo la scadenza dell'offerta sottoscritta, entro 30 giorni

Se il Rappresentante legale procede al rinnovo dopo la scadenza dell'offerta precedentemente sottoscritta ed entro 30 giorni dalla scadenza stessa, potrà selezionare una delle offerte al momento disponibili ed effettuare il pagamento con le modalità e gli strumenti abilitati. La data di validità del rinnovo e di decorrenza della durata della nuova offerta sottoscritta corrisponderà con l'istante in cui il pagamento viene perfezionato grazie all'incasso dell'importo del costo del servizio, rinnovando contestualmente il servizio di ID SPID ad uso professionale per persona giuridica. Il Rappresentante legale riceverà apposita comunicazione sulle pagine del servizio e/o via e-mail con la conferma sull'avvenuto rinnovo e l'aggiornamento delle date di validità del contratto di servizio.

Nel tempo che intercorre tra la data di scadenza dell'offerta precedentemente sottoscritta e i successivi 30 giorni, le ID associate all'organizzazione vengono disabilitate.

Nel caso in cui le procedure di rinnovo / pagamento abbiano esito negativo, il Rappresentante legale viene informato sulle pagine del servizio della necessità di procedere nuovamente al rinnovo entro i 30 giorni successivi alla scadenza, per non incorrere nella disattivazione completa del servizio.

10.4 Recesso anticipato dal servizio di ID SPID ad uso professionale per persona giuridica

Nel caso in cui il Rappresentante legale ritenga di voler recedere dal contratto di servizio prima della naturale scadenza dell'offerta sottoscritta, dovrà accedere alla propria area riservata sul sito https://posteid.poste.it/organizzazione, previa autenticazione di livello SPID 2, tramite pulsante ACCEDI. Nella scheda "Organizzazione" dell'area riservata sarà disponibile un link alla funzionalità di recesso anticipato. Avviata la procedura di recesso dal contratto di servizio, previa conferma della volontà di disattivare tutte le ID associate all'organizzazione, l'utilizzo delle ID verrà sospeso.

Nel caso di recesso anticipato non è previsto nessun rimborso per la quota parte di offerta sottoscritta

e non goduta.

A fronte dell'avvenuto richiesta di recesso anticipato, il Rappresentante legale riceverà all'indirizzo e-mail di contatto una conferma di avvenuta disabilitazione.

Qualora l'utente riceva la e-mail senza che abbia fatto alcuna richiesta di recesso, deve contattare il Servizio Clienti (vedi capitolo 11 Rapporti con gli utenti) per ricevere adeguato supporto.

Qualora l'utente voglia procedere alla revoca del servizio, ma non ricordi le credenziali per accedere all'area riservata, può recuperarle dalle pagine del sito https://posteid.poste.it/organizzazione, con le modalità previste.

11 Rapporti con gli utenti

Per i titolari del servizio ***PosteID abilitato a SPID per uso personale e professionale per persona fisica***, 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 al numero 06.977.977.77, sia dall'Italia che dall'estero.

Relativamente al servizio di ***PosteID SPID ad uso professionale per persona giuridica SPID Tipo 4)***, 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 al numero 06.977.977.77, sia dall'Italia che dall'estero.

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
E-mail: responsabilemanualeposteid@posteitaliane.it

12 Condizioni di fornitura

Il Servizio PosteID abilitato a SPID per uso personale (SPID Tipo 1) prevede un corrispettivo annuo per l'utilizzo della funzionalità di accesso ai servizi che espongono il pulsante "ENTRA CON SPID", a partire dalla scadenza del primo anno dall'attivazione del Servizio.

Il Servizio PosteID SPID ad uso professionale per persone fisiche (SPID Tipo 3) è a pagamento e prevede un corrispettivo legato alla durata selezionata dal cliente (1-3 anni di copertura del servizio).

Le condizioni economiche, connesse anche ad eventuali funzionalità opzionali aggiuntive o accessorie, ad eventuali servizi di natura professionale o rivolti alle persone giuridiche, delle relative funzionalità e dei servizi opzionali / accessori sono specificate nell'apposito documento Condizioni Generali del Servizio e Condizioni Economiche, disponibile sul sito https://www.poste.it/posteid e sul portale del Servizio https://posteid.poste.it.

La durata del servizio, le modalità di recesso o risoluzione sono riportate nelle Condizioni Generali del Servizio e Condizioni Economiche, disponibili sul sito https://www.poste.it/posteid e sul portale del Servizio https://posteid.poste.it.

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.

Il Servizio PosteID SPID ad uso professionale per persone giuridiche (SPID Tipo 4) è a pagamento per le persone giuridiche.

Le condizioni economiche sono descritte nel documento Condizioni Generali del Servizio e Condizioni Economiche.

La durata del servizio, le modalità di recesso o risoluzione sono riportate nelle Condizioni Generali del Servizio e Condizioni Economiche.

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/organizzazione, 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.

13 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.

13.1 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 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

Descrizione obblighi del Gestore
Adeguare i propri sistemi a seguito dell'aggiornamento della normativa
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 conservarne 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 e-mail 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
Mantenere l'identità sospesa su richiesta dell'utente fino alla ricezione 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
Mantenere l'identità sospesa su richiesta dell'utente finché non riceve una richiesta di revoca o riattivazione 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 livello SPID 2 o SPID 3
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

13.2 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
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
Garantire 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

13.3 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.

14 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 di 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

15 Livelli di servizio

Il Gestore garantisce la continuità operativa dei servizi di sua competenza afferenti allo SPID, conformemente agli indicatori di qualità e livelli di servizio allegati alla Convenzione per l'adesione a SPID.

Codice	Indicatore di qualità	Modalità funzionamento	Valore limite
IQ-01	Disponibilità del sotto-servizio di registrazione identità	*Erogazione automatica*	>= 99,5%
			Singolo evento di indisponibilità <= 6 ore
		Erogazione in presenza	>= 98,0%
IQ-02	Tempo di risposta del sotto-servizio di registrazione identità		<= 12h (ore lavorative) per il 95% di richieste registrazione utente
IQ-03	Disponibilità del sotto-servizio di gestione rilascio credenziali	*Erogazione automatica*	>= 99,5%
			Singolo evento di indisponibilità <= 6 ore
		Erogazione in presenza	>= 98,0%
IQ-04	Tempo di rilascio credenziali	*Erogazione da remoto*	<= 5 giorni lavorativi
		Erogazione in presenza	<= 3 giorni lavorativi
IQ-05	Tempo riattivazione delle credenziali		<= 2 giorni lavorativi
IQ-06	Disponibilità del sotto-servizio di sospensione e revoca delle credenziali		>= 99,5%
			Singolo evento di indisponibilità <= 6 ore
IQ-07	Tempo di sospensione delle credenziali	*Erogazione automatica*	<= 1 minuto
		Erogazione in presenza	<= 10 minuti
IQ-08	Tempo di revoca delle credenziali successiva alla sospensione		<= 5 giorni lavorativi
IQ-09	Disponibilità del sotto-servizio di rinnovo e sostituzione delle credenziali	*Erogazione automatica*	>= 99,5%
			Singolo evento di indisponibilità <= 6 ore
		Erogazione in presenza	>= 98,0%

Codice	Indicatore di qualità	Modalità funzionamento	Valore limite
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		<= 2 giorni lavorativi
IQ-10-bis[21]	Tempo di dispiegamento/aggiornamento metadata		<= 2 giorno lavorativi
IQ-11	Disponibilità del sotto-servizio di autenticazione		>= 99,5%
			Singolo evento indisponibilità <= 6 ore
IQ-12	Tempo di risposta del sotto-servizio di autenticazione		*Coefficiente moltiplicativo = 300* *300: tot. eID nazionale = xx : tot. eID gestore* $xx = \frac{300 \times \text{tot. eID gestore}}{\text{tot. eID nazionali}}$ *xx = numero effettivo di richieste di autenticazioni al secondo (auth sec) correlate alle identità rilasciate dal gestore.* *Se xx < 100, il gestore deve garantire almeno 100 auth sec. Tempi di risposta ≤ 2 sec per il 98% delle richieste di autenticazione* *Per un numero di richieste di auth sec superiore al coefficiente moltiplicativo, lo SLA andrà concordato in anticipo tra AgID e gestori.*
IQ-13	RPO (*) sotto-servizio registrazione e rilascio delle identità		1 ora
IQ-14	RTO (*) sotto-servizio registrazione e rilascio delle identità		8 ore
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

[21] Indicatore calcolabile a valle del completo dispiegamento della piattaforma di scambio automatico dei metadata

***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.*

16 Sicurezza del servizio PosteID abilitato a SPID

16.1 Conservazione evidenze per il rilascio dell'Identità Digitale

Al fine di poter documentare la corretta attribuzione di una Identità Digitale PosteID, sia relativamente all'attivazione dell'identità ad "uso personale" che all'abilitazione dell'"uso professionale", 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 (*). Copia dei documenti utilizzati per l'identificazione (documento di identità e tessera sanitaria/codice fiscale). Log del processo di identificazione tramite CIE o Passaporto Elettronico e foto estratta dal documento. 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 (CNS) attiva	Modulo di richiesta del servizio (*). Log del processo di identificazione tramite Carta Nazionale dei Servizi (CNS) attiva. Log verifiche effettuate.
Identificazione tramite Firma Digitale	Modulo di richiesta di adesione, firmato digitalmente. Modulo di adesione (*). Log verifiche effettuate.
Identificazione mediante strumenti Poste Italiane preesistenti allo SPID	Modulo di richiesta del servizio (*). Log del processo di identificazione tramite strumenti Poste Italiane preesistenti allo SPID. Log verifiche effettuate.
Identificazione mediante strumenti di identificazione informatica preesistenti a SPID rilasciati da Enti Terzi autorizzati da AgID ad operare come GIP	Modulo di richiesta del servizio (*). Log del processo di identificazione tramite strumenti preesistenti allo SPID. Log verifiche effettuate.
Identificazione presso uno sportello della Pubblica Amministrazione (R.A.O.)	Modulo di richiesta del servizio (*). Log del processo di identificazione tramite pacchetto di attivazione (token).

Modalità di richiesta	Evidenze sottoposte a conservazione
	Log verifiche effettuate.
Richiesta da parte di un soggetto rappresentante dotato di identità digitale PosteID abilitato a SPID attiva	Log del processo di identificazione del soggetto rappresentante tramite identità digitale PosteID abilitato a SPID. Modulo di richiesta del servizio (*). Copia dei documenti del soggetto rappresentato (documento di identità e tessera sanitaria/codice fiscale). Copia del documento che attesta la titolarità del rappresentante ad effettuare la richiesta. Log verifiche effettuate. Identificativo operatore che ha eseguito la verifica della documentazione in backoffice.
Identificazione del Genitore richiedente, dotato di identità digitale PosteID abilitato a SPID attiva, in fase di creazione della pratica di attivazione dell'identità digitale di un minore	Log del processo di identificazione del soggetto rappresentante tramite identità digitale PosteID abilitato a SPID. Log verifiche effettuate. Log delle dichiarazioni di responsabilità rilasciate ai sensi del DPR 445/2000.
Identificazione "a vista" del minore	Modulo di richiesta del servizio (*), comprensivo dei dati identificativi personali del Genitore richiedente. Copia dei documenti utilizzati per l'identificazione (documento di identità e tessera sanitaria/codice fiscale). Copia del documento utilizzato per l'identificazione del Genitore richiedente. Copia del documento del Secondo genitore (se esistente). Copia della documentazione ulteriore eventualmente presentata dal Genitore richiedente (stato di famiglia con rapporti di parentela, certificato di morte del Secondo genitore, provvedimento del tribunale, estratto di nascita del minore con indicazioni di maternità/paternità, et al.). Log di conferma della richiesta di adesione. Log verifiche effettuate. Identificativo operatore che ha eseguito l'identificazione a vista.
Richiesta dell'abilitazione all'uso professionale per persona fisica da parte di un cliente già dotato di identità digitale PosteID abilitato a SPID attiva	Log del processo di identificazione del richiedente tramite identità digitale PosteID abilitato a SPID. Modulo di richiesta del servizio (*). Log verifiche effettuate.

Modalità di richiesta	Evidenze sottoposte a conservazione
Richiesta di attivazione del contratto di servizio per l'ID SPID Tipo 4 (Rappresentante legale)	Log del processo di identificazione del richiedente tramite firma digitale (vedi sopra) Modulo di richiesta del servizio (*). Visura camerale dell'organizzazione o certificato equipollente. Log verifiche effettuate.
Richiesta dell'ID SPID Tipo 4 (Referente di governo, Referente di gestione, Utilizzatore finale) – identificazione tramite identità digitale PosteID abilitato a SPID	Log del processo di identificazione del richiedente tramite identità digitale PosteID abilitato a SPID (vedi sopra). Modulo di richiesta del servizio (*). Log verifiche effettuate.
Richiesta dell'ID SPID Tipo 4 (Referente di governo, Referente di gestione, Utilizzatore finale) – identificazione tramite firma digitale	Modulo di richiesta del servizio (*). Log verifiche effettuate.
Richiesta dell'ID SPID Tipo 4 (Referente di governo, Referente di gestione, Utilizzatore finale) – identificazione tramite Referente di gestione	Log del processo di identificazione tramite Referente di gestione. Modulo di richiesta del servizio (*). Copia dei documenti utilizzati per l'identificazione (documento di identità e tessera sanitaria/codice fiscale). Log verifiche effettuate. Identificativo operatore dell'organizzazione che ha eseguito l'identificazione a vista.

(*) I moduli di richiesta del servizio riportano gli attributi dell'identità, riferimenti alle Condizioni Generali del Servizio e Condizioni Economiche applicabili ed ai consensi privacy espressi, riferimenti temporali delle operazioni effettuate.

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 (ad es. certificato di morte);
- 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).

16.2 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;
- tipologia di "uso" dell'identità (personale, professionale).

16.3 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 alle transazioni, inviando un apposito modulo di richiesta compilato e sottoscritto, corredato, nel caso dell'utente, 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.

Il modulo disponibile sul sito *https://posteid.poste.it*, nella sezione "Richiedi Assistenza", riporta gli indirizzi di posta elettronica a cui vanno inoltrate le richieste.

L'operatore, verifica l'autenticità della richiesta, in termini di:

- 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, previa autenticazione con credenziali SPID 2.

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

16.4 Misure anticontraffazione

16.4.1 Misure per SPID 1 (primo livello SPID)

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.

Per rafforzare l'utilizzo delle credenziali di primo livello SPID, il sistema notificherà sulla e-mail di contatto scelta dall'utente un "tentativo di accesso" ad un servizio online del circuito SPID tramite l'identità, a seguito di ogni richiesta di livello SPID 1, invitando l'utente a contattare l'Assistenza Clienti nel caso in cui non si riconoscesse nella richiesta di autenticazione.

16.4.2 Misure per SPID 2 (secondo livello SPID)

Per rafforzare l'utilizzo delle credenziali di secondo livello SPID, il sistema notificherà sulla e-mail di contatto scelta dall'utente ogni "tentativo di accesso" ad un servizio online del circuito SPID tramite l'identità, a seguito di una richiesta di autenticazione di livello SPID 2 tramite app PosteID o tramite codice di verifica OTP via SMS, invitando l'utente a contattare l'Assistenza Clienti nel caso in cui non si riconoscesse nella richiesta di autenticazione.

Inoltre la notifica via e-mail verrà inviata all'utente anche a seguito di:

- tentativo di enrollment dell'app PosteID su un nuovo dispositivo, sia in caso di esito positivo che di esito negativo. In caso di enrollment dell'app su un nuovo dispositivo è previsto anche l'invio di una push notification sulle app installate su tutti gli altri dispositivi attivi;
- operazione di disattivazione di un'installazione dell'app PosteID da un dispositivo, conseguentemente alla cancellazione del codice PosteID dal suddetto dispositivo.

Dopo 13 mesi di non utilizzo di un'app enrollata, avviene una disassociazione automatica dal dispositivo su cui è installata.

16.4.2.1 App PosteID

Il servizio genera specifici fattori di sicurezza crittografici che sono salvati sul dispositivo dell'utente in un "area sicura" di memoria accessibile solo all'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.

L'App PosteID una volta ricevuti e verificati i dati della transazione, in modalità "Password + Push in app + codice PosteID" oppure "QR code/deeplink + codice PosteID", richiede l'inserimento del codice PosteID, per consentire l'utilizzo del codice di sicurezza generato e conservato in maniera protetta.

La risposta viene generata solo se:

- L'App è installata su uno specifico dispositivo;
- La sandbox sicura dell'App contiene il codice segreto scambiato nella fase di installazione/configurazione;
- L'utente fornisce la password numerica corretta (codice PosteID) durante il processo di autenticazione.

Sono ammessi massimo 5 tentativi di immissione errati consecutivi, con impostazione di un blocco temporale in caso di raggiungimento.

Nel caso di utilizzo dell'App PosteID nella modalità "Password + PIN temporaneo (OTP) generato in App", il fattore di sicurezza generato tramite l'app correttamente inizializzata costituisce il "fattore di possesso" che si aggiunge al "fattore di conoscenza" della password per assolvere i requisiti del secondo livello di sicurezza, attraverso un'autenticazione multifattore.

La funzionalità "Generatore PIN temporaneo (OTP)", si attiva e viene associata all'identità digitale in fase di inizializzazione dell'app con il codice di sicurezza inviato al numero di telefono cellulare fornito e verificato in fase di registrazione; consente di generare e visualizzare la one time password su richiesta dell'utente.

La funzionalità assolve ai requisiti di sicurezza e affidabilità previsti dalle norme e utilizza modalità operative coerenti con le best practice internazionali per la generazione e protezione dei codici OTP. Il PIN temporaneo (OTP) è generato con un algoritmo conforme allo standard HOTP ed ha una lunghezza di almeno 6 cifre decimali.

NB: l'App PosteID non è uno strumento utilizzabile dagli utenti dotati di PosteID SPID ad uso professionale per persona giuridica (SPID Tipo 4).

16.4.2.2 Codice di verifica OTP via SMS

In questo caso le credenziali sono rappresentate dalla password come già descritta al paragrafo 16.4.1 "Misure per SPID 1 (primo livello SPID)" 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.

16.4.3 Misure per SPID 3 (terzo livello SPID)

Il dispositivo sicuro su cui sono custodite le chiavi associate ai certificati rispetta le seguenti conformità:

- Il Dispositivo sicuro è conforme all'articolo 35 del Decreto legislativo 7 marzo 2005, n. 82 e s.m.i..
- Il dispositivo sicuro nShield Solo 6000 F3 della società Thales è certificato FIPS 140-2 level 3 e Common Criteria EAL 4+.
- Il dispositivo nShield Solo 6000 F3 della società Thales è parte della famiglia "nShield HSM Family v.11.72.02" ed è stato oggetto di valutazione da parte dell'Organismo di Certificazione della Sicurezza Informatica (OCSI) in aderenza allo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT (DPCM 30 ottobre 2003) e certificato EAL4+ (AVA_VAN.5) in conformità ai requisiti dello standard ISO/IEC 15408 (certificato OCSI 1/16).
- In particolare tali dispositivi sono idonei all'utilizzo come "Dispositivi sicuri di firma elettronica (Secure Signature-Creation Device, SSCD)".
- Il Dispositivo sicuro viene utilizzato in accordo all'ambiente di sicurezza previsto nel Traguardo di Sicurezza (TDS) e nell'ambiente operativo in cui è posto in esercizio, nel rispetto delle politiche di sicurezza descritte nel TDS.
- La decifratura delle chiavi private ed il loro utilizzo per la sottoscrizione avviene esclusivamente all'interno del dispositivo sicuro.
- Il PIN per lo sblocco della chiave crittografica è verificato direttamente dal Dispositivo sicuro a cui viene veicolato utilizzando protocolli sicuri (https -TLS versione almeno 1.2).

Per rafforzare l'utilizzo delle credenziali di terzo livello SPID, il sistema notificherà sulla e-mail di contatto scelta dall'utente ogni "tentativo di accesso" ad un servizio online del circuito SPID tramite l'identità, a seguito di una richiesta di autenticazione di livello SPID 3 tramite app PosteID, invitando l'utente a contattare l'Assistenza Clienti nel caso in cui non si riconoscesse nella richiesta di autenticazione.

16.5 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 connessioni 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 www.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 Italiane 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.

16.5.1 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.

17 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.
- **Delegato**: con riferimento ai dati di clienti e fornitori le strutture che riferiscono direttamente ai primi livelli organizzativi, 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.

17.1 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.

17.1.1 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.

17.2 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*****