Procedura rilascio SPID

Linee guida sull’identificazione e gestione SPID

22 novembre 2022

History

Protocollo	Documento	Revisione	Data	Autori	Approvazioni
SPIDID	Rilascio SPID	1.0	24/10/2022	B. Tafini	F. Barcellini
SPIDID	Modifiche par. 3.1, 3.2 e 3.3	1.1	09/11/2022	B. Tafini	F. Barcellini

1 Sommario

2 Obiettivo del documento

Il presente documento è stato redatto al fine di descrivere e formalizzare le modalità di identificazione nonché le procedure che devono essere poste in essere dai registration authority officer (di seguito anche solo "RAO") per emettere e gestire identità digitali SPID - Sistema Pubblico di Identità Digitale istituito ai sensi dell'art. 64 del Decreto Legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione Digitale (di seguito anche solo "CAD")

Infatti, in conformità all'articolo 7 del 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*, il rilascio di identità SPID può avvenire solo "*previa verifica dell'identità del soggetto richiedente e mediante consegna in modalità sicura delle credenziali di accesso".*

Giova precisare fin da subito che Intesi Group ha attualmente previsto solo le seguenti modalità di identificazione:

a) identificazione del soggetto richiedente in presenza;
b) identificazione del soggetto richiedente da remoto con video intervista;
c) identificazione del soggetto richiedente tramite acquisizione del modulo di adesione allo SPID sottoscritto con firma elettronica qualificata.

A tal proposito i RAO, se diversi da personale di Intesi Group, dovranno seguire un apposito corso di formazione della durata di mezza giornata ed eseguire un quiz a risposta multipla per poter essere abilitato a svolgere attività di riconoscimento.

Eventuali errori del quiz saranno valutati dai soggetti che tengono il corso per verificare se l'errore è dovuto ad una semplice incomprensione della domanda e/o risposta oppure ad una lacuna/non conoscenza dell'argomento da parte del diretto interessato.

3 Modalità di Identificazione

3.1 Identificazione in presenza

L'identificazione in presenza presuppone che l'operatore abilitato all'attività di identificazione, Registration Authority Officer, verifichi l'identità della persona che richiede SPID, mediante presentazione di un modulo di richiesta di adesione al servizio, acquisendo i suoi dati e verificandone la correttezza e veridicità per mezzo dei documenti di riconoscimento esibiti dall'utente stesso.

I documenti di riconoscimento accettati da Intesi Group sono i seguenti:

- Carta identità
- Passaporto
- Patente

Oltre al documento di riconoscimento, l'operatore deve acquisire il tesserino sanitario che deve essere in corso di validità.

Ai documenti sopra citati, nei casi in cui l'identità SPID sia richiesta per persona giuridica, l'utente deve presentare anche la visura camerale attestante i poteri di rappresentanza conferiti alla persona fisica che richiede lo SPID.

L'operatore che effettua l'identificazione deve accertare che i documenti presentati dall'utente siano integri, in corso di validità, rilasciati da un'Amministrazione dello Stato, muniti di fotografia.

Effettuate con successo le verifiche, l'operatore deve acquisire copia digitale dei documenti presentati e deve inviarli ad Intesi Group attraverso l'applicazione RAO pkra. A seguito della ricezione, verranno svolte ulteriori verifiche sui documenti presentati utilizzando il servizio SCIPAFI - *Sistema pubblico di prevenzione delle frodi nel settore del credito al consumo con specifico riferimento al Furto d'identità* con cui viene verificata in modo automatico la corrispondenza dei dati presentati coi dati contenuti nei documenti.

Al fine di non compiere trattamenti illeciti in fase di identificazione, prima di acquisire i documenti il RAO mostra l'informativa privacy relativa al servizio SPID per informare l'utente circa la natura, la finalità e la base giuridica del trattamento.

3.2 Identificazione da remoto

L'identificazione da remoto presuppone che l'operatore abilitato all'attività di identificazione, verifichi l'identità della persona che richiede SPID tramite una video-intervista registrata.

L'operatore prima della video intervista dovrà visionare i documenti precedentemente caricati sul portale di Intesi Group dagli utenti. Tale verifica è necessaria per valutare se proseguire con la video intervista oppure contattare l'utente e chiedere di uploadare nuovamente i documenti laddove riscontrasse delle non conformità ad es. documenti di riconoscimento non leggibili, fotocopiati in bianco e nero ecc.

Infatti, sul portale di Intesi Group devono essere caricati e quindi accettati solo i documenti di riconoscimento integri e in corso di validità. L'operatore deve altresì accertare che i documenti presentati dall'utente siano rilasciati da un'Amministrazione dello Stato e muniti di fotografia.

I documenti di riconoscimento accettati da Intesi Group sono i seguenti:

- Carta identità
- Passaporto
- Patente

Oltre al documento di riconoscimento, l'utente deve caricare il tesserino sanitario che deve essere in corso di validità.

Ai documenti sopra citati, nei casi in cui l'identità SPID sia richiesta per persona giuridica, l'utente deve presentare anche la visura camerale attestante i poteri di rappresentanza conferiti alla persona fisica che richiede lo SPID.

Per supportare l'operatore nell'attività di verifica dei documenti presentati è stato integrato nel sistema il servizio SCIPAFI - *Sistema pubblico di prevenzione delle frodi nel settore del credito al consumo con specifico riferimento al Furto d'identità* con cui viene verificata in modo automatico la corrispondenza dei dati presentati coi dati contenuti nei documenti. L'operatore ha immediatamente l'esito di questa verifica e può decidere se procedere col riconoscimento, richiedere una modifica dei dati o rigettare la richiesta.

Se tutti i controlli si completano con successo si può procedere con la video intervista.

Orbene, affinché la video intervista possa ritenersi idonea è necessario che:

- nel video sia presente la sola persona che deve essere riconosciuta (salvo nel caso di persone con disabilità);
- le immagini video siano a colori e consentono una visualizzazione chiara dell'utente in termini di luminosità, nitidezza, contrasto e fluidità delle immagini;
- l'audio sia chiaro e privo di disturbi;
- l'utente sia immediatamente informato che la sessione è registrata e che verrà conservata per 20 anni come da informativa ricevuta nell'email di conferma appuntamento;
- l'operatore svolga la sessione lontano da terzi soggetti e in ogni caso in una stanza chiusa per motivi di privacy;
- i documenti mostrati a video siano chiaramente visibili.

Di seguito si riporta l'intera conversazione che deve tenersi tra l'operatore e l'utente.

Si precisa che lo script della conversazione è impostato sul portale, utilizzato per la video intervista, e tale portale prevede che l'operatore per ogni domanda posta all'utente debba necessariamente inserire una spunta in segno di "completamento", l'assenza della spunta non permette all'operatore di proseguire. Intesi Group ha creato questo sistema per minimizzare i rischi di eventuali dimenticanze in sede di riconoscimenti.

- ***Operatore:*** *acquisisce il consenso alla videoregistrazione e alla sua conservazione per 20 anni. Informando l'utente che la conservazione avviene in modalità protetta e sicura;*
- ***Utente:*** *dichiara i propri dati identificativi;*
- ***Utente:*** *conferma le proprie generalità;*

- ***Utente:*** *conferma la data e l'ora della registrazione;*
- ***Utente:*** *conferma di volersi dotare di un'identità digitale e conferma i dati inseriti nella modulistica online in fase di pre-registrazione;*
- ***Utente:*** *conferma il proprio numero di telefonia mobile e l'indirizzo mail;*
- ***Operatore:*** *richiede di mostrare l'SMS ricevuto a seguito delle verifiche svolte prima della videointervista ;*
- ***Operatore:*** *chiede e ottiene conferma dall'utente circa la conoscenza delle tipologie di credenziali di cui disporrà per l'accesso ai servizi in rete;*
- ***Operatore:*** *chiede di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal soggetto, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le informazioni contenute nello stesso (dati anagrafici, numero del documento, data di rilascio e di scadenza, amministrazione rilasciante);*
- ***Operatore:*** *chiede di mostrare la tessera sanitaria su cui è riportato il codice fiscale;*
- ***Operatore:*** *conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità;*
- ***Operatore:*** *chiede di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;*
- ***Operatore:*** *riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.*

3.3 Identificazione con firma elettronica qualificata

Nel caso di identificazione informatica tramite firma elettronica qualificata all'utente viene chiesto di compilare una apposita form in cui deve inserire i propri dati personali con cui verrà generato il modulo di richiesta dell'identità SPID compilato. L'utente deve scaricare il modulo così generato, deve firmarlo con il proprio certificato di firma digitale qualificata e caricarlo nuovamente sulla pagina web da cui verrà inviato ai server di backend. Alla ricezione del documento viene verificato che:

1. il file sia il medesimo generato dal sistema e non sia stato modificato dall'utente.
2. la firma sia valida e sia stata apposta con un certificato di firma digitale qualificata valido.

3. i dati personali dell'utente contenuti all'interno del certificato di firma (Nome, Cognome, Codice fiscale) corrispondano ai dati inseriti nel contratto e che siano coincidenti con i dati del richiedente l'identità digitale.
4. che il certificato non contenga l'OID 1.3.76.16.5 per certificati emessi tramite autenticazione SPID e che non contenga la limitazione d'uso per i certificati di firma automatica.

Se tutte queste condizioni sono verificate il riconoscimento viene ritenuto valido e l'identificazione viene automaticamente approvata. Al contrario l'identificazione viene rigettata.

4 Consegna Credenziali di Accesso

A fronte di una identificazione completata con successo, l'utente riceve una email di conferma all'indirizzo che è stato verificato nel corso dell'identificazione e che diventerà lo username delle credenziali SPID. Tale email contiene un link di attivazione della credenziale SPID. Cliccando su questo link all'utente verrà richiesto di:

1. Prendere visione dei termini e condizioni di utilizzo del servizio SPID
2. Firmare il contratto con il certificato qualificato rilasciato a seguito dell'identificazione. Per firmare viene richiesto l'inserimento di un OTP inviato via SMS al numero di telefono verificato nel corso dell'identificazione.
3. Se la firma si completa correttamente all'utente viene richiesto di definire la password con le modalità descritte di seguito.

Al completamento l'utente riceverà una email di conferma di attivazione della credenziale SPID

4.1 Dettagli sulle credenziali di accesso

Le credenziali di Accesso consentono al Titolare di eseguire il processo di autenticazione informatica volto alla verifica dell'identità digitale associata ai fini dell'erogazione di un servizio fornito in rete.

In altre parole, le credenziali di Accesso sono funzionali a comprovare l'associazione tra il Titolare e la sua identità digitale che lo rappresenta in rete, pertanto è importante raccomandare all'utente di non comunicarle a terzi o divulgarle in alcun modo, curandone la relativa conservazione e protezione con la massima diligenza, per tutto il tempo di validità dell'identità digitale.

Prima di entrare nel merito delle modalità di consegna delle credenziali di accesso è opportuno precisare i livelli di sicurezza previsti da Intesi Group per le identità digitali SPID emesse dalla stessa.

Ai sensi dell'art. 6 del DPCM 24 ottobre 2014, Intesi group ha previsto il livello 1 e il livello 2 di SPID.

Indipendentemente dal Livello di SPID richiesto dall'utente, l'operatore ha l'obbligo di informare compiutamente l'utente circa l'importanza della gestione e conservazione in maniera sicura delle credenziali consegnando la Guida Utente che descrive:

- le modalità d'uso del sistema di autenticazione di Intesi Group;
- le modalità con cui l'utente può richiedere la sospensione o la revoca delle credenziali con gli strumenti messi a disposizione da Intesi Group;
- le cautele che l'utente deve adottare per la conservazione e protezione.

4.2 Livello 1 SPID

Il Livello 1 SPID è gestito tramite una coppia username e password. Per le identità digitali SPID di Intesi Group lo username corrisponde all'indirizzo e-mail richiesto come attributo secondario in fase di registrazione.

La policy di definizione delle password, come precisato nella "Guida Utente", è la seguente:

1. lunghezza minima di otto caratteri;
2. uso di caratteri maiuscoli e minuscoli;
3. inclusione di uno o più caratteri numerici;
4. non deve contenere più di due caratteri identici consecutivi;
5. inclusione di almeno un carattere speciali ad es #, $, %;

4.3 Livello 2 SPID

Il Livello 2 SPID viene realizzato tramite l'adozione di una OTP (one time password) che deve essere inviata per mezzo di SMS al numero di telefono indicato dall'utente in fase di registrazione. Per la conservazione di questa credenziale è opportuno raccomandare agli utenti di:

- inserire le funzioni di blocco per impedire a terzi di avere accesso al proprio dispositivo mobile;
- mantenere aggiornato il sistema operativo (e anche le applicazioni) del proprio dispositivo;
- disattivare l'opzione di connessione Wi-Fi automatica e fare particolare attenzione al Wi-Fi pubblico ed aperto;
- utilizzare solo i market ufficiali per il download delle app. L'installazione di programmi di provenienza non fidata è il principale mezzo con cui vengono veicolati software potenzialmente pericolosi;
- disabilitare la funzione di "anteprima sms" sul proprio smartphone al fine di evitare la visualizzazione degli sms OTP da parte di terzi;
- utilizzare la funzione di "blocco-schermo".

5 Responsabilità dei RAO

I RAO si assumono la responsabilità della corretta verifica dell'identità dell'utente e sono tenuti a mantenere e/o inviare ad Intesi Group le evidenze/ risultanze dell'identificazione.

Le indicazioni presenti su questo documento e sulla documentazione di riferimento (es. Manuale Operativo) sono essenziali per una corretta identificazione ed è obbligatoria l'integrazione o addirittura la ripetizione in toto del processo di identificazione qualora non vengano rispettati.

Se i RAO fanno parte di LRA esterne da Intesi Group si dovranno impegnare per mezzo di apposito documento a non svolgere le suddette operazioni di identificazione e registrazione con modalità diverse, anche solo parzialmente, rispetto a quelle indicate nella Documentazione SPID e durante il

Corso di formazione e a utilizzare nei confronti dei soggetti identificati esclusivamente la modulistica indicata a tal fine da Intesi Group.