Servizio SPID

Manuale operativo

09 novembre 2022

History

Protocollo	Modifiche	Revisione	Data	Autori	Approvazioni
SPIDMO	Prima versione	1.0	23/06/2022	F.Barcellini B.Tafini	P.Sironi
SPIDMO	Paragrafo 6	1.1	21/10/2022	F.Barcellini B.Tafini	P.Sironi
SPIDMO	Paragrafo 6.3	1.2	09/11/2022	F.Barcellini B.Tafini	P.Sironi

Sommario

1 Introduzione 7

1.1 Responsabile del Manuale Operativo 7

1.2 Definizioni, abbreviazioni e termini tecnici 8

1.2.1 Definizioni 8

1.2.2 Acronimi e abbreviazioni 9

1.2.3 Riferimenti normativi 10

2 Disposizioni generali 11

2.1 Obblighi dell'utente 11

2.2 Obblighi del gestore 12

2.3 Obblighi dei fornitori di Servizi 15

2.4 Obblighi dei Soggetti esterni che svolgono l'attività di riconoscimento 15

2.5 Obblighi connessi al trattamento dei dati personali 16

3 Descrizione del servizio SPID 16

3.1 Caratteristiche generali dell'autenticazione SPID SAML 17

3.2 Caratteristiche generali dell'autenticazione SPID OpenID 18

3.3 Architettura applicativa 20

3.4 Sicurezza credenziali SPID 22

3.5 Architettura dei sistemi di autenticazione 22

4 Notifiche di accesso 24

5 Codici e formato messaggi di anomalie 24

6 Verifica identità e rilascio credenziali 24

6.1 Identificazione e registrazione de-visu 26
6.2 Identificazione e registrazione IDentify-web 27
6.3 Identificazione con firma elettronica qualificata 29
6.4 Processo rilascio identità SPID 30
2.1.1 Certificato identificazione 31
7 Metodi di gestione dei rapporti con gli utenti 32
8 Gestione del ciclo di vita dell'identità digitale 32
8.1 Sospensione e Riattivazione 32
8.2 Revoca dell'identità digitale 34
9 Livelli si servizio 35
9.1 Orari garantiti per le diverse fasi della registrazione 35
9.2 Registrazione e gestione ciclo di vita dell'identità 36
9.3 Continuità operativa 37
9.3.1 Registrazione e rilascio identità 37
9.3.2 Revoca o sospensione Identità 38
9.3.3 Autenticazione 38
10 Misure anticontraffazione 38
10.1 Misure per prevenire furti d'identità 38
10.2 Protezione credenziali di firma 39
10.2.1 Misure per credenziali SPID di livello L1 39
10.2.2 Misure per credenziali SPID di livello L2 39
11 Monitoraggio 40
12 Tracciature degli accessi al servizio di autenticazione 40
12.1 Contenuto dei log 40

12.2 Tracciamento log autenticazioni 41

12.3 Lista accessi servizi 42

1 Introduzione

Il presente Manuale Operativo definisce le regole e descrive le procedure utilizzate dal Gestore di identità, Intesi Group S.p.A., per l'erogazione del servizio di SPID (sistema pubblico di Identità Digitale).

Il presente documento è pubblicato sul sito ufficiale di Intesi Group a garanzia dell'affidabilità del servizio offerto.

Il gestore del servizio SPID è Intesi Group che si identifica nel seguente modo:

Nome della società: Intesi Group S.p.A.

Sede Legale: Via Torino, 48 – 20123 Milano (MI) – ITALIA

Rappresentante Legale: Paolo Sironi (Amministratore Delegato e Presidente)

Partita IVA e Codice Tributario: IT02780480964

Telefono: +39 02 6760641

Identificatore di Oggetto ISO (OID): 1.3.6.1.4.1.48990

Sito web della società: http://www.intesigroup.com

Sito web della servizio SPID: https://spid.intesigroup.com/

Indirizzo e-mail della società: tsp@intesigroup.com

1.1 Responsabile del Manuale Operativo

Il presente Manuale Operativo viene redatto, revisionato, e aggiornato da personale di Intesi Group S.p.A appositamente incaricato e viene pubblicato solamente dopo essere stato approvato dalla Direzione di Intesi Group. Il responsabile del manuale operativo è:

- Francesco Barcellini

- responsabile del servizio SPID

Richieste di informazioni o chiarimenti riguardo al presente Manuale Operativo possono essere inviate scrivendo una e-mail all'indirizzo tsp@intesigroup.com.

Il presente Manuale Operativo e le successive modifiche sono depositati presso AgID - Agenzia per l'Italia Digitale – ed è reso pubblico da Intesi Group attraverso il proprio repository dei documenti presente sul sito istituzionale: http://www.intesigroup.com.

1.2 Definizioni, abbreviazioni e termini tecnici

1.2.1 Definizioni

AgID	Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Gestori di Identità Digitali).
Attributi	Le informazioni o qualità di un Utente utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari.
Attributi identificativi	Nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, il codice fiscale o la partita IVA 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, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni.
Attributi qualificati	Le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.
Codice identificativo	Codice univoco assegnato dal gestore dell'identità digitale che identifica univocamente un'identità digitale nell'ambito della federazione SPID.
Credenziale	il particolare attributo di cui l'utente si avvale, unitamente al codice identificativo, per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi che aderiscono allo SPID.
Fattore di autenticazione	Elemento di informazione e/o processo usato per autenticare o verificare l'identità di una entità.
Service Provider SPID	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.
Identity Provider Spid	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 dell'utente al fine della sua identificazione informatica. Il Gestore dell'identità digitale, inoltre, 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 Intesi Group che agisce in qualità di Gestore dell'identità digitale.
Gestori di attributi qualificati	I soggetti accreditati ai sensi dell'art. 16 del DPCM che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
Identità digitale	La 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.
(Utente) Titolare o Richiedente	E' il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v). Prima dell'attribuzione dell'identità digitale tale soggetto è chiamato Richiedente.

1.2.2 Acronimi e abbreviazioni

AgID	Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Gestori di Identità Digitali).
ETSI	European Telecommunications Standards Institute.
HSM	È un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.
HMAC	HMAC-based One-time Password algorithm.
IDP	Identity Provider – vedi Identity Provider SPID.
LRA	Local Registration Authority, persona giuridica al quale è affidato il compito di identificare in maniera certa i Richiedenti SPID
OTP	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione.
OIDC	OpenID connect.
RAO	Registration Authority Office. Ente Terzo, pubblico o privato, è stato autorizzato da Intesi Group ad effettuare identificazioni a norma SPID.

RPO	Recovery Point Objective - Rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza.
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.
SSHA2	Salted SHA-256 algoritmo di hashing usato per il salvataggio delle password.
SMS	Short Message Service.
SSL	Secure Socket Layer.
SP	Service provider – vedi Service Provider Spid.
SPID	Il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificatodall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98.

1.2.3 Riferimenti normativi

a) Decreto Legislativo 7 marzo 2005, n.82*, Codice dell'amministrazione digitale* (di seguito anche "CAD");

b) ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements;*

c) ISO/IEC 29115:2013 - *Information technology — Security techniques — Entity authentication Assurance framework;*

d) Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, recante le *"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"* e s.m.i.;

Referenziato nel seguito come **DPCM.**

e) Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio *2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;*

f) Regolamento, emanato da AgID, recante le *modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale*, di cui art. 4 co. 1 lett. a) DPCM 24 ottobre 2014;

g) Determinazione AgID n. 44 del 28 luglio 2015 (come modificata dalla Determinazione n. 189 del 22 luglio 2016) *con la quale sono stati emanati i Regolamenti SPID* di cui all'art. 4 commi 2, 3 e 4 del DPCM 24 ottobre 2014;

h) ISO 9001:2015 *Quality management systems — Requirements;*

i) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo *alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);*

2 Disposizioni generali

2.1 Obblighi dell'utente

L'Utente ossia il Titolare dell'Identità Digitale si impegna a :

1. Esibire ad Intesi Group i documenti richiesti e necessari ai fini delle operazioni per l'emissione e gestione dell'identità digitale.
2. Fare un uso esclusivamente personale delle credenziali connesse all'Identità Digitale.
3. 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.
4. Non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine.
5. Utilizzare le credenziali di accesso per i soli scopi, leciti, per il quale sono state rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendosi ogni eventuale responsabilità per l'utilizzo di SPID per finalità diverse.
6. A mantenere l'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private.
7. Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite.
8. Fornire/comunicare ad Intesi Group dati ed informazioni veritiere e complete, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni false o mendaci.
9. Verificare la correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare immediatamente eventuali inesattezze.

10. Informare tempestivamente il Gestore di ogni variazione degli attributi precedentemente comunicati e registrati.
11. 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.
12. Conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i seguenti rischi :
    - divulgazione, rivelazione e manomissione,
    - furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale,
    - la non autenticità del fornitore di servizi o dell'identity Provider.
13. Attenersi alle indicazioni fornite da Intesi Group e riportate in questo Manuale operativo e in ogni altro documento ufficiale, reperibile e liberamente scaricabile al seguente link https://www.intesigroup.com/it/documenti/, in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele da adottare per la conservazione e protezione delle credenziali.
14. In caso di smarrimento, furto o altri danni e/o compromissioni richiedere immediatamente ad Intesi Group la sospensione delle credenziali.
15. 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.

2.2 Obblighi del gestore

Intesi Group, come Gestore di identità digitali SPID, deve:

1. Rilasciare l'identità SPID su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta (se presente)
2. Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale.

3. Conservare copia per immagine del documento di identità esibito
4. 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.
5. Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso si identificazione tramite firma digitale.
6. Verificare gli attributi identificativi del richiedente.
7. Consegnare in modalità sicura le credenziali di accesso all'utente.
8. Conservare la documentazione inerente al processo di identificazione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale.
9. Cancellare la documentazione inerente il processo di identificazione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale.
10. Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.
11. Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione, notificandone le relative modifiche
12. 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.
13. Revocare l'identità digitale, e se del caso, informarne l'utente via posta elettronica e numero di telefono mobile, 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.
14. Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente.
15. Verificare la provenienza della richiesta di sospensione da parte dell'utente e fornire all'utente conferma della ricezione della richiesta di sospensione.
16. Su richiesta del Titolare sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni, informandolo, e poi procedere con il ripristino o la revoca dell'identità digitale sospesa.
17. Su richiesta del Titolare revocare tempestivamente l'identità digitale con le modalità previste nel paragrafo 8.3 .

18. Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale.
19. Adottare misure contro la contraffazione come descritto nel paragrafo 10,.
20. 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.
21. Effettuare con cadenza almeno annuale un'analisi dei rischi.
22. 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.
23. Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa.
24. Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, alla procedura di autenticazione e ai necessari requisiti tecnici per accedervi.
25. Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione.
26. 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.
27. In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
28. Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID.
29. 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 (art. 32 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.) ed utilizzando meccanismi di cifratura.

2.3 Obblighi dei fornitori di Servizi

I fornitori di servizi che utilizzano le identità digitali al fine dell'erogazione dei propri servizi hanno i seguenti obblighi:

1. Informare immediatamente, nel caso in cui rilevi un uso anomalo di un'identità digitale, sia l'AgID sia il Gestore dell'identità digitale che l'ha rilasciata.
2. Osservare scrupolosamente la vigente normativa unionale e nazionale in materia di protezione dei dati personali e i provvedimenti del Garante per la protezione dei dati personali.
3. Conservare gli attributi ricevuti dal Gestore nelle sessioni di autenticazione esclusivamente per la finalità di prestazione del servizio per cui l'accesso è stato effettuato, in conformità al DPCM, ai Regolamenti attuativi del sistema SPID e alla normativa in materia di protezione dei dati personali.
4. Assistere l'Utente nella risoluzione di eventuali problematiche che si dovessero verificare nel corso dell'autenticazione (help desk di primo livello), facendosi carico, se necessario, di sentire il Gestore delle identità digitali coinvolto nella transazione (assistenza tecnica). Il Fornitore di Servizi è responsabile della presa in carico della issue (fase – accoglienza), quindi della Verifica Incident e gestione della richiesta di assistenza. In particolare il Fornitore di Servizi interviene in caso di errore relativo ad accesso e fruizione del servizio, crash del sistema e procedura di autenticazione, network.

2.4 Obblighi dei Soggetti esterni che svolgono l'attività di riconoscimento

Intesi Group può delegare le funzioni di registrazione e riconoscimento a soggetti esterni, dette LRA, a seguito della firma del "Contratto di mandato LRA". Le LRA si avvalgono di operatori di registrazione (di seguito " RAO") che devono obbligatoriamente seguire un corso di formazione, erogato da personale Intesi Group, e in cui sono spiegate le procedure, i controlli e gli strumenti da usare per l'identificazione dei richiedenti di identità digitale. Ogni operatore viene abilitato a svolgere attività di identificazione solo dopo aver seguito il corso di formazione e solo a seguito della firma di un "Contratto di mandato RAO".

Le LRA e i RAO devono:

1. attenersi scrupolosamente alle procedure indicate da Intesi Group,
2. accertare scrupolosamente l'autenticità di ciascuna richiesta

3. rilasciare identità digitali SPID previa verifica dell'identità del soggetto richiedente e mediante consegna in modalità sicura delle credenziali di accesso.
4. usare solamente gli strumenti di identificazione forniti o concordati con Intesi Group.
5. segnalare a Intesi Group qualsiasi tentativo di frode, furto o uso fraudolento dell'identità digitale.
6. attenersi a tutto quanto descritto nel presente documento, nei documenti ufficiali pubblicati al seguente link https://www.intesigroup.com/it/documenti/ nonché al relativo contratto tra le Parti

In ogni caso Intesi Group mantiene le responsabilità per quanto non espressamente indicato nei documenti di mandato e nella complessità delle attività svolte come IdP SPID.

2.5 Obblighi connessi al trattamento dei dati personali

Intesi Group tutela la riservatezza dei dati personali e ne garantisce la protezione necessaria da ogni evento che possa ledere i diritti e le libertà degli interessati (utenti).

Infatti, Intesi Group tratta i dati personali in maniera lecita, corretta e trasparente in conformità alla vigente normativa in materia.

Come previsto dal Regolamento dell'Unione Europea n. 2016/679 ("GDPR"), ed in particolare gli artt. 13 e 14, sono fornite all'Interessato tutte le informazioni, relative al trattamento dei propri dati personali mediante apposita, specifica e preventiva informativa, resa altresì sempre disponibile all'interno del proprio sito istituzionale.

3 Descrizione del servizio SPID

Il Sistema Pubblico di Identità Digitale (SPID), previsto dall'articolo 64 del Codice per l'Amministrazione Digitale, è volto a favorire l'accesso ai servizi online erogati dalle Pubbliche Amministrazioni e dai Fornitori di servizi privati. Al Sistema partecipano i seguenti attori:

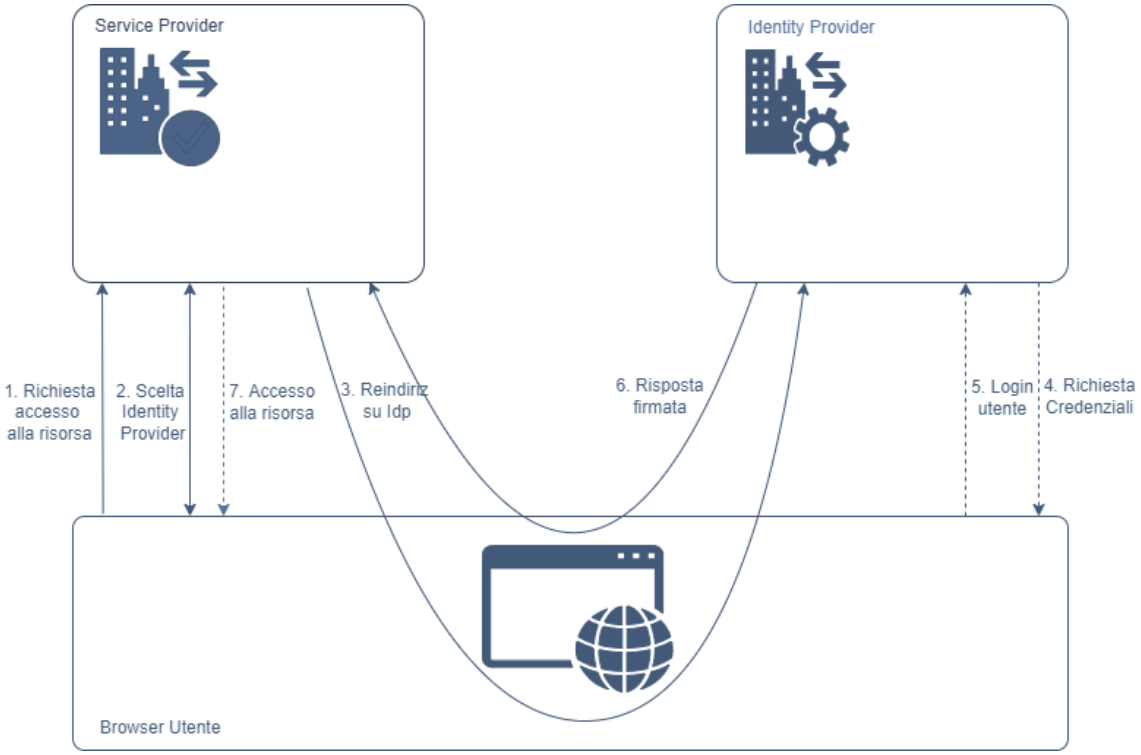
- Gestori dell'Identità Digitale;
- Gestori di Attributi Qualificati (ad es: Ordini e collegi professionali, CC.I.AA., MISE, ecc.);
- Fornitori di Servizi (ad es: PP.AA., Gestori di Pubblici Servizi, Imprese, …);
- Agenzia per l'Italia Digitale;

- Utenti titolari di credenziale SPID.

Il Sistema SPID mette in relazione questi attori per soddisfare la richiesta degli utenti di usufruire di un servizio online di un Fornitore di servizi previa autenticazione volta a confermare la propria identità ed, eventualmente, anche di ruoli e qualifiche per mezzo dei Gestori degli attributi qualificati.

3.1 Caratteristiche generali dell'autenticazione SPID SAML

Il sistema SPID si basa sul protocollo di autenticazione SAML nelle due versioni "SP-Initiated": "Redirect/POST binding" e "POST/POST binding" secondo il seguente scenario di interazione:



1. **Richiesta accesso alla risorsa l'utente:** l'utente sul sito del Fornitore di Servizi, chiede accesso a funzionalità per le quali è necessaria l'autenticazione informatica del richiedente.
2. **Scelta Identity provider**: l'utente, sul sito del Fornitore di servizi, seleziona il proprio Gestore dell'identità.
3. **Reindirizzamento 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.

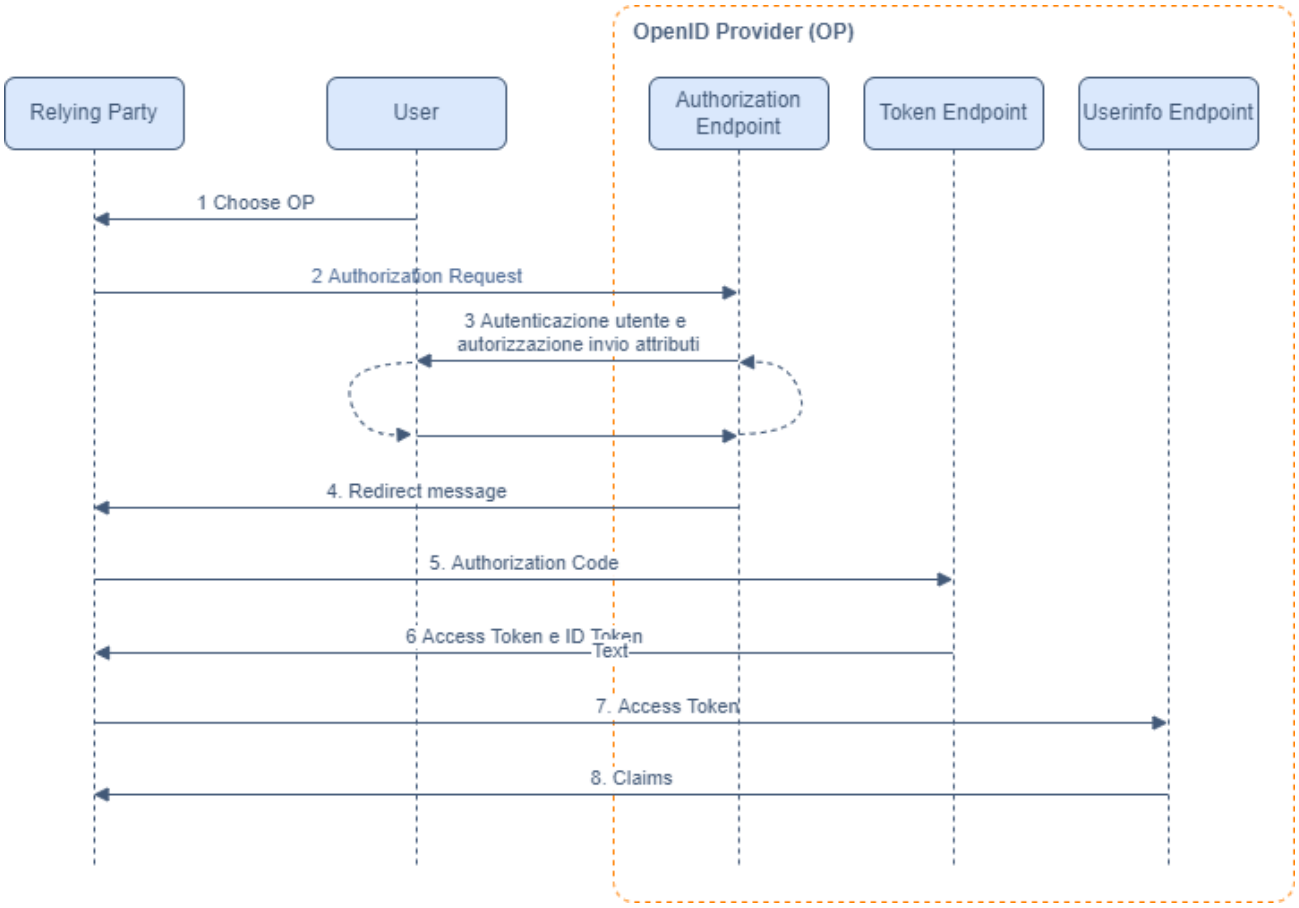
4. **Richiesta credenziali:** il Gestore dell'identità richiede all'utente l'inserimento delle proprie credenziali SPID in aderenza al livello di sicurezza necessario.
5. **Login utente:** il Gestore dell'identità richiede all'utente l'autenticazione con le proprie credenziali SPID in aderenza al livello di sicurezza richiesto e con il processo proposto dal gestore stesso.
6. **Restituzione risposta fermata:** il Gestore dell'identità restituisce al Fornitore di servizi l'esito del processo di autenticazione e, in caso positivo, i dati richiesti.
7. **Accesso alla risorsa:** il Fornitore di servizi ha a disposizione l'evidenza del processo di autenticazione e, in caso di esito positivo, ne autorizza la fruizione.

3.2 Caratteristiche generali dell'autenticazione SPID OpenID

Il sistema di autenticazione SPID deve supportare anche il protocollo **OpenID Connect** come descritto nel documento "Linee Guida OpenID Connect in SPID" pubblicato sul sito di AgID.

Le specifiche del protocollo OpenID Connect definiscono le entità OpenID Provider (OP) e Relying Party (RP) che, nell'ambito del servizio SPID, devono intendersi rispettivamente come Gestori dell'identità digitale (Identity Provider - IdP) e i Fornitori di servizi (Service Provider - SP) di cui al DPCM.

Il modello di flusso che implementato è l'"**Authorization Code Flow**" che segue il seguente schema:



1. **Scelta OpenID Provider (OP)**: l'utente, all'interno della pagina di accesso del Relying Party (RP), seleziona, sul pulsante SPID, l'OpenID Provider (OP) con cui autenticarsi.
2. **Authentication Request**: il Relying Party (RP) invia una richiesta di autenticazione verso l'Authorization Endpoint dell'OpendID Provider selezionato dall'utente.
3. **Autenticazione utente e autorizzazione :** L'OpenID Provider (OP) richiede all'utente l'inserimento delle credenziali, secondo il livello SPID richiesto dal Relying Party (RP) e, una volta autenticato, richiede di autorizzare agli attributi richiesti dal Relying Party (RP).
4. **Redirect Message:** L'OpenID Provider (OP) reindirizza l'utente verso l'url di reindirizzamento specificato dal Relying Party (RP), passando un codice di autorizzazione.
5. **Authorization Code:** Il Relying Party (RP) invia il codice autorizzazione al Token endpoint dell'OpenID Provider (OP).

6. **Access Token e ID Token:** l'OpenID Provider (OP) Token endpoint rilascia un ID Token, un Access token e se richiesto un Refresh token.
7. **Access Token:** Il Relying Party (RP) riceve e valida l'Access token e l'ID token. Per chiedere gli attributi che erano stati autorizzati dall'utente al punto 3, invia una richiesta all'UserInfo endpoint utilizzando l'Access token per l'autenticazione.
8. **Claims:** l'OpenID Provider (OP) rilascia gli attributi richiesti al Relying Party (RP).

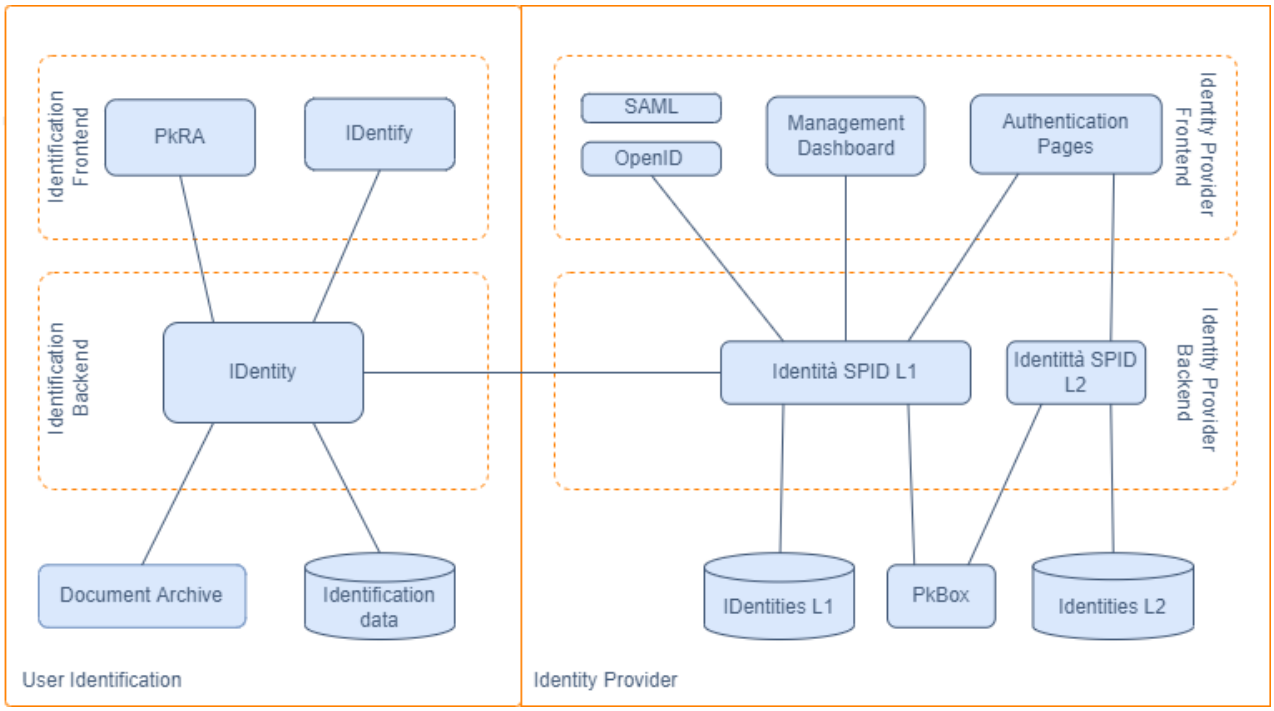
3.3 Architettura applicativa

Il servizio SPID di Intesi Group per la gestione del servizio dell'Identità digitale di intesi Group espone funzionalità per l'**Identificazione** e **Registrazione** degli utenti, le funzionalità di **Autenticazione** e per la gestione del ciclo di vita della credenziale di autenticazione.

Il servizio di Gestione delle Identità SPID può essere logicamente suddiviso in due componenti:

1 Componenti Identificazione (nel riquadro User component in figura).

2 Componenti per la gestione delle autenticazione (nel riquadro Identity Provider in figura).



Nel riquadro **User identification** sono inseriti l'insieme dei componenti dell'infrastruttura Intesi Group che consentono di effettuare l'identificazione certa dei titolari delle identità SPID. Questo componente è composto dai seguenti sottomoduli:

1. PkRA: interfaccia web per la gestione dell'identificazione dell'utente in presenza di un operatore (DeVisu).
2. 'Identify': interfaccia web per la gestione dell'identificazione tramite video intervista, tramite un certificato di una firma elettronica qualificata o altra identità SPID.

Tutti questi elementi si basano su un componente di backend, denominato 'Identity' dedicato alla gestione delle varie fasi del processo di identificazione e alla gestione dell'archivio delle evidenze raccolte durante l'identificazione della persona (immagini dei documenti, filmati ecc.). Alla conclusione del processo di identificazione le informazioni raccolte passano al componente per la gestione delle credenziali SPID, indicato col nome **Identity Provider** nel riquadro di figura, che fornisce le funzionalità di autenticazione tramite protocollo SAML e OIDC, le primitive per la gestione della credenziale SPID (attivazione, sospensione, revoca e rinnovo) e funzionalità amministrative. Il componente IDP SPID è composto dai seguenti sotto-componenti:

1. management dashboard: applicazione web ad uso dei titolari SPID per la gestione della credenziale.
2. Authentication pages: l'insieme delle pagine di autenticazione.
3. SAML: componente per la gestione del protocollo di autenticazione SAML.
4. OpenID: componente per la gestione dei protocolli di autenticazione OpenID Connect.

Questi componenti si avvalgono delle funzionalità esposte dai seguenti componenti di back-end:

1. Identità SPID L1: componente, denominato Time4User, che gestisce l'identità digitale. All'interno di questo componente viene implementata la gestione e l'aggiornamento delle entità SPID, la logica di autenticazione SPID per le credenziali di livello L1 e L2 tramite la connessione con il componente Time4ID.
2. Identità SPID L2: responsabile, denominato Time4eID, per la gestione dei token OTP utilizzati per le credenziali di livello L2.

Sia Time4User che Time4ID utilizzano per firmare le asserzioni di identità e per conservare le chiavi di generazione dei token OTP degli utenti il server di firma remota di Intesi Group denominato PkBox.

L'infrastruttura è inoltre costituita da altri moduli, non rappresentati nella figura, che consentono di gestire:

1. le notifiche email e la verifica delle credenziali scadute e inutilizzate.
2. il monitoraggio dello stato di attivazione dei servizi:
3. la conservazione dei log;

3.4 Sicurezza credenziali SPID

Affinché l'utente possa usufruire dei servizio richiesto tramite SPID, le credenziali che utilizza devono essere coerenti con il livello di sicurezza richiesto dal Fornitore dei Servizi.

Nell'ambito della federazione SPID esistono tre differenti livelli di sicurezza delle credenziali SPID che possono essere richiesti dal Fornitore dei Servizi:

- **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; 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.

  Intesi Group realizza le credenziali di livello L1 con password.
- **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. Questo livello è adeguato per tutti i servizi che possono subire un danno consistente da un utilizzo indebito dell'identità digitale.

  Intesi Group realizza le credenziali di livello L2.

  Intesi Group realizza le credenziali di livello L2 con OTP generato tramite algoritmo HOTP e inviato tramite SMS sul numero di telefono indicato dall'utente in fase di attivazione del servizio.
- **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.

  Intesi Group non gestisce credenziali di livello L3

I livelli di sicurezza necessari per l'accesso ai servizi sono attribuiti dai gestori stessi.

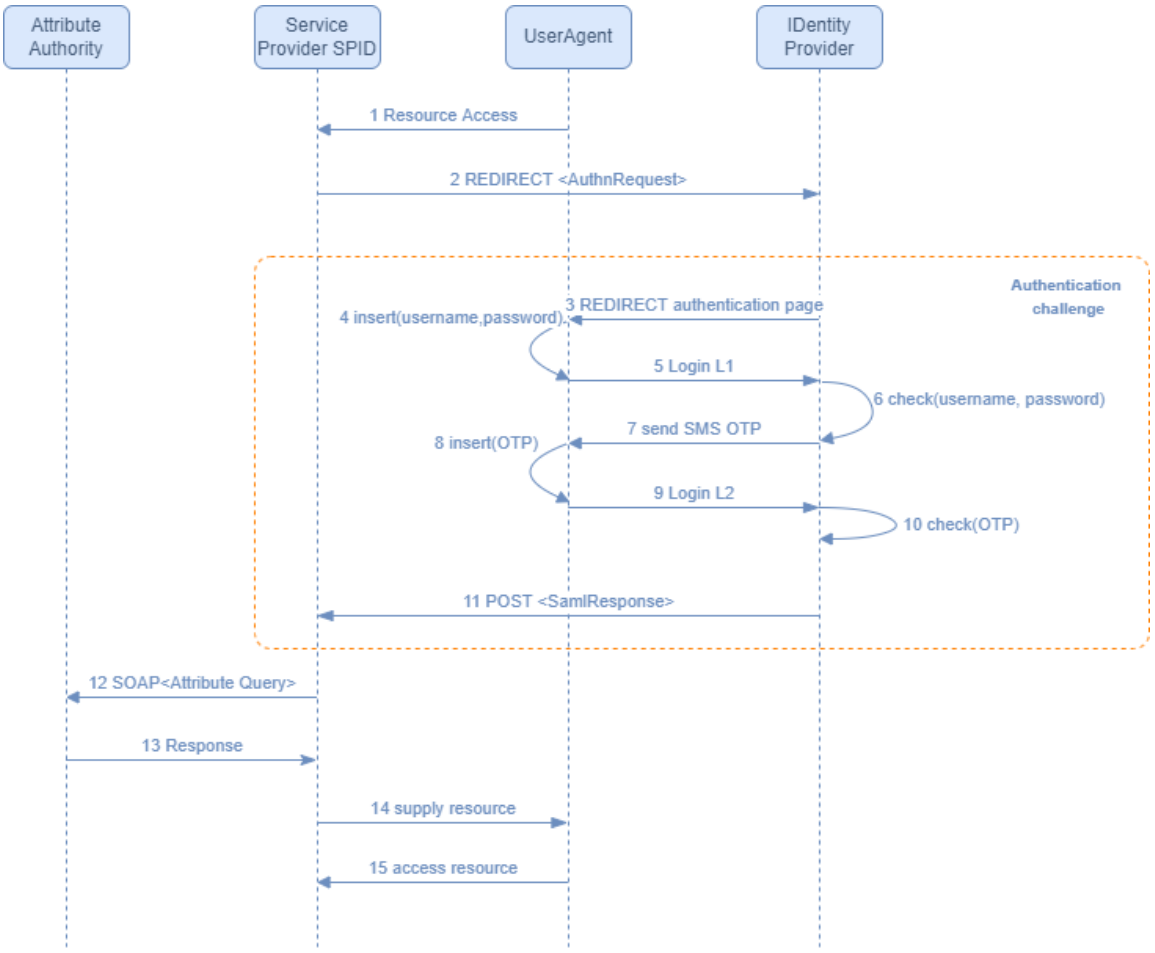
3.5 Architettura dei sistemi di autenticazione

Il gestore delle identità deve prevedere tutti i meccanismi atti all'autenticazione dell'entità digitale secondo i livelli di sicurezza richiesti nell'ambito SPID.

Il processo di autenticazione SPID prevede i seguenti attori:

1. **User agent**: utente che richiede l'accesso ad un servizio tramite una credenziale SPID;
2. **Service Provider**: ente fruitore del servizio;
3. **Identity Provider**: ente gestore dell'identità;
4. **Attribute Authority**: autorità attestante attributi di qualifica di una persona fisica;

Il processo di autenticazione sviluppato da Intesi Group avviene attraverso il flusso seguente:



1. L'utente richiede l'accesso ad una risorsa messa a disposizione da un Service Provider.
2. L'utente seleziona l'Identity provider che gestisce la propria identità SPID ed il Service Provider inoltra un richiesta di autenticazione SAML all'Identity Provider.
3. L'Identity Provider, a fronte della ricezione di una richiesta, dopo averla validata avvia l'autenticazione.
4. L'utente inserisce il proprio username e la propria password SPID.
5. Lo UserAgent invia username e password all'Identity provider.

6. L’Identity Provider verifica le credenziali ricevute.
7. Se il livello di autenticazione richiesto e di tipo L2, viene inviato un OTP SMS.
8. L’utente inserisce l’OTP.
9. Lo UserAgent invia l’OTP all’identity provider.
10. L’identity Provider verifica l’OTP Ricevuto.
11. L’Identity Provider produce la risposta SAML con il risultato dell'autenticazione e la restituisce al Service Provider.
12. Se necessario, il Service Provider effettua in proprio controlli sugli attributi presso un Attribute Authority.
13. Il Service Provider attesta gli attributi dell'utente.
14. Il Service Provider, a fronte di riscontri positivi, consente l'accesso all'utente.
15. L'utente accede alla risorsa che ha richiesto.

4 Notifiche di accesso

Su richiesta del Titolare, il Gestore dell’identità digitale, comunicherà al titolare stesso ogni utilizzo delle Credenziali di Accesso mediante comunicazione all’indirizzo email comunicato in fase di registrazione o eventualmente all’indirizzo mail indicato successivamente dall’utente.

5 Codici e formato messaggi di anomalie

Il servizio di autenticazione SPID dell’IdP Intesi Group soddisfa le specifiche di messaggistica e codifica dei casi di errore previste dalle regole tecniche di cui all’Art 4, comma 2 del DPCM e pubblicate sul sito Agid e denominate (SPID – Tabella messaggi di anomalia v1.4) e che sono riportate in forma abbreviata in § APPENDICE A - Codici e formati dei messaggi di anomalia.

6 Verifica identità e rilascio credenziali

Intesi Group prima di rilasciare l’ identità digitale SPID, notificata ai sensi dell’art. 9 del Regolamento Europeo 910/2014 eIDAS, identifica in maniera certa le persone fisiche in conformità all’art. 7 del DPCM. La verifica dell’identità del soggetto richiedente avviene in uno dei seguenti modi:

a) identificazione in presenza del soggetto richiedente;

b) identificazione da remoto tramite strumenti di registrazione audio/video;

c) identificazione informatica tramite acquisizione del modulo di adesione allo SPID sottoscritto con firma elettronica qualificata.

Al fine di poter documentare la corretta attribuzione della stessa, Intesi Group, in conformità all'art. 7 co. 8 DPCM, conserva per il periodo venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale, in relazione alle modalità di identificazione sopra elencate, copia per immagine del documento di identità esibito, tessera sanitaria,) o il modulo firmato digitalmente di cui alla lettera c), nonché' i documenti e i dati utilizzati per l'associazione e la verifica degli attributi.

In ogni caso il processo di Identificazione viene sempre condotto dai RAO o da un Pubblico Ufficiale (in base a quanto disposto dalle normative che disciplinano la loro attività) che devono operare secondo le seguenti procedure di identificazione applicate da Intesi Group:

- Identificazione de-visu che avviene con un incontro tra un RAO ed il richiedente.
- Identificazione e registrazione tramite processo IDentify Web.
- Identificazione attraverso verifica firma elettronica qualificata.

Intesi Group garantisce che tutti i metodi di riconoscimento applicati sono conformi alla normativa vigente in materia.

Per la verifica dell'identità il richiedente deve presentare documenti di riconoscimento tra uno dei seguenti:

- carta d'identità
- passaporto
- patente

Oltre al documento d'identità il titolare deve sempre presentare la tessera sanitaria italiana che deve essere in corso di validità.

Si precisa, inoltre, che al fine di rilasciare un identità digitale SPID per persona giuridica l'identity provider dovrà altresì verificare che il richiedente abbia il titolo per richiedere tale identità.

In altre parole, i dati che l'identity provider deve acquisire in fase di identificazione dipendono dal tipo di identità digitale SPID richiesta.

Per SPID per persone fisiche i dati obbligatori sono i seguenti:

a) cognome e nome;
b) sesso, data e luogo di nascita;
c) codice fiscale;
d) estremi di un valido documento di identità
e) gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM.

Per SPID per persone giuridiche i dati obbligatori, oltre i summenzionati, sono:

a) denominazione/ragione sociale;
b) codice fiscale o P.IVA (se uguale al codice fiscale);
c) sede legale;
d) visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società (in alternativa atto notarile di procura legale).

6.1 Identificazione e registrazione de-visu

Questa modalità di identificazione viene condotta da un operatore (RAO) qualificato, o da un Pubblico Ufficiale, e opportunamente formato e richiede la presenza fisica del richiedente, il quale deve farsi riconoscere presentando documenti di identità in corso di validità).

L'operatore, per una corretta e sicura attuazione del processo:

a) fornisce l'informativa sul trattamento dei dati (artt. 13 e 14 Regolamento (UE) 2016/679);
b) si assicura che il richiedente sia consapevole dei termini e delle condizioni associati all'utilizzo del servizio di identità digitale;

c) si assicura che il richiedente sia consapevole delle raccomandazioni e delle precauzioni da adottare per l'uso delle identità digitale e propone l'attivazione del servizio di segnalazione di ogni avvenuto utilizzo delle credenziali di accesso;
d) acquisisce i dati necessari alla dimostrazione di identità.

Il RAO deve verificare la documentazione presentata e nel caso in cui la ritenga sufficiente e valida, procedere con

1. La registrazione dei dati anagrafici del richiedente attraverso il portale RAO di Intesi Group.
2. La digitalizzazione di una copia dei documenti di identificazione presentati.
3. L'approvazione dell'identificazione attraverso l'apposizione di una firma digitale qualificata sui dati personali dell'utente.

L'approvazione dell'identificazione si conclude con l'invio all'utente di una email di attivazione contenente le istruzioni per attivare l'identità SPID.

6.2 Identificazione e registrazione IDentify-web

Questa modalità di identificazione viene condotta da un operatore RAO attraverso una videointervista con il richiedente. Il sistema di video conferenza utilizzato è messo a disposizione da Intesi Group che si occupa di fornire al richiedente le istruzioni necessarie per potervi accedere. Il richiedente, da parte sua, deve essere munito di un dispositivo (PC, Smartphone o Tablet) dotato di una webcam e di un sistema audio funzionante.

Il processo di identificazione avviene attraverso questi passi:

1. L'utente riceve una email con le istruzioni ed un link di avvio del processo di riconoscimento. L'email può essere inviata da un operatore abilitato o a seguito di un acquisto dallo store di Intesi Group (https://store.intesigroup.com/).
2. L'utente viene reindirizzato su una pagina Web di Intesi Group in cui deve inserire i propri dati personali, le immagini dei documenti di riconoscimento e fissare un appuntamento per il video riconoscimento.
3. Un operatore RAO verifica i dati e le immagini inserite dal cliente e può decidere se confermare i dati e la data del video riconoscimento oppure chiedere una correzione o rigettare la richiesta di riconoscimento.
4. Alla data concordata il richiedente ed il RAO si collegano in video call tramite la piattaforma IDentify Web.

5. All'avvio della video conferenza l'operatore acquisisce il consenso dell'utente trattamento dei dati personali e all'erogazione del servizio SPID. L'utente viene preventivamente informato circa le modalità di erogazione del servizio e dei propri diritti in quanto lo stesso riceve tutta la documentazione prima dell'avvio della sessione audio-video con operatore. In mancanza del consenso la video conferenza ed il processo di riconoscimento sono interrotti dal RAO.
6. La sessione audio- video si svolge nel seguente modo:
   a) l'acquisizione del consenso alla videoregistrazione e alla sua conservazione per 20 anni informando l'utente che la videoregistrazione sarà conservata in modalità protetta;
   b) l'operatore dichiara i propri dati identificativi;
   c) l'utente conferma le proprie generalità;
   d) l'utente conferma la data e l'ora della registrazione;
   e) l'utente conferma di volersi dotare di un'identità digitale e conferma i dati inseriti nella modulistica online in fase di pre-registrazione;
   f) l'utente conferma il proprio numero di telefonia mobile e l'indirizzo mail;
   g) l'operatore invia un sms che il richiedente è tenuto a mostrare o ripetere al RAO durante la videointervista, e una mail all'indirizzo di posta elettronica dichiarato, con un link ad una URL appositamente predisposta per la verifica;
   h) l'operatore chiede e ottiene conferma dall'utente circa la conoscenza delle tipologie di credenziali di cui disporrà per l'accesso ai servizi in rete;
   i) l'operatore chiede di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal richiedente, 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);
   j) l'operatore chiede di mostrare la tessera sanitaria su cui è riportato il codice fiscale del soggetto;
   k) l'utente conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità;
   l) l'operatore chiede al soggetto di compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta;
   m) l'operatore riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.

L'identificazione da remoto deve avvenire in una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte dell'utente nel rispetto delle seguenti condizioni:

a) le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;
b) l'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi;
c) la sessione audio/video, che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'identità e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.
d) La sessione audio/video deve essere completata senza nessuna interruzione.

Nel corso della video intervista il RAO può:

a) bloccare e rifiutare l'identificazione se ritiene che un documento presentato non rispetti le caratteristiche di validità e autenticità,
b) interrompere il processo di identificazione nel caso in cui la qualità audio/video sia di scarsa qualità o ritenuta non adeguata a a consentire la verifica dell'identità del richiedente.

L'approvazione dell'identificazione si conclude con l'invio all'utente di una email di attivazione contenente le istruzioni per attivare l'identità SPID.

6.3 Identificazione con firma elettronica qualificata

L'identificazione di un utente può avvenire attraverso la verifica di una firma digitale qualificata emessa da un prestatore di servizi fiduciari qualificati apposta sul modulo di richiesta SPID.

Il processo di identificazione avviene attraverso questi passi:

1. L'utente riceve una email con le istruzioni ed un link di avvio del processo di riconoscimento. L'email può essere inviata da un operatore abilitato o a seguito di un acquisto dallo store di Intesi Group (https://store.intesigroup.com/).
2. L'utente viene reindirizzato su una pagina Web di Intesi Group in cui deve inserire i propri dati personali con cui viene generato il modulo da firmare.

3. L'utente deve scaricare il modulo, firmarlo con il proprio certificato di firma digitale qualificata e caricarlo nuovamente sulla pagina web e inviarlo al server Intesi Group.
4. Alla ricezione del documento viene verificato che
   a. Il file sia il medesimo generato dal sistema,
   b. Il file non sia stato modificato dall'utente,
   c. Il file sia stato firmato con una firma digitale qualificata valida.

      Il processo di verifica controlla che i dati personali dell'utente contenuti all'interno del certificato (Nome, Cognome, Codice fiscale) corrispondano ai dati inseriti nel contratto e che siano coincidenti con i dati del richiedente l'identità digitale.

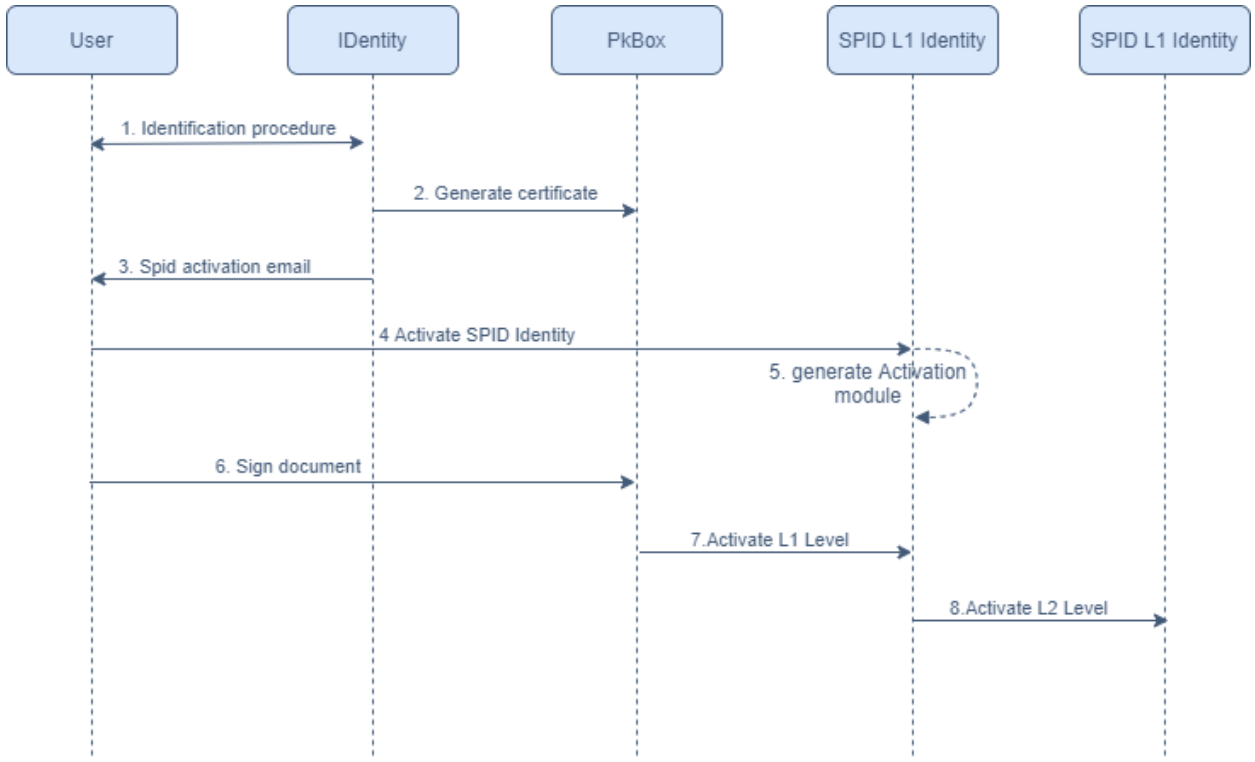
      Si verifica anche che il certificato non contenga l'OID 1.3.76.16.5 per certificati emessi tramite autenticazione SPID e non contenga la limitazione d'uso per i certificati di firma automatica.

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

L'approvazione dell'identificazione si conclude con l'invio all'utente di una email di attivazione contenente le istruzioni per attivare l'identità SPID.

6.4 Processo rilascio identità SPID

Il processo di identificazione ed attivazione della credenziale SPID è descritto nella diagramma seguente:



ed avviene attraverso questi passi:

1. L'utente effettua l'identificazione con una delle procedure descritte nei paragrafi precedenti.
2. Al termine dell'identificazione all'utente viene emesso un certificato qualificato della durata di 1 anno.
3. L'utente riceve una email con le istruzioni per procedere con l'attivazione della propria identità SPID ed un link per completare la procedura.
4. Cliccando sul link si apre una pagina Web in cui viene proposto il contratto di adesione al servizio SPID che l'utente deve firmare con il certificato rilasciato a seguito dell'identificazione.
5. Se la firma si conclude con successo all'utente viene chiesto di definire la password della credenziale SPID e la configurazione del token OTP SMS ad essa associato.

2.1.1 Certificato identificazione

Il processo di identificazione si conclude con anche l'emissione di un certificato qualificato di firma remota di Intesi Group che l'utente potrà utilizzare, solo ed esclusivamente, per eventuali attivazioni di altri servizi fiduciari di Intesi Group. Tale certificato ha le seguenti caratteristiche:

1. Durata: 1 anno
2. OID: 1.3.6.1.4.1.48990.1.1.1.7
3. userNotice (limitazione d'uso): "Il Presente certificato è utilizzabile solo per la sottoscrizione di contratti e/o moduli relativi ai servizi di Intesi Group".

Per evitare usi impropri, questo certificato verrà opportunamente mascherato negli strumenti di firma normalmente dati in uso ai clienti Intesi Group (IGSign, IGDesk e IGSmart) è sarà reso visibile solo nei casi di richiesta di attivazione di un nuovo servizio di Intesi Group.

7 Metodi di gestione dei rapporti con gli utenti

Intesi Group fornisce assistenza tecnica ai Titolari di identità SPID dalle 09.00 alle 18.00 da lunedì al venerdì. Il supporto è contattabile:

tramite email all'indirizzo: **support.tsp@intesigroup.com**

tramite ticket all'indirizzo: **https://support.intesigroup.com/**

Il personale Intesi Group risponde alle richieste di supporto entro 48h lavorative dalla presa in carico della richiesta di supporto.

8 Gestione del ciclo di vita dell'identità digitale

8.1 Sospensione e Riattivazione

L'Utente Titolare, può chiedere la sospensione immediata dell'Identità Digitale, anche nel caso in cui sospetti che la propria Identità Digitale sia stata utilizzata abusivamente o fraudolentemente ex art. 9 DPCM

La richiesta di sospensione immediata può essere effettuata direttamente dall'utente sul portale web Spid all'indirizzo https://spid.intesigroup.com.

Ricevuta la richiesta di sospensione, l'Identity Provider sospende l'Identità Digitale per un periodo massimo di trenta giorni, al termine del quale, in mancanza di altre azioni dell'utente (es. presentazione della copia di

denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione.) la credenziale viene riattivata.

Nel caso in cui l'utente ritenga di voler riattivare le proprie credenziali, può farne richiesta dal portale https://spid.intesigroup.com nella sezione dedicata alla gestione delle credenziali.
Per chiedere la sospensione e riattivazione dell'identità SPID si può procedere anche con via email o PEC scaricando l'apposito modulo di richiesta di revoca dal portale istituzionale di Intesi Group all'indirizzo **https://www.intesigroup.com/it/documenti** oppure collegandosi all'area privata della propria identità SPID sul sito **https://spid.intesigroup.com**

Per procedere con la sospensione o riattivazione occorre inviare una e-mail all'indirizzo **support.tsp@ig-trustmail.com** allegando:

1. copia scannerizzata del modulo di richiesta sospensione/riattivazione compilato e firmato;
2. copia del documento d'identità del richiedente;
3. copia del codice fiscale/tessera sanitaria;

Oppure, se il richiedente dispone di un certificato di firma digitale qualificata e di un indirizzo PEC (Posta Elettronica Certificata), può inviare solo copia del modulo di richiesta di sospensione e riattivazione firmato digitalmente all'indirizzo PEC (Posta Elettronica Certificata) **support.tsp@ig-trustmail.com** allegando:

1. copia digitale del modulo di richiesta sospensione/riattivazione compilato e firmato;
2. copia della denuncia sporta presso autorità nei casi copia di revoca per "Sospetto utilizzo abusivo / fraudolento da parte di un soggetto terzo" o di "furto/smarrimento credenziali".

Infine, si ricorda che la sospensione delle credenziali potrà avvenire anche ad opera del Gestore nei seguenti casi:

a) l'identità digitale SPID risulta non attiva per un periodo superiore a 24 mesi;
b) per decesso della persona fisica;
c) per estinzione della persona giuridica;
d) per uso illecito dell'identità digitale;
e) per scadenza contrattuale;
f) per scadenza documento identità

Nel caso della scadenza del documento di riconoscimento rilasciato dal cliente all'atto della registrazione il titolare dell'Identità Digitale dovrà aggiornare il proprio documento di riconoscimento accedendo alla propria area personale sul sito **https://spid.intesigroup.com.**

8.2 Revoca dell'identità digitale

L'utente può richiedere la revoca di una identità SPID per:

1. recesso dal servizio per esigenze personali oppure a seguito della perdita della disponibilità del numero di cellulare o della e-mail di contatto o nome utente;
2. sospetto utilizzo abusivo o fraudolento da parte di un soggetto terzo;
3. furto o smarrimento credenziali;

Per chiedere la revoca dell'identità SPID è necessario scaricare il modulo di richiesta di revoca dal portale istituzionale di Intesi Group all'indirizzo:

https://www.intesigroup.com/it/documenti

oppure collegandosi all'area privata della propria identità SPID sul sito:

https://spid.intesigroup.com

Per procedere con la revoca occorre inviare una e-mail all'indirizzo **support.tsp@ig-trustmail.com** allegando:

4. copia scannerizzata del modulo di richiesta revoca compilato e firmato;
5. copia del documento d'identità del richiedente;
6. copia del codice fiscale/tessera sanitaria;
4. copia della denuncia sporta presso autorità nei casi copia di revoca per "Sospetto utilizzo abusivo / fraudolento da parte di un soggetto terzo" o di "furto/smarrimento credenziali".

Se il richiedente dispone di un certificato di firma digitale qualificata e di un indirizzo PEC (Posta Elettronica Certificata), può inviare solo copia del modulo di richiesta di revoca firmato digitalmente all'indirizzo PEC (Posta Elettronica Certificata):

support.tsp@ig-trustmail.com

allegando:

3. copia digitale del modulo di richiesta revoca compilato e firmato;
4. copia della denuncia sporta presso autorità nei casi copia di revoca per “Sospetto utilizzo abusivo / fraudolento da parte di un soggetto terzo” o di “furto/smarrimento credenziali”.

Intesi Group invia conferma dell’avvenuta revoca a:

1. Indirizzo email definito come attributo secondario dell’identità SPID
2. Indirizzo email mittente della richiesta di revoca.

9 Livelli si servizio

9.1 Orari garantiti per le diverse fasi della registrazione

Indicatore di qualità	Modalità funzionamento	SLA (Livelli di servizio garantiti)
Disponibilità del servizio di richiesta	Erogazione automatica	erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi
	Erogazione in presenza	erogazione in giorni lavorativi dalle 09.00 alle 18.00
Identificazione de-visu		Attivo nei giorni lavorativi dalle 9:00 alle 18:00. Durata massima del processo 4h.
Identificazione con Firma Digitale		Attivo tutti i giorni della settimana. festivi inclusi. Durata massima del processo 1h.
Identificazione con sessioni audio/video		Attivo tutti i giorni lavorativi dalle 9:00 alle 18:00. Durata del processo 24h.

Identificazione con SPID.		Tutti i giorni della settimana, festivi inclusi Durata massima del processo 1h.
Creazione dell'identità digitali e delle relative credenziali		La creazione dell'identità avviene in modalità self-service, è disponibile tutti i giorni della settimana, festivi inclusi.
Attivazione dell'identità digitale		erogazione in modalità self-service con finestra 24h, tutti i giorni della settimana, festivi inclusi.

9.2 Registrazione e gestione ciclo di vita dell'identità

Indicatore di qualità	Modalità funzionamento	SLA (Livelli di servizio garantiti)
Disponibilità del servizio di registrazione identità	Erogazione automatica	≥ 99 % Singolo evento di indisponibilità ≤ 6 ore
	Erogazione in presenza	≥ 98 %
Tempo di risposta del sottoservizio di registrazione identità		≤ 24h ore (lavorative)
Disponibilità del servizio di rilascio credenziali	Erogazione automatica	≥ 99 % Singolo evento di indisponibilità ≤ 6 ore
	Erogazione in presenza	≥ 98 %
Tempo di rilascio credenziali		≤ 5 giorni lavorativi
Tempo riattivazione delle credenziali		≤2 giorni lavorativi

Disponibilità del servizio di sospensione e revoca delle credenziali		≥ 99 % Singolo evento di indisponibilità ≤ 6 ore
Tempo di sospensione delle credenziali		≤ 30 minuti
Tempo di revoca delle credenziali		≤ 5 giorni lavorativi
Disponibilità del servizio di rinnovo e sostituzione delle credenziali	Erogazione automatica	≥ 99 %
Tempo di rinnovo e sostituzione delle credenziali		≤ 5 giorni lavorativi
Disponibilità del sottoservizio di autenticazione		≥ 99,0% Singolo evento indisponibilità ≤ 4 ore
Tempo di risposta del sottoservizio di autenticazione		Tempo di risposta ≤3 sec almeno nel 95,0% delle richieste

9.3 Continuità operativa

9.3.1 Registrazione e rilascio identità

Indicatore di qualità	Valore limite
RPO sottoservizio registrazione e rilascio delle identità	1 ora
RTO sottoservizio registrazione e rilascio delle identità	8 ore

9.3.2 Revoca o sospensione Identità

Indicatore di qualità	Valore limite
RPO sottoservizio di sospensione e revoca delle credenziali	1 ora
RTO sottoservizio di sospensione e revoca delle credenziali	8 ore

9.3.3 Autenticazione

Indicatore di qualità	Valore limite
RPO sottoservizio di Autenticazione	1 ora
RTO sottoservizio di Autenticazione	8 ore

10 Misure anticontraffazione

10.1 Misure per prevenire furti d'identità

Come misura anti contraffazione per prevenire il verificarsi del furto d'identità, inteso come impersonificazione totale o parziale, Intesi Group ha integrato il sistema Scipafi (Sistema Centralizzato Informatico per la Prevenzione Amministrativa del Furto d'Identità) nei propri processi di identificazione.

Scipafi è il sistema pubblico di prevenzione della frode, che consente la verifica della veridicità delle informazioni contenute nei documenti di riconoscimento attraverso il riscontro con le informazioni presenti in banche dati pubbliche e private.

Nel processo di verifica dell'identità, in back-office l'IdP esegue i seguenti controlli tramite chiamate al sistema SCIPAFI:

- correttezza del codice fiscale e corrispondenza coi dati anagrafici del richiedente;
- esistenza e validità del documento di riconoscimento e corrispondenza col richiedente (disponibile solo per documenti emessi da autorità italiana)
- esistenza e validità della Tessera sanitaria e corrispondenza col codice fiscale del richiedente

Oltre a questi controlli, operatori appositamente formati da Intesi Group, effettuano una verifica visiva della validità del documento di riconoscimento e la corrispondenza con i dati anagrafici del richiedente. Per questo tipo di controlli gli operatori possono consultare siti messi a disposizione dalle pubbliche amministrazioni come il sito dell'Agenzia delle Entrate o il portale PRADO (Registro pubblico online dei documenti d'identità e di viaggio autentici). Nel caso in cui i controlli diano esito negativo, l'operatore può rigettare la richiesta.

Inoltre le procedure di identificazione prevedono questi vincoli:

- non sono ammessi documenti che non siano in corso di validità;
- Non sono ammessi documenti fotocopiati;
- Non sono ammesse immagini digitalizzate di documenti di scarsa qualità.

Infine tutta la documentazione raccolta è archiviata in maniera non modificabile;

10.2Protezione credenziali di firma

10.2.1 Misure per credenziali SPID di livello L1

Le credenziali di primo livello sono rappresentate dalla password. La password policy applicata è la seguente:

- lunghezza minima di otto caratteri;
- uso di caratteri maiuscoli e minuscoli;
- presenza di uno o più caratteri numerici;
- inclusione di almeno un carattere speciale;

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;

Le password sono salvate sul database di Intesi Group in formato sicuro usando l'algoritmo Salted SHA2.

10.2.2 Misure per credenziali SPID di livello L2

Alla sicurezza data dalla segretezza della password, il secondo livello aggiunge la sicurezza del possesso di un dispositivo fisico al quale viene inviata, tramite SMS, una password variabile.

Il sistema OTP di Intesi Group genera codici di autenticazione utilizzando l'algoritmo HOTP, il "seme" di generazione dell'OTP è differente per ogni credenziale di firma ed è conservato sul server QSCD di firma remota di Intesi Group denominato PkBox.

11 Monitoraggio

Allo scopo di garantire i livelli di servizio tutti i sistemi di erogazione del servizio SPID sono sottoposti al monitoraggio attraverso apposite sonde installate sui server. Lo scopo è quello di controllare:

- lo stato di efficienza in termini di performance, occupazione di spazi fisici e logici;
- la disponibilità dei sistemi (check di raggiungibilità, controlli sulle connessioni attive, ecc.);
- l'esecuzione ed il corretto funzionamento delle applicazioni;
- la 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.

Lo strumento di monitoraggio è raggiungibile via web, protetto mediante opportuno sistema di autenticazione. L'interfaccia web consente, ad ogni utente autenticato, di visualizzare lo stato globale dei servizi ed anche lo stato dettagliato d un dato controllo. Eventuali anomalie o errori sono segnalate mediante l'invio di messaggi inviati sugli smartphone del personale addetto che può prendere in carico l'anomalia nel più breve tempo possibile e intraprendere le azioni necessarie per risolverla.

12 Tracciature degli accessi al servizio di autenticazione

Il sistema mantiene traccia di tutte le operazioni svolte, registrando su di un apposito log tutta una serie di informazioni relative all'utilizzo dell'identità digitale. Tali dati sono conservati secondo quanto dettato dalle normative, archiviati e resi disponibili ai titolari dell'identità digitale su richiesta tramite procedura descritta nel seguito.

12.1Contenuto dei log

Vengono salvati i log per le seguenti operazioni:

- Richiesta di verifica dell'anagrafica del Richiedente presso le fonti autoritative di verifica.
- Esito della verifica di cui al punto precedente.

- Data e ora di inizio/fine del processo di richiesta dell'identità digitale.
- Data e ora di inizio/fine del processo di identificazione remota (se applicabile).
- In caso di identificazione informatica, i tracciamenti delle transazioni.
- Tracciamenti dei processi relativi all'emissione dell'identità digitale.
- Data, ora, destinatario e contenuto delle segnalazioni di utilizzo delle credenziali SPID di accesso.
- Tracciamenti degli utilizzi delle credenziali SPID di accesso, inseriti all'interno del Registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 (ventiquattro) mesi.
- Tracciamenti dei processi di sospensione, revoca e ripristino delle credenziali.

Tutti i dati sopra elencati saranno mantenuti dal Gestore nel rispetto del Codice della Privacy

12.2Tracciamento log autenticazioni

In ottemperanza al DPCM, vengono tracciate tutte le operazioni di autenticazione che coinvolgono le Identità Digitali SPID. Il tracciamento delle transazioni verrà effettuato tramite appositi file di log. Il tracciato dei record contiene le seguenti informazioni, in riferimento alla richiesta di autenticazione SAML:

- **AuthnRequestIdentifier**: identificativo univoco della richiesta SAML.
- **AuthnRequest**: richiesta SAML.
- **Issuer**: valore del campo issuerNameQualifier della richiesta authnRequest.
- **IssuerInstant**: istante di generazione della richiesta.

Per le risposte SAML a fronte di una autenticazione avvenuta con successo:

- **SpidCode**: codice univoco dell'identità SPID.
- **SamlResponse**: risposta completa SAML restituita all'utente.
- **AuthnRequestIdentifier**: identificativo univoco della richiesta SAML.
- **SamlResponseIdentifer**: identificativo univoco della risposta SAML.
- **SamlRespone Issuer** : valore del campo issuerNameQualifier della risposta SAML.
- **SamlRespone IssueInstant**: istante di generazione della richiesta.

Per le risposte SAML a fronte di una autenticazione conclusa con errore:

- **SamlResponse**: risposta SAML restituita all'utente.

- **AuthnRequestIdentifier**: identificativo univoco della richiesta SAML.
- **SamlResponseIdentifer**: identificativo univoco della risposta SAML.
- **SamlRespone Issuer** : valore del campo issuerNameQualifier della risposta SAML.
- **SamlRespone IssueInstant**: istante di generazione della richiesta.

12.3Lista accessi servizi

Tutti gli utilizzi dell'identità digitale sono salvati sui database di Intesi Group e resi disponibili ai Titolari di identità attraverso un portale Web, accessibile con la propria identità SPID, da cui è possibile estrarre la lista degli accessi effettuati.

Le informazioni estratte potranno essere utilizzate dal Titolare per gli usi consentiti dalla legge.

APPENDICE A Codici e formati dei messaggi di anomalia

Error Code	Scenario di riferimento	Binding	http Status Code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata IdP	Troubleshooting utente	Troubleshooting SP
1	Autenticazione corretta	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)	n.a.	n.a.	n.a.
2	Indisponibilità sistema	HTTP-Redirect HTTP POST	HTTP 500	n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio più tardi	n.a.
3	Errore di sistema	HTTP-Redirect HTTP POST	HTTP 500	n.a.	Utente	Pagina di cortesia con messaggio *"Sistema di autenticazione non disponibile - Riprovare più tardi"*	Ripetere l'accesso al servizio più tardi	n.a.

4	Formato *binding* non corretto	HTTP-Redirect HTTP-POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Formato richiesta non corretto - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta
5	Verifica della firma fallita	HTTP-Redirect HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Impossibile stabilire l'autenticità della richiesta di autenticazione - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma
6	*Binding* su metodo HTTP errato	HTTP-Redirect HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Formato richiesta non ricevibile - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare *metadata* Gestore dell'identità (IdP)
7	Errore sulla verifica della firma della richiesta	HTTP-Redirect HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma

						"*Formato richiesta non corretto - Contattare il gestore del servizio*"		
8	Formato della richiesta non conforme alle specifiche SAML	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr08	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID Fornire pagina di cortesia all'utente
9	Parametro *version* non presente, malformato o diverso da '2.0'	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch ErrorCode nr09	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID Fornire pagina di cortesia all'utente
10	*Issuer* non presente, malformato o non corrispondete all'entità che sottoscrive la richiesta	HTTP-Redirect HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Formato richiesta non corretto - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare formato delle richieste prodotte
11	*ID* (Identificatore richiesta) non presente, malformato o non conforme	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr11	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente

12	*RequestAuthnContext* non presente, malformato o non previsto da SPID	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "*Autenticazione SPID non conforme o non specificata*"		Informare l'utente
13	*IssueInstant* non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente
14	*destination* non presente, malformata o non oincidente con ill Gestore delle identità ricevente la richiesta	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)	n.a	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente
15	attributo *isPassive* presente e attualizzato al valore true	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15	Fornitore del servizio (SP)	n.a	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente
16	AssertionConsumerService non correttamente valorizzato	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupporte ErrorCode nr16	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente

17	Attributo *Format* dell'elemento *NameIDPolicy* assente o non valorizzato secondo specifica	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr17	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente
18	*Attributo* che riferiscea un valore non registrato nei metadati di SP	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18	Fornitore del servizio (SP)	n.a.	n.a.	Riformulare la richiesta con un valore dell'indice presente nei metadati
19	Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero tentativi secondo le policy adottate)	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19	Fornitore del servizio (SP)	Messaggi di errore specifico ad ogni interazione prevista	Inserire credenziali corrette	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
20	Utente privo di credenziali compatibili con il livello richiesto dal fornitore del servizio	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20	Fornitore del servizio (SP)	n.a	Acquisire credenziali di livello idoneo all'accesso al servizio richiesto	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto

21	Timeout durante l'autenticazione utente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21	Fornitore del servizio (SP)	n.a.	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinato periodo di tempo	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
22	Utente nega il consenso all'invio di dati al SP in caso di sessione vigente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22	Fornitore del servizio (SP)	n.a.	Dare consenso	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
23	Utente con identità sospesa/revocata o con credenziali bloccate	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "*Credenziali sospese o revocate*"		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
25	Processo di autenticazione annullato dall'utente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr25	Fornitore del servizio (SP)	n.a.		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
26	Processo di erogazione dell'identità digitale andata a buon fine	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)		Identità Digitale erogata con successo	

27	Utente già presente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr27	Fornitore del servizio (SP)		Utente già in possesso dell'Identità Digitale con il Fornitore di Identità Digitale selezionato	
28	Operazione annullata	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr28	Fornitore del servizio (SP)		Operazione di richiesta identità digitale annullata dall'utente	
29	Identità non erogata	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr29	Fornitore del servizio (SP)		Il fornitore non ha erogato l'identità digitale	
30	SP ha richiesto di autenticare l'utente con una identità digitale diversa da quella utilizzata dall'utente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr30	Fornitore del servizio (SP)		n.a.	Utilizzare un'identità digitale conforme a quanto richiesto dal SP.