Manuale Operativo SPID

Codice documento: MO-SPID

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 04/02/2016

Revisione: 01

REVISIONI

Revisione n°:	**01**	**Data Revisione:**	**04/02/2016**
Descrizione modifiche:	**Nessuna**		
Motivazioni:	**Prima emissione**		

SOMMARIO

A. Introduzione

A.1. Generalità del documento

Il presente *Manuale Operativo del Sistema Pubblico per la gestione dell'Identità Digitale* (nel seguito anche solo *Manuale Operativo*) descrive le regole generali e le procedure operative seguite da In.Te.S.A. S.p.A. (nel seguito anche solo *Identity Provider Gestore* o *INTESA*) nello svolgimento della propria attività di Identity Provider. Il Manuale Operativo è pubblicato a garanzia dell'affidabilità dei servizi offerti ai propri utenti e ai loro corrispondenti.

A.1.1. Scopo e campo d'applicazione

Il presente documento costituisce il Manuale Operativo del Sistema Pubblico per la gestione dell'Identità Digitale della società In.Te.S.A. S.p.A., già iscritta nell'elenco pubblico dei Certificatori accreditati, ed è redatto in conformità al Decreto del Presidente del Consiglio dei Ministri 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"* e ai successivi regolamenti.

A.1.2. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale.

Quanto fornito da In.Te.S.A. S.p.A. ai propri titolari e addetti per utilizzare la funzioni del servizio di Gestione dell'identità SPID offerto da In.Te.S.A. S.p.A. è coperto da diritti sulla proprietà intellettuale.

A.1.3. Procedure per l'aggiornamento

Gli aggiornamenti al presente documento saranno sottoposti ad approvazione di AgID e, successivamente, pubblicati sul sito del Gestore.

L'utente è tenuto a verificare periodicamente sul sito del Gestore la presenza di una eventuale nuova versione del Manuale Operativo.

A.1.4. Validità

Quanto descritto in questo documento si applica a In.Te.S.A. S.p.A., cioè alle sue infrastrutture logistiche e tecniche, al suo personale, ai Titolari di Identità Digitale e ai Service Provider che utilizzino i servizi di INTESA per verificare l'identità dei titolari.

A.1.5. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la Versione n.01 del Manuale Operativo dell'Identity Provider In.Te.S.A. S.p.A. rilasciata il 04/02/2016 in conformità al Decreto del Presidente del Consiglio dei Ministri 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"* e ai successivi regolamenti.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica presso l'indirizzo Internet:

http://e-trustcom.intesa.it/spid/manuale.htm

A.1.6. Responsabile del Manuale Operativo

Il Responsabile del Manuale Operativo è:
Antonio Raia
In.Te.S.A. S.p.A.
Indirizzo: Strada Pianezza, 289 - 10151 Torino (TO)
N. Telefono: +39-011-19216.111
N. Fax: +39-011-19216.375
Indirizzo di Posta Elettronica: ***uff_spid@intesa.it***

A.1.7. Responsabile dell'approvazione del Manuale Operativo

Il Responsabile dell'approvazione del Manuale Operativo è:
Franco Tafini
In.Te.S.A. S.p.A.
Indirizzo: Strada Pianezza, 289 - 10151 Torino (TO)
N. Telefono: +39-011-19216.111
N. Fax: +39-011-19216.375
Indirizzo di Posta Elettronica: ***uff_spid@intesa.it***

B. Generalità del Gestore

B.1. Dati identificativi del Gestore

Il Gestore - di cui il presente documento costituisce il Manuale Operativo è la società In.Te.S.A. S.p.A., di cui di seguito sono forniti i dati identificativi e una breve presentazione.

Denominazione sociale	In.Te.S.A. S.p.A.
Indirizzo della sede legale	Strada Pianezza, 289 - 10151 Torino (TO)
Legale Rappresentante	Amministratore Delegato
Registro delle Imprese di Torino	N. Iscrizione 1692/87
N. di Partita I.V.A.	05262890014
N. di telefono (centralino)	+39-011-19216.111
Indirizzo delle sede operativa	Strada Pianezza, 289 - 10151 Torino (TO)
Sito Internet	*https://www.intesa.it/*
N. di fax	+39-011-19216.375
Indirizzo di posta elettronica	***marketing@intesa.it***
ISO Object Identifier (OID)	1.3.76.21.7.1

In.Te.S.A. S.p.A. opera sul mercato dal 1987 come fornitore di soluzioni per l'e-business, che facilitano e rendono possibile la comunicazione e la collaborazione in rete di comunità aziendali. Basandosi su tecnologie all'avanguardia nei settori organizzativo, gestionale e operativo, offre soluzioni a valore aggiunto personalizzate, nel quadro di un'offerta di servizio globale al Cliente.

Nel corso degli ultimi anni ha rafforzato la propria presenza nell'offerta di soluzioni per la Business Process Integration, proponendosi quale partner in grado di gestire un'attività di business nel suo complesso per conto del cliente.

Dal marzo 2001 è iscritta all'albo dei Certificatori Accreditati tenuto da AgID.

In.Te.S.A. S.p.A. è composta da circa 150 dipendenti dislocati nella sede centrale di Torino e negli uffici tecnico/commerciali distribuiti in Italia.

Le unità periferiche sono dislocate a:

- MILANO - Piazzale Biancamano, 8 - 20121 Milano (MI)
- ROMA - Piazza Marconi, 15- 00144 Roma (RM)

In questo ambito, Intesa, come società facente parte del gruppo IBM, ha pertanto conseguito la certificazione UNI EN ISO 9001:2008 per *Sales, Design, Development, Consultancy, Delivery, Services, Installation and Support of all activities culminating in the provisions of IT and business solutions*. Tale certificazione è relativa a tutti i processi aziendali. In tale specifico ambito, il servizio di Identity Provider SPID è stato progettato, realizzato ed è erogato e assistito nel pieno rispetto dei processi di qualità di cui sopra.

B.2. Sito WEB del Gestore

Le informazioni relative ai servizi di Gestione dell'Identità Digitale offerti da Intesa sono disponibili on-line all'URL:

https://www.intesa.it/identita-digitale/

B.3. Descrizione dei metodi di gestione dei rapporti con gli utenti

INTESA mette a disposizione un servizio di helpdesk per gestire in modo efficiente i rapporti con i titolari di un'identità digitale, mettendo a disposizione operatori specializzati per supportare in modo efficiente le eventuali problematiche che possono sorgere durante l'utilizzo dell'identità digitale ovvero per fornire informazioni sul servizio offerto.

INTESA mette a disposizione tre diverse canali di accesso al servizio:

1) Via telefono, attraverso due diversi numeri:
    a) Numero verde per l'Italia: 800-805093;
    b) Numero chiamate dall'estero: +39 02-87119396;
2) Via web, attraverso l'indirizzo web www.hda.intesa.it nella sezione "Area clienti";
3) Via e-mail, attraverso l'indirizzo di posta elettronica hdintesa@advalia.com.

Le credenziali di accesso all'helpdesk vengono inviate ai titolari dell'identità digitale previa richiesta inviata collegandosi al sito www.hda.intesa.it. Tali credenziali dovranno essere utilizzate per autenticarsi presso uno dei servizi di helpdesk messi a disposizione da INTESA.

Modalità di accesso al servizio: telefono

L'accesso telefonico al servizio consente:

1) Apertura del ticket di assistenza;

2) Assistenza tecnica telefonica da parte di operatori.

Per accedere al servizio telefonico:

1) Chiamare il numero verde o il numero chiamate dall'estero;
2) Seguire le indicazioni del risponditore automatico;
3) Inserire il proprio HELPDESKCODE;
4) Attendere di essere messi in comunicazione con il primo operatore disponibile.

Modalità di accesso al servizio: e-mail

L'accesso via e-mail al servizio consente:

1) Apertura del ticket di assistenza;
2) Ricezione via e-mail di notifica dell'apertura del ticket;
3) Ricezione via e-mail di notifica della presa in carico del ticket.

Per accedere al servizio via e-mail:

1) Scrivere in lingua italiana o inglese all'indirizzo messo a disposizione;
2) Utilizzare l'indirizzo mail censito in fase di rilascio delle credenziali.

Modalità di accesso al servizio: web

L'accesso all'AREA CLIENTI consente:

1) Apertura del ticket di assistenza online;
2) Consultazione dello stato di avanzamento del proprio ticket;
3) Consultazione archivio contenente lo storico dei propri ticket;
4) Download degli aggiornamenti sui servizio.

Il sito dell'Helpdesk è raggiungibile anche dal sito istituzionale www.intesa.it selezionando dal Menù di navigazione la voce "Helpdesk".

Per accedere al sito dell'Helpdesk:

1) Collegarsi all'indirizzo www.hda.intesa.it;
2) Cliccare su "Area Clienti" per accedere all'area riservata e inserire le credenziali ricevute;
3) Accedere al Portale di Assistenza di INTESA e procedere alla compilazione del ticket.

Orari di accesso al servizio

Il servizio di Helpdesk è reso disponibile dal Lunedì al Venerdì dalle ore 8,30 alle ore 19,00 attraverso uno dei tre canali descritti.

B.4. Definizioni e acronimi

Sono qui riportati i significati di acronimi e di termini specifici aggiuntivi rispetto a quanto indicato all'Art.1 del DPR 445/00 al quale si fa espresso riferimento.

Non sono riportati i significati di alcuni acronimi e termini specifici di uso comune.

Termine o acronimo	***Significato***
AgID	Agenzia per l'Italia Digitale
Gestore	L'azienda che si pone come Identity Provider nel contesto SPID
HASH	Funzione che prende in input una stringa di lunghezza variabile e ritorna una stringa di lunghezza fissa
HSM	Hardware Security Module, insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
Identità Digitale	Insieme di attributi identificativi atti a contraddistinguere in modo certo e univoco l'identità di un utente sul web.
Identity Provider	Soggetto accreditato presso AgID che ha il ruolo di creare e gestire le Identità Digitali
OTP	One Time Password, è una password che è valida solo per una singola sessione di accesso o una transazione
Richiedente	L'utente che si avvale del servizio di SPID per la richiesta di ottenimento di Identità Digitale
Salting	Procedura che prevede di associare una sequenza casuale di bit assieme ad una password come input a una funzione unidirezionale, di solito una funzione hash, il cui output è conservato al posto della sola password, e può essere usato per autenticare gli utenti
SAML	Security Assertion Markup Language (SAML) è uno standard informatico per lo scambio di dati di autenticazione e autorizzazione (dette asserzioni) tra domini di sicurezza distinti, tipicamente un identity provider (entità che fornisce informazioni di identità) e un service provider (entità che fornisce servizi).
Service Provider	Soggetto pubblico o privato che eroga servizi on-line, previo riconoscimento dell'utente da parte del gestore dell'Identità Digitale
SPID	Sistema Pubblico per la gestione dell'Identità Digitale
Token OTP	Vedi OTP

B.5. Riferimenti normativi

CAD	Decreto Legislativo n. 82 del 7 Marzo 2005 (G.U. n. 112 del 16 Maggio 2005). “Codice dell’amministrazione Digitale” aggiornato dal Decreto Legislativo n. 159 del 4 Aprile 2006 (G.U. n. 99 del 29 Aprile 2006).
Direttiva 1999/93/CE	Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 Relativa ad un quadro comunitario per le firme elettroniche
DPCM 24/10/2014	Decreto del Presidente del Consiglio dei Ministri 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”
ISO-IEC 29115	ISO/IEC 29115:2013 definisce un framework per la gestione la garanzia di autenticazione di un’entità in un dato contesto.

C. Obblighi

C.1. Obblighi del gestore dell'identità digitale

Nello svolgimento della sua attività il gestore dell'identità digitale, opera in conformità con quanto disposto da:

a) il Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014;

b) i regolamenti di cui all'art. 4 del suddetto Decreto;

In particolare il Gestore dell'identità digitale è conforme a quanto stabilito dall'Art.11 del DPCM 24/10/2014:

a) utilizza sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale;

b) adotta adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso;

c) effettua 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;

d) effettua, con cadenza almeno annuale, un'analisi dei rischi;

e) definisce il piano per la sicurezza dei servizi SPID, da trasmettere all'Agenzia, e ne garantisce l'aggiornamento;

f) allinea le procedure di sicurezza agli standard internazionali, la cui conformità e' certificata da un terzo abilitato;

g) conduce, con cadenza almeno semestrale, il «*Penetration Test*»;

h) garantisce la continuità operativa dei servizi afferenti allo SPID;

i) effettua ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna;

j) garantisce la gestione sicura delle componenti riservate delle identità digitali degli utenti, assicurando che le stesse non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata;

k) garantisce la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dal presente decreto e dai regolamenti attuativi adottati dall'Agenzia ai sensi dell'art. 4;

l) si sottopone, con cadenza almeno biennale, ad una verifica di conformità alle disposizioni vigenti da parte di un organismo di valutazione accreditato ai sensi del Regolamento CE 765/2008 del Parlamento Europeo e del Consiglio del 9 luglio 2008. Invia all'Agenzia l'esito della verifica, redatto dall'organismo di valutazione in lingua inglese, entro tre giorni lavorativi dalla sua ricezione;

m) informa tempestivamente l'Agenzia e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali, secondo le modalità individuate nei regolamenti adottati ai sensi dell'art. 4;

n) adegua i propri sistemi a seguito degli aggiornamenti emanati dall'Agenzia;

o) invia all'Agenzia, in forma aggregata, i dati da questa richiesti a fini statistici, che potranno essere resi pubblici.

Inoltre, ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del DPCM, il Gestore si impegna a revocare l'identità digitale nei seguenti casi:

a) 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 richiesta dell'utente;

f) per scadenza contrattuale.

C.2. Obblighi del Titolare

Il Titolare è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (Art.32, comma 1 del CAD).

Il Titolare dell'Identità Digitale deve inoltre:

a) fornire tutte le informazioni richieste dal Gestore, garantendone l'attendibilità e l'autenticità sotto la propria responsabilità;

b) inoltrare la richiesta di rilascio dell'Identità Digitale secondo le modalità indicate nel presente Manuale Operativo;

c) comunicare al Gestore eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici o di Internet, ecc.;

d) conservare con la massima diligenza le credenziali di autenticazione ricevute dal Gestore al fine di garantirne l'integrità e la massima riservatezza;

e) richiedere immediatamente al Gestore la sospensione dell'identità digitale nel caso in cui ritenga che sia stata utilizzata fraudolentemente;

f) fornire entro trenta giorni copia della denuncia presentata all'autorità giudiziaria in seguito ad aver richiesto la sospensione dell'identità digitale per utilizzo illecito o fraudolento;

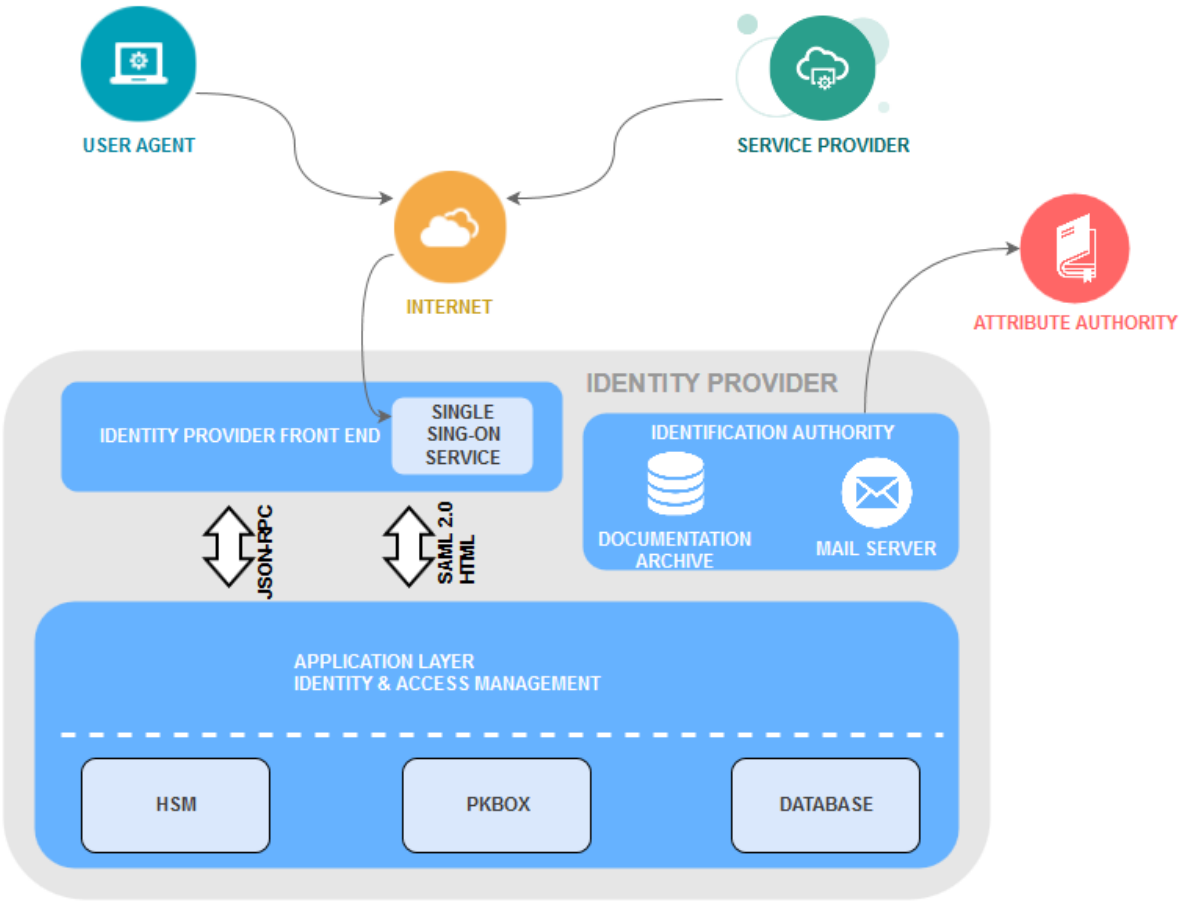
g) sottoscrivere la richiesta di revoca attraverso le modalità previste dal presente Manuale Operativo, specificandone la motivazione e la sua decorrenza;

h) sottoscrivere la richiesta di sospensione attraverso le modalità previste dal presente Manuale Operativo, specificandone la motivazione e la sua decorrenza.

D. Descrizione del servizio

D.1. Architetture applicative e di dispiegamento

La figura seguente mostra l'architettura logica adottata dell'Identity Provider per l'erogazione del servizio di gestione delle identità digitali.



La figura evidenzia le principali componenti che costituiscono il servizio di gestione dell'identità digitale:

- **IdP Front End**: layer applicativo che presenta visualmente tutte le funzionalità offerte dal portale INTESA e si pone come interfaccia tra Internet (di cui costituisce l'unico punto di accesso) e la componente di back end di gestione del ciclo di vita dell'identità digitale
- **Identification Autority**: componente di gestione dell'identificazione delle richiesta di un'identità digitale da parte di un utente. L'Identity Provider deve garantire l'archiviazione di tutta la documentazione, eventualmente anche audio/video, atta a

provare il processo di identificazione (vedi E.1) nonché il tracciato del flusso di validazione verso *Attribute Autority* esterne.

L'architettura di gestione delle identità digitali è costruita su 2 livelli applicativi:

- livello crittografico e di storage;
- livello di back end;

Il livello crittografico e di storage è identificato dai servizi offerti tramite HSM, PkBox e Database.

Il livello di back-end è caratterizzato dai seguenti servizi applicativi:

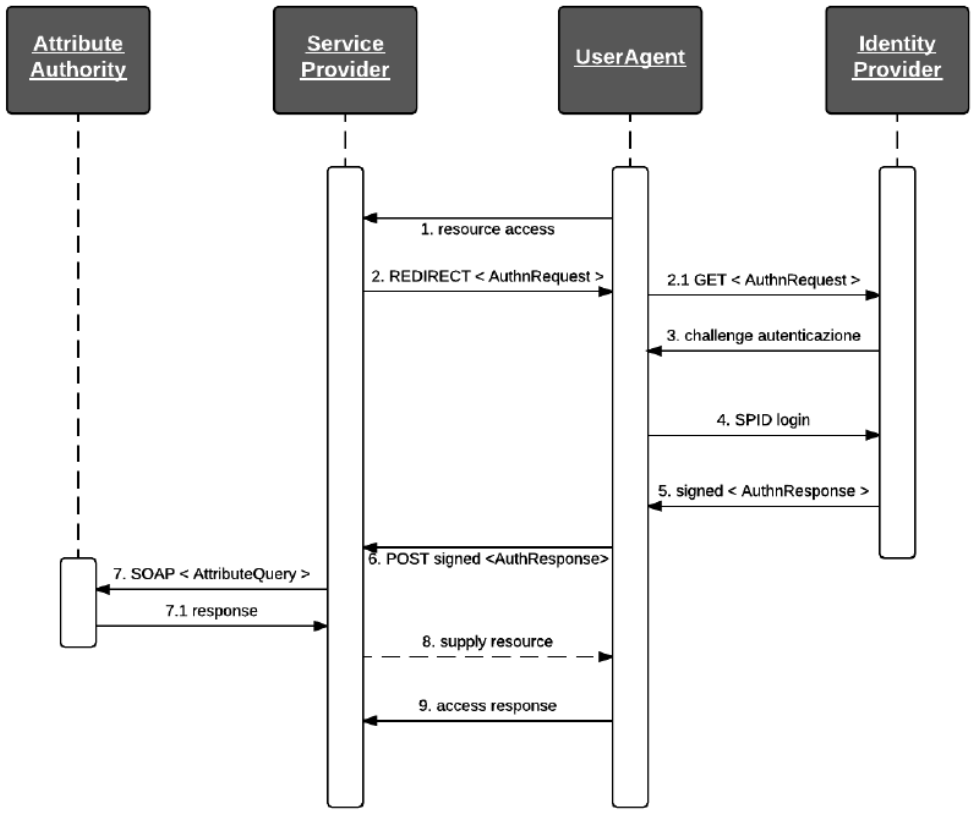
- **Time4ID**: componente responsabile della gestione delle credenziali di livello L2 tramite token OTP su canale e-mail.
- **Time4User**: componente che gestisce l'identità digitale nonché le credenziali SPID di livello L1. All'interno di questo componente viene implementata la logica di autenticazione SPID tramite asserzioni SAML v.2.0, interfacciandosi con la componente Time4ID per supportare l'autenticazione basata su credenziali di livello L2.

D.2. Architetture 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 (cfr D.3).

Il processo di autenticazione descritto nell'immagine sottostante prevede i seguenti attori:

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



D.2.1. Processo di autenticazione

Questi i passi previsti per effettuare l'autenticazione di un entità SPID presso un Identity Provider:

1. L'utente richiede l'accesso ad una risorsa messa a disposizione da un Service Provider;
2. Il Service Provider ridirige la richiesta, tramite richiesta SAML all'Identity Provider che gestisce l'identità SPID;
3. L'Identity Provider, a fronte della ricezione di una richiesta, inizia una fase di autenticazione con l'utente;
4. L'utente si identifica attraverso la sua credenziale SPID;
5. L'Identity Provider, a fronte della verifica della credenziale, invia una conferma al Service Provider tramite risposta SAML;
6. Il Service Provider riceve la conferma dall'Identity Provider contenente il risultato dell'autenticazione;

7. Se necessario il Service Provider effettua in proprio controlli sugli attributi presso un Attribute Authority;
8. Il Service Provider attesta gli attributi dell'utente;
9. Il Service Provider, a fronte di riscontri positivi, consente l'accesso all'utente;
10. L'utente accede alla risorsa come richiesto.

D.2.2. Requisiti funzionali

Questi i requisiti funzionali che il gestore delle identità deve garantire per la gestione del profilo di autenticazione:

1. Garantire il rispetto del protocollo SAML per un corretto espletamento della fase di autenticazione tra Service Provider, utente e Identity Provider;
2. L'Identity Provider deve mantenere un registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi;
3. Garantire una facile ricerca e consultazione dei dati di tracciatura estraendo nel record alcune informazioni dei messaggi SAML;
4. Le tracciature devono essere mantenute nel rispetto del codice della privacy;
5. Prevedere meccanismi di cifratura dei dati o persistenza cifrata delle informazioni;
6. Garantire integrità dei dati memorizzati.

D.3. Credenziali di autenticazione

Il processo di autenticazione informatica è finalizzato alla verifica dell'identità digitale associata a un soggetto, ai fini della erogazione di un servizio fornito in rete. A tale verifica dell'identità è associato un livello di sicurezza o di garanzia (*Level of Assurance* - *LoA*) progressivamente crescente in termini di sicurezza.

Il livello di sicurezza è il risultato dell'intero procedimento che sottende all'attività di autenticazione. Tale processo va dalla preliminare associazione tra un soggetto e un'identità digitale che lo rappresenta in rete, con annessa attribuzione di credenziali in grado di comprovare tale associazione, ai meccanismi che realizzano il protocollo di autenticazione al momento della richiesta di un servizio in rete.

In SPID sono definiti tre livelli di sicurezza, corrispondenti ad altrettanti livelli specificati nella ISO-IEC 29115.

In particolare:

a) Livello 1 (corrispondente al LoA2 dell'ISO-IEC 29115): garantisce con un buon grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione.

A tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema autenticazione a singolo fattore, ad es. la password.

Questo livello può essere considerato applicabile nei casi in cui il danno causato da un utilizzo indebito dell'identità digitale, abbia un basso impatto per le attività del cittadino/impresa/amministrazione.

b) Livello 2 (corrispondente al LoA3 dell'ISO-IEC 29115): garantisce con un alto grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione.

   A tale livello è associato un rischio ragguardevole e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali.

   Questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale possa provocare un danno consistente.

c) Livello 3 (corrispondente al LoA4 dell'ISO-IEC 29115): garantisce con un altissimo grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione.

   A tale livello è associato un rischio altissimo e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'Allegato 3 della Direttiva 1999/93/CE;

   Questo è il livello di garanzia più elevato e da associare a quei servizi che possono subire un serio e grave danno per cause imputabili ad abusi di identità; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell' identità digitale può provocare un danno serio e grave.

D.3.1. Livello 1 SPID

Per il livello 1 SPID l'Identity Provider chiede al Richiedente di creare una credenziale a singolo fattore costituita da una password.

In particolare, per garantire di ottenere password complesse e difficilmente attaccabili, vengono imposti i vincoli descritti in E.4.1.

A livello 1, i file delle credenziali devono essere protetti da un sistema di controllo in modo da limitare l'accesso agli amministratori e alle applicazioni autorizzate.

D.3.2. Livello 2 SPID

In questo scenario, la credenziale è costituita dalla combinazione di una password, come descritto nel paragrafo precedente, e l'adozione di una OTP generata a richiesta e inviata all'indirizzo e-mail, verificato preventivamente durante la fase di identificazione e sul quale si garantisce quindi un possesso certo.

La validità dell'OTP deve essere limitata ad una sola transazione nell'ambito della sessione applicativa e per un tempo limitato.

D.3.3. Livello 3 SPID

Non implementato dal Gestore.

D.4. Descrizione dei codici e dei formati dei messaggi di anomalia

Nella presente sezione si intendono fornire ai titolari di identità digitale indicazioni di cosa fare e a chi rivolgersi nel caso in cui si verifichino anomalie o vengano restituiti errori durante l'utilizzo dei servizi telematici offerti da INTESA per l'autenticazione SPID.

Segue una descrizione dei principali messaggi di anomalia che possono essere restituiti dal sistema.

D.4.1. Registrazione

in caso di…	a chi rivolgersi… o cosa fare….
Password non valida	Verificare la correttezza della password come descritto in E.4.1
Email già utilizzata	Se possibile, inserire un indirizzo alternativo. In caso contrario utilizzare l'apposita procedura presente sulla pagina per richiedere un nuovo indirizzo e-mail.
Codice verifica telefono non corretto	Il codice inserito per la verifica del numero di telefono non è corretto. Controllare il codice ricevuto via sms e inserirlo nuovamente.
Identità non valida	Errore di consistenza nei dati inseriti oppure ricevuto in seguito alla consultazione delle fonti autoritative. Verificare i dati inseriti.

D.4.2. Identificazione a vista da remoto

in caso di…	a chi rivolgersi… o cosa fare….
Errore dispositivo di input	Verificare il corretto funzionamento dei dispositivi di input (microfono, webcam).
Impossibile stabilire una connessione	Verificare lo stato della connessione di rete e di non essere connessi attraverso un proxy. Nel caso in cui il problema persista, contattare l'amministratore di sistema.

D.4.3. Autenticazione

in caso di…	a chi rivolgersi… o cosa fare….
Credenziali non corrette	Verificare la correttezza delle credenziali inserite.
UserID non presente nel sistema	Verificare la correttezza dello UserID e di aver selezionato il corretto Identity Provider.
Errore di autenticazione	Nel caso in cui il problema persista, contattare il Gestore.

Per una descrizione dettagliata di tutti i possibili messaggi di errore che il sistema restituirà nelle diverse fasi del processo di autenticazione, si rimanda alla lettura dell'Appendice A.

D.5. Livelli di servizio

D.5.1. Registrazione e gestione ciclo di vita dell'identità

Gli indicatori utilizzati per la misurazione dei livelli di servizio garantiti per le diverse fasi del servizio di registrazione e gestione del ciclo di vita dell'identità, sono riportati nella seguente tabella.

NOME INDICATORE	*PARAMETRI DI MISURAZIONE*	*VALORI DI SOGLIA*
Disponibilità del servizio di registrazione dati	Rapporto tra il tempo di disponibilità e il tempo totale nel periodo di riferimento	7 giorni su 7 24 ore su 24 disponibilità ≥ 99%
Servizio di identificazione a vista	Tempo di identificazione, a partire dalla richiesta acquisita fisicamente negli uffici di INTESA nel seguente orario: Da lunedì a venerdì Dalle ore 8.30 alle 17.30	20 minuti

Servizio di identificazione a vista da remoto	Tempo di identificazione, a partire dall'avvio della sessione audio/video nel seguente orario: Da lunedì a venerdì Dalle ore 8.30 alle 17.30	20 minuti
Servizio di identificazione informatica tramite firma digitale	Tempo di identificazione, a partire richiesta acquisita digitalmente attraverso l'invio della stessa via web.	2 giorni
Emissione dell'identità digitale	Tempo di emissione dell'identità digitale e consegna delle credenziali, a partire dall'avvenuta identificazione del Richiedente.	2 giorni
Sospensione/revoca dell'identità digitale	Tempo di sospensione/revoca dell'identità digitale, a partire richiesta acquisita attraverso le modalità descritte in F.1.	4 ore

D.5.2. Autenticazione

Gli indicatori utilizzati per la misurazione dei livelli di servizio garantiti per le diverse fasi del servizio di registrazione, sono riportati nella seguente tabella.

NOME INDICATORE	*PARAMETRI DI MISURAZIONE*	*VALORI DI SOGLIA*
Disponibilità del servizio di autenticazione	Rapporto tra il tempo di disponibilità e il tempo totale nel periodo di riferimento	7 giorni su 7 24 ore su 24 disponibilità ≥ 99%
Livello di Servizio Gestione problemi	Tempi di evasione delle chiamate pervenute all'HelpDesk, classificate secondo la loro gravità	Tempi di chiusura chiamata: 98% entro 2 giorni

D.6. Tracciature

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 a norma e resi disponibili ai titolari dell'identità digitale su richiesta tramite apposita procedura descritta nel seguito.

I dati memorizzati costituiscono inoltre la base per le elaborazioni statistiche e la misurazioni del livello di servizio descritte nel paragrafo "Sistema di monitoraggio".

D.6.1. Contenuti dei log

I log vengono registrati 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 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.

D.6.1.1. Tracciamento 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 prodotti tramite libreria Log4J.

Il tracciato dei record prevederà le seguenti informazioni in riferimento alla sessione di autenticazione SAML:

- SpidCode;
- AuthnRequest;
- Response;
- AuthnReq_ID;
- AuthnReq_IssueInstant;
- AuthnReq_Issuer;

- Resp_ID;
- Resp_IssueInstant;
- Resp_Issuer;
- Assertion_ID;
- Assertion_subject;
- Assertion_subject_NameQualifier;

I file di log giornalieri verranno firmati elettronicamente e conservati in directory giornalieri permettendo l'archiviazione annuale di questi.

D.6.2. Modalità di richiesta dei log

In qualunque momento, il titolare di identità digitale può richiedere copia dei log registrati come prova della propria attività. A tale proposito il Gestore Intesa prevede la seguente procedura per la richiesta:

1. il Titolare compila l'apposito modulo, fornito su richiesta dal Gestore utilizzando i canali definiti nel paragrafo "Metodi di gestione dei rapporti con gli utenti", indicando i seguenti dati:
    - dati anagrafici del Titolare;
    - periodo temporale del quale si richiedono i log;
    - ulteriori dettagli circa la tipologia di azione per la quale si richiedono i log dell'attività;
    - motivazione della richiesta;
    - autorizzazione relativa alla normativa sulla privacy;
    - modalità di invio dei dati di log (raccomandata postale ovvero Posta Elettronica Certificata);
    - recapito del Titolare da utilizzare nell'invio;
2. il modulo compilato deve essere inviato al Gestore in una delle seguenti modalità:
    - tramite PEC all'indirizzo uff_spid@pec.trustedmail.intesa.it;
    - tramite raccomandata postale;
3. il personale del Gestore, dopo aver verificato la correttezza della richiesta, recupera le informazioni dal registro mediante l'accesso ai server o agli archivi presso i quali si reperiscono i file di log;

4. il personale del Gestore invia i dati al Titolare entro 3 giorni lavorativi dalla ricezione della richiesta. I dati sono inviati nella modalità indicata nella richiesta. Il log è prodotto in formato testo, firmato digitalmente (.p7m), con i dati minimi di riferimento previsti dalla normativa. Per l'apertura di tale file, il titolare dovrà utilizzare un'applicazione di verifica di firma qualificata, tra cui *DigitalSign Reader*, che è disponibile sul sito del Gestore Intesa all'indirizzo:

   http://e-trustcom.intesa.it/softwarediverifica.html

D.7. Misure anti-contraffazione

INTESA mette in atto tutti i processi volti a garantire la protezione delle credenziali contro abusi e usi non autorizzati ovvero ad assicurare la sicurezza della conservazione delle credenziali o dei mezzi usati per loro produzione. Per via della diversa natura tecnologica che caratterizza le diverse credenziali, per ogni livello di sicurezza SPID vengono adottate diverse misure anti-contraffazione.

Qualunque sia il livello SPID al quale si collochi una credenziale richiesta, INTESA applica come prima misure anti-contraffazione la verifica delle informazioni fornite attraverso accertamenti effettuati tramite fonti autoritative istituzionali, in grado di dare conferma della veridicità dei dati raccolti.

Attraverso apposite convenzioni stipulate, INTESA usufruisce del servizio di verifica del codice fiscale e dei dati anagrafici ad esso strettamente correlati fornito dall'Agenzia delle Entrate.

D.7.1. Livello 1 SPID

A questo livello è associata una credenziale composta da una password, la cui principale misura anti-contraffazione è rappresentata dalla riservatezza di conservazione da parte del titolare dell'identità digitale.

Per aumentare il grado di sicurezza al fine di evitare il rischio di utilizzi non autorizzati dell'identità, INTESA mette in atto le seguenti misure anti-contraffazione:

a) i file delle credenziali sono protetti da un sistema di controllo in modo da limitare l'accesso agli amministratori e alle applicazioni autorizzate;

b) all'atto del salvataggio delle credenziali, questo vengono processate applicando tecniche di salt e hashing al fine di garantire maggior sicurezza contro attacchi di tipo brute force o dizionario;

D.7.2. Livello 2 SPID

Alla sicurezza data dalla segretezza della password, il secondo livello aggiunge quella data dal possesso di un dispositivo fisico al quale viene inviata una seconda credenziale variabile e a durata limitata. INTESA adotta un sistema di OTP via e-mail, che assicura dunque una sicurezza maggiore in quanto si suppone che l'utente, oltre che conoscere la password, debba garantire l'accesso all'indirizzo e-mail fornito in fase di sottoscrizione del servizio e verificato durante il riconoscimento del titolare.

Oltre alla garanzia di sicurezza data dall'accesso all'indirizzo di posta, l'architettura dell'autenticazione OTP permette di generare codici di autenticazione a durata limitata (60 secondi) e dinamici, il che rende inutile entrare in possesso della credenziale in un secondo momento rispetto a quello della sua richiesta.

La contraffazione di questa tipologia di credenziali risulta dunque estremamente complessa, perché richiederebbe di entrare in possesso sia della password di primo livello che dell'indirizzo e-mail, andando in contrasto con l'obbligo a cui è soggetto il titolare relativo alla diligenza nella conservazione delle credenziali fornite.

D.7.3. Livello 3 SPID

Non implementato dal Gestore.

D.8. Sistema di monitoraggio

I gestori di identità digitali rendono disponibile all'AgID le seguenti informazioni:

a) livello di soddisfazioni dei propri clienti;

b) le caratteristiche di eventuali servizi aggiuntivi offerti;

c) le informazioni relative a disservizi; l'Identity Provider ha l'obbligo di comunicare all'Agenzia, il codice del disservizio entro uno SLA prestabilito (entro 30 minuti o due ore a seconda della classificazione del disservizio);

d) l'Identity Provider dovrà comunicare all'Agenzia, con cadenza almeno bimestrale, i dati statistici relativi all'utilizzo del sistema, le metriche qualitative e quantitative concordate.

Per un monitoraggio costante dello stato dei servizi offerti, il Gestore dispone di una piattaforma di monitoraggio in grado di rilevare in real time anomalie o disservizi e di segnalarli con differenti livelli di gravità alle strutture preposte alla gestione operativa.

Le funzioni principali disponibili sono:

- monitoraggio dell'intera infrastruttura tecnologica (HW, Networking, Storage occupancy, etc.);

- sonde di monitoraggio e controllo dei processi automatici;
- correlazione indicatori applicativi e infrastrutturali;
- implementazione e modifica di regole di gestione degli allarmi;
- gestione degli allarmi;
- gestione reportistica KPI-SLA.

L'architettura è monitorata nei suoi componenti attraverso plugin sulla piattaforma Nagios, tramite plugin base e plugin specifici creati da Intesi Group per il monitoraggio dei sistemi Time4Mind. Si riportano di seguito alcuni esempi.

Plugin base, per i server RedHat:

- PING;
- NTP-Time;
- File System free space;
- Load average;
- Swap Usage;
- SSH;
- VMWareTools (se virtualizzati).

Plugin Applicativi specifici:

- Time4User-service;
- PkCA-service;
- PkBox-service;
- NetHSM.

E. Rilascio identità digitali

E.1. Identificazione del soggetto richiedente

L'Identity Provider deve verificare con certezza l'identità del Richiedente alla prima richiesta di emissione di un'Identità Digitale, al fine di evitare furti d'identità.

Tali operazioni vengono svolte dall'Identity Provider in ottemperanza con quanto previsto dalla vigente normativa e secondo le modalità descritte nel seguito, il quale provvede all'identificazione degli utenti e all'emissione delle identità digitali.

Per i successivi rinnovi (per le credenziali soggette a scadenza), tale attività non dovrà essere ripetuta: sarà cura del Titolare mantenere aggiornati i propri dati sulla pagina personale messa a disposizione dall'Identity Provider su un portale dedicato.

Nel caso in cui il Richiedente sia una persona fisica, i dati di registrazione necessari all'emissione dell'identità digitale sono:

- Nome e Cognome;
- Data di nascita;
- Comune o stato estero di nascita;
- Codice fiscale;
- Sesso;
- Estremi del documento d'identità esibito.

Per le persone giuridiche sono obbligatorie le seguenti informazioni:

- Denominazione/ragione sociale;
- Codice fiscale o P.IVA (se uguale al codice fiscale);
- Sede legale;
- Visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società (in alternativa atto notarile di procura legale);
- Estremi del documento di identità utilizzato dal rappresentate legale.

In entrambi i casi potranno essere forniti all'Identity Provider i seguenti attributi secondari:

- Numero di telefonia fissa o mobile;
- Indirizzo di posta elettronica;
- Domicilio fisico e/o digitale;
- Eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni.

Per gli attributi secondari, sono forniti almeno un indirizzo di posta elettronica e un recapito di telefonia mobile, entrambi verificati dal gestore di identità digitale nel corso del processo di identificazione, inviando un messaggio di posta all'indirizzo dichiarato, contenente una URL per la verifica, e un SMS al numero di cellulare con un codice numerico di controllo che deve essere riportato in fase di identificazione.

Per quanto riguarda l'indirizzo di posta elettronica, il gestore dovrà accertarsi, oltre che lo stesso sia un indirizzo corrispondente a una reale casella di posta, che sia unico in ambito SPID, ovvero che esso non sia stato precedentemente indicato dallo stesso soggetto per l'acquisizione di una identità digitale SPID presso lo stesso o un altro gestore dell'identità digitale. Tale controllo potrà essere effettuato anche consultando la directory delle identità SPID. Nel caso tale verifica non dovesse andare a buon fine, il gestore dovrà dare obbligo al richiedente dell'indicazione di un indirizzo alternativo.

E.1.1. Identificazione a vista

L'attività di identificazione del richiedente viene effettuata:

a) Dall'Identity Provider, tramite il personale preposto all'operazione presso gli uffici di INTESA;

b) Da Local Identification Authorities (LIA) esterne. L'Identity Provider, infatti, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale, ai sensi dell'Art.1717 del codice civile, di ulteriori soggetti per svolgere una parte delle attività proprie dell'Ufficio di registrazione.

   In particolare le LIA esterne espletano le seguenti funzioni:

   - identificazione certa del Richiedente;
   - raccolta del modulo di adesione compilato e sottoscritto dal Titolare;
   - consegna delle credenziali di autenticazioni SPID;
   - trasmissione all'ufficio dell'Identity Provider preposto alla gestione delle Identità Digitali.
   - Le LIA esterne sono attivate dall'Identity Provider a seguito di un adeguato addestramento del personale indicato dall'Azienda o Ente con il quale viene stipulato un regolare Contratto di Mandato sottoscritto da entrambe le parti. In tale contratto sono esplicitati gli obblighi cui si deve attenere l'Azienda o Ente cui INTESA assegna l'incarico di LIA;

     In particolare l'Azienda/Ente deve:

     I. vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente;

II. impedire ai propri dipendenti la prosecuzione dell'attività di riconoscimento e curare l'immediato ritiro di ogni materiale qualora, per qualsiasi causa, si interrompa il rapporto in essere tra l'Azienda e il dipendente stesso, dandone tempestivamente notizia per iscritto a INTESA;

III. utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il Dlgs. 196/03.

In ogni caso la persona che fa richiesta di emissione dell'Identità Digitale viene identificata con certezza e viene archiviata da INTESA la fotocopia di almeno un documento ufficiale valido per lo Stato di appartenenza. Nel caso di persona giuridica, oltre ad un documento d'identità, verrà inoltre raccolta la visura camerale attestante i poteri di rappresentanza conferiti alla persona fisica che sottoscrive e presenta l'istanza.

Sarà cura degli operatori accertare l'identità del Richiedente tramite la verifica della validità del documento, della presenza su di esso di una fotografia e di una firma autografa, controllando inoltre la validità del codice fiscale.

Gli operatori si riservano la possibilità di non accettare i documenti esibiti nel caso in cui questi risultino carenti delle caratteristiche di cui sopra, sospendendo il processo di iscrizione fino all'esibizione di documenti validi e integri.

E.1.2. Identificazione a vista da remoto

L'identificazione a vista da remoto permette di avviare il processo di rilascio dell'identità digitale anche in quei casi dove, per motivi logistici, non sia possibile ottenere la presenza fisica di entrambe le parti (Richiedente e personale dell'Identity Provider) e quindi procedere con il riconoscimento a vista.

Il servizio di identificazione da remoto sarà gestito come segue:

- Il Richiedente, purché in possesso di un device (PC, tablet, smartphone) abilitato ad una connessione Internet e dotato sia di una webcam che di un sistema audio funzionante, si connette al sito dell'Identity Provider dove sono riportate tutte le istruzioni necessarie per eseguire i passi successivi e dove sono indicati i documenti necessari per l'identificazione.
- Si precisa, a tal proposito, che la buona qualità del collegamento audio-video è fondamentale affinché la procedura di identificazione possa essere effettuata con successo; infatti, in caso di disturbi sulla linea e/o problemi che non rendessero possibile la verifica certa dell'identità del Richiedente, l'operatore dell'Identity Provider interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.
- Il Richiedente compila sul sito dell'Identity Provider un form in cui è previsto vengano inseriti tutti i dati utili all'emissione dell'Identità Digitale.

- Compilato questo form, viene richiesto al Richiedente di prendere visione del Manuale Operativo dell'Identity Provider - lo stesso Manuale Operativo sarà anche agevolmente scaricabile dal sito dell'Identity Provider. Viene chiesto inoltre il consenso al trattamento dei dati personali al fine dell'emissione dell'Identità Digitale.
- Il Richiedente, sempre grazie alle funzionalità esposte sul sito, dovrà inviare all'Identity Provider una copia scannerizzata di un documento di identità (ad esempio carta d'identità, passaporto, tesserino fiscale) in corso di validità.
- Completata la fase di inserimento dati ed invio dei documenti necessari per l'identificazione, sarà cura dell'Identity Provider effettuare le opportune verifiche per accertarne la veridicità, descritte nel par. E.2 "Verifica dell'identità dichiarata".
- Solo quando l'Identity Provider avrà effettuato le verifiche di cui sopra sarà possibile avviare la sessione di videocomunicazione remota, attraverso funzionalità rese disponibili sul proprio sito.
- L'operatore
  a) deve essere libero di rifiutare la registrazione dell'utente, qualora abbia o emerga dubbio, anche soggettivo, circa l'effettiva identità del soggetto richiedente.
  b) chiede all'utente, durante la registrazione, di effettuare azioni estemporanee al fine di accertare la reale presenza nella postazione remota del soggetto richiedente

La sessione audio/video prevede le seguenti attività:

a) acquisizione del consenso alla videoregistrazione e alla sua conservazione per 20 anni come previsto dalla normativa vigente in materia, informando il Richiedente che la conservazione avverrà in modalità protetta;
b) l'operatore dichiara i propri dati identificativi;
c) il soggetto conferma le generalità che vengono contestualmente verificate dall'operatore consultando la documentazione fornita in fase di richiesta di emissione;
d) il soggetto conferma la data e l'ora della registrazione;
e) il soggetto conferma di volersi dotare di un'identità digitale e conferma i dati inseriti nella modulistica online in fase di pre-registrazione;
f) il soggetto conferma il proprio numero di telefonia mobile e l'indirizzo e-mail;
g) l'operatore invia un sms che il soggetto richiedente è tenuto a esporre al dispositivo di ripresa in modo da dimostrare il possesso del dispositivo associato al numero di telefono dichiarato;

h) l'operatore chiede e ottiene conferma dal soggetto 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 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);

j) l'operatore chiede di mostrare la tessera sanitaria su cui è riportato il codice fiscale del soggetto;

k) il soggetto 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'intera sessione viene registrata in modalità audio e video, la sequenza viene poi cifrata e conservata a norma per venti anni. L'Identity Provider provvede alla conservazione della chiave privata, impegnandosi a renderla disponibile ad un perito di parte in caso di contenzioso e/o agli enti di vigilanza che richiedessero un controllo sulle attività svolte.

La registrazione audio/video della sessione deve essere di buona qualità (immagine a colori, definizione delle riprese chiare e a fuoco, adeguata luminosità e contrasto, ripresa del testo eventualmente inquadrato distinguibile. L'intera sessione audio/video deve essere fluente e continua, senza alcuna interruzione.

E.1.3. Identificazione informatica tramite firma elettronica qualificata o firma digitale

Nel caso di identificazione informatica tramite firma elettronica qualificata o firma digitale si procede con l'acquisizione del modulo di richiesta di adesione in formato digitale, messo a disposizione in rete dal gestore dell'identità digitale, compilato e sottoscritto con firma elettronica qualificata o con firma digitale.

A tal fine verrà disposta dall'Identity Provider una sezione dedicata nella pagina di richiesta di adesione, dove il Richiedente avrà la possibilità di caricare il modulo firmato digitalmente.

L'identificazione avviene tramite la verifica della corrispondenza tra i dati presenti all'interno della Firma Elettronica Qualificata o Firma Digitale apposta sulla richiesta e quelli dichiarati nel modulo di richiesta di adesione. Anche questa modalità di identificazione si basa su una presunzione di correttezza relativa al processo di identificazione espletato dal gestore che ha precedentemente rilasciato un certificato di Firma Elettronica Qualificata o Firma Digitale.

Se i dati riscontrati all'interno della firma corrispondono a quelli sottoscritti nel modulo di adesione, l'Identity Provider procederà con le attività necessarie a finalizzare l'emissione dell'identità digitale.

E.2. Verifica dell'identità dichiarata

La verifica dell'identità consiste nel rafforzamento del livello di attendibilità degli attributi di identità, raccolti in fase di identificazione, compiuta attraverso accertamenti effettuati tramite fonti autoritative istituzionali, in grado di dare conferma della veridicità dei dati raccolti.

A tal proposito il Gestore, grazie ad apposita convezione stipulata con l'Agenzia, ha accesso al servizio di verifica del codice fiscale e dei dati anagrafici fornito dall'Agenzia delle Entrate.

Il personale preposto alla verifica dell'identità del Richiedente si connette al servizio di verifica del codice fiscale e dei dati anagrafici fornito dall'Agenzia delle Entrate e confronta le informazioni fornite dal Richiedente con quelle memorizzate negli archivi pubblici.

Al fine di garantire l'opponibilità verso terzi in caso di contenzioso, il Gestore conserva i riscontri ottenuti a seguito degli accessi alle fonti autoritative.

E.3. Emissione dell'identità digitale

Espletate con successo tutte le attività di identificazione e verifica dell'identità del richiedente previste dai processi precedenti, l'identità digitale viene creata e rilasciata dal gestore.

L'identità digitale è costituita da un insieme di attributi:

a) attributi identificativi, come specificato dalla lettera c) del comma 1 dell'articolo 1 del DPCM;
b) attributi secondari, come specificato dalla lettera d) del comma 1 dell'articolo 1 del DPCM ;
c) codice identificativo, come specificato dalla lettera d) del comma 1 dell'articolo 1 del DPCM ;
d) identificativo Utente;

Il codice identificativo è assegnato dal gestore dell'identità digitale, deve essere univoco in ambito SPID.

Tale codice identificativo è definito dalla seguente regola:

<codice Identificativo> = <cod_IdP><numero unico>

Dove:

e) *<cod_IdP>*: è un codice composto da 4 lettere che identifica l'Identity Provider;

f) *<numero unico>*: è un codice alfanumerico composto da 10 caratteri univoco nel dominio del gestore.

E.4. Creazione delle credenziali

Il processo di creazione delle credenziali comprende le attività necessarie a dare origine ad una credenziale o ai mezzi per la sua produzione, con metodologie differenti a seconda del livello di sicurezza a cui si pone la credenziale.

E.4.1. Livello 1 SPID

Per il livello 1 SPID (corrispondente al LoA2 dell'ISO-IEC 29115) l'Identity Provider fornirà al Richiedente una credenziale a singolo fattore costituita da una password.

In particolare, per garantire di ottenere password complesse e difficilmente attaccabili, verranno imposti i seguenti vincoli:

a) lunghezza minima di 8 caratteri;

b) lunghezza massima di 16 caratteri;

c) inclusione di almeno un carattere minuscolo e uno maiuscolo;

d) inclusione di almeno un carattere numerico;

e) inclusione di almeno un carattere speciali ad es #, $,% ecc.

f) impossibilità di inclusione di più di due caratteri identici consecutivi.

g) divieto di utilizzo di formati comuni (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.).

Le password devono inoltre avere una durata massima non superiore a 180 giorni e non possono essere riusate, o avere elementi di similitudine, prima di cinque variazioni e comunque non prima di 15 mesi. L'Identity Provider adotta una procedura di sollecito con la quale invita l'utente a modificare periodicamente la password.

E.4.2. Livello 2 SPID

Per il livello 2 SPID (corrispondente al LoA3 dell'ISO-IEC 29115) l'Identity Provider fornirà al Richiedente una credenziale a singolo fattore costituita da una password abbinata all'adozione di una OTP inviata via e-mail.

Per la creazione della credenziale OTP, il Gestore utilizza la tecnologia messa a disposizione dal sistema PkBox in ambito di Strong Authentication. Il processo prevede che venga generato il seed segreto di derivazione del token, dal quale poi viene di volta in volta calcolato il codice OTP secondo le logiche di generazione proprie del dispositivo adottato.

Per creare la credenziale di secondo livello, il seed viene generato utilizzando una chiave base che viene salvata su HSM ed una chiave di derivazione che è specifica del singolo token OTP ed è ottenuta tramite hashing di quantità che caratterizzano il token stesso.

Queste due chiavi sono soggette ad un processo di derivazione e decimalizzazione mediante algoritmi standard per la generazione di una quantità (il segreto) che è utilizzata per la generazione degli otp e/o la verifica della loro validità.

E.4.3. Livello 3 SPID

Non gestito dal Gestore.

E.5. Consegna delle credenziali

La complessità del processo dipende dal livello di sicurezza di autenticazione informatica SPID associato alla determinata credenziale. La consegna delle credenziali deve essere operata con modalità e strumenti che assicurino che la stessa sia effettuata al legittimo destinatario con adeguati criteri di riservatezza che salvaguardino il contenuto.

In qualunque caso, all'atto della consegna delle credenziali, il gestore dell'identità digitale garantisce:

a) che il Richiedente, attraverso una specifica informativa rilasciata in fase di emissione dell'Identità Digitale, sia espressamente informato in modo compiuto e chiaro riguardo:
   - agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza delle credenziali;
   - sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi;

b) la rispondenza del proprio sistema di sicurezza dei dati alle misure di sicurezza per il trattamento dei dati personali, secondo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196.

E.5.1. Livello 1 SPID

Per il livello 1 SPID, che si ricorda essere composto da una credenziale a singolo fattore (password), dal momento che in fase di richiesta di emissione dell'Identità Digitale è a carico del Richiedente la scelta della password da adottare come credenziale di accesso SPID, il processo di consegna della credenziale si considera automaticamente concluso al termine del processo di emissione dell'Identità Digitale.

E.5.2. Livello 2 SPID

Per il livello 2 SPID, essendo costituito da una password e da un OTP, il processo di consegna delle credenziali si divide in due modalità:

a) Per quanto riguarda la password, il processo di consegna è analogo a quello del livello 1.

b) L'OTP inviato su un indirizzo di posta elettronica non prevede invece la consegna della credenziale al momento del termine del processo di emissione dell'Identità Digitale. Tale momento viene invece prorogato all'istante di'utilizzo della credenziale per l'accesso ad un servizio offerto da un Service Provider, dove il gestore dell'identità digitale provvederà ad inviare via e-mail l'OTP da spendere per la sessione corrente. La sicurezza della credenziale si basa sulla presunzione del possesso dell'indirizzo di posta verificato in fase di emissione dell'Identità Digitale;

E.5.3. Livello 3 SPID

Non gestito dal Gestore.

E.6. Attivazione delle credenziali

L'attivazione delle credenziali è il processo durante il quale le credenziali o i mezzi usati per produrle, sono rese effettivamente operative e pronte all'utilizzo.

E.6.1. Livello 1 SPID

Come per la consegna, le credenziali di livello 1 SPID per natura non prevedono una fase di attivazione in quanto si possono considerare già attive al momento del primo rilascio. Si considera inoltre che anche in seguito ad una sospensione le credenziali si intendono automaticamente attivate.

E.6.2. Livello 2 SPID

Per le credenziali di livello 2 SPID, la parte della credenziale composta dalla password è soggetta alle stesse condizioni del livello 1. Per quanto riguarda la OTP le fasi di prima attivazione e riattivazione in seguito a sospensione non sono previste data la volatilità della credenziale, che per definizione è valevole solo per la sessione in corso, per cui è da considerarsi già attivata nel momento in cui viene spedita via e-mail al all'indirizzo di posta elettronica del Richiedente.

E.6.3. Livello 3 SPID

Non gestito dal Gestore.

E.7. Conservazione e registrazione dei documenti

Il processo di registrazione dei documenti completa la fase di rilascio di un'identità SPID a un soggetto. La documentazione da conservare include le informazioni e i documenti che sono stati raccolti nel corso dell'attività di registrazione.

L'Identity Provider, al fine di poter documentare la corretta esecuzione dei precedenti processi relativi all'attività di rilascio di un'identità, conserva i riscontri relativi ai processi di identificazione e verifica.

In merito al processo di richiesta e identificazione del Richiedente devono essere conservati:

1. nel caso di identificazione tramite esibizione a vista:
    - identificazione "de visu": copia per immagine di tutta la documentazione esibita (documento d'identità e codice fiscale per persone fisiche, procura per persone giuridiche) e modulo di richiesta su supporto cartaceo sottoscritto in modalità autografa;

- identificazione remota con strumenti audio/video: i dati di registrazione, nonché l'esplicita volontà del soggetto di dotarsi di identità digitale memorizzati in file audio/video, immagini e metadati strutturati in formato elettronico;

2. nel caso di firma elettronica qualificata o digitale:
   - modulo di richiesta di adesione allo SPID in formato digitale sottoscritto digitalmente;
   - tutti i documenti e dati utilizzati per l'associazione e la verifica degli attributi.

In merito al processo di verifica devono essere conservati i riscontri ottenuti a seguito degli accessi alle fonti autoritative.

Tutte le informazioni e la documentazione descritta nei paragrafi precedenti viene conservata a norma per 20 (venti) anni:

1. Nel caso di documentazione cartacea la conservazione avviene in casseforti poste in ambiente protetto, nel rispetto della normativa vigente;
2. Nel caso di informazioni rappresentate in formato digitale, queste vengono inserite all'interno di un archivio informatico, il quale viene firmato con una chiave pubblica dell'Identity Provider e conservato secondo le normative vigenti.
   L'Identity Provider si impegna a conservare la relativa chiave privata e a metterla a disposizione in caso di contenzioso.

E.8. Segnalazioni sull'utilizzo delle credenziali

Il gestore dell'identità digitale, su richiesta dell'utente, segnala via e-mail alla casella di posta indicata dall'utente, ogni avvenuto utilizzo delle credenziali di accesso.

F. Revoca e sospensione dell'Identità Digitale

La revoca è il processo che annulla definitivamente la validità delle credenziali. Diversamente, la sospensione è associata ad un processo di annullamento temporaneo.

La revoca è disposta nei seguenti casi:

1) smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria);
2) utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto;
3) emissione di una nuova credenziale in sostituzione di una già in possesso dell'utente;
4) emissione di una nuova credenziale in sostituzione di una scaduta.

Nel caso previsto dal punto 1), l'utente deve effettuare immediata richiesta di sospensione delle credenziali. Se la richiesta dell'utente non viene effettuata tramite posta elettronica certificata, o sottoscritta con firma digitale o firma elettronica qualificata, il Gestore verifica, anche attraverso uno o più attributi secondari, la provenienza della richiesta di sospensione da parte del soggetto utente.

Il Gestore sospende tempestivamente l'identità digitale per un periodo massimo di trenta giorni informandone il richiedente. Durante questo periodo può accadere che:

a) il richiedente annulla la richiesta di sospensione (ad es. per ritrovamento) e quindi l'identità digitale viene ripristinata;
b) il richiedente formalizza la richiesta presentando copia della denuncia presentata all'autorità giudiziaria, quindi l'identità digitale viene revocata.

In assenza di quanto indicato nelle lettere a) o b), l'identità digitale sarà automaticamente ripristinata scaduto il periodo di 30 giorni dalla data della richiesta.

Nel caso previsto dal numero 2, anche a seguito di segnalazioni ai sensi dell' articolo 8, comma 4 del DPCM, l'utente richiede la sospensione immediata dell'identità digitale al gestore del servizio.

F.1. Modalità di revoca o sospensione dell'identità digitale

Ai sensi dell'articolo 8, comma 3, e dell'articolo 9 del DPCM, il Gestore revoca l'identità digitale nei casi seguenti:

1) risulta non attiva per un periodo superiore a 24 mesi;
2) per decesso della persona fisica;
3) per estinzione della persona giuridica;

4) per uso illecito dell'identità digitale;
5) per richiesta dell' utente;
6) per scadenza contrattuale.

Nel caso previsto dai punti 1 e 6, il Gestore revoca di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca all'utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).

Nei casi previsti dai punti 2 e 3, il Gestore procede alla revoca dell'identità digitale, previo accertamento operato anche utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM. In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del soggetto utente (eredi o procuratore, amministrazione, società subentrante) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'identità digitale. Il gestore, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.

Nel caso previsto dal punto 4, cioè nel caso in cui l'utente ritenga che la propria identità digitale sia stata utilizzata fraudolentemente, lo stesso può chiederne la sospensione con una delle seguenti modalità:

a) richiesta al gestore inviata via PEC;
b) richiesta, in formato elettronico e sottoscritta con firma digitale o elettronica, inviata tramite la casella di posta appositamente predisposta dal gestore.

Il gestore deve fornire esplicita evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.

Trascorsi trenta giorni dalla suddetta sospensione, il Gestore provvede al ripristino dell'identità precedentemente sospesa qualora non riceva copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione. In caso contrario l'identità digitale viene ripristinata.

Nel caso previsto dal punto 5, l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione o la revoca della propria identità digitale seguendo modalità analoghe a quelle previste dal precedente punto 4, ovvero attraverso:

a) richiesta al gestore inviata via PEC;
b) richiesta inviata tramite la casella di posta nota al gestore in formato elettronico e sottoscritta con firma digitale o elettronica.

Nel caso di richiesta di sospensione, trascorsi trenta giorni dalla suddetta sospensione, il Gestore provvede al ripristino dell'identità precedentemente sospesa qualora non pervenga con le modalità sopra indicate una richiesta di revoca.

La revoca di una identità digitale comporta conseguentemente la revoca delle relative credenziali.

Il Gestore conserva la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'Identità Digitale.

Appendice A – Codici e formati dei messaggi di anomalia

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario Notifica	Scheramta IDP	Troubleshooting utente	Troubleshooting sp
n.a	Autenticazione Corretta	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)	-	-	-
				Anomalie servizio				
100	Errore Sistema	HTTP Post/Http Redirect	HTTP 500	-	Utente	Schermata con messaggio di errore	Si prega di ritentare a connettersi al servizio in un secondo momento	-
				Anomalie binding SAML				
200	Formato Binding non corretto	HTTP Post/Http Redirect	HTTP 403	-	Utente	Schermata con messaggio di errore	Si prega di contattare il fornitore del servizio	Verificare la corretta composizione della richiesta SAML
325	Verifica della firma fallita	HTTP Post/Http Redirect	HTTP 403	-	Utente	Schermata con messaggio di errore	Si prega di contattare il fornitore del servizio	Verificare firma richiesta
				Anomalie sul formato della richiesta SAML (AuthnRequest)				
300	Identificatore richiesta (ID) non presente, malformato o non conforme	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester Code 300	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
301	Parametro version non presente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch Code 301	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
302	Parametro version specificato con valore diverso da 2.0	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch Code 302	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
303	IssueInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied Code 303	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
304	Destination non presente, malformata o non coincidente con il Gestore delle identità ricevente della richiesta	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 304	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
305	AssertionConsumerServiceIndex o AssertionConsumerServiceURL contemporaneamente specificati	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 305	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
306	AssertionConsumerServiceURL e ProtocolBinding nulli o non corretti	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 306	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
307	ProtocolBinding non corretto	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 307	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
308	Assertion consumerServiceIndex non si riferice ad un indice dei metadati	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 308	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente

309	AttributeConsumerServiceIndex malformato o che riferisce a un valore non presente nei metadati SP	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 309	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
310	Attributo isPassive presente e attualizzato al valore true	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive Code 310	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
311	Subject malformato: attributo format non presente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal Code 311	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
312	Subject malformato: attributo NameQualfier non presente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal Code 312	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
313	Subject malformato: campo NameId non presente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal Code 313	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
314	NameIDPolicy assente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 314	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
315	Attributo format del campo NameIDPolicy errato	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:statusRequester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 315	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
316	Attributo format del campo NameIDPolicy assente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 316	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
317	Parametro Issuer non presente	HTTP Post/Http Redirect	HTTP 403	n.a.	Utente	Schermata con messaggio di errore	Si prega di contattare il fornitore del servizio	Richiesta non formulata correttamente
318	Parametro Issuer con campo Format non presente o errato	HTTP Post/Http Redirect	HTTP 403	n.a.	Utente	Schermata con messaggio di errore	Si prega di contattare il fornitore del servizio	Richiesta non formulata correttamente
319	Parametro Issuer con campo Name qualifier non presente	HTTP Post/Http Redirect	HTTP 403	n.a.	Utente	Schermata con messaggio di errore	Si prega di contattare il fornitore del servizio	Richiesta non formulata correttamente
320	Conditions presente ma con NotBefore o NotOnOrAfter nulli	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 320	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
321	Conditions presente ma conUte NotBefore o NotOnOrAfter nel passato	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported Code 321	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
322	RequestAuthnContext non presente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext Code 322	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
323	RequestAuthnContext con attributo Comparison non presente	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext Code 323	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
324	RequestAuthnContext con attributo AuthnContextClassRefs non SPID	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext Code 324	Fornitore del servizio (SP)	-	-	Richiesta non formulata correttamente
325	Signature presente e non valida	HTTP Post/Http Redirect	HTTP 403	n.a.	Utente	Schermata con messaggio di errore	Si prega di contattare il fornitore del servizio	Richiesta non formulata correttamente

Anomalie operatività utente								
400	Autenticazione fallita per ripetuta sottomissione di credenziali errate	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed Code 400	Fornitore del servizio (SP)	Schermata con messaggio di errore	Verificare le credenziali inserite	Mostrare una pagina che indica all'utente il problema sollevato
401	Utente privo di credenziali compatibili con il livello richiesto dal fornitore del servizio	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed Code 401	Fornitore del servizio (SP)	-	Non si dispone di credenziali di livello sufficente per accedere al servizio	Mostrare una pagina che indica all'utente il problema sollevato
402	Utente con identità sospesa/revocata o con credenziali bloccate	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed Code 402	Fornitore del servizio (SP)	-	Identità sospesa o revocata	Mostrare una pagina che indica all'utente il problema sollevato
403	Errore generico di autenticazione	HTTP Post/Http Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed Code 403	Fornitore del servizio (SP)	Messaggio di errore	-	Mostrare una pagina che indica all'utente il problema sollevato