

MANUALE OPERATIVO SPIDITALIA

Sistema Pubblico di Identità Digitale



SpidItalia
REGISTER.IT

Codice documento: REGIT-SPID-MO

Versione: 1.0

Data: 01/05/2019

Indice del Manuale Operativo

Indice del Manuale Operativo.....	2
1 Dati identificativi del Gestore Register SpA.....	5
1.1 Sistemi di qualità	5
2 Dati identificativi del Manuale	6
2.1 Scopo del documento.....	6
2.2 Riferimenti normativi per la verifica dei contenuti.....	6
2.3 Altri riferimenti.....	7
2.4 Standard tecnici.....	8
2.5 Definizioni abbreviazioni e termini tecnici.....	8
2.5.1 Attori del Sistema Pubblico per l'Identità Digitale.....	9
2.5.2 Altre definizioni	9
2.5.3 Acronimi/Abbreviazioni	11
2.6 Organizzazione del personale	12
3 Struttura e storia del Manuale Operativo	13
3.1 Reperibilità del Manuale Operativo	13
3.2 Versione e storia del Manuale Operativo	13
3.3 Convenzioni utilizzate.....	13
3.4 Tabella di corrispondenza Normativa – Manuale Operativo	14
3.5 Procedure per l'aggiornamento del Manuale Operativo.....	15
3.5.1 Responsabile del Manuale Operativo.....	15
3.5.2 Revisione del Manuale Operativo ed approvazione delle modifiche.....	15
4 Caratteristiche del servizio SpidItalia	16
4.1 Caratteristiche generali del servizio	16
4.2 Livelli di sicurezza	17
4.3 Descrizione delle componenti applicative	18
4.3.1 Applicazioni di Front End	19
4.3.1.1 Login.....	19
4.3.1.2 Registrazione	19
4.3.1.3 Selfcare	19

4.3.1.4	Backoffice.....	20
4.3.2	Applicazioni di Back End.....	20
4.3.2.1	Gestione Utenti.....	20
4.3.2.2	Gestione Documenti.....	20
4.4	Strumenti di autenticazione.....	21
4.4.1	Metodo di autenticazione di primo livello.....	21
4.4.2	Metodo di autenticazione di secondo livello.....	22
4.4.3	Metodo di autenticazione di terzo livello (ancora non implementato e non utilizzato dai SP)	22
4.5	Messaggi di anomalia.....	23
5	Modalità di identificazione e di rilascio delle credenziali.....	24
5.1	Identificazione del Richiedente ed attivazione del servizio.....	25
5.2	Rilascio delle credenziali.....	27
5.3	Attributi qualificati.....	27
5.4	Conservazione delle evidenze.....	27
6	Gestione del ciclo di vita dell'ID.....	29
6.1	Gestione attributi.....	29
6.2	Sospensione dell'Identità Digitale.....	29
6.2.1	Sospensione volontaria da parte del Titolare.....	29
6.2.2	Sospensione da parte dell'IdP.....	30
6.3	Revoca dell'Identità Digitale.....	30
6.3.1	Richiesta di revoca da parte del Titolare.....	30
6.3.2	Revoca da parte dell'IdP.....	31
6.4	Richiesta di assistenza (canali e tempistiche).....	32
7	Livelli di servizio.....	33
8	Procedure e standard tecnologici e di sicurezza.....	35
8.1	Conservazione delle evidenze per il rilascio delle Identità Digitale.....	35
8.2	Tracciatura degli accessi al servizio (log eventi).....	36
8.3	Richiesta del log certificato.....	36
8.4	Misure anticontraffazione.....	37

8.5	Sistema di monitoraggio	37
9	Indicazione delle condizioni di fornitura	39
9.1	Obblighi e responsabilità del Gestore per l'erogazione del servizio SpidItalia	39
9.2	Obblighi del Titolare dell'Identità Digitale	43
9.3	Obblighi del Richiedente	44
9.4	Clausola risolutiva espressa.....	44
9.5	Polizza assicurativa	44
9.6	Protezione dei dati personali	44
	Allegato A – SPID-Tabella messaggi di anomalia	45

Indice delle Figure

Figura 1	– Schema di funzionamento del Sistema Pubblico per l'Identità Digitale	16
Figura 2	– Architettura logico-applicativa IdP.....	18
Figura 3	– Schema di funzionamento del Sistema Pubblico per l'Identità Digitale	24

Indice delle Tabelle

Tabella 1	– Dati Gestore.....	5
Tabella 2	– Versione del Manuale e storia delle modifiche.....	13
Tabella 3	– Manuale Operativo con riferimento al Regolamento di accreditamento.....	14
Tabella 4	– Livelli di servizio per registrazione, ciclo di vita ed autenticazione SpidItalia.....	33
Tabella 5	– Livelli di servizio di continuità operativa	34

1 Dati identificativi del Gestore Register SpA

Register SpA è Gestore dell'Identità Digitale in funzione del quale rilascia, previa verifica dell'identità ed in modalità sicura le credenziali di accesso al soggetto Utente Titolare e Richiedente, operando in conformità al DPCM, alle Regole Tecniche e secondo quanto prescritto dal CAD.

In questo documento si usa il termine Identity Provider, o per brevità "IdP", per indicare Register SpA.

Register SpA (nel seguito anche "Register" o "la Società") è leader storico in Italia nella fornitura di servizi di registrazione di domini, hosting, protezione del brand e pubblicità in rete e si pone altresì sul mercato quale "Gestore di Posta Elettronica Certificata" (nel seguito, per semplicità, anche indicato con l'acronimo "PEC"), regolarmente iscritto all'elenco pubblico dei gestori PEC coordinato dall'Agenzia per l'Italia Digitale.

Ragione sociale:	Register SpA
Legale rappresentante	Claudio Corbetta
Sede legale:	Firenze, Viale della Giovine Italia, 17
Sedi operative:	<ul style="list-style-type: none"> • Firenze, Viale della Giovine Italia, 17 • Bergamo, Via Zanchi 22
Data Center:	c/o BT Italia S.p.A., I.NET Building, Via Darwin 85, Settimo Milanese (MI)
Partita IVA:	04628270482
Iscrizione Registro Delle Imprese:	04628270482
REA:	FI-467460
Capitale sociale:	€ 5.108.619,32
Sito Web:	www.register.it
PEC gestore IdP:	gestoreidp@pec.register.it

Tabella 1 – Dati Gestore

1.1 Sistemi di qualità

ISO9001:2015 - Progettazione, Sviluppo e Conduzione di servizi di posta elettronica certificata (PEC)

ISO27001:2013 - Progettazione, sviluppo e conduzione di servizi di Posta elettronica certificata (PEC).
Progettazione, sviluppo di servizi e di identificazione e autenticazione digitale.

2 Dati identificativi del Manuale

2.1 Scopo del documento

Il presente documento costituisce il **Manuale Operativo** del servizio SPID (nel seguito, per brevità, anche indicato come “Manuale”) del Gestore Register richiesto dal 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”*, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014.

Scopo del presente Manuale è fornire in maniera esaustiva regole, caratteristiche e procedure adottate da Register nella conduzione del servizio di Identità Digitale (nel seguito, per brevità, anche indicato come “ID”) aderente al Sistema Pubblico per la gestione dell’Identità Digitale (per brevità SPID).

Il presente Manuale Operativo è conforme alla normativa vigente alla data di sua emissione, in particolare a quanto predisposto dal DPCM 24 ottobre 2014 ed alla regolamentazione emanata da AgID in attuazione dell’art.4 del sopra citato DPCM.

Oltre alle informazioni di carattere generale, tale Manuale contiene tutte le indicazioni necessarie alla spiegazione dell’offerta del servizio di ID erogato da Register in qualità di IdP.

Al fine di un corretto utilizzo del servizio, Register raccomanda all’Utente una attenta lettura del presente Manuale.

Il diritto di autore sul presente documento è di Register SpA ed è riservato ogni diritto ed utilizzo.

2.2 Riferimenti normativi per la verifica dei contenuti

Il servizio di Identità Digitale erogato da Register e il presente Manuale Operativo sono stati sviluppati in ottemperanza alla vigente normativa, specifica in materia, e ad altre normative cogenti. Di seguito si riporta l’elenco delle normative prese in considerazione.

- [1] Decreto Legislativo, 7 marzo 2005 n. 82 – *“Codice dell’Amministrazione Digitale”* (di seguito anche “CAD”) e successive modifiche e integrazioni;
- [2] 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 (pubblicato in Gazzetta Ufficiale Serie Generale n.285 del 9-12-2014)* (di seguito anche “DPCM”);
- [3] Decreto Legislativo 30 giugno 2003, n. 196 – *“Codice in materia di protezione dei dati personali”* e successive modificazioni e integrazioni.
- [4] Regolamento AgID per l’accreditamento – *“Modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM del 24 ottobre 2014)”*.
- [5] Regolamento AgID recante *“le regole tecniche (articolo 4, comma 2, DPCM del 24 ottobre 2014)”*
- [6] Regolamento AgID recante *“le modalità per l’accreditamento e la vigilanza dei gestori dell’identità digitale (articolo 1, comma 1, lettera l), DPCM del 24 ottobre 2014”*

- [7] 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 pubblicato in Gazzetta ufficiale dell'Unione europea serie L257 del 28 agosto 2014.
- [8] Determinazione n.44 del 28 luglio 2015 *“Emanazione dei regolamenti SPID previsti dall’art.4, commi 2,3 e 4 del DPCM 24 ottobre 2014”*.
- [9] Regolamento AgID recante le procedure per consentire ai gestori dell’identità digitale, tramite l’utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell’identità digitale ai sensi del DPCM 24 Ottobre 2014;
- [10] Provvedimento Garante Privacy, 17 gennaio 2008 – *“Sicurezza dei dati di traffico telefonico e telematico”* e successive modificazioni ed integrazioni.
- [11] Provvedimento Garante Privacy, 27 novembre 2008 – *“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”*.

L’elenco è da considerarsi non esaustivo; si è fatto ad ogni modo riferimento a quanto pubblicato sul sito dell’Agenzia per l’Italia Digitale, con aggiornamento alla data di redazione del presente Manuale.

2.3 Altri riferimenti

REGIT-SPID-GU	Guida Utente SpidItalia
REGIT-SPIT-MO	Manuale Operativo
	Carta dei Servizi
REGIT-SPID-GuidaSicurezzaID	Guida alla sicurezza per l’utilizzo dell’Identità Digitale SpidItalia
	Informativa privacy

Altri riferimenti

2.4 Standard tecnici

FIPS 140-2	FIPS PUB 140-2 Security requirements for cryptographic modules
ISO-IEC 18014	Time-stamping
ISO-IEC 19790:2012	Security requirements for cryptographic modules
ISO-IEC 24760-1	A framework for identity management -- Part 1: Terminology and concept
ISO-IEC 27001	Information security management
ISO-IEC 29003	Identity proofing
ISO-IEC 29100	Basic privacy requirements
ISO-IEC 29115:2013	Entity authentication assurance framework
ITU-T X.1254	Entity Authentication Framework
ITU-T Rec. X.1252 (2010)	Baseline identity management terms and definitions
SPID-TabAttr	Tabella Attributi (http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_attributi_idp.pdf)
SPID-TabErr	Tabella Codici di Errore (http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_codici_Errore.pdf)

Standard tecnici

2.5 Definizioni abbreviazioni e termini tecnici

Al fine di facilitare la comprensione del presente Manuale Operativo e consentirne una corretta interpretazione, in questa sezione vengono definiti termini e acronimi usati comunemente in materia.

2.5.1 Attori del Sistema Pubblico per l'Identità Digitale

Termine	Definizione
AgID (Agenzia per l'Italia Digitale)	Ente Nazionale per la Digitalizzazione della Pubblica Amministrazione
Identity Provider (IdP) o Gestore	Gestore dell'Identità Digitale, ossia persona giuridica accreditata allo SPID che, in qualità di gestore di servizio pubblico, fornisce il servizio di identità digitale. Nel presente documento il termine è utilizzato per identificare Register SpA.
Fornitore di servizi o Service Provider (SP)	Definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, sono soggetti pubblici o privati che erogano servizi 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.
Gestore degli attributi qualificati o Attribute Authority (AA)	Soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
Utente o Titolare	Soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SpidItalia, corrisponde all'Utente del DPCM art. 1 comma 1 lettera v).

2.5.2 Altre definizioni

Termine	Definizione
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	Qualifiche, abilitazioni professionali, poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.

Autenticazione informatica	Verifica effettuata dal gestore dell'identità digitale, su richiesta del fornitore di servizi, della validità delle credenziali di accesso presentate dall'Utente allo stesso gestore, al fine di convalidarne l'identificazione informatica.
Cookie o Cookie-id	Identificativo univoco di una sessione di accesso ad una risorsa.
Credenziali di accesso o Credenziali SpidItalia	Attributi di cui l'Utente si avvale, per accedere in modo sicuro, tramite autenticazione informatica, ai servizi erogati in rete dai SP aderenti allo SPID.
Firma elettronica	Ctf. CAD
Firma digitale	Cfr. CAD
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 secondo quanto richiesto dal DPCM.
Intestatario della fattura	Persona fisica o giuridica a cui è intestata la fattura relativa al servizio di emissione dell'identità digitale. Può coincidere con l'Utente Titolare o con il Richiedente.
Manuale Operativo	Documento che definisce le procedure che l'IdP applica nello svolgimento del servizio.
Registrazione	L'insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione previsti dal presente decreto e dai suoi regolamenti attuativi, è attribuita un'identità digitale a un Utente, previa raccolta, verifica e certificazione degli attributi da parte del gestore dell'identità digitale, garantendo l'assegnazione e la consegna delle credenziali di accesso prescelte in modalità sicura.
Richiedente	Persona fisica o giuridica che richiede una o più identità SpidItalia da attribuire ai Titolari. Può coincidere con l'Utente Titolare o con l'intestatario della fattura.
Sistema Pubblico per la gestione dell'identità digitale di cittadini ed imprese	Sistema di cui all'rt. 64 del CAD.
Tempo universale coordinato	Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5

Webcam	Videocamera di dimensioni ridotte destinata a trasmettere immagini in streaming via internet e catturare immagini fotografiche. Collegata a pc o integrata può essere utilizzata per chat video o videoconferenze.
--------	--

2.5.3 Acronimi/Abbreviazioni

Acronimo/abbreviazione	Definizione
AgID	Agenzia per l'Italia Digitale
IdP	Identity Provider (il gestore delle identità digitali in ambito SPID)
IETF	Internet Engineering Task Force
ID	Identità Digitale
IdP	Identity Provider
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LoA	Level of Assurance
OTP	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione
PIN	Personally Identifiable Number
SLA	Service Level Agreement (Livelli di Servizio Garantiti)
SSL	Secure Socket Layer
SSO	Single Sign-on, identificazione unica
SP	Service provider – vedi Fornitore Servizi
SPID	Il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98

2.6 Organizzazione del personale

Al fine di rispondere in modo efficace alle specifiche esigenze che AgID richiede, è stata costituita una struttura organizzativa interna con il compito di gestire e monitorare gli aspetti previsti dalla normativa:

- Responsabile del Servizio;
- Responsabile della Sicurezza;
- Conduzione tecnica dei sistemi (Servizi Tecnici);
- Verifica e Ispezioni Interne;
- Sicurezza;
- Verifica dell'identità del Titolare, della gestione e conduzione del servizio;
- Formazione dei soggetti coinvolti nella conduzione e gestione del servizio;
- Rapporti e documentazione presso AgID;
- Referente per la protezione dei dati personali.

A presidio di ciascuna delle funzioni identificate, in accordo a quanto richiesto dalla normativa di riferimento, Register ha identificato specifici soggetti responsabili. Tali responsabili, per lo svolgimento delle funzioni di loro competenza, possono avvalersi di addetti ed operatori dipendenti di Register ed, in casi di emergenza, anche di personale del fornitore BT Italia S.p.A. appositamente incaricato¹.

¹ BT Italia S.p.A: è fornitore per Register del servizio di connettività e housing dell'architettura del servizio IdP. Per servizio di housing si intende un servizio che prevede la concessione in locazione di uno spazio fisico dedicato esclusivamente agli apparati Register all'interno di un data center, ove sono collocati i rack, accessibili ai soli operatori di Register o, in casi straordinari definiti e autorizzati da Register stessa, al personale del fornitore. Register ha la gestione diretta del servizio IdP ed il controllo delle sue varie fasi e degli apparati tecnologici che forniscono il servizio stesso ed è l'unico soggetto in grado di accedere ai dati ed alle informazioni relative al servizio contenute negli apparati collocati presso la sede di BT Italia. Il rapporto tra Register e BT Italia è disciplinato da un contratto che garantisce i livelli di servizio ed il controllo di Register sui singoli servizi forniti da BT Italia. Register provvede alla gestione e soluzione di eventuali guasti o malfunzionamenti attraverso il proprio personale. In caso di necessità, Register può avvalersi del personale incaricato di BT Italia per effettuare operazioni fisiche sui server quali ad esempio sostituzione di parti guaste ed interventi di ripristino di emergenza; tali interventi sono garantiti da BT Italia S.p.A. a Register dal servizio di assistenza "Eyes&hands", che prevede l'intervento di un tecnico nel Data Center su richiesta esplicita di Register, entro due ore dalla richiesta stessa al fine di velocizzare eventuali interventi di ripristino. I singoli servizi forniti da BT Italia, inclusi gli interventi di assistenza, sono controllati da Register. Tutti gli accessi ai rack sono controllati tramite badge identificativi, rilasciati e gestiti da Register.

3 Struttura e storia del Manuale Operativo

3.1 Reperibilità del Manuale Operativo

Il presente Manuale è un documento *pubblico*, secondo le disposizioni del DPCM 24 ottobre 2014 ed ai Regolamenti attuativi emanati da AgID in attuazione dell’art.4 del DPCM.

Scritto da Register, ha il fine di costituire garanzia di affidabilità del servizio di erogazione di ID nei confronti degli utilizzatori finali ed è accessibile e scaricabile dal sito di Register nella sezione dedicata al servizio Spid: <https://www.register.it/spid>

La versione del Manuale Operativo, resa disponibile e pubblicata all’indirizzo citato, è l’ultima rilasciata e approvata dalla Società.

3.2 Versione e storia del Manuale Operativo

La versione corrente del Manuale Operativo è esclusivamente la versione in formato elettronico disponibile agli indirizzi citati [si veda il paragrafo 3.1 del presente Manuale].

Versione	Data versione	Paragrafo	Note sui cambiamenti
1.0	01/05/2019	N.A.	Prima versione del documento

Tabella 2 – Versione del Manuale e storia delle modifiche

3.3 Convenzioni utilizzate

Si riportano di seguito le diciture e le convenzioni lessicali e tecniche correntemente utilizzate nel presente Manuale, fornendone relativa connotazione interpretativa.

Quando viene utilizzata la dicitura “*deve*”, “*occorre*”, “*è necessario*” (ed altre varianti di egual e paritario valore) è sotto intesa l’obbligatorietà di quanto riportato; l’oggetto della frase è condizione *sine qua non* per la corretta interpretazione della valenza di quanto riportato o il corretto funzionamento di quanto specificato.

Quando viene utilizzata la dicitura “*è consigliato*”, “*è opportuno*” (ed altre varianti di egual e paritario valore) si fa rimando all’interpretazione del lettore in merito alla valenza di quanto riportato o al corretto funzionamento di quanto specificato.

Con il termine “Manuale Operativo” si fa sempre riferimento alla versione corrente del Manuale Operativo [si veda il paragrafo 3.2 del presente Manuale].

3.4 Tabella di corrispondenza Normativa – Manuale Operativo

Contenuto Regolamento accreditamento	Paragrafo
Dati identificativi del Gestore	1
Dati identificativi della versione del manuale	3.2
Responsabile del manuale Operativo	3.5.1
Descrizione architetture adottate per i sistemi run-time	4.3
Descrizione architetture dei sistemi di autenticazione e delle credenziali	4.4
Descrizione dei codici e dei formati dei messaggi di anomalia sia relativi ai protocolli che ai dispositivi di autenticazione	4.5
Livelli di servizio garantiti per le diverse fasi della registrazione e della gestione del ciclo di vita delle identità	7
Livelli di servizio garantiti per le diverse fasi del processo di autenticazione	7
Descrizione contenuti dei tracciamenti accessi al servizio autenticazione e modalità di acquisizione ai fini dell'opponibilità a terzi	8.1 - 8.2
Guida Utente	<i>Guida Utente SpidItalia</i>
Descrizione processi e procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali	5
Descrizione metodi di gestione dei rapporti con gli utenti	6.4
Descrizione generale delle misure anti-contraffazione	8.4
Descrizione generale sistema di monitoraggio	8.5
Descrizione obblighi del gestore e dei titolari dell'identità digitale	9.1
Indirizzo/i del/dei sito/i web del gestore ove viene resa disponibile la descrizione del servizio in lingua italiana ed in lingua inglese	1
Descrizione modalità disponibili agli utenti per la revoca e sospensione dell'identità digitale.	6.2 e 6.3

Tabella 3 – Manuale Operativo con riferimento al Regolamento di accreditamento

3.5 Procedure per l'aggiornamento del Manuale Operativo

3.5.1 Responsabile del Manuale Operativo

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

Domande, osservazioni e richieste di chiarimento in ordine al presente manuale dovranno essere rivolte all'indirizzo ed alla persona sotto indicata:

Responsabile del Manuale Operativo	
Nome	Ruben
Cognome	Pandolfi
Email	gestoreidp@pec.register.it
Call Center	035 630 5561

Dati identificativi del Responsabile del Manuale Operativo

3.5.2 Revisione del Manuale Operativo ed approvazione delle modifiche

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

Ogni nuova versione annulla e sostituisce le precedenti.

Nel caso in cui si ravveda necessità di aggiornamento del contenuto, il Manuale stesso sarà verificato e approvato internamente, a cura del Responsabile sopra identificato, e sarà sottoposto a validazione a cura dell'Agenzia per l'Italia Digitale.

4 Caratteristiche del servizio SpidItalia

4.1 Caratteristiche generali del servizio

Il Sistema Pubblico di identità Digitale (SPID) mette in relazione gli attori del sistema [paragrafo 2.5.1] per le attività necessarie alla richiesta e fruizione di un servizio online, erogato da un Fornitore di servizi a seguito della richiesta da parte di un Utente ed a seguito di eventuali accertamento di ruoli e qualifiche presso i Gestori degli attributi qualificati.

Le principali funzionalità dell'IdP sono quindi quella di **Registrazione** degli utenti e quella di **Autenticazione** degli utenti.

Il sistema di Gestione delle Identità digitali può essere schematicamente rappresentato attraverso il seguente diagramma seguente che descrive le principali componenti logiche dell'infrastruttura.

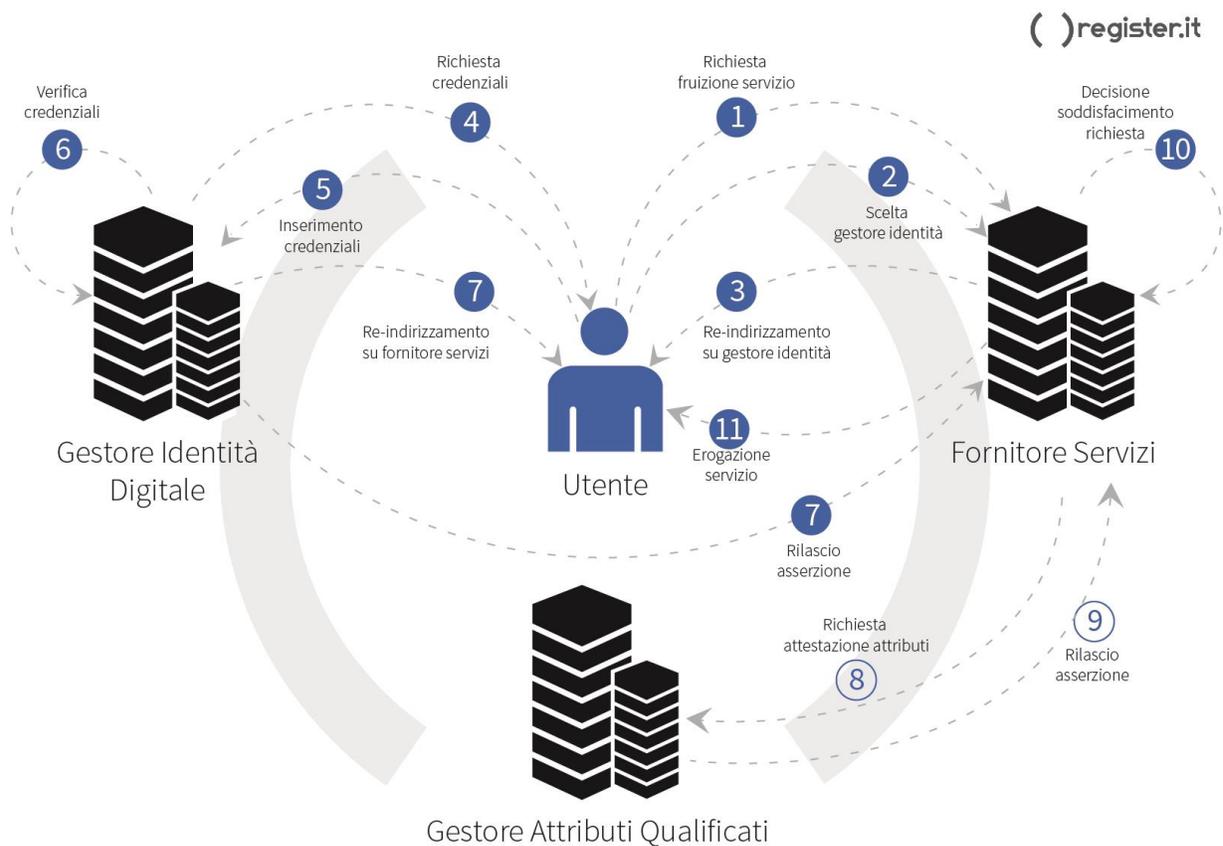


Figura 1 – Schema di funzionamento del Sistema Pubblico per l'Identità Digitale

1 - Richiesta fruizione servizio: l'Utente, sul sito Service Provider, chiede accesso a funzionalità per le quali è richiesta l'autenticazione informatica.

2 - Scelta del Gestore di identità: Il Service Provider sottopone all'Utente il Form tramite il quale quest'ultimo può effettuare la scelta dell'IDP.

3 - Re-indirizzamento sull'IdP: l'Utente viene indirizzato sul sito del Gestore di identità con la richiesta di autenticazione, il livello di sicurezza SPID necessario ed il set dati richiesto.

4 - Richiesta credenziali: l'IdP, consultato il Registro SPID presente nella propria cache (secondo le tempistiche previste da AgID) per verificare il corretto accreditamento del Service Provider richiedente ed ottenuti i certificati del Service Provider con i quali verifica l'autenticità, sottopone all'Utente l'interfaccia web di login tramite la quale potrà autenticarsi con livello richiesto dall'SP.

5 - Inserimento credenziali: l'Utente inserisce le credenziali richieste dall'IdP utilizzando le modalità proposte ed avvalendosi di eventuali dispositivi di autenticazione.

6 - Verifica delle credenziali: l'IdP verifica la correttezza delle credenziali immesse.

7 - Re-indirizzamento sul SP: l'IdP, dopo la verifica positiva delle credenziali e dello stato dell'identità digitale, restituisce al SP l'esito dell'autenticazione ed i dati richiesti.

8 - Richiesta di specifici attributi qualificati (opzionale): processo opzionale che non coinvolge l'IdP. Attività finalizzata alla raccolta di attributi qualificati dell'Utente eventualmente necessari ai fini della fruizione di servizi dei SP.

9 - Rilascio di specifici attributi qualificati (opzionale): nei casi previsti, il Gestore di attributi qualificati rilascia gli attributi richiesti (esempio qualifiche, iscrizione albo...).

10 - Decisione soddisfacimento richiesta: il Service Provider ha evidenza del processo di autenticazione e gli eventuali attributi qualificati necessari e decide se autorizzare l'accesso.

11 - Erogazione del servizio: il Service Provider, in caso di esito positivo, autorizza la fruizione dei servizi.

Le credenziali SPID utilizzate dall'Utente devono essere coerenti con il livello di sicurezza richiesto dal Service Provider così che l'Utente possa utilizzare il servizio richiesto.

4.2 Livelli di sicurezza

Esistono 3 livelli di sicurezza delle credenziali SPID, conformi a quanto previsto dal DPCM e dai Regolamenti attuativi, che possono essere richiesti dai Fornitori di Servizi in funzione del servizio/dati ai quali si richiede l'accesso.

Livello di sicurezza 1: corrisponde al Level of Assurance 2 dello standard ISO/IEC DIS 29115. Si basa su di un sistema di autenticazione ad un solo fattore, basato su password. A questo livello vengono rilasciate all'Utente uno Username ed una Password.

Il primo livello di autenticazione viene utilizzato nei casi in cui il rischio derivante dall'utilizzo indebito dell'identità digitale, abbia un basso impatto per le attività del cittadino/impresa/pubblica amministrazione.

Livello di sicurezza 2: corrisponde al Level of Assurance 3 dello standard ISO/IEC DIS 29115. Si basa su di un sistema di autenticazione a due fattori non necessariamente basato su certificati digitali. A questo

livello vengono rilasciate all'Utente uno Username, una Password ed un codice di sicurezza (OTP - One-Time Password) gestiti tramite sistema SMS ed applicazioni che assicurino l'ottemperanza alla normativa. Possono essere gestiti anche sistemi biometrici di accesso nel rispetto delle previsioni del Garante per la Protezione dei dati Personali.

Questo livello di autenticazione viene utilizzato per i servizi che possono subire un danno consistente in caso di utilizzo indebito dell'identità digitale.

Livello di sicurezza 3: (non ancora gestito) corrisponde al Level of Assurance 4 dello standard ISO/IEC DIS 29115. Si basa su di un sistema di autenticazione informatica basata su certificati digitali le cui chiavi private sono custodite su dispositivi sicuri che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo.

Corrisponde al livello di garanzia maggiore associato ai servizi che possono subire un danno serio e grave in caso di utilizzo indebito dell'identità digitale.

4.3 Descrizione delle componenti applicative

Nel presente capitolo vengono descritte le architetture, applicative e di dispiegamento, dei sistemi di autenticazione delle credenziali che compongono il sistema di gestione delle identità SpidItalia.

Di seguito viene riportato lo schema della architettura logico-applicativa del servizio IdP di Register.

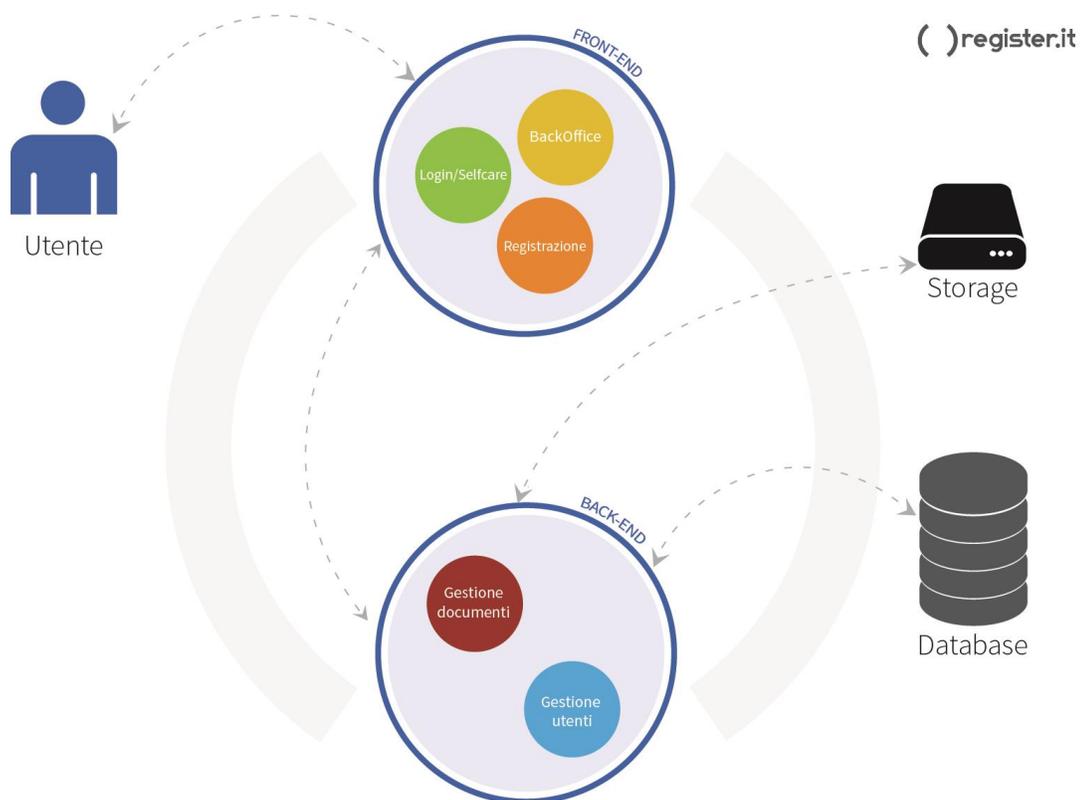


Figura 2 – Architettura logico-applicativa IdP

L'architettura è di tipo SOA (service-oriented architectures) in cui ogni container rappresenta un servizio e ciascun servizio comunica con gli altri tramite i più comuni protocolli di rete.

Il servizio di gestione delle Identità digitali può essere logicamente suddiviso in:

- Applicazioni di Front End: applicazioni che si interfacciano con l'Utente.
- Applicazioni di Back End: sistema applicativo di provisioning.

4.3.1 Applicazioni di Front End

4.3.1.1 Login

Il Titolare in possesso di credenziali Spiditalia che volesse accedere ai servizi messi a disposizione da un Service Provider, deve dimostrare di possedere realmente tali credenziali e che siano in corso di validità mediante verifica delle stesse all' Identity Provider.

L'applicazione di *Login* implementa la suddetta verifica, fornendo all'Utente l'interfaccia di autenticazione e comunicando con il Service Provider mediante il protocollo di autenticazione SAML 2.0 in cui ogni messaggio è firmato digitalmente per garantirne l'integrità, come previsto dal DPCM.

L'IdP invia in modo sicuro, confidenziale e non ripudiabile l'asserzione di identità in base al metodo di autenticazione richiesto ed utilizzato e degli attributi qualificati che il Titolare ha autorizzato a concedere al Service Provider.

4.3.1.2 Registrazione

Al fine di ottenere una identità Spiditalia, viene richiesto al richiedente di fornire una serie di informazioni mediante l'applicazione di *Registrazione*.

In particolare, mediante questa applicazione, l'Utente può:

- registrare le proprie credenziali
- registrare la propria anagrafica
- effettuare il proprio riconoscimento mediante l'uso della Carta Nazionale dei Servizi, Firma Digitale, de visu o de visu da remoto (webcam).

L'applicazione tiene memoria dei flussi di registrazione non conclusi, permettendo all'Utente che ne avesse necessità, di riprendere in un secondo momento un flusso già iniziato in precedenza.

Tutte le informazioni fornite dall'utente sono scambiate in maniera sicura e confidenziale grazie ai protocolli di sicurezza usati dall'applicazione di *Registrazione*.

4.3.1.3 Selfcare

L'applicazione di *Selfcare* permette al Titolare che sia in possesso di credenziali Spiditalia di:

- modificare i dati inseriti in fase di registrazione
- sospendere la propria identità digitale SpidItalia

L'applicazione di *Selfcare* tratta i dati in modo sicuro e confidenziale utilizzando gli appropriati protocolli di sicurezza.

4.3.1.4 *Backoffice*

Mediante un applicativo di *Backoffice* il personale autorizzato di SpidItalia, previa autenticazione, può svolgere l'attività di assistenza ai Titolari, potendo attivare, sospendere e revocare le Identità Digitali.

4.3.2 Applicazioni di Back End

Gli applicativi di Back End sono realizzati con architettura a Micro Servizi ma le loro funzioni possono essere catalogate in due macro categorie: la gestione degli utenti e la gestione documentale

4.3.2.1 *Gestione Utenti*

Mediante l'esposizione di API REST verso le applicazioni di Front End, ciascuno dei servizi di questa categoria si occupa di:

- gestire l'anagrafica dell'Utente
- gestire le credenziali SPID
- gestire l'invio delle comunicazioni all'Utente

4.3.2.2 *Gestione Documenti*

Mediante l'esposizione di API REST verso le applicazioni di Front End, ciascuno dei servizi di questa categoria si occupa di:

- gestire i documenti firmati digitalmente
- archiviare i documenti forniti dall'Utente in fase di riconoscimento
- archiviare gli eventi legati alle richieste di registrazione al servizio IdP SpidItalia
- archiviare gli eventi di login di un Titolare di una Identità Digitale SpidItalia

4.4 Strumenti di autenticazione

Attualmente Register mette a disposizione dell'Utente 2 metodi di autenticazione in aderenza alla normativa DPCM:

1. **Primo Livello** (Livello SPID 1): corrisponde al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115 ed è un sistema di autenticazione a singolo fattore
2. **Secondo Livello** (Livello SPID 2): corrisponde al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115 ed è un sistema di autenticazione informatica a due fattori

Il Titolare di SpidItalia, tramite area di gestione di SpidItalia (*Selfcare*), avrà la possibilità di ricevere notifica ogni volta che vengano utilizzate le sue credenziali.

4.4.1 Metodo di autenticazione di primo livello

Secondo questo metodo viene richiesta all'Utente "*una cosa che conosce*", in particolare una **password** associata al proprio **username**, entrambi scelti dall'Utente in fase di registrazione. Tali credenziali non vengono memorizzate mai in chiaro, ma in forma cifrata in maniera irreversibile mediante algoritmo di hashing allo scopo di garantirne la segretezza e di poterne verificare la validità in fase di autenticazione.

Il sistema impone l'utilizzo di password complesse sia in fase di primo inserimento che di modifica.

Le politiche di creazione/aggiornamento della password seguono i seguenti requisiti minimi vincolati a policy di robustezza, quali:

- avere una lunghezza di almeno 8 caratteri
- contenere almeno un numero (1; 2; 3; ...);
- contenere almeno un carattere speciale (*; \$; !; %; ...).
- avere durata massima di 180 giorni
- non riutilizzabilità: non è possibile inserire una password precedentemente usata se non prima di 5 variazioni e comunque non prima di 15 mesi.

Opportuni sistemi per la gestione della scadenza della password provvedono ad informare l'Utente, con determinati tempi di preavviso, attraverso messaggi inviati via email e SMS al numero di cellulare del Titolare.

Il processo di autenticazione consta di uno scambio di richieste e risposte fra i tre attori Utente, Service Provider e IdP SpidItalia schematizzabile come segue:

- L'utente richiede l'accesso ad un servizio esposto da un Service Provider
- Il Service Provider genera una richiesta di autenticazione SAML e la inoltra a SpidItalia attraverso il browser dell'Utente
- L'Utente viene reindirizzato all'applicazione di *Login* di SpidItalia
- L'Utente inserisce le proprie credenziali SPID nel form di login
- L'applicazione di Login, interrogando i servizi di Back End, verifica la correttezza delle credenziali inserite dall'Utente

- Se la verifica delle credenziali va a buon fine e se l'account SPID risulta attivo, l'autenticazione si conclude con successo
- Sul browser dell'Utente viene installato un cookie che identifica la sessione di SSO attivata
- L'Utente viene reindirizzato sul sito del Service Provider alla pagina di erogazione del servizio richiesto

4.4.2 Metodo di autenticazione di secondo livello

Secondo questo metodo viene richiesta all'Utente "*una cosa che ha*", in particolare il numero di **telefono cellulare** verificato in fase di registrazione. In seguito alla corretta verifica delle credenziali di primo livello, all'Utente viene infatti richiesta l'immissione di una One Time Password (OTP) che il sistema invia mediante SMS al numero di telefono del Titolare.

La One Time Password generata è una stringa di 6 caratteri numerici generata in modo casuale, è unica, ha validità limitata nel tempo ed è univocamente associata al Titolare.

A seguito dell'inserimento della corretta OTP e del consenso a passare i dati al SP, l'autenticazione può considerarsi conclusa con successo.

Il processo di autenticazione di secondo livello può essere dettagliato come segue:

- Si verificano le credenziali SPID del titolare come descritto nell'autenticazione di primo livello
- Il servizio di autenticazione di SpidItalia genera e memorizza una OTP a durata temporale limitata associandola al numero di cellulare verificato del Titolare
- Il servizio di gestione delle comunicazioni di SpidItalia invia un SMS al numero di telefono del Titolare contenente l'OTP generata
- L'applicazione di Front End di *Login* propone un form con un campo adibito all'inserimento della OTP
- L'Utente riceve l'SMS ed inserisce la OTP nel form di login
- L'applicazione di Login, interrogando i servizi di Back End, verifica la correttezza della OTP inserita
- Se la OTP risulta corretta e non scaduta il servizio di Back End provvede ad eliminarlo e informa l'applicazione di Login che l'autenticazione ha avuto successo
- L'Utente viene reindirizzato sul sito del Service Provider alla pagina di erogazione del servizio richiesto, in assenza di sessione di autenticazione

4.4.3 Metodo di autenticazione di terzo livello (ancora non implementato e non utilizzato dai SP)

Il metodo prevede un sistema di autenticazione informatica basata su certificati digitali le cui chiavi private sono custodite su dispositivi sicuri. Tra questi dispositivi sono compresi la Carta Nazionale dei Servizi e la Smart card di Firma Digitale.

4.5 Messaggi di anomalia

In fase di autenticazione il sistema di identità digitale segnala eventuali anomalie riscontrate. Register ha recepito la tabella degli errori identificata da AgID e disponibile in Allegato A.

5 Modalità di identificazione e di rilascio delle credenziali

Questa sezione descrive le procedure di richiesta e creazione delle Identità Digitali di Register.

Ad oggi potranno essere richieste solo credenziali di livello 1 e 2. In ogni caso, le credenziali di livello 3, al momento non disponibili, potranno essere richieste solo dopo aver ottenuto le credenziali di livello inferiore.

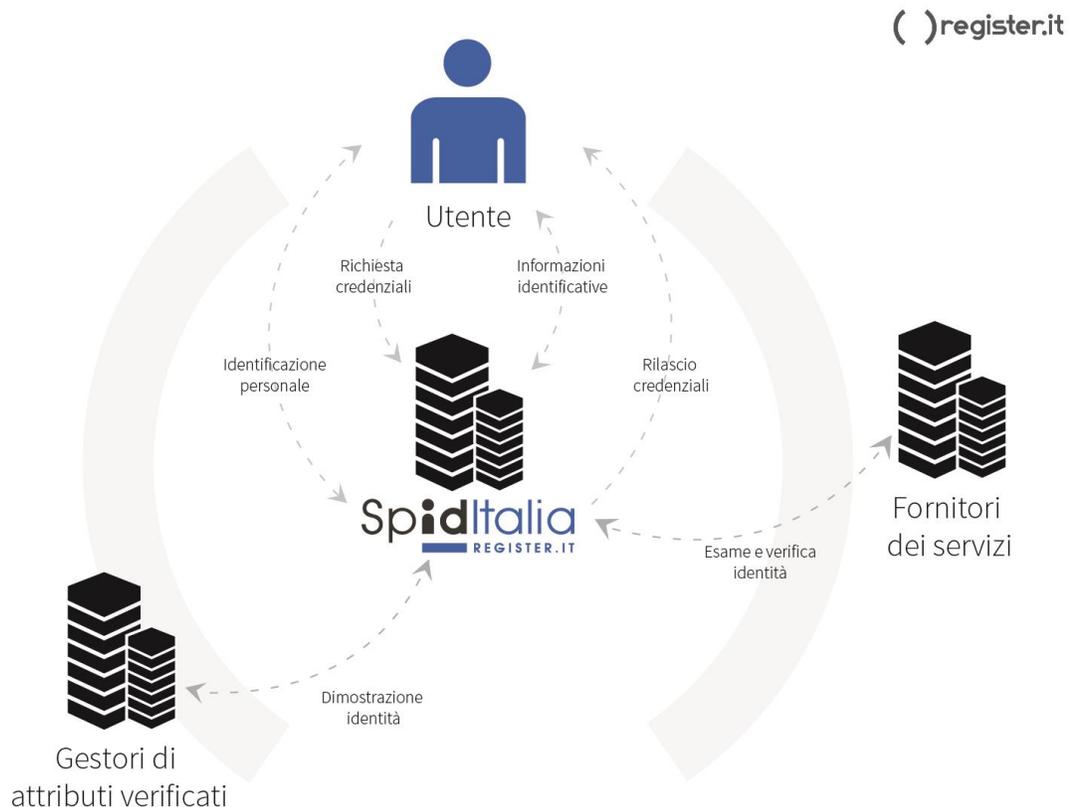


Figura 3 – Schema di funzionamento del Sistema Pubblico per l'Identità Digitale

La procedura di rilascio prevede l'identificazione del Richiedente, la sottoscrizione del contratto di adesione al servizio con una delle modalità previste e la scelta da parte del Titolare delle credenziali di autenticazione minime.

Il punto rilevante per il rilascio dell'Identità Digitale SpidItalia, è la verifica da parte di Register dell'identità del Richiedente.

5.1 Identificazione del Richiedente ed attivazione del servizio

La verifica dell'identità del soggetto Titolare avviene secondo le seguenti modalità:

- Identificazione informatica:
 - utilizzo di firma digitale o firma elettronica qualificata del Titolare;
 - utilizzo di una carta CIE, CNS o TS-CNS del Titolare;
- Identificazione a vista in presenza di un operatore dell'IdP

Attualmente il servizio è erogato con credenziali di Livello 1 e 2, pertanto non viene richiesta la scelta del Livello di sicurezza.

Al fine di facilitare il processo di identificazione, è stato uniformato nelle parti comuni e diviso solo dove necessario.

Ecco le principali fasi:

1. Il processo ha inizio dalla pagina di richiesta dell'identità digitale (<https://spid.register.it/registration>).
Fin dall'inizio l'interfaccia visualizzerà, mediante tab, le fasi dell'intero processo di richiesta identità.
2. Il Richiedente compila un form contenente:
 - Username
 - Password: sarà possibile visualizzare il grado di sicurezza della password prescelta. Questo per aiutare l'Utente nella scelta di una password che rispetti le regole di complessità previste dalle regole attuative di AgID.Fin dal primo step viene fornito il link all'Informativa Privacy contenente tutte le informazioni sul trattamento dei dati personali.
3. Inserimento dell'indirizzo di posta elettronica.
Se l'Utente non possiede un indirizzo mail valido può richiederne uno a Register secondo le offerte pubblicate sul canale Email del sito Register.
4. Conferma dell'indirizzo email inserito mediante inserimento di un codice di sicurezza inviato sull'indirizzo inserito al punto 3.
5. Inserimento del numero di cellulare su cui riceverà una OTP da inserire nella form per verificarne l'esistenza.
6. Inserimento dei dati identificativi obbligatori e richiesti dalla normativa.
 - a. **Per le persone fisiche** sono considerate obbligatori:
 - cognome e nome;
 - sesso, data e luogo di nascita;
 - codice fiscale;

- estremi di un valido documento di identità;
 - numero e data scadenza della tessera sanitaria;
 - gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM.
- b. **Per le persone giuridiche** sono considerate obbligatorie:
- denominazione/ragione sociale;
 - codice fiscale o P.IVA (se uguale al codice fiscale);
 - sede legale;
 - certificazione con indicazione amministratori e/o rappresentanti legale (in alternativa atto notarile di procura legale) e data di rilascio e validità dello stesso;
 - estremi del documento di identità utilizzato dal rappresentante legale;
 - gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM.

I documenti ammessi per l'identificazione sono quelli ammessi dal DPR 445/2000, art. 35.

I più comuni e consigliati sono: Carta di Identità italiana, Patente di guida italiana, Passaporto.

All'interno della stessa pagina sarà possibile caricare copie per immagine fronte/retro del documento di identità.

Possono essere richiesti dati aggiuntivi (cittadinanza, residenza e domicilio, al fine di migliorare l'esperienza d'uso per l'Utente.

7. Scelta del livello SPID: attualmente il servizio viene sempre erogato con credenziali di Livello 2, pertanto non viene richiesta la scelta del Livello di sicurezza.
8. Register procede all'identificazione del Titolare secondo la modalità scelta dal Richiedente. Attualmente quelle messe a disposizione sono:
 - a. utilizzo di **firma digitale** o firma elettronica qualificata. Il Titolare sottoscrive il modulo di richiesta del servizio con proprio certificato qualificato di firma. Register riceve il documento e verifica la firma apposta. In questo caso si considera che la fase di identificazione e verifica sia stata correttamente espletata dal gestore che ha precedentemente rilasciato il documento digitale di identità.
 - b. utilizzo di una carta **CIE, CNS o TS-CNS** del Titolare. Il Titolare dovrà autenticarsi con la carta ed inserire il PIN.
 - c. identificazione **via Webcam**. Il Titolare accetta le condizioni contrattuali e procede a sottoscrivere il modulo di richiesta del servizio. Un operatore di Register contatterà il Titolare e procederà all'identificazione mediante riscontro di dati e documenti identità.
 - d. identificazione **de-visu (ad oggi non ci sono ancora sedi disponibili)**. Il Titolare accetta le condizioni contrattuali e procede a sottoscrivere il modulo di richiesta del servizio. In caso di scelta de-visu visualizzerà le sedi dove presentarsi ed incontrare l'operatore di Register che procederà all'identificazione mediante esibizione di un valido documento di identità.

Nei metodi Webcam e de-visu, terze parti possono agire per conto di Register previa sottoscrizione di un contratto apposito e condiviso con AgID e dopo adeguato corso di formazione. Essi potranno agire solo per le pratiche di identificazione, riconoscimento e registrazione utilizzando strumenti telematici sicuri messi a disposizione da Register.

9. Il Titolare accetta esplicitamente le condizioni contrattuali del servizio ed i consensi relativi alla privacy;
10. Dopo la validazione delle informazioni raccolte da parte di Register, si comunica al Titolare l'esito del processo di richiesta attivazione.

Il servizio è disciplinato e fornito in conformità con la normativa vigente [paragrafo 2.2] e con quanto previsto dalla documentazione fornita all'Utente di seguito elencata e presente sul sito web di Register, area dedicata a SpidItalia (<https://www.register.it/spid>):

- Carta dei Servizi SpidItalia
- il presente Manuale Operativo
- Guida Utente SpidItalia
- Informativa sulla Privacy

5.2 Rilascio delle credenziali

A seguito del perfezionamento delle fasi di riconoscimento, viene inviata al Titolare una comunicazione via email di riepilogo dati ed informazioni con allegati i documenti contrattuali.

Register, in qualità di IdP, procederà alla verifica dei dati secondo le metodologie ed i tempi previsti per l'erogazione del servizio al termine delle quali convaliderà o meno la registrazione (vedi anche paragrafo 8.4).

In caso di esito positivo sarà inviata all'Utente comunicazione di avvenuta attivazione delle credenziali SpidItalia oltre a tutte le informazioni per procedere all'utilizzo del servizio stesso.

5.3 Attributi qualificati

La gestione di attributi qualificati (qualifiche, abilitazioni professionali, poteri di rappresentanza ed ogni altro attributo specifico del Titolare) è affidata ai gestori di attributi qualificati che hanno il potere di attestarli su richiesta dei fornitori.

5.4 Conservazione delle evidenze

Tutta la documentazione comprovante la corretta attribuzione dell'identità digitale al Titolare viene archiviata in conservazione.

Il sistema invia il fascicolo di richiesta del servizio contenente evidenze, documenti e dati in conservazione per l'associazione e la verifica degli attributi. Maggiori dettagli al capitolo 8.

6 Gestione del ciclo di vita dell'ID

6.1 Gestione attributi

L'Utente Titolare può modificare i propri attributi identificativi accedendo all'**area selfcare** di SpidItalia di Register. Mediante accesso con credenziali livello 2 SPID, può modificare:

- Estremi documento di riconoscimento
- Data scadenza documento di riconoscimento
- Numero di telefono cellulare
- Indirizzo di posta elettronica
- Dati di domicilio

Ogni modifica viene fatta sotto la responsabilità del Titolare stesso. In caso di modifica del numero di cellulare Register procederà alla verifica dello stesso con le stesse modalità indicate al paragrafo 5.1.

6.2 Sospensione dell'Identità Digitale

La sospensione comporta la disattivazione momentanea dell'identità che non potrà essere utilizzata durante il periodo in cui risulterà sospesa. Trascorso il periodo di sospensione può essere riattivata oppure revocata (paragrafo 6.3).

La riattivazione consiste nel rendere di nuovo utilizzabili le credenziali precedentemente sospese.

6.2.1 Sospensione volontaria da parte del Titolare

Nei casi previsti dall'art.9 del DPMC o qualora ritenga che la propria identità sia stata utilizzata in modo fraudolento, il Titolare può richiederne la sospensione immediata.

Il Titolare può procedere alla richiesta di sospensione accedendo alla propria area selfcare ed inoltrando apposita richiesta seguendo le indicazioni riportate all'interno dell'area stessa.

A seguito del corretto invio della richiesta di sospensione, l'IdP provvederà:

- alla messa in stato 'sospeso' dell'ID per un massimo di 30 giorni ed
- all'invio di apposita comunicazione all'indirizzo email di riferimento con la conferma dell'avvenuta sospensione ed i passi da seguire per procedere alla riattivazione o alla revoca.

Trascorsi trenta giorni dalla suddetta sospensione ed in mancanza di richiesta di revoca secondo quanto indicato al paragrafo 6.3, l'IdP provvederà al ripristino dell'identità precedentemente sospesa.

Nel caso il Titolare avesse dimenticato la password di accesso al Selfcare può procedere alla richiesta di Sospensione nei seguenti modi:

1. Recuperando la password mediante la procedura sicura di recupero password messa a disposizione e procedendo poi da Selfcare;
2. Inviando la richiesta via PEC all'indirizzo: gestoreidp@pec.register.it;

3. Inviando la richiesta dall'indirizzo di posta elettronica associata all'identità da sospendere o revocare. La richiesta deve essere in formato elettronico e sottoscritta con firma digitale o elettronica ed inviata a: gestoreidp@pec.register.it.

6.2.2 Sospensione da parte dell'IdP

Register può procedere in autonomia alla sospensione dell'Identità Digitale qualora accerti attività relativa ad usi impropri o tentativi di violazione delle credenziali di accesso.

Il Titolare sarà tempestivamente avvertito utilizzando uno degli attributi secondari.

6.3 Revoca dell'Identità Digitale

La revoca comporta la disattivazione definitiva della Identità Digitale rendendola definitivamente inutilizzabile (sospensione a tempo indeterminato e irrevocabile). I casi di revoca, ai sensi dell'articolo 8 comma 3 e dell'articolo 9 del DPCM possono essere obbligatori o facoltativi.

6.3.1 Richiesta di revoca da parte del Titolare

Il Titolare dell'ID è obbligato a chiedere la revoca della stessa nel momento in cui accerti il venir meno delle caratteristiche di riservatezza e segretezza delle proprie credenziali, incluso casi di furto o smarrimento delle stesse.

Il Titolare può richiedere in qualsiasi momento, senza necessità di motivazione, la revoca della propria Identità Digitale.

Il Titolare può procedere alla richiesta di revoca accedendo alla propria area selfcare ed inoltrando apposita richiesta seguendo le indicazioni riportate all'interno dell'area stessa.

Nel caso il Titolare avesse dimenticato la password di accesso al Selfcare può procedere alla richiesta di Revoca nei seguenti modi:

1. Recuperando la password mediante la procedura sicura di recupero password messa a disposizione e procedendo poi da Selfcare;
2. Inviando la richiesta via PEC all'indirizzo: gestoreidp@pec.register.it;
3. Inviando la richiesta dall'indirizzo di posta elettronica associata all'identità da sospendere o revocare. La richiesta deve essere in formato elettronico e sottoscritta con firma digitale o elettronica ed inviata a: gestoreidp@pec.register.it.

6.3.2 Revoca da parte dell'IdP

Register procede alla revoca dell'Identità Digitale del Titolare, anche senza esplicita richiesta, nei seguenti casi:

1. in caso di inattività dell'Identità Digitale per un periodo superiore a ventiquattro mesi;
2. in caso di decesso della persona fisica o di estinzione della persona giuridica;
3. in caso di cessazione delle attività decorsi trenta giorni dalla comunicazione della cessazione di cui all'art. 12, 1° comma del DPCM;
4. in caso di provvedimento dell'AgID;
5. in caso di scadenza del contratto intercorrente tra Register ed il Titolare;
6. in caso di scadenza del documento di identità del Titolare.

In caso di revoca per inattività dell'identità o per scadenza contrattuale (punti 1 e 5), l'IdP fornisce apposite comunicazioni al Titolare mediante avvisi ripetuti a 90, 30 e 10 giorni, nonché il giorno prima della revoca, utilizzando gli attributi secondari certificati e presenti nel sistema.

Nei casi di revoca per decesso della persona fisica o giuridica (punti 2 e 3), l'IdP procederà alla revoca dell'Identità Digitale, previo accertamento alle banche dati messe a disposizione tramite le convenzioni AgID oppure a seguito di comunicazione ufficiale, opportunamente verificata, da parte di eredi o di una autorità competente.

Nel caso di revoca per scadenza del documento di identità (punto 6), l'IdP non revoca subito l'identità digitale ma procede alla sua sospensione, mettendo in atto meccanismi per comunicare la causa e la data della sospensione al Titolare, utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile indicato dal Titolare negli attributi secondari.

A fronte dell'avvenuto processo di revoca, il Titolare riceverà apposita comunicazione mediante uno degli attributi messi a disposizione.

6.4 Richiesta di assistenza (canali e tempistiche)

I Titolari di una identità digitale di Register possono richiedere assistenza e informazioni mediante i seguenti canali:

Form Online

Il Cliente può contattare l'assistenza clienti utilizzando il form "Richiedi Assistenza" presente nel Pannello di Controllo di Register.

"Register.it Chat"

Il Cliente può contattare l'assistenza clienti utilizzando anche la funzione di "Live Chat" presente sul sito di Register.

Assistenza Telefonica

Il servizio di assistenza telefonica prevede il supporto tecnico.

Tutti i dettagli sono consultabili sulla pagina:

https://www.register.it/support/asstel_scheda.html

Il servizio di assistenza è operativo tutti i giorni con orario 9-18 incluso sabato e domenica.

Gli obiettivi di presa in carico sono i seguenti:

- Form online: >=90% entro le 4 ore;
- Register.it Chat: >=80% entro 20 secondi
- Assistenza telefonica: >=80% entro 20 secondi

7 Livelli di servizio

Il servizio è erogato secondo quanto descritto nella Carta dei Servizi recuperabile all'interno dell'area SpidItalia sul sito di Register.

I livelli di servizio garantiti possono essere riassunti nella seguente tabella:

Codice	Indicatore di qualità	Modalità funzionamento	SLA
IQ-01	Disponibilità del sotto servizio di registrazione identità	Erogazione automatica	>=99.0% Durata massima di indisponibilità <= 6 ore
		Erogazione in presenza	>=98.0%
IQ-02	Tempo di risposta del sotto servizio di registrazione identità		<= 24h (ore lavorative)
IQ-03	Disponibilità del sotto servizio di gestione rilascio credenziali	Erogazione automatica	>=99.0% - Durata massima di indisponibilità <= 6 ore
		Erogazione in presenza	>=98.0%
IQ-04	Tempo di rilascio delle credenziali		<= 5gg lavorativi
IQ-05	Tempo di riattivazione credenziali		<= 2gg lavorativi
IQ-06	Disponibilità del sotto servizio di sospensione e revoca delle credenziali		>=99.0% Durata massima di indisponibilità <= 6 ore
IQ-07	Tempo di sospensione delle credenziali		<= 30 minuti
IQ-08	Tempo di revoca delle credenziali		<= 5gg lavorativi
IQ-09	Disponibilità del sotto servizio di rinnovo e sostituzione delle credenziali.	Erogazione automatica	>=99.0%
		Erogazione in presenza	>=98.0%
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		<= 5gg lavorativi
IQ-11	Disponibilità del sotto servizio di autenticazione.		>=99.0% Singolo evento indisponibilità <=4 ore
IQ-12	Tempo di risposta del sotto servizio di autenticazione		Tempo di risposta <=3 sec almeno nel 95,0% delle richieste

Tabella 4 – Livelli di servizio per registrazione, ciclo di vita ed autenticazione SpidItalia

Codice	Servizio	SLA RPO ²	SLA RTO ³
IQ-13/IQ-14	Registrazione Rilascio identità	1 ora	8 ore
IQ-15/IQ-16	Sospensione e Revoca identità	1 ora	8 ore
IQ-17/IQ-18	Autenticazione	1 ora	8 ore

Tabella 5 – Livelli di servizio di continuità operativa

Il presidio del servizio che garantisce il monitoraggio e la gestione dei sistemi, delle apparecchiature e delle reti funzionali all'erogazioni del servizio, prevedono un orario H24x7.

Il servizio di assistenza clienti è raggiungibile con orario 09.00-18.00 dal lunedì al venerdì, escluso festivi.

² **RPO** si intende **Recovery Point Objective** e rappresenta il tempo massimo tra la produzione di un dato e la sua messa in sicurezza. Fornisce pertanto la misura della massima quantità di dati che il sistema può perdere a causa di un guasto improvviso.

³ **RTO** si intende **Recovery Time Objective** e rappresenta il tempo necessario per il pieno recupero dell'operatività di un sistema a seguito della sua indisponibilità a causa di un guasto improvviso.

8 Procedure e standard tecnologici e di sicurezza

Register, in accordo ai requisiti normativi, si pone l'obiettivo di assicurare un adeguato livello di qualità nell'erogazione del servizio SpidItalia, garantendo altresì un appropriato livello di protezione delle informazioni.

Per salvaguardare i dati e gli asset che costituiscono il patrimonio informativo aziendale, Register ha adottato una serie di misure tecniche, organizzative e procedurali fondate sul rispetto dei seguenti principi cardine:

- **Riservatezza:** garantire l'accessibilità dell'informazione solamente a coloro che hanno l'autorizzazione ad accedervi;
- **Integrità:** garantire l'accuratezza e la completezza dell'informazione e dei metodi di elaborazione;
- **Disponibilità:** garantire l'accessibilità dell'informazione da parte degli utenti autorizzati, quando vi è necessità.

Ai fini dello sviluppo della piattaforma di erogazione del servizio SpidItalia, Register ha fatto ricorso ad un approccio orientato alla Sicurezza delle Informazioni, prendendo in considerazione i principali standard internazionali, metodologie e best practices specifiche di settore (e.g. lo standard *ISO/IEC 27002:2005: Information technology – Security Techniques - Code of practice for information security*).

Inoltre, per la gestione dei processi di erogazione del servizio SpidItalia, Register si attiene ai principi previsti dalle norme di riferimento di settore per l'implementazione di un Sistema di Gestione della Qualità, finalizzato al miglioramento continuo dell'efficacia e dell'efficienza nella realizzazione del prodotto e nell'erogazione del servizio, con lo scopo di ottenere e incrementare la soddisfazione del Cliente (norma UNI EN ISO 9001:2015).

Il rispetto dei requisiti di sicurezza adottati per lo sviluppo della piattaforma e la gestione dei processi di erogazione del servizio vengono costantemente controllati attraverso opportune verifiche ispettive interne, al fine di individuare eventuali punti vulnerabili e attuare azioni di miglioramento continuo dei livelli di sicurezza e gestione.

8.1 Conservazione delle evidenze per il rilascio delle Identità Digitale

Sono registrati in appositi log tutti gli eventi relativi alla richiesta dell'identità SpidItalia, funzionali alla tipologia di registrazione e contrattualizzazione utilizzata:

- log accesso applicazione da personale Register
- log verifica email
- log verifica numero di cellulare
- log con verifiche su attributi identificativi
- log accesso alla piattaforma di gestione pratica riconoscimento via webcam

Vengono inoltre registrate le evidenze documentali a corredo della richiesta dell'identità, conservate a norma nel sistema di conservazione elettronica documentale certificato:

- contratto sottoscritto con firma digitale;

- foto fronte/retro del documento di identità presentato per il de-visu
- foto fronte/retro del codice fiscale/Tessera Sanitaria presentato per il de-visu
- streaming audiovideo della sessione di riconoscimento

8.2 Tracciatura degli accessi al servizio (log eventi)

Gli accessi al servizio sono registrati sotto forma di log certificato. Il log certificato è composto da un file di testo prodotto dall'applicativo che gestisce il processo di autenticazione e dialogo con i Service Provider, viene firmato e marcato temporalmente e messo in conservazione.

È garantita l'integrità nonché la disponibilità secondo quanto previsto dal DPCM.

Contiene le seguenti informazioni corrispondenti a quanto richiesto e consigliato nelle regole tecniche:

SPID code (come chiave del tracciato)

- richiesta del SP
- risposta del IdP
- ID della richiesta
- timestamp della richiesta
- SP richiedente autenticazione (issuer richiesta)
- ID della risposta
- timestamp della risposta
- IdP autenticante (issuer risposta)
- ID dell'asserzione di risposta
- soggetto dell'asserzione di risposta (subject)

8.3 Richiesta del log certificato

Il Titolare di SpidItalia può richiedere le informazioni contenute nei log mediante accesso all'area selfcare con le proprie credenziali e seguendo le indicazioni fornite sulla stessa. La richiesta dovrà essere validata con l'inserimento delle credenziali SPID di livello 2 ovvero con l'inserimento di una OTP ricevuta via SMS sul numero di telefono cellulare verificato.

Register procederà alla produzione di quanto richiesto e lo fornirà al Titolare.

Le attestazioni rilasciate potranno essere utilizzate dal Titolare per gli usi consentiti dalla legge.

8.4 Misure anticontraffazione

Register ha sviluppato misure anticontraffazione mirate a prevenire il furto d'identità ed il conseguente utilizzo indebito di dati relativi all'identità di un altro soggetto in vita o deceduto.

Tra le misure rientrano:

- Password: sono consentite solo password con caratteristiche di altissima sicurezza (vedi paragrafo 4.4.1);
- Il codice OTP è composto da 6 caratteri numerici ed ha durata limitata (vedi paragrafo 4.4.2);
- Verifica dell'attendibilità degli attributi, compiuta attraverso l'accesso alle fonti autoritative effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM.

Questo significa che, una volta effettuato il riconoscimento certo e concluso il processo di registrazione, Register, in qualità di IdP (Identity Provider o Gestore di Identità), procede alla verifica dei dati secondo le metodologie ed i tempi previsti per l'erogazione del servizio al termine delle quali convaliderà o meno la registrazione.

L'Identità Digitale non viene attivata subito, ma messa in stato 'sospeso' in attesa delle verifiche di cui sopra.

In attesa siano rese disponibili le fonti autoritative vengono effettuati controlli accedendo ai sistemi pubblici esposti dagli Enti competenti. Esempi, non esaustivi, possono essere la verifica del codice fiscale presso il servizio messo a disposizione dall'Agenzia delle Entrate sul suo portale, la verifica per smarrimento, furto o contraffazione del codice del documento sul portale della Polizia dello Stato per verifica e smarrimento, verifica del numero della tessera sanitaria sul portale del Progetto Tessera Sanitaria;

- Viene fornita una Guida per la sicurezza dell'utilizzo del servizio dove vengono suggerite corrette abitudini al Titolare che possono evitare azioni fraudolente;
- Le procedure di identificazione prevedono ulteriori controlli:
 - o utilizzo di firma digitale, tessera sanitaria/CNS e CIE come metodo di riconoscimento vengono verificati i certificati delle stesse e la corrispondenza con quanto certificato dalle Autorità;
 - o l'operatore incaricato del riconoscimento de-visu (sia in presenza che da remoto) richiede vengano presentati solo documenti originali e non fotocopie;
 - o le immagini della documentazione sono messe in conservazione;
 - o i documenti ammessi sono limitati ai più diffusi le cui caratteristiche sono verificabili anche da remoto (carta identità, patente, passaporto) .

8.5 Sistema di monitoraggio

Per verificare la disponibilità del servizio SpidItalia sono state attivate sonde e strumenti per il controllo dei singoli elementi che compongono l'architettura del sistema IdP e per la verifica dei vari servizi che la piattaforma IdP eroga. I controlli agiscono a livello di singolo modulo di sistema e servizio, in modo tale da rilevare i malfunzionamenti in tempo reale e prevenire eventuali interruzioni del servizio stesso.

Il sistema di monitoraggio del servizio SpidItalia è attivo 24 ore su 24, 7 giorni su 7.

Il monitoraggio implementato sui sistemi è orientato a verificare:

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

Qualora venissero riscontrate anomalie nel funzionamento del servizio, vengono subito attivate analisi al fine di comprenderne cause e conseguenze nonché determinare le azioni da intraprendere.

Register si avvale di gruppi specialistici per il monitoraggio della sicurezza dei Sistemi informativi.

Sono svolte attività di rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica per mezzo della continua osservazione dell'infrastruttura gestita.

Le consolle di monitoraggio sono configurate per il controllo continuo e la produzione di allarmi e report di sicurezza per le diverse tipologie di controlli effettuati.

9 Indicazione delle condizioni di fornitura

9.1 Obblighi e responsabilità del Gestore per l'erogazione del servizio SpidItalia

Register si impegna a fornire il servizio in conformità a quanto stabilito nel Manuale Operativo e negli altri documenti che compongono il Contratto per l'erogazione del Servizio, nel rispetto della vigente normativa e degli obblighi assunti con AgID mediante la Convenzione per l'adesione al sistema pubblico per la gestione dell'identità digitale

In particolare, Register si impegna a:

Descrizione
Rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta.
Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale.
Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione de visu.
Conservare copia del log della transazione nei casi di identificazione tramite documenti digitali di identità, identificazione informatica tramite altra identità digitale SPID o altra identificazione informatica autorizzata.
Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso si identificazione tramite firma digitale.
Verifica degli attributi identificativi del richiedente.
Consegnare in modalità sicura le credenziali di accesso all'utente.
Conservare la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale.
Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale.
Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.
Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione.
Effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso.
Revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica.

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

<p>Informare tempestivamente l'AGID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali.</p>
<p>Adeguare i propri sistemi a seguito dell'aggiornamento della normativa.</p>
<p>Inviare all'AGID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici.</p>
<p>In caso intendesse cessare la propria attività, comunicarlo all'AGID "e ai titolari".</p>
<p>almeno 30 giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali rilasciate.</p>
<p>In caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e ne conserva le informazioni.</p>
<p>In caso di cessazione dell'attività, scaduti i 30 giorni, revocare le identità digitali rilasciate e per le quali non si è avuto subentro.</p>
<p>Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi.</p>
<p>Se richiesto dall'utente, segnalargli via email o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso.</p>
<p>Notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale.</p>
<p>Nel caso l'identità digitale risulti non attiva per un periodo superiore a 24 mesi o il contratto sia scaduto, revocarla e informarne l'utente via posta elettronica e numero di telefono mobile.</p>
<p>In caso di decesso del titolare (persona fisica) o di estinzione della persona giuridica, revocare previo accertamento l'identità digitale.</p>
<p>Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.</p>
<p>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.</p>
<p>Nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale.</p>
<p>Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.</p>

In caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.
Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa.
All'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta.
In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID.
Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, adottando idonee misure di sicurezza (art. 31 D.LGS 196/2003) ed utilizzando meccanismi di cifratura.

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

- Attribuisce l'Identità Digitale e rilascia le credenziali connesse attenendosi alle Regole Tecniche emanate dall'AGID;
- Si attiene alle misure di sicurezza previste dal "Codice in materia di protezione dei dati personali" ai sensi del D.lgs n.196 del 30.06.2003 e s.m.i. nonché alle indicazioni fornite nell'informativa pubblicata sul sito <https://www.register.it/spid>;
- Procede alla sospensione o revoca delle credenziali in caso di richiesta avanzata dall'utente per perdita del possesso o compromissione della segretezza, per provvedimento dell'AGID o su propria iniziativa per acquisizione della conoscenza di cause limitative della capacità dell'utente, per sospetti di abusi o falsificazioni.

9.2 Obblighi del Titolare dell'Identità Digitale

Il Titolare dell'Identità Digitale assume gli obblighi e le responsabilità previste dalla normativa vigente, in particolare assume gli obblighi di:

Descrizione
Esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione.
Si obbliga all'uso esclusivamente personale delle credenziali connesse all'Identità Digitale.
Si obbliga a non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti. A tale proposito, si precisa che l'utente è tenuto ad adottare tutte le misure tecniche e organizzative idonee ad evitare danni a terzi.
Si obbliga a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine.
deve garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi.
L'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private.
Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite.
Fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci.
Accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze.
Informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati.
Mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi: <ul style="list-style-type: none"> • 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.
Conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i rischi seguenti: <ul style="list-style-type: none"> • divulgazione, rivelazione e manomissione, • furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale. accertarsi dell'autenticità del fornitore di servizi o del gestore dell'identità digitale quando viene richiesto di utilizzare l'identità digitale.

Attenersi alle indicazioni fornite dal Gestore in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele che da adottare per la conservazione e protezione delle credenziali.

In caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali.

In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali.

9.3 Obblighi del Richiedente

La Persona fisica o giuridica che richiede una o più identità digitali da attribuire ai Titolari è tenuto a prendere attenta visione e a rispettare il presente Manuale Operativo.

9.4 Clausola risolutiva espressa

L'inadempimento da parte del Titolare o del Richiedente agli obblighi sopra indicati costituisce grave inadempimento ai sensi dell'art. 1456 codice civile e conferisce facoltà al Gestore di risolvere il contratto in essere, mediante invio di una comunicazione a mezzo raccomandata A/R o messaggio di PEC contenente la contestazione dell'inadempimento e l'intento di avvalersi della risoluzione stessa.

9.5 Polizza assicurativa

Register, nell'ambito della propria attività di Gestore di identità digitale è dotato di polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi (art. 14 comma 6 lett. i del Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata", con massimale pari a euro 5.000.000,00 per sinistro ed euro 5.000.000,00 in aggregato annuo.

9.6 Protezione dei dati personali

I dati personali dei Titolari, dei Richiedenti e dei soggetti con i quali Register venga in contatto nell'esercizio delle proprie attività sono trattati nel rispetto della vigente normativa e in conformità con il Codice sulla protezione dei dati personali (D.Lgs. 196/2003), garantendo la tutela degli interessati, in particolare assicurando agli stessi il diritto di ricevere adeguata informativa sul trattamento dei dati personali ai sensi dell'art. 13 D.Lgs. 196/2003.

Il Gestore si impegna altresì a trattare i dati personali nell'ambito dell'erogazione del servizio di identità digitale nel rispetto del principio di necessità e delle altre garanzie fissate dal Codice sulla protezione dei dati personali, per le finalità e secondo le modalità fissate nel CAD, nel DPCM e nei Regolamenti attuativi dello SPID emessi da AgID.

Allegato A – SPID-Tabella 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	Note
1	Autenticazione corretta	HTTP POST HTTP Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)	n.a.	n.a.	n.a.	
Anomalie del sistema									
2	Indisponibilità sistema	HTTP POST	n.a.	n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio più tardi	n.a.	
3	Errore di sistema	HTTP Redirect	HTTP 500	n.a.	Utente	Pagina di cortesia con messaggio "Sistema di autenticazione e non disponibile - Riprovare più tardi"	Ripetere l'accesso al servizio più tardi	n.a.	Tutti i casi di errore di sistema in cui è possibile mostrare un messaggio informativo all'utente
Anomalie delle richieste									
Anomalie sul binding									
4	Formato binding non corretto	HTTP Redirect	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	Parametri obbligatori: SAMLRequest SigAlg Signature
		HTTP POST							Parametri non obbligatori: RelayState
									Parametri obbligatori: SAMLRequest
									Parametri non obbligatori: RelayState

5	Verifica della firma fallita	http:Redirec t	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Impossibile stabilire l'autenticità della richiesta di autenticazion e- Contatare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati
6	Binding su metodo HTTP errato	HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non ricevibile- Contatare il gestore del servizio"	Contattare il gestore del servizio	Verificare metadata Gestore dell'identita (IdP)	invio richiesta in HTTP-Redirect su endpoint HTTP-POST dell'identity
		HTTP POST							invio richiesta in HTTP-POST su endpoint HTTP-Redirect dell'identity
Anomalie sul formato della AuthnReq									
7	Errore sulla verifica della firma della richiesta	HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contatare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o non corrispondente ad un fornitore di servizi riconosciuto o non associato al corretto EntityID nei metadati registrati

8	Formato della richiesta non conforme alle specifiche SAML	HTTP POST HTTP Redirect	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	Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente alla verifica positiva della firma
9	Parametro version non presente, malformato o diverso da '2.0'	HTTP POST HTTP Redirect	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 corrisponde all'entità che sottoscrive la richiesta	HTTP POST/HTTP Redirect	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 POST HTTP Redirect	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	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata solo a seguito di una positiva verifica della firma.
12	RequestAuthnContext non presente, malformato o non previsto da SPID	HTTP POST HTTP Redirect	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	Auth livello richiesto diverso da: urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3

13	IssuedInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP POST/HTTP Redirect	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 coincidente con il Gestore delle identità ricevente la richiesta	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupport ed 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 aggiornato al valore true	HTTP POST/HTTP Redirect	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 POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsup ported ErrorCode nr16	Fornitore del servizio (SP)	n.a.	n.a.	AssertionConsumerServiceIndex presente e aggiornato con valore non riportato nei metadata
								AssertionConsumerServiceIndex riportato in presenza di uno od entrambi gli attributi AssertionConsumerServiceURL e ProtocolBinding
								AssertionConsumerServiceIndex non presente in assenza di almeno uno attributi AssertionConsumerServiceURL e ProtocolBinding
								La response deve essere inoltrata presso AssertionConsumerService di default riportato nei metadata

17	Attributo Format dell'elemento NameIDPolicy assente o non valorizzato secondo specifica	HTTP POST HTTP Redirect	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	Nel caso di valori diversi dalla specifica del parametro opzionale AllowCreate si procede con l'autenticazione senza riportare errori
18	AttributeConsumerServiceIndex malformato o che riferisce a un valore non registrato nei metadati di SP	HTTP POST HTTP Redirect	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	-
Anomalie derivante dall'utente									
19	Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero tentativi secondo le policy adottate)	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19	HTTP POST/HTTP Redirect	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	Si danno indicazioni specifiche e puntuali all'utente per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi di determinate condizioni legate alle policy di sicurezza aziendali, ad esempio dopo 3 tentativi falliti, si risponde al SP.

20	Utente privo di credenziali compatibili con il livello richiesto dal fornitore del servizio	HTTP POST HTTP Redirect	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	
21	Timeout durante l'autenticazione utente	HTTP POST HTTP Redirect	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 POST HTTP Redirect	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)		Dare consenso	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1.
23	Utente con identità sospesa/revocata o con credenziali bloccate	HTTP POST HTTP Redirect	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	

