InfoCamere SPID

Manuale Operativo del servizio di gestione del Sistema Pubblico di Identità Digitale

Versione	4	Data Versione:	10 / 11 / 2023
Codice Documento	IC_MO_SPID	Classificazione	Pubblico
Redatto da	InfoCamere	Verificato da	
Approvato da	Gianni Coppa		

Indice

1. Storia delle modifiche e precedenti emissioni

Versione:	4	Data Versione:	10 / 11 / 2023
Descr. modifiche:	Intero documento: correzioni puntuali §5.4.2 aggiornata modalità di Autenticazione Forte proposta per il livello di sicurezza 2; §5.4.4.2 aggiornata modalità di Autenticazione Forte proposta per il livello di sicurezza 2; §6.5 aggiornata modalità di generazione OTP; §2.1 aggiornamento a portale id.infocamere.it; §3.1 aggiornamento a portale id.infocamere.it; §3.2 aggiornamento a portale id.infocamere.it; §11.1 aggiornamento a portale id.infocamere.it		
Motivazioni:			

Versione:	3	Data Versione:	07 / 11 / 2022
Descr. modifiche:	Intero documento: correzioni puntuali §2.3 aggiornata tabella riferimenti normativi; §4.7 Modifica sotto paragrafi; §5.4.1 Aggiornati criteri; §5.4.3 aggiornati riferimenti normativi; § 5.4.4.3 aggiornati riferimenti normativi; §6.2 Eliminazione sotto paragrafo Requisiti Tecnici; § 6.2.1.2 inseriti riferimenti normativi; §6.4.2 Inseriti dettagli verifica attributi secondari; §7.2.2.1 Modifica sulla modalità di richiesta di Revoca; §7.2.3 Inserita modalità tramite prenotazione telefonica; §11 Modifica sotto paragrafi.		
Motivazioni:			

Versione:	2	Data Versione:	15 / 09 / 2022
Descr. modifiche:	Intero documento: correzione puntuali. § 2.3 Riferimenti Normativi – inserito DPCM 19 ottobre 2021; § 6.2.2.2 Documenti da presentare allo sportello: chiariti gli attributi secondari (persona fisica e persona giuridica); Inserito nuovo paragrafo specifico per Identificazione da remoto con CNS, TS-CNS, CIE, Firma digitale (firma elettronica qualificata). § 6.2.3.2 Chiarite le modalità relative al codice numerico “di verifica” § 6.2.3.3 Aggiunti dettagli su Sessioni video, riportate verifiche liveness. § 5.4.4.3. Credenziali SPID 3 rivisto il paragrafo. §. 7.2.2.2 Revoca da parte del Gestore – adeguati i paragrafi § 7.2.2.3 Chiarite le modalità di autenticazione. §9 Livelli di servizio garantiti aggiornati in riferimento a All. 3) Indicatori qualità e Livelli servizio v.1.2” presente nella Convenzioni dei Gestori di identità digitale.		
Motivazioni:	Modifiche puntuali su alcuni paragrafi e modifica § 9 per aggiornamento SLA AgID		

Versione:	1	Data Versione:	30 / 04 / 2021
Descr. modifiche:			
Motivazioni:	Prima versione del documento		

2. Introduzione

2.1. Scopo e ambito di applicazione del documento

Questa sezione illustra lo scopo del Manuale Operativo e fornisce alcune raccomandazioni per il corretto utilizzo del sistema pubblico per la gestione dell'Identità digitale di cittadini e imprese (SPID).
Si prega di leggere l'intero testo del Manuale in quanto le raccomandazioni contenute nella presente sezione sono incomplete e molti altri importanti punti sono trattati negli altri capitoli.
Per una più agevole e scorrevole lettura del Manuale Operativo si raccomanda la consultazione dell'elenco di acronimi e abbreviazioni posti alla fine della presente sezione. Il presente Manuale Operativo ha lo scopo di illustrare e definire le modalità operative adottate da InfoCamere nell'attività di Gestore dell'Identità digitale ai sensi del 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 ss.mm.ii., pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014.
In particolare, il presente documento illustra le modalità di richiesta, registrazione, validazione, verifica, rilascio, utilizzo, sospensione, revoca, scadenza e rinnovo delle Identità digitali nonché le responsabilità e gli obblighi del Gestore dell'Identità digitale, dei gestori degli attributi qualificati, dei fornitori di servizi, degli utenti titolari dell'Identità digitale e di tutti coloro che accedono al sistema pubblico per la gestione dell'Identità digitale per la verifica delle Identità digitali.
In ottemperanza all'obbligo di informazione richiesto dalla legge (DPCM 24 ottobre 2014 e ss.mm.ii.), InfoCamere pubblica il presente Manuale Operativo in modo da permettere ad ogni singolo Utente di valutare il grado di affidabilità del servizio offerto. Nel presente Manuale Operativo, si parte dal presupposto che il lettore abbia un'adeguata conoscenza della materia relativa alle identità digitali ed alle infrastrutture di identificazione informatica.
L'Utente titolare dell'Identità digitale SPID si impegna a proteggere e a tenere segrete le proprie credenziali d'accesso nonché a dare avviso al Gestore delle Identità digitali dell'eventuale smarrimento, sottrazione o compromissione (vedi definizioni) delle credenziali stesse. Per ulteriori informazioni, si faccia riferimento al portale web dedicato a SPID di InfoCamere id.infocamere.it oppure alla sezione Supporto del portale stesso.

2.2. Standard di riferimento

Standard	Descrizione
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
NIST 800-63-2	Electronic Authentication Guideline
OASIS	https://www.oasis-open.org/
SAML	Security Assertion Markup Language Specifications http://saml.xml.org/samlspecifications
SAML-Core	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
SAML-Bin	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

SAMLAuthContext	Authentication Context for the OASIS Security Assertion Markup Language SAML V2.0 http://docs.oasis-open.org/security/saml/v2.0/samlauthncontext-2.0-os.pdf
SAML-Metadata	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 (http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)
SAML-TechOv	SAML Technical Overview http://www.oasisopen.org/committees/download.php/20645/sstc-samltechoverview-2%200-draft-10.pdf
XML Signature	XMLSig W3C WG http://www.w3.org/Signature/
SAML-IdpDisc	Identity Provider Discovery Service Protocol and Profile (http://docs.oasisopen.org/security/saml/Post2.0/sstc-saml-idpdiscovery.pdf)
SPID-TabAttr	Tabella Attributi (http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_attributi_idp.pdf)
SPID-TabErr	Tabella Codici di Errore - https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche/spid-messaggi.pdf

2.3. Riferimenti, termini, acronimi e definizioni

Riferimento	Descrizione
[1] Regolamento (UE) n. 910/2014	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 (Gazzetta Ufficiale dell'Unione Europea – serie L257 del 28 agosto 2014)
[2] CAD	Codice Amministrazione Digitale - D.lgs. 7 marzo 2005 n. 82 (G.U. n.112 del 16 maggio 2005) e s.m.i.
[3] DPCM	DPCM del 24 ottobre 2014 (pubblicato in GU Serie Generale n.285 del 9-12-2014) e ss.mm.ii.: 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.
[4] Determinazione n. 44 del 28 luglio 2015	Determinazione di AgID n. 44 del 28 luglio 2015 concernente l'emanazione dei regolamenti SPID previsti dall'art. 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014
[5] Regolamento AgID	Regolamento di AgID del 22 luglio 2016 recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014) e ss.mm.ii.
[6] Regolamento accreditamento AgID	Regolamento di AgID recante le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale (articolo 1, comma 1, lettera l) , DPCM 24 ottobre 2014) del 22 luglio 2016
[7] Note Tecniche AgID	Note tecniche emanate da AgID in data 13 luglio 2020 sulle interfacce e le informazioni IDP/SP
[8] Determinazione 426/2020	Determinazione di AgID n. 426/2020 del 1 ottobre 2020 sul rilascio dello SPID tramite audiovideo e bonifico.
[9] Determinazione n. 505/2020	Determinazione di AgID n. 505/2020 del 30 novembre 2020 per l'utilizzo della tessera sanitaria e il codice fiscale nel rilascio dello SPID.
[10] Linee guida AgID 18 luglio 2022	Linee guida recanti le regole tecniche dei gestori di attributi qualificati; Determinazione di adozione DT 215 del 18 luglio 2022
[11] Regolamento (UE) 2016/679	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al

	trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
[12] Codice Privacy	Codice in materia di protezione dei dati personali – D.lgs. 30 giugno 2003 n. 196 e ss.mm.ii.
[13] Guida Utente	La Guida Utente è un manuale specifico delle funzionalità del servizio SPID definito per gli utenti che vogliono accedere al servizio.
[14] DPCM 19 ottobre 2021	DPCM 19 ottobre 2021 (pubblicato in GU serie speciale n. 296 del 14-12-2021: Modifiche al decreto del Presidente del Consiglio dei ministri 24 ottobre 2014, recante: «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».

Acronimo	Descrizione
AA	Attribute Authority
Adesione	E' il recepimento del framework SPID da parte di entità di certificazione o di fornitori di servizi in rete
Agenzia (anche AgID)	Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Gestori di Identità Digitali)
Attributi Identificativi	Nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, il codice fiscale o la partita IVA e gli estremi del documento d'identità utilizzato ai fini dell'identificazione;
Attributi secondari	Il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni
Attributi qualificati	Le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.
Autenticazione	Disposizione di garanzia sull'identità dell'entità (ISO-IEC 18014-2)
Autenticazione multi-fattore	Autenticazione con almeno due fattori di autenticazione indipendenti (ISOIEC 19790)
BCP	Best Current Practice (IETF)
CA	Certification Authority
RA	Registration Authority o Ufficio di Registrazione
CNS	Carta Nazionale dei Servizi
CIE	Carta di Identità Elettronica
Codice identificativo	Il particolare attributo assegnato dal gestore dell'identità digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID
Credenziale	Un insieme di dati presentati come evidenza dell'identità dichiarata/asserita o di un proprio diritto (ITU-T X.1252), in pratica il Titolare/Utente si avvale di questo attributo (a singolo o doppio fattore) unitamente al codice identificativo (entrambi rilasciati dal Gestore dell'identità digitale) per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi (Amministrazioni e privati) che aderiscono allo SPID
EAA	Entity Authentication Assurance
Entità	Può essere una persona fisica o un soggetto giuridico
ETSI	European Telecommunications Standards Institute
Fattore di autenticazione	Elemento di informazione e/o processo usato per autenticare o verificare l'identità di una entità (ISO-IEC 19790)
Fornitore di servizi	Il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'Utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al Gestore dell'identità digitale che l'ha fornita

Gestori dell'Identità digitale (anche Gestori)	Le persone giuridiche accreditate presso AgID al sistema pubblico SPID che, in qualità di gestori del servizio, previa identificazione certa dell'Utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo Utente al fine della sua identificazione informatica. Esse inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'Identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti.
Gestori di attributi qualificati	I soggetti accreditati ai sensi dell'art. 16 del DPCM [3] che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
HSM	È un dispositivo sicuro per la creazione della firma digitale, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.
ICT	Information and Communications Technology
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
IdM	Identity Management
IdP	Identity Provider (il gestore delle identità digitali in ambito SPID) – Vedi anche Gestori dell'Identità digitale
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
InfoCamere	InfoCamere S.C.p.A.
IP	Internet Protocol
IPV	Identity Proofing and Verification
IR	Incaricato alla Registrazione
IS	International Standard
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
LoA	Level of Assurance
NIST	National Institute of Standards and Technology
OTP	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione
PEC	Posta elettronica certificata
Penetration Test	Il Penetration test è il processo operativo di analisi o valutazione della sicurezza di un sistema informatico o di una rete.
PII	Personally Identifiable Information
RPO	Recovery Point Objective (Tempo di ripristino richiesto) - Tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.
RTO	Recovery Time Objective (Obiettivo temporale di recupero) - Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto.
SAML	Security Assertion Markup Language
SSL	Secure Socket Layer
SP	Service provider – vedi Fornitore Servizi
SPID	Il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD [2], modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98 e notificato, ai sensi del Regolamento (UE) n. 910/2014 [1] alla Commissione Europea
Titolare o Richiedente (Utente)	Per Titolare si intende il soggetto (persona fisica o giuridica) a cui è attribuita l'identità digitale SPID, corrispondente all'Utente di cui all'art. 1 comma 1 lettera v) del DPCM [3]. Prima dell'attribuzione dell'identità digitale tale soggetto è chiamato Richiedente

TCP	Transmission Control Protocol
Token DDNA	Dispositivo di ultima generazione per l'autenticazione con certificato CNS e/o SPID livelli 2 e 3 e la firma digitale
User Agent	Sistema utilizzato dall'Utente per l'accesso ai servizi (di solito il browser per la navigazione in rete).

2.4. Tabella delle corrispondenze

Argomento	Manuale Operativo
1 dati identificativi del Gestore	§ 3.1
2 dati identificativi della versione del manuale	§ 3.2
3 responsabile del manuale operativo	§ 3.4
4 descrizione delle architetture, applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche	§ 5.1 - § 5.2
5 descrizione delle architetture dei sistemi di autenticazione e delle credenziali	§ 5.3
6 descrizione dei codici e dei formati dei messaggi di anomalia sia relativi ai protocolli che ai dispositivi di autenticazione utilizzati	§ 12
7 livelli di servizio garantiti per le diverse fasi della registrazione e della gestione del ciclo di vita delle identità	§ 9.1 - § 9.2 - § 9.3 - § 9.4
8 livelli di servizio garantiti per le diverse fasi del processo di autenticazione	§ 9.5
9 descrizione dei contenuti delle tracciature degli accessi al servizio di autenticazione e delle modalità di acquisizione ai fini dell'opponibilità a terzi	§ 5.5
10 guida Utente del servizio in cui devono essere particolarmente curate le modalità d'uso del sistema di autenticazione, le modalità con cui l'Utente può richiedere la sospensione o la revoca delle credenziali, le cautele che l'Utente deve adottare per la conservazione e protezione delle credenziali. La guida Utente può costituire documento a sé stante	§ 6 - § 7
11 descrizione dei processi e delle procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali	§ 6.4 –§ 6.5
12 descrizione dei metodi di gestione dei rapporti con gli utenti	§ 7.4
13 descrizione generale delle misure anticontraffazione	§ 5.4.4
14 descrizione generale del sistema di monitoraggio	§ 8
15 definizione degli obblighi dell'Utente e del Gestore dell'Identità digitale	§ 4.1- § 4.2
16 indirizzo (o indirizzi) del sito web del Gestore ove è resa direttamente disponibile la descrizione del servizio in lingua italiana e lingua inglese	§ 2.1
17 descrizione delle modalità disponibili agli utenti per richiedere la revoca e sospensione dell'Identità digitale	§ 7.2.2

3. Dati identificativi – Pubblicazione del Manuale Operativo

3.1. Dati identificativi del Gestore dell'Identità digitale

Denominazione sociale	InfoCamere S.C.p.A.
Indirizzo della sede legale	Via G. B. Morgagni, 13 - 00161 Roma
Legale Rappresentante	Lorenzo Tagliavanti
Partita IVA	02313821007
Codice LEI	815600EAD78C57FCE690
Capitale sociale	17.670.000 Euro
N. Telefono (centralino)	06 442851
PEC	protocollo@pec.infocamere.it
Sito web generale	www.infocamere.it
Sito web del servizio	https://id.infocamere.it

3.2. Versione e pubblicazione del Manuale Operativo

Il presente Manuale Operativo è di proprietà di InfoCamere, tutti i diritti sono ad essa riservati. La versione di questo documento è riportata nel frontespizio e in ogni pagina ed è individuato da codice interno IC_MO_SPID.
InfoCamere, nel rispetto delle normative vigenti, esegue eventuali modifiche al Manuale Operativo sottoponendole ad AgID per l'approvazione prima della loro adozione. AgID, se approva le modifiche al Manuale Operativo, lo sottoscrive con firma elettronica e lo pubblica sul proprio sito istituzionale con le informazioni atte a identificare il Gestore.

Il documento è pubblicato in formato PDF firmato digitalmente, in modo tale da assicurarne l'origine e l'integrità.
Il presente Manuale Operativo è reperibile in formato elettronico presso il portale id.infocamere.it alla sezione Documentazione.

Il riferimento al presente Manuale Operativo e le altre informazioni relative al Gestore previste dal DPCM [2] sono pubblicate presso il registro SPID gestito dall'AgID.

3.3. Procedure per l'aggiornamento del Manuale Operativo

InfoCamere si riserva il diritto di apportare variazioni al presente documento nei casi previsti al successivo cap. 11.

Variazioni che non hanno un impatto significativo sugli utenti, o variazioni con un impatto significativo sugli utenti (come, ad esempio, modifiche rilevanti alle procedure operative) comporteranno in ogni caso all'incremento del numero di versione del documento. Il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste.

Ogni variazione al presente Manuale Operativo sarà sottoposta ad AgID per la preventiva approvazione e sarà pubblicata e resa operativa solo a seguito di tale approvazione.

Il presente documento, indipendentemente da eventuali aggiornamenti riconducibili alle variazioni su esposte e in base alle procedure previste dal Sistema di Gestione Qualità aziendale, è comunque soggetto a riesame annuale e, se necessario, aggiornato.

3.4. Responsabile del Manuale Operativo

La responsabilità del presente Manuale Operativo è del Gestore, nella figura del "Responsabile per l'aggiornamento della documentazione depositata presso l'AgID SPID" (art. 2 punto 7 del Regolamento accreditamento AgID recante le modalità per l'accreditamento e la vigilanza dei gestori dell'Identità digitale [6]) il quale ne cura la revisione, la pubblicazione e l'aggiornamento.

Le comunicazioni riguardanti il presente documento possono essere inviate all'attenzione del suddetto responsabile contattabile mediante il seguente indirizzo: spid@pec.infocamere.it

4. Disposizioni generali, obblighi e responsabilità

In questa sezione sono descritti i termini e le condizioni generali in forza dei quali sono erogati i servizi di rilascio e gestione delle Identità digitali descritti nel Manuale.

4.1. Obblighi dell'Utente

L'Utente Titolare dell'Identità digitale si obbliga a:

- esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione, nonché all'uso esclusivamente personale delle credenziali connesse all'Identità digitale;
- 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;
- non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine.
- garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi;
- 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, assumendo le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci;
- accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze;
- informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati;
- mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi:
    - se persona fisica: estremi del documento di riconoscimento e relativa scadenza, numero di telefonia mobile, indirizzo di posta elettronica, domicilio;
    - se persona giuridica: denominazione/ragione sociale, codice fiscale o P.IVA, indirizzo sede legale, visura camerale, estremi documento identità del rappresentante legale della società, numero di telefonia 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:
    - 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;
- aggiornare la propria password secondo le indicazioni e le raccomandazioni previste dai regolamenti di cui all'Art 4, comma 2, del DPCM [3] e descritti al paragrafo 5.4.1 del presente documento.

4.2. Obblighi e responsabilità del Gestore dell'Identità digitale

InfoCamere in qualità di Gestore dell'Identità digitale, ai sensi degli artt. 1 lett. l, 7, 8 e 11 del DPCM [3], è tenuto a:

- attribuire l'Identità digitale, rilasciare le credenziali e gestire le procedure connesse al ciclo di vita dell'identità e delle credenziali attenendosi al DPCM [3] e alle Regole Tecniche tempo per tempo emanate dall'AgID;
- rilasciare l'identità su domanda del Richiedente ed acquisire e conservare il relativo Modulo di adesione;
- 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 di identificazione tramite firma digitale;
- verificare gli attributi identificativi del Richiedente;
- consegnare in modalità sicura le credenziali di accesso al Titolare;
- 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 personali nel rispetto della normativa in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679 [11] ed al Codice Privacy e s.m.i. [12];
- verificare e aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione;
- effettuare tempestivamente e a titolo gratuito su richiesta del Titolare, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso;
- revocare l'identità digitale se si riscontra l'inattività per un periodo superiore a 24 (ventiquattro) mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica;
- segnalare su richiesta del Titolare ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dal Titolare;
- verificare la provenienza della richiesta di sospensione da parte del Titolare (ad eccezione dei casi in cui è inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata);
- fornire al Titolare che l'ha inviata conferma della ricezione della richiesta di sospensione;
- in caso di sospensione, per le ragioni previste dalla normativa vigente e dalle disposizioni delle Condizioni Generali di Contratto che disciplinano il servizio di Identità digitale, sospendere tempestivamente l'Identità digitale per un periodo massimo di 30 (trenta) giorni e informare il Titolare; ripristinare o revocare l'Identità digitale sospesa, nei casi previsti dalla normativa vigente e dalle Condizioni Generali di Contratto che disciplinano il servizio di Identità digitale;
- utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale;
- adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso;
- effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'Identità digitale di ciascun Titolare, procedendo alla sospensione dell'Identità digitale in caso di attività sospetta;
- effettuare con cadenza almeno annuale un'analisi dei rischi;
- definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID;
- allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato;
- condurre con cadenza almeno semestrale il *Penetration Test*;
- garantire la continuità operativa dei servizi afferenti allo SPID;
- effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna;

- garantire la gestione sicura delle componenti riservate delle Identità digitali assicurando non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata;
- garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa;
- sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti;
- informare tempestivamente l'AgID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali;
- adeguare i propri sistemi a seguito dell'aggiornamento della normativa;
- inviare all'AgID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici;
- in caso intendesse cessare la propria attività, comunicarlo all'AgID "e ai Titolari" almeno 30 (trenta) giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le Identità digitali rilasciate;
- in caso di subentro ad un Gestore cessato, gestire le Identità digitali che tale Gestore ha rilasciato conservandone le relative informazioni
- in caso di cessazione dell'attività, scaduti i 30 giorni, revocare le Identità digitali rilasciate e per le quali non si è avuto subentro;
- informare espressamente il Richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi;
- se richiesto dal Titolare, segnalargli via email o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso;
- notificare al Titolare la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua Identità digitale;
- nel caso l'Identità digitale risulti non attiva per un periodo superiore a 24 (ventiquattro) mesi o il contratto sia scaduto, revocarla e informarne il Titolare via posta elettronica e numero di telefono mobile;
- in caso di decesso del Titolare (persona fisica) o di estinzione della persona giuridica, revocare, previo accertamento, l'Identità digitale;
- nel caso in cui il Titolare 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;
- trascorsi 30 (trenta) giorni dalla sospensione su richiesta del Titolare per sospetto uso fraudolento, ripristinare l'Identità digitale sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione;
- nel caso in cui il Titolare 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 al Titolare dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'Identità digitale;
- ripristinare l'identità sospesa su richiesta del Titolare se non riceve entro 30 (trenta) giorni dalla sospensione una richiesta di revoca da parte del Titolare medesimo;
- 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 (venti) 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 al Titolare 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 – salvo diversamente disposto da disposizioni normative o regole tecniche specificamente emanate - alcuna sessione di autenticazione con il Titolare 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 (ventiquattro) mesi precedenti, curandone riservatezza, inalterabilità e integrità, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

secondo quanto previsto dalla normativa vigente in materia di trattamento dei dati personali ed utilizzando meccanismi di cifratura.

4.3. Obblighi dei fornitori di servizi

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

- conoscere l'ambito di utilizzo delle identità digitali, le limitazioni di responsabilità e i limiti di indennizzo del IdP, riportati nel presente Manuale Operativo;
- osservare quanto previsto dall'art. 13 del DPCM [3] e dagli eventuali Regolamenti di cui all'art. 4 del DPCM medesimo;
- adottare tutte le misure organizzative e tecniche idonee a evitare danno ad altri.

4.4. Obblighi dei soggetti esterni che svolgono l'attività di registrazione e/o riconoscimento (*de visu*)

InfoCamere può delegare le funzioni di registrazione e riconoscimento a soggetti esterni (come le Camere di Commercio) previo corso di formazione e sottoscrizione dei documenti specifici che ne disciplinano il rapporto.

Il Gestore di Identità digitali, previa sottoscrizione di apposite Convenzioni, delega a soggetti esterni (come, tra gli altri, le Camere di Commercio) le attività di raccolta dei dati relativi ai Richiedenti le credenziali SPID, la loro identificazione, nonché il successivo eventuale rilascio delle medesime credenziali. Tali soggetti esterni, che fungono da Ufficio di Registrazione o IR, vengono opportunamente formati a tal fine dal Gestore, ed hanno l'obbligo di:

- garantire che il Richiedente sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza delle credenziali SPID;
- garantire che il Richiedente sia espressamente informato in modo compiuto e chiaro sulla procedura di identificazione e rilascio dell'Identità digitale e sui requisiti tecnici necessari;
- adempiere a tutte le obbligazioni derivanti dalla normativa vigente per la protezione dei dati personali;
- verificare l'identità del Richiedente, controllare e registrare i dati dello stesso, secondo le procedure di identificazione e registrazione previste nel presente Manuale Operativo;
- inviare tempestivamente al Gestore delle Identità digitali gli originali delle richieste di credenziali SPID;
- tenere direttamente i rapporti con il Richiedente e con i Titolari e a informarli circa le disposizioni contenute nel presente Manuale Operativo.

4.5. Obblighi del richiedente

Il Richiedente che, avendo preso visione del presente Manuale Operativo, richiede il rilascio delle Identità digitali è tenuto ad attenersi a quanto disposto dal presente Manuale Operativo e dalle Condizioni Generali.

4.6. Obblighi connessi al trattamento dei dati personali

Con riguardo al trattamento dei dati personali, InfoCamere garantisce il rispetto della normativa vigente, attraverso l'implementazione di misure tecniche e organizzative adeguate, per la tutela dei diritti e le libertà delle persone fisiche e assicurando tutte le garanzie fissate dalla normativa vigente.
Nel rispetto del principio di trasparenza, InfoCamere mette a disposizione del Richiedente e del Titolare (c.d. "Interessato") tutte le informazioni specificamente richieste dalla vigente normativa, relativamente al trattamento dei dati personali mediante apposita, specifica e preventiva informativa, resa in forma accessibile e chiara, disponibile anche all'interno del sito istituzionale del servizio SPID.
Con riguardo ai diritti che la normativa riconosce agli interessati, InfoCamere mette in atto misure utili per agevolare, la gestione e l'esercizio di tutti i diritti esercitabili, in quanto applicabili, conformemente alla normativa privacy vigente. Affinché il relativo esercizio risulti quanto più possibile semplice e immediato, vengono messe a disposizione dell'Interessato, in maniera accessibile ed efficace, i dati di contatto dei soggetti individuati cui ricorrere per richieste o informazioni sia nella sezione Supporto del portale SPID e sia nella sezione Self Care in cui è presente un riferimento che porta l'utente alla sezione Supporto.

4.7. Limitazioni di responsabilità ed eventuali limitazioni agli indennizzi

In relazione alle ipotesi di esclusione o limitazione di responsabilità del Gestore, compresa l'ipotesi di mancata conoscenza o non corretto utilizzo da parte del Richiedente e/o del Titolare delle procedure descritte nel presente Manuale Operativo, si rinvia alle corrispondenti clausole delle Condizioni Generali di Contratto del Servizio SPID.

5. Architettura

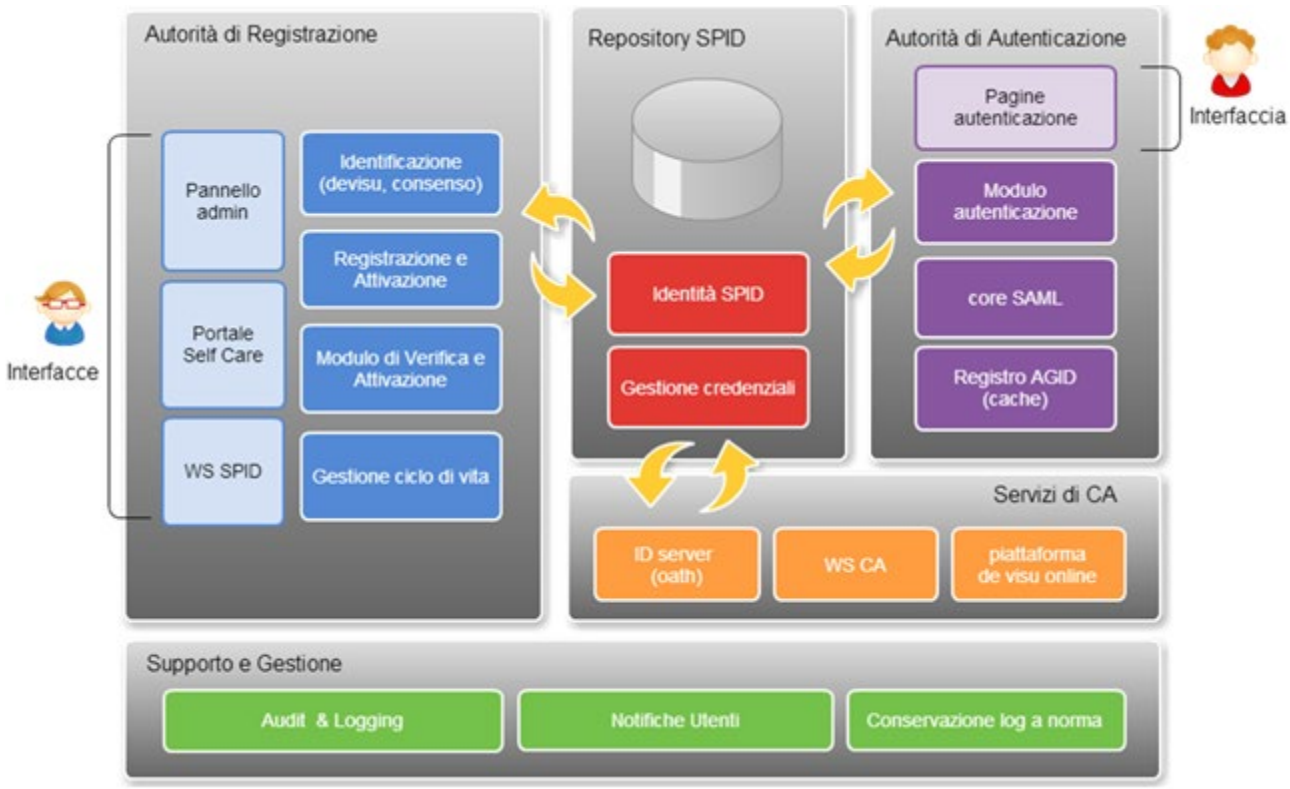
5.1. Architettura Applicativa

Il sistema SPID (Sistema Pubblico di Identità Digitale) è un sistema alternativo a CNS e CIE, per la gestione dell'identificazione certa del cittadino in rete, che consente ai Titolari, siano essi persone fisiche o giuridiche che utilizzano i servizi erogati in rete, di avvalersi dei Gestori dell'Identità digitale per consentire ai Fornitori di Servizi l'immediata verifica della propria identità e di eventuali attributi qualificati.
Tale Sistema SPID è costituito, quindi, da un insieme aperto di soggetti pubblici e privati che gestiscono i servizi di registrazione, attivazione e gestione del ciclo di vita delle credenziali di autenticazione e degli strumenti di accesso in rete.

Il Servizio di Gestione delle Identità digitali può essere logicamente suddiviso in due componenti:

- **Autorità di Registrazione**, alla quale vengono demandate le procedure di registrazione dei soggetti per i quali l'IdP gestisce l'Identità digitale, di associazione delle credenziali di autenticazione al soggetto stesso e di gestione del ciclo di vita della specifica Identità digitale e delle credenziali associate.
- **Autorità di Autenticazione**, alla quale vengono demandate le procedure di autenticazione dei soggetti da essa gestiti, di verificare le credenziali di autenticazione e di generare una asserzione di autenticazione dove indicare gli attributi identificativi richiesti dal Fornitore dei Servizi per la specifica applicazione.

Le principali funzionalità del Gestore delle identità sono quindi: quella di Registrazione dei Richiedenti e quella di Autenticazione dei Titolari.
Il sistema di Gestione delle Identità digitali può essere schematicamente rappresentato attraverso il seguente diagramma che descrive le principali componenti logiche dell'infrastruttura.



Il nucleo centrale del sistema è rappresentato dal Repository delle Identità digitali (SPID), un sistema che contiene tutte le informazioni relative alle identità dei soggetti, compresi gli attributi identificativi e non identificativi, lo stato dell'identità (attivo, sospeso, revocato), i risultati delle verifiche effettuate, ecc. Fa parte

del Repository anche il modulo di Gestione delle credenziali che si interfaccia con i vari servizi messi a disposizione dal modulo Servizi di CA.

Con il Repository delle Identità digitali interagisce l'Autorità di Registrazione mediante alcuni moduli quali: il modulo di attivazione che effettua la registrazione delle informazioni e la creazione vera e propria dell'Identità digitale SPID ed il modulo di identificazione che si occupa del riconoscimento del soggetto Richiedente. All'interno dell'Autorità di registrazione è inoltre presente un modulo di gestione del ciclo di vita delle Identità digitali. Le funzionalità, a seconda della tipologia, vengono esposte attraverso un'interfaccia web di amministrazione, un portale Self Care ed una serie di web service.
L'Autorità di registrazione si interfaccia con il modulo di Gestione delle credenziali (che dialoga a sua volta con i servizi di CA) per la creazione delle credenziali, per la gestione del ciclo di vita, per l'integrazione con la piattaforma per il devisu online.

L'Autorità di Autenticazione realizza il servizio di autenticazione vero e proprio attraverso una serie di pagine web ed il nucleo centrale di autenticazione rappresentato dal modulo core SAML che implementa il dialogo AuthRequest/AuthResponse con i Service Provider. Anche il modulo di autenticazione si interfaccia con il modulo di Gestione delle Credenziali per la verifica delle credenziali di accesso.

Sono inoltre presenti una serie di componenti di Supporto e Gestione che si occupano di servizi a corredo quali la tracciatura delle operazioni (log), e le notifiche.

È inoltre presente il modulo Interfaccia di Conservazione che si incarica di raccogliere tutte le informazioni importanti e inviarle al servizio di Conservazione Sostitutiva.

Sono infine presenti alcuni moduli che si occupano del monitor delle attività e della sicurezza dei componenti.

5.2. Architettura fisica

Il servizio Private Cloud offerto da InfoCamere mette a disposizione risorse computazionali (CPU, RAM e Spazio Disco) e di networking. Il catalogo prevede diverse tipologie di Hypervisor (Vmware, Microsoft, KVM), di sistema operativo (Microsoft/Linux) e di piattaforme Middleware.

Il servizio SPID InfoCamere è erogato in architettura logica e fisica di alta affidabilità e continuità operativa. Il Data Center è protetto con architetture di Continuous Availability e Disaster Recovery.

In particolare il Data Center primario eroga i servizi di Produzione e di Continuità Operativa ed è interconnesso con il sito di Disaster Recovery mediante linee in fibra ottica 10 Gigabit Ethernet ad alta affidabilità con doppio operatore

Il Data Center primario è situato a Padova, in Corso Stati Uniti, 14.

Il secondo Data Center, situato a Milano, in Via Viserba, 20, funziona come Disaster Recovery Center e come secondo access point di rete.

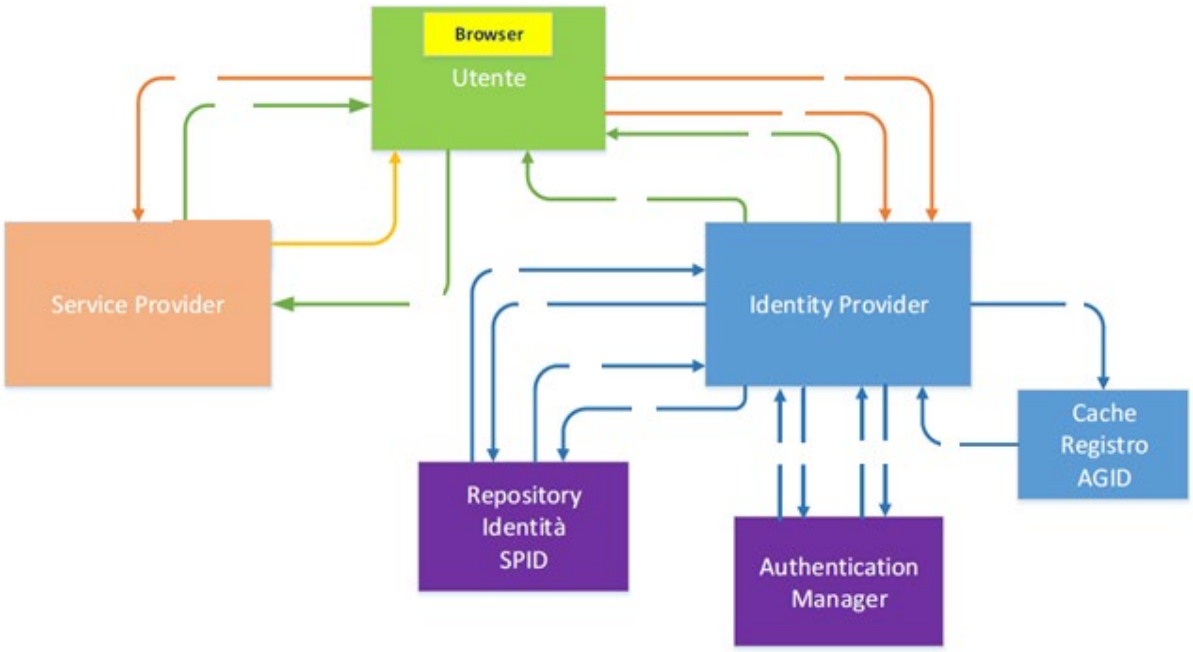
Il sistema di erogazione del servizio SPID è fisicamente e logicamente suddiviso in più livelli per garantire isolamento, sicurezza e modularità.

Il modello Multi-Tier garantisce flessibilità e riutilizzo delle componenti software e, conseguentemente, in presenza di carico, l'adeguamento del servizio andando a scalare solo la parte che necessita di essere rafforzata, lasciando invariate le altre componenti del sistema.

Questo approccio garantisce alla piattaforma di erogazione del servizio SPID caratteristiche di scalabilità, efficienza, performance, adattabilità e resilienza.

5.3. Architettura dei sistemi di autenticazione

La procedura di autenticazione del Titolare avviene attraverso il colloquio di una serie di componenti applicativi rappresentati nel diagramma seguente.



Il soggetto Titolare della Identità digitale richiede l'accesso ad un servizio collegandosi tramite un browser al portale del fornitore dei servizi, e si procede secondo le seguenti fasi:

- il Service Provider sottopone al Titolare il Form tramite il quale quest'ultimo può effettuare la scelta dell'Identity Provider;
- il Titolare sceglie il Gestore della Identità digitale direttamente dall'elenco proposto;
- il Service Provider, tenendo conto della scelta del Titolare, restituisce al browser dello stesso una richiesta di autenticazione (AuthRequest) contenente eventuali attributi associati al profilo del Titolare;
- il browser reindirizza la richiesta di autenticazione all'Identity Provider;
- al fine di verificare che la richiesta provenga da un Service Provider accreditato, all'Identity Provider consulta il Registro AgID presente nella propria cache;
- all'Identity Provider ottiene dal Registro AgID i certificati del Service Provider con i quali verifica l'autenticità del messaggio (che il messaggio appartenga effettivamente a quel Service Provider) e la sua integrità;
- viene interrogato l'Authentication Manager indicandogli il livello SPID richiesto;
- l'Authentication manager risponde con l'elenco delle relative modalità di autenticazione disponibili per il Titolare (nel caso il soggetto abbia, per uno specifico livello di sicurezza, più credenziali di autenticazione);
- l'Identity Provider sottopone al Titolare la pagina Web tramite la quale lo stesso potrà autenticarsi con una delle modalità disponibili;
- il Titolare dimostra la sua identità utilizzando una delle modalità proposte anche avvalendosi di dispositivi di autenticazione (smart card, OTP, ecc.);
- L'Identity Provider delega la procedura di autenticazione all'Authentication Manager;
- l'Authentication manager risponde con l'esito della verifica dell'identità e, in caso di esito positivo, con il codice identificativo SPID;
- l'Identity Provider, ottenuto il codice identificativo SPID ne verifica lo stato di validità (revoca, sospensione) consultando il Repository delle Identità digitali;
- l'Identity Provider, dopo la verifica positiva dello stato dell'Identità digitale, richiede ed ottiene gli attributi indicati nell'AuthRequest;

- l'Identity Provider sottopone il Titolare una pagina Web nella quale sono mostrati gli attributi richiesti dal Service Provider e quelli che gli verranno inviati;
- il Titolare fornisce esplicito consenso per l'invio dei dati;
- l'Identity Provider costruisce l'asserzione SAML e la trasmette, col tramite del browser del Titolare, al Service Provider;
- il Service Provider, riceve l'asserzione SAML creata dall'Identity Provider.

In particolare, l'architettura del sistema di autenticazione è basata principalmente su queste componenti:

Pagine di autenticazione del portale dell'IdP
Il portale dell'IdP è lo strumento che permette l'autenticazione del Titolare SPID sul servizio richiesto.
Le pagine presentano i possibili livelli di autenticazione utilizzabili in base al livello SPID richiesto dal Service Provider. In particolare, ogni Titolare ha la possibilità di autenticarsi con il livello richiesto dal Service Provider o con i livelli superiori (se presenti). Ad esempio, se il Service Provider richiede un livello 1, le pagine di autenticazione offrono la possibilità di autenticarsi con il livello 1, 2, 3 (a condizione che il titolare li abbia attivati), se il Service Provider richiede autenticazione di livello 2, il servizio mette a disposizione l'autenticazione di livello 2 e 3.
Maggiori dettagli sul contenuto, l'organizzazione e l'esperienza d'uso delle pagine di autenticazione InfoCamere sono riportati nella Guida Utente [13].

Modulo di autenticazione
Le pagine si appoggiano a uno specifico modulo che effettua l'autenticazione ed è collegato con i moduli Identità SPID e Gestione Credenziali. Tale modulo verifica:
1. la validità dell'identità SPID: viene verificato che l'identità SPID sia attiva (non sospesa o revocata)
2. la validità delle credenziali: tramite l'ausilio del modulo di Gestione delle Credenziali viene verificato che la credenziale fornita per la transazione sia valida.

Nel caso in cui il Titolare abbia richiesto di ricevere la notifica per ogni accesso, il modulo di autenticazione richiama modulo notifica utenti per l'invio di appositi messaggi via email o sms a seconda delle disposizioni date dal Titolare e memorizzate nel repository SPID.

Registro SPID dell'AgID (cache)
Il Registro SPID contiene le informazioni relative ai soggetti aderenti a SPID e costituisce l'evidenza del cosiddetto "circolo di fiducia" (circle of trust) in esso stabilito.
La relazione di fiducia su cui si basa la federazione stabilita in SPID si realizza per il tramite dell'intermediazione dell'Agenzia per l'Italia Digitale, terza parte garante, attraverso l'adesione dei Gestori dell'Identità digitale, dei Gestori di attributi qualificati e dei fornitori di servizi.
L'adesione a SPID dei Gestori dell'Identità digitale, dei Gestori di attributi qualificati e dei fornitori di servizi, si traduce nella presenza dei loro riferimenti all'interno del Registro SPID gestito dall'Agenzia per l'Italia Digitale.
La consultazione del registro consente agli aderenti a SPID di conoscere tutti i soggetti facenti parte del sistema federato e le loro caratteristiche.
Il modulo di autenticazione recupera le informazioni relative ai servizi erogati in SPID in modalità applicativa secondo i protocolli e le specifiche previsti dalle regole tecniche di cui all'Art 4, comma 2 del DPCM [3].
Inoltre, ai fini dell'ottimizzazione dei servizi, è previsto un meccanismo di caching interno all'Autorità di Autenticazione che permette una replica del registro SPID gestito da AgID.

5.3.1. Notifiche di accesso

Su richiesta del Titolare, il Gestore dell'Identità digitale, comunicherà al Titolare stesso ogni utilizzo delle credenziali di accesso mediante comunicazione a uno degli indirizzi comunicati in fase di registrazione (ad esempio per email).

5.3.2. Codici e formato messaggi di anomalie

Il servizio di autenticazione SPID dell'IdP InfoCamere soddisfa pienamente le specifiche di messaggistica e codifica dei casi di errore previste dalle regole tecniche di cui all'Art 4, comma 2 del DPCM [3] e descritte nella tabella indicata in § APPENDICE A - Codici e formati dei messaggi di anomalia.

5.4. Sistemi di autenticazione e credenziali

5.4.1. Livello di sicurezza 1

Il sistema di Autenticazione proposto per il livello di sicurezza 1 si basa sull'uso di credenziali composte da un singolo fattore (ad es. password).
In particolare, nel rispetto delle modalità attuative per lo SPID che impongono di adottare regole per ottenere password complesse difficilmente attaccabili e considerando le policy aziendali InfoCamere, vengono rispettati le raccomandazioni baseline per l'ottenimento di password complesse e difficilmente attaccabili:

a. lunghezza minima di otto caratteri;
b. lunghezza massima di venti caratteri;
c. deve contenere almeno una maiuscola e una minuscola;
d. deve contenere almeno un numero;
e. deve contenere almeno un carattere speciali ad es #, §, % ecc;
f. non deve contenere più di due caratteri identici consecutivi;
g. non deve contenere il carattere spazio vuoto;
h. non deve contenere una data (formati ddMMyyyy e ddMMyy, ma parametrizzato).

Il Repository SPID inoltre impone i seguenti meccanismi di protezione:

- Fissa la scadenza delle password non oltre i 180 giorni e ne impedisce il riuso o che abbiano elementi di similitudine prima di 5 variazioni o comunque non prima di 15 mesi.
- Implementa una procedura di sollecito con la quale invita il Titolare a modificare la Password secondo le raccomandazioni sopra indicate.

5.4.2. Livello di sicurezza 2

Il sistema di Autenticazione Forte proposto per il livello di sicurezza 2, in aggiunta all'uso di username e password così come previste da § 5.4.1, è arricchito dall'adozione di un "Identification Server" OATH Compliant che consente di utilizzare i più disparati sistemi presenti in commercio.
Nella soluzione proposta verranno utilizzati, a seconda del caso d'uso, vari meccanismi: OTP mobile, OTP via SMS.

L'OTP via SMS è un sistema di autenticazione OTP destinato a essere utilizzato dagli utenti che non possiedono uno smartphone ma un semplice cellulare anche di vecchia generazione. All'atto dell'autenticazione l'Utente riceverà un SMS sul proprio cellulare con il codice OTP.
La OTP è un codice di 6 cifre decimali.

L'OTP Mobile è un'applicazione per smartphone installabile sui più comuni cellulari. Consiste in un'applicazione a eventi che, una volta inizializzata con il codice di attivazione fornito in fase di registrazione, genera one time password su richiesta.
In questo caso il secondo fattore ("something you have") è rappresentato dal dispositivo sul quale si trova installato il software di generazione OTP. La OTP è generata con un algoritmo conforme allo standard OATH ed ha una lunghezza di almeno 6 cifre decimali.

5.4.3. Livello di sicurezza 3

Il sistema di Autenticazione Forte proposto per il livello di sicurezza 3 si basa, così come previsto dall'art 6 del DPCM [3], sull'utilizzo di certificati digitali le cui chiavi private sono custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 2 del Regolamento (UE) n. 910/2014 [1].

Tra questi dispositivi sono compresi:

- Carta Nazionale dei Servizi;
- Smart card conformi ai requisiti di cui all'Allegato 2 del Regolamento (UE) n. 910/2014 [1] da parte dell'Organismo di Certificazione della sicurezza informatica (OCSI) o da altro organismo all'uopo designato da un altro Stato membro e notificato;
- Hardware Security Modules (HSM) per i quali sia stata riconosciuta la conformità ai requisiti di cui all'Allegato 2 del Regolamento (UE) n. 910/2014 [1] da parte dell'Organismo di Certificazione della

sicurezza informatica (OCSI) o da altro organismo all'uopo designato da un altro Stato membro e notificato.

5.4.4. Misure anticontraffazione

Le misure anticontraffazione sviluppate da InfoCamere mirano a prevenire il verificarsi del furto d'identità, inteso sia come occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità di un altro soggetto in vita o deceduto e sia come occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi a un altro soggetto.
Qualunque sia il livello SPID al quale si collochi una credenziale richiesta, l'Identity Provider InfoCamere applica come prima misure anticontraffazione la verifica delle informazioni fornite attraverso accertamenti effettuati tramite fonti autoritative istituzionali, in grado di dare conferma della veridicità dei dati raccolti.

5.4.4.1. Livello 1

A questo livello è associata una credenziale composta da una password, la cui principale misura anticontraffazione è rappresentata dalla riservatezza della conservazione della stessa da parte del Titolare dell'Identità digitale.

5.4.4.2. Livello 2

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. Viene adottato da InfoCamere un sistema di OTP - One Time Password via SMS ed un sistema di OTP Mobile basato su un'applicazione per smartphone, installabile sui più comuni cellulari, che assicura una sicurezza maggiore, in quanto si suppone che il Titolare, oltre a conoscere la password, abbia l'accesso esclusivo al numero di telefono cellulare verificato durante la fase di sottoscrizione.

In particolare si precisa che tutte le tipologie di credenziali fornite permettono il soddisfacimento dei più stringenti requisiti previsti dagli standard di sicurezza adottati in ambito di firma remota con credenziali di tipo OTP, ovvero:
1. Il codice OTP non deve essere duplicabile.
2. Il codice OTP deve avere un meccanismo in grado di rilevare o contrastare attivamente i tentativi di manomissione.
3. Ogni codice OTP può essere identificato in modo univoco.

5.4.4.3. Livello 3

Le credenziali di livello 3 sono basate sull'uso di certificati digitali le cui chiavi private sono custodite in dispositivi che soddisfano i requisiti di cui all'Allegato 2 del Regolamento (UE) n. 910/2014 [1].

Ognuno dei dispositivi indicati nel paragrafo 5.4.3 possiede un rapporto di conformità ai requisiti di cui all'Allegato 2 del Regolamento (UE) n. 910/2014 [1] emesso dal pertinente organismo pubblico o privato designato dallo Stato membro e opportunamente notificato.

5.5. Tracciatura degli accessi

I sistemi che offrono ed erogano il servizio SPID possiedono livelli di protezione logica estremamente elevati. La medesima collocazione fisica di tali sistemi garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali.
Tutti gli accessi ai sistemi sono controllati e registrati.

5.5.1. Accessi servizio SPID

Prima di qualsiasi interazione con il sistema IdP, l'utente privilegiato (es. operatore, amministratore, ecc.) deve dichiarare e dimostrare al sistema la propria identità (associata ad una "utenza") mediante sistemi di autenticazione (es. password, smart card, ecc.) caratterizzati da un livello di sicurezza commisurato alla sensibilità dei dati richiesti e/o delle operazioni richieste al sistema. Ad ogni persona (interna o esterna) viene assegnata un'utenza personale e univoca.

5.5.2. Tracciature accessi di autenticazione utenti

A valle di ogni autenticazione utente, l'IdP InfoCamere registra sui propri sistemi un log denominato tracciatura di accesso al servizio di autenticazione e contenente le seguenti informazioni:

- Indirizzo IP pubblico di provenienza
- Identificativo univoco dell'utente
- Operazione effettuata
- Riferimento temporale dell'operazione

Tutti i dati sopra elencati saranno mantenuti dal Gestore nel rispetto del Codice della Privacy [12] e del Regolamento (UE) n. 910/2014 [1].

Oltre la tracciatura degli accessi vengono tracciate tutte le evidenze documentali poste a corredo della richiesta dell'identità, che vengono poi conservate a norma nel sistema di conservazione elettronica documentale di InfoCamere secondo le procedure descritte nel documento specifico di InfoCamere.

Quanto sopra è parte di un meccanismo che permette di garantire la resilienza, l'integrità e l'autenticità delle informazioni relative ai log di accesso anche ai fini dell'opponibilità ai terzi. Questo fa sì che il log prodotto rappresenti un log certificato.

Secondo quanto definito dall'art. 24 del Regolamento AgID [5], InfoCamere mantiene il Registro delle transazioni che contiene i tracciati delle richieste di autenticazione dell'Utente 24 mesi.

L'accesso in lettura e scrittura ai sistemi che custodiscono le tracciature è garantito al solo personale tecnico dell'IdP nel rispetto delle policy aziendali.
In caso di richiesta di accesso ai log da parte delle autorità, le modalità di acquisizione delle tracciature prevedono il coinvolgimento tecnico dell'IdP e il recupero di una versione dei log relativamente piccola, indicizzata e adatta a una rapida identificazione di Titolare, operazione e riferimento orario.
Rimane sempre garantita la possibilità di accesso a una versione più ricca di informazioni.

6. Operatività

Questa sezione descrive le modalità con le quali opera il Gestore dell'Identità digitale e in particolare le funzioni del personale addetto al servizio in relazione alle modalità di adesione a SPID e alla richiesta dell'Identità digitale, alla verifica dell'identità del Richiedente, al rilascio e gestione delle Identità digitali e alle modalità di comunicazione con il Richiedente l'Identità digitale ovvero con il Titolare dell'Identità digitale.

6.1. Funzioni del personale addetto al servizio di gestione delle identità digitali

Tutto il personale di InfoCamere S.C.p.A. è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità.

Il personale addetto alla gestione di SPID è dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi SPID, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore e della dimestichezza con procedure di sicurezza appropriate che gli consentono di garantire il rispetto delle norme del CAD [2].

La gestione di SPID, nel rispetto dell'art. 2 del Regolamento accreditamento AgID [6], prevede le seguenti figure responsabili:

a) responsabile della sicurezza;
b) responsabile della conduzione tecnica dei sistemi;
c) responsabile delle verifiche e delle ispezioni;
d) responsabile delle attività di verifica dell'identità del soggetto richiedente e della gestione e conduzione del servizio;
e) responsabile dell'istruzione dei soggetti coinvolti nelle diverse attività necessarie alla conduzione e gestione del servizio;
f) responsabile per l'aggiornamento della documentazione depositata presso l'Agenzia;
g) referente per la protezione dei dati personali.

6.2. Richiesta dell'identità digitale

InfoCamere S.C.p.A., in qualità di IdP, rilascia le identità digitali su richiesta di un Utente secondo quanto previsto dall'art. 7 del DPCM [3]. L'istanza viene effettuata attraverso la presentazione di una richiesta di adesione che contiene tutte le informazioni necessarie per l'identificazione del Richiedente.

La richiesta può essere effettuata *online* o da sportello.

6.2.1. Richiesta da sportello dell'identità SPID (de *visu*)

La richiesta dell'identità SPID viene effettuata dal richiedente presso un soggetto incaricato dal Gestore dell'Identità digitale denominato Ufficio di Registrazione o Incaricato alla Registrazione il quale può essere persona fisica o giuridica.

In questa modalità è prevista la presenza fisica del soggetto Richiedente dinanzi a un incaricato dell'Ufficio di Registrazione o davanti a ad un Incaricato alla Registrazione.

Si precisa che l'Ufficio di Registrazione o l'Incaricato alla Registrazione (IR) operano in forza e previa stipula di specifica Convenzione con InfoCamere; in detta Convenzione tali soggetti indicano anche il personale di cui si intendono avvalere per la sua esecuzione: detto personale, che dovrà operare nel contesto delle pratiche operative di identificazione e registrazione, è tenuto a sottoscrivere un mandato di accettazione di incarico SPID.

L'autorizzazione e successivamente la qualificazione degli operatori degli Uffici di Registrazione e degli IR come abili alle operazioni di identificazione, registrazione e rilascio, avviene mediante un corso di formazione e superamento di una verifica erogata attraverso una piattaforma online.

A seguito della firma della convenzione da parte dei rispettivi legali rappresentanti del certificatore e degli Uffici di Registrazione o degli IR, e previa qualificazione degli operatori, il Gestore dell'Identità digitale rende disponibili agli Uffici di Registrazione o agli IR stessi, gli strumenti telematici sicuri per consentire lo svolgimento delle attività di identificazione e registrazione.

I privilegi di accesso agli strumenti telematici sicuri e le operazioni degli operatori degli Uffici di Registrazione e degli IR sono sotto il costante controllo del Gestore dell'Identità digitale.

6.2.1.1. Modalità di identificazione

L'identificazione *de visu* avviene mediante una rete di soggetti che hanno aderito alla Convenzione con InfoCamere dislocati su tutto il territorio nazionale ed è prevista la presenza fisica del soggetto richiedente dinanzi a un incaricato addetto all'identificazione.

Al Richiedente vengono messi a disposizione, anche mediante indicazione del luogo in cui è possibile reperire la documentazione:

- le informazioni inerenti ai rischi derivanti dal possesso dell'Identità digitale SPID, le cautele e le contromisure adottabili dagli stessi;
- l'informativa relativa al trattamento dei dati personali per l'adesione al servizio ai sensi del Regolamento UE 2016/679 [11];
- le Condizioni Generali di Contratto del Servizio SPID;
- il presente Manuale Operativo;
- la Guida Utente.

Il Richiedente riceve via mail, oltre ai documenti di cui sopra anche il Modulo di adesione di firma digitale *one shot* utilizzata al fine della sottoscrizione del Modulo di adesione al Servizio SPID.

Il Titolare potrà in qualsiasi momento prendere visione della documentazione di cui sopra nel portale SPID alla sezione documentazione.

Durante il processo di rilascio l'operatore effettua un riconoscimento *de visu* del Richiedente e ne verifica l'identità facendosi consegnare ed effettuando la copia di un documento di riconoscimento, munito di fotografia, rilasciate da un'Amministrazione dello Stato, secondo quanto previsto dall'art 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445, tra i quali:

- Carta d'Identità
- Passaporto
- Patente di guida

In particolare, durante la fase di identificazione a vista del soggetto richiedente, il soggetto incaricato procede con l'acquisizione di tutti i dati necessari per la registrazione sul sistema e per la compilazione del Modulo di adesione al Servizio SPID.

In questo caso:

a) se il soggetto richiedente è una persona fisica, dovrà essere esibito un valido documento di riconoscimento;
b) se il soggetto richiedente è una persona giuridica, l'operatore verificherà la visura camerale attestante i poteri di rappresentanza conferiti alla persona fisica che materialmente presenta l'istanza che a sua volta è tenuta a esibire un valido documento di riconoscimento.

L'operatore che effettua l'identificazione verifica l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità rilasciato da un'Amministrazione dello Stato, munito di fotografia recente riconoscibile del richiedente e firma autografa dello stesso, e controlla la validità del codice fiscale verificando il relativo tesserino o la tessera sanitaria o il certificato di attribuzione della stessa o del codice fiscale.

Se i documenti esibiti dal Richiedente risultano privi, in tutto o in parte, dei requisiti di cui sopra, l'operatore ne esclude l'ammissibilità ed il processo di iscrizione viene sospeso o bloccato fino alla esibizione di documenti validi ed integri.

Inoltre, dovranno essere forniti un indirizzo di posta elettronica e un recapito di telefonia mobile che verranno entrambi verificati. I riferimenti forniti, indirizzo mail e recapito di telefonia, saranno opportunamente convalidati tramite procedure di verifica.

Per ciò che concerne le credenziali SPID, l'utente durante il processo di riconoscimento, avrà la possibilità di scegliere una passphrase che sarà utilizzata per decodificare il file pdf che riceverà alla chiusura delle operazioni da parte dell'operatore. Tale file pdf conterrà i dati di accesso al portale SelfCare.

6.2.1.2. Documentazione da presentare allo sportello

Per le persone fisiche sono considerate obbligatorie le seguenti informazioni:
a. cognome e nome;
b. sesso, data, luogo e nazione di nascita, e domicilio;
c. codice fiscale o certificato di attribuzione dello stesso;
d. estremi della tessera sanitaria o certificato di attribuzione della stessa (se prevista - es. cittadino straniero non prevista);
e. estremi del documento di riconoscimento presentato per l'identificazione;
f. gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM [3].

Sono considerate obbligatorie per le persone giuridiche le seguenti informazioni:
1. cognome e nome (legale rappresentante);
2. sesso, data, luogo e nazione di nascita e domicilio (legale rappresentante);
3. codice fiscale o certificato di attribuzione dello stesso (legale rappresentante);
4. estremi della tessera sanitaria o certificato di attribuzione della stessa (se prevista - es. cittadino straniero non prevista) (legale rappresentante);
5. denominazione/ragione sociale;
6. codice fiscale azienda o P.IVA (se uguale al codice fiscale);
7. sede legale;
8. visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società;
9. estremi del documento di identità utilizzato dal rappresentante legale;
10. gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM [3].

6.2.2. Identificazione informatica mediante TS-CNS, CNS o firma digitale

Il Richiedente accede al portale del Gestore dell'Identità digitale e richiede un'Identità digitale secondo il flusso di seguito descritto:
1. Pagina di selezione della modalità di identificazione in cui l'Utente potrà scegliere tra le seguenti:
    a. informatica via CNS/TS-CNS/CIE;
    b. acquisizione del Modulo di adesione al Servizio SPID attraverso sottoscrizione con Firma Digitale;
    c. a vista da remoto per riconoscimento via webcam.

2. Al Richiedente vengono messi a disposizione sul portale:
    a. le informazioni inerenti ai rischi derivanti dal possesso dell'Identità digitale SPID, le cautele e le contromisure adottabili dagli stessi;
    b. l'informativa relativa al trattamento dei dati personali per l'adesione al servizio ai sensi del Regolamento UE 2016/679 [11];
    a. le Condizioni Generali di Contratto del Servizio SPID;
    b. il presente Manuale Operativo;
    c. la Guida Utente.

Il Titolare potrà in qualsiasi momento prendere visione della documentazione di cui sopra nel portale SPID alla sezione documentazione.

6.2.2.1. Modalità di identificazione

Così come previsto dall'Art. 7 del DPCM [3] e dalle procedure di richiesta del Gestore dell'Identità digitale, l'identità del soggetto richiedente può essere verificata anche attraverso procedure di identificazione informatica basate su documenti digitali di identità (quali CNS, TS-CNS, CIE) o su acquisizione del Modulo di adesione al Servizio SPID sottoscritto con firma elettronica qualificata o con firma digitale.
In particolare:

- Nel caso di scelta dell'identificazione via CIE, CNS o TS-CNS verrà richiesto all'Utente di utilizzare uno di questi dispositivi e di autenticarsi per completare il riconoscimento.
  Verrà eseguita la verifica di alcuni dati attraverso le fonti autoritative, verrà salvata la tracciatura dei log (client authentication) e versata in conservazione come previsto dal Regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014) [5].
- Nel caso in cui il richiedente abbia un certificato di firma verrà richiesto di compilare un Modulo di adesione al Servizio SPID in formato elettronico sottoscritto con firma elettronica qualificata o digitale. Anche in questo caso il Gestore della Identità digitale considera effettuata la verifica dell'identità del soggetto richiedente per effetto e in conseguenza della verifica dell'identità già espletata dal Prestatore di Servizi Fiduciari che ha rilasciato certificato di firma.

I possessori di TS-CNS o di CNS o di CIE o di certificati di firma digitale rilasciate da Pubbliche Amministrazioni, Camere di Commercio, ecc. sono stati già sottoposti a una fase di riconoscimento della propria identità. Tale identificazione può essere mutuata per il rilascio dell'Identità digitale. Questo permette di costruire procedure informatiche mediante le quali il richiedente può ottenere la propria Identità digitale in completa autonomia.

6.2.2.2. Inserimento dati

Il Titolare avrà a disposizione il form con richiesta di inserimento dei seguenti dati.

Dati di accesso

- username
- password
- conferma password

Nel caso in cui la username fornita sia già associata a un'Identità digitale il sistema ne dà evidenza e offre la possibilità di inserirne una nuova.
Nel corso dell'inserimento dei dati verrà effettuata una verifica sulla correttezza della password prescelta e sarà anche possibile generarla casualmente.
Questi accorgimenti garantiscono che la password rispetti le regole di complessità previste dalle regole attuative e descritte in § 5.4.1

Dati di contatto

- indirizzo email
- numero di cellulare

È possibile modificare l'indirizzo mail e/o il numero di cellulare, se ci si accorge di aver fornito un indirizzo e/o un numero sbagliato.

Si precisa che, in base alla modalità di riconoscimento, il sistema precarica sul form i dati acquisiti direttamente dai dispositivi utilizzati.

Dati personali

- Codice fiscale
- Nome
- Cognome
- Sesso
- Data nascita

- Luogo nascita (Nazione, Provincia, Comune)
- Numero di Tessera Sanitaria e data di scadenza
- Email PEC

Dati aziendali (per persona giuridica)
- Ragione Sociale
- Partita IVA
- Codice fiscale azienda
- Visura Camerale o documento equivalente (file da caricare)
- Luogo della sede legale (Nazione, sede, comune, CAP, indirizzo)

Dati di domicilio
- Luogo domicilio (Nazione, Provincia, Comune)
- Indirizzo domicilio (via, civico, CAP)

Documento di identità
- Tipo di documento
- Numero documento
- Data emissione
- Data scadenza
- Ente emittente

Al termine del flusso descritto si ha un un'Identità digitale creata, ma non attiva.

6.2.3. Identificazione attraverso sessione audio-video (identificazione con webcam)

La procedura di identificazione attraverso la sessione audio video consente all'operatore o incaricato del Gestore dell'Identità digitale di identificare in maniera certa i Richiedenti l'Identità digitale mediante l'ausilio di strumenti di registrazione audio/video.
Così come previsto dai regolamenti di cui all'Art. 4 comma 2 del DPCM [3], ed in particolare dal Regolamento AgID [5] l'identificazione da remoto avviene in una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'Identità digitale da parte del Richiedente della stessa e perciò devono essere rispettate le condizioni di seguito illustrate.

Le immagini video sono a colori e tali da consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini. L'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi. La sessione audio/video, che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'Identità digitale, deve essere effettuata in ambienti privi di particolari elementi di disturbo e che possano condurre all'identificazione di possibili dati sensibili del Richiedente e dell'operatore.

Il Gestore dell'Identità digitale si assume la responsabilità della valutazione in merito alla sussistenza delle condizioni suddette, e l'operatore preposto all'attività può quindi sospendere o non avviare il processo di identificazione nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a consentire la verifica dell'identità del Richiedente.

In una prima fase, il richiedente inserirà le informazioni necessarie per procedere al video riconoscimento. Tale informazioni, includono:

1. l'inserimento dei dati personali:
   - Obbligatori quali
     - Nome;
     - Cognome;
     - Codice fiscale;
     - Data di Nascita;
     - Sesso;
     - Nazione di Nascita;
     - Provincia di Nascita;

    - Comune di Nascita;
    - Cittadinanza;
  - non obbligatori quali
    - PEC;
2. la scelta di una username e una password;
3. l'inserimento e la verifica dei contatti quali mail e numero di cellulare
4. l'inserimento dei dati di domicilio e di residenza, quali
   - Nazione;
   - Provincia;
   - Comune;
   - Cap;
   - Tipo indirizzo;
   - Indirizzo;
   - Numero.
5. l'inserimento dei dati della Tessera Sanitaria e di un documento di riconoscimento a scelta tra Carta D'identità, Patente Di Guida, Passaporto.

Nella seconda fase, l'Operatore seguirà delle particolari procedure volte a garantire l'autenticità della richiesta del corso della sessione in videoconferenza. Di seguito è descritto il flusso principale per l'espletamento dell'identificazione attraverso sessione audio-video:

- Prima di collegarsi alla sessione di video riconoscimento, il Richiedente deve assicurarsi di avere a disposizione il documento di riconoscimento utilizzato in fase di richiesta (carta d'identità, patente di guida, passaporto) e la tessera sanitaria o certificato di attribuzione della stessa o il tesserino del codice fiscale o certificato di attribuzione dello steso.
- Previo appuntamento con l'operatore, il Richiedente, all'ora e data stabilite, cliccando il link ricevuto nella mail a termine della richiesta online, si connette alla piattaforma di video riconoscimento ed effettua le verifiche del funzionamento di videocamera e microfono.
- Dopo la verifica di microfono e videocamera, il sistema indirizza il Richiedente in una pagina di Benvenuto dove il medesimo può iniziare la sessione di video riconoscimento.
- Una volta connessi: l'utente segue le istruzioni dell'operatore per il video riconoscimento, ovvero:
  - viene chiesto il consenso alla registrazione;
  - vengono acquisiti il documento di riconoscimento dell'utente e la tessera sanitaria per una verifica dell'identità del soggetto richiedente.

  Mentre, l'operatore seguirà una procedura che dovrà prevedere l'esecuzione di azioni o richiesta di informazioni volte a rafforzare il processo di verifica dell'identità del richiedente.
- Terminata la fase di identificazione, l'operatore ricorda al Richiedente che sarà necessario l'accettazione delle successive condizioni contrattuali e la firma digitale in modalità *oneshot* dei contratti. Se necessario l'operatore di riconoscimento chiederà un ulteriore supporto telefonico per l'accettazione e la firma dei contratti. Successivamente l'Identità digitale sarà attivata dopo la verifica sulle fonti autoritative dei documenti presentati e il Richiedente potrà effettuare l'autenticazione in autonomia.

La Sessione audio-video non prevede una soluzione di continuità.

6.3. Procedura per il recupero del numero di cellulare da associare all'identità digitale

Il telefono cellulare costituisce, nell'ambito dello SPID, un importante fattore di autenticazione. Può verificarsi il caso che lo stesso numero di telefono sia già in uso per una diversa Identità digitale nell'ambito dello stesso Gestore dell'Identità digitale.
Al fine di evitare tale circostanza, in ottemperanza all'Avviso AgID n. 31 del 05/10/2020, l'operatore dell'IdP InfoCamere effettua il controllo dell'univocità del numero in fase di registrazione dei dati del Richiedente sia in modalità *online* che *de visu*. Inoltre, il sistema verifica l'univocità del numero di cellulare anche nella fase di gestione delle credenziali all'atto della modifica del cellulare da parte del Titolare.

6.4. Verifica degli attributi associati all'identità digitale

Completata la fase di registrazione e riconoscimento, così come previsto dal Regolamento AgID [5] e dagli ulteriori regolamenti di cui all'Art 4 comma 2 del DPCM [3], il sistema effettua una verifica degli attributi identificativi forniti dal Richiedente (anche detta 'identità dichiarata').
L'Identità digitale è rappresentata mediante un insieme di attributi intesi come informazioni o qualità di un soggetto utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari. Tali attributi sono costituiti da:

- **Attributi identificativi**, quali il nome, cognome, data di nascita, sesso ovvero ragione sociale o denominazione sociale, sede legale, codice fiscale, partita iva, visura camerale e gli estremi del documento di identità utilizzato ai fini dell'identificazione (lettera c) del comma 1 dell'art.1 del DPCM [3]);
- **Attributi non identificativi (o secondari)**, quali il numero di cellulare, indirizzo di posta elettronica, domicilio fiscale, nonché eventuali altri attributi individuati dall' AgID (lettera d) del comma 1 dell'art.1 del DPCM [3])
- **Codice identificativo**: come specificato alla lettera d) del comma 1 dell'art. 1 del DPCM [3] e valorizzato in aderenza ai regolamenti di cui all'art. 4 comma 2 del DPCM [3];
- **Identificativo Utente**: attributo corrispondente allo username prescelto dal Titolare.

6.4.1. Verifica degli attributi identificativi (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.
L'accesso alle fonti autoritative disponibili da parte dei gestori dell'identità ai fini dell'attività di verifica è effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM [3] e, nei casi in cui le informazioni necessarie non siano accessibili per mezzo dei servizi convenzionati, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445. Per quanto riguarda la verifica sulla visura camerale, l'IdP InfoCamere effettua il controllo attraverso sistemi che acquisiscono le informazioni dal Registro Imprese.
Il rilascio dell'Identità digitale è subordinato al superamento di tali verifiche.

6.4.2. Verifica degli attributi secondari

La verifica degli attributi non identificativi (secondari) viene effettuata durante la fase di richiesta dell'Identità digitale.
In particolare, la verifica dell'indirizzo mail avviene attraverso l'utilizzo di un link dedicato presente nella comunicazione che il Richiedente riceve tramite mail. Nella stessa comunicazione il Richiedente riceve un codice di verifica di 6 cifre che rappresenta parte del codice di emergenza.
La verifica del cellulare avviene attraverso l'inserimento di un codice numerico di 6 cifre ricevuto tramite SMS che rappresenta la seconda parte del codice di emergenza. Il codice di emergenza è utile al Titolare per effettuare alcune operazioni sul ciclo di vita dell'Identità digitale.

6.5. Attivazione dell'Identità digitale

Le credenziali rilasciate al Richiedente, associate all'identità e al livello SPID richiesti saranno consegnate in modalità "sospesa".

Solo dopo aver effettuato l'iter completo, cioè dopo aver completato l'identificazione, le verifiche delle fonti autoritative e la conservazione a norma della documentazione fornita, l'Identità digitale e le relative credenziali di accesso potranno essere attivate.

Al Richiedente verrà inviata opportuna notifica dell'avvenuta attivazione dello SPID di livello di sicurezza 1, mediante l'email fornita in fase di richiesta.

Si ricorda che il soggetto può richiedere uno dei livelli di sicurezza SPID corrispondenti ad analoghi livelli previsti dallo standard ISO/IEC DIS 29115, ovvero:

- Livello 1 (corrispondente al LoA2 dell'ISO-IEC 29115): garantisce un buon grado di affidabilità. 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, ha un basso impatto per le attività del cittadino/impresa/amministrazione;
- Livello 2 (corrispondente al LoA3 dell'ISO-IEC 29115): garantisce un alto grado di affidabilità. 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 può provocare un danno consistente;
- Livello 3 (corrispondente al LoA4 dell'ISO-IEC 29115): garantisce un altissimo grado di affidabilità. 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.

In particolare i livelli di sicurezza richiedono i seguenti fattori di accesso:

- Il primo livello (o a singolo fattore) permette di accedere ai servizi online attraverso un nome Utente e una password scelti dall'Utente.
- Il secondo livello (o a due fattori) – necessario per servizi che richiedono un grado di sicurezza maggiore - permette l'accesso attraverso un nome Utente e una password scelti dall'Utente, più la generazione di un codice temporaneo di accesso (one time password), fornito attraverso sms o con l'uso di un app (fornita dal Gestore di Identità digitale) fruibile attraverso un dispositivo, come ad esempio smartphone o tablet.
- Il terzo livello (o a due fattori basato su certificati digitali) di sicurezza SPID, oltre al nome Utente e la password, richiede un supporto fisico particolare che gestisce delle chiavi crittografiche. Tale supporto può essere un token DDNA o un dispositivo per la firma digitale remota (HSM).

Credenziali SPID 1

Nel caso di credenziali di primo livello, il Titolare può da subito utilizzare la propria Identità digitale, come descritta in precedenza. Tale credenziale ha durata 2 anni.

Credenziali SPID 2

Relativamente alle credenziali di secondo livello, il Titolare può inoltre richiedere l'attivazione della credenziale:

1) autonomamente sul pannello di Self Care, accedendo nella sezione riservata alla gestione delle credenziali. In questa sezione il Titolare riceve, tramite sms o APP, il codice di verifica che andrà inserito nel portale, l'OTP tramite sms o APP, per la sincronizzazione che dovrà anch'esso essere inserito nel portale. A questo punto la credenziale di livello 2 è attiva.
2) allo sportello, tramite il sistema interno a InfoCamere con il codice di verifica del cellulare del Titolare e l'OTP, tramite sms o APP, che dovranno essere inseriti nel portale .

Tale credenziale ha durata 2 anni.

Credenziali SPID 3

Le credenziali di terzo livello possono essere ottenute configurando in tal senso la propria credenziale, utilizzando la modalità da sportello e successiva attivazione in modalità *online* autonomamente sul pannello di Self Care del portale SPID. Tale credenziale ha durata 2 anni.

7. Gestione delle Identità digitali

Il Gestore dell'Identità digitale garantisce un aggiornamento tempestivo delle Identità digitali a seguito di richieste da parte del Titolare o all'occorrenza di particolari eventi.

Il Titolare, da parte sua, ha l'obbligo di informare tempestivamente il Gestore dell'Identità digitale di ogni variazione degli attributi previamente comunicati. Oltre alle modifiche degli attributi il Titolare potrà effettuare il recupero della username e della password nel caso ne abbia perso memoria nel pannello di Self Care.

Si ricorda che il Titolare è tenuto ad aggiornare la propria password trascorsi 180 giorni dalla creazione ovvero ultima variazione.

7.1. Conservazione a norma dati raccolti

I dati personali raccolti durante le fasi di registrazione verranno trattati e conservati nel rispetto della normativa vigente in materia di tutela dei dati personali (Regolamento UE 2016/679 [9]).

I dati verranno conservati per un periodo non inferiore a 20 anni dalla scadenza, revoca o disattivazione dell'Identità digitale. Il Gestore dell'Identità digitale conserverà le suddette informazioni per tutta la durata contrattuale, al termine della quale le invierà ad AGID o ad altro ente da essa incaricato.

Il processo di registrazione dei documenti completa la fase di rilascio di un'Identità digitale.
La documentazione da conservare include le informazioni e i documenti che sono stati raccolti nel corso dell'attività di registrazione. I Gestori dell'Identità digitale, al fine di poter documentare la corretta esecuzione dei precedenti processi relativi all'attività di rilascio di una identità, conservano 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 de visu: copia per immagine di tutta la documentazione esibita (documento d'identità e codice fiscale o tessera sanitaria o certificati di attribuzione per persone fisiche, procura per persone giuridiche) e modulo di richiesta su supporto cartaceo sottoscritto in modalità autografa;
2) nel caso di 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;
3) nel caso di identificazione informatica: log della transazione contestualizzato alla specifica richiesta di rilascio dell'Identità digitale;
4) nel caso di firma elettronica qualificata o digitale: Modulo di adesione al Servizio SPID in formato digitale sottoscritto digitalmente.

In merito al processo di verifica devono essere conservati i riscontri ottenuti a seguito degli accessi alle fonti autoritative.
Tutta la documentazione inerente alla creazione e al rilascio di una Identità digitale deve essere conservata ai sensi dell'articolo 7, commi 8 e 9, del DPCM [3].

7.2. Gestione del ciclo di vita

Le Identità digitali rilasciate hanno un ciclo di vita che si articola nei seguenti processi:

a) gestione degli attributi;
b) sospensione e revoca dell'Identità digitale;
c) gestione del ciclo di vita delle credenziali che si articola in:
    1. sospensione e revoca delle credenziali;
    2. rinnovo e sostituzione delle credenziali.

7.2.1. Gestione degli attributi

Il Titolare è tenuto a mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore dell'Identità digitale, i contenuti degli attributi identificativi di seguito elencati.

a) Per le persone fisiche:
    1. estremi del documento di riconoscimento e relativa scadenza;

2. contatti del Titolare: telefono cellulare, indirizzo email
3. tessera Sanitaria, tesserino codice fiscale
4. domicilio (Nazione, Provincia, Comune, indirizzo, CAP, civico)

a) Per le persone giuridiche:
1. indirizzo sede legale
2. codice fiscale o P.IVA (nei rari casi di variazione a seguito di particolari mutazioni societarie)
3. rappresentante legale della società
4. contatti del rappresentante: telefono cellulare, indirizzo email
5. domicilio del rappresentante (Nazione, Provincia, Comune, indirizzo, CAP, civico)

Il Titolare, in caso di dichiarazioni non fedeli o mendaci assume le responsabilità previste dalla legislazione vigente.

Le modalità operative per gli aggiornamenti sono rese possibili attraverso una sezione web dedicata del Gestore delle Identità digitali "Self Care" accessibile mediante l'Identità digitale in possesso del Titolare. Maggiori informazioni sono riportate nella Guida Utente [13].

A ogni variazione da operare sugli attributi relativi a una identità, il Gestore dell'Identità digitale, a seguito di una variazione dei contatti del Titolare (telefono cellulare e/o indirizzo email), verifica ed esegue gli opportuni controlli prima di aggiornare i dati inseriti dal Titolare e l'aggiornamento viene notificato utilizzando un attributo secondario funzionale alle comunicazioni (ad esempio l'indirizzo email e/o il cellulare in base alla modifica effettuata).

7.2.2. Sospensione e Revoca dell'Identità

La sospensione di un'Identità digitale ne comporta la disattivazione temporanea, e la medesima non potrà essere utilizzata durante il periodo di sospensione. Un'Identità digitale sospesa può essere riattivata o revocata al termine del periodo di sospensione.
La revoca è il processo che annulla definitivamente la validità delle credenziali.

Prima di descrivere le modalità operative per gestire la sospensione o la revoca di un'Identità digitale si precisa che:
- la sospensione di un'Identità digitale causa una disattivazione temporanea delle credenziali associate;
- la sospensione dura fino a quando l'Identità digitale non viene riattivata o definitivamente revocata;
- la riattivazione consiste nel rendere di nuovo utilizzabili le credenziali precedentemente sospese;
- la revoca rende inutilizzabili per sempre le credenziali digitali.

7.2.2.1. Revoca da parte del Titolare

Il Titolare può richiedere immediatamente la revoca della propria identità SPID nel momento in cui accerti il venir meno delle caratteristiche di riservatezza e segretezza delle proprie credenziali, ivi compresi i casi di furto e di smarrimento delle credenziali e ha la facoltà di richiedere in ogni momento, senza necessità di motivazione, la revoca della propria Identità digitale.

Per richiedere la revoca dell'Identità digitale il Titolare può accedere a una sezione dedicata sul portale SPID di InfoCamere e disporre di tutte le informazioni necessarie per effettuare la richiesta che può avvenire attraverso l'indirizzo PEC che InfoCamere mette a disposizione:
- via PEC all'indirizzo blocco.spid@pec.infocamere.it, indicando il motivo della richiesta e allegando il modulo di "RICHIESTA REVOCA/SOSPENSIONE" sottoscritto con firma digitale o con firma autografa e un documento di riconoscimento.

7.2.2.2. Revoca da parte del Gestore

Ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del DPCM [3], il Gestore dell'Identità digitale 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 scadenza contrattuale.

Nel caso previsto dal punto 1 il Gestore dell'Identità digitale revoca di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca al Titolare, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il cellulare (attributi secondari essenziali forniti per la comunicazione).

Nei casi previsti dai punti 2 e 3, il Gestore dell'Identità digitale 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 [3]. In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del Titolare (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 dell'Identità digitale, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.

Per il punto 4, il Gestore dell'Identità digitale revoca di propria iniziativa l'identità, comunicando la causa e la data della revoca all'utente con un avviso utilizzando gli attributi secondari forniti in precedenza e segue la procedura di violazione dei dati personali (data breach) dettata dal Garante per la protezione dei dati personali presente al seguente link https://www.garanteprivacy.it/regolamentoue/databreach.

7.2.2.3. Sospensione da parte del Titolare

Il Titolare può chiedere al Gestore dell'Identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione della propria Identità digitale:

- via PEC all'indirizzo blocco.spid@pec.infocamere.it;
- attraverso il portale SPID di InfoCamere, nella sezione dedicata, ove il Titolare può effettuare il blocco di emergenza dell'Identità digitale (equivale alla sospensione dell'Identità digitale).
- attraverso il portale SPID di InfoCamere, nella sezione Self Care, accedendo con la credenziale di livello più alta attivata, ove il Titolare può autonomamente sospendere la propria Identità digitale. In qualsiasi momento il Titolare può riattivare la propria Identità digitale attraverso la sezione di Self Care presente sul portale SPID di InfoCamere.
- Prenotando un appuntamento telefonico con il Contact Center InfoCamere

Nel caso di richiesta di sospensione, trascorsi trenta giorni dalla suddetta sospensione, il Gestore dell'Identità digitale provvede al ripristino dell'Identità digitale precedentemente sospesa qualora non pervenga allo stesso entro il medesimo termine, con le modalità sopra indicate, una richiesta di revoca.

Nel caso in cui il Titolare ritenga che la propria Identità digitale sia stata utilizzata fraudolentemente, lo stesso può chiederne la sospensione con la seguente modalità:

- via PEC all'indirizzo blocco.spid@pec.infocamere.it, indicando il motivo della richiesta e allegando il modulo di "RICHIESTA REVOCA/SOSPENSIONE" sottoscritto con firma digitale o con firma autografa allegando un documento di riconoscimento.

Il Gestore dell'Identità digitale deve fornire esplicita evidenza al Titolare dell'avvenuta presa in carico della richiesta e procedere all'immediata sospensione dell'Identità digitale.

Trascorsi trenta giorni dalla suddetta sospensione, il Gestore dell'Identità digitale provvede al ripristino dell'Identità digitale 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.

7.2.2.4. Sospensione da parte del Gestore

In caso di scadenza del documento d'identità del Titolare e in caso di uso illecito, il Gestore dell'Identità digitale sospende di propria iniziativa l'Identità digitale, mettendo in atto meccanismi con i quali comunica la

causa e la data della sospensione al Titolare, utilizzando l'indirizzo di posta elettronica fornito dal Titolare al momento della registrazione o successivamente.

7.2.3. Gestione ciclo di vita delle credenziali

Il sistema di gestione del ciclo di vita delle credenziali comprende i processi previsti dai regolamenti di cui all'Art 4 comma 2 del DPCM [3], ovvero:

a. creazione delle credenziali;
b. attivazione delle credenziali o dei mezzi usati per la loro produzione;
c. sospensione e revoca delle credenziali o mezzi usati per la loro produzione;
d. rinnovo e sostituzione delle credenziali.

InfoCamere, per l'intero ciclo di vita della credenziale conserva opportuna documentazione atta ad avere traccia delle seguenti informazioni:

a. la creazione della credenziale
b. l'identificativo della credenziale;
c. il soggetto per il quale è stata emessa;
d. lo stato della credenziale.

Il Titolare dell'Identità digitale può gestire autonomamente le sue credenziali accedendo al portale SPID di InfoCamere, alla sezione Self Care ed effettuare le operazioni che ritiene opportuno.

Relativamente alla sostituzione delle credenziali, sia essa richiesta dal Titolare o su iniziativa del Gestore dell'Identità digitale, quest'ultimo emette la nuova credenziale e revoca automaticamente la vecchia.
In entrambi i casi devono essere previsti meccanismi con i quali il Gestore dell'Identità digitale comunica la revoca al Titolare, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il cellulare (attributi secondari essenziali forniti per la comunicazione) comunicati dal Titolare in sede di registrazione o successivamente.

Per quanto riguarda il rinnovo delle credenziali, il sistema avvisa ripetutamente l'Utente (90, 30 e 10 giorni nonché il giorno precedente la scadenza), utilizzando l'indirizzo di posta elettronica e il cellulare (attributi secondari essenziali forniti per la comunicazione al momento della registrazione o successivamente) e attiva dalla sezione Self Care del portale InfoCamere la possibilità di rinnovo 30 giorni prima della scadenza.

Relativamente alle credenziali di livello 3, il Titolare può effettuare il rinnovo soltanto presso uno sportello di un Ufficio di Registrazione o IR.

Qualora il Titolare decida di non rinnovare le proprie credenziali, esso potrà revocarle come descritto nel paragrafo 7.2.2.1 del presente Manuale Operativo.

7.3. Richiesta dei dati da parte del titolare

In qualsiasi momento il Titolare potrà richiedere al Gestore dell'Identità digitale di conoscere, gratuitamente, i propri dati personali memorizzati nel sistema IdP, in conformità con quanto previsto dalla normativa.

7.4. Gestione rapporti con utenti

InfoCamere mette a disposizione dei propri Utenti, relativamente a questioni riguardanti problematiche o richieste di qualsiasi tipo aventi ad oggetto le credenziali SPID, i seguenti canali:

- Un form online, raggiungibile dalla sezione Supporto presente sul portale SPID di InfoCamere;
- La possibilità di prenotare un appuntamento con un operatore direttamente online scegliendo il giorno e la data tra i disponibili, dalla sezione Supporto presente sul portale SPID di InfoCamere;
- Un indirizzo PEC ove fare pervenire richieste di sospensione e revoca delle credenziali blocco.spid@pec.infocamere.it, indicando il motivo della richiesta e allegando il modulo di "RICHIESTA REVOCA/SOSPENSIONE" sottoscritto con firma digitale o con firma autografa e un documento di riconoscimento;

- La documentazione relativa al servizio, sempre disponibile sul portale nella sezione Documenti;
- Le FAQ, rispondenti ai quesiti più frequenti relativi all'utilizzo del servizio SPID, presenti nella sezione Supporto del portale SPID di InfoCamere.

7.5. Guida utente del servizio

Per quanto riguarda la guida Utente si rimanda integralmente al documento Guida Utente [13].

8. Sistema di monitoraggio

Il sistema di monitoraggio presente in InfoCamere consente di avere una visione centralizzata delle prestazioni dei sistemi, di generare operazioni riguardanti le componenti dell'infrastruttura, di produrre dati statistici e di generare metriche qualitative e quantitative, il tutto rilevato attraverso l'interfaccia web messa a disposizione.

Tale interfaccia è protetta da opportuno sistema di autenticazione e *accounting* che consente all'Utente di visualizzare quando descritto precedentemente.

Il personale impiegato provvede al controllo costante e, nel caso in cui vengano riscontrate anomalie nel funzionamento del servizio, esegue le opportune analisi per la comprensione delle cause e per le azioni correttive idonee a garantire la qualità dei servizi erogati ed il rispetto del livello di servizio dettato dalla normativa vigente.

Il sistema di monitoraggio configurato per il continuo controllo e per la produzione di allarmi segnala o l'evento anomalo o il disservizio indicandone il differente livello di gravità, al fine di consentire il corretto avvio delle operazioni di Escalation e di Incident Management. Inoltre, vi sono delle specifiche sezioni per la produzione di report.

9. Livelli di servizio garantiti

Di seguito vengono riportati gli indicatori di qualità (*Service Level Agreement*) e le caratteristiche sulla continuità operativa garantiti da InfoCamere e relativi alla convenzione per l'adesione dei Gestori delle Identità digitali nell'ambito di SPID.

9.1. Livelli di servizio per fasi della registrazione

Il processo garantisce la gestione della registrazione Utente titolare con tutti gli attributi qualificati e non qualificati richiesti.

ID	Indicatore di qualità	Modalità di funzionamento	Valore Limite
IQ-01	Disponibilità del sottoservizio di registrazione identità	Erogazione automatica	>= 99,5%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-02	Tempo di risposta del sottoservizio di registrazione identità		<= 12h (ore lavorative) per il 95% di richieste registrazione utente

9.2. Livelli di servizio per rilascio - riattivazione credenziali

Il processo garantisce la gestione del rilascio di una Identità digitale richiesta dall'Utente con il livello di sicurezza desiderato tra quelli erogati dal servizio InfoCamere.

ID	Indicatore di qualità	Modalità di funzionamento	Valore Limite
IQ-03	Disponibilità del sottoservizio di gestione rilascio credenziali	Erogazione automatica	>= 99,5%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-04	Tempo di rilascio credenziali	Erogazione da remoto	<= 5 giorni lavorativi
		Erogazione in presenza	<= 3 giorni lavorativi
IQ-05	Tempo riattivazione delle credenziali		<= 2 giorni lavorativi

9.3. Livelli di servizio per sospensione e revoca credenziali

Il processo garantisce la gestione del servizio di sospensione e revoca delle credenziali.

ID	Indicatore di qualità	Modalità di funzionamento	Valore Limite
IQ-06	Disponibilità del sottoservizio di sospensione e revoca delle credenziali		>= 99,5%
			Singolo evento di indisponibilità < =6 ore
IQ-07	Tempo di sospensione delle credenziali	Erogazione automatica	<= 1 minuto
		Erogazione in presenza	<= 10 minuti
IQ-08	Tempo di revoca delle credenziali		<= 5 giorni lavorativi

9.4. Livelli di servizio per rinnovo e sostituzione credenziali

Il processo garantisce la gestione del servizio delle credenziali.

ID	Indicatore di qualità	Modalità di funzionamento	Valore Limite
IQ-09	Disponibilità del sottoservizio di rinnovo e sostituzione delle credenziali	Erogazione automatica	>= 99,5%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		<= 2 giorni lavorativi
IQ-10-bis	Tempo di dispiegamento/aggiornamento metadata		<= 2 giorni lavorativi

9.5. Livelli di servizio per autenticazione

Il processo garantisce la gestione del servizio di autenticazione del Titolare.

ID	Indicatore di qualità	Modalità di funzionamento	Valore Limite
IQ-11	Disponibilità del sotto-servizio di autenticazione		>= 99,5% Singolo evento indisponibilità <= 6 ore
IQ-12	Tempo di risposta del sotto-servizio di autenticazione		Coefficiente moltiplicativo = 300 300: tot. eID nazionale = x: tot. eID gestore $x = \frac{300 \times \text{Tot. eID Gestore}}{\text{Tot. eID Nazionale}}$ x = numero effettivo di richieste di autenticazioni al secondo (*auth sec*) correlate alle identità rilasciate dal gestore. Se x<100, il gestore deve garantire almeno 100 *auth sec*. Tempi di risposta ≤ 2 sec per il 98% delle richieste di autenticazione Per un numero di richieste di *auth sec* superiore al *coefficiente moltiplicativo*, lo SLA andrà concordato in anticipo tra AgID e gestori.

9.6. Livello di servizio per la continuità operativa

L'erogazione dei servizi è garantita con la seguente continuità operativa.

ID	Indicatore di qualità	Modalità di funzionamento	Valore Limite
IQ-13	RPO sotto-servizio registrazione e rilascio delle identità		1 ora
IQ-14	RTO sotto-servizio registrazione e rilascio delle identità		8 ore
IQ-15	RPO sotto-servizio di sospensione e revoca delle credenziali		1 ora
IQ-16	RTO sotto-servizio di sospensione e revoca delle credenziali		8 ore
IQ-17	RPO sotto-servizio di Autenticazione		1 ora
IQ-18	RTO sotto-servizio di Autenticazione		8 ore

10. Modalità di protezione dei dati personali

In qualità di Titolare del trattamento, InfoCamere riconosce l'importanza dei principi e delle norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali, nel rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla protezione dei dati personali.

Pertanto, con riguardo al trattamento dei dati personali effettuato per il rilascio e la gestione del servizio di Identità digitale, InfoCamere ha strutturato le attività di trattamento, nel rispetto dei principi individuati nella normativa privacy vigente e dando attuazione agli obblighi ivi previsti.

In ossequio al principio di trasparenza, agli interessati vengono fornite tutte le informazioni relative alle modalità con cui i dati personali sono raccolti, utilizzati e, in generale, trattati. I relativi contenuti sono messi a disposizione degli interessati in forma facilmente accessibile, comprensibile ed attraverso un linguaggio semplice e chiaro. In linea con le indicazioni del Regolamento (UE) 2016/679 [11] in tema di informativa all'interessato vengono quindi forniti gli elementi utili per comprendere le caratteristiche strutturali e portanti del trattamento. Attraverso tali modalità, sono chiaramente esplicitate le finalità, le basi giuridiche del trattamento, i termini di conservazione e gli elementi necessari per assicurare un trattamento corretto e trasparente nei confronti dell'interessato.

InfoCamere si impegna pienamente per assicurare e garantire all'interessato l'esercizio e la tutela dei diritti riconosciuti dalla normativa in materia di protezione dei dati personali. Per tale fine, vengono fornite informazioni dettagliate e facilmente accessibili, con riguardo alle modalità ed ai recapiti utili per poterli esercitare.

Infine, nel rispetto degli obblighi di legge e dei principi di privacy by design e by default, i dati personali raccolti per il rilascio e la gestione dell'Identità digitale, vengono trattati in modo lecito e corretto, nei confronti dell'interessato, nel rispetto degli ambiti normativi che ne inquadrano la legittimità.

Per dare piena ed efficace attuazione ai richiamati principi, InfoCamere si impegna a raccogliere ed a trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, circoscrivendo il periodo di conservazione ai termini di legge.

10.1. Archivi contenenti dati personali

I dati personali raccolti ai fini del rilascio dell'Identità digitale e della gestione del ciclo di vita della stessa vengono trattati con le garanzie e nel rispetto delle normative vigenti in materia di conservazione documentale.

10.2. Misure per la protezione dei dati personali

Nel rispetto del disposto normativo, InfoCamere ha implementato misure tecniche ed organizzative per garantire un elevato livello di sicurezza, al fine di contrastare i rischi di distruzione, perdita, modifica, divulgazione non autorizzati. Tali misure sono state attuate al fine di preservare la riservatezza, l'integrità e la disponibilità dei dati personali dell'interessato.

Di conseguenza, i dati personali sono trattati da InfoCamere e/o da soggetti interni, previamente formati ed istruiti, debitamente designati/autorizzati che operano per suo conto a norma del Regolamento (UE) 2016/679 [11]. I dati personali possono, inoltre, essere trattati da soggetti esterni formalmente nominati quali Responsabili del trattamento, ai sensi del Regolamento (UE) 2016/679 [11], contrattualmente vincolati a rispettare le istruzioni impartite da InfoCamere per garantire la sicurezza, la riservatezza nonché la protezione dei dati da possibili violazioni di sicurezza.

11. Disposizioni finali

11.1. Comunicazioni

Qualora una persona desideri o sia tenuta a effettuare delle comunicazioni, domande o richieste verso il Gestore dell'Identità digitale in relazione al presente Manuale Operativo ed al Servizio SPID di InfoCamere, tali comunicazioni dovranno avvenire sul sito id.infocamere.it, attraverso la sezione Supporto dedicata all'assistenza per l'Utente.

11.2. Intestazioni e appendici del presente manuale operativo

Le intestazioni, sottotitoli e altri titoli del presente Manuale Operativo sono utilizzati solo per comodità e riferimento, e non saranno utilizzati nell'interpretazione o applicazione di qualsiasi disposizione ivi contenuta. Le appendici, comprese le definizioni del presente Manuale Operativo, sono parte integrante e vincolante del presente Manuale Operativo a tutti gli effetti.

11.3. Modifiche del Manuale Operativo

Fermo quanto previsto nelle Condizioni Generali, InfoCamere si riserva il diritto di aggiornare periodicamente il presente Manuale Operativo in caso di modifiche normative o regolamentari relative al Servizio SPID o qualora esigenze tecniche, di sicurezza o di organizzazione e/o ottimizzazioni del ciclo lavorativo di InfoCamere rendano necessarie tali modifiche.
Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni.

12. 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	Schermata Idp	Trouble shooting 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 di 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 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 POST	HTTP 403	n.a	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il Gestore del servizio	Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta	Parametri obbligatori: SAMLRequest SigAlg Signature Parametri non obbligatori: RelayState Parametri obbligatori: SAMLRequest Parametri non obbligatori: RelayState

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario notifica	Schermata Idp	Trouble shooting Utente	Troubleshooting SP	Note
5	Verifica della firma fallita	http:Redirect	HTTP 403	n.a	Utente	Pagina di cortesia con messaggio "Impossibile stabilire l'autenticità della richiesta di autenticazione - Contattare il gestore del	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 POST	HTTP 403	n.a	Utente	Pagina di cortesia con messaggio "Formato richiesta non ricevibile- Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare metadata Gestore dell'identita (IdP)	invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell'identity invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity
7	Errore sulla verifica della firma della richiesta	HTTP POST	HTTP 403	n.a	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare 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

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario notifica	Schermata Idp	Trouble shooting Utente	Troubleshooting SP	Note
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 corrispondente 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.

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario notifica	Schermata Idp	Trouble shooting Utente	Troubleshooting SP	Note
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:statuss:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: “Autenticazione e 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	IssueInstant 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 ill 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:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)	n.a	n.a	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
15	attributo isPassive presente e attualizzato al valore true	HTTP 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	

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario notifica	Schermata Idp	Trouble shooting Utente	Troubleshooting SP	Note
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:RequestUnsupported ErrorCode nr16	Fornitore del servizio (SP)	n.a	n.a	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	AssertionConsumerServiceIndex presente e attualizzato 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

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario notifica	Schermata Idp	Trouble shooting Utente	Troubleshooting SP	Note
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 servizio richiesto	

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario notifica	Schermata Idp	Trouble shooting Utente	Troubleshooting SP	Note
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	
24	RISERVATA								

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/Status Message	Destinatario notifica	Schermata Idp	Trouble shooting Utente	Troubleshooting SP	Note
25	Processo di autenticazione annullato dall'utente	HTTP POST	n.a	ErrorCode nr25	Fornitore del servizio (SP)			Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
26	Processo di erogazione dell'identità digitale andata a buon fine	HTTP POST	n.a	ErrorCode nr26	Fornitore del servizio (SP)		Identità Digitale erogata con successo		
27	Utente già presente	HTTP POST	n.a	ErrorCode nr27	Fornitore del servizio (SP)		Utente già in possesso dell'Identità Digitale con il Fornitore di Identità Digitale selezionato		
28	Operazione annullata	HTTP POST	n.a	ErrorCode nr28	Fornitore del servizio (SP)		Operazione di richiesta identità digitale annullata dall'utente		
29	Identità non erogata	HTTP POST	n.a	ErrorCode nr29	Fornitore del servizio (SP)		Il fornitore non ha erogato l'identità digitale		