Aruba PEC S.p.A.

Manuale Operativo Sistema Pubblico per la gestione dell'Identità Digitale (SPID)

Versione: 3.1
Data: 10/06/2026
Approvato da: Andrea Sa
Classificazione documento

Sassetti
Andrea
11.06.2026
14:33:04
UTC

VERSIONE	DATA	NATURA DELLA MODIFICA
1.0	15/02/2016	Prima versione.
1.1	24/05/2017	Aggiornamento sede legale. **Par.2.3**: modificati i riferimenti normativi **Par.2.4**: aggiunti RTO e RPO in definizioni e acronimi **Par.3.5**: aggiornati riferimenti del Responsabile del Manuale operativo **Par.6.2.2:** sostituito termine "residenza" con "domicilio" **Cap.9**: formattazione livelli di servizio
1.2	21/06/2017	**Inserimento devisu remoto con dispositivi mobile** **Tutto il documento**: aggiornata la definizione ed uniformati riferimenti a "Titolare" e "Cliente" in "Richiedente"; migliorato uso terminologia legata all'identificazione **Par 6.2.1.**: precisate condizioni per operatività CDRL per OdR ed IR **Par.6.3 p.to 8** aggiornate modalità di riconoscimento **Par.6.3.1.2:** inseriti dettagli per riconoscimento con dispositivo mobile; aggiornata Figura 3 e inserite Figura 4, Figura 5, Figura 6 e Figura 7; modificata Fig.4 (ora figura 8) **Par 6.4.2.**: modificate tabelle 2 e 3
1.3	08/09/2017	**Par 3.4**: integrate procedure per l'aggiornamento del Manuale Operativo **Par 4.1**: aggiornate le responsabilità del Titolare dell'Identità **Par 4.2**: aggiornate le responsabilità dell'IdP **Par.4.4**: aggiunto "Obblighi dei Soggetti esterni che svolgono l'attività di registrazione e/o riconoscimento (de visu)"

1.4	27/09/2018	**Par. 2.3:** aggiornati riferimenti normativi **Par. 5.2:** modificato titolo ed inseriti dettagli su architettura fisica **Par. 5.6.3:** inserito tempo di conservazione dei tracciati delle richieste di autenticazione dell'utente e aggiornate modalità gestione **Par. 6.2.2:** aggiornato flusso richiesta online identità SPID **Par. 6.3.1:** aggiornato elenco documenti validi per attivazione **Par. 7.2.3:** aggiunto collegamento modalità di rinnovo **Cap.11:** modificate disposizioni finali **Tutto il documento:** rimossi rimandi a documento esterno di Piano per la Sicurezza; inseriti e aggiornati riferimenti a GDPR e tolti riferimenti non più pertinenti a D.Lgs. 196/2003 e misure minime di sicurezza.
1.5	22/11/2018	**Par. 6.2.2:** aggiornata descrizione passaggi richiesta online identità SPID
1.6	25/06/2019	**Par. 6.2.2, 6.3, 6.3.2, 6.6, 7.1 e 9.1:** aggiunto riconoscimento con CIE **Par 3.6:** modificato legale rappresentante.
1.7	25/03/2021	**2.4:** Integrazioni alle Definizioni; **6.2.1:** Integrato par 6.2.1.1 ed eliminato par. 6.2.1.2; **6.2.2:** modifiche minori; Eliminato **6.6.1** Aggiunto paragrafo Procedura per il recupero del numero di cellulare da associare all'identità digitale**;** Aggiunto paragrafo**; 7.1:** modifiche minori; **7.2.4:** "Sospensione e revoca delle credenziali" ed il paragrafo **7.2.5: "**Gestione delle credenziali in caso di impossibilità di accesso ai canali di contatto". Corretti refusi minori nell'intero documento.
1.8	14/04/2022	**3.2**: modifica al paragrafo; **4.4**: modifica titolo paragrafo; **6.6.1:** modifiche al paragrafo per il recupero del numero cellulare; **6.2:** aggiunto rilascio SPID persona fisica per uso professionale **6.3** e **6.2.2:** modifiche al paragrafo e aggiunto riconoscimento con SPID; **6.3.1.2**: modifiche al processo di identificazione attraverso sessione audio-video; **6.3.2**: aggiunto riconoscimento con SPID persona fisica; **7.2.2**: modifiche al paragrafo; **7.2.4**: modifiche al paragrafo;
1.9	29/08/2022	**Paragrafi 2.4; 4.3; 6.2, 6.3.1; 6.3.2; 6.4.4; 6.7; 7.2.4; 7.2.6:** introdotti riferimenti all'identità SPID per minori; **6.4.2:** modifica al paragrafo relativamente agli Avvisi SPID n. 7 e 17; **Modifiche ai paragrafi: 5.4.2; 4.3, 6.3.1.2; 7.2.2;7.2.3;**
2.0	26/01/2023	**2.3, 2.4:** Integrazioni a Riferimenti e Definizioni. **4.2**: eliminato punto n. 43; **Paragrafi: 6.2, 6.2.1.1, 6.2.2, 6.2.2.1:** introdotti riferimenti all'identità SPID persona giuridica uso professionale. I par. 6.2.1.1 e 6.2.1.2 precedenti sono confluiti nel 6.2.1. Il par. 6.2.1.1 attuale è stato rinominato. Il par. 6.2.2.1 è stato inserito. **6.3.2:** introdotta specifica relativa al riconoscimento tramite firma digitale. **6.2.2, 6.3:** modificato passaggio identificazione con SPID Persona Fisica. **7.2.2:** apportati chiarimenti al punto n.6 in elenco; introdotto punto n.7 in elenco; apportati chiarimenti rispetto ai casi di sospensione; modificato link per riattivazione/sospensione/revoca.
2.1	13/09/2023	**Par. 5.3.2:** aggiornamento codici e formato messaggi di anomalie. **Par. 6.6:** revisione procedure per il rilascio, consegna e attivazione delle credenziali. **Par. 7.2.4:** aggiornamento modalità di sospensione e revoca delle credenziali. **Modifiche minori ai paragrafi: 2.1, 5.4.2, 5.5.1, 5.6.3, 6.3.1.1, 6.3.1.2, 7.4.**
2.2	02/10/2024	**Par. 6.2.1, 6.2.2, 6.3.2:** inserito riferimento per rilascio SPID Aziendale con Legale Rappresentante non italiano. **Par. 6.3.1:** integrazione delle verifiche effettuate dal Gestore sul processo di identificazione con operatore. **Par 6.4.2:** esplicitato riferimento al RUNTS quale fonte autorevole per la verifica della persona giuridica. **Par 6.7**: esplicitata revoca dell'Identità SPID Minore in caso nel caso in cui il genitore non sia più titolare di un'identità SPID attiva. **Par 7.2.2:** integrazione delle modalità di rinnovo dell'Identità Digitale e modifica alla denominazione del paragrafo. **Par. 9.3:** Inserimento descrizione della tabella, allineamento degli indicatori IQ-4 e IQ-5. Corretti refusi minori nell'intero documento.

3.0	24/11/2025	Nuova numerazione paragrafi e riformattazione **Par. 1.4:** inserimento definizione Operatori Supervisori e conseguente inserimento della denominazione al par. 5.3.1. **Par. 4.4:** inserimento della modalità di autenticazione tramite QR Code, modifiche ai metodi in uso **Par. 5:** aggiornamento formale e di contenuto in relazione al rilascio di SPID minori **Par. 8:** aggiornamento formale e di contenuto sui livelli di servizio in tutto il paragrafo **Par. 9.3:** aggiunta paragrafo Modalità di protezione dei dati personali in ambito SPID minori **Appendice A**: revisione formale
3.1	10/06/2026	**Par. 5.4.2.1:** aggiunta del paragrafo in relazione agli aggiornamenti degli Avvisi SPID n. 7 v.3 e 17 v.2. **Par. 5.4.2**: aggiornamento verifiche ANPR

Sommario

1 Introduzione 7
1.1 Scopo del documento e principali raccomandazioni ai lettori 7
1.2 Standard di riferimento 7
1.3 Riferimenti 8
1.4 Definizioni ed acronimi 9
2 Dati identificativi – Pubblicazione del Manuale Operativo 14
2.1 Dati identificativi del gestore dell'identità digitale 14
2.2 Versione del manuale operativo 14
2.3 Pubblicazione del manuale operativo 14
2.4 Procedure per l'aggiornamento del Manuale Operativo 14
2.5 Responsabile del Manuale operativo 15
3 Disposizioni generali 15
3.1 Obblighi dell'utente 15
3.2 Obblighi e Responsabilità del Gestore dell'Identità Digitale 16
3.3 Obblighi dei fornitori di Servizi 19
3.4 Delega a Soggetti esterni che svolgono l'attività di registrazione e/o riconoscimento (de visu) 19
3.5 Obblighi del Richiedente 20
3.6 Obblighi connessi al trattamento dei dati personali 20
3.7 Limitazioni di Responsabilità ed eventuali limitazioni agli indennizzi 20
3.7.1 Conoscenza del Manuale Operativo 20
3.7.2 Forza Maggiore 20
3.7.3 Declinazioni e Limitazioni del Gestore 20
4 Architettura 21
4.1 Architettura applicativa 21
4.2 Architettura fisica 23
4.3 Architettura dei sistemi di autenticazione 23
4.3.1 Notifiche di accesso 25
4.3.2 Codici e formato messaggi di anomalie 25
4.4 Sistemi di autenticazione e credenziali 29
4.4.1 Livello di sicurezza 1 29
4.4.2 Livello di sicurezza 2 29
4.4.3 Livello di sicurezza 3 32
4.5 Misure anticontraffazione 32
4.5.1 Livello 2 32
4.5.2 Livello 3 34
4.6 Tracciatura degli accesi 34
4.6.1 Accessi fisici 35
4.6.2 Accessi logici 35

4.6.3 Tracciature accessi di autenticazione utenti *35*
5 Operatività 36
5.1 Funzioni del personale addetto al servizio di gestione delle identità digitali 36
5.2 Richiesta dell'identità digitale 36
5.2.1 Richiesta dell'identità SPID da sportello *37*
5.2.2 Richiesta dell'identità SPID online *39*
5.2.3 Richiesta dell'identità digitale per un soggetto minore *42*
5.3 Modalità di identificazione ai fini del rilascio dell'identità digitale 43
5.3.1 Identificazione con operatore *43*
5.3.2 Identificazione informatica mediante TS-CNS, CNS, CIE, firma digitale o SPID *47*
5.4 Verifica degli attributi associati all'identità digitale 48
5.4.1 Identità digitale e attributi *48*
5.4.2 Verifica degli attributi identificativi (identità dichiarata) *49*
5.4.3 Verifica degli attributi secondari *51*
5.4.4 Verifica attributi del soggetto minore *51*
5.5 Attivazione dell'identità digitale 52
5.6 Rilascio, consegna e attivazione delle credenziali 52
5.6.1 Procedura per il recupero del numero di cellulare da associare all'identità digitale *53*
6 Gestione delle identità digitali 54
6.1 Gestione dati raccolti per la verifica dell'identità digitale 54
6.2 Gestione del ciclo di vita 54
6.2.1 Gestione degli attributi *55*
6.2.2 Sospensione, Revoca e Rinnovo dell'Identità *55*
6.2.3 Gestione ciclo di vita delle credenziali *57*
6.2.4 Sospensione e revoca delle credenziali *58*
6.2.5 Gestione delle credenziali in caso di impossibilità di accesso ai canali di contatto *58*
6.2.6 Gestione dell'identità digitale di un soggetto minore *59*
6.3 Richiesta dei dati da parte del Titolare 60
6.4 Gestione rapporti con utenti 60
6.5 Guida utente del servizio 61
7 Sistema di monitoraggio 61
8 Livelli di servizio 62
8.1 Livelli di servizio garantiti per le diverse fasi della registrazione 62
8.2 Livelli di servizio garantiti per le diverse fasi della gestione del ciclo di vita delle identità 63
8.3 Livello di servizio garantito per le diverse fasi del processo di autenticazione 64
8.4 Continuità operativa 66
9 Modalità di protezione dei dati personali 66
9.1 Archivi contenenti dati personali 66
9.2 Misure di tutela della riservatezza 67
9.3 Protezione dei dati personali in ambito SPID minori 67
10 Disposizioni finali 68

10.1 Nullità od inapplicabilità di clausole 68
10.2 Interpretazione 68
10.3 Nessuna rinuncia 68
10.4 Comunicazioni 68
10.5 Intestazioni e Appendici del Presente Manuale Operativo 68
10.6 Modifiche del Manuale Operativo 69
10.7 Violazioni e altri danni materiali 69
10.8 Norme applicabili 69
10.9 Foro competente 69

1 Introduzione

1.1 Scopo del documento e principali raccomandazioni ai lettori

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 dalla Aruba PEC S.p.A. 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", 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), Aruba PEC S.p.A., come *prestatore di servizi fiduciari*, 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.
Aruba PEC S.p.A., allo scopo di consentire un corretto utilizzo del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese raccomanda all'utente un'attenta lettura del presente documento.
L'utente titolare dell'identità digitale SPID si impegna a proteggere ed a tenere segrete le proprie credenziali d'accesso (vedi definizioni) alle identità digitali nonché a dare avviso al gestore delle identità digitali dell'eventuale smarrimento, sottrazione o compromissione (vedi definizioni) delle credenziali stesse. Per ulteriori informazioni, vedi il sito web di Aruba PEC S.p.A. www.pec.it oppure inviare una richiesta di assistenza tramite compilazione del form online presente all'indirizzo: supportoecs.aruba.it.

1.2 Standard di riferimento

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-2.0os.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)
XMLSig	W3C XML Signature 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 (https://www.agid.gov.it/sites/default/files/repository_files/tabella_attributi_v.1.3.pdf)
SPID-TabErr	Tabella Codici di Errore (https://www.agid.gov.it/sites/default/files/repository_files/tabella-messaggi-spid-v1.4.pdf)

1.3 Riferimenti

[1]	Documento ArubaPEC: “Servizio IdP - Infrastruttura SPID”
[2]	Documento ArubaPEC: “Servizio IdP – Piano per la sicurezza”
[3]	Documento ArubaPEC: “Servizio IdP - Guida Utente”

[4]	CAD - Codice Amministrazione Digitale - D.lgs. 7 marzo 2005 n. 82 (G.U. n.112 del 16 maggio 2005) e s.m.i.
[5]	DPCM - DPCM del 29-10-2014 (pubblicato in GU Serie Generale n.285 del 9-12-2014): 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.
[6]	Codice Privacy - Codice in materia di protezione dei dati personali – D.lgs. 30 giugno 2003 n. 196
[7]	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche (Gazzetta Ufficiale dell'Unione Europea – serie L257 del 28 agosto 2014)
[8]	Determinazione n. 44 del 28 luglio 2015 – Emanazione dei regolamenti SPID previsti dall'art. 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014
[9]	Regolamento recante le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale
[10]	Regolamento recante le modalità attuative per la realizzazione dello SPID
[11]	Regolamento recante le regole tecniche
[12]	Regolamento recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM 24 ottobre 2014
[13]	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.
[14]	Decreto legislativo n.101 del 10 agosto 2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
[15]	Linee guida operative per la fruizione dei servizi SPID da parte dei minori
[16]	Linee guida per il rilascio dell'identità digitale per uso professionale
[17]	Linee guida per il rilascio dell'identità di persona giuridica a persona fisica non dotata di un documento di riconoscimento rilasciato in Italia

1.4 Definizioni ed acronimi

Sono di seguito elencate le definizioni, i termini e gli acronimi utilizzati nella stesura del presente Manuale Operativo. Per i termini definiti dal CAD e dal DPCM si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato anche il termine inglese corrispondente, generalmente usato in letteratura tecnica e negli standard.

AA	Attribute Authority

Adesione	È 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 multi-fattore	Autenticazione con almeno due fattori di autenticazione indipendenti (ISOIEC 19790)
Autenticazione	Disposizione di garanzia sull'identità dell'entità (ISO-IEC 18014-2)
BCP	Best Current Practice (IETF)
CA	Certification Authority
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
Genitore richiedente (o solo genitore)	il soggetto che esercita la responsabilità genitoriale sul minore e che chiede il rilascio di SPID in favore di quest'ultimo
Genitore non richiedente	Altro soggetto – diverso dal genitore richiedente - che esercita la responsabilità genitoriale sul minore
Gestori dell'identità digitale	Le persone giuridiche accreditate allo SPID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi 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 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, 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;
identità digitale uso professionale della persona fisica (di tipo 3)	identità digitale che contiene gli attributi della persona fisica cui sono state rilasciate le credenziali di autenticazione
identità digitale uso professionale della persona giuridica (di tipo 4)	l'identità digitale che contiene gli attributi della persona giuridica e della persona fisica cui sono state rilasciate le credenziali di autenticazione
IdM	Identity Management
IdP	Identity Provider (il gestore delle identità digitali in ambito SPID)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPV	Identity Proofing and Verification
IR	Incaricato al Riconoscimento
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
ODR	Operatore di Registrazione, soggetto incaricato al riconoscimento del soggetto richiedente l'identità SPID ed all'accesso agli applicativi dell'IdP.
OS	Operatore Supervisore: persona fisica, titolare di un rapporto contrattuale con il Gestore SPID (in via esemplificativa rapporto di lavoro dipendente full o part time, consulenza o collaborazione a tempo determinato etc.), formalmente incaricata dall'IdP stesso a svolgere in suo nome e per suo conto le attività di controllo e verifica della documentazione e delle evidenze inerenti alle attività di riconoscimento del Richiedente, nel rigoroso rispetto delle istruzioni impartite dall'IdP.

Organizzazione	la persona giuridica che stipula un accordo con un IdP al fine del rilascio delle identità digitali SPID (di tipo 4) in favore di soggetti che agiscono in qualità di dipendenti o, comunque, in nome o per conto dell'organizzazione stessa.
OTP	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione
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, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98
(Utente) Titolare o Richiedente	È il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v). Prima dell'attribuzione dell'identità digitale tale soggetto è chiamato Richiedente
TCP	Transmission Control Protocol
User Agent	Sistema utilizzato dall'utente per l'accesso ai servizi (di solito il browser per la navigazione in rete);

2 Dati identificativi – Pubblicazione del Manuale Operativo

2.1 Dati identificativi del gestore dell'identità digitale

Denominazione Sociale:	**Aruba Posta Elettronica Certificata S.p.A.**
Indirizzo della sede legale:	**Via San Clemente n. 53 – 24036 Ponte San Pietro (BG)**
Legale Rappresentante:	**Giorgio Cecconi**
N° iscrizione al Registro delle imprese:	**N° REA: 145843**
N° Partita IVA:	**01879020517**
N° Telefono (centralino):	**+39 0575 0500**
N° FAX:	**+39 0575 862022**
E-mail PEC:	**direzione.ca@arubapec.it**
ISO OID (private enterprise number):	**1.3.6.1.4.1.29741**
Sito web generale (informativo ITA/ENG):	https://www.pec.it/

2.2 Versione del manuale operativo

Il presente Manuale Operativo è di proprietà di Aruba PEC S.p.A., tutti i diritti sono ad essa riservati.
La versione del manuale attualmente in vigore è quella riportata nella tabella delle revisioni.
Il documento è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.

2.3 Pubblicazione del manuale operativo

Il presente Manuale Operativo è reperibile in formato elettronico presso il sito web del Gestore indicato nel paragrafo 2.1.
Riferimento al presente Manuale Operativo e le altre informazioni relative al Gestore previste dal DPCM sono pubblicate presso il registro SPID gestito dall'AgID.

2.4 Procedure per l'aggiornamento del Manuale Operativo

L'IdP si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.
Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni. Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste.
Ogni variazione è visionata e verificata dalla Direzione dei servizi di CA ed approvata dalla Direzione Aziendale, dopo eventuali consultazioni con le parti delle funzioni aziendali interessate,

e viene preventivamente comunicata all'Agenzia che, per approvazione, provvederà a sottoscrivere e pubblicare sul proprio sito la nuova versione o release.
La redazione e approvazione di questo Manuale segue le procedure previste dal Sistema di Gestione Qualità aziendale e viene riesaminato e, se necessario, aggiornato con frequenza almeno annuale.

2.5 Responsabile del Manuale operativo

Le comunicazioni riguardanti il presente documento possono essere inviate all'attenzione di:

Andrea Sassetti
Aruba PEC S.p.A.
Tel. +39 0575 1939715
Fax. +39 0575 862022
E-mail: direzione.ca@arubapec.it

3 Disposizioni generali

In questa sezione sono descritti i termini e le condizioni generali sotto cui sono erogati i servizi di rilascio e gestione delle identità digitali descritti nel Manuale.

3.1 Obblighi dell'utente

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

1. Esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione
2. Si obbliga all'uso esclusivamente personale delle credenziali connesse all'Identità Digitale
3. Si obbliga a non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti. A tale proposito, si precisa che l'utente è tenuto ad adottare tutte le misure tecniche e organizzative idonee ad evitare danni a terzi
4. Si obbliga a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine
5. Deve garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi
6. L'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private
7. Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite
8. Fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci

9. Accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze
10. Informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati
11. Mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi:
    - se persona fisica: estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale;
    - se persona giuridica: indirizzo sede legale, codice fiscale o P.IVA, rappresentante legale della società, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale.
12. Conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i 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.
13. 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.
14. In caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali.
15. In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali.

L'utente è tenuto ad aggiornare la propria password secondo le indicazioni e le raccomandazioni previste dai regolamenti di cui all'Art 4 comma 2 del DPCM e descritti al par. 6 del presente documento.

3.2 Obblighi e Responsabilità del Gestore dell'Identità Digitale

Aruba PEC, in qualità di Gestore dell'Identità Digitale, ai sensi dell'Art 1 let l, 7, 8 e 11 del DPCM, è tenuta a:

1. Attribuire l'Identità Digitale, rilasciare le credenziali e gestire le procedure connesse al ciclo di vita dell'identità e delle credenziali attenendosi al DPCM e alle Regole Tecniche tempo per tempo emanate dall'AgID
2. Rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta
3. Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale
4. Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione de visu

5. 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
6. Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso di identificazione tramite firma digitale
7. Verifica degli attributi identificativi del richiedente
8. Consegnare in modalità sicura le credenziali di accesso all'utente
9. Conservare la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale
10. Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale
11. Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al Regolamento (UE) 2016/679 ed al Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.
12. Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione
13. Effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso
14. Revocare l'identità digitale in caso di decesso della persona fisica o di estinzione della persona giuridica; oppure qualora il contratto sia scaduto o si riscontri l'inattività per un periodo superiore a 24 mesi, informando l'utente via posta elettronica e numero di telefono mobile
15. Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente
16. Verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata)
17. Fornire all'utente che l'ha inviata conferma della ricezione della richiesta di sospensione
18. Sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni ed informarne il richiedente.
19. Rispristinare o revocare l'identità digitale sospesa, nei casi previsti
20. Revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione
21. Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale
22. Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso
23. Effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta
24. Effettuare con cadenza almeno annuale un'analisi dei rischi
25. Definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID

26. Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato
27. Condurre con cadenza almeno semestrale il Penetration Test
28. Garantire la continuità operativa dei servizi afferenti allo SPID
29. Effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna
30. 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
31. Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa
32. Sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti
33. Informare tempestivamente l'AGID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali
34. Adeguare i propri sistemi a seguito dell'aggiornamento della normativa
35. Inviare all'AGID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici.
36. In caso intendesse cessare la propria attività, comunicarlo all'AGID "e ai titolari" almeno 30 giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali rilasciate
37. In caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e ne conserva le informazioni
38. In caso di cessazione dell'attività, scaduti i 30 giorni, revocare le identità digitali rilasciate e per le quali non si è avuto subentro
39. 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
40. Se richiesto dall'utente, segnalargli via email o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso.
41. Notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale
42. Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.
43. Nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale.
44. Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.

45. In caso di richiesta di revoca dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.
46. Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa.
47. All'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta.
48. In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
49. Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID.
50. Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 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.

3.3 Obblighi dei fornitori di Servizi

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

1. Conoscere l'ambito di utilizzo delle identità digitali, le limitazioni di responsabilità e i limiti di indennizzo del IdP, riportati nel presente Manuale Operativo;
2. Osservare quanto previsto dall'art. 13 del DPCM e dagli eventuali Regolamenti di cui all'art. 4 del DPCM medesimo;
3. Adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
4. In conformità a quanto definito dalle Linee Guida operative per la fruizione dei servizi SPID da parte dei minori [15], effettuare una valutazione con riferimento alla tipologia e alla finalità del servizio erogato al minore. Aruba PEC, in qualità di Identity Provider, non svolge alcun controllo rispetto ai servizi per i quali il soggetto minore richiede l'accesso.

3.4 Delega a Soggetti esterni che svolgono l'attività di registrazione e/o riconoscimento (de visu)

ArubaPEC può delegare le funzioni di registrazione e riconoscimento a soggetti esterni (detti Partner ArubaPEC) previo corso di formazione e sottoscrizione dei documenti "Modulo di adesione - Partner Aruba Pec", "Condizioni Generali Contratto - Partner Aruba PEC" e "Condizioni particolari di fornitura Aruba ID - Partner Aruba Pec", la cui ultima versione è visionabile sul sito all'url https://www.pec.it/partner-documentazione.aspx.
In ogni caso ArubaPEC mantiene le responsabilità per quanto non espressamente indicato nei documenti sopracitati e nel complesso delle attività svolte come IdP SPID.

3.5 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.

3.6 Obblighi connessi al trattamento dei dati personali

Aruba PEC tutela la riservatezza dei dati personali e garantisce ad essi la protezione necessaria da ogni evento che possa metterli a rischio di violazione, trattandoli secondo le specifiche previsioni della vigente normativa in materia.
Come previsto dal Regolamento dell'Unione Europea n. 2016/679, ed in particolare all'art. 13, sono fornite all'utente ("Interessato") tutte le informazioni richieste dalla normativa relative al trattamento dei propri dati personali mediante apposita, specifica e preventiva informativa, resa altresì sempre disponibile all'interno del proprio sito.

3.7 Limitazioni di Responsabilità ed eventuali limitazioni agli indennizzi

La sezione illustra le limitazioni di responsabilità assunte dal gestore dell'identità digitale nell'esercizio della propria attività.

3.7.1 Conoscenza del Manuale Operativo

L'utente, persona fisica o giuridica titolare dell'identità digitale SPID è tenuto a consultare preventivamente e conoscere il presente Manuale Operativo, le modalità in esso contenute per le operazioni di rilascio e gestione delle identità digitali. È espressamente esclusa ogni responsabilità del gestore che sia derivante dalla non conoscenza o dal non corretto utilizzo delle procedure descritte nel presente manuale.

3.7.2 Forza Maggiore

La responsabilità del Gestore sarà esclusa nel caso di eventi che esulino dalla propria volontà o da cause a lui non imputabili. Il Gestore quindi non sarà responsabile per i danni di qualsiasi natura, da chiunque subiti e causati da caso fortuito o forza maggiore, impossibilità della prestazione, ordine o divieto dell'autorità quali, a titolo esemplificativo e non esaustivo, mancato funzionamento di reti o apparati tecnici al di fuori del controllo del Gestore, interruzione nella fornitura di energia elettrica, allagamenti, incendi, azioni di guerra, epidemie, colpi di stato, terremoti e altri disastri.

3.7.3 Declinazioni e Limitazioni del Gestore

Il Gestore non assume alcun ulteriore obbligo, garanzia o responsabilità rispetto a quanto previsto nel presente Manuale Operativo, ovvero dalle vigenti disposizioni di legge, e non sarà responsabile per i danni di qualsiasi natura, da chiunque subiti, qualora tali danni derivino dalla violazione di quanto previsto e contenuto nel presente Manuale Operativo, ovvero dalle vigenti disposizioni di legge.

4 Architettura

4.1 Architettura applicativa

Il sistema SPID è costituito da un insieme di soggetti pubblici o privati, denominati Gestori dell'Identità digitale, che realizzano i servizi di registrazione, attivazione e gestione del ciclo di vita delle identità digitali e delle credenziali di autenticazione utilizzate come strumenti di accesso e autenticazione in rete.
Le principali funzionalità del Gestore delle identità sono quindi: quella di **Registrazione** degli utenti e quella di **Autenticazione** degli utenti.
Il Servizio di Gestione delle Identità digitali può essere logicamente suddiviso in due componenti di Front-End/Interfaccia:

1. **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.
2. **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.

e quattro componenti di Back-End:

1. **Repository SPID**
2. **Modulo di supporto e gestione**
3. **Modulo monitoring e sicurezza**
4. **Modulo servizi di certificazione e autenticazione (CA)**

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

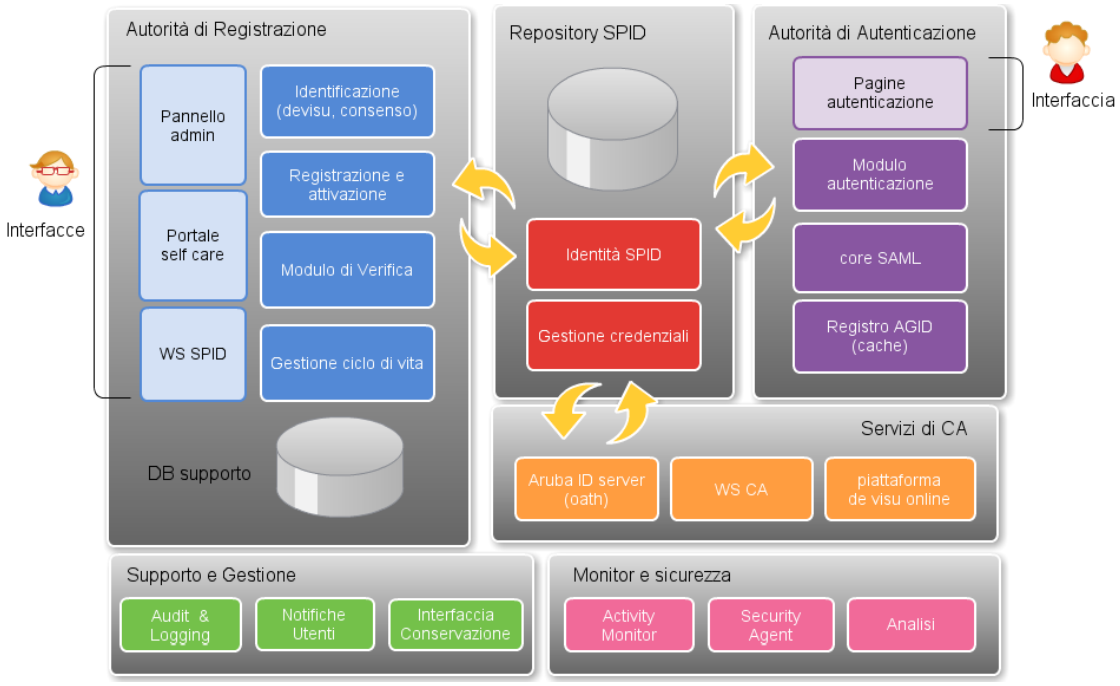

Figura 1 - Architettura applicativa SPID

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 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 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 di 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 (audit e log), e le notifiche.

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

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

4.2 Architettura fisica

Il sistema SPID Aruba è basato, come altri servizi fiduciari erogati da Aruba PEC S.p.A, su infrastrutture di elaborazione ridondate, progettate e realizzate in modo fa garantire alta affidabilità e continuità di servizio.
Sono pertanto utilizzati diversi data center di proprietà del Gruppo Aruba:

1. un sito **primario** ubicato in Via Gobetti 96, Arezzo;
2. un sito **secondario** ubicato in via Ramelli 8, Arezzo;
3. un sito di **disaster recovery** ubicato in Via S. Clemente 53, Ponte San Pietro (BG).

4.3 Architettura dei sistemi di autenticazione

La procedura di autenticazione dell'utente SPID avviene attraverso il colloquio di una serie di componenti applicativi rappresentati nel diagramma seguente.

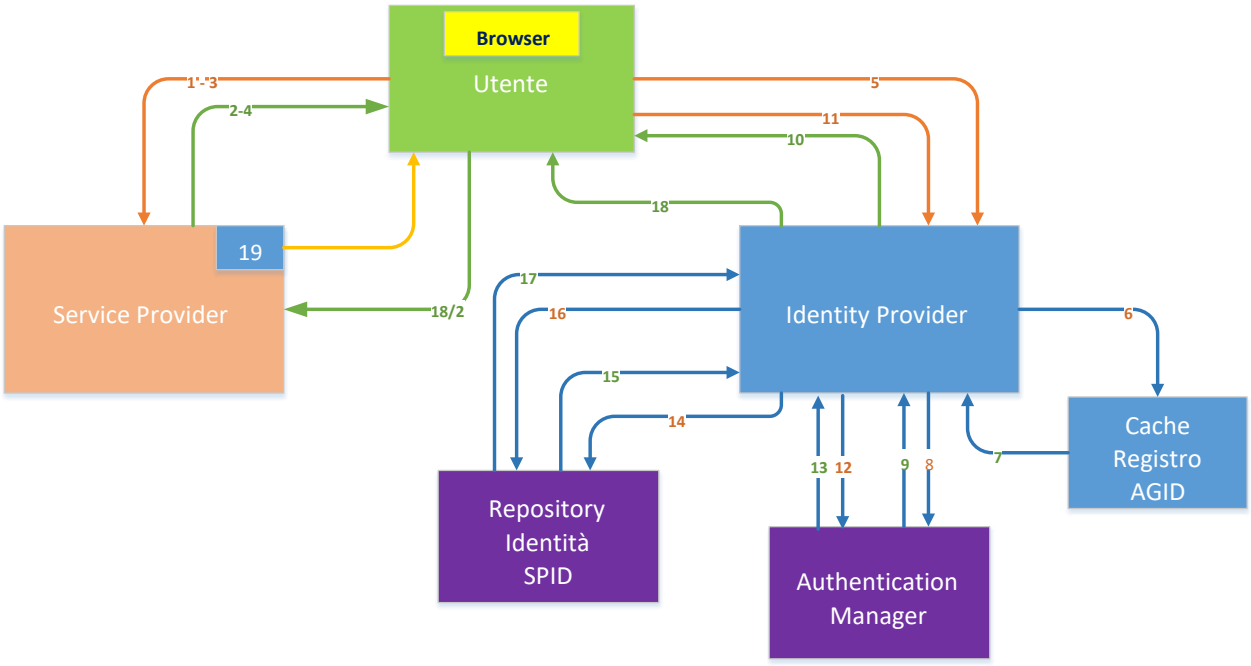

Figura 2 - Architettura sistema di autenticazione

1. Il soggetto titolare della identità digitale (utente) richiede l'accesso ad un servizio collegandosi tramite un browser al portale del fornitore dei servizi (Service Provider)
2. Il Service Provider sottopone all'Utente il Form tramite il quale quest'ultimo può effettuare la scelta dell'IdP
3. L'Utente sceglie il gestore della identità digitale direttamente dall'elenco proposto.
4. Il Service Provider, tenendo conto della scelta dell'utente, restituisce al browser dell'utente una richiesta di autenticazione (*AuthRequest*) contenente eventuali attributi associati al profilo utente
5. Il browser reindirizza la richiesta di autenticazione all'IdP
6. Alfine di verificare che la richiesta provenga da un Service Provider accreditato, l'IdP consulta il Registro AGID presente nella propria cache

7. L'IdP 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.
8. Viene interrogato l'Authentication Manager indicandogli il livello SPID richiesto
9. L'Authentication manager risponde con l'elenco delle relative modalità di autenticazione disponibili per l'Utente (nel caso il soggetto abbia, per uno specifico livello di sicurezza, più credenziali di autenticazione)
10. L'Identity Provider sottopone all'utente la pagina Web tramite la quale lo stesso potrà autenticarsi con una delle modalità disponibili
11. L'Utente dimostra la sua identità utilizzando una delle modalità proposte anche avvalendosi di dispositivi di autenticazione (smart card, OTP, ecc.)
12. L'Identity Provider delega la procedura di autenticazione all'Authentication Manager
13. L'Authentication manager risponde con l'esito della verifica dell'identità e, in caso di esito positivo, con il codice identificativo SPID
14-15. L'Identity Provider, ottenuto il codice identificativo SPID ne verifica lo stato di validità (revoca, sospensione) consultando il Repository delle Identità Digitali
16-17. L'Identity Provider, dopo la verifica positiva dello stato dell'identità digitale, richiede ed ottiene gli attributi indicati nell'AuthRequest
18. L'Identity Provider sottopone all'utente una pagina Web nella quale sono mostrati gli attributi richiesti dal SP e quelli che gli verranno inviati. L'utente fornisce esplicito consenso per l'invio dei dati
19 e 20. L'Identity Provider costruisce l'asserzione SAML e la trasmette, col tramite del browser dell'utente, al Service Provider
21. Il Service Provider, riceve l'asserzione SAML creata dall'IdP
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 SP o con i livelli superiori (se presenti). Ad esempio se il SP richiede un livello 1, le pagine di autenticazione offrono la possibilità di autenticarsi con i livelli 1, 2, 3 (a condizione che il titolare li abbia attivati), se il SP 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 Aruba PEC sono riportarti nella Guida Utente [3].

Modulo di autenticazione
Le pagine si appoggiano ad uno specifico Modulo di Autenticazione che effettua l'autenticazione vera e propria interfacciandosi con i moduli Identità SPID e Gestione Credenziali e verificando:

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 (es codice OTP) 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 dall'utente 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, terza parte garante, attraverso l'adesione dei gestori dell'identità digitale, dei gestori degli attributi qualificati e dei fornitori di servizi.
L'adesione a SPID dei gestori dell'identità digitale, dei gestori degli attributi qualificati e dei fornitori di servizi, si traduce nella presenza dei loro riferimenti all'interno del Registro SPID gestito dall'Agenzia.
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.
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.

4.3.1 Notifiche di accesso

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

4.3.2 Codici e formato messaggi di anomalie

Il servizio di autenticazione SPID dell'IdP Aruba PEC 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 e descritte nella tabella indicata in APPENDICE A - Codici e formati dei messaggi di anomalia.
In aggiunta ai codici e formati sopraindicati, con l'obbiettivo di rendere più esplicativi i messaggi di errore e supportare l'utente nella comprensione dell'evento scatenante, oltreché per massimizzare l'efficacia delle sessioni di assistenza, il servizio di autenticazione SPID integra l'impianto di messaggistica previsto dalla normativa con la seguente tabella di codici e messaggi.

ID	Codice	Evento scatenate
0001	ERRORE_GENERICO	Errore interno al servizio SPID

0002	USERNAME_OBBLIGATORIO	username non specificato
0005	PASSWORD_OBBLIGATORIA	password non specificata
0008	PASSWORD_NON_VALIDA	password non valida
0041	USERNAME_NON_ESISTENTE_IN_ARUBAIdP	username errata
0042	USERNAME_PASSWORD_MISMATCH	username e/o password errati
0043	USERNAME_PASSWORD_OTP_MISMATCH	username e OTP non corrispondono
0045	TIPO_CREDENZIALE_OBBLIGATORIA	tipoCredenziale non corretta o mancante
0046	TIPO_LIVELLO_SPID_OBBLIGATORIO	tipoLivelloSpid non corretto o mancante
0078	OTP_OBBLIGATORIO	otp obbligatorio
0164	ASSENTI_CREDENZIALI_PER_LIVELLO_S PID	assenti credenziali per il livello spid indicato
0168	ERRORE_INVIO_SMS	Impossibile inviare il messaggio SMS
0177	ERRORE_INVIO_EMAIL	Errore durante l'invio della email
0185	IDSPID_PASSWORD_MISMATCH	utente e/o password errati
0205	PASSWORD_SCADUTA	password scaduta
0213	PASSWORD_BLOCCATA_FINO_AL	password bloccata per troppi tentativi falliti, riprovare tra n minuti
0289	USERNAME_PASSWORD_MISMATCH_TENTATIVI_RIMASTI	username e/o password errati: rimangono n tentativi di accesso
0290	IDENTITA_STATO_SOSPESO	Identità in stato sospeso
0291	IDENTITA_STATO_REVOCATO	Identità in stato revocato
0292	IDENTITA_STATO_INATTIVO	Identità in stato inattivo

0293	IDENTITA_STATO_UNDEFINED	Identità in stato non gestito
0294	CONSENSI_CODICE_OBBLIGATORIO	Codice consenso obbligatorio
0303	CREDENZIALE_STATO_SOSPESO	Credenziale in stato sospeso
0304	CREDENZIALE_STATO_REVOCATO	Credenziale in stato revocato
0305	CREDENZIALE_STATO_INATTIVO	Credenziale in stato inattivo
0306	CREDENZIALE_STATO_UNDEFINED	Credenziale in stato non gestito
0309	SESSION_SIGNIN_ERROR	Errore generico su sessione SignIn
0310	SIGNIN_SESSION_MISMATCH	La sessione SignIn non corrisponde
0311	SIGNIN_SESSION_EXPIRED	Sessione SignIn scaduta
0312	ERRORE_ARUBAIDSERVER_VERIFY_OTP	Errore durante la verifica dell'OTP su ArubaIdServer
0313	OTP_LOCKED	Token OTP bloccato su ArubaIdServer
0323	IDENTITA_STATO_NON_ATTIVA	Identità in stato non attiva
0342	CREDENZIALE_STATO_NON_ATTIVA	Credenziale in stato non attiva
0865	CODICE_SICUREZZA_RESET_PASSWORD_ATTESA_INVIO_SENDER “KO”	Codice verifica non valido
0867	CODICE_SICUREZZA_RESET_PASSWORD_BLOCCATO_ATTENDERE_SENDER “KO”	Troppi tentativi di reset password consecutivi
0877	CODICE_SICUREZZA_RESET_PASSWORD_ATTESA_INVIO_VERIFIER “KO”	Codice di verifica expired per reset password
0868	CODICE_SICUREZZA_BLOCCO_IDENTITA_ATTESA_INVIO_SENDER “KO”	Codice di verifica expired per blocco identità
0869	CODICE_SICUREZZA_BLOCCO_IDENTITA_BLOCCATO_ATTENDERE_SENDER “KO”	Troppi tentativi di blocco identità consecutivi

0870	CODICE_SICUREZZA_BLOCCO_IDENTITA_ATTESA_INVIO_VERIFIER “KO”	Codice di verifica expired per sospensione identità
0871	CODICE_SICUREZZA_SOSPENSIONE_CREDENZIALE_ATTESA_INVIO_SENDER “KO”	Codice di verifica expired per sospensione credenziali
0872	CODICE_SICUREZZA_SOSPENSIONE_CREDENZIALE_BLOCCATO_ATTENDERE_SENDER “KO”	Troppi tentativi di sospensione credenziali consecutivi
0873	CODICE_SICUREZZA_SOSPENSIONE_CREDENZIALE_ATTESA_INVIO_VERIFIER “KO”	Codice di verifica expired per sospensione credenziali L2
0881	CODICE_SICUREZZA_SBLOCCO_CREDENZIALE_ATTESA_INVIO_SENDER “KO”	Codice di verifica expired per riattivazione credenziali
0882	CODICE_SICUREZZA_SBLOCCO_CREDENZIALE_BLOCCATO_ATTENDERE_SENDER “KO”	Troppi tentativi di riattivazione credenziali consecutivi
0883	CODICE_SICUREZZA_SBLOCCO_CREDENZIALE_ATTESA_INVIO_VERIFIER “KO”	Codice di verifica expired per sospensione identità verifica
0874	CODICE_SICUREZZA_SOSPENSIONE_IDENTITA_ATTESA_INVIO_SENDER “KO”	Codice di verifica expired per sospensione identità
0875	CODICE_SICUREZZA_SOSPENSIONE_IDENTITA_BLOCCATO_ATTENDERE_SENDER “KO”	Troppi tentativi di sospensione identità consecutivi
0876	CODICE_SICUREZZA_SOSPENSIONE_IDENTITA_ATTESA_INVIO_VERIFIER “KO”	Codice di verifica expired per sospensione identità
0884	CODICE_SICUREZZA_RIATTIVAZIONE_IDENTITA_ATTESA_INVIO_SENDER “KO”	Codice di verifica expired per riattivazione identità
0885	CODICE_SICUREZZA_RIATTIVAZIONE_IDENTITA_BLOCCATO_ATTENDERE_SENDER “KO”	Troppi tentativi di riattivazione identità consecutivi
0866	CODICE_SICUREZZA_RIATTIVAZIONE_IDENTITA_ATTESA_INVIO_VERIFIER “KO”	Codice di verifica expired

		per riattivare identità
0867	CODICE_SICUREZZA_NON_VALIDO “KO”	Codice di verifica non valido

Tabella 1 - Codici aggiuntivi anomalia e messaggi

4.4 Sistemi di autenticazione e credenziali

4.4.1 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, in relazione al tipo della password, il Repository delle Identità SPID impone l’uso delle raccomandazioni baseline per l’ottenimento di password complesse e difficilmente attaccabili:

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

Il Repository SPID inoltre impone i seguenti meccanismi di protezione

1. Impedisce l’uso di formati comuni (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.).
2. 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.
3. Implementa una procedura di sollecito con la quale invita l’utente a modificare la Password secondo le raccomandazioni sopra indicate
4. Memorizzazione cifrata delle password: Le password non sono mai memorizzate in chiaro se non in forma irreversibile (tramite hash crittografico) all’unico scopo di verificare la validità della credenziale sottoposta dall’utente in fase di autenticazione

4.4.2 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 dal par. 4.4.1, 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 Fisici,
OTP mobile, ArubaCall e OTP SMS. Inoltre il sistema è già predisposto per utilizzare strumenti OTP di altra natura quali, a titolo di esempio, OTP con display a eventi o a tempo, OTP USB, display card, ecc.

4.4.2.1 Autenticazione tramite OTP fisico e SMS

OTP Fisici event-based o time based con display

Il Token OTP hardware-display si presenta come una chiavetta dotata di display LCD e pulsante per la generazione dei codici temporanei. Il punto di forza di questi dispositivi è la loro totale similarità con i dispositivi di accesso sicuro ai portali di home-banking, sempre più diffusi ed utilizzati dagli utenti.
Le caratteristiche tecniche e di sicurezza dei dispositivi OTP fisici event-based e time based forniti da Aruba PEC sono tali da garantire i seguenti requisiti funzionali:

1. Il dispositivo OTP è conforme alle specifiche OATH
2. Il dispositivo OTP non può essere clonato
3. Il dispositivo OTP possieda un sistema antitampering basato su meccanismi di tamper evidence e tamper response
4. Il dispositivo OTP è univocamente identificabile

OTP Fisici event-based a sfioramento

Il Token OTP hardware-touch si presenta come una chiavetta USB per PC che viene rilevata come un normale dispositivo di input (es: tastiera o mouse). Dopo il collegamento è possibile generare codici OTP semplicemente sfiorando con le dita l'area appositamente predisposta sopra il token.
Le caratteristiche tecniche e di sicurezza di questi dispositivi OTP sono tali da garantire i seguenti requisiti:

1. Il dispositivo OTP è conforme alle specifiche OATH
2. Il dispositivo OTP non può essere clonato
3. Il dispositivo OTP possieda un sistema antitampering basato su meccanismi di tamper evidence e tamper response
4. Il dispositivo OTP è univocamente identificabile

OTP SMS

Si tratta di un sistema di autenticazione OTP destinato ad essere utilizzato, per alcuni casi specifici e a fronte di accordi con l'IdP, 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.

4.4.2.2 Autenticazione tramite App Aruba ID

OTP Mobile

OTP Mobile è un'applicazione per smartphone di ultima generazione installabile sui più comuni cellulari quali iPhone e Android. Consiste in una applicazione ad eventi che, una volta inizializzata con il codice di attivazione fornito in fase di registrazione, genera one time password su richiesta. L'applicazione presenta tutte le caratteristiche di sicurezza e facilità d'uso ed è già utilizzata da decine di migliaia di utenti.

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.

QR Code

L'utente Aruba ID ha la possibilità di effettuare il processo di autenticazione anche tramite App Aruba ID.

Per poter effettuare l'autenticazione tramite QR Code è necessario configurare la App Aruba ID.

La configurazione consiste nei seguenti passaggi:

- L'utente, tramite l'App store relativo al proprio sistema operativo (Google Play Store per Android o Apple App Store per iOS), scarica l'applicazione sul proprio dispositivo;
- L'utente configura nell'app il token per lo specifico servizio SPID, scansionando un QR Code o inserendo un codice di attivazione, ed inserendo nelle apposite maschere delle pagine web di attivazione del token un primo codice OTP generato dall'App;
- L'accesso all'App può essere protetto tramite PIN (facoltativo) o biometria;
- La biometria è necessaria per abilitare il token alla modalità di autenticazione tramite scansione del QR Code e per completare una autenticazione dopo aver scansionato il QR Code presente nella sezione di autenticazione.

L'utente, a questo punto, può utilizzare l'autenticazione tramite QR Code, eseguendo i seguenti step.

Per l'accesso tramite altro device (PC, tablet etc.):

- L'utente si collega al sito del Service provider presso cui deve fare accesso;
- L'utente sceglie il Gestore di identità Aruba;
- Il portale di autenticazione mostra, a fianco alla consueta sezione di autenticazione con username e password, un QR Code con validità limitata nel tempo (qualora tale validità si esaurisca, è possibile ricaricare il codice);
- L'utente, a questo punto, può scansionare il QR Code direttamente dall'App della fotocamera dello smartphone (l'app si aprirà automaticamente) o in alternativa, dopo aver aperto l'App, tramite il bottone "SCANSIONA QR CODE";
- L'utente, dunque, inquadra tramite la fotocamera del proprio dispositivo il QR Code presente nell'apposito riquadro di login;
- L'applicazione Aruba ID chiede all'utente di effettuare il riconoscimento biometrico;
- Una volta che l'utente risulta autenticato tramite biometria e scansionato correttamente il QR Code, apparirà in applicazione un messaggio all'utente che gli conferma l'avvenuta autorizzazione all'accesso;
- A questo punto, il portale di autenticazione su cui l'utente sta navigando sul browser del dispositivo PC/Tablet intercetterà l'avvenuta autenticazione avvenuta tramite l'App Aruba ID ed aggiornerà la propria pagina rimandando l'utente allo step successivo

dell'autenticazione SPID, ovvero la pagina di autorizzazione all'invio degli attributi al Service Provider.

Per l'accesso tramite lo stesso dispositivo mobile:

- L'utente si collega al sito del Service provider presso cui deve fare accesso;
- L'utente sceglie il Gestore di identità Aruba;
- All'utente, a questo punto, verrà fornita la possibilità di accedere tramite username e password o tramite Applicazione mobile;
- L'utente seleziona l'opzione "Usa l'app ARUBA ID – Accedi più rapidamente";
- A questo punto, l'utente, che verrà reindirizzato sulla App Aruba ID, viene riconosciuto con biometria;
- La app conferma all'utente l'autorizzazione di accesso concessa e indica all'utente di tornare alla schermata di autenticazione;
- A questo punto, il portale di autenticazione su cui l'utente sta navigando intercetterà l'avvenuta autenticazione avvenuta tramite l'App Aruba ID ed aggiornerà la propria pagina rimandando l'utente allo step successivo dell'autenticazione SPID, ovvero la pagina di autorizzazione all'invio degli attributi al Service Provider.

4.4.3 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, sull'utilizzo di certificati digitali le cui chiavi private sono custodite su dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo.
Tra questi dispositivi sono compresi:

1. Carta Nazionale dei Servizi
2. Smart card conformi ai requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo da parte dell'Organismo di Certificazione della sicurezza informatica (OCSI) o da altro organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della Direttiva
3. Hardware Security Modules (HSM) per i quali sia stata riconosciuta la conformità ai requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo da parte dell'Organismo di Certificazione della sicurezza informatica (OCSI) o da altro organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della Direttiva

4.5 Misure anticontraffazione

4.5.1 Livello 2

Di seguito è riportata una descrizione generale delle misure anticontraffazione garantite dalle credenziali di livello 2.
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 SPID con credenziali di tipo OTP, ovvero:

1. Il dispositivo OTP non deve essere duplicabile;
2. Il dispositivo OTP deve avere un meccanismo in grado di rilevare o contrastare attivamente i tentativi di manomissione;
3. Ogni dispositivo OTP può essere identificato in modo univoco.

OTP Fisici event-based o time based con display

Questi dispositivi garantiscono i 3 requisiti indicati sopra attraverso l'adozione delle seguenti tecniche

Requisito	Conformità
1	Ogni dispositivo è inizializzato con seed segreti ed univoci (informazioni seme). Questi seed sono generati randomicamente attraverso motori PRNG e sono memorizzati in fase di costruzione del token all'interno del guscio plastico antitamper
2	Il supporto è progettato in modo da prevedere meccanismi di protezione antitampering che permetto di rilevare (fisicamente e logicamente) tentativi di manomissione del token e, nel caso si verifichino, cancellare in modo sicuro tutte le informazioni memorizzate al suo interno.
3	Ogni dispositivo possiede un numero di serie univoco cablato a livello fisico e logico

OTP Fisici event-based a sfioramento

Questi dispositivi garantiscono i 3 requisiti indicati sopra attraverso l'adozione delle stesse tecniche descritte nel caso degli OTP Fisici con display

App Aruba ID

L'applicazione per smartphone Aruba ID è in grado di garantire i 3 requisiti indicati sopra oltre che livelli di sicurezza equivalenti a quelli offerti dai tradizionali dispositivi hardware-based.

Requisito	Conformità
1	L'applicazione, dopo l'inizializzazione, effettua un binding crittografico al particolare smart phone impendendo l'esecuzione al di fuori di esso.
2	L'applicazione, in fase di avvio, prevede meccanismi di controllo della firma del codice per prevenire sostituzioni malevole o accidentali delle proprie componenti
3	L'app, dopo l'inizializzazione, genera un proprio unique ID derivandolo dal set di dati utilizzati per il binding al dispositivo

In aggiunta ai meccanismi di protezione sopradescritti l'App Aruba ID prevede un sistema di controllo e notifica per l'utente come strumento cautelativo nel caso che il dispositivo stia operando in condizioni anomale: es privilegi di amministratore (Rooting o Jailbreak).

OTP SMS

OTP SMS è il servizio di strong authentication di Aruba PEC nel quale, prima dell'autenticazione, l'utente riceve un SMS dalla CA in cui è contenuto il codice OTP.
L'utente, per completare il processo di firma, sottopone al sistema il codice contenuto nel messaggio questo permetterà di completare il processo di firma.
Questo meccanismo OTP è in grado di garantire il soddisfacimento dei 3 requisiti indicati sopra oltre che livelli di sicurezza equivalenti a quelli dei dispositivi hardware-based.

Requisito	Conformità
1	Per clonare il dispositivo OTP sarebbe necessario clonare la SIM telefonica. In ogni caso il messaggio, e quindi il codice OTP, perverrebbe all'attaccante e al titolare allertando quest'ultimo.
2	Questo tipo di OTP non presenta vulnerabilità a possibili tentativi di manomissione
3	Lo unique ID è dato dal numero di telefono del titolare

Ulteriori valutazioni sulle misure anticontraffazione sono effettuate da Aruba e descritte all'interno dei propri documenti di Analisi di Rischio e di Piano della Sicurezza.

4.5.2 Livello 3

Le credenziali di livello 3, così come indicato in 5.4.3, sono basate sull'uso di certificati digitali le cui chiavi private sono custodite in dispositivi che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo e s.m.i.
Ognuno dei dispositivi indicati in 5.4.3 possiede un rapporto di conformità ai requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE emesso dal pertinente organismo pubblico o privato designato dallo Stato membro e opportunamente notificato ai sensi dell'Art 11 comma 1 let b.
Per eventuali ulteriori approfondimenti di natura tecnica sulle misure anticontraffazione previste per le credenziali di livello 3 si può far riferimento alle norme in materia secondo le quali vengono condotte le valutazioni di conformità all'Allegato 3 della Direttiva sopraindicate:

https://www.commoncriteriaportal.org/files/ppfiles/pp0004b.pdf
https://www.commoncriteriaportal.org/files/ppfiles/pp0059b_pdf.pdf
https://www.commoncriteriaportal.org/files/ppfiles/pp0075b_pdf.pdf

4.6 Tracciatura degli accesi

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 logici e fisici ai sistemi sono controllati e registrati.

4.6.1 Accessi fisici

Viene garantito che l'accesso ai locali sia possibile solo a coloro che ne hanno effettiva necessità, previa registrazione alla reception, e che l'accesso alle sale tecniche sia consentito solo agli addetti autorizzati, previa identificazione mediante badge e relativo PIN.
I server del sistema IdP sono ospitati in sale tecniche ad accesso controllato attraverso badge e/o fattore biometrico.
Solo il personale autorizzato può accedere a tali sale.

4.6.2 Accessi logici

Prima di qualsiasi interazione con il sistema IdP, l'utente privilegiato (es. operatore di registrazione, 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 od esterna) viene assegnata un'utenza personale e univoca. Le utenze "di gruppo" sono ammesse solo per specifiche eccezioni espressamente autorizzate.

4.6.3 Tracciature accessi di autenticazione utenti

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

1. Indirizzo IP pubblico di provenienza;
2. Identificativo univoco dell'utente;
3. Operazione effettuata;
4. Riferimento temporale dell'operazione.

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 di un **log certificato**.
Secondo quanto definito dalle Regole Tecniche, Aruba mantiene il Registro delle transazioni che contiene i tracciati delle richieste di autenticazione dell'utente 24 mesi. Nel caso di SPID minori, Aruba mantiene per 24 mesi anche i log delle autorizzazioni fornite dal Genitore per l'accesso del minore ai servizi, come previsto dalle "Linee guida operative per la fruizione dei servizi SPID da parte dei minori" [15].
L'accesso in lettura e scrittura ai sistemi che custodiscono le tracciature è garantito al solo personale tecnico dell'IdP secondo le policy descritte ai paragrafi 4.6.1 e 4.6.2.
In caso di richiesta di accesso ai log da parte delle autorità, le modalità di acquisizione delle tracciature prevedono il coinvolgimento tecnico dell'IdP ed il recupero di una versione dei log relativamente piccola, indicizzata e adatta ad una rapida identificazione di utente, operazione e riferimento orario.
Rimane sempre garantita la possibilità di accesso ad una versione più ricca di informazioni.

5 Operatività

Questa sezione descrive le modalità con le quali opera il Gestore ed 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 soggetto 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.

5.1 Funzioni del personale addetto al servizio di gestione delle identità digitali

Tutto il personale di Aruba PEC S.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.
I soggetti addetti alla gestione del SPID, nel rispetto del regolamento di cui all'Art 4, comm. 3, del DPCM, 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

Le cariche di cui alle lettere a) e c) sono incompatibili con le altre. Le cariche di cui alle lettere a) e d) sono ricoperte da personale alle dirette dipendenze di Aruba PEC S.p.A.

5.2 Richiesta dell'identità digitale

Aruba PEC S.p.A., in qualità di IdP, rilascia le identità digitali su richiesta di un soggetto interessato secondo quanto previsto dall'art. 7 del DPCM. L'istanza viene effettuata attraverso la presentazione di una richiesta di adesione che contiene tutte le informazioni necessarie per l'identificazione del soggetto richiedente.
Di seguito si descrivono le procedure utilizzate per l'identificazione del richiedente al fine di rilasciare una delle seguenti tipologie di identità digitali erogate da Aruba PEC:

- Identità digitale SPID Persona Fisica;
- Identità digitale SPID Persona giuridica (di tipo 2 standard oppure finalizzata al rilascio e alla gestione di identità SPID Persona Giuridica Uso Professionale, come descritto ai paragrafi 5.2.1.1 e 5.2.2.1);
- Identità digitale SPID Persona Fisica Uso Professionale;

- Identità digitale SPID Persona Fisica Minore;
- Identità digitale SPID Persona giuridica Uso Professionale.

La richiesta può essere effettuata online o da sportello, come descritto di seguito. Il titolare dell'identità digitale dovrà effettuare l'identificazione per concludere il processo di rilascio.

5.2.1 Richiesta dell'identità SPID da sportello

La richiesta dell'identità SPID viene effettuata dal richiedente presso un soggetto incaricato dal Gestore denominato Centro di Registrazione Locale (CDRL).
In questa modalità di richiesta, è prevista la presenza fisica del soggetto Richiedente dinnanzi ad un incaricato del CDRL definito Operatore di Registrazione (OdR).
Si precisa che il CDRL opera in forza e previa stipula di specifico contratto con Aruba PEC; in detto contratto il CDRL indica anche il personale di cui intende avvalersi per la sua esecuzione: detto personale, che dovrà operare nel contesto delle pratiche operative di identificazione e registrazione sarà definito Operatore di Registrazione (OdR).
L'autorizzazione e successivamente la qualificazione degli OdR come abili alle operazioni di identificazione, registrazione e rilascio, avviene mediante corso di formazione e superamento di una verifica scritta. A seguito della firma da parte dei rispettivi legali rappresentati del certificatore e del CDRL e previa qualificazione degli OdR, il Gestore rende disponibili agli OdR 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 OdR sono sotto il costante controllo del Gestore.
Inoltre rimane la facoltà per Aruba PEC di nominare degli Incaricati al Riconoscimento (IR) direttamente all'interno della propria organizzazione al fine di espletare le attività operative di identificazione e registrazione.

L'istanza viene effettuata attraverso la presentazione di un modulo di richiesta di adesione che contiene tutte le informazioni necessarie per l'identificazione del soggetto richiedente.
Nel modulo di richiesta di adesione sono contenuti:

1. i dati identificativi del richiedente, che andranno a costituire gli attributi identificativi dell'identità digitale;
2. informazioni che consentono di gestire in maniera efficace il rapporto tra il gestore ed il titolare della identità digitale, che andranno a costituire gli attributi secondari dell'identità digitale (email, cellulare);

Per le persone fisiche sono considerate obbligatorie le seguenti informazioni:

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

Sono considerate obbligatorie per le persone giuridiche le seguenti informazioni:

a. denominazione/ragione sociale;
b. codice fiscale o P.IVA (se uguale al codice fiscale);
c. sede legale;
d. certificazione con indicazione amministratori e/o rappresentanti legali (in alternativa atto notarile di procura legale) e data di rilascio e validità dello stesso;
e. estremi del documento di identità utilizzato dal rappresentante legale;
f. gli attributi secondari così come definiti all'art. 1 comma 1 lettera d) del DPCM.

Nel caso in cui il soggetto richiedente l'identità digitale in nome e per conto della persona giuridica non sia cittadino italiano e non sia dotato di un documento di riconoscimento rilasciato in Italia, è prevista una modalità di richiesta del servizio esclusivamente online così come descritto al par. 5.2.2.
Relativamente agli attributi secondari, dovranno essere forniti almeno un indirizzo di **posta elettronica ed un recapito di telefonia mobile** che verranno entrambi verificati dagli operatori Aruba PEC S.p.A. o suoi delegati, ad esempio inviando una mail all'indirizzo di posta elettronica dichiarato, con il link ad una URL per la verifica e certificazione e un SMS o chiamata di verifica al numero di cellulare veicolanti un codice numerico di controllo che dovrà essere riportato all'IdP come risposta.

5.2.1.1 Richiesta a sportello dell'identità SPID Persona Giuridica Uso Professionale

Secondo quanto stabilito dalle "Linee guida per il rilascio dell'identità digitale per uso professionale" emanate da AgID [16], Aruba PEC può rilasciare identità digitali SPID per uso professionale per la persona giuridica (identità di tipo 4, come da Avviso n.18 v.2/2020).
Tale identità digitale, come definito dall'Avviso SPID n. 40/2022, è utile a provare l'appartenenza di una persona fisica all'Organizzazione di una persona giuridica e/o la sua qualità di professionista e di conseguenza, può essere utilizzata per le attività lavorative svolte quale dipendente o collaboratore, a qualunque titolo, della persona giuridica che ha autorizzato il rilascio.

L'IdP prevede la possibilità che l'attivazione di una o più identità digitali di tipo 4 possa essere richiesta presso un soggetto incaricato dal Gestore denominato Centro di Registrazione Locale (CDRL). Il processo di richiesta deve avvenire nel rispetto dei seguenti pre-requisiti:

1. L'Organizzazione deve disporre di un'identità SPID Persona giuridica rilasciata da Aruba PEC per l'esclusiva finalità di richiedere e gestire identità SPID di tipo 4;
2. Il dipendente/collaboratore che richiede l'emissione di una identità di tipo 4 deve essere appartenente all'Organizzazione di cui al punto 1.

Di seguito è descritto il flusso di richiesta, registrazione e rilascio di una identità SPID di tipo 4:

L'operatore incaricato svolge l'attività di registrazione dei dati identificativi del richiedente che andranno a costituire gli attributi identificativi dell'identità digitale come previsto dal presente Manuale (si veda il par. 5.4).

Il richiedente sceglie una modalità di identificazione tra:

- modalità di identificazione con webcam (descritta al par. 5.3.1.2), oppure:
- una tra le modalità di identificazione informatica (descritte al par. 5.3.2.) supportate, ossia tramite TS-CNS, CNS, SPID persona fisica, CIE o firma digitale. Nel caso di identificazione tramite firma digitale, è prevista la possibilità che l'operatore del CDRL rilasci al richiedente un certificato di firma elettronica qualificata col quale sottoscrivere, anche contestualmente al rilascio, il modulo di richiesta di adesione SPID ed espletare la fase di riconoscimento per il rilascio dell'identità SPID di tipo 4.

L'attivazione dell'identità digitale di tipo 4 è subordinata alla corretta esecuzione dei punti precedenti nonché all'attestazione da parte dell'Organizzazione dell'appartenenza del Richiedente all'Organizzazione stessa, in qualità di dipendente o collaboratore. L'attestazione avviene tramite la raccolta di un'evidenza informatica (es. checkbox o altra forma di evidenza elettronica) da parte di un apposito servizio messo a disposizione dall'IdP, al quale l'Organizzazione accede attraverso l'identità SPID Persona giuridica rilasciata per tale finalità (e credenziali di livello 2).
Il Richiedente, una volta che è stata autorizzata la richiesta, riceverà indicazioni da parte dell'IdP per portare a termine il processo di attivazione dell'identità SPID di tipo 4 ed eventualmente le istruzioni per effettuare l'identificazione, qualora non sia ancora stata completata.

5.2.2 Richiesta dell'identità SPID online

Il richiedente accede al portale messo a disposizione dall'IdP e richiede una delle tipologie di identità digitale indicate al paragrafo 5.2 (ad esclusione dell'identità SPID Persona giuridica Uso professionale, cft. 6.2.2) secondo il flusso di seguito descritto:

1. L'utente richiedente accede al sito web dell'IdP e richiede di attivare l'identità digitale SPID prescelta, selezionando una tra le seguenti modalità di identificazione:
   I. Identificazione informatica via CNS/TS-CNS-CIE;
   II. Identificazione tramite sottoscrizione con Firma Digitale o Remota;
   III. Identificazione a vista da remoto con riconoscimento via webcam (DVO);
   IV. Identificazione con SPID Persona Fisica (precedentemente rilasciata da Aruba PEC e limitatamente all'ottenimento di identità SPID di tipologia diversa da Persona Fisica).

   Dopo aver scelto la modalità di identificazione, vengono raccolti i consensi al trattamento dei dati personali e all'adesione al servizio e vengono fornite opportune notifiche al fine di:
   I. Fornire informativa sul trattamento dei dati (art. 13 del Regolamento UE 2016/679) ed ottenere i necessari consensi
   II. Rendere esplicitamente consapevole il richiedente del fatto che chiunque renda dichiarazioni mendaci è punibile ai sensi del codice penale e delle leggi speciali in materia (art. 76 del DPR 445/2000)
   III. Assicurarsi che il richiedente sia consapevole dei termini e condizioni associati all'utilizzo del servizio di identità digitale

IV. Assicurarsi che il richiedente sia consapevole delle raccomandazioni e precauzioni da adottare per l'uso delle identità digitali

Su questa pagina l'utente dovrà dare esplicita approvazione e presa visione dei punti sopra indicati.

2. Form con richiesta di inserimento dei seguenti dati

Dati di accesso:

I. username
II. password
III. conferma password

Nel caso in cui la username fornita sia già associata ad un'identità digitale il sistema ne dà evidenza ed offre la possibilità di inserirne una nuova.
Nel corso dell'inserimento dei dati verrà effettuata una verifica sul grado di sicurezza 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 al par. 4.4.1.

Dati di contatto:

I. email
II. numero di cellulare

Dati anagrafici

I. Codice fiscale
II. Nome
III. Cognome
IV. Sesso
V. Data nascita
VI. Luogo nascita (Stato, Provincia, Comune)
VII. Numero di Tessera Sanitaria
VIII. Email PEC
IX. File con scansione fronte retro della Tessera Sanitaria e del Documento di Identità (nel caso di riconoscimento de visu)

Dati di domicilio

I. Luogo domicilio (Stato, Provincia, Comune)
II. Indirizzo domicilio (via, civico, CAP)

Documento di identità

I. Tipo di documento
II. Numero documento

III. Data emissione
IV. Data scadenza
V. Ente emittente

3. Form di verifica email.

Al termine del passo precedente viene inviata una mail con un codice che deve essere digitato e verificato in questo passo.
È possibile modificare in questo passaggio l'indirizzo mail se ci si accorge di aver fornito un indirizzo sbagliato (es. errore di battitura).

4. Form di verifica del numero di cellulare.

Al termine del passo precedente viene inviato un SMS con un codice che deve essere digitato e verificato in questo passo.
È possibile modificare in questo passaggio il numero di telefono se il cliente si accorge di aver fornito il recapito sbagliato (es. errore di battitura).
Al termine del flusso descritto si ha un un'identità digitale creata (ma non attiva).

Nel caso in cui il soggetto richiedente l'identità digitale in nome e per conto della persona giuridica non sia cittadino italiano e non sia dotato di documento di riconoscimento rilasciato in Italia, è prevista la sola modalità di identificazione tramite sottoscrizione con Firma Digitale o Remota – punto 1-II.

5.2.2.1 Richiesta online dell'identità SPID Persona Giuridica Uso Professionale

In riferimento alle "Linee guida per il rilascio dell'identità digitale per uso professionale" emanate da AgID [16], l'IdP prevede la possibilità che l'attivazione di una o più identità digitali SPID Persona Giuridica Uso Professionale, possa essere richiesta online dall'identità SPID Persona Giuridica rilasciata da Aruba PEC per l'esclusiva finalità di richiedere identità SPID di tipo 4, tramite apposito servizio messo a disposizione dall'IdP.
In questo caso, il processo di richiesta e rilascio avviene secondo le modalità di seguito descritte:

- Accesso al servizio messo a disposizione dall'IdP tramite l'utilizzo dell'identità digitale Persona Giuridica rilasciata per tale finalità (con credenziali di livello 2);
- Richiesta di attivazione di una o più identità digitali di tipo 4 per i propri collaboratori/dipendenti. In corrispondenza di ciascuna identità richiesta è necessario indicare: nome, cognome, codice fiscale e indirizzo email del collaboratore/dipendente.
- Attestazione della persona giuridica dell'appartenenza del collaboratore/dipendente alla propria Organizzazione (es. checkbox o altra forma di evidenza elettronica raccolta tramite il servizio messo a disposizione dall'IdP);
- Ricezione, all'indirizzo email del collaboratore/dipendente, di un link per portare a termine il processo di registrazione. Il collaboratore/dipendente dovrà:
  - scegliere username e password;
  - inserire i dati personali necessari alla registrazione per il rilascio dell'identità SPID di tipo 4;

  - selezionare un metodo di riconoscimento tra quelli descritti al par. 5.3 (ad eccezione del punto 1, identificazione de visu);
  - configurare eventuali strumenti per il rilascio delle credenziali di autenticazione forte;
- Esecuzione dell'identificazione attraverso il metodo scelto al punto precedente;
- Una volta compiuti i controlli di sicurezza previsti (si veda il par. 5.4), l'IdP attiverà l'identità digitale di tipo 4.

Il livello dell'identità SPID di tipo 4 è sempre pari o inferiore a quello dell'identità SPID Persona Giuridica alla quale è associata.
L'IdP mette a disposizione dell'Organizzazione un servizio tramite cui permette di gestire le identità SPID di tipo 4 associate all'Organizzazione stessa. Accedendo al servizio tramite l'identità SPID Persona Giuridica rilasciata per tale finalità (con credenziali di livello 2), l'Organizzazione può:

1. Visualizzare tutte le identità collegate alla persona giuridica e il relativo stato;
2. Richiedere l'attivazione di ulteriori identità collegate (secondo le modalità descritte sopra);
3. Richiedere la revoca delle singole identità collegate;
4. Richiedere il rinnovo delle singole identità collegate.

In caso di revoca o sospensione dell'identità SPID Persona Giuridica rilasciata per gestire le identità SPID di tipo 4 associate, Aruba PEC procede alla revoca o sospensione delle identità di tipo 4 associate almeno entro i due mesi successivi, per permettere alla Persona Giuridica la riattivazione dell'identità (in caso di sospensione) o la richiesta di una nuova identità SPID Persona Giuridica (in caso di revoca) per continuare a gestire anche le identità della Persona Giuridica ad Uso professionale, già rilasciate e associate alla stessa.

5.2.3 *Richiesta dell'identità digitale per un soggetto minore*

In coerenza con quanto previsto dalle "Linee guida operative per la fruizione dei servizi SPID da parte dei minori" pubblicate da AgID, Aruba PEC permette il rilascio dell'identità digitale SPID in favore dei minori (di età compresa tra 5 e 17 anni) rendendo apposita informativa sul trattamento dei dati personali del minore [15].

Il rilascio dell'identità digitale SPID al minore è subordinato alla richiesta da parte del genitore richiedente all'IdP Aruba PEC, tramite credenziali SPID di almeno livello 2 fornite da Aruba PEC. Il genitore per effettuare la richiesta deve:

- fornire i dati relativi al minore in favore del quale intende chiedere il rilascio di SPID: nome, cognome, codice fiscale, data nascita, email.
- fornire il consenso al trattamento dei dati personali del minore forniti;
- accettare la ricezione di notifiche da parte di Aruba PEC per l'autorizzazione all'utilizzo di SPID da parte del minore, ove previsto.

Inoltre come previsto dalle Linee guida [15], prima del rilascio dell'identità digitale al minore, Aruba PEC è tenuta a richiedere e acquisire a sistema:

- dichiarazione del Genitore, ai sensi dell'art. 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i., di essere autorizzato alla richiesta di SPID da parte dell'eventuale Genitore non richiedente (allegando documento di identità in corso di validità dell'eventuale Genitore non richiedente) o di essere l'unico esercente la responsabilità genitoriale sul minore, fornendo apposita documentazione a conferma (presentando copia di un documento che attesti di essere l'unico esercente la responsabilità genitoriale, ad es. stato di morte dell'altro genitore, nomina in qualità di tutore, ecc.).

Successivamente all'invio della richiesta, Aruba PEC assegna al minore un codice di verifica, comunicandolo al genitore richiedente. Il minore utilizza tale codice di verifica per ottenere l'identità digitale SPID all'avvio della procedura di identificazione messa a disposizione dal Gestore Aruba PEC.

Aruba PEC permette al soggetto minore di scegliere tra più modalità di identificazione (si veda il par. 5.3) verificando la corrispondenza della sua identità con i dati precedentemente forniti dal genitore.

Si specifica che il genitore richiedente è l'unico soggetto che può avere diritto a gestire l'identità digitale SPID del minore per il quale ha fatto richiesta, in particolare il Gestore revocherà l'identità SPID del minore nel caso in cui il genitore non sarà più titolare di un'identità SPID attiva.

5.3 Modalità di identificazione ai fini del rilascio dell'identità digitale

Una volta terminata la fase di registrazione online, si passa alla verifica dell'identità del soggetto richiedente. Detta verifica, come anticipato nella fase di richiesta dell'identità, può essere svolta attraverso:

1. Identificazione *De-visu*;
2. Identificazione con webcam (attraverso sessione audio/video);
3. Identificazione mediante TS-CNS, CNS, CIE;
4. Identificazione mediante firma digitale o firma remota;
5. Identità SPID Persona Fisica precedentemente rilasciata da Aruba PEC e limitatamente all'ottenimento di identità SPID di tipologia diversa da Persona Fisica.

Le prime due modalità prevedono la presenza di personale opportunamente formato ed abilitato, mentre le altre possono essere completate in autonomia dal richiedente mediante apposita procedura guidata.

5.3.1 Identificazione con operatore

Per quanto riguarda le modalità di cui ai punti 1) e 2), le pratiche operative per l'identificazione del richiedente sono svolte dalle stesse strutture indicate al par. 5.2.1.

In riferimento all'identità digitale SPID rilasciata ai minori, il Gestore mette a disposizione come metodo di identificazione con operatore l'identificazione attraverso sessione audio-video.

In entrambi i casi, il processo di identificazione del soggetto Richiedente potrà essere soggetto a ulteriore verifica da parte di Operatori Supervisori (OS), il quale si riserva il diritto - qualora siano riscontrate irregolarità - di rigettare la richiesta di adesione al Servizio.

5.3.1.1 IDENTIFICAZIONE DE-VISU (DA SPORTELLO)

L'identificazione de visu avviene mediante una rete di sportelli dislocati su tutto il territorio nazionale (CDRL e IR) ed è prevista la presenza fisica del soggetto richiedente dinnanzi ad un incaricato del Gestore addetto all'identificazione.
Durante il processo di rilascio l'operatore effettua un riconoscimento de visu del richiedente e ne verifica l'identità facendosi consegnare un documento di riconoscimento, munito di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato. Sono ammessi i seguenti documenti di identità e di riconoscimento equipollenti tra di loro, così come previsto dall'art. 35 del DPR 28 dicembre 2000, n. 445 e s.m.i.:

- Carta d'Identità italiana
- Passaporto italiano
- Patente di guida italiana

In particolare durante la fase di identificazione a vista del soggetto richiedente l'incaricato dell'IdP procede con acquisizione del modulo di richiesta di adesione compilato su supporto cartaceo sottoscritto in modalità autografa.
In questo caso:

1. se il soggetto richiedente è una persona fisica, dovrà essere esibito un valido documento d'identità;
2. se il soggetto richiedente è una persona giuridica, dovrà essere fornita procura attestante i poteri di rappresentanza conferiti alla persona fisica che materialmente presenta l'istanza che a sua volta è tenuta ad esibire un valido documento d'identità.

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 la tessera sanitaria.
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 interrotto fino alla esibizione di documenti validi ed integri.

5.3.1.2 IDENTIFICAZIONE ATTRAVERSO SESSIONE AUDIO-VIDEO (IDENTIFICAZIONE CON WEBCAM)

La procedura di Identificazione attraverso la sessione audio-video consente all'operatore o incaricato del Gestore, di identificare in maniera certa il richiedente dell'identità digitale mediante l'ausilio di strumenti di registrazione audio-video e nel rispetto delle misure prescritte dal Garante Privacy in merito al trattamento dei dati personali.

Così come previsto dai regolamenti di cui all'Art 4 comma 2 del DPCM, l'identificazione da remoto avviene attraverso modalità tali da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte del Richiedente.
La sessione audio-video che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'identità e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di distorsione o disturbo: le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto e fluidità; l'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi.
Il Gestore si assume la responsabilità della valutazione in merito alla sussistenza delle condizioni suddette e l'operatore preposto all'attività può quindi interrompere 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 soggetto richiedente.
Per il riconoscimento con operatore via webcam, il richiedente è tenuto a:

- effettuare un test audio-video per verificare la compatibilità del microfono e della webcam;
- visualizzare ed accettare il modulo di richiesta identità SPID contenente i dati confermati in fase di pre-registrazione;
- confermare di aver preso visione dell'informativa privacy, esprimere il consenso al trattamento dei dati personali per la registrazione audio-video.

In riferimento al rilascio dell'identità digitale SPID ad un soggetto minore (si veda il par. 5.2.3), si specifica che la fase di identificazione del minore prevede obbligatoriamente, per la modalità di identificazione con webcam, la compresenza del genitore nel caso in cui il minore sia infraquattordicenne o la presenza facoltativa del genitore nel caso in cui sia ultraquattordicenne [15].
Nel caso di un minore infraquattordicenne, inoltre, il consenso al trattamento dei dati personali per la registrazione audio-video deve essere espresso dal genitore.

Di seguito si descrive il processo di identificazione del Richiedente l'Identità digitale attraverso una sessione audio-video. Il Richiedente può effettuare la procedura di riconoscimento tramite webcam in due modi:

1. Con un normale PC che soddisfi i seguenti requisiti:
   a. Presenza di webcam
   b. sistema audio dotato di casse e microfono funzionanti
   c. browser aggiornato con supporto alla tecnologia webrtc (come ad esempio Chrome o Firefox)
   d. connessione internet a banda larga
2. Con un dispositivo mobile, smartphone o tablet, che soddisfi i seguenti requisiti:
   a. sistema operativo Android o iOS di ultima generazione
   b. fotocamera frontale
   c. sistema audio dotato di casse e microfono funzionanti
   d. connessione dati che supporti lo stream audio-video

L'Operatore/Incaricato seguirà delle particolari procedure volte a garantire l'autenticità della richiesta nel corso della sessione in videoconferenza.
L'Operatore/Incaricato verificherà l'identità del Richiedente tramite documento di riconoscimento in corso di validità, purché munito di fotografia e riconoscibile del Richiedente rilasciato da un'Amministrazione dello Stato. L'elenco dei documenti ammessi è lo stesso indicato nel par. 5.3.1.1.
Si ricorda che durante il riconoscimento è obbligatorio avere a disposizione documenti e contatti forniti in fase di registrazione (vedi par.5.2.2).
Durante la registrazione, su esplicita richiesta dell'operatore, il Richiedente è tenuto a:

- fornire le proprie generalità, in coerenza quanto contenuto nel modulo di richiesta dell'Identità digitale SPID;
- dichiarare giorno e ora della registrazione e compiere un'azione casuale come elementi rafforzativi del processo di verifica dell'identità del richiedente;
- inquadrare fronte e retro del documento di identificazione e della tessera sanitaria. Aruba PEC si riserva la facoltà di supportare la verifica dei documenti mostrati dal richiedente durante la registrazione utilizzando il raffronto con le immagini degli stessi caricate dall'utente;
- confermare che i dati contenuti nel modulo di richiesta dell'identità digitale accettato siano completi, corretti e che i documenti mostrati a video siano validi e originali. Nel corso della registrazione, in caso di mancata corrispondenza tra i dati contenuti nel modulo e quelli presenti sui documenti, l'utente può richiederne l'aggiornamento all'operatore (esclusivamente per i dati relativi al documento d'identità e alla tessera sanitaria). Il modulo aggiornato deve essere accettato dall'utente.
- compiere l'azione richiesta dall'operatore per la corretta verifica del possesso dei contatti richiesti.
- confermare la volontà di voler effettuare l'identificazione attraverso la videoregistrazione per ottenere il rilascio dell'identità digitale.

Se il soggetto richiedente è una persona giuridica, dovrà essere fornita la documentazione attestante i poteri di rappresentanza conferiti alla persona fisica che presenta l'istanza, che a sua volta è tenuta ad esibire un valido documento d'identità.

Ulteriori dettagli tecnici relativi allo svolgimento della procedura di riconoscimento con webcam sono descritti all'interno della Guida Utente SPID (disponibile su https://www.pec.it/termini-condizioni.aspx) alla quale si rimanda.
Terminata la sessione di audio-video, il sistema provvederà ad elaborare i file audio-video in formato elettronico, da inviare in conservazione in modalità protetta e sicura per un periodo pari a 20 anni decorrenti dalla scadenza o dalla revoca dell'identità digitale.

L'accesso ai suddetti file conservati a norma sarà garantito esclusivamente dietro richiesta dell'autorità giudiziaria, dell'Agenzia nel corso delle attività di vigilanza, dell'utente e dell'autorità giudiziaria in caso di disconoscimento della stessa, nonché al personale di Aruba PEC, esclusivamente autorizzato, limitatamente alle attività di verifica della qualità e della correttezza dei dati conservati e al soddisfacimento degli oneri normativamente previsti a cui Aruba PEC è sottesa. I dati di

registrazione, costituiti da file audiovideo, immagini e metadati strutturati in formato elettronico, vengono conservati e trattati in base all'art. 7 commi 8 e 9 del DPCM [5].
Come detto sopra, l'operatore che effettua l'identificazione con webcam ha la facoltà di escludere l'ammissibilità della sessione audio-video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal richiedente (ad esempio perché logoro o carente delle caratteristiche elencate).
L'operatore, inoltre, svolge la sessione di identificazione audio-video seguendo una procedura certificata dal gestore di identità digitale che include, come minimo, tutti i passaggi previsti dalle regole attuative SPID per questa modalità di riconoscimento.
In linea generale tutte le attività di registrazione con operatore (si veda il par. 5.2.1 Identificazione con operatore) sono svolte dalla funzione di Autorità di Registrazione del Gestore.
L'Autorità di Registrazione è il soggetto ufficialmente riconosciuto che ha il compito di rilasciare l'identità digitale SPID mediante un processo formale, affidabile e sicuro, e gestirne l'intero ciclo di vita fino alla loro dismissione.
I CDRL e gli IR appartengono alla funzione dell'Autorità di Registrazione del Gestore.

5.3.2 Identificazione informatica mediante TS-CNS, CNS, CIE, firma digitale o SPID

Così come previsto dall'Art. 7 del DPCM e dalle procedure di richiesta dell'IdP, l'identità del soggetto richiedente può essere verificata anche attraverso procedure di identificazione informatica basate su documenti digitali di identità (quali TS-CNS, CNS, CIE o carte ad essa conformi) o su acquisizione del modulo di adesione allo 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 inserire la smartcard/CIE e di autenticarsi per completare il riconoscimento.

I dati estratti dal supporto saranno confrontati con quelli inseriti dall'utente e in caso positivo il riconoscimento sarà considerato concluso e verrà salvata la tracciatura dei log (client authentication) e versata in conservazione come previsto dal [10] Regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014).
In questo caso il Gestore delle identità digitali considera effettuata la verifica dell'identità del soggetto richiedente per effetto ed in conseguenza della verifica dell'identità già espletata dal gestore che ha rilasciato il documento digitale di identità.

- Nel caso in cui il richiedente abbia un certificato di firma verrà richiesto di compilare un modulo di richiesta di adesione in formato elettronico sottoscritto con firma elettronica qualificata o digitale. Anche in questo caso il Gestore delle identità digitali considera effettuata la verifica dell'identità del soggetto richiedente per effetto ed in conseguenza della verifica dell'identità già espletata dal gestore che ha rilasciato certificato di firma.
- Nel caso in cui il richiedente non abbia un certificato di firma, è prevista la possibilità recandosi a sportello (cft. 6.2.1) di richiedere il rilascio di un certificato di firma elettronica qualificata col quale sottoscrivere, anche contestualmente, il modulo di richiesta di adesione SPID ed espletare la fase di riconoscimento per il rilascio dell'identità SPID.
- Limitatamente all'ottenimento dell'identità digitale SPID Persona fisica ad uso professionale è possibile procedere all'identificazione tramite identità SPID Persona Fisica (precedentemente rilasciata da Aruba PEC). In questo caso, tale riconoscimento può essere svolto

utilizzando un'identità SPID persona fisica con livello di sicurezza pari o superiore a quello dell'Identità SPID che si richiede, in ottemperanza alla normativa vigente.

Il Gestore applica la sola modalità di riconoscimento con certificato di firma qualificata in possesso del Richiedente, vedasi secondo bullet del precedente elenco, nel caso in cui il soggetto richiedente l'identità digitale in nome e per conto della persona giuridica non sia cittadino italiano e non sia dotato di un documento di riconoscimento rilasciato in Italia.

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 ad 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.

In riferimento all'identità digitale SPID rilasciata ai minori, è possibile scegliere come metodi di identificazione a distanza citati in questo paragrafo solo TS-CNS o CIE.

5.4 Verifica degli attributi associati all'identità digitale

Aruba PEC può rilasciare l'identità digitale a:

- Cittadini italiani residenti in Italia;
- Cittadini italiani residenti all'estero;
- Cittadini stranieri residenti in Italia.

5.4.1 Identità digitale e attributi

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:

1. **Attributi identificativi**, quali il nome, cognome, data di nascita, sesso ovvero ragione sociale o denominazione sociale, sede legale, codice fiscale, partita iva e gli estremi del documento di identità utilizzato ai fini dell'identificazione. Così come specificato alla lettera c) del comma1 dell'art.1 del DPCM
2. **Attributi non identificativi** (o secondari), quali il numero di telefono, indirizzo di posta elettronica, domicilio fiscale e digitale, nonché eventuali altri attributi individuati dall'AgID. Così come specificato alla lettera d) del comma1 dell'art.1 del DPCM
3. **Codice identificativo**: come specificato alla lettera d) del comma1 dell'art.1 del DPCM e valorizzato in aderenza ai regolamenti di cui all'art 4 comm. 2 del DPCM
4. **Identificativo utente**: attributo corrispondente allo username prescelto dall'utente

Dopo la fase di registrazione ed identificazione dell'identità del richiedente, l'IdP, così come previsto dai regolamenti di cui all'Art 4 comma 2 del DPCM, effettua la verifica degli attributi identificativi.

5.4.2 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.

Prima del rilascio dell'identità digitale a una persona fisica, sono verificati i dati identificativi del richiedente, ivi inclusi ove disponibili, il domicilio digitale o altro indirizzo di contatto, mediante consultazione dei dati disponibili presso l'ANPR di cui all'articolo 62 del D.lgs. 82/2005. Tali verifiche sono svolte anche successivamente al rilascio dell'identità digitale, con cadenza almeno annuale, anche ai fini della verifica dell'esistenza in vita.

L'accesso alle fonti autoritative 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 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. Il rilascio dell'Identità SPID è subordinato al superamento di tali verifiche.

Quanto sopra, anche in relazione allo specifico livello di sicurezza di autenticazione informatica (livello SPID) gestito, sull'identità del soggetto richiedente prima di procedere alla registrazione.
Di seguito sono riportate le tabelle che rappresentano i requisiti relativi alla verifica di identità condotta da Aruba PEC in relazione al livello di sicurezza nel caso di persona fisica e di persona giuridica.

Livello di sicurezza	Requisiti/Verifiche effettuate
Per tutti i livelli SPID	Può essere ragionevolmente assunto che la persona in possesso dei documenti di identità e codice fiscale/tessera sanitaria rappresenti l'identità dichiarata. I documenti sono ritenuti autentici e validi sulla base di quanto risulta da soggetti istituzionali competenti (articolo 4, comma 1, lettera c del DPCM 24 ottobre 2014 o, in assenza di convenzioni con l'Agenzia, 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). Il codice fiscale è verificato presso il servizio messo a disposizione dall'Agenzia delle Entrate sul suo portale;

Tabella 2 - Requisiti da soddisfare/Livelli di sicurezza SPID (persona fisica)

Livello di garanzia	Requisiti
Tutti i livelli SPID	L'esistenza della persona giuridica è basata su evidenze riconosciute dal sistema delle imprese in ambito nazionale (es. Visura Camerale, RUNTS ecc..). Dette evidenze sono ritenute valide ed autentiche sulla base di quanto risulta da soggetti istituzionali competenti. Effettuata l'associazione amministratore o rappresentante legale, all'impresa-persona giuridica, si procede alla verifica - come persona fisica - dell'amministratore o del legale rappresentante, come indicato nella tabella precedente per l'identificazione di una persona fisica.

Tabella 3 - Requisiti da soddisfare/Livelli di sicurezza SPID (persona giuridica)

5.4.2.1 Verifica del codice fiscale in assenza di Tessera Sanitaria

Sulla base di quanto previsto dall'Avviso AgID n.7/2026 v. 3.0, Aruba PEC rilascia l'identità digitale SPID anche ai cittadini italiani residenti all'estero, purché siano in possesso dei documenti necessari per la registrazione, ossia un documento di identità valido e la Tessera Sanitaria con codice fiscale.

In assenza della Tessera Sanitaria, il cittadino può esibire il tesserino del codice fiscale, purché riporti sul retro il "Numero di identificazione della tessera", che il Gestore dell'identità digitale verifica rispetto ai dati anagrafici dell'utente mediante i sistemi oggetto delle convenzioni di cui all'art. 4, comma 1, lett. c), del DPCM 24 ottobre 2014.

Qualora il cittadino italiano residente all'estero sia sprovvisto anche del tesserino del codice fiscale, è possibile procedere al rilascio dell'identità digitale SPID sulla base di uno dei documenti idonei alla verifica del codice fiscale, ove ne sia verificabile la corrispondenza con i dati anagrafici dell'utente, ovvero del Certificato prodotto dall'Agenzia delle Entrate contenente il codice fiscale, vidimato dall'Ufficio consolare o dell'Attestazione consolare scaricabile dal portale dei servizi consolari - Fast-It .

Ai fini della verifica del codice fiscale, dunque, sono nel complesso accettabili le seguenti tipologie di documenti:

- Tessera Sanitaria con codice fiscale;
- tesserino del codice fiscale riportante sul retro il "Numero di identificazione della tessera";
- certificato prodotto dall'Agenzia delle Entrate contenente il codice fiscale, vidimato dall'Ufficio consolare;
- attestazione consolare scaricabile dal portale dei servizi consolari Fast-It.

Inoltre, secondo quanto previsto dall'Avviso AgID n. 17 v. 2.0, Aruba PEC può rilasciare l'identità digitale SPID anche ai soggetti residenti in Italia sprovvisti di Tessera Sanitaria, applicando quanto previsto per gli italiani residenti all'estero dall'Avviso AgID n. 7 v. 3.0 e riportato sopra.

Quanto agli specifici controlli operati, in fase di supervisione delle pratiche di riconoscimento, gli Operatori Supervisori effettuano verifiche documentali e di coerenza dei dati, integrate tramite chiamata a sistema oggetto delle convenzioni di cui all'articolo 4, comma 1, lettera c), del DPCM 24 ottobre 2014.

In particolare, le verifiche riguardano la corrispondenza del codice fiscale del Richiedente e l'autenticità della documentazione prodotta:

- nel caso di certificato rilasciato dall'Agenzia delle Entrate, mediante controllo del glifo digitale o della firma digitale, con verifica della validità della firma e identificazione del Funzionario Tecnico dell'Agenzia delle Entrate;
- nel caso di Attestazione Consolare attestante il codice fiscale del Richiedente, mediante verifica digitale apposta sull'Attestazione stessa.

In entrambi i casi è inoltre previsto il controllo dei dati anagrafici e del codice fiscale tramite il Sistema di cui sopra.

Tali controlli, analogamente a quanto previsto nel caso in cui il Richiedente presenti la Tessera Sanitaria, sono eseguiti per ogni modalità di identificazione riportate al par. 5.3. La verifica tramite i sistemi previsti dal processo è effettuata prima del rilascio dell'identità digitale. In caso di esito negativo della verifica, la procedura di riconoscimento si conclude con esito negativo e non prosegue alle fasi successive, salvo specifiche eccezioni previste dalla modalità di riconoscimento adottata.

5.4.3 Verifica degli attributi secondari

La verifica degli attributi non identificativi (secondari) viene effettuata durante la fase di richiesta dell'identità digitale.

5.4.4 Verifica attributi del soggetto minore

Come descritto all'interno del par. 5.2.3, Aruba PEC rilascia l'identità digitale SPID ai richiedenti aventi un'età compresa tra i 5 ed i 17 anni [15].

Si specifica che per l'attivazione dell'identità digitale, gli attributi richiesti al soggetto minore sono i seguenti:

- **attributi identificativi obbligatori**: cognome e nome, sesso, data e luogo di nascita, codice fiscale, estremi di un valido documento di identità, ai sensi dell'art. 1, comma 1, lett. c) del D.P.C.M. 24 ottobre 2014 e all'art. 5, terzo capoverso del "Regolamento recante le modalità attuative per la realizzazione dello SPID";
- **attributi secondari obbligatori**: e-mail (verificata durante la fase di richiesta dell'identità digitale);
- **attributi secondari facoltativi**: il domicilio fisico, il domicilio digitale e il numero di telefono mobile (in deroga all'art. 5, quinto capoverso del "Regolamento recante le modalità attuative per la realizzazione dello SPID").

Se il minore non è in possesso di un numero di cellulare (o di uno smartphone) potrà acquisire come secondo fattore, tramite le modalità messe a disposizione da Aruba, un dispositivo OTP Display, in quanto il minore non può utilizzare il telefono e numero del genitore.

5.5 Attivazione dell'identità digitale

Solo dopo aver effettuato l'iter completo, cioè dopo aver completato l'identificazione e le verifiche necessarie, l'identità digitale e le relative credenziali di accesso potranno essere attivate. Al Richiedente verrà inviata opportuna notifica dell'avvenuta attivazione mediante i canali di contatto forniti in fase di richiesta (email e/o sms).

5.6 Rilascio, consegna e attivazione delle credenziali

Le credenziali rilasciate al Richiedente, associate all'identità e al livello SPID richiesti, saranno consegnate in modalità sospesa.
Il Richiedente, per attivare le credenziali e poterle quindi utilizzare con la propria identità digitale, dovrà accedere al pannello di gestione dell'identità digitale (cfr. par. 6) e disporre l'attivazione.
A tal proposito 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.

Come descritto nei precedenti paragrafi username e password vengono scelte dal richiedente in fase di richiesta.
Per completare l'attivazione, l'utente riceverà:

- una email contenente il link al pannello di registrazione (con indicazione che la password provvisoria verrà inviata tramite SMS) https://registrazionespid.aruba.it/#/login per il completamento della procedura di rilascio (verifica contatti e configurazione OTP) e l'attivazione dell'identità digitale;

- un SMS contenente la password provvisoria da cambiare obbligatoriamente al primo accesso al pannello di registrazione sopra indicato.

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

Considerando che il telefono cellulare costituisce nell'ambito del sistema SPID un importante fattore di autenticazione, al fine di limitare il rischio che detto canale di comunicazione possa essere usato impropriamente o che possa essere utilizzato da chi lo ha sottratto al legittimo proprietario in maniera fraudolenta o comunque non autorizzata per ottenere l'identità digitale SPID, Aruba PEC ha predisposto il processo di verifica e riassegnazione descritto di seguito.
Questo processo viene attivato nei casi in cui i Richiedenti l'identità digitale si vedano rifiutare da Aruba PEC l'indicazione del numero di cellulare da associare alla propria identità, in quanto già associato ad altro utente.
Il processo prevede i seguenti passaggi:

1. Il Richiedente, inserendo il numero di cellulare nelle apposite schermate di registrazione, riceve un errore in quanto quel numero di cellulare risulta già associato ad altra identità;
2. Il Richiedente prende contatto (attraverso i canali messi a disposizione dall'IdP) con l'assistenza Aruba per chiedere la risoluzione dell'errore e lo sblocco del numero di cellulare indicato in fase di registrazione;
3. L'assistenza Aruba prende in carico la richiesta e provvede ad effettuare una verifica del possesso, da parte del Richiedente, del cellulare indisponibile. L'assistenza Aruba a questo punto tenta di stabilire un contatto telefonico al numero conteso, due volte nell'arco temporale delle 48 ore dalla richiesta, per accertarsi che il Richiedente ne sia in possesso. Durante la telefonata verranno verificate alcune informazioni tra le quali anche le generalità del Richiedente.
4. L'assistenza Aruba, sempre nell'arco delle 48 ore, procede ad eseguire una verifica analoga attraverso i contatti dell'attuale assegnatario. Verranno quindi inviate due mail nell'arco temporale compreso tra le 24 e 48 ore all'attuale assegnatario chiedendo di confermare se è in possesso del numero di cellulare conteso attraverso l'apertura di un ticket all'assistenza Aruba. Qualora non si riuscisse ad ottenere una risposta, si lasciano trascorrere fino a 15 giorni:
    a. Se durante questo arco temporale l'attuale assegnatario dimostra l'effettivo possesso del numero di cellulare contesto o non intende provvedere ad associare alla propria identità un diverso numero di cellulare, la richiesta del Richiedente è rigettata ed il processo si interrompe;
    b. Qualora l'attuale assegnatario non abbia provveduto all'aggiornamento del cellulare associato alla propria Identità Digitale o a dimostrarne il possesso, Aruba provvede alla sospensione dell'identità dell'attuale assegnatario e, trascorsi 15 giorni senza contatti da parte dell'attuale assegnatario, alla revoca dell'identità stessa. Una volta revocata l'identità dell'attuale assegnatario, il richiedente può associare il numero di cellulare alla propria identità ed il processo prosegue al punto successivo.
5. Accertato che il Richiedente è in possesso del numero di cellulare conteso ed in assenza della dimostrazione di possesso da parte dell'attuale assegnatario, l'assistenza Aruba provvede a rimuovere il blocco riepilogando le verifiche eseguite e confermando che il Richiedente è in possesso del numero di telefono.

6 Gestione delle identità digitali

L'autorità di Registrazione 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 l'Autorità di Registrazione non appena gli attributi ad esso associati subiscano delle variazioni. La tempestiva modifica da parte del Gestore delle Identità, passa, come già avviene in fase di registrazione, da una verifica delle informazioni comunicate, mediante documenti e dati ottenibili da fonti affidabili ed indipendenti.
Oltre alle modifiche degli attributi, il Titolare potrà effettuare la modifica della password statica o richiederne il ripristino nel caso ne abbia perso memoria.
Si ricorda che l'utente è tenuto ad aggiornare la propria password trascorsi 180 giorni dalla creazione ovvero ultima variazione.

6.1 Gestione dati raccolti per la verifica dell'identità digitale

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).
I dati verranno conservati per un periodo non inferiore a 20 anni dalla scadenza, revoca o disattivazione dell'identità digitale.
Tra le informazioni conservate saranno presenti anche:

1. le copie dei documenti di identità e dei relativi moduli di richiesta provvisti di firma autografa in caso di riconoscimento da sportello;
2. i log di transazione in caso di riconoscimento via web e via CNS/CIE, i documenti firmati digitalmente in caso di utilizzo di un dispositivo di firma come metodo di riconoscimento;
3. le registrazioni audio-video in caso di riconoscimento attraverso piattaforma web video
4. la copia del modulo di adesione.

Il Gestore del servizio si impegna a fornire su richiesta, all'Autorità Giudiziaria ed al Garante per il trattamento dei dati personali, le informazioni relative all'identità personale di un utente registrato.

6.2 Gestione del ciclo di vita

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

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

6.2.1 Gestione degli attributi

L'utente è tenuto a mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del gestore, i contenuti degli attributi identificativi di seguito elencati.

1. Per le persone fisiche:
   a. estremi del documento di riconoscimento e relativa scadenza;
   b. gli attributi secondari così come definiti all'articolo 1, comma d) del DPCM;

2. Per le persone giuridiche:
   a. indirizzo sede legale
   b. codice fiscale o P.IVA (nei rari casi di variazione a seguito di particolari mutazioni societarie)
   c. rappresentante legale della società
   d. attributi secondari così come definiti all'articolo 1, comma d) del DPCM

L'utente, in caso di dichiarazioni non fedeli o mendaci, si assume le responsabilità previste dalla legislazione vigente.
Le modalità operative per gli aggiornamenti sono rese possibili attraverso un'area web dedicata del gestore delle identità digitali accessibile mediante le credenziali SPID, almeno di livello due, in possesso dell'utente. Maggiori informazioni sono riportate nella Guida Utente [3].
Il gestore dell'identità digitale mette inoltre a disposizione un servizio di help desk tramite mail o compilando un form on-line sul sito web. Inoltre potrà essere previsto un sistema attraverso il quale l'utente potrà effettuare autonomamente alcune operazioni.
Ad ogni variazione da operare sugli attributi relativi ad una identità, il gestore dell'identità digitale, prima di aggiornare i dati registrati, esegue le fasi di esame e verifica in relazione al livello SPID associato all'identità digitale. La richiesta di aggiornamento e l'aggiornamento sono notificati all'utente utilizzando un attributo secondario funzionale alle comunicazioni (ad es. l'indirizzo di posta elettronica se non è stato modificato durante la sessione di aggiornamento).
Futuri sviluppi potranno includere aggiornamenti automatici sulla base di modifiche degli attributi identificativi o secondari effettuati da pubbliche amministrazioni (ad es. ANPR, comuni, motorizzazione ecc.).

6.2.2 Sospensione, Revoca e Rinnovo dell'Identità

Prima di descrivere le modalità operative per operare 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 non viene riattivata su richiesta dell'utente o definitivamente revocata.
La **riattivazione** consiste nel rendere di nuovo utilizzabili le credenziali precedentemente sospese.
La **revoca** rende inutilizzabili per sempre le credenziali digitali. In pratica si tratta di una sospensione a tempo indeterminato e irrevocabile di un'identità digitale.
Ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del DPCM, il gestore revoca l'identità digitale nei casi seguenti:

1. risulta non attiva per un periodo superiore a 24 mesi;

2. per decesso della persona fisica;
3. per estinzione della persona giuridica;
4. per uso illecito dell'identità digitale;
5. per richiesta dell'utente;
6. per termine contrattuale, a qualsiasi causa dovuto;
7. per scadenza del documento di identità.

Nel caso previsto ai punti 1 e 6, 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 all'utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).
A tal proposito il sistema SPID Aruba PEC è in grado di notificare al Titolare il mancato utilizzo dell'identità digitale con cadenze personalizzabili che, di default, sono impostate a 90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva.
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.
In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del soggetto utente (eredi o procuratore, amministrazione, società subentrante) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'identità digitale. Il gestore, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.
Nel caso previsto dal punto 7, il gestore dell'identità digitale sospende di propria iniziativa l'identità, comunicando la causa e la data della sospensione all'utente attraverso l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per le comunicazioni).
Nel caso previsto dal punto 4, ovvero nel caso in cui l'utente ritenga che la propria identità digitale sia stata utilizzata fraudolentemente, lo stesso può chiederne la sospensione con una delle seguenti modalità:

1. richiesta al gestore inviata via PEC;
2. richiesta, in formato elettronico e sottoscritta con firma digitale o elettronica qualificata, inviata alla casella di posta appositamente predisposta da Aruba PEC.

Le modalità operative per procedere con le azioni sopra descritte sono riportate al link https://guide.pec.it/sospensione-riattivazione-revoca.aspx
Aruba PEC fornirà esplicita evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.
Nel caso previsto al punto 4, a seguito della richiesta di sospensione, qualora pervenga ad Aruba PEC copia della denuncia depositata presso l'Autorità Giudiziaria, l'IdP provvederà immediatamente alla revoca.
Nel caso previsto dal punto 5, l'utente può chiedere ad Aruba PEC, in qualsiasi momento e a titolo gratuito, la sospensione o la revoca della propria identità digitale seguendo modalità almeno analoghe a quelle previste dal precedente punto 4.

Inoltre, secondo quanto previsto dall'art. 20 del Regolamento recante le modalità attuative SPID, e ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del DPCM, il Gestore può sospendere, ovvero revocare l'identità digitale SPID, e comunicando la causa e la data della sospensione al Titolare tramite i canali forniti per le comunicazioni, oltre che nei casi descritti sopra anche al verificarsi di specifiche condizioni come:

- attività sospette dell'identità digitale SPID;
- problematiche legate al processo di identificazione certa o al possesso dei recapiti registrati;
- modifica del legale rappresentante in caso di SPID persona giuridica.

In questi casi, la riattivazione dell'identità SPID sospesa su iniziativa del Gestore viene effettuata dal Gestore stesso solo dopo aver effettuato le verifiche e i controlli necessari a ripristinare le informazioni e/o condizioni presenti prima della sospensione.

La revoca di una identità digitale comporta conseguentemente la revoca delle relative credenziali. Aruba PEC, così come previsto dalle norme di cui all'Art 4 comma 2 del DPCM, conserva la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'identità digitale.

Il **rinnovo** del servizio SPID prolunga la possibilità di utilizzo dell'Identità SPID di ulteriori 12 mesi e prevede un corrispettivo da parte del Titolare. La procedura di rinnovo non prevede la sostituzione delle credenziali di autenticazione e garantisce la piena continuità del servizio
In questa fase il Gestore può applicare misure di verifica supplementari al fine di garantire la sicurezza del servizio per il periodo contrattuale previsto.

Il mancato completamento della procedura di rinnovo dell'identità digitale comporta la sospensione della stessa e conseguente revoca per scadenza contrattuale così come previsto dal Regolamento recante le modalità attuative per la realizzazione dello SPID [10], il Titolare dovrà quindi procedere all'acquisto di una nuova identità SPID con le modalità indicate nel presente manuale.

La documentazione, le informazioni e i dati eventualmente raccolti durante la fase di rinnovo dell'Identità sono verificati e conservati in maniera sicura dal Gestore per il tempo richiesto dalla normativa nazionale e nel pieno rispetto della vigente normativa in materia di tutela dei dati personali.

6.2.3 Gestione ciclo di vita delle credenziali

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

1. creazione delle credenziali;
2. consegna delle credenziali o dei mezzi usati per la loro produzione; maggiori dettagli sono riportati nel par. 5.6;
3. attivazione delle credenziali o dei mezzi usati per la loro produzione; maggiori dettagli sono riportati in nel par. 5.6;
4. conservazione delle credenziali;

5. sospensione e revoca delle credenziali o mezzi usati per la loro produzione;
6. rinnovo e sostituzione delle credenziali o mezzi usati per la loro produzione (cfr. https://guide.pec.it/pagamenti-fatturazione-rinnovo/rinnovo.aspx);

Alcuni dei processi sopra elencati possono essere influenzati dal fatto che le credenziali siano rese operative attraverso l'ausilio di un dispositivo hardware.
Aruba PEC, per l'intero ciclo di vita della credenziale conserva opportuna documentazione atta ad avere traccia delle seguenti informazioni:

1. la creazione della credenziale
2. l'identificativo della credenziale;
3. il soggetto per il quale è stata emessa;
4. lo stato della credenziale.

Aruba PEC conserva opportuna documentazione per ogni sottoprocesso (creazione, emissione, attivazione, revoca, sospensione, rinnovo e sostituzione) del processo di gestione delle credenziali, nel pieno rispetto della vigente normativa in materia di tutela dei dati personali.
Aruba PEC conserva almeno le informazioni relative alla data di creazione della credenziale, allo stato della stessa, alle date di consegna, di attivazione (se prevista) e di eventuale sospensione, revoca o cancellazione.

6.2.4 Sospensione e revoca delle credenziali

Aruba PEC ha implementato le funzionalità necessarie per consentire al Titolare la sospensione e la riattivazione delle proprie credenziali di Livello 2 e/o Livello 3.
La descrizione di queste funzionalità è stata dettagliata nelle guide dedicate reperibili all'indirizzo https://guide.pec.it/spid/sospensione-revoca-aruba-id.aspx.
Il Titolare per sospendere le proprie credenziali dovrà autenticarsi al Self Care SPID con le proprie credenziali ed inserire il codice OTP che verrà inviato tramite email o SMS sul cellulare associato all'utenza SPID.

In merito alle identità digitali SPID rilasciate ai soggetti minori (cft. 6.7), il genitore può sospendere/revocare/ri-attivare l'identità SPID del minorenne fino a quando non raggiunge la maggiore età. Il minorenne, invece, solo al raggiungimento del 14esimo anno di età avrà la possibilità di sospendere/riattivare in maniera del tutto autonoma la sua identità SPID (tramite la sua area di Selfcare).

6.2.5 Gestione delle credenziali in caso di impossibilità di accesso ai canali di contatto

Questo paragrafo ha lo scopo di descrivere quali strumenti Aruba PEC mette a disposizione del Titolare nel caso in cui quest'ultimo non sia più in possesso delle sue credenziali per l'autenticazione con SPID e non possa recuperarle attraverso i metodi messi a sua disposizione da Aruba PEC in quanto non ha più accesso agli attributi secondari (email/cellulare).
Si delineano due scenari a seconda dello stato in cui si trova la richiesta di emissione SPID:

1. Se lo SPID risulta in stato "Richiesta", il cliente può chiedere l'annullamento dell'ordine e procedere all'inserimento di un nuovo ordine.
2. Se lo SPID risulta in stato "Attivo" può, in via alternativa tra di loro:

a) chiedere la sospensione o la revoca dell'identità, con o senza formale denuncia all'Autorità, inoltrando l'apposito modulo, reperibile all'indirizzo o https://guide.hosting.aruba.it/guida-alla-gestione-dei-servizi/recuperocodici-autenticazione.aspx tramite PEC unitamente a copia del documento di riconoscimento, oppure in formato elettronico sottoscritto con firma elettronica qualificata. In questo modo, revocata l'identità, può richiedere una nuova identità SPID e utilizzarla;
b) chiedere – qualora non fosse in possesso né della PEC né della firma elettronica qualificata – il recesso dal servizio ed ordinare una nuova identità SPID secondo le modalità descritte nelle Condizioni Generali del servizio;
c) chiedere – qualora non fosse in possesso né della PEC né della firma elettronica qualificata e qualora avesse effettuato la denuncia formale all'Autorità Giudiziaria (es.: per smarrimento, furto, ecc) – la revoca del servizio aprendo una richiesta autenticata sul portale di assistenza cui allegherà la denuncia, il modulo di revoca e copia del documento di riconoscimento;
d) non avanzare alcuna richiesta ed attendere 24 mesi per la revoca d'ufficio, periodo durante il quale comunque non può utilizzare l'identità di Aruba.

6.2.6 Gestione dell'identità digitale di un soggetto minore

In linea con quanto previsto dalle "Linee guida operative per la fruizione dei servizi SPID da parte dei minori" pubblicate da AgID [15], si specifica che:

- Nel caso in cui il fornitore di servizi (SP) non richieda l'autorizzazione del genitore per l'accesso ai servizi con SPID, Aruba PEC, al momento della richiesta di accesso con identità digitale SPID da parte del minore, effettua la procedura di autenticazione del soggetto minore, verificando la congruenza fra l'età richiesta dal fornitore di servizi (SP) e l'età effettiva del minore: qualora la verifica dia esito negativo, la procedura di autenticazione è interrotta con esito negativo; qualora invece la verifica dia esito positivo, Aruba PEC porta a termine il processo di autenticazione del minore presso il SP.
- Nel caso in cui il fornitore di servizi (SP) richieda l'autorizzazione del genitore per l'accesso ai servizi con SPID, Aruba PEC effettua la procedura di autenticazione del soggetto minore, verificando la congruenza fra l'età richiesta dal SP e l'età effettiva del minore: qualora la verifica dia esito negativo, la procedura di autenticazione è interrotta con esito negativo; qualora invece la verifica dia esito positivo, Aruba PEC continua la procedura di autenticazione. Aruba PEC, inoltre, comunica al minore la richiesta di conferma della sua volontà di chiedere al genitore l'autorizzazione all'accesso: qualora il minore non confermi tale volontà, la procedura di autenticazione è interrotta con esito negativo; qualora invece il minore confermi tale volontà, la procedura di autenticazione prosegue, come descritto di seguito:
  - Aruba PEC invia al genitore una notifica per autorizzare l'accesso del minore;
  - qualora il genitore non autorizzi l'accesso, la procedura di autenticazione è interrotta con esito negativo; qualora invece il genitore fornisca l'autorizzazione all'accesso, Aruba PEC porta a termine il processo di autenticazione del minore presso il SP.

Nel caso in cui l'età del soggetto non coincida con quelle della richiesta pervenuta dal SP, o nel caso in cui nel metadata del SP non sia previsto il valore "AgeLimit" relativo all'età del richiedente, Aruba PEC non permette l'autenticazione.

Per la gestione dell'identità digitale del minore, Aruba PEC consente al genitore di:

- autorizzare l'accesso ai servizi richiesti dal minore entro 24 ore dalla richiesta;
- fornire l'autorizzazione all'accesso ai servizi, ove previsto, da parte del minore indicandone la durata nel tempo: nel caso l'autorizzazione sia fornita dal genitore in modo continuativo, Aruba PEC autentica il minore senza chiedere una nuova autorizzazione. Trascorsa tale durata impostata dal genitore, in presenza di una nuova richiesta di accesso al servizio da parte del minore, Aruba PEC richiede nuovamente l'autorizzazione al genitore;
- richiedere la sospensione e revoca dell'identità digitale SPID del minore.

Aruba PEC consente al genitore di accedere esclusivamente alle informazioni necessarie all'espletamento delle attività di gestione dell'identità digitale SPID del minore come previsto dalle "Linee guida operative per la fruizione dei servizi SPID da parte dei minori" [15], garantendo la riservatezza del minore con riferimento a ulteriori informazioni di utilizzo della propria identità digitale.

Nel caso in cui il minore sia ultraquattordicenne, Aruba PEC permette al minore di poter gestire la propria identità digitale, oltre che consultare gli accessi effettuati.

Al compimento del diciottesimo anno di età, Aruba PEC:

- permette al soggetto neo-maggiorenne di ottenere un'identità digitale SPID persona fisica, o revocare l'identità SPID persona fisica minore;
- rimuove le limitazioni imposte per la minore età;
- elimina i legami con l'identità digitale del genitore;
- cancella le informazioni relative all'utilizzo dell'identità digitale del minore eventualmente rese disponibili al genitore (ad eccezione del Log, di veda il par. 4.6.3).

6.3 Richiesta dei dati da parte del Titolare

In qualsiasi momento il Titolare potrà richiedere all'Autorità di Registrazione di conoscere, gratuitamente, i propri dati personali memorizzati nel sistema IdP, in conformità con quanto previsto dalla normativa.

6.4 Gestione rapporti con utenti

L'IdP Aruba PEC, relativamente a questioni riguardanti problematiche o richieste di qualsiasi tipo aventi ad oggetto le credenziali SPID, gestisce i rapporti con i propri utenti attraverso i seguenti canali:

1. Sottomissione di comunicazioni da parte dell'utente verso l'IdP
   i. Canale telefonico (centralino) - 0575 0500
   ii. Fax - 0575 862022

iii. Portale Web – www.pec.it
iv. Form online – supportoecs.aruba.it
v. PEC: assistenza.spid@arubapec.it

2. Sottomissione di comunicazioni da parte dell'IdP verso l'utente

i. Con l'ausilio degli attributi secondari previsti dall'art. 1 comma d) del DPCM

6.5 Guida utente del servizio

Per quanto riguarda la guida utente si rimanda integralmente al documento Guida dell'Utente [3].

7 Sistema di monitoraggio

Il sistema utilizzato per il monitoraggio delle componenti del servizio di IdP consente di valutare e di verificare continuamente, mediante l'aggiunta di appositi controlli, il regolare funzionamento di tutti i sottoservizi erogati nell'ambito dell'architettura descritta nel par. 4.1, nonché le prestazioni dei medesimi.
Il sistema di monitoraggio utilizzato nei Data Center permette di controllare i servizi critici simulando le richieste "client-side" assicurando quindi la corretta erogazione dei servizi. I controlli vengono effettuati ogni sessanta secondi in contemporanea su centinaia di sistemi e in caso di errore visualizza un alert (rosso ed evidente) all'interno de pannelli sinottici dei NOC Aruba PEC (Network Operations Center).
Ogni errore visualizzato veicola tutte le informazioni necessarie a descrivere passo per passo le operazioni da compiere in presenza di quel determinato errore. Questo permette a qualsiasi ora e a chiunque di garantire la corretta esecuzione di tutte le procedure (precedentemente collaudate) e tempi brevissimi di intervento.
Il sistema permette inoltre di controllare, oltre che simulando le attività di un utente, anche l'attività dei servizi (es. Autorità di Registrazione, Autorità di Autenticazione, CA etc.) effettuando controlli complessi come l'esecuzione corretta di procedure: che vanno dal semplice invio e ricezione di richieste di autenticazione (SignIn) o registrazione (SignUp) fino alla verifica della corretta elaborazione di procedure di backup oppure che lo spazio disponibile all'interno di un certo ambiente non sia inferiore ad una determinata soglia.
Il sistema offre la possibilità, in ogni momento, di verificare lo stato globale ed il dettaglio dei servizi monitorati. Lo strumento di monitoraggio è raggiungibile via web, protetto mediante opportuno sistema di autenticazione e accounting: l'interfaccia web consente dunque, ad ogni utente autenticato, di visualizzare lo stato globale dei servizi ed anche lo stato dettagliato di un dato controllo.
Viene predisposto altresì un sistema di rilevamento delle caratteristiche e dei parametri di funzionamento dei server e dei servizi (quali ad esempio il traffico di rete sviluppato, l'occupazione della CPU, l'utilizzo della memoria, l'attività di I/O, ecc.) in grado di presentare graficamente l'andamento attuale e lo storico dei parametri di rilevamento.

Viene inoltre garantito il monitoraggio del sistema di firewalling predisposto che, tramite accesso ad un'interfaccia web protetta, consente la rilevazione degli eventi di sicurezza e la conseguente tempestiva gestione degli eventuali incidenti di sicurezza.
Tutte le piattaforme di monitoraggio inoltre gestiscono/ricevono gli eventi (log) e li condividono con una piattaforma centrale di correlazione che assicura, oltre ad una gestione degli eventi stessi in tempo reale, anche la loro archiviazione in modo sicuro, secondo principi di sicurezza quali la non alterabilità dei log stessi. Queste informazioni (log) sono disponibili alle operazioni di audit al fine di poter analizzare ogni attività compiuta sul sistema di elaborazione secondo le specifiche necessità di controllo e quanto richiesto dai provvedimenti normativi in materia. Il personale dei Data Center - presente tutti i giorni con orario H24x365 giorni all'anno - provvede al controllo costante dello strumento di monitoraggio in modo da avere in ogni momento una visione aggiornata dello stato globale di tutti servizi. Nel caso in cui si evidenzino anomalie verranno effettuati tutti gli ulteriori controlli necessari per predisporre le azioni correttive o gli interventi preventivi atti a garantire la qualità dei servizi erogati ed il rispetto dei livelli di servizio garantiti. Il monitoraggio garantisce la corretta reattività in caso di evento anomalo e l'avvio delle operazioni di Escalation e di Incident Management quando l'evento individuato risulta essere significativo.

8 Livelli di servizio

Il Gestore garantisce la continuità operativa dei servizi di sua competenza afferenti allo SPID, conformemente agli indicatori di qualità e livelli di servizio allegati alla convenzione per l'adesione a SPID. Tali indicatori sono riportati e definiti nei paragrafi che seguono.

8.1 Livelli di servizio garantiti per le diverse fasi della registrazione

Richiesta online da parte dell'utente

Indicatore di qualità	Valore
Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi	Disponibilità ≥ 99%

Riconoscimento/Identificazione

Indicatore di qualità	Valore
Riconoscimento/Identificazione de-visu Tutti i giorni lavorativi	dalle 9:00 alle 18:00
Riconoscimento/Identificazione con TS-CNS/CNS/CIE	Tutti i giorni della settimana, festivi inclusi

Riconoscimento/Identificazione con Firma Digitale	Tutti i giorni della settimana, festivi inclusi
Riconoscimento/Identificazione con sessioni audio/video	Tutti i giorni lavorativi, dalle 9:00 alle 18:00

Creazione delle identità digitali e delle relative credenziali

Indicatore di qualità	Valore
Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi	Disponibilità ≥ 99%

Consegna delle credenziali

Indicatore di qualità	Valore
Tutti i giorni lavorativi, dalle 9:00 alle 18:00	Disponibilità ≥ 98%

Attivazione dell'identità

Indicatore di qualità	Valore
Tutti i giorni lavorativi, dalle 9:00 alle 18:00	Disponibilità ≥ 98%

8.2 Livelli di servizio garantiti per le diverse fasi della gestione del ciclo di vita delle identità

Sospensione, riattivazione revoca tramite WEB

Indicatore di qualità	Valore
Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi	Disponibilità ≥ 99%

Sospensione, riattivazione revoca tramite CALL-CENTER

Indicatore di qualità	Valore
Tutti i giorni lavorativi, dalle 9:00 alle 18:00	Disponibilità ≥ 98%

Sospensione, riattivazione revoca tramite PEC

Indicatore di qualità	Valore
Tutti i giorni lavorativi, dalle 9:00 alle 18:00	Disponibilità ≥ 98%

8.3 Livello di servizio garantito per le diverse fasi del processo di autenticazione

Si riporta di seguito la tabella sinottica degli indicatori di qualità previsti per il Servizio SPID. La frequenza di misurazione è trimestrale su dati relativi al trimestre precedente al momento della misurazione.

ID	Indicatore di qualità	Modalità funzionamento	Valore di soglia
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
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
IQ-06	Disponibilità del sottoservizio di sospensione 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 successiva alla sospensione		≤ 5 giorni lavorativi
IQ-09		Erogazione automatica	≥ 99,5%

	Disponibilità del sottoservizio di rinnovo e sostituzione delle credenziali		Singolo evento di indisponibilità ≤ 6 ore
		Erogazione in presenza	≥ 98,0%
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		≤ 2 giorni lavorativi
IQ-10bis[1]	Tempo di dispiegamento/aggiornamento metadata		≤ 2 giorno lavorativi
IQ-11	Disponibilità del sottoservizio di autenticazione		≥ 99,5%
			Singolo evento di indisponibilità ≤ 6 ore
IQ-12	Tempo di risposta del sottoservizio di autenticazione		Tempo di risposta <=2 sec almeno nel 98,0% delle richieste
IQ-13	RPO sottoservizio registrazione e rilascio delle identità		1 ora
IQ-14	RTO sottoservizio registrazione e rilascio delle identità		8 ore
IQ-15	RPO sottoservizio di sospensione e revoca delle credenziali		1 ora

[1] *Indicatore calcolabile a valle del completo dispiegamento della piattaforma di scambio automatico dei metadata*

IQ-16	RTO sottoservizio di sospensione e revoca delle credenziali		8 ore
IQ-17	RPO sottoservizio di Autenticazione		1 ora
IQ-18	RTO sottoservizio di Autenticazione		8 ore

8.4 Continuità operativa

Registrazione e rilascio Identità

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

Revoca o sospensione Identità

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

Autenticazione

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

9 Modalità di protezione dei dati personali

9.1 Archivi contenenti dati personali

Tutta la documentazione cartacea ed in formato elettronico raccolta durante le fasi di elaborazione delle richieste di identità digitale è conservata negli elaboratori utilizzati dagli addetti alle procedure di autenticazione e validazione in locali altamente sicuri.

9.2 Misure di tutela della riservatezza

Aruba PEC dispone l'utilizzo di adeguate misure di sicurezza al fine di preservare la riservatezza, l'integrità e la disponibilità di dati personali dell'Interessato. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

9.3 Protezione dei dati personali in ambito SPID minori

Aruba PEC rilascia l'identità digitale SPID ai minori nel rispetto dei diritti dei minori stessi e dei loro genitori in tema di trasparenza e protezione dei dati personali, secondo quanto previsto dalle "Linee guida per la fruizione dei servizi SPID da parte dei minori" adottate da AgID, redatte in conformità al GDPR (art. 8) e al Codice Privacy (art. 2 quinquies). Nello specifico, Aruba PEC garantisce che:

A) i minori abbiano diritto a:
   1. ricevere un'informativa sul trattamento dei dati personali chiara, semplice e comprensibile, adeguata alla loro età, facilmente accessibile, concisa, ma esaustiva, così da rendere comprensibile il trattamento svolto dal Titolare del trattamento;
   2. fruire di una specifica protezione dei dati personali nella piena applicazione dei principi dettati dall'art. 5 del GDPR (liceità, correttezza e trasparenza, minimizzazione dei dati trattati, esattezza e aggiornamento, limitazione della conservazione, integrità e riservatezza, accountability);
   3. ottenere un'identità digitale sicura e proporzionata, tramite la raccolta dei soli attributi necessari all'identificazione (es. nome, CF, data di nascita ecc);
   4. fruire di sistemi di autenticazione adeguati alla loro età, senza dover ricorrere a strumenti dei genitori (es. il telefono del genitore);
   5. accedere in maniera riservata a specifici servizi senza l'autorizzazione del genitore (es istituti scolastici, prevenzione o consulenza diretta al minore);
   6. gestire la propria identità digitale, per gli ultraquattordicenni, compresa la possibilità di sospendere autonomamente la propria identità digitale e consultare gli accessi effettuati tramite SPID;
   7. Essere tutelati nel passaggio alla maggiore età mediante la rimozione delle restrizioni legate alla minore età, la cancellazione delle informazioni rese disponibili al genitore (fatti salvi i log necessari per obbligo di legge) e la possibilità di decidere se mantenere o revocare l'identità digitale.

B) i genitori abbiano il diritto a:
   1. ricevere una informativa completa sul trattamento dei dati del minore;
   2. Essere informati tramite notifiche qualora il minore richieda l'attivazione dello SPID o tenti l'accesso a servizi soggetti a preventiva autorizzazione del genitore
   3. verificare le identità digitali dei figli associate alla propria identità SPID;
   4. controllare gli accessi del minore mediante la possibilità di autorizzare o negare l'accesso ai servizi che lo richiedono, stabilire la durata dell'autorizzazione e revocarla in qualunque momento;
   5. gestire l'identità digitale del minore potendo disporre la sospensione o revoca dell'identità digitale del minore, gestire le autorizzazioni di accesso ai servizi e accedere solo alle informazioni strettamente necessarie;

6. ricevere adeguato supporto e tutela dall'IdP rispetto al trattamento dei dati personali del minore attraverso l'adozione di misure di sicurezza adeguate, l'osservanza dei principi di minimizzazione e di necessità e la conservazione dei log di autorizzazione nei soli limiti temporali previsti, senza includere dati non necessari.

10 Disposizioni finali

10.1 Nullità od inapplicabilità di clausole

Se una qualsivoglia disposizione del presente Manuale Operativo, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente Manuale Operativo (così come l'applicazione della disposizione invalida o inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

10.2 Interpretazione

Salvo disposizioni diverse, questo Manuale Operativo dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù degli usi commerciali internazionali.

10.3 Nessuna rinuncia

La mancata applicazione da parte di qualsivoglia persona di una delle disposizioni di cui al presente Manuale Operativo non sarà ritenuta rinuncia a future applicazioni di suddetta disposizione o di qualsiasi altra disposizione.

10.4 Comunicazioni

Qualora una persona desideri o sia tenuta ad effettuare delle comunicazioni, domande o richieste in relazione al presente Manuale Operativo, tali comunicazioni dovranno avvenire attraverso messaggi PEC indirizzati alla seguente casella assistenza.spid@arubapec.it oppure in forma scritta.

Le comunicazioni scritte dovranno essere consegnate da un servizio di posta che confermi la consegna per iscritto oppure tramite assicurata convenzionale, raccomandata a/r, indirizzate all'indirizzo indicato al par. 2.1.

10.5 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.

10.6 Modifiche del Manuale Operativo

Aruba PEC S.p.A. si riserva il diritto di aggiornare periodicamente il presente Manuale Operativo in modo estensibile al futuro e non retroattivo.

Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del Manuale Operativo.

10.7 Violazioni e altri danni materiali

I titolari e i richiedenti dell'identità digitale rappresentano e garantiscono che la loro presentazione al Gestore e l'utilizzo delle informazioni relative alla richiesta dell'identità digitale non interferiscano né danneggino i diritti di una qualsiasi terza parte di qualunque giurisdizione in merito a marchi, marchi di identificazione di servizio, nomi commerciali, nomi societari, o ogni altro diritto di proprietà intellettuale, e che non tenteranno di utilizzare l'identità digitale (e le informazioni in esso contenute) per scopi illegali, ivi compresi interferenze illecite su vantaggi contrattuali o potenziali vantaggi aziendali, concorrenza sleale, azioni volte a ledere la reputazione di altra persona, pubblicità ingannevole, e ingenerare confusione su persone fisiche o giuridiche.
I titolari e i richiedenti dell'identità digitale si obbligano a manlevare e indennizzare il Gestore contro qualunque perdita o danno derivanti da una tale interferenza o infrazione.

10.8 Norme applicabili

Le operazioni di gestione e rilascio delle identità digitali contenute nel presente Manuale Operativo sono assoggettate alle leggi dell'ordinamento italiano. L'applicabilità, l'esecuzione, l'interpretazione e la validità del presente Manuale Operativo sono regolate dalle leggi italiane, indipendentemente dal contratto o altre scelte di disposizioni di legge e senza la necessità di stabilire un punto di contatto commerciale in Italia. Questa scelta è volta a garantire a tutti gli utenti un'uniformità di procedure e interpretazioni, indipendentemente dal luogo in cui essi risiedono o utilizzano le loro identità digitali.

10.9 Foro competente

Per tutte le eventuali controversie giudiziarie nelle quali risulti attore o convenuto il Gestore Aruba PEC S.p.A. e relative all'utilizzo del servizio di identità digitale e, alle modalità operative e all'applicazione delle disposizioni del presente Manuale sarà competente esclusivamente il Foro di Arezzo.

APPENDICE A - Codici e formati dei messaggi di anomalia

Rif. Tabella messaggi di anomalia SPID v. 1.4 – AgID

Error Code	Scenario di riferimento	Binding	HTTP Status Code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata IdP	Troubleshooting utente	Troubleshooting SP	Note
1	Autenticazione corretta	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)	n.a.	n.a.	n.a.	
Anomalie del sistema									
2	Indisponibilità sistema	HTTP-Redirect HTTP POST	HTTP 500	n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio più tardi	n.a.	
3	Errore di sistema	HTTP-Redirect HTTP POST	HTTP 500	n.a.	Utente	Pagina di cortesia con messaggio *"Sistema di autenticazione non disponibile - Riprovare più tardi"*	Ripetere l'accesso al servizio più tardi	n.a.	Tutti i casi di errore di sistema in cui è possibile mostrare un messaggio informativo all'utente
Anomalie delle richieste									
Anomalie sul binding									

4	Formato *binding* non corretto	HTTP-Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Formato richiesta non corretto - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta	Parametri obbligatori: *SAMLRequest* *SigAlg* *Signature* Parametri non obbligatori: *RelayState*
		HTTP-POST							Parametri obbligatori: *SAMLRequest* Parametri non obbligatori: *RelayState*
5	Verifica della firma fallita	HTTP-Redirect HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Impossibile stabilire l'autenticità della richiesta di autenticazione - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto *EntityID* nei metadati registrati

6	*Binding* su metodo HTTP errato	HTTP-Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Formato richiesta non ricevibile - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare *metadata* Gestore dell'identità (IdP)	Invio richiesta in HTTPRedirect su entrypoint HTTP-POST dell'identity
		HTTP POST							Invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity
Anomalie sul formato della AuthnReq									
7	Errore sulla verifica della firma della richiesta	HTTP-Redirect HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "*Formato richiesta non corretto - Contattare il gestore del servizio*"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o non corrispondente ad un fornitore di servizi riconosciuto o non associato al corretto EntityID nei metadati registrati

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

11	*ID* (Identificatore richiesta) non presente, malformato o non conforme	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr11	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata solo a seguito di una positiva verifica della firma.
12	*RequestAuthnContext* non presente, malformato o non previsto da SPID	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "*Autenticazione SPID non conforme o non specificata*"		Informare l'utente	Auth livello richiesto diverso da: https://www.spid.g ov.it/SpidL1 https://www.spid.g ov.it/SpidL2 https://www.spid.g ov.it/SpidL3
13	*IssueInstant* non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente	
14	*destination* non presente, malformata o non coincidente con ill Gestore delle identità ricevente la richiesta	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)	n.a	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente	

15	attributo *isPassive* presente e attualizzato al valore true	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15	Fornitore del servizio (SP)	n.a	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente	
16	AssertionConsumerService non correttamente valorizzato	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupporte ErrorCode nr16	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente	*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-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr17	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta Fornire pagina di cortesia all'utente	Nel caso di valori diversi dalla specifica del parametro opzionale *AllowCreate* si procede con l'autenticazione senza riportare errori
18	*AttributeConsumerServiceIndex* malformato o che riferisce a un valore non registrato nei metadati di SP	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18	Fornitore del servizio (SP)	n.a.	n.a.	Riformulare la richiesta con un valore dell'indice presente nei metadati	
Anomalie derivante dall'utente									
19	Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero tentativi secondo le policy adottate)	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19	Fornitore del servizio (SP)	Messaggi di errore specifico ad ogni interazione prevista	Inserire credenziali corrette	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso	Si danno indicazioni specifiche e puntuali all'utente per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi

								al servizio richiesto	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-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20	Fornitore del servizio (SP)	n.a	Acquisire credenziali di livello idoneo all'accesso al servizio richiesto	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
21	Timeout durante l'autenticazione utente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21	Fornitore del servizio (SP)	n.a.	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinato periodo di tempo	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	

22	Utente nega il consenso all'invio di dati al SP in caso di sessione vigente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22	Fornitore del servizio (SP)	n.a.	Dare consenso	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1.
23	Utente con identità sospesa/revocata o con credenziali bloccate	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: *"Credenziali sospese o revocate"*		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
24	Riservata								
25	Processo di autenticazione annullato dall'utente	HTTP-Redirect HTTP POST	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr25	Fornitore del servizio (SP)	n.a.		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	

Tabella 4 - Codici anomalie