Andrea Sassetti
Firmato digitalmente il 14/04/2022 10:20:08 CEST

**Aruba PEC S.p.A.**

# Manuale Operativo Sistema Pubblico per la gestione dell'Identità Digitale (SPID) v.1.8

Versione: 1.8
Data: 14/04/2022
Redazione: Alessandro Capobianco
Verificato da: Federico Ciofi e Nicole Mazzoni
Approvato da: Andrea Sassetti
Classificazione documento: Pubblico

| VERSIONE N° | DATA | NATURA DELLA MODIFICA |
|---|---|---|
| 1.0 | 15/02/2016 | Prima versione |
| 1.1 | 24/05/2017 | Aggiornamento sede legale.<br>**Par.2.3**: modificati i riferimenti normativi<br>**Par.2.4**: aggiunti RTO e RPO in definizioni e acronimi<br>**Par.3.5**: aggiornati riferimenti del Responsabile del Manuale operativo<br>**Par.6.2.2:** sostituito termine "residenza" con "domicilio"<br>**Cap.9**: formattazione livelli di servizio |
| 1.2 | 21/06/2017 | **Inserimento devisu remoto con dispositivi mobile**<br><br>**Tutto il documento**: aggiornata la definizione ed uniformati riferimenti a "Titolare" e "Cliente" in "Richiedente"; migliorato uso terminologia legata all'identificazione<br>**Par 6.2.1.**: precisate condizioni per operatività CDRL per OdR ed IR<br><br>**Par.6.3 p.to 8**: aggiornate modalità di riconoscimento<br><br>**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)<br>**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<br>**Par 4.1**: aggiornate le responsabilità del Titolare dell'Identità<br>**Par 4.2**: aggiornate le responsabilità dell'IdP<br>**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<br>**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<br><br>**Par. 7.2.3:** aggiunto collegamento modalità di rinnovo<br><br>**Cap.11:** modificate disposizioni finali<br><br>**Tutto il documento:**<br>- rimossi rimandi a documento esterno di Piano per la Sicurezza;<br>- 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<br>**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 Sommario

**2 Introduzione** ..... 5
*2.1 Scopo del documento e principali raccomandazioni ai lettori* ..... 5
*2.2 Standard di riferimento* ..... 5
*2.3 Riferimenti* ..... 7
*2.4 Definizioni ed acronimi* ..... 7
**3 Dati identificativi – Pubblicazione del Manuale Operativo** ..... 11
*3.1 Dati identificativi del gestore dell'identità digitale* ..... 11
*3.2 Versione del manuale operativo* ..... 11
*3.3 Pubblicazione del manuale operativo* ..... 11
*3.4 Procedure per l'aggiornamento del Manuale Operativo* ..... 11
*3.5 Responsabile del manuale operativo* ..... 12
**4 Disposizioni generali** ..... 12
*4.1 Obblighi dell'utente* ..... 12
*4.2 Obblighi e Responsabilità del Gestore dell'Identità Digitale* ..... 13
*4.3 Obblighi dei fornitori di Servizi* ..... 16
*4.4 Obblighi dei Soggetti esterni che svolgono l'attività di registrazione e/o riconoscimento (de visu)* 16
*4.5 Obblighi del Richiedente* ..... 16
*4.6 Obblighi connessi al trattamento dei dati personali* ..... 17
*4.7 Limitazioni di Responsabilità ed eventuali limitazioni agli indennizzi* ..... 17
*4.7.1 Conoscenza del Manuale Operativo* ..... 17
*4.7.2 Forza Maggiore* ..... 17
*4.7.3 Declinazioni e Limitazioni del Gestore* ..... 17
**5 Architettura** ..... 17
*5.1 Architettura applicativa* ..... 17
*5.2 Architettura fisica* ..... 19
*5.3 Architettura dei sistemi di autenticazione* ..... 19
*5.3.1 Notifiche di accesso* ..... 22
*5.3.2 Codici e formato messaggi di anomalie* ..... 22
*5.4 Sistemi di autenticazione e credenziali* ..... 23
*5.4.1 Livello di sicurezza 1* ..... 23
*5.4.2 Livello di sicurezza 2* ..... 24
*5.4.3 Livello di sicurezza 3* ..... 25
*5.5 Misure anticontraffazione* ..... 26
*5.5.1 Livello 2* ..... 26
*5.5.2 Livello 3* ..... 28
*5.6 Tracciatura degli accesi* ..... 28
*5.6.1 Accessi fisici* ..... 28
*5.6.2 Accessi logici* ..... 28

*5.6.3 Tracciature accessi di autenticazione utenti* ..... *29*
**6 Operatività** ..... 29
*6.1 Funzioni del personale addetto al servizio di gestione delle identità digitali* ..... 29
*6.2 Richiesta dell'identità digitale* ..... 30
*6.2.1 Richiesta da sportello dell'identità SPID* ..... *30*
*6.2.2 Richiesta online identità SPID* ..... *31*
*6.3 Modalità di identificazione ai fini del rilascio dell'identità digitale* ..... 33
*6.3.1 Identificazione con operatore* ..... *34*
*6.3.2 Identificazione informatica mediante TS-CNS, CNS, CIE o firma digitale* ..... *37*
*6.4 Verifica degli attributi associati all'identità digitale* ..... 37
*6.4.1 Identità digitale e attributi* ..... *37*
*6.4.2 Verifica degli attributi identificativi (identità dichiarata)* ..... *38*
*6.4.3 Verifica degli attributi secondari* ..... *39*
*6.5 Attivazione dell'identità digitale* ..... 39
*6.6 Rilascio, consegna e attivazione delle credenziali* ..... 40
**7 Gestione delle identità digitali** ..... 42
*7.1 Gestione dati raccolti per la verifica dell'identità digitale* ..... 42
*7.2 Gestione del ciclo di vita* ..... 43
*7.2.1 Gestione degli attributi* ..... *43*
*7.2.2 Sospensione e Revoca dell'Identità* ..... *44*
*7.2.3 Gestione ciclo di vita delle credenziali* ..... *45*
*7.3 Richiesta dei dati da parte del Titolare* ..... 46
*7.4 Gestione rapporti con utenti* ..... 47
**8 Sistema di monitoraggio** ..... 47
**9 Livelli di servizio** ..... 48
*9.1 Livelli di servizio garantiti per le diverse fasi della registrazione* ..... 48
*9.2 Livelli di servizio garantiti per le diverse fasi della gestione del ciclo di vita delle identità* ..... 49
*9.3 Livello di servizio garantito per le diverse fasi del processo di autenticazione* ..... 49
*9.4 Continuità operativa* ..... 50
**10 Modalità di protezione dei dati personali** ..... 50
*10.1 Archivi contenenti dati personali* ..... 50
*10.2 Misure di tutela della riservatezza* ..... 50
**11 Disposizioni finali** ..... 51
*11.1 Nullità od inapplicabilità di clausole* ..... 51
*11.2 Interpretazione* ..... 51
*11.3 Nessuna rinuncia* ..... 51
*11.4 Comunicazioni* ..... 51
*11.5 Intestazioni e Appendici del Presente Manuale Operativo* ..... 51
*11.6 Modifiche del Manuale Operativo* ..... 51
*11.7 Violazioni e altri danni materiali* ..... 51

*11.8 Norme applicabili* ..... 52
*11.9 Foro competente* ..... 52
**APPENDICE A - Codici e formati dei messaggi di anomalia** ..... 53

# 2 Introduzione

## *2.1 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 contattare il servizio clienti all'indirizzo: assistenza.spid@staff.aruba.it.

## *2.2 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 (http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_attributi_idp.pdf) |
| SPID-TabErr | Tabella Codici di Errore (http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_codici_Errore.pdf) |

## 2.3 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).

## 2.4 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** | E' il recepimento del framework SPID da parte di entità di certificazione o di fornitori di servizi in rete. |
| **Agenzia (anche AgID)** | Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Gestori di Identità Digitali) |
| **Attributi identificativi** | Nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, il codice fiscale o la partita IVA e gli estremi del documento d' identità utilizzato ai fini dell'identificazione; |
| **Attributi secondari** | Il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni |
| **Attributi qualificati** | Le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati. |
| **Autenticazione 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 |
| **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.<br>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; |
| **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. |
| **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<br>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** | E' il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v). Prima dell'attribuzione dell'identità digitale tale soggetto è chiamato Richiedente |
| **TCP** | Transmission Control Protocol |
| **User Agent** | Sistema utilizzato dall'utente per l'accesso ai servizi (di solito il browser per la navigazione in rete); |

# 3 Dati identificativi – Pubblicazione del Manuale Operativo

## *3.1 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/ |

## *3.2 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.

## *3.3 Pubblicazione del manuale operativo*

Il presente Manuale Operativo è reperibile in formato elettronico presso il sito web del Gestore indicato nel paragrafo 3.1.
Riferimento al presente Manuale Operativo e le altre informazioni relative al Gestore previste dal DPCM sono pubblicate presso il registro SPID gestito dall'AgID.

## *3.4 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.

### *3.5 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

## 4 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.

### *4.1 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 §7 del presente documento.

## *4.2 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. Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione.
44. 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.
45. Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.

46. In caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.
47. Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa.
48. 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.
49. In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
50. Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID.
51. 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.

## *4.3 Obblighi dei fornitori di Servizi*

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

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.

## *4.4 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 ArubaID - 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.

## *4.5 Obblighi del Richiedente*

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

## *4.6 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.

## *4.7 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.

### 4.7.1 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.

### 4.7.2 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.

### 4.7.3 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.

# 5 Architettura

## *5.1 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.

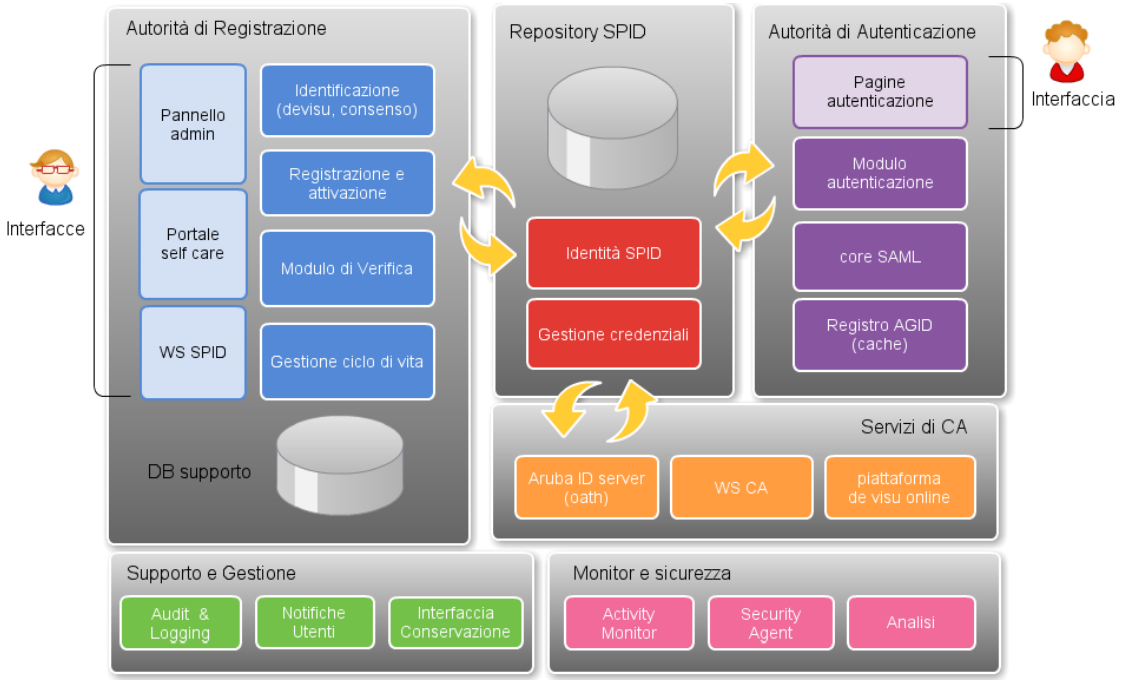


**Figura 1 - Architettura applicativa SPID**

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.

## *5.2 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).

## *5.3 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.

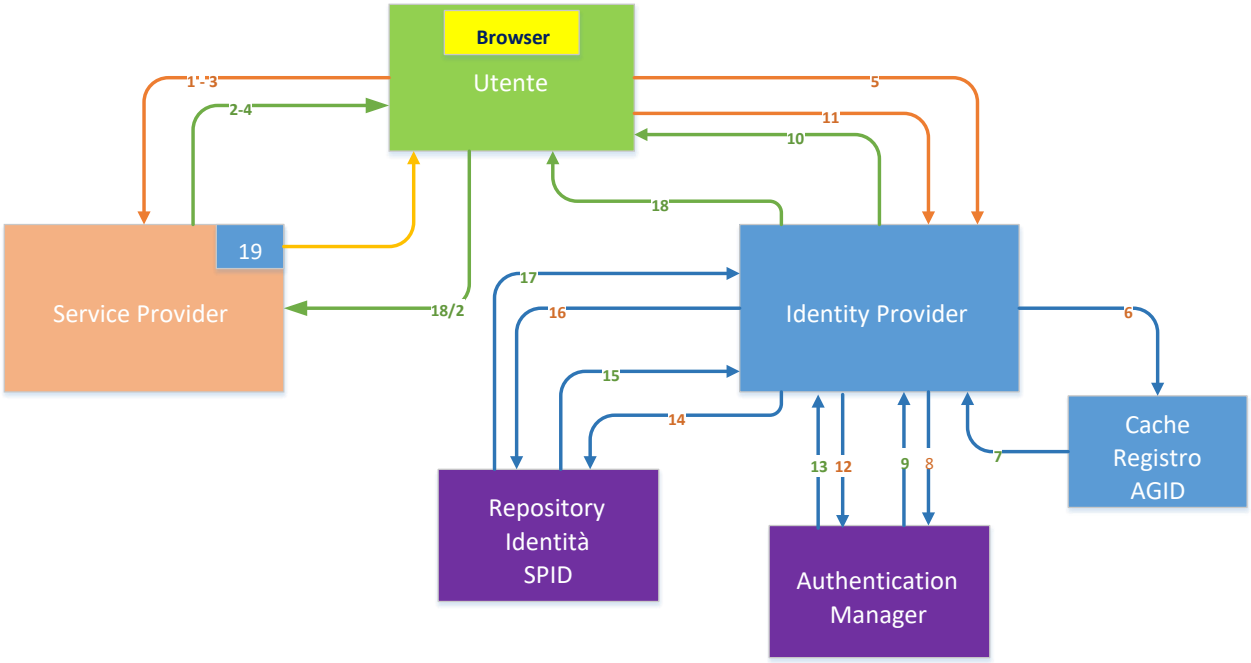


**Figura 2 - Architettura sistema di autenticazione**

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. Al fine 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.

### 5.3.1 Notifiche di accesso

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

### 5.3.2 Codici e formato messaggi di anomalie

Il servizio di autenticazione SPID dell'IdP 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_SPID | 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 |
| 0326 | ERRORE_DECRYPT_EMERGENCY_CODE | Errore gestione codice emergenza (decrypt) |
| 0327 | CODICE_EMERGENZA_NON_TROVATO | Codice emergenza non presente in tabella UTENTI_SPID |
| 0328 | CODICE_EMERGENZA_MISMATCH | Codice emergenza non corretto |
| 0342 | CREDENZIALE_STATO_NON_ATTIVA | Credenziale in stato non attiva |

**Tabella 1 - Codici aggiuntivi anomalia e messaggi**

## *5.4 Sistemi di autenticazione e credenziali*

### 5.4.1 Livello di sicurezza 1

Il sistema di Autenticazione proposto per il livello di sicurezza 1 si basa sull'uso di credenziali composte da un singolo fattore (ad es. password).

In particolare, 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

### 5.4.2 Livello di sicurezza 2

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

**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:

5. Il dispositivo OTP è conforme alle specifiche OATH
6. Il dispositivo OTP non può essere clonato
7. Il dispositivo OTP possieda un sistema antitampering basato su meccanismi di tamper evidence e tamper response
8. Il dispositivo OTP è univocamente identificabile

**OTP Mobile**

OTP Mobile è un'applicazione per smartphone di ultima generazione installabile sui più comuni cellulari quali iPhone, BlackBerry, Android e Windows phone. 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.

**Aruba Call**

Si tratta di un sistema di autenticazione OTP destinato ad essere utilizzato dagli utenti che non possiedono uno smartphone ma un semplice cellulare anche di vecchia generazione. All'atto dell'autenticazione l'utente riceverà una chiamata sul proprio cellulare (comunicato e validato, come previsto dalla norma, in fase di registrazione) da un numero chiamante le cui ultime 4 cifre rappresentano il codice OTP da utilizzare. Il sistema non comporta costi per l'utente finale in quanto non è necessaria alcuna connessione dati, avviene in tempo reale (più velocemente di un sms) ed è rivolto anche ai cittadini che hanno meno familiarità con la tecnologia.

**Aruba SMS**

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

### 5.4.3 Livello di sicurezza 3

Il sistema di Autenticazione Forte proposto per il livello di sicurezza 3 si basa, così come previsto dall'Art 6 del DPCM, 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

## *5.5 Misure anticontraffazione*

### 5.5.1 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 di Firma Remota 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

**OTP Mobile**

L'applicazione OTP per smartphone di Aruba PEC 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 OTP mobile Aruba PEC 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).

**Aruba CALL**

Aruba CALL è il servizio di strong authentication di Aruba PEC nel quale, prima dell'autenticazione, l'utente riceve una telefonata dal sistema dell'IdP che viene immediatamente interrotta.
Il numero chiamante è diverso per le ultime cifre.
Queste cifre rappresentano il codice HOTP generato dal sistema di autenticazione del Gestore e trasmesso all'utente attraverso la rete telefonica.
L'utente, per completare il processo di autenticazione, dovrà semplicemente inserire le ultime cifre del numero chiamante all'interno della maschera di proposizione della credenziale di strongauth e questo permetterà di completare il processo di autenticazione.
Come si può facilmente intuire 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.<br>In ogni caso la chiamata, 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 |

**Aruba SMS**

Aruba 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.<br>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.

### 5.5.2 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

## *5.6 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.

### 5.6.1 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.

### 5.6.2 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.

### 5.6.3 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

Ogni tracciatura di accesso viene inviata in Conservazione.
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.
L'accesso in lettura e scrittura ai sistemi che custodiscono le tracciature è garantito al solo personale tecnico dell'IdP secondo le policy descritte in § Accessi fisici5.6.1 e 5.6.2.
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.

# 6 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.

## *6.1 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.

## *6.2 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;
- Identità digitale SPID Persona Fisica Uso Professionale.

La richiesta può essere effettuata online o da sportello, successivamente il titolare dovrà effettuare l'identificazione per concludere il processo di rilascio.

### 6.2.1 Richiesta dell'identità SPID da sportello

#### *6.2.1.1 MODALITÀ 1 - CDRL*

La richiesta dell'identità SPID viene effettuata dal richiedente presso un soggetto incaricato dal Gestore denominato Centro di Registrazione Locale (CDRL).
In questa modalità 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.

#### *6.2.1.2 DOCUMENTAZIONE DA PRESENTARE ALLO SPORTELLO*

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:

1. cognome e nome;
2. sesso, data e luogo di nascita;
3. codice fiscale;
4. estremi del documento di riconoscimento presentato per l'identificazione;
5. 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:

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

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.

### 6.2.2 Richiesta dell' identità SPID online

Il richiedente accede al portale messo a disposizione dall'IdP e richiede una delle identità digitali indicate al cap. 6.2 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 dell'identità SPID Persona Fisica Uso Professionale)

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 in § 5.4.1.

Dati di contatto:

i. email
ii. numero di cellulare

Dati anagrafici

iii. Codice fiscale
iv. Nome
v. Cognome
vi. Sesso
vii. Data nascita
viii. Luogo nascita (Stato, Provincia, Comune)
ix. Numero di Tessera Sanitaria
x. Email PEC

xi. 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. typo).

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. typo).
Al termine del flusso descritto si ha un un'identità digitale creata (ma non attiva).

## *6.3 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 dell'identità SPID Persona Fisica Uso Professionale.

La 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.

### 6.3.1 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 nel paragrafo § 6.2.1.

#### *6.3.1.1 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, secondo quanto previsto dall'art 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445, tra i quali:

- 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.

#### *6.3.1.2 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 biometrici.
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 informativa privacy, esprimere il consenso al trattamento dei dati personali per la registrazione audio-video. Il consenso è nuovamente raccolto non appena iniziata la registrazione.

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:
    1. Presenza di webcam
    2. sistema audio dotato di casse e microfono funzionanti
    3. browser aggiornato con supporto alla tecnologia webrtc (come ad esempio Chrome o Firefox)
    4. connessione internet a banda larga
2. Con un dispositivo mobile, smartphone o tablet, che soddisfi i seguenti requisiti:
    1. sistema operativo Android o iOS di ultima generazione
    2. fotocamera frontale
    3. sistema audio dotato di casse e microfono funzionanti
    4. 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 in § 6.3.1.1.
Si ricorda che durante il riconoscimento è obbligatorio avere a disposizione documenti e contatti forniti in fase di registrazione (vedi par.6.2.2).
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;
- 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;
- 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. I dati di registrazione, costituiti da file audio-video, 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 (§ 3.2.1 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.

### 6.3.2 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.
La possibilità di perseguire le modalità di identificazione sopraindicate è fornita al richiedente nella fase finale di richiesta online dell'identità SPID (§ 6.2.2).
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.
- 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.

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.

## *6.4 Verifica degli attributi associati all'identità digitale*

### 6.4.1 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.

### 6.4.2 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. 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 tale 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.<br><br>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).<br><br>Il codice fiscale è verificato presso il servizio messo a disposizione dall'Agenzia delle Entrate sul suo portale; |

**Tabella 1 - 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).<br><br>Dette evidenze sono ritenute valide ed autentiche sulla base di quanto risulta da soggetti istituzionali competenti.<br><br>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 2 - Requisiti da soddisfare/Livelli di sicurezza SPID (persona giuridica)**

### 6.4.3 Verifica degli attributi secondari

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

## *6.5 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).

## *6.6 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 (§ 7) 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. Insieme a queste credenziali, per i livelli 2 e 3 verranno consegnate al Richiedente delle scratch card che conterranno diverse informazioni a seconda del livello.

In linea generare verranno consegnate, o rese disponibili con uso esclusivo:

**Per il livello2:**

1. Scratch card contenente:
   1. il codice utente da utilizzare per le operazioni di ciclo di vita delle proprie credenziali (sospensione e riattivazione);
   2. il codice di attivazione da utilizzare per la prima configurazione della APP OTP mobile (nel caso in cui sia stato scelto questo tipo di OTP) □ Dispositivo OTP tra quelli indicati in § 5.5

**Per il livello 3:**

2. Scratch card contenente:
   1. il codice utente da utilizzare per le operazioni di ciclo di vita delle proprie credenziali (sospensione e riattivazione);
   2. il codice di attivazione da utilizzare per la prima configurazione della APP OTP mobile (nel caso in cui sia stato scelto questo tipo di OTP)

3. Dispositivo crittografico che soddisfa i requisiti dell'Allegato 3 della Direttiva 1999/93/CE contenente i certificati di autenticazione a SPID

Si precisa che le scratch card possono essere sia fisiche che virtuali.
In aggiunta, i dispositivi sopra indicati possono essere consegnati secondo diverse modalità a seconda della tipologia di identificazione che è stata scelta dal Richiedente.
Nel caso in cui il richiedente si presenti presso uno sportello fisico, l'operatore di sportello consegnerà una scratch card.
Nel caso di riconoscimento via webcam o mediante CNS o CIE o Firma digitale, potranno essere inviati al richiedente questi dispositivi:

1. scratch card virtuale
2. scratch card fisica (indirizzo dichiarato in fase di autenticazione) dispositivo OTP o crittografico fisico (indirizzo dichiarato in fase di autenticazione)

### *6.6.1 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.

# 7 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.

## *7.1 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.

## *7.2 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:
    1. conservazione;
    2. sospensione e revoca;
    3. rinnovo e sostituzione

### 7.2.1 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:
    1. estremi del documento di riconoscimento e relativa scadenza;
    2. gli attributi secondari così come definiti all'articolo 1, comma d) del DPCM;

2. Per le persone giuridiche:
    1. indirizzo sede legale
    2. codice fiscale o P.IVA (nei rari casi di variazione a seguito di particolari mutazioni societarie)
    3. rappresentante legale della società
    4. 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.).

### 7.2.2 Sospensione e Revoca 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 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 scadenza contrattuale.

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 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 modalità sopra descritte sono riportate al link https://guide.pec.it/revoca-spid.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.
Nel caso di richiesta di sospensione, trascorsi trenta giorni dalla suddetta sospensione, Aruba PEC provvede al ripristino dell'identità precedentemente sospesa qualora non pervenga con le modalità sopra indicate una richiesta di revoca.
La revoca di una identità digitale comporta conseguentemente la revoca delle relative credenziali.
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

### 7.2.3 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 in §6.6
3. attivazione delle credenziali o dei mezzi usati per la loro produzione; maggiori dettagli sono riportati in § 6.6
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/spid/rinnovo-del-servizio.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.

### 7.2.4 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 di emergenza ricevuto in fase di registrazione.

### 7.2.5 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 https://guide.hosting.aruba.it/guida-alla-gestione-dei-servizi/recupero-codici-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 nè della PEC nè 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.

## *7.3 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.

### *7.4 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. Email - assistenza.spid@staff.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

### *7.5 Guida utente del servizio*

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

# 8 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 in § 5.1, 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.

# 9 Livelli di servizio

Gli orari di disponibilità del servizio sono definiti nei paragrafi che seguono.

## *9.1 Livelli di servizio garantiti per le diverse fasi della registrazione*

1. **Richiesta online da parte dell'utente**

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

2. **Riconoscimento/Identificazione**
   1. Riconoscimento/Identificazione de-visu Tutti i giorni lavorativi, dalle 9:00 alle 18:00
   2. Riconoscimento/Identificazione con TS-CNS/CNS/CIE Tutti i giorni della settimana, festivi inclusi
   3. Riconoscimento/Identificazione con Firma Digitale Tutti i giorni della settimana, festivi inclusi
   4. Riconoscimento/Identificazione con sessioni audio/video

Tutti i giorni lavorativi, dalle 9:00 alle 18:00

3. **Creazione dell'identità digitali e delle relative credenziali**

Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi. Disponibilità ≥ 99%

4. **Consegna delle credenziali**

Tutti i giorni lavorativi, dalle 9:00 alle 18:00. Disponibilità ≥ 98%

5. **Attivazione dell'identità digitale**

Tutti i giorni lavorativi, dalle 9:00 alle 18:00. Disponibilità ≥ 98%

## *9.2 Livelli di servizio garantiti per le diverse fasi della gestione del ciclo di vita delle identità*

1. **Sospensione, riattivazione revoca tramite WEB**

Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi

2. **Disponibilità** ≥ 99%
3. **Sospensione, riattivazione revoca tramite CALL-CENTER** Tutti i giorni lavorativi, dalle 9:00 alle 18:00. Disponibilità ≥ 98%
4. **Sospensione, riattivazione revoca tramite PEC**

Tutti i giorni lavorativi, dalle 9:00 alle 18:00. Disponibilità ≥ 98%

## *9.3 Livello di servizio garantito per le diverse fasi del processo di autenticazione*

| Indicatore di qualità | Modalità funzionamento | Valore limite |
|---|---|---|
| **Disponibilità del sottoservizio di registrazione identità** | Erogazione automatica | ≥ 99,0%<br>Singolo evento di indisponibilità ≤6 ore |
| | Erogazione in presenza | ≥ 98,0% |
| **Tempo di risposta del sottoservizio di registrazione identità** | | ≤ 24h (ore lavorative) |
| **Disponibilità del sottoservizio di gestione rilascio credenziali** | Erogazione automatica | ≥ 99,0%<br>Singolo evento di indisponibilità < =6 ore |
| | Erogazione in presenza | ≥ 98,0% |
| **Tempo di rilascio credenziali** | | ≤ 5 giorni lavorativi |
| **Tempo riattivazione delle credenziali** | | ≤ 2 giorni lavorativi |
| **Disponibilità del sottoservizio di sospensione e revoca delle credenziali** | | ≥ 99,0%<br>Singolo evento di indisponibilità < =6 ore |
| **Tempo di sospensione delle credenziali** | | < =30 minuti |
| **Tempo di revoca delle credenziali** | | ≤ 5 giorni lavorativi |
| **Disponibilità del sottoservizio di rinnovo e sostituzione delle credenziali** | Erogazione automatica | ≥ 99,0% |
| | Erogazione in presenza | ≥ 98,0% |

| | | |
|---|---|---|
| **Tempo di rinnovo e sostituzione delle credenziali** | | ≤ 5 giorni lavorativi |
| **Disponibilità del sottoservizio di autenticazione** | | ≥ 99,0%<br>Singolo evento indisponibilità ≤ 4 ore |
| **Tempo di risposta del sottoservizio di autenticazione** | | Tempo di risposta ≤3 sec almeno nel 95,0% delle richieste |

## *9.4 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 |

# 10 Modalità di protezione dei dati personali

## *10.1 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.

## *10.2 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.

# 11 Disposizioni finali

## *11.1 Nullità od inapplicabilità di clausole*

Se una qualsivoglia disposizioni 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.

## *11.2 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.

## *11.3 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.

## *11.4 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 in § 3.1.

## *11.5 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.

## *11.6 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.

## *11.7 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.

## *11.8 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 dalla 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.

## *11.9 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

| Error Code | Casistica | Binding | http status code | SAML Status code/Sub status/Status message | Destinatario notifica | Screen IDP | Messaggio utente | Troubleshooting SP | Note |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Autenticazione corretta | HTTP POST Redirect | HTTP 200 | urn:oasis:names:tc:SAML:2.0:status:Success | Fornitore servizio | n.a. | n.a. | n.a. | |
| **Anomalie del sistema** | | | | | | | | | |
| 2 | Indisponibilità sistema | HTTP POST Redirect | n.a. | n.a. | Utente | Messaggio errore generico | Ripetere l'accesso al servizio più tardi | n.a. | |
| 3 | Errore di sistema | HTTP POST Redirect | HTTP 500 | n.a. | Utente | Pagina di cortesia con messaggio "Sistema di autenticazione non disponibile riprovare più tardi" | Ripetere l'accesso al servizio più tardi | n.a. | |
| **Anomalie delle richieste** | | | | | | | | | |
| **Anomalie binding** | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | Formato binding non corretto | HTTP POST<br>Redirect<br>----------<br>HTTP POST | HTTP 403 | n.a. | Utente | Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio" | Contattare il gestore del servizio | Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta | Parametri obbligatori: SAML Req, SigAlg, Signature<br>Parametri non obbligatori: RelayState<br>----------<br>Parametri obbligatori: SAML Req<br>Parametri non obbligatori: RelayState | |
| 5 | Verifica della firma fallita | HTTP POST<br>Redirect | 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 POST<br>Redirect<br>----------<br>HTTP POST | HTTP 403 | n.a. | Utente | Pagina di cortesia con messaggio "Formato richiesta non ricevibile- Contattare il gestore del servizio" | Contattare il gestore del servizio | Verificare metadata Gestore dell'identità (IdP) | invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell'identity<br>----------<br>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 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 POST | n.a. | n.a. | Fornitore del servizio (SP) | n.a. | n.a. | Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente | Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente alla verifica positiva della firma |
| 9 | Parametro version non presente, malformato o diverso da '2.0' | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:VersionMismatch ErrorCode nr09 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente | |
| 10 | Issuer non presente, malformato o non corrispondete all'entità che sottoscrive la richiesta | HTTP POST/HTTP Redirect | HTTP 403 | n.a. | Utente | Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio" | Contattare il gestore del servizio | Verificare il formato delle richieste prodotte | |
| 11 | Identificatore richiesta(ID) non presente, malformato o non conforme | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr11 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente | Identificatore necessario per la correlazione con la risposta |
| 12 | RequestAuthnContext non presente, malformato o non previsto da SPID | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext ErrorCode nr12 | Fornitore del servizio (SP) | Pagina temporanea con messaggio di errore: "Autenticazione SPID non conforme o non specificata" | | Informare l'utente | Auth livello richiesto diverso da: urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3 |
| 13 | IssueInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare correttamente la richiesta - Fornire | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | pagina di cortesia all'utente | |
| 14 | destination non presente, malformata o non coincidente con il Gestore delle identità ricevente la richiesta | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente | |
| 15 | attributo isPassive presente e attualizzato al valore true | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente | |
| 16 | AssertionConsumerServi ce non correttamente valorizzato | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr16 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente | AssertionConsumerServiceIndex presente e attualizzato con valore non riportato nei metadata<br><br>AssertionConsumerServiceIndex riportato in presenza di uno od entrambi gli attributi AssertionConsumerServiceURL e ProtocolBinding<br><br>AssertionConsumerServiceIndex non presente in assenza di almeno uno attributi AssertionConsumerServiceURL e ProtocolBinding |
| 17 | Attributo Format dell'elemento NameIDPolicy assente o non valorizzato secondo specifica | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr17 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente | Nel caso di valori diversi dalla specifica del parametro opzionale AllowCreate si procede con l'autenticazione senza riportare errori |
| 18 | AttributeConsumerServiceIndex malformato o che riferisce a un valore non registrato nei metadati di SP | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18 | Fornitore del servizio (SP) | n.a. | n.a. | Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente | |
| **Anomalie delle richieste** | | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 19 | Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero tentativi secondo le policy adottate) | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19 | Utente | Messaggi di errore specifico ad ogni interazione prevista | Inserire le credenziali corrette | Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto | Si danno indicazioni specifiche e puntuali all'utente per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi di determinate condizioni legate alle policy di sicurezza aziendali, ad esempio dopo 3 tentativi falliti, si risponde al SP. |
| 20 | Utente privo di credenziali compatibili con il livello richiesto dal fornitore del servizio | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20 | Fornitore del servizio (SP) | n.a. | acquisire credenziali di livello idoneo all'accesso al servizio richiesto | Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto | |
| 21 | Timeout durante l'autenticazione utente | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21 | Fornitore del servizio (SP) | n.a. | Si ricorda che l'operazione di autenticazione deve essere completata entro un determinati periodo di tempo | Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto | |
| 22 | Utente nega il consenso all'invio di dati al SP in caso di sessione vigente | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22 | Fornitore del servizio (SP) | | Dare consenso | Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto | Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1. |
| 23 | Utente con identità sospesa/revocata o con credenziali bloccate | HTTP POST/HTTP Redirect | n.a. | urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23 | Fornitore del servizio (SP) | Pagina temporanea con messaggio di errore: "Credenziali sospese o revocate" | | Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto | |

**Tabella 3 - Codici anomalie**