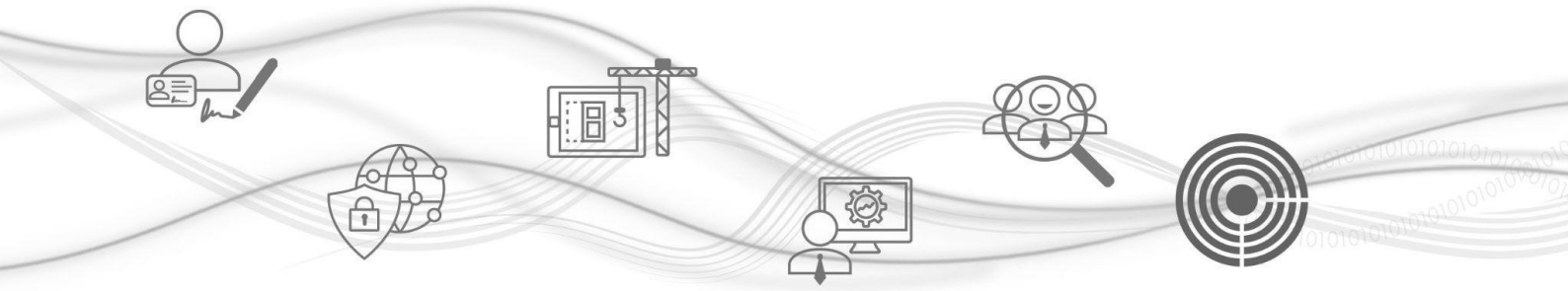
Namirial ID

Manuale Operativo del servizio di gestione del Sistema Pubblico dell'Identità Digitale (SPID)



Categoria	**SPID**	Codice Documento	**NAM-SPID-MO**	**Namirial S.p.A.**
Redatto da	**Margherita Menghini**	Nota di riservatezza	**Documento Pubblico**	**Il Legale Rappresentante**
Verificato da	**Franco Tafini**	Versione	**1.9**	**Massimilano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**24/11/2022**	—

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 24-11-2022 14:10:23
IP address: 88.51.218.18

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295
Codice destinatario T04ZHR3 | Capitale sociale € 7.762.625,20 i.v.

Indice

Storia delle modifiche apportate

VERSIONE	1.9
Data	03/10/2022
Motivazione	Revisione minore.
Modifiche	Variazioni informazioni assistenza

VERSIONE	1.8
Data	01/08/2022
Motivazione	Revisioni minori in tutti i capitoli.
Modifiche	Variazioni informazioni assistenza Aggiunto paragrafo su identificazione mediante App IDCheck

VERSIONE	1.7
Data	17/03/2021
Motivazione	Revisione minore
Modifiche	• Variazione informazioni assistenza; • Allineamento del processo di attivazione delle credenziali OTP; • Inserimento FEA nel processo di riconoscimento de visu; • Inserimento dettagli su SPID Professionale; • Inserimento delle modalità adottate per la verifica della titolarità del soggetto che richiede lo SPID Professionale per la Persona Giuridica; • Inserimento specifiche sul trattamento dati

VERSIONE	1.6
Data	23/10/2020
Motivazione	Revisione minore.
Modifiche	Variazione informazioni assistenza

VERSIONE	1.5
Data	11/03/2020
Motivazione	Revisione annuale del documento.
Modifiche	§2 Dati identificativi del Gestore: aggiornati link

	§2.1 Descrizione e certificazioni del gestore: aggiornate le certificazioni §12.4 Guida utente: aggiornato link §8.3.3 Aggiunta identificazione attraverso sessione audio-video (identificazione con webcam) §8.4.3.3 Aggiunta verifica attributi secondari a seguito di identificazione a vista da remoto (webcam)

VERSIONE	**1.4**
Data	06/02/2019
Motivazione	Revisione annuale e adeguamento normativo.
Modifiche	Sez. 4 - Modalità di protezione dei dati personali. Adeguamento al Regolamento (UE) 2016/679

VERSIONE	**1.3**
Data	04/07/2017
Motivazione	Quarta emissione del documento.
Modifiche	• Aggiornamento nome servizio SPID • Aggiornamento link portale e caselle e-mail

VERSIONE	**1.2**
Data	08/05/2017
Motivazione	Terza emissione del documento.
Modifiche	• Revisione obblighi Gestore e Utenti • Revisione SLA • Lievi integrazioni e precisazioni

VERSIONE	**1.1**
Data	30/03/2017
Motivazione	Seconda emissione del documento.
Modifiche	• Inserito riconoscimento con Firma Digitale, CNS, TS/CNS e CIE • Inserito il supporto per token OTP hardware OATH compliant

VERSIONE	**1.0**
Data	26/01/2017

Motivazione	Prima emissione del documento.
Modifiche	---

Riferimenti

NUMERO	DESCRIZIONE
[I]	Decreto del Presidente della Repubblica (DPR) 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001
[II]	Decreto del Presidente del Consiglio (DPCM) 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 azione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese", pubblicato sulla Gazzetta Ufficiale del 9 dicembre 2014, n.285
[III]	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) (Testo rilevante ai fini del SEE)
[IV]	Decreto Legislativo (CAD) 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale", pubblicato nella Gazzetta Ufficiale n.112 del 16 maggio 2005 con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179
[V]	Decreto Legislativo (DLGS 69) 21 giugno 2013, n. 69, convertito con modificazioni dalla legge del 9 agosto 2013, n. 69 che "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese"
[VI]	Regolamento UE n.910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, pubblicato nella Gazzetta Ufficiale dell'Unione Europea – serie L 257 del 28 agosto 2014
[VII]	Regolamento recante le regole tecniche (articolo 4, comma 2, DPCM 24 Ottobre 2014) per il gestore dell'identità digitale
[VIII]	Regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014)
[IX]	Regolamento recante le modalità per l'accreditamento e la vigilanza dei Gestori dell'identità digitale (articolo 1, comma 1, lettera l), DPCM 24 ottobre 2014)

[X]	Determinazione AgID n.16/2016: Pubblicazione di "Avvisi" sulle procedure tecniche inerenti il Sistema Pubblico per la gestione dell'Identità digitale (SPID) sul portale istituzionale dell'Agenzia
[XI]	AgID – SPID: Note tecniche sulle interfacce e sulle informazioni IDP/SP
[XII]	ISO EN UNI 9001:2015 – Sistema di Gestione della Qualità
[XIII]	ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements
[XIV]	ISO/IEC 29115:2013 Information technology - Security techniques - Entity authentication assurance framework
[XV]	Regolamento UE n.1502/2015 della Commissione dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
[XVI]	ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

Tabella 0 - Riferimenti Normativi

1. Introduzione

1.1 Scopo del documento e campo di applicazione

Il presente manuale operativo ha lo scopo di illustrare e definire le modalità operative adottate da Namirial 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 dal DPCM 24 ottobre 2014, Namirial S.p.A., come struttura di certificazione digitale, pubblica il presente Manuale Operativo in modo da permettere ad ogni singolo utente di valutare il grado di affidabilità del servizio offerto.
Si prega di leggere l'intero testo del Manuale Operativo 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 testo si raccomanda la consultazione dell'elenco di acronimi e abbreviazioni elencati al §1.2
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. Ulteriori informazioni sono disponibili anche presso il sito internet di Namirial S.p.A. http://www.namirialtsp.com/spid oppure è possibile contattare il servizio clienti all'indirizzo e-mail: supportospid@namirial.com.
Questo Manuale Operativo è parte integrante del documento Trust Services Practice Statement che descrive le procedure operative per i servizi qualificati come previsto dal regolamento eIDAS (electronic IDentification Authentication and Signature) UE n° 910/2014 sull'Identità Digitale.
In caso di conflitto tra le dichiarazioni contenute nei documenti in lingua inglese ed il presente documento, la versione originale in lingua inglese prevarrà.

1.2 Definizioni ed acronimi usati all'interno del documento

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

TERMINE	SIGNIFICATO
AA	Attribute Authority.
Adesione	È il recepimento del framework SPID da parte di entità di certificazione o di fornitori di servizi in rete.
Agenzia (anche AgID)	Agenzia per l'Italia Digitale (anche Autorità di Accreditamento e Vigilanza sui Gestori di Identità Digitali).
Analisi dei rischi	Processo di comprensione della natura del rischio e di determinazione del livello di rischio.
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.
Autenticazione multi-fattore	Autenticazione con almeno due fattori di autenticazione indipendenti (ISO-IEC 19790).
Autenticazione	Disposizione di garanzia sull'identità dell'entità (ISO-IEC 18014-2).
Autorizzazione	Processo volto all'accertamento che l'informazione sia accessibile esclusivamente da/a coloro che sono autorizzati all'accesso.
CA	Certification Authority
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.
Criteri di rischio	Valori di riferimento rispetto ai quali è ponderato il rischio.

TERMINE	SIGNIFICATO
Dato Personale	Si intende “qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale” (art. 4, com. 1) del [III]).
Dati Particolari	Sono quei “dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona” (art. 9 .dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale” (art. 9, com. 1) [III]).
Dati giudiziari	Vedi Dati Particolari
Disponibilità	Processo volto all’accertamento che gli utenti autorizzati abbiano accesso all'informazione e alle attività associate quando richiesto.
Definizione del rischio	Processo di individuazione, riconoscimento e descrizione del rischio.
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.

TERMINE	SIGNIFICATO
Gestione del rischio	Attività coordinate per dirigere e controllare una organizzazione in merito al rischio o ai rischi esistenti.
Gestori dell'identità digitale	Le persone giuridiche accreditate allo SPID che, in qualità di gestori di servizio pubblico, previa identificazione certa dell'utente, assegnano, rendono disponibili e gestiscono gli attributi utilizzati dal medesimo utente al fine della sua identificazione informatica. Essi inoltre, forniscono i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica degli utenti.
Gestori di attributi qualificati	I soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.
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.
IS	International Standard.
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission.
Integrità	Salvaguardia dell'esattezza e della completezza dei dati e delle modalità di processo.
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector.
LoA	Level of Assurance.
NIST	National Institute of Standards and Technology.
RAO	Operatore o Incaricato del Gestore al riconoscimento del soggetto richiedente l'identità SPID.

TERMINE	SIGNIFICATO
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.
Ponderazione del rischio	Processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.
Riservatezza	Garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate.
SAML	Security Assertion Markup Language.
SSL	Secure Socket Layer.
SP	Service provider – vedi Fornitore Servizi.
SPID	Il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98.
TCP	Transmission Control Protocol.
Titolare	È il soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale SPID, corrisponde all'utente del DPCM art. 1 comma 1 lettera v).
Trattamento del rischio.	Processi di selezione e implementazione di attività volte a diminuire o comunque modificare il rischio presente.
User Agent	Sistema utilizzato dall'utente per l'accesso ai servizi (di solito il browser per la navigazione in rete);
Valutazione del rischio	Processo complessivo di identificazione, analisi e ponderazione del rischio.

Tabella 1 - Definizioni ed Acronimi

1.3 Tabella di corrispondenza

La seguente tabella incrocia i temi previsti dal Regolamento di cui al [IX] (si veda il Par. 2, lettera p) dell'Allegato) con le corrispondenti sezioni del presente documento:

Regolamento	Manuale Operativo
1 dati identificativi del gestore	§2
2 dati identificativi della versione del manuale	§2.2
3 responsabile del manuale operativo	§2.3

Regolamento		Manuale Operativo
4	descrizione delle architetture, applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche	§7
5	descrizione delle architetture dei sistemi di autenticazione e delle credenziali	§10
6	descrizione dei codici e dei formati dei messaggi di anomalia sia relativi ai protocolli che ai dispositivi di autenticazione utilizzati	§11
7	livelli di servizio garantiti per le diverse fasi della registrazione e della gestione del ciclo di vita delle identità	§5.1, 5.2
8	livelli di servizio garantiti per le diverse fasi del processo di autenticazione	§5.1
9	descrizione dei contenuti delle tracciature degli accessi al servizio di autenticazione e delle modalità di acquisizione ai fini dell'opponibilità a terzi	§12
10	guida utente del servizio in cui devono essere particolarmente curate le modalità d'uso del sistema di autenticazione, le modalità con cui l'utente può richiedere la sospensione o la revoca delle credenziali, le cautele che l'utente deve adottare per la conservazione e protezione delle credenziali. La guida utente può costituire documento a sé stante	§10
11	descrizione dei processi e delle procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali	§8.4
12	descrizione dei metodi di gestione dei rapporti con gli utenti	§2.4
13	descrizione generale delle misure anticontraffazione	§6
14	descrizione generale del sistema di monitoraggio	§13
15	definizione degli obblighi del gestore e dei titolari dell'identità digitale	§3
16	indirizzo (o indirizzi) del sito web del gestore ove è resa direttamente disponibile la descrizione del servizio in lingua italiana e lingua inglese	§2.2
17	descrizione delle modalità disponibili agli utenti per richiedere la revoca e sospensione dell'identità digitale	§9

Tabella 2 - Corrispondenza tra Regolamento e Manuale Operativo

1.4 Tabella riepilogativa delle tipologie SPID

Di seguito sono rappresentate due tabelle che riassumono le modalità in cui SPID può essere erogata.

Livelli di sicurezza	Caratteristiche
Livello 1 (corrispondente al LoA2 dell'ISO-IEC 29115)	è caratterizzato da un'affidabilità e una qualità delle specifiche tecniche, norme e procedure dello strumento di identificazione elettronica tali da ridurre il rischio di uso abusivo o di alterazione di identità. 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	è caratterizzato da un'affidabilità e una qualità delle specifiche tecniche, norme e procedure dello strumento di identificazione elettronica tali da ridurre significativamente il rischio di uso abusivo o di alterazione di identità. A tale livello è associato un rischio notevole 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)	è caratterizzato da un'affidabilità e una qualità delle specifiche tecniche, norme e procedure dello strumento di identificazione elettronica il cui scopo è quello di impedire l'uso abusivo o l'alterazione dell'identità e garantisce con un altissimo grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio altissimo e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell' Allegato II del Regolamento 910/2014; 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.

Tabella 3 – Livelli di sicurezza SPID

Tipologia identità	Caratteristiche
1. della persona fisica (SPID 1)	veicola solo i dati della persona fisica; l'utilizzo di questa tipologia SPID è finalizzato alla fruizione di servizi non professionali destinati ai cittadini.
2. della persona giuridica (SPID 2)	veicola solo i dati afferenti alla persona giuridica; l'utilizzo di questa tipologia SPID è finalizzato alla fruizione di servizi professionali per i quali è necessario conoscere solo gli attributi della persona giuridica.
3 uso professionale della persona fisica (SPID 3)	veicola solo i dati della persona fisica; l'utilizzo di questa tipologia SPID è finalizzato alla fruizione di servizi professionali per i quali è necessario conoscere solo gli attributi della persona fisica che può essere o non essere dotati di una partita IVA personale.
4 uso professionale per la persona giuridica (SPID 4)	veicola solo i dati della persona fisica e della persona giuridica; l'utilizzo di questa tipologia SPID è finalizzato alla fruizione di Servizi professionali per i quali è necessario conoscere sia gli attributi della persona fisica sia gli attributi della persona giuridica per la quale la persona fisica opera.

Tabella 4 – Tipologie identità SPID

2. Dati identificativi del gestore (1)

Ragione Sociale:	Namirial S.p.A.
Sede Legale:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Sede di erogazione del servizio:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Partita IVA:	IT02046570426
Iscrizione registro delle imprese:	Ancona
REA:	02046570426
Capitale Sociale:	7.762.625,20 € I.V.
Sito web del servizio:	http://www.namirialtsp.com/spid
URL della Portale rivolto al Titolare:	https://portal.namirialtsp.com/
Sito web del gestore:	http://www.namirialtsp.com/spid
E-mail PEC del servizio :	namirial.id@sicurezzapostale.it
E-mail del gestore:	supportospid@namirial.com

Tabella 5 - Dati identificativi del Gestore

2.1 Descrizione e certificazioni del gestore

Namirial S.p.A. è una società di informatica e web engineering che ha trovato una propria specifica collocazione all'interno dell'Information Technology orientando la propria produzione di software verso le nuove e sempre più manifeste esigenze di adeguamento del sistema produttivo italiano ai nuovi scenari economici fortemente competitivi e globalizzati. All'interno di una struttura economica nazionale caratterizzata per la gran parte dall'attività di piccole e medie realtà imprenditoriali si è ritenuto essenziale sviluppare soluzioni e servizi software accessibili anche sulla rete internet ed in grado di rispondere alle problematiche tecnologico-innovative emergenti in maniera professionale mantenendo una grande economicità di esercizio. La società ha sede in una moderna struttura di oltre duemila metri quadrati, dove è operativo un Internet Data Center dotato di tutti i sistemi di sicurezza necessari all'inviolabilità della struttura ed in grado di supportare gli utenti anche per quanto concerne eventuali necessità di hosting, housing e in genere di server farm.

Namirial S.p.A. è:

eIDAS Qualified Trust Service Provider (Certificato N. IT269191)

Per i servizi di:

- emissione, verifica e validazione di marche temporali qualificate

- autorità di certificazione per l'emissione di certificati di firma elettronica qualificata e sigilli elettronici qualificati

secondo gli standard

- **ETSI EN 401**
- **ETSI EN 411 parti 1 e 2**
- **ETSI EN 421**
- **ETSI EN 422**
- **ETSI EN 319 412 per quanto applicabile.**

Gestore di PEC, dal 26/02/2007, accreditato presso AgID (ex DigitPA) ed autorizzato alla gestione di **caselle** e **domini** di Posta Elettronica Certificata.

Identity Provider accreditato presso AgID per l'erogazione di credenziali **SPID**

strongdox	**Soggetto Conservatore**, in conformità a: • Regole Tecniche ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale; • Regolamento (UE) 910/2014 eIDAS, art. 24; per la prestazione di servizi fiduciari di Conservazione a Norma.
ISO 9001 BUREAU VERITAS Certification N. 223776	**Certificata UNI EN ISO 9001.** Namirial ha conseguito il certificato n. 223776 rilasciato da **Bureau Veritas Italia S.p.A.**
ISO 27001 BUREAU VERITAS Certification	**Certificata ISO/IEC 27001.** Namirial ha conseguito il certificato n. IT280490 rilasciato da **Bureau Veritas Italia S.p.A.**
Approved Trust List MEMBER	**Certificata da Adobe**. Da giugno 2013 Namirial è **membro dell'AATL** (Adobe Approved Trust List).

Tabella 6 - Certificazioni dei Gestore

Namirial può inoltre vantare le acquisizioni strategiche di Netheos, azienda leader nel mercato francese specializzato in soluzioni per l'identificazione e l'onboarding digitale e di Evicertia, QTSP spagnolo affermato nella penisola iberica e in America Latina.
Entrambe le acquisizioni rafforzano il portafoglio di Namirial, così come la sua presenza sul mercato internazionale, determinando inoltre un ampliamento ed un improvement delle competenze dell'Azienda.

2.2 Versione e pubblicazione del manuale operativo (2, 16)

Il presente Manuale Operativo è di proprietà di Namirial S.p.A. e tutti i diritti sono ad essa riservati. La versione di questo documento è riportata nel frontespizio e in ogni pagina ed è individuato da codice interno NAM-MO-SPID. Il documento è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità. Questo documento è pubblicato, in pdf firmato digitalmente, sulle pagine principali del sito informativo del Gestore indicato all'interno del §2.4.
Il Gestore esegue, almeno una volta all'anno, un controllo di conformità del processo di erogazione del servizio SPID e, ove necessario, aggiorna questo documento anche in considerazione dell'evoluzione della normativa e standard tecnologici.

2.3 Responsabile del Manuale Operativo (3)

La responsabilità del presente Manuale Operativo è del Gestore, nella figura del "Responsabile delle attività di verifica dell'identità del soggetto richiedente e della gestione e conduzione del servizio" (art. 2 punto 7 del Regolamento di cui al [IX]) il quale ne cura la revisione, la pubblicazione e l'aggiornamento. Le comunicazioni riguardanti il presente documento possono esse re inviate all'attenzione del suddetto responsabile contattabile mediante i seguenti recapiti:

Namirial S.p.A.
via Caduti sul Lavoro, 4
60019 Senigallia (AN)
E-mail: namirial.id@namirialtsp.com
Telefono: (+39) 071 63494
Fax: (+39) 071 60910

2.4 Rapporti con gli utenti (12)

Per ottenere informazioni sul servizio, anche di carattere commerciale, e per ricevere assistenza in caso di malfunzionamenti è possibile mettersi in contatto con il Gestore via telefono, via e-mail o via web ai seguenti recapiti:

- Richiesta informazioni sul servizio o commerciali: tel 071-63494.
  Dalle 9.00 alle 13.00 e dalle 15.00 alle 19.00, dal lunedì al venerdì;
- Richieste di assistenza o supporto: supportospid@namirial.com;
- e-mail: supportospid@namirial.com (per l'assistenza tecnica);
- e-mail: commercialespid@namirial.com (per informazioni di natura commerciale);
  web: www.namirialtsp.com/spid;

ll Gestore Namirial S.p.A. ha predisposto uno specifico canale di comunicazione con l'utenza finale, circa la gestione di problematiche relative al servizio SPID. L'Help Desk risponde ai numeri sopra indicati. Le richieste effettuate tramite posta elettronica o attraverso il portale, se pervenute fuori dall'orario lavorativo o nei giorni festivi, sono prese in carico a partire dal primo giorno lavorativo successivo.

Gli operatori dell'HD sono formati, e regolarmente aggiornati, in modo da fornire risposte complete ed esatte a fronte delle richieste di informazioni che possono provenire dagli utenti.
Il cliente può anche segnalare eventuali problemi riscontrati durante l'uso della propria identità digitale. Le segnalazioni pervenute tramite portale sono gestite attraverso un sistema di trouble ticketing che segnala, via e-mail, ogni aggiornamento fino alla risoluzione definitiva.
Il servizio di Assistenza Namirial ha l'obiettivo di accogliere tempestivamente le richieste di supporto e di gestire la risoluzione del problema entro il termine massimo previsto.
Nel caso in cui sia il Gestore a dover comunicare con i propri utenti, vengono utilizzati gli attributi secondari previsti dall'Art. 1 comma d) del DPCM [II] e descritti al §1.2.
In aggiunta ai canali sopraindicati, qualora il Gestore debba propagare con urgenza informazioni di carattere generale applicabili al servizio SPID, quali ad esempio eventuali modifiche alla definizione del servizio e/o ai termini, alle condizioni e all'informativa sulla privacy, vengono utilizzati appositi pop-up attivati nel sito istituzionale del Gestore e nelle pagine di autenticazione.
Il gestore dell'identità digitale, ai sensi del Regolamento [VIII], su richiesta dell'utente, segnala via e-mail alla casella di posta indicata dall'utente, ogni avvenuto utilizzo delle credenziali di accesso, inviandone gli estremi di utilizzo della credenziale (data, ora, fornitore del servizio).

2.4.1 Trouble ticketing

Attraverso il sistema di trouble ticketing, Namirial S.p.A. tiene traccia di tutte le segnalazioni effettuate dai propri clienti. Il sistema è basato su un'applicazione web-based attraverso la quale il personale Help Desk è in grado di:

- creare un nuovo ticket a seguito di una segnalazione da parte del cliente
- seguire la "vita" del ticket nel corso degli aggiornamenti e cambi di stato fino alla risoluzione finale
- aggiornare il ticket annotando gli interventi fatti e le comunicazioni con il cliente
- ricercare i ticket in base ad una serie di informazioni quali la data di creazione, la categoria, l'identificativo dell'operatore che segue la segnalazione, etc.

Tutte le modifiche di stato significative vengono comunicate all'utente che ha effettuato la segnalazione attraverso un messaggio di posta elettronica.

3. Definizione degli obblighi del gestore e dei titolari dell'Identità Digitale [15]

Sulla base della normativa vigente, sono di seguito riassunti:

- gli obblighi che il Titolare dell'identità digitale SPID assume in relazione alla richiesta e all'utilizzo dell'Identità Digitale rilasciata dal Gestore, con indicazione dei rispettivi riferimenti normativi;
- gli obblighi che Namirial S.p.A., nel ruolo di Gestore delle Identità Digitali SPID, assume in relazione alla propria attività;
- gli obblighi che il fornitore di servizi (SP) assume in relazione alla propria attività.

Nella documentazione contrattuale del servizio che il Gestore sottoporrà all'Utente nell'ambito delle operazioni necessarie per il rilascio dell'Identità Digitale, sono indicati gli ulteriori elementi di natura contrattuale derivanti dal rapporto di erogazione del servizio. La documentazione contrattuale, unitamente alle sue successive versioni, sarà resa disponibile nel sito internet http://www.namirialtsp.com/spid

3.1 Obblighi del titolare dell'Identità Digitale

Il Titolare di una Identità Digitale è obbligato a:

- esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione;
- usare esclusivamente e personalmente le credenziali connesse all'Identità Digitale;
- 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;
- non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine;
- garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi;
- l'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private;
- sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite;

- fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci;
- accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze;
- informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati;
- mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi:
    - se persona fisica: estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale;
    - se persona giuridica: indirizzo sede legale, codice fiscale o P.IVA, rappresentante legale della società, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale;
- conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i rischi seguenti:
    - divulgazione, rivelazione e manomissione;
    - furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale;
    - accertarsi dell'autenticità del fornitore di servizi o del gestore dell'identità digitale quando viene richiesto di utilizzare l'identità digitale;
- attenersi alle indicazioni fornite dal Gestore in merito all’uso del sistema di autenticazione, alla richiesta di sospensione e/o revoca delle credenziali, alle cautele da adottare per la conservazione e protezione delle credenziali;
- in caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all’autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali;
- in caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali.

3.2 Obblighi del Gestore dell’Identità Digitale

Il Gestore delle Identità Digitali è obbligato a:

- rilasciare l'identità digitale su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta;
- verificare l'identità del soggetto richiedente prima del rilascio dell’Identità Digitale;
- conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione “de-visu”;

- conservare copia del log della transazione nei casi di identificazione tramite documenti digitali di identità, identificazione informatica tramite altra identità digitale SPID o altra identificazione informatica autorizzata;
- conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso si identificazione tramite firma digitale;
- verifica degli attributi identificativi del richiedente;
- consegnare in modalità sicura le credenziali di accesso all'utente;
- conservare la documentazione inerente al processo di adesione per un periodo pari a 20 (venti) anni decorrenti dalla scadenza o dalla revoca dell'identità digitale;
- cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale;
- trattare e conservare i dati nel rispetto del Regolamento (UE) 2016/679 in materia di protezione dei dati personali;
- verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione;
- effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione e/o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso;
- revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 (ventiquattro) mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica;
- segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente;
- verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata);
- fornire all'utente che l'ha inviata, una conferma della ricezione della richiesta di sospensione;
- sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni ed informarne il richiedente;
- rispristinare o revocare l'identità digitale sospesa, nei casi previsti;
- revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione;
- utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale;
- adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso;
- effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta;
- effettuare con cadenza almeno annuale un'analisi dei rischi;
- definire, aggiornare e trasmettere ad AgID il piano per la sicurezza dei servizi SPID;

- allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato;
- condurre con cadenza almeno semestrale il Penetration Test;
- garantire la continuità operativa dei servizi afferenti allo SPID;
- effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna;
- garantire la gestione sicura delle componenti riservate delle identità digitali assicurando non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata;
- garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa;
- sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti;
- informare tempestivamente l'AgID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali;
- adeguare i propri sistemi a seguito dell'aggiornamento della normativa;
- inviare all'AgID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici;
- in caso intendesse cessare la propria attività, comunicarlo all'AGID e ai Titolari delle Identità Digitali almeno 30 (trenta) giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali rilasciate;
- in caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e ne conserva le informazioni;
- in caso di cessazione dell'attività, scaduti i 30 (trenta) giorni, revocare le identità digitali rilasciate e per le quali non si è avuto subentro;
- informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi;
- se richiesto dall'utente, segnalargli via e-mail o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso;
- notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale;
- nel caso l'identità digitale risulti non attiva per un periodo superiore a 24 (ventiquattro) mesi o il contratto sia scaduto, revocarla e informarne l'utente via posta elettronica e numero di telefono mobile;
- in caso di decesso del titolare (persona fisica) o di estinzione della persona giuridica, revocare previo accertamento l'identità digitale;
- nel caso in cui 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;

- trascorsi 30 (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;
- 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;
- ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 (trenta) giorni dalla sospensione una richiesta di revoca da parte dell'utente;
- in caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 (venti) anni dalla revoca dell'identità digitale.
- proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa;
- all'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta;
- in caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita;
- non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID;
- tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, adottando idonee misure di sicurezza ed utilizzando meccanismi di cifratura.

3.3 Obblighi dei fornitori di servizi

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

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

3.4 Obblighi della Registration Authority (RA)

La LRA è tenuta a:

- informare il Titolare in modo compiuto e chiaro, sulla procedura di rilascio SPID e sui necessari requisiti per accedervi, sulle caratteristiche, sulle precauzioni e sulle limitazioni d'uso delle identità emesse sulla base del servizio SPID;
- informare il Titolare riguardo agli obblighi da quest'ultimo assunti in merito a conservare con la massima diligenza, le credenziali (password, dispositivi otp, anche software) associate all'identità, al fine di garantirne l'integrità e la massima riservatezza;
- informare il Titolare riguardo agli obblighi da quest'ultimo assunti in merito a conservare con la massima diligenza la credenziale OTP eventualmente fornita;
- informare il titolare delle misure di sicurezza adottate per il trattamento dei dati personali;
- provvedere con certezza all'identificazione della persona che fa richiesta dell'identità SPID mediante l'utilizzo dell'APP IdCheck qualora l'identificazione avvenga de visu salvo casi particolari descritti al §8.3.1.2;
- verificare che i documenti presentati per l'identificazione non siano contraffatti;
- accertare l'autenticità della richiesta di adesione al servizio SPID;
- comunicare al Gestore tutti i dati e documenti acquisiti durante l'identificazione del Titolare e previsti dalle procedure al fine di avviare tempestivamente le attività di emissione dell'identità digitale;
- attenersi scrupolosamente alle regole impartite dal Gestore e presenti su questo documento;
- verificare ed accertarsi che l'utente abbia preso visione e compreso le regole per l'uso del sistema SPID.

I RAO sono autorizzati ad operare dal Gestore a seguito di adeguata formazione del personale addetto. Il Gestore, salvo diritto di rivalsa, resta comunque l'unico ed il solo responsabile verso terzi dell'attività svolta dall'LRA.
Il Gestore verifica periodicamente la rispondenza delle procedure adottate dalla LRA e dai suoi RAO e quanto indicato nel presente documento. In ogni caso, a semplice richiesta del Gestore, la LRA è tenuta a trasmettere allo stesso tutta la documentazione in proprio possesso, relativa a ciascuna richiesta di emissione dell'identità digitale proveniente da ciascun Titolare.

3.5 Responsabilità e limitazioni agli indennizzi

3.5.1 Limitazioni di responsabilità del Gestore

Il Gestore è responsabile, verso i Titolari, per l'adempimento degli obblighi di legge derivanti dalle attività previste dal [I], [II], [III], [IV], [V], [VI], [VII], e successive modifiche ed integrazioni.
Il Gestore, ove previsto, mette a disposizione del Titolare l'identità SPID associandola alle credenziali descritte in §10.

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

- attribuisce l'Identità Digitale e rilascia le credenziali connesse attenendosi alle Regole Tecniche emanate dall'AGID;
- si attiene alle misure di sicurezza previste dal Regolamento (UE) 2016/679 in materia di protezione dei dati personali nonché alle indicazioni fornite nell'informativa pubblicata sul sito https://docs.namirialtsp.com/documents/Informativa-privacy.pdf;
- procede alla sospensione e/o revoca delle credenziali in caso di richiesta avanzata dall'utente per perdita del possesso o compromissione della segretezza, per provvedimento dell'AgID o su propria iniziativa per acquisizione della conoscenza di cause limitative della capacità dell'utente, per sospetti di abusi o falsificazioni.

Il Gestore non si assume la responsabilità:

- per l'uso improprio delle Credenziali e in generale dell'Identità Digitale. Il Titolare in particolare prende atto e accetta che Namirial S.p.A. non risponderà di qualsivoglia uso abusivo, lesivo o comunque improprio della Identità Digitale;
- per le conseguenze derivanti dalla non conoscenza o dal mancato rispetto, da parte del Titolare, delle procedure e delle modalità operative indicate nel presente documento;
- per il mancato adempimento degli obblighi previsti a suo carico dovuto a cause ad esso non imputabili;
- per la mancata o non corretta esecuzione degli obblighi su di esso incombenti in caso di impossibilità, anche parziale, di erogare il Servizio oppure al verificarsi di qualsivoglia causa di forza maggiore nei limiti dei Livelli di Servizio garantiti dal Gestore (§5), ivi incluse calamità naturali, eventi bellici, furti, interventi dell'autorità, caso fortuito e in tutti gli altri casi in cui il mancato o non corretto adempimento sia comunque dovuto a cause a lei non direttamente imputabili;
- circa il corretto funzionamento e la sicurezza dei dispositivi, hardware e software, utilizzati dal Titolare, sul regolare funzionamento di linee elettriche, telefoniche nazionali e/o internazionali o altri fattori esterni alla propria organizzazione che possano limitare la fruizione del Servizio;
- del funzionamento del Servizio al di fuori di quanto imposto dalla legge al gestore dell'identità digitale ed in particolare al rapporto tra il Titolare medesimo ed il Fornitore di servizi, essendo detto rapporto disciplinato esclusivamente dalle relative condizioni contrattuali adottate in assoluta autonomia dal Fornitore di servizi medesimo.

3.5.2 Limitazioni e indennizzi

In riferimento ai regolamenti emanati ai sensi dell'art. 4, comma 3 del [II], il Gestore ha stipulato polizza assicurativa per la copertura dei rischi dell'attività e dei danni a tutte le parti (Titolari, Destinatari e Terze Parti) non superiore ai massimali espressamente indicati nei regolamenti stessi.

4. Modalità di protezione dei dati personali

Di seguito vengono descritti i processi e le modalità operative adottate da Namirial S.p.A., in qualità di titolare del trattamento dei dati personali, nello svolgimento della propria attività. Le informazioni personali dei titolari delle identità digitali e, più in generale dei clienti del servizio erogato, vengono trattate, conservate e protette in conformità a quanto previsto nel Regolamento (UE) 2016/679 in materia di protezione dei dati personali.

4.1 Struttura organizzativa di Namirial S.p.A. in materia di trattamento dei dati personali

Namirial S.p.A. è il **Titolare del trattamento dei dati personali**, secondo quanto previsto dal Regolamento (UE) 2016/679 in materia di protezione dei dati personali.
Namirial S.p.A. individua e nomina gli incaricati al trattamento che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni dagli stessi impartite.

4.2 Tutela e diritti degli interessati

Namirial S.p.A. garantisce la tutela degli interessati, in ottemperanza al Regolamento (UE) 2016/679 in materia di protezione dei dati personali. In particolare, fornisce agli interessati tutte le informazioni necessarie, in relazione al diritto di accesso ai dati personali ed agli usi degli stessi, consentiti dalla legge.
L'accesso ai propri dati da parte degli interessati è consentito tramite richiesta scritta utilizzando l'apposita forma disponibile al seguente link: https://support.namirial.com/it/contatta-il-dpo/.
In alternativa è possibile inviare la richiesta al responsabile per la protezione dei dati anche tramite e-mail ordinaria all'indirizzo dpo@namirial.com o tramite PEC all'indirizzo dpo.namirial@sicurezzapostale.it. Le richieste vengono evase senza ingiustificato ritardo.
Gli interessati devono prestare consenso scritto al trattamento dei propri dati da parte di Namirial S.p.A.

4.3 Modalità del trattamento

Tutte le informazioni personali raccolte durante le fasi di erogazione dell'Identità Digitale vengono trattate da Namirial S.p.A. con tutte le misure di sicurezza descritte all'interno del presente manuale allo scopo di prevenirne la perdita, evitarne usi illeciti o accessi da parte di personale non espressamente autorizzato.

I dati in formato elettronico vengono conservati come da normativa vigente. Namirial S.p.A. si riserva l'opportunità di conservare i dati cartacei presso la propria sede centrale, all'interno di archivi cartacei cui hanno accesso solo gli incaricati espressamente autorizzati.

4.4 Finalità del trattamento

I dati personali vengono raccolti per le seguenti finalità:

- Erogazione del servizio: richieste di adesione a SPID, attribuzione identità digitale rilascio e gestione della stessa. I dati raccolti saranno utilizzati per l'iscrizione del richiedente, nonché per l'emissione, la sospensione, la revoca e la gestione delle identità digitali. Il Gestore, inoltre, utilizza le informazioni esclusivamente per l'erogazione del servizio di gestore dell'identità digitale e di ogni altra attività connessa e derivante da tale servizio quale, a mero titolo esemplificativo, la gestione della fatturazione. Eventuali controlli sulla qualità dei servizi e di sicurezza del sistema senza procedere, in alcun modo, alla sua profilazione.
- Solo nel caso in cui l'interessato fornisca esplicito consenso al trattamento, i dati personali possono essere utilizzati per scopi di natura commerciale. Il Gestore potrà utilizzare i riferimenti raccolti come attributi secondari al momento dell'adesione a SPID e della sottoscrizione del contratto per inviare comunicazioni relative a prodotti e/o servizi analoghi a quelli acquistati.

I dati raccolti non verranno in alcun modo utilizzati per attività di profiling da parte di Namirial S.p.A. e non verranno venduti o forniti a terze parti per usi commerciali o di marketing o per statistiche ed indagini di mercato.

I dati personali vengono acquisiti in osservanza alle finalità esplicitate nell'informativa fornita al richiedente durante le fasi di richiesta dell'identità digitale.
L'informativa è anche disponibile su: https://docs.namirialtsp.com/documents/Informativa-privacy.pdf
Di seguito sono elencate le finalità del trattamento:

- gestione del rapporto contrattuale;
- eventuali controlli sulla qualità del servizio e sulla sicurezza del sistema;
- attività di natura commerciale, effettuata tramite invio di informative legate alla emissione di prodotti e/o servizi analoghi o direttamente connessi ai servizi SPID.

L'interessato ha la possibilità di opporsi al trattamento dei dati personali, avente ad oggetto tale tipologia di comunicazioni.

4.5 Altre forme di utilizzo dei dati

I dati personali possono essere usati con finalità diverse rispetto alla fornitura dei servizi descritti dal presente manuale e possono essere comunicati a soggetti pubblici, quali forze dell'ordine, autorità pubbliche e autorità giudiziarie, qualora gli stessi soggetti ne facciano richiesta, per motivi di ordine pubblico e nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, la prevenzione, l'accertamento e/o la repressione dei reati.

4.6 Sicurezza dei dati

Come previsto dalla normativa vigente, Namirial S.p.A. adotta tutte le misure di sicurezza necessarie al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati;
- i rischi di danneggiamento risorse hardware su cui sono memorizzati i dati;
- i rischi di danneggiamento ai locali nei quali sono custoditi i dati;
- l'accesso non autorizzato ai dati;
- le modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Attraverso le misure di sicurezza adottate da Namirial S.p.A. (cfr §7.3) vengono garantite:

- l'integrità e la salvaguardia dei dati contro manomissioni o modifiche da parte di soggetti non autorizzati;
- la disponibilità dei dati e quindi la loro fruibilità;
- la riservatezza dei dati cioè la garanzia che le informazioni vengano accedute dalle sole persone autorizzate.

5. Livelli di servizio del gestore

Di seguito vengono descritti gli SLA (Service Level Agreement) che il Gestore Namirial garantisce a seguito di:

- fasi della registrazione del Titolare;
- ciclo di vita delle Identità Digitali;
- fasi del processo di autenticazione.

Ove non diversamente specificato, l'intervallo temporale di riferimento per il calcolo della disponibilità è il trimestre.

5.1 Livelli di servizio garantiti per le diverse fasi della registrazione, della gestione del ciclo di vita delle identità e dell'autenticazione(7-8)

Indicatore di qualità	Modalità funzionamento	Valore limite
Disponibilità del sottoservizio di registrazione identità	*Erogazione automatica*	>= 99,0%
		Singolo evento di indisponibilità < =6 ore
	Erogazione in presenza	>= 98,0%
Tempo di risposta del sottoservizio di registrazione identità		<= 12h (ore lavorative) per il 95% di richieste registrazione utente
Disponibilità del sottoservizio di gestione rilascio credenziali	*Erogazione automatica*	>= 99,5%
		Singolo evento di indisponibilità < =6 ore
	Erogazione in presenza	>= 98,0%
Tempo di rilascio credenziali	*Erogazione da remoto*	<= 5 giorni lavorativi
	Erogazione in presenza	<= 3 giorni lavorativi

Indicatore di qualità	Modalità funzionamento	Valore limite
Tempo riattivazione delle credenziali		<= 2 giorni lavorativi
Disponibilità del sottoservizio di sospensione e revoca delle credenziali		>= 99,5%
		Singolo evento di indisponibilità < =6 ore
Tempo di sospensione delle credenziali	*Erogazione automatica*	< =1 minuto
	Erogazione in presenza	< = 10 minuti
Tempo di revoca delle credenziali successiva alla sospensione		<= 5 giorni lavorativi
Disponibilità del sottoservizio di rinnovo e sostituzione delle credenziali	*Erogazione automatica*	>= 99,5% singolo evento di indisponibilità < = 6h
	Erogazione in presenza	>= 98,0%
Tempo di rinnovo e sostituzione delle credenziali		<= 2 giorni lavorativi
Disponibilità del sottoservizio di autenticazione		>= 99,5%
		Singolo evento di indisponibilità <= 6 ore
Tempo di risposta del sottoservizio di autenticazione		<= 2 sec per il 98% delle richieste di autenticazione
RPO sottoservizio registrazione e rilascio delle identità		1 ora
RTO sottoservizio registrazione e rilascio delle identità		8 ore
RPO sottoservizio di sospensione e revoca delle credenziali		1 ora
RTO sottoservizio di sospensione e revoca delle credenziali		8 ore
RPO sottoservizio di Autenticazione		1 ora

Indicatore di qualità	Modalità funzionamento	Valore limite
RTO sottoservizio di Autenticazione		8 ore

Tabella 7 - SLA per le fasi della registrazione del Titolare

5.2 Continuità operativa

Fase	Indice
Registrazione e rilascio Identità (o credenziale)	RPO 1h - RTO 8h
Revoca o sospensione Identità (o credenziale)	RPO 1h - RTO 8h
Autenticazione	RPO 1h - RTO 8h

Tabella 8 - Indici di continuità operativa

6. Misure anticontraffazione(13)

Le misure anti contraffazione predisposte dal Gestore mirano a prevenire il verificarsi del furto d'identità, inteso sia come impersonificazione totale (occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità di un altro soggetto in vita o deceduto) sia come impersonificazione parziale (occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto).
Tra le misure attuate dal Gestore, rientra la verifica dell'identità, che consiste nel rafforzamento del livello di attendibilità degli attributi, compiuta attraverso l'accesso alle fonti autoritative effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM.

6.1 Identificazione da parte di un RAO tramite APP IDCheck

L'identificazione è effettuata de visu da parte di un RAO, che procederà utilizzando l'app Namirial IDCheck, sviluppata secondo le linee guida OWASP[1]. L'applicazione è disponibile soltanto previa emissione di un voucher e solo ai RAO che hanno completato con successo il percorso formativo obbligatorio.
Durante tale processo, il RAO acquisisce il documento di riconoscimento e il codice fiscale, presente sulla tessera sanitaria, mediante l'app che effettua una lettura dei dati in essi contenuti sfruttando la tecnologia OCR. L'app vincola, inoltre, il Richiedente ad essere riconosciuto in presenza previa acquisizione di una fotografia, che viene scattata dal RAO. L'app effettua poi un face match tra tali acquisizioni e la fotografia presente all'interno del documento di riconoscimento, oltre a fornire un riscontro sulla liveness dell'utente.
Nel caso in cui l'esito del riconoscimento sia positivo, il RAO può procedere con l'emissione dell'identità. Diversamente, dovrà effettuare un nuovo riconoscimento.

6.2 Verifica dell'identità con riconoscimento a vista

I controlli eseguiti da Namirial si incardinano principalmente sull'utilizzo del sistema SCIPAFI, Sistema pubblico di prevenzione che consente il riscontro dei dati contenuti nei principali documenti d'identità e riconoscimento con quelli registrati nelle banche dati degli enti di riferimento. Il riscontro si configura quindi come efficace strumento di prevenzione per i furti d'identità sia totali che parziali. Nell'attesa che i gestori di identità digitale ottengano le autorizzazioni all'accesso alle fonti autoritative, l'IdP esegue una serie di controlli manuali

[1] La top 10 OWASP (Open Web Application Security Project) è un documento di linee guida di sviluppo sicuro in ambiente web.

accedendo ai sistemi pubblici esposti dagli Enti competenti. I controlli possono essere eseguiti dall'operatore di riconoscimento, ovvero da una LRA del Gestore Namirial S.p.A. Nelle more del pieno accesso al sistema SCIPAFI, le identità digitali rilasciate e verificate manualmente sono rese individuabili nel sistema dell'IdP, al fine di poter eseguire ulteriori riscontri in corso d'opera.

6.3 Verifica dell'identità con strumenti di identificazione informatica

Le misure anticontraffazione, qualora per l'identificazione vengano utilizzati strumenti di identificazione informatica, si poggiano anche sui seguenti elementi tecnologici:

- Sono utilizzati algoritmi crittografici robusti per garantire riservatezza e integrità dei dati, sulla base di quanto prescritto normativamente, in conformità con gli standard tecnologici internazionali;
- La firma qualificata, la CNS, TS/CNS e la CIE, ove utilizzate, devono superare i seguenti controlli:
    - Il certificato memorizzato all'interno del dispositivo sicuro deve essere stato emesso da un certificatore accreditato (firma qualificata) o dalla PA responsabile del circuito CNS (CNS, attributo OU), ovvero dalla PA responsabile del circuito CIE;
    - Il certificato deve essere in stato di validità (non scaduto, non revocato o sospeso);
    - Il certificato deve essere intestato allo stesso codice fiscale del richiedente;

L'identificazione mediante i dispositivi di firma o autenticazione sopradescritti eredita le garanzie di rilascio e sicurezza già in essere nei rispettivi circuiti di erogazione.
Per quanto riguarda le misure anticontraffazione offerte dalle credenziali fornite si rimanda al paragrafo §10.

7. Descrizione delle architetture, applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche[4]

In questa sezione sono descritte le architetture applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche. Inoltre, si descrivono anche le architetture dei sistemi di autenticazione delle credenziali che compongono il sistema di gestione delle identità digitali di Namirial S.p.A. Nell'immagine di seguito riportata è possibile individuare i principali attori e componenti dell'architettura SPID realizzata:

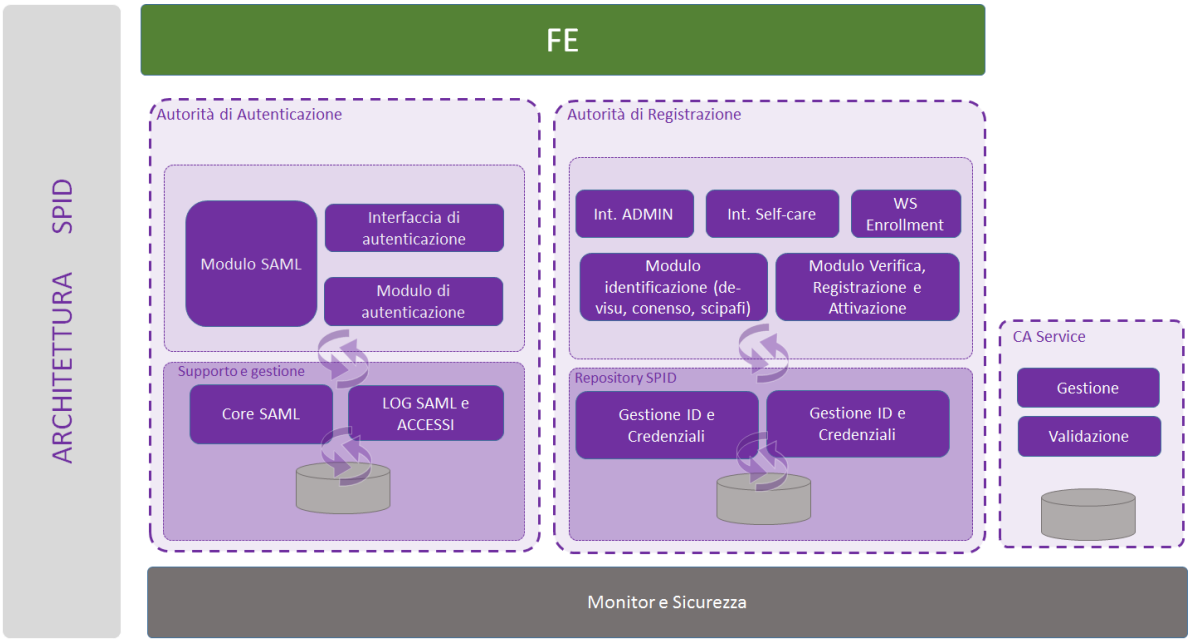


Figura 1 - Architettura applicativa SPID

Il Servizio di Gestione delle Identità digitali può essere logicamente suddiviso in due componenti di Front-End/Interfaccia:

- **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;
- **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:

- Repository SPID;
- Modulo di supporto, gestione e operatività del servizio;
- Modulo monitoring e sicurezza;
- Modulo servizi di certificazione e autenticazione (CA).

Il componente primario 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, i moduli di richiesta sottoscritti, etc. etc.
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 il modulo di identificazione che si occupa del riconoscimento del soggetto richiedente ed al modulo di attivazione che effettua la registrazione delle informazioni e la creazione vera e propria dell'identità SPID. 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 identificazione de-visu con procedura remota.
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 sottoporle al servizio di Conservazione Sostitutiva. Sono infine presenti alcuni moduli che si occupano del monitor delle attività e della sicurezza dei componenti.

7.1 Architettura di dispiegamento

L'architettura di dispiegamento è descritta all'interno del Piano della Sicurezza, documento riservato a disposizione dell'AgID.

7.2 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.

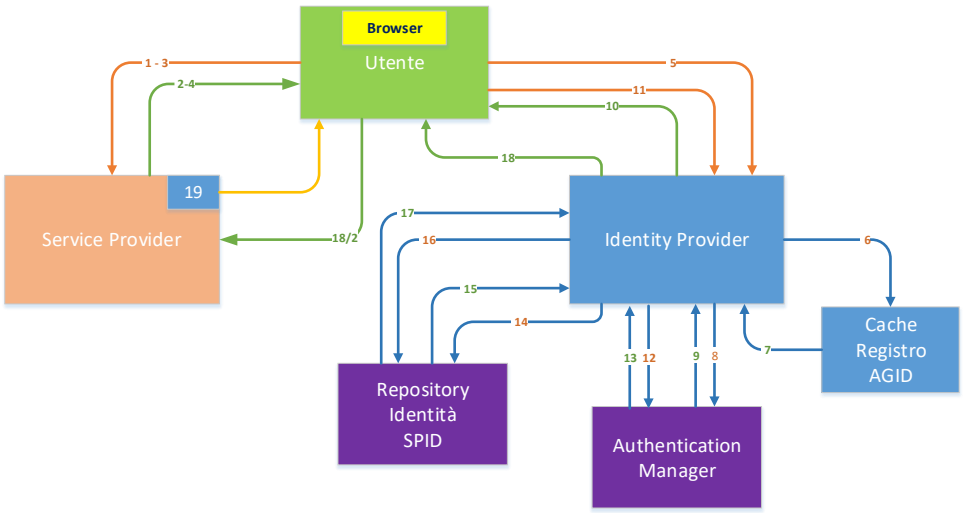


Figura 2 - Architettura dei sistemi di autenticazione

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 (AuthnRequest) 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.
17. L'Identity Provider sottopone all'utente una pagina Web nella quale sono mostrati gli attributi richiesti dal Service Provider e quelli che gli verranno inviati.
18. L'utente fornisce esplicito consenso per l'invio dei dati.
19. 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 almeno su queste componenti:

- interfaccia di autenticazione del portale dell'IDP;
- modulo di autenticazione;
- supporto alla verifica dei SP (cache registro AGiD).

7.3 Interfaccia di autenticazione del portale dell'IDP

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

7.4 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 che verifica:

- la validità dell'identità SPID, controllando che l'identità SPID sia attiva (non sospesa o revocata);
- la validità delle credenziali, con l'ausilio del modulo di Gestione Credenziali.

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

7.5 Supporto alla verifica dei Service Provider (cache AgID)

Il modulo di autenticazione recupera le informazioni da una cache che è replica dell'indice SPID gestito da AGID. Le informazioni recuperate sono ad esempio i servizi erogati in modalità SPID, i service provider, ecc.

8. Descrizione dei processi e delle procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali(11)

Questa sezione descrive le modalità con le quali il Gestore svolge la verifica, il rilascio, e la gestione delle identità digitali, in particolare come opera il personale addetto al servizio, quali sono le modalità di adesione a SPID e come richiedere l'identità digitale, le procedure di identificazione del soggetto richiedente l'identità digitale e le modalità di comunicazione con esso.

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

Il personale addetto alla gestione del servizio SPID è dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore e della dimestichezza con procedure di sicurezza appropriate che consentono di garantire il rispetto delle norme.
Gli operatori addetti alla gestione delle identità digitali, nel rispetto del regolamento di cui all'Art 4, com 3, del DPCM, sono i seguenti:

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.

8.2 Richiesta dell'identità digitale

Namirial 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. La richiesta può essere effettuata online o de visu.

8.2.1 Richiesta de visu dell'identità digitale

8.2.1.1 Modalità 1 – LRA

La richiesta dell'identità SPID viene effettuata dal Richiedente presso una LRA. In questa modalità è prevista la presenza fisica del richiedente dinnanzi ad un RAO.
Le LRA possono operare successivamente alla stipula di un contratto con il Gestore Namirial S.p.A. in cui la terza parte indica uno o più RAO deputati alle attività di identificazione, riconoscimento e registrazione.
L'autorizzazione e successivamente la qualificazione dei RAO ad effettuare le operazioni di identificazione, registrazione e rilascio, avviene mediante corso di formazione e superamento di un test. A seguito della firma di un contratto tra la terza parte ed il Gestore, nonché previa qualificazione dei RAO, l'IdP rende disponibili ai RAO gli strumenti per consentire lo svolgimento delle attività di identificazione (tra cui l'APP IdCheck), riconoscimento e registrazione. I privilegi di accesso a tali strumenti e l'operato dei RAO sono sotto il costante controllo del Gestore.

8.2.1.2 Modalità 2 – IR

La richiesta dell'identità SPID viene effettuata dal richiedente presso un soggetto incaricato dal Gestore o dalla LRA denominato Incaricato alla Registrazione (IR). In questa modalità è prevista la presenza fisica del soggetto Titolare dinnanzi all'Incaricato. Tali soggetti (IR) possono operare successivamente alla stipula di un contratto con Namirial S.p.A. in cui la società terza indica uno o più operatori, che saranno individuati come Incaricati alla Registrazione (IR) e che dovranno effettuare le attività di registrazione come indicate dal Gestore.

8.2.1.3 Documentazione necessaria

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:

- i dati identificativi del richiedente, che costituiscono gli attributi identificativi dell'identità digitale;
- informazioni che consentono di gestire in maniera efficace il rapporto tra il gestore delle identità digitali ed il richiedente l'identità digitale, che costituiscono gli attributi secondari dell'identità digitale (e-mail, cellulare);

Per le **persone fisiche** sono considerate obbligatorie le seguenti informazioni:

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

Per le **persone giuridiche** sono considerate obbligatorie le seguenti informazioni:

a. denominazione/ragione sociale;
b. codice fiscale o P.IVA (se uguale al codice fiscale);
c. sede legale;
d. certificazione con indicazione amministratori e/o rappresentante legale (in alternativa atto notarile di procura legale) e data di rilascio e validità dello stesso;
e. estremi del documento di identità utilizzato dal rappresentante legale o del delegato a richiede l'identità digitale in nome e per conto della persona giuridica;
f. 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 dal Gestore Namirial S.p.A., inviando un'e-mail all'indirizzo di posta elettronica dichiarato, con un codice da riportare al Gestore per la verifica e certificazione e un SMS di verifica al numero di cellulare veicolante un codice numerico di controllo che deve essere riportato all'IdP come risposta.

In aggiunta la procedura dell'operatore prevede che questi si assicuri che il richiedente abbia preso contezza e che approvi le condizioni generali del servizio SPID contenute (o riferite) nel modulo di adesione e recanti:

- informativa sul trattamento dei dati sul quale il richiedente fornisce esplicito assenso;
- indicazione di esplicita consapevolezza sulle responsabilità penali e civili di coloro che rendono dichiarazioni mendaci (art. 76 del DPR 445/2000);
- consapevolezza del richiedente dei termini e condizioni associati all'utilizzo del servizio di identità digitale;
- consapevolezza delle raccomandazioni e precauzioni da adottare per l'uso delle identità digitale.

In questa fase il richiedente indica nel contratto anche la tipologia di credenziale richiesta: Livello 1 o Livello 2.

8.2.2 Richiesta on-line dell'identità digitale

La richiesta online dell'identità SPID si sviluppa attraverso un processo guidato che accomuna la fase di registrazione con quella di identificazione. Nella fattispecie il richiedente accede al portale dell'IdP e richiede un'identità digitale secondo un flusso che prevede i seguenti passaggi (non necessariamente nell'ordine di descrizione riportato):

- Form di selezione della tipologia di identità richiesta:
  - Persona Fisica
  - Persona Giuridica
- Form di creazione dell'account – la pagina richiede all'utente l'inserimento dei seguenti dati:
  - Selezione dello username
  - Indirizzo e-mail
  - Numero di telefonia mobile

  L'indirizzo di posta elettronica indicato viene immediatamente verificato tramite l'invio di un'e-mail contenente un codice da inserire all'interno della pagina del processo di registrazione/identificazione.

  Il cellulare viene registrato e verificato contestualmente all'identificazione.
- Form di inserimento anagrafica - la pagina richiede all'utente l'inserimento dei seguenti dati:
  - Nome
  - Cognome
  - Codice fiscale
  - Sesso
  - Data nascita
  - Luogo nascita (Stato, Provincia, Comune)
  - Indirizzo di residenza (via, civico, cap, comune, provincia)

  In caso si stia richiedendo un'identità digitale per persona giuridica, vengono richieste anche le seguenti informazioni:
  - denominazione/ragione sociale;
  - codice fiscale o P.IVA (se uguale al codice fiscale);
  - sede legale;
  - copia della certificazione con indicazione amministratori e/o rappresentanti legale o atto notarile di procura legale complete di data di rilascio e validità dello stesso;

  In questo caso il richiedente deve corrispondere con il legale rappresentante ovvero con il rappresentante indicato nell'atto notarile
- Scelta della modalità di identificazione:
  - Identificazione informatica via CNS/TS-CNS/CIE

    - Acquisizione del modulo di adesione allo SPID attraverso sottoscrizione con Firma Digitale
    - Identificazione a vista da remoto tramite piattaforma audio/video (webcam)
- Form di inserimento del documento di identità (carta di identità, patente, passaporto, altro tipo di documento come indicato in §8.3.1.1). Viene chiesto di inserire:
    - Tipo di documento
    - Numero documento
    - Data emissione
    - Data scadenza
    - Ente emittente
    - Luogo Emissione
    - Copia fronte retro per scansione del documento
- Scelta del livello e tipologia di credenziali:
    - Livello: **L1/L2**
    - Tipo credenziali: **OTP Virtuale/OTP SMS**

  Pagina di accettazione condizioni e privacy e raccolta del consenso all'adesione al servizio. In questa pagina verranno fornite opportune notifiche al fine di:
    - Fornire informativa sul trattamento dei dati e ottenere esplicito assenso (art. 13 del [III])
    - 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)
    - Assicurarsi che il richiedente sia consapevole dei termini e condizioni associati all'utilizzo del servizio di identità digitale
    - Assicurarsi che il richiedente sia consapevole delle raccomandazioni e precauzioni da adottare per l'uso delle identità digitale
- Su questa pagina l'utente dovrà dare esplicita approvazione e presa visione dei punti sopraindicati attivando apposite checkbox.

Al termine del flusso sopradescritto, i dati di richiesta sono registrati a sistema e il richiedente può procedere con la fase di identificazione.

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

Una volta terminata la fase di registrazione, si passa al secondo momento fondamentale del processo di rilascio, ovvero il riconoscimento certo del soggetto richiedente. La funzione di identificazione del richiedente può essere svolta attraverso le seguenti modalità:

a. Identificazione de-visu.
b. Identificazione mediante TS-CNS, CNS, CIE.
c. Identificazione mediante dispositivi contenenti certificati di firma digitale o dispositivi di firma elettronica qualificata;

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

Le modalità a. e d. prevedono la presenza di personale opportunamente formato ed abilitato, mentre le modalità b. e c. possono essere completate in autonomia dal richiedente mediante apposita procedura guidata.

8.3.1 Identificazione con operatore

Per quanto riguarda le modalità di cui al punto a) le pratiche operative per l'identificazione ed il riconoscimento del richiedente sono svolte dalle stesse strutture indicate al §8.2.1.
Per quanto riguarda le modalità di cui ai punti b) e c) le pratiche operative per l'identificazione ed il riconoscimento del richiedente sono svolte dal Gestore tramite suoi incaricati.

8.3.1.1 Identificazione "de visu" mediante APP IdCheck

L'identificazione "de-visu" avviene in presenza dell'operatore della LRA (RAO o IRA) è prevista la presenza fisica del soggetto richiedente dinanzi 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, ed effettuando la copia fronte/retro, uno dei seguenti documenti di riconoscimento, munito di fotografia e di timbro, rilasciati da un'Amministrazione dello Stato, secondo quanto previsto dall'art 35, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445:

- Carta d'Identità
- Passaporto
- Patente di guida

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 ovvero tramite documento informatico sottoscritto elettronicamente.
In questo caso:

a. se il soggetto richiedente è una persona fisica, deve essere esibito un valido documento d'identità;
b. se il soggetto richiedente è una persona giuridica, qualora esso non sia il legale rappresentante della persona giuridica richiedente, deve essere fornito atto notarile di procura legale 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 accerta 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 in corso di validità. Qualora il richiedente non sia munito di Tessera Sanitaria l'incaricato non effettuerà il riconoscimento per SPID.
Se i documenti esibiti dal richiedente risultano carenti delle caratteristiche di cui sopra, l'operatore ne esclude l'ammissibilità ed il processo di onboarding viene sospeso o bloccato fino alla esibizione di documenti validi ed integri.

8.3.1.2 Identificazione "de visu" senza l'ausilio dell'APP

Dati casi espressamente autorizzati da AgID, progetti specifici o situazioni in cui non si renda possibile l'installazione e l'utilizzo dell'APP, l'identificazione si svolge "de visu" come descritto nel precedente paragrafo, ma senza l'ausilio dell'applicativo.
L'IdP, non potendo il RAO avvalersi dello strumento sopra menzionato, svolge tutti i controlli necessari ad accertare la corretta identificazione.

8.3.3 Identificazione informatica mediante TS-CNS, CNS, CIE o Firma Digitale

Così come previsto dall'Art 7 del DPCM e dalle procedure di richiesta dell'IdP, l'identità del soggetto richiedente può essere accertata anche attraverso procedure di identificazione informatica basate su documenti digitali di identità (quali TS-CNS, CNS, CIE o carte ad esse 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 descritte nel seguente paragrafo è fornita al richiedente nella fase finale di richiesta online dell'identità SPID (§8.2.2).
In particolare:

- **TS/CNS, CNS, CIE:** nel caso di scelta dell'identificazione via CNS, TS-CNS o CIE viene richiesto al titolare di inserire la smartcard e di autenticarsi. A questo punto il sistema dell'IdP forza la client authentication TLS 1.2 o superiore richiedendo all'utente l'inserimento del PIN per l'utilizzo della chiave privata custodita all'interno della smartcard.

La firma ricevuta viene verificata con il certificato acquisito e se tutti i controlli andranno a buon fine (compresi anche quelli sulla validità del certificato), l'utente risulta identificato.

In questo caso il Gestore delle identità digitali, considera che la fase di identificazione e verifica sia stata correttamente espletata dal Gestore che ha precedentemente rilasciato il documento digitale di identità cioè la Pubblica Amministrazione Emittente.

- **Firma Digitale:** è il caso in cui il richiedente abbia richiesto di compilare un modulo di richiesta di adesione in formato elettronico sottoscritto con firma elettronica qualificata o digitale e sottoposto dalle pagine. Anche in questo caso il Gestore delle identità effettua le stesse verifiche sulla validità della firma e del certificato considerando che la fase di identificazione sia stata correttamente espletata dal Prestatore di servizio di firma elettronica qualificata, ovvero dal Certificatore.

Per il corretto espletamento della fase di identificazione con strumenti di identificazione informatica, il sistema IdP richiede anche la verifica del numero di telefonia mobile indicato durante la registrazione (§8.2.2). La verifica viene condotta secondo la procedura indicata in §8.4.3.

8.3.4 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 i richiedenti l'identità digitale mediante l'ausilio di strumenti di registrazione audio/video e nel rispetto delle misure prescritte dal Garante in merito al trattamento dei dati personali.

Così come previsto dai regolamenti di cui all'Art 4 comma 2 del DPCM, l'identificazione da remoto prevede l'acquisizione di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte del titolare dell'identità.

In fase di videoidentificazione devono dunque essere rispettate le condizioni di seguito illustrate.

Le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini. L'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi. Il RAO acquisisce tale materiale durante il flusso di videoriconoscimento dell'utente. La sessione deve essere effettuata in ambienti privi di particolari di disturbo.

Il gestore si assume la responsabilità della valutazione del materiale acquisito. L'operatore può quindi sospendere o decidere di non avviare il processo di identificazione nel caso in cui la

qualità audio/video sia scarsa o ritenuta non adeguata a consentire la verifica dell'identità del soggetto richiedente.
Di seguito sono descritti il flusso ed il sistema utilizzati per l'espletamento dell'identificazione attraverso sessione audio-video:

Il Richiedente può effettuare la procedura di riconoscimento in due modi:

1. Con un normale PC che soddisfi i seguenti requisiti:
    - Webcam;
    - sistema audio dotato di casse e microfono;
    - browser aggiornato con supporto alla tecnologia webrtc (come, ad esempio, Chrome o Firefox);
    - connessione internet a banda larga.
2. Con un dispositivo mobile, smartphone o tablet, che soddisfi i seguenti requisiti:
    - sistema operativo Android o iOS di ultima generazione;
    - fotocamera frontale;
    - sistema audio dotato di casse e microfono;
    - 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 verifica l'identità del Richiedente tramite documento di riconoscimento in corso di validità, munito di fotografia riconoscibile del Richiedente e rilasciato da un'Amministrazione dello Stato.

Il Sistema permette di eseguire i riconoscimenti con modalità per cui, al fine di avviare una sessione di videoconferenza, l'operatore incaricato dovrà accedere ad un apposito pannello di Amministrazione, tramite doppio fattore di autenticazione, e raccogliere la chiamata pendente per la video identificazione.
L'Operatore dovrà selezionare la sessione di autenticazione e dopo aver verificato che tutte le componenti software, audio, video e banda internet siano correttamente impostate, guiderà il soggetto richiedente verso la stanza video nella quale è collegato l'operatore.
Al momento dell'identificazione il Richiedente dovrà confermare:

- l'accettazione delle condizioni contrattuali e del trattamento dei dati personali per il rilascio dell'identità digitale;
- gli Attributi identificativi e gli Attributi secondari registrati che verranno utilizzati per il rilascio dell'identità digitale.

Prima di iniziare la registrazione, l'operatore chiede l'assenso alla registrazione audio e video, informando il soggetto interessato circa la sua conservazione. L'assenso è nuovamente raccolto non appena iniziata la registrazione.
In ogni momento l'Operatore/Incaricato avrà la possibilità, tramite appositi tasti, di catturare le immagini, di iniziare una registrazione e di interromperla.

Il richiedente e l'operatore si immettono nella piattaforma ed iniziano la sessione di riconoscimento.
Una volta instaurata la sessione audio/video e previa autorizzazione da parte dell'utente finale, l'utente avvia la registrazione della sessione.

L'Operatore avvia la registrazione, dichiara i propri dati identificativi e chiede al Richiedente se acconsente al trattamento dei dati personali contenuti nella registrazione audio/video e lo informa che la registrazione sarà conservata per 20 anni in modalità protetta, decorrenti dalla scadenza o dalla revoca dell'identità digitale.
Il Richiedente acconsente e l'Operatore chiede conferma dei seguenti dati: generalità, data ed orario della videochiamata, volontà del Richiedente di dotarsi dell'Identità Digitale, dati inseriti nel Modulo di Adesione, numero di cellulare ed indirizzo di posta elettronica (come previsto dall'Art. 8, commi c), d), e) e f).
Il Richiedente dovrà rispondere alle domande di conferma di cui sopra, che l'Operatore in modo casuale gli porrà in modo diretto, indicando chiaramente e specificatamente i dati richiesti, evitando risposte affermative o non sufficientemente esaustive, onde evitare la non ammissibilità della sessione.
L'Operatore chiede al Richiedente di mostrare il fronte e retro del documento di riconoscimento e tessera sanitaria (come previsto dall'Art. 8, commi i) e j) del Regolamento). I documenti devono essere gli originali delle copie che il Richiedente ha inserito in fase di Registrazione.
L'Operatore chiede e ottiene conferma dal soggetto di aver preso visione ed accettare le condizioni contrattuali (come previsto dall'Art. 8, comma k) del Regolamento), disponibili sul sito web ed in fase di registrazione.
L'Operatore comunica che la fase di identificazione è andata a buon fine,termina la registrazione ed informa il Richiedente circa la tipologia di credenziali di cui disporrà per l'accesso ai servizi in rete. L'utente riceverà una mail per attivare la sua Identità Digitale (come previsto dall'Art. 8, comma h) del Regolamento).

Durante la sessione di riconoscimento via webcam, l'intero tracciato audio/video viene registrato e conservato.

Terminata la sessione di videoconferenza il sistema provvederà, autonomamente, ad elaborare le tracce audio-video per la produzione del file cifrato. I file così generati verranno inviati al sistema di Namirial in forma cifrata e saranno archiviati per un periodo pari a 20 anni decorrenti dalla scadenza o dalla revoca dell'identità digitale secondo quanto indicato nell'art. 7, comma 8, del DPCM.
Il sistema Namirial salverà i file in modo garantirne l'accesso esclusivamente su richiesta dell'autorità giudiziaria, dell'Agenzia nel corso delle attività di vigilanza, del titolare dell'identità SPID in caso di disconoscimento della stessa.

8.4 Verifica degli attributi associati all'Identità Digitale

8.4.1 Identità digitale e attributi

L'Identità digitale è rappresentata mediante un insieme di attributi intesi come informazioni o qualità di un utente utilizzate per rappresentare la sua identità, il suo stato altre caratteristiche peculiari. Tali attributi sono costituiti da:

- **attributi identificativi**, quali il nome, cognome, data di nascita, sesso ovvero ragione sociale o denominazione sociale, sede legale, codice fiscale, partita iva 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);
- **attributi non identificativi (o secondari)**, quali il numero di telefono, indirizzo di posta elettronica, domicilio fisico e digitale, nonché eventuali altri attributi individuati da AgID funzionali alle comunicazioni (così come specificato alla lettera d) del comma1 dell'art.1 del DPCM);
- **codice identificativo** come specificato alla lettera g) del comma1 dell'art.1 del DPCM e valorizzato in aderenza ai regolamenti di cui all'art 4 com 2 del DPCM;
- **identificativo utente** attributo corrispondente allo username prescelto dall'utente.

Dopo la fase di registrazione e 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.

8.4.2 Verifica degli attributi identificativi (identità dichiarata)

La verifica dell'identità consiste nel rafforzamento del livello di confidenza sugli attributi di identità, collezionati in fase di identificazione, compiuto attraverso accertamenti, operati per mezzo di fonti autoritative istituzionali, in grado di dare conferma sulla veridicità dei dati raccolti. L'accesso alle fonti autoritative da parte del Gestore ai fini dell'attività di verifica è agevolato grazie alla stipula delle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM

e, nei casi in cui le informazioni necessarie non siano accessibili per mezzo dei servizi convenzionati, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445. Il rilascio dell'Identità SPID è subordinato al superamento di tali verifiche.
Di seguito sono riportate le tabelle che rappresentano i requisiti relativi alle prove di identità e alla verifica condotte da Namirial in relazione al livello di garanzia (LoA SPID) nel caso di persona fisica e di persona giuridica.

Livello di sicurezza	Requisiti/Verifiche effettuate
Per tutti i livelli SPID	Viene assunto che la persona in possesso dei documenti di identità e codice fiscale/tessera sanitaria rappresenti l'identità dichiarata. Viene verificata l'autenticità e la validità dei documenti, nonché l'identità del richiedente sulla base di quanto risulta da soggetti istituzionali competenti (articolo 4, comma 1, lettera c del DPCM 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). Con specifico riferimento al Furto d'Identità il sistema dell'IdP prevede, oltre alla verifica degli attributi mediante SCIPAFI, la consultazione di ulteriori banche dati che garantiscono il rilevamento di eventuali documenti smarriti o rubati.

Tabella 9 - Requisiti da soddisfare/Livelli di sicurezza SPID (persona fisica)

Livello di garanzia	Requisiti
Tutti i livelli SPID	Viene appurata l'esistenza della persona giuridica basandosi su evidenze riconosciute dal sistema delle imprese in ambito nazionale (es. richiesta di Visura Camerale).

	Viene verificata la validità e l'autenticità sulla base di quanto risulta da soggetti istituzionali competenti. Viene effettuata l'associazione certa amministratore o rappresentante legale con l'impresa-persona giuridica, esempio visura camerale o verifica procura notarile. 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 10 - Requisiti da soddisfare/Livelli di sicurezza SPID (persona giuridica)

8.4.3 Verifica degli attributi secondari

La verifica degli attributi non identificativi (secondari) si differenzia a seconda della modalità:

a) a seguito di identificazione con operatore;
b) a seguito di identificazione informatica mediante CIE/CNS e firma digitale
c) a seguito di video identificazione.

8.4.3.1 Modalità A: verifica a seguito di identificazione con operatore

La procedura utilizzata dagli operatori, nel corso della fase di identificazione, innesca l'invio di un SMS e di un'e-mail verso i riferimenti indicati dall'utente all'interno del modulo di adesione.

- **Verifica dell'e-mail:** Il soggetto richiedente legge all'incaricato il codice ricevuto via e-mail e quest'ultimo lo verifica all'intero delle pagine di registrazione. L'e-mail contiene anche ulteriori indicazioni sull'uso del servizio SPID unitamente ad una password temporanea da utilizzare al primo accesso.
- **Verifica del cellulare:** Il soggetto richiedente legge all'incaricato il codice ricevuto via SMS e quest'ultimo lo verifica all'interno delle pagine di registrazione.

Qualora, limitatamente ai soli casi di identificazione de visu, il richiedente non abbia la possibilità di accedere all'e-mail o al cellulare (ad. es. indisponibilità dello strumento), l'incaricato seleziona l'opportuna opzione di verifica postuma all'interno della procedura e la verifica degli attributi viene eseguita secondo le indicazioni riportate in §8.6.

8.4.3.2 Modalità B: verifica a seguito di identificazione mediante CIE/CNS o certificato di firma digitale

La procedura web utilizzata dal richiedente, nel corso della fase di identificazione, innesca l'invio di un SMS e di un'e-mail verso i recapiti indicati dall'utente all'interno del form di registrazione.

- **Verifica dell'e-mail:** l'utente inserisce l'indirizzo e-mail ed il sistema invia alla casella indicata un codice da riportare all'interno delle pagine di registrazione. Se il codice è corretto, la verifica avviene e le pagine permettono all'utente di procedere con la registrazione dei dati. L'e-mail contiene anche ulteriori indicazioni sull'uso del servizio SPID unitamente ad una password temporanea da utilizzare al primo accesso.
- **Verifica del cellulare:** l'utente inserisce il numero di cellulare immediatamente dopo la fase di identificazione. Il sistema invia al cellulare indicato un codice da riportare all'interno delle pagine di registrazione. Se il codice è corretto, la verifica avviene e le pagine permettono all'utente di procedere con il completamento della procedura di identificazione/rilascio.

8.4.3.3 Modalità C: verifica a seguito di videoidentificazione

La procedura web utilizzata dal richiedente, nel corso della sessione di riconoscimento audio/video, innesca, così come previsto dall'Art 8 comma g) del Regolamento per le modalità attuative dello SPID, l'invio di un SMS e di un'e-mail verso i recapiti indicati dall'utente all'interno del form di registrazione.

- **Verifica dell'e-mail:** La piattaforma di video riconoscimento invia alla casella indicata in fase di registrazione un URL da cliccare da parte dell'utente al fine di sbloccare la procedura in corso nella piattaforma di video riconoscimento. Dopo che l'utente ha cliccato, il processo di riconoscimento audio/video passa allo step successivo.
- **Verifica del cellulare:** La piattaforma di video riconoscimento invia al cellulare indicato in fase di registrazione un codice da riportare all'interno delle pagine della piattaforma di video riconoscimento. Se il codice è corretto, la verifica avviene e le pagine permettono all'utente di procedere con il completamento della procedura di video identificazione.

8.5 Attivazione dell'identità digitale

Solo dopo aver effettuato l'iter completo, cioè dopo aver completato l'identificazione e le verifiche necessarie nonché gli ulteriori ed eventuali controlli che il Gestore riterrà opportuno implementare sugli attributi identificativi e secondari, l'identità digitale e le relative credenziali di accesso possono essere attivate. Il gestore invia al titolare opportuna comunicazione dell'avvenuta attivazione mediante i canali di contatto forniti in fase di richiesta (e-mail e/o sms).

8.6 Rilascio, consegna e attivazione delle credenziali

Le credenziali rilasciate all'utente, associate all'identità e al livello SPID richiesti, sono consegnate all'utente solo dopo aver completato con successo l'identificazione e la verifica degli attributi identificativi e secondari.
A tal proposito si ricorda che Il soggetto può richiedere e ricevere 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 con un buon grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema autenticazione a singolo fattore, ad es. la password; questo livello può essere considerato applicabile nei casi in cui il danno causato, da un utilizzo indebito dell'identità digitale, ha un basso impatto per le attività del cittadino/impresa/amministrazione;
- **livello 2** (corrispondente al LoA3 dell'ISO-IEC 29115): garantisce con un alto grado di affidabilità l'identità accertata nel corso dell'attività di autenticazione. A tale livello è associato un rischio ragguardevole e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori non necessariamente basato su certificati digitali; questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un danno consistente.

La **username** viene normalmente scelta dall'utente in fase di registrazione.

8.6.1 Consegna password tramite piattaforma utente gestione SPID

L'utente recupera l'e-mail di verifica inviata nella fase di registrazione e seguendo le indicazioni ivi contenute accede all'area riservata. L'accesso è effettuato con lo username prescelto e con la password temporanea contenuta nell'email.
Dal momento che l'utente in questa fase sta effettuando il primo accesso all'area riservata, il sistema dell'IdP, come misura di irrobustimento del livello di sicurezza, richiede un'autenticazione di livello 2 inviando un codice via SMS al numero di cellulare indicato come attributo secondario. Se l'autenticazione avviene con successo, le pagine forzano il cambio della **password** imponendo le policy di sicurezza descritte in §10.1 e previste dalla normativa SPID per le credenziali di livello 1. Durante la creazione dalla nuova password il sistema guida l'utente nella scelta visualizzandone il grado di sicurezza e lasciando, se richiesto, la possibilità di poterla generare casualmente. Questi accorgimenti sono propedeutici per far sì che la password rispetti le regole di complessità previste dalle regole attuative.

8.6.2 Consegna password tramite prima autenticazione

L'utente effettua il primo accesso tramite un SP accreditato e viene reindirizzato sulle pagine di autenticazione dell'IdP.
L'utente inserisce lo username e la password temporanea contenuta nell'email. Le pagine dell'IdP rilevano che l'utente sta effettuando il primo accesso e quindi richiedono un'autenticazione di livello 2 inviando un codice al numero indicato come attributo secondario.
Se l'autenticazione avviene con successo, le pagine forzano il cambio della **password** imponendo le policy di sicurezza descritte in §10.1 e previste dalla normativa SPID per le credenziali di livello 1.
Durante la creazione dalla nuova password il sistema guida l'utente nella scelta visualizzandone il grado di sicurezza e lasciando, se richiesto, la possibilità di poterla generare casualmente.
Questi accorgimenti sono propedeutici per far sì che la password rispetti le regole di complessità previste dalle regole attuative.

8.6.3 Consegna credenziali livello 2

Nel caso delle credenziali di **livello 2** il processo di consegna/attivazione può essere applicato alle tipologie OTP di tipo virtuale (applicazione Virtual OTP) e SMS (§10.2.1 e §10.2.2). oppure, eventualmente, alle tipologie OTP di tipo fisico (§10.2.3).

8.6.3.1 Virtual OTP e OTP SMS

Nel caso di OTP di tipo **Virtual OTP** e **SMS** è previsto l'uso di un dispositivo personale, come lo smartphone. La procedura prevede la comunicazione di un codice segreto via SMS che permette l'attivazione dell'App OTP Virtuale.
Nella fattispecie, l'utente, per l'attivazione dell'App Virtual OTP, svolge le seguenti operazioni:

1. accede all'area riservata SPID tramite credenziale di livello 1;
2. richiede esplicitamente l'attivazione della credenziale di livello 2 di tipo Virtual OTP;
3. inserisce il codice ricevuto per SMS all'atto dell'attivazione delle credenziali di livello 1 (questa operazione innesca l'invio di un'e-mail con QRCode e codice di attivazione dell'App);
4. avvia l'App Virtual OTP ed esegue la procedura di attivazione;
5. inserisce il codice ricevuto per e-mail allo step 3 o fotografa il QRCode;
6. l'applicazione viene attivata.

La procedura sopra descritta viene eseguita successivamente al cambio password, dopo il primo accesso (attivazione credenziale di livello 1). Trascorsi oltre 30 (trenta) minuti l'utente è costretto a richiedere l'invio di un nuovo codice OTP via SMS. Il flusso di attivazione prevede

che, per il corretto completamento, siano verificati la conoscenza della password di livello 1, il controllo dell'e-mail e del cellulare dichiarati nell'identificazione.
La consegna (attivazione) della credenziale Virtual OTP può essere espletata sia all'interno della piattaforma del Gestore che all'interno delle schermate di prima autenticazione sull'IdP.
Nel caso in cui l'utente abbia scelto l'uso di credenziali di livello 2 di tipo NAMIRIAL SMS (§10.2.2), non è necessaria la consegna di codici di attivazione perché la credenziale risulta automaticamente consegnata in quanto collegata alla SIM del titolare. All'interno della procedura di consegna e attivazione delle credenziali l'utente può attivare la funzione di segnalazione di ogni avvento utilizzo delle credenziali, attraverso l'invio degli estremi d'uso ad uno degli attributi secondari.

8.6.3.2 OTP fisico

Nel caso di OTP di tipo hardware si distinguono due ulteriori casistiche:

- OTP già in possesso del richiedente
- OTP da consegnare

Per il caso di OTP fisico già in possesso del richiedente[2], è previsto l'uso di un dispositivo personale già fornito dal Gestore Namirial S.p.A. nell'ambito dell'utilizzo di altro servizio fiduciario (ad esempio firma remota).
Per il caso di OTP da consegnare, i dispositivi vengono assegnati e consegnati al Titolare dall'operatore della LRA, in sua presenza e successivamente all'identificazione e registrazione dello stesso.

9. Gestione delle identità digitali[17]

Il Gestore 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 il Gestore 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 onboarding, da una verifica delle informazioni comunicate, mediante documenti e dati ottenibili da fonti affidabili ed indipendenti. Oltre alle modifiche degli attributi il Titolare può effettuare la modifica della password statica o richiederne il ripristino.
Si ricorda che l'utente è tenuto ad aggiornare la propria password trascorsi 180 giorni dalla creazione ovvero ultima variazione.

9.1 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 in materia di tutela dei dati personali di cui Regolamento (UE) 2016/679 in materia di protezione dei dati personali.
I dati sono conservati per un periodo non inferiore a venti (20) anni dalla scadenza, revoca o disattivazione dell'identità digitale. Il Gestore conserva le suddette informazioni per tutta la durata contrattuale. Tra le informazioni conservate sono presenti anche:

- le copie dei documenti di identità;
- moduli di richiesta firmati;
- i log di transazione in caso di riconoscimento via web e via CNS;

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

9.2 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, a sua voltasi articola in:
    a. conservazione;
    b. sospensione e revoca;
    c. rinnovo e sostituzione.

9.2.1 Gestione degli attributi

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

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

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

L'utente, in caso di dichiarazioni non fedeli o mendaci, si assume le responsabilità previste dalla legislazione vigente.
L'utente che deve modificare i propri attributi identificativi può farlo accedendo al portale del Gestore. Mediante accesso con le proprie credenziali SPID di livello 2, il Titolare può modificare:

- gli estremi del documento di riconoscimento;
- la data di scadenza del documento di riconoscimento;
- il numero di telefonia mobile;
- l'indirizzo di posta elettronica;
- il domicilio.

Ogni informazione è inserita dal Titolare sotto la sua piena responsabilità. Ad ogni variazione operata sugli attributi sopraindicati, 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 (ad es. per la modifica del numero di telefonia mobile l'IdP procede alla sua certificazione con modalità analoghe a quelle previste per la sua verifica in fase di identificazione §8.3).
L'aggiornamento delle informazioni è comunicato 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).
Nel caso in cui sia modificato l'indirizzo di posta elettronica la comunicazione viene inviata al vecchio e nuovo indirizzo di posta.

Inoltre, all'interno del pannello di gestione sopraindicato, è previsto un sistema attraverso il quale l'utente potrà effettuare autonomamente le operazioni descritte nei paragrafi che seguono.
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.).

9.2.2 Sospensione e revoca dell'identità

Prima di descrivere le modalità operative per Sospensione o la Revoca di un Identità Digitale si precisa che:

- la **sospensione** di un'identità digitale causa una disattivazione temporanea delle credenziali associate. Così come previsto dalle norme attuative di cui all'art 4 comma 2 del DPCM.
- la **riattivazione** consiste nel rendere di nuovo utilizzabili le credenziali precedentemente sospese.
- la **revoca** rende inutilizzabili per sempre le credenziali.

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;
7) per scadenza del documento di identità.

Nel caso previsto ai punti 1) e 6), il gestore dell'identità digitale revoca di propria iniziativa l'identità, comunicando la causa e la data della revoca all'utente, con avvisi ripetuti (90 (novanta), 30 (trenta) e 10 (dieci) 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 Namirial ID è in grado di comunicare al Titolare il mancato utilizzo dell'identità digitale con cadenze personalizzabili che, di default, sono impostate a 90 (novanta), 30 (trenta) e 10 (dieci) 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 già menzionati 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, dovrà procedere tempestivamente alla revoca.
Nel caso previsto dal punto 7), il gestore dell'identità digitale sospende di propria iniziativa l'identità, comunicando la causa e la data della sospensione all'utente, utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).
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:

- richiesta al gestore inviata via PEC;
- richiesta, in formato elettronico e sottoscritta con firma digitale o elettronica, inviata alla casella e-mail del l Gestore.

Namirial S.p.A. fornisce esplicita evidenza all'utente dell'avvenuta presa in carico della richiesta e procede alla immediata sospensione dell'identità digitale.
Trascorsi 30 (trenta) giorni dalla sospensione, il Gestore si riserva di riattivare l'identità all'esito della valutazione che confermi il soddisfacimento degli stessi requisiti di garanzia posseduti prima della sospensione.
Nel caso previsto dal punto 5), l'utente può chiedere al Gestore, 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, cioè attraverso:

- richiesta al gestore inviata via PEC;
- richiesta inviata tramite la casella di posta nota al Gestore in formato elettronico e sottoscritta con firma digitale.
- richiesta inviata tramite una casella di posta elettronica diversa da quella nota al Gestore, allegando la scansione del modulo di richiesta di revoca o sospensione firmato e copia del documento d'identità.

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

Il Gestore, 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 20 (venti) anni decorrenti dalla revoca dell'identità digitale.

9.2.3 Gestione ciclo di vita delle credenziali

Il sistema di gestione del ciclo di vita delle credenziali di Namirial S.p.A. comprende i processi previsti dai regolamenti di cui all'Art 4 comma 2 del DPCM, ovvero:

- creazione delle credenziali;
- consegna delle credenziali o dei mezzi usati per la loro produzione.
- attivazione delle credenziali o dei mezzi usati per la loro produzione.
- conservazione delle credenziali;
- sospensione e revoca delle credenziali;
- rinnovo e sostituzione delle credenziali;

Alcuni dei processi sopra elencati possono essere influenzati dal fatto che le credenziali possano eventualmente essere rese operative attraverso l'ausilio di un dispositivo hardware. Come descritto nei paragrafi precedenti, i processi sopraelencati sono resi disponibili all'interno dell'area Web dedicata all'utente e alla quale si accede con credenziale almeno di livello 2 o codice di emergenza.
Il Gestore, per l'intero ciclo di vita della credenziale conserva opportuna documentazione atta ad avere traccia delle seguenti informazioni:

- creazione della credenziale;
- identificativo della credenziale;
- soggetto per il quale è stata emessa;
- stato della credenziale.

Il Gestore conserva opportuna documentazione per ogni sottoprocesso (creazione, emissione, attivazione, revoca, sospensione, rinnovo e sostituzione) del processo di gestione delle credenziali, nel pieno rispetto del Regolamento (UE) 2016/679 in materia di protezione dei dati personali. Namirial S.p.A. 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.

10. Descrizione delle architetture dei sistemi di autenticazione e delle credenziali(5)

Il Gestore Namirial S.p.A. rende disponibili al Titolare tre metodi di autenticazione, descritti di seguito, denominati:

- Basic Authentication (Livello SPID 1, LoA 2)
- Time Based One Time Password (Livello SPID 2, LoA 3)
- One Time Password via SMS (Livello SPID 2, LoA 3)

Nei paragrafi che seguono sono descritte le caratteristiche dei sistemi di autenticazione sopra indicati.

10.1 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: username e password.
La password viene scelta direttamente dal Titolare in fase di generazione della stessa, nel corso della procedura di consegna della credenziale (§8.6)
In particolare, in relazione al tipo della password, il sistema IdP di Namirial impone l'uso delle raccomandazioni baseline per l'ottenimento di password complesse e difficilmente attaccabili:

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

Il Repository SPID inoltre impone i seguenti meccanismi di protezione:

- impedisce l'uso di formati comuni (ad es. codice fiscale, patente auto, sigle documenti, date, includere nomi, account-Id ecc.);
- fissa la scadenza delle password non oltre i 180 (centottanta) giorni e ne impedisce il riuso o che abbiano elementi di similitudine prima di 5 variazioni o comunque non prima di 15 (quindici) mesi;
- implementa una procedura di sollecito con la quale invita l'utente a modificare la Password secondo le raccomandazioni sopra indicate;
- 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.

10.2 Livello di sicurezza 2

Il sistema di Autenticazione Forte proposto per il livello di sicurezza 2 si basa su un "Identification Server" OATH Compliant che consente di utilizzare gli standard di autenticazione maggiormente diffusi: TOTP e HOTP. Il sistema del Gestore Namirial S.p.A. consente l'utilizzo di vari meccanismi tra cui: OTP event-based (HOTP) o time-based (TOTP) e OTP su SMS.

10.2.1 Namirial Virtual OTP

Il Gestore Namirial S.p.A. ha sviluppato un sistema di generazione di OTP per dispositivi mobili basati su iOS e Android che rispettano le specifiche OATH. Il metodo prevede che il Titolare installi una App gratuita sul proprio smartphone, scaricabile dai principali app-store. L'App può operare secondo le due diverse modalità di seguito descritte.

10.2.1.1 Generatore codici OATH-TOTP

Questa modalità operativa è destinata alla classe d'utenza che predilige utilizzare il proprio smartphone come dispositivo generatore di OTP (similmente ai token rilasciati dai principali istituti di credito per l'autorizzazione delle disposizioni in ambito home banking).
L'utente installa l'App nel proprio smartphone e la utilizza come token TOTP: il metodo è basato su un'estensione dell'algoritmo per la generazione di HOTP per aggiungere al calcolo un fattore legato al tempo corrente.
Nella fattispecie, l'utente, a seguito alla corretta verifica delle credenziali di primo livello sul portale dell'IdP, avvia l'App Namirial Virtual OTP e genera un codice TOTP. Questo codice deve essere inserito nelle maschere di autenticazione mostrate dall'IdP a seguito della corretta autenticazione di primo livello, e serve a dimostrare l'effettivo possesso e controllo del dispositivo personale: smartphone.
Questo meccanismo si identifica come secondo fattore di identificazione in quanto prova il possesso del segreto comune utilizzato per la generazione degli OTP. Il segreto è scambiato in fase di consegna della credenziale e non è ottenibile neanche intercettando la serie di OTP generati.
La sincronizzazione tra la device mobile ed il server dell'IdP può essere gestita attraverso l'uso di server NTP o semplicemente abilitando sensori GPS sempre più disponibili sulle device mobili.
Il seme, generato al momento dell'emissione e trasmesso dall'IdP al device con cifratura end-to-end, viene memorizzato sulla device mobile cifrato.
L'App, inoltre, può proteggere la generazione dei codici OTP con l'ausilio di un PIN personale che l'utente dovrà inserire ad ogni avvio dell'App.

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.

10.2.1.2 Recettore codici OTP su notifica PUSH

Questa modalità è indirizzata alla classe d’utenza che, per l’uso di codici OTP, predilige un’esperienza d’uso simile a quella di codici inviati per SMS. L’utente installa l’App nel proprio smartphone e la utilizza come client per la ricezione di codici OTP OATH compliant generati server-side e inviati esclusivamente all’istanza dell’App associata al particolare utente-dispositivo.
I codici OTP sono generati server-side utilizzando un algoritmo OATH compliant e vengono inviati alla particolare istanza dell’App usando cifratura end-to-end basata su algoritmo AES.
Nella fattispecie, l’utente, a seguito alla corretta verifica delle credenziali di primo livello sul portale dell’IdP, innesca la generazione del codice OTP server side (di durata temporale molto limitata e legata alla particolare sessione) che viene inviato all’App attraverso i meccanismi di notifica proprietari del Sistema Operativo del device.
L’utente riceve questo codice e deve inserirlo nelle maschere di autenticazione mostrate dall’IdP a seguito della corretta autenticazione di primo livello, per dimostrare l’effettivo possesso e controllo del dispositivo personale: smartphone.
Questo meccanismo si identifica come secondo fattore di identificazione in quanto prova il possesso del segreto comune utilizzato per ricezione e decifratura dei codici OTP trasmessi dal server. Il segreto è scambiato in fase di consegna della credenziale e non è ottenibile neanche intercettando la serie di OTP generati.
Il segreto viene memorizzato sulla device mobile in modo cifrato. In questo caso il secondo fattore (“something you have”) è rappresentato dal dispositivo sul quale si trova installato il software di ricezione e decifratura dei codici OTP. La OTP è generata server-side con un algoritmo conforme allo standard OATH ed ha una lunghezza di almeno 6 cifre decimali.

10.2.2 Namirial SMS (OTP 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 riceve un SMS sul proprio cellulare con il codice OTP composto di 6 cifre decimali.
Nella fattispecie il metodo prevede, in seguito alla corretta verifica delle credenziali di primo livello, l'invio di una OTP sul numero di telefono verificato in possesso del Titolare: il meccanismo si identifica come secondo fattore di identificazione in quanto prova il possesso

della SIM mobile. La One-Time Password generata è casuale, unica e con validità limitata nel tempo.
Nel caso in cui l'OTP ricevuto si rivelasse corretto entro il limite di 3 tentativi l'autenticazione può considerarsi conclusa con successo. In seguito, viene installato nel browser dell'utente un cookie con un identificativo che viene utilizzato per identificare la sessione di SSO attivata. Per l'invio dei messaggi si utilizza un pool di dispositivi appositi che si occupano del colloquio con la rete GSM.

10.2.3 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 Namirial S.p.A. sono tali da garantire i seguenti requisiti funzionali:

- il dispositivo OTP è conforme alle specifiche OATH;
- il dispositivo OTP non può essere clonato;
- il dispositivo OTP possieda un sistema anti-tampering basato su meccanismi di tamper evidence e tamper response;
- il dispositivo OTP è univocamente identificabile.

In particolare, tali dispositivi hardware garantiscono il rispetto dei seguenti requisiti:

Requisito	Conformità
Anti-cloning	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.
Anti-tampering	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.
Unique identification	Ogni dispositivo possiede un numero di serie univoco cablato a livello fisico e logico.

Tabella 11 - Caratteristiche OTP fisici

11. Descrizione dei codici e dei formati dei messaggi di anomalia sia relativi ai protocolli che ai dispositivi di autenticazione utilizzati(6)

Durante il processo di autenticazione da parte del gestore delle identità potrebbero verificarsi degli errori che devono essere presentati all'utente che sta tentando di utilizzare il servizio. In allegato a questo Manuale Operativo viene inserita la tabella degli errori indicata dall'Agenza disponibile come Appendice A- Codici e formati dei messaggi di anomalia.

12. Tracciature degli accessi al servizio e di autenticazione e delle modalità di acquisizione ai fini dell'opponibilità a terzi(9)

12.1 Tracciature degli accessi al servizio

Gli accessi al servizio sono registrati sotto forma di log certificato per un periodo pari a 24 (ventiquattro) mesi. Il log certificato è composto da un file di testo prodotto dall'applicativo che gestisce il processo di autenticazione e dialogo con i Service Provider, il quale viene salvato, firmato e marcato temporalmente nei sistemi IdP di Namirial S.p.A. Su tali log è garantita la disponibilità e l'integrità secondo quando previsto dalle regole tecniche di cui all'art 4 del DPCM. Le registrazioni garantiscono il collegamento per ogni transazione tra codice identificativo dell'Identità Digitale, richiesta di autenticazione generata dal Fornitore di servizi e relativa risposta generata dal Gestore in seguito all'autenticazione dell'utente, mediante le credenziali fornite in fase di rilascio dell'Identità Digitale.
In particolare, per ogni transazione vengono registrati i seguenti dati:

- codice identificativo dell'Identità SPID;
- la richiesta del SP conforme ai protocolli definiti dalle Regole Tecniche;
- la risposta del IdP conforme ai protocolli definiti dalle Regole Tecniche;
- ID della richiesta;
- timestamp della richiesta;
- SP richiedente autenticazione (issuer richiesta);
- ID della risposta;
- timestamp della risposta;
- IdP autenticante (issuer risposta);
- ID dell'asserzione di risposta;
- Soggetto dell'asserzione di risposta (subject).

Procedura per la richiesta del log certificato

Il Titolare dell'identità si collega con le proprie credenziali al portale di gestione dell'identità, da cui inoltra una richiesta di informazioni contenute nel log certificato indicando l'intervallo di date dell'utilizzo delle credenziali SPID di cui intende ricevere informazioni. La richiesta è validata con l'inserimento delle credenziali SPID di livello 2. Namirial S.p.A. provvede alla produzione della/delle attestazione/i richiesta/e dal Titolare e le visualizza all'interno del pannello. L'utente, tramite apposita funzione, può effettuare il download in locale. Le attestazioni rilasciate conterranno almeno le seguenti informazioni: SP, data e ora di accesso, attributi richiesti, livello SPID usato, dettagli contenenti ulteriori informazioni tra cui: SAML di

richiesta/risposta. Le attestazioni potranno essere utilizzate dal Titolare per gli usi consentiti dalla legge.

12.3 Registrazione degli eventi relativi alla richiesta dell'Identità

Al fine di poter documentare la corretta attribuzione di una Identità Digitale emessa dal Gestore Namirial S.p.A., vengono archiviate nel sistema IdP (per una durata pari ad anni 20 (venti) decorrenti dalla scadenza o dalla revoca dell'identità digitale) le seguenti informazioni, in funzione della modalità di identificazione utilizzata dall'utente.

Modalità di richiesta	Evidenze da archiviare
Identificazione "de visu"	• Modulo di richiesta del servizio[3] con condizioni generali del contratto e consensi privacy. • Copia dei documenti utilizzati per l'identificazione (documento di identità e tessera sanitaria/codice fiscale). • Log di conferma della richiesta di adesione. • Log verifiche effettuate. • Identificativo operatore che ha eseguito l'identificazione a vista
Identificazione tramite Carta Nazionale dei Servizi/Tessera Sanitaria-Carta Nazionale dei Servizi/Carta di Identità Elettronica	• Modulo di richiesta del servizio con condizioni generali del contratto e consensi privacy. • Log del processo di identificazione tramite CNS, TS/CNS e CIE. • Log verifiche effettuate.
Identificazione tramite Firma Digitale	• Modulo di richiesta del servizio con condizioni generali del contratto e consensi privacy, firmato digitalmente dal richiedente. • Log verifiche effettuate.

Tabella 12 - Evidenze archiviate per durante il processo di identificazione

12.4 Guida Utente(10)

La guida utente è un documento esplicativo e di facile comprensione per l'Utente che può essere reperito al link sul sito https://support.namirial.com/it/docs/docs-tsp-identita-digitale. All'interno del documento è riportata una descrizione dettagliata delle modalità d'uso e di attivazione delle credenziali, le modalità per richiedere la sospensione e/o la revoca e le cautele in capo al Titolare per la conservazione e la protezione delle credenziali.

[3] I moduli di richiesta del servizio riportano il riferimento alla versione delle Condizioni Generali del Servizio applicabili.

13 Descrizione generale del sistema di monitoraggio(14)

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 al §7.1, nonché le prestazioni dei medesimi.
I controlli vengono effettuati con cadenza regolare in contemporanea su centinaia di sistemi e in caso di errore visualizza un alert (rosso ed evidente) all'interno dei pannelli sinottici dei NOCs (Network Operations Centers).
Il monitoraggio implementato sui sistemi è orientato a verificare:

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

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.
Qualora nel corso delle operazioni di verifica e monitoraggio, il team di gestione rilevi anomalie nel funzionamento del servizio, vengono attivate le analisi al fine di comprenderne cause e conseguenze nonché determinare le azioni da intraprendere. Gli eventi significativi che hanno impatto sul servizio sono notificati alla Service Control Room del Gestore dell'Identità Digitale.
I cambiamenti di stato dell'evento vengono monitorati e notificati agli attori interessati. Il Gestore si avvale di gruppi specialistici per il monitoraggio della sicurezza dei Sistemi informativi che erogano il servizio Namirial ID. In particolare, sono svolte attività di rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica per mezzo della continua osservazione dell'infrastruttura gestita. I suddetti eventi/allarmi sono rilevati attraverso piattaforme di Intrusion Prevention atte a difendere applicazioni e dati critici da attacchi avanzati e piattaforme di "Security Information and Event Management" per la raccolta degli eventi 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 l'archiviazione in modo sicuro, secondo principi di sicurezza quali la non ripudiabilità/alterabilità dei log legali. 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.
Le consolle di monitoraggio sono configurate per il controllo continuo e la produzione di allarmi e report di sicurezza per le diverse tipologie di controlli effettuati. Con cadenza trimestrale è prodotta la reportistica degli eventi verificatisi, al fine di valutare l'efficacia dei controlli attuati.

13.1 Presidi di sicurezza

Il Gestore si avvale di gruppi specialistici per il monitoraggio della sicurezza dei sistemi informativi che erogano il servizio SPID. L'infrastruttura di sicurezza è costituita dall'insieme dei sistemi e degli apparati adibiti alla protezione dell'ambiente tecnologico ed applicativo dedicato al servizio Namirial ID, nonché dai meccanismi di protezione dei dati che transitano o risiedono sui sistemi. Sono abilitate attività di rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica per mezzo della continua osservazione dell'infrastruttura gestita. I suddetti eventi/allarmi sono visualizzati principalmente attraverso specifiche console di monitoraggio. Ciascuna console è configurata per monitorare eventi diversi e produrre allarmi e report in funzione della tipologia dei controlli effettuati. Con cadenza settimanale è prodotta la reportistica degli eventi verificatisi al fine di valutare l'efficacia dei controlli attuati. Le attività di monitoraggio delle componenti di sicurezza attraverso il controllo e l'analisi dei report viene utilizzata anche ai fini della prevenzione degli incidenti di sicurezza. Gli eventi riscontrati sono classificati in funzione della loro gravità e degli impatti che possono avere sugli asset; in relazione a tale classificazione, sono identificate le contromisure idonee a gestire l'evento. Quando dall'evento scaturisce un danno, sono svolte le attività necessarie ad accertare e valutare il danno subìto nonché a definire il piano di ripristino.

13.2 Funzionalità di fraud detection

Sono adottate tipiche tecniche di fraud detection, sviluppate prendendo come benchmark i sistemi di utilizzo delle carte di credito, di account bancari e i principali provider di posta elettronica. In dettaglio viene:

- monitorato il numero consecutivo di tentativi di login falliti fissando una soglia per password e otp. Superata la soglia password viene innescato un meccanismo di

slowdown per mitigare attacchi di brute-force e, allo stesso tempo, non creare effetti DoS sul Titolare. Superata la soglia della credenziale otp la stessa viene bloccata;
- inviata una e-mail per ogni accesso effettuato. La frequenza di invio può essere configurata dall'utente;
- verificato il numero di login per fascia oraria, inviando alert qualora si superi la soglia massima (10);
- verificato giornalmente la provenienza geografica delle connessioni e sollevato un alert in caso di discrepanze significative;
- monitorato il cambio password e sollevato un alert in caso di frequenza superiore ad una determinata soglia (5 per mese);
- monitorato l'utilizzo delle credenziali: ad ogni login all'utente verrà indicata la data della sua ultima connessione; in caso di inattività superiore alla soglia prevista normativamente l'utenza viene sospesa.

13.3 Monitoring del servizio di autenticazione

Il servizio di autenticazione viene costantemente monitorato al fine di verificare che l'intero sistema di autenticazione garantisca i livelli di servizio forniti e risponda nel modo corretto. Nel dettaglio viene simulato il comportamento di un utente eseguendo tutti i passi richiesti dal processo:

- la richiesta di autenticazione,
- l'inserimento delle credenziali e
- la verifica della risposta

La sonda di navigazione è implementata tramite un software di virtualizzazione dell'utente che realizza le navigazioni automatiche, come descritto sopra, per il controllo dello stato dei servizi. Tale utility viene utilizzata a supporto del processo di Incident Management e concorre di fatto al calcolo e gestione degli SLA di servizio.

14 Clausola risolutiva espressa ai sensi dell'Art. 1456 C.C.

L'inadempimento da parte del Titolare o del Richiedente dei rispettivi obblighi descritti nel precedente §3.1, costituisce inadempimento essenziale ai sensi dell'art. 1456 C.C. e dà facoltà all'IdP di risolvere il contratto eventualmente intercorso con tali soggetti. La risoluzione opererà di diritto al semplice ricevimento di una comunicazione, inviata dall'IdP tramite raccomandata A/R. o Posta Elettronica Certificata (PEC), contenente la contestazione dell'inadempienza e l'intendimento di avvalersi della risoluzione stessa.

Appendice A – Codici e formati dei messaggi di anomalia(6)

Error Code	Casistica	Binding	http status code	SAML Satus 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 Redirect ---------- HTTP POST	HTTP 403	n.a	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contatare il gestore del servzio"	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 Parametri non obbligatori: RelayState ---------- Parametri obbligatori: SAML Req Parametri non obbligatori: RelayState

Error Code	Casistica	Binding	http status code	SAML Satus code / Sub status / Status message	Destinatario notifica	Screen IDP	Messaggio utente	Troubleshooting SP	Note
5	Verifica della firma fallita	HTTP POST 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 Redirect ---------- HTTP POST	HTTP 403	n.a	Utente	Pagina di cortesia con messaggio "Formato richiesta non ricevibile- Contatare il gestore del servzio"	Contattare il gestore del servizio	Verificare metdata Gestore dell'identita (IdP)	invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell'identity ---------- invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity
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 - Conttatare 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	

Error Code	Casistica	Binding	http status code	SAML Satus code / Sub status / Status message	Destinatario notifica	Screen IDP	Messaggio utente	Troubleshooting SP	Note
10	Issuer non presente, malformato o non corrispondete all'entita che sottoscrive la richiesta	HTTP POST/HTTP Redirect	HTTP 403	n.a	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Conttatare il gestore del servizio"	Contatare il gestore del servzio	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:cla sses:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:cla sses:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:cla sses:SpidL3
13	IssueInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
14	destination non presente, malformata o non coincidente con ill Gestore delle identità ricevente la richiesta	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
15	attributo isPassive presente e attualizzato al valore true	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	

Error Code	Casistica	Binding	http status code	SAML Satus code / Sub status / Status message	Destinatario notifica	Screen IDP	Messaggio utente	Troubleshooting SP	Note
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 AssertionConsumerServiceIndex riportato in presenza di uno od entrambi gli attributi AssertionConsumerServiceURL e ProtocolBinding AssertionConsumerServiceIndex non presente in assenza di almeno uno attibuti 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	

Error Code	Casistica	Binding	http status code	SAML Satus code / Sub status / Status message	Destinatario notifica	Screen IDP	Messaggio utente	Troubleshooting SP	Note
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 comunicando 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 comunicando 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 comunicando 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 comunicando 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.

Error Code	Casistica	Binding	http status code	SAML Satus code / Sub status / Status message	Destinatario notifica	Screen IDP	Messaggio utente	Troubleshooting SP	Note
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 sospesie o revocate"		Fornire una pagina di cortesia comunicando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	