MANUALE OPERATIVO SPID

Servizio di Gestione
Sistema Pubblico dell'Identità Digitale
di TeamSystem S.p.A.

INFORMAZIONI SUL DOCUMENTO

Controllo Documentale

- Livello di Classificazione: PUBBLICO
- Ente di Emissione: TeamSystem S.p.A.
- Versione: 1.7
- Data di edizione: 01/02/2023
- Codice documento: TS-MO-SPID

Registro delle modifiche

Rev.	Data	Parti modificate	Descrizione modifiche
1.0	11/01/2021	Prima Emissione	Nessuna
1.1	13/04/2021	Prima Revisione	Aggiornamento contenuti
1.2	02/08/2021	Seconda revisione	Aggiornamento contenuti
1.3	04/01/2022	Architettura applicativa	Revisione dettagli tecnici
1.4	31/01/2022	Architettura applicativa	Aggiornamento schema di alto livello
		Registrazione del soggetto Richiedente	Inserimento dettagli su SPID professionale
1.5	14/04/2022	Service Level Agreement	Eliminazione descrizione modalità di riconoscimento video del richiedente, descrizione delle modalità di riconoscimento implementate dall'IdP nei processi di richiesta di identità SPID ad uso professionale, eliminazione del riferimento alla Carta dei Servizi. Inserimento delle modalità adottate per la verifica della titolarità del soggetto che richiede lo SPID professionale per la persona giuridica, Rimozione Carta dei Servizi. Inserimento Avvisi AgID nel paragrafo dei Riferimenti normativi. Inserimento url piattaforma dedicata al servizio di Gestore SPID. Revisione generale del documento.
1.6	06/07/2022	Capitoli 2, 3 e 5	Aggiornamento sito web e PEC dell'IdP, eliminazione riferimenti agli obblighi dei RAO e dei Service Provider, inserimento riferimenti alla procedura di revoca/sospensione attraverso portale dedicato al titolare.
1.7	01/02/2023	Capitoli 3,5 e 7	Introduzione della modalità di riconoscimento de visu da remoto

Altre informazioni sul documento

- N° Allegati: 0

SOMMARIO

1. INTRODUZIONE

1.1 Scopo

Questo documento pubblico, chiamato "MANUALE OPERATIVO SPID Servizio di Gestione Sistema Pubblico dell'Identità Digitale di TeamSystem S.p.A." o anche "Manuale Operativo", descrive le procedure operative seguite da TeamSystem nell'erogazione del servizio di Gestione dell'Identità Digitale (Identity Provider - IdP) per aderire al Sistema Pubblico per la gestione dell'Identità Digitale conforme ai sensi del DPCM del 24 ottobre 2014 del CAD e del DPR n. 445.

1.2 Definizioni e acronimi

Le definizioni e acronimi del presente Manuale Operativo sono in linea con quanto indicato all'interno dei seguenti riferimenti normativi:

- Codice Amministrazione Digitale - CAD (rif. [7]);
- Regolamento (UE) n. 910/2014 eIDAS (rif. [8]);
- DPCM del 24 ottobre 2014 (rif. [10]).

Per i termini definiti dalle suddette disposizioni, si rimanda alle definizioni in esse stabilite.

Qualora, all'interno del documento, venga riscontrata la presenza di termini o acronimi non ricompresi nelle seguenti definizioni, dovrà attribuirsi alle stesse il significato proprio secondo la normativa applicabile.

Adesione
Recepimento del framework SPID da parte di entità di certificazione o di fornitori di servizi in rete.

Aggregatori di servizi SPID
sono pubbliche amministrazioni o privati che offrono a terzi (soggetti aggregati) la possibilità di rendere accessibili tramite lo SPID i rispettivi servizi, svolgendo per il soggetto aggregato la funzione di autenticazione con SPID.

AgID (o anche "Agenzia", ex DigitPA)
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 qualificati
Le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.

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
Disposizione di garanzia sull'identità dell'entità (ISO/IEC 18014-2).

Autenticazione multi-fattore
Autenticazione con almeno due fattori di autenticazione indipendenti (ISO/IEC 19790).

Autorizzazione
Disposizione di garanzia sull'identità dell'entità (ISO/IEC 18014-2).

CIE
Carta d'Identità Elettronica.

CNS
Carta Nazionale dei Servizi.

Codice identificativo
Il particolare attributo assegnato dal gestore dell'identità digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID.

Confidenzialità
Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati.

Credenziale
Un insieme di dati presentati come evidenza dell'identità dichiarata/asserita o di un proprio diritto (ITU-T X.1252). In definitiva, 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.

D. Lgs
Decreto Legislativo.

Dato personale
Si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" (art. 4, lett. b, del Codice della Privacy - Dlgs 196/2003).

Dati sensibili
Sono quei "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. 4, lett. d, del Codice della Privacy - Dlgs 196/2003).

Dati giudiziari
Sono "i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale" (art. 4, lett. e, del Codice della Privacy - Dlgs 196/2003).

Disponibilità
Accertarsi che gli utenti autorizzati abbiano accesso all'informazione e alle attività associate quando richiesto.

Distributore o Rivenditore che funge da Ufficio di Registrazione
Persona Giuridica che si impegna a compiere le preliminari operazioni di raccolta dei dati relativi ai richiedenti le credenziali SPID, la loro identificazione nonché il successivo eventuale rilascio delle medesime credenziali, nel pieno rispetto degli obblighi definiti dalla Convenzione sottoposta dall'IdP e successivamente sottoscritta.

Definizione del rischio
Processo di individuazione, riconoscimento e descrizione del rischio.

Entità
Può essere una persona fisica o un soggetto giuridico.

Evidenza informatica
Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

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 [SP]
Il Fornitore di Servizi (Service Provider - SP) erogano servizi agli utenti attraverso sistemi informativi accessibili in rete mediante l'identità digitale SPID. 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.

Gestione del rischio
Attività coordinate per dirigere e controllare una organizzazione in merito al rischio o ai rischi esistenti.

Gestori dell'Identità Digitale
È il gestore dell'identità digitale di cui alla lett. l) dell'art. 1 del DPCM.
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.
Nel presente documento è TeamSystem S.p.A. (nel seguito Teamsystem), nella sua qualità di Gestore dell'Identità SPID accreditato presso l'AgID.

Gestori di attributi qualificati
I soggetti accreditati ai sensi dell'art. 16 del DPCM, che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.

Hardware Security Module [HSM]
È un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.

Identificazione informatica
L'identificazione di cui all'art. 1 co. 1 lett. u-ter) del Decreti legislativo 7 marzo 2005 n. 82 (CAD)

Identità digitale [ID]
La rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al DPCM e dei suoi regolamenti attuativi.

Identity Provider [IDP]
Vedi Gestori dell'Identità Digitale.

IETF - Internet Engineering Task Force
Una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

Incaricato alla Registrazione [IR]
Persona fisica o giuridica cui è affidato lo svolgimento delle attività di identificazione dell'Utente e registrazione dei dati identificativi. Gli Incaricati alla Registrazione operano sulla base delle istruzioni ricevute dall'IdP con il quale hanno stipulato apposita Convenzione, oppure hanno sotto scritto apposito mandato con il RAO su modello proposto dall'IdP stesso.

Integrità
Salvaguardia dell'esattezza e della completezza dei dati e delle modalità di processo.

Intermediario Finanziario
Entità soggetta alla vigilanza di Banca d'Italia che ha l'obbligo di identificare i propri clienti ai sensi della normativa antiriciclaggio in ossequio a quanto previsto dal D.Lgs 231/2007.

Intestatario della fattura
Persona fisica o giuridica cui è emessa la fattura relativa al servizio di emissione dell'identità digitale attribuita al Titolare. Può coincidere con l'Utente Titolare e/o con il Richiedente.

IR
Vedi Incaricato alla Registrazione

ISO - International Organization for Standardization
Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union
Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

Manuale Operativo
Il Manuale Operativo definisce le procedure che l'IdP applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Autorità di vigilanza e quelle della letteratura internazionale.

One-Time Password - OTP
Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Titolare in un momento immediatamente

antecedente all'utilizzo delle credenziali SPID di livello 2. Può essere basata su dispositivi hardware o su procedure software.

OTP
Vedi One-Time Password ossia in senso generale i mezzi per l'autenticazione multi-fattore, quali codici temporanei, QR-code temporanei o accesso con verifica biometrica.

Parte interessata
Persona o organizzazione che può influenzare o essere influenzata da una decisione o un'attività.

Persona Fisica
Soggetto dotato di capacità giuridica.

Persona Giuridica
Organismo unitario, caratterizzato da una pluralità di individui o da un complesso di beni, al quale viene riconosciuta dal diritto capacità di agire in vista di scopi leciti e determinati.

PIN - Personal Identification Number
Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso.

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.

Pubblico ufficiale
Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

Registration Authority Officer [RAO o RA]
Soggetto o Operatore Incaricato del Gestore Teamsystem al riconoscimento del soggetto Richiedente e/o Titolare dell'identità SPID e alla registrazione degli attributi identificativi utili per il rilascio dell'identità digitale.

Registrazione
L'insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione previsti dal presente decreto e dai suoi regolamenti attuativi, è attribuita un'identità digitale a un utente, previa raccolta, verifica e certificazione degli attributi da parte del gestore dell'identità digitale, garantendo l'assegnazione e la consegna delle credenziali di accesso prescelte in modalità sicura.

Richiedente [Subscriber]
Persona fisica o giuridica che richiede una o più identità SPID da attribuire ai Titolari, sostenendone i costi. Può coincidere con l'Utente Titolare e/o con l'Intestatario della Fattura.

Riservatezza
Garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate.

SAML
Security Assertion Markup Language

Service Provider
Vedi Fornitore di Servizi

Sicurezza delle informazioni
Conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni; inoltre, possono essere coinvolte altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità.

Sistema
Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione.

SP
Service Provider - vedi Fornitore di 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.

Tempo Universale Coordinato [UTC]
Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5

Titolare o Utente Titolare
È il soggetto (persona fisica o giuridica) a cui è attribuita la titolarità dell'identità digitale SPID, ai sensi del art. 1 comma 1 lettera v) del DPCM. È il soggetto richiedente che deve essere identificato dall'IdP al fine del rilascio dell'identità digitale.

Trattamento del rischio
Processi di selezione e implementazione di attività volte a diminuire o comunque modificare il rischio presente.

Ufficio di Registrazione
Vedi Registration Authority Officer [RAO].

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.

1.3 Riferimenti normativi

[1] Regolamento Europeo UE 2016/679 del 27 aprile 2016 (General Data Protection Regulation - **GDPR**) relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali, pienamente vincolante dal 25 maggio 2018.

[2] Codice Privacy - D. Lgs 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali (G.U. N. 174 del 29 luglio 2003)", così come modificato dal D. Lgs 10 agosto 2018, n. 101.

[3] D. Lgs 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

[4] ISO-IEC 29115:2013 - Information technology - Security techniques - Entity authentication assurance framework: definisce un framework per la gestione la garanzia di autenticazione di un'entità in un dato contesto.

[5] Regolamento di esecuzione (UE) 2015/1502 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.

[6] Circolare Accredia DC N° 35/2016 – Schema di accreditamento degli Organismi di Certificazione, per il processo di certificazione degli operatori SPID, secondo le disposizioni dell'Agenzia per l'Italia Digitale (DC2016SSV439).

[7] **CAD** - Codice Amministrazione Digitale - D.lgs. 7 marzo 2005 n. 82 (G.U. n.112 del 16 maggio 2005) e s.m.i.

[8] 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 ("Regolamento eIDAS") (Gazzetta Ufficiale dell'Unione Europea – serie L257 del 28 agosto 2014).

[9] ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[10] DPCM del 24 ottobre 2014 (pubblicato in GU Serie Generale n.285 del 9-12-2014): Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. Referenziato nel seguito come **DPCM**.

[11] Determinazione n. 44 del 28 luglio 2015 - Emanazione dei regolamenti SPID previsti dall'art. 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014.

[12] 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).

[13] Regolamento AgID recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014) (di seguito "Regolamento SPID di AgID").

[14] Regolamento recante le regole tecniche per il gestore dell'identità digitale (articolo 4, comma 2, DPCM 24 ottobre 2014).

[15] Regolamento recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM del 24 ottobre 2014.

[16] Avvisi AgID, che contengono specificazioni, chiarimenti, note informative e casi esemplificativi dei Regolamenti SPID già emanati dall'AgID ed hanno un carattere cogente che ne comporta l'obbligo di applicazione da parte degli attori convolti nel Sistema SPID. Gli avvisi sono pubblicati nell'apposita sezione del sito istituzionale di AgID al seguente path https://www.agid.gov.it/it/piattaforme/spid/avvisi-spid.

2. DATI IDENTIFICATIVI

2.1 Dati identificativi del Gestore

I dati identificativi dell'Organizzazione sono i seguenti:
Ragione Sociale: TeamSystem SpA
Partita Iva: 01035310414
N° iscrizione al Registro delle imprese: N° REA: Pesaro 103483
Sede legale e Operativa: Via Sandro Pertini, 88 - 61122 PESARO (PU)
E-mail: amministrazione@teamsystem.com
PEC: teamsystemgroup@pecteamsystem.com
Sito web generale (informativo ITA/ENG): www.teamsystem.com/
Sito web dedicato al servizio IDP: www.teamsystem.com/store/firma-digitale/spid/

2.2 Dati identificativi della versione del Manuale

Il presente documento pubblico, chiamato "MANUALE OPERATIVO SPID Servizio di Gestione Sistema Pubblico dell'Identità Digitale di TeamSystem S.p.A." o anche "Manuale Operativo", è consultabile sul sito web del gestore TeamSystem SPA all' indirizzo: www.teamsystem.com/store/firma-digitale/spid/.
La versione aggiornata del presente documento è pubblicata ed è consultabile sul sito web dedicato: www.teamsystem.com/store/firma-digitale/spid/ e sul sito web di AgiD.

2.3 Responsabile del Manuale Operativo

TeamSystem è responsabile del Manuale Operativo e cura gli aggiornamenti e la pubblicazione del presente documento.
Eventuali comunicazioni possono essere inviate alla cortese attenzione di

TeamSystem S.p.A.
Responsabile del Manuale Operativo
Indirizzo: https://www.teamsystem.com/
Fax +39 0721 400502
Tel. +39 0721 42661
E-mail: amministrazione@teamsystem.com
PEC: teamsystemgroup@pecteamsystem.com
Sito web dedicato al servizio IDP: www.teamsystem.com/store/firma-digitale/spid/

2.4 Certificazioni

Le procedure operative descritte in questo Manuale Operativo, così come ogni altra attività del Gestore, sono conformi agli standard di riferimento.
Inoltre, TeamSystem è in possesso delle seguenti certificazioni

- **ISO 9001 [Sistema di gestione per la qualità]**
  - Scopo: Progettazione, sviluppo e assistenza di prodotti software - Erogazione di servizi di formazione. Progettazione e erogazione di servizi volti alla elaborazione dati per la gestione del personale. Erogazione di servizi volti alla elaborazione dati per la gestione contabile,

alla fatturazione elettronica, alla conservazione in cloud dei documenti e al trasferimento elettronico dei dati.
  - Progettazione, sviluppo, erogazione ed assistenza per il Servizio Pubblico di Identità Digitale (SPID)

- **ISO/IEC 27001** [Sistema di gestione della sicurezza delle informazioni]
  - Erogazione dei servizi di progettazione e gestione dell'infrastruttura ICT, di gestione delle applicazioni interne al Gruppo e di gestione dell'infrastruttura Cloud (IaaS) in accordo con la Dichiarazione di Applicabilità vers.3.1 dd02 aprile 2019
  - Erogazione ed assistenza per il Servizio Pubblico di Identità Digitale (SPID)

3. OBBLIGHI E RESPONSABILITÀ

In questa sezione vengono, sulla base della normativa vigente applicabile, descritti gli obblighi e responsabilità:

- di TeamSystem S.p.A., relativamente alla propria attività di Gestore delle Identità Digitali SPID;
- del Titolare dell'Identità Digitale SPID, relativamente alla richiesta e all'utilizzo dell'Identità Digitale rilasciata dal Gestore.

3.1 Obblighi e responsabilità del Gestore (idP)

TeamSystem S.p.A opera in qualità di Gestore delle Identità Digitali SPID.
Pertanto, ai sensi della normativa vigente applicabile (art. 1, 7, 8 e 11 del DPCM) si fa carico di:

- Gestire i processi relativi al ciclo di vita dell'identità digitale e al rilascio delle credenziali in ottemperanza al DPCM, alle Regole Tecniche emanate da AgID e alla normativa applicabile vigente alla data di stesura del presente manuale Operativo;
- Rilasciare l'identità digitale su domanda del Titolare, acquisendo la relativa richiesta (pervenuta mediante la modulistica opportunamente redatta e messa a disposizione del Titolare);
- Verificare opportunamente, prima del rilascio dell'identità digitale, l'identità del Titolare;
- Conservare per venti anni (a decorrere dalla scadenza o revoca dell'identità digitale) i seguenti dati:
    - copia (immagine o scansione) del documento di identità del Titolare (acquisita in fase di verifica dell'identità);
    - copia (immagine o scansione) del tesserino del codice fiscale oppure della tessera sanitaria del Titolare (acquisita in fase di verifica dell'identità)
    - originale del modulo di adesione allo SPID
    - copia del log della transazione, nel caso in cui l'identificazione del Titolare avvenga tramite l'utilizzo di documenti digitali di identità (CIE, CNS o TS-CNS), altra identità digitale SPID in possesso del Titolare o altra identificazione informatica autorizzata;
    - modulo di adesione sottoscritto con firma elettronica qualificata o digitale, in caso di identificazione tramite firma digitale;
    - le informazioni di registrazione, nonché l'esplicita volontà del soggetto di dotarsi di identità digitale SPID, memorizzate in specifici file audio/video, immagini e metadati strutturati in formato elettronico, in caso di identificazione de visu da remoto:
- Consegnare in modalità sicura le credenziali di accesso all'utente;
- Verificare gli attributi identificativi del Titolare;
- Cancellare la documentazione raccolta per il rilascio dell'identità trascorsi venti anni dalla scadenza o revoca dell'identità digitale;
- Effettuare il trattamento dei dati personali nel rispetto del Regolamento in materia di protezione dei dati personali;
- Attenersi alle misure di sicurezza previste dal Regolamento in materia di protezione dei dati personali e alle indicazioni fornite nell'informativa pubblicata sul sito www.teamsystem.com/store/firma-digitale/spid/;
- Informare tempestivamente AgID e il Garante per la Protezione dei Dati Personali in caso di accertata violazione dei dati personali;
- Verificare e aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione;

- Verificare la provenienza della richiesta di sospensione da parte del Titolare, nel caso in cui questa non risulti inviata via PEC o sottoscritta con firma elettronica qualificata o digitale;
- Fornire al Titolare la conferma della ricezione della richiesta di sospensione o di revoca dell'identità;
- Effettuare tempestivamente e a titolo gratuito la sospensione (per massimo 30 giorni) o la revoca di una identità digitale su richiesta del legittimo Titolare, ovvero la modifica degli attributi secondari e delle credenziali di accesso;
- Revocare l'identità digitale quando se ne riscontra l'inattività per un periodo superiore a 24 mesi, per scadenza del contratto o in caso di accertato decesso della persona fisica o dell'estinzione della persona giuridica, ovvero per sospetti di abusi o falsificazioni o su provvedimento dell'AgID;
- Ripristinare o revocare l'identità digitale sospesa se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte del Titolare;
- Ripristinare l'identità digitale sospesa nel caso non si riceva, entro 30 giorni dalla sospensione, copia della denuncia presentata all'autorità giudiziaria, per gli stessi fatti su cui è basata la richiesta di sospensione;
- Revocare l'identità digitale sospesa, nel caso non si riceva dal Titolare copia della denuncia presentata all'autorità giudiziaria;
- Segnalare, su richiesta del Titolare, ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi a uno degli attributi secondari indicati dallo stesso;
- In prossimità della scadenza dell'identità digitale, comunicarla al Titolare e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva, e alla revoca di quella scaduta;
- Utilizzare sistemi affidabili che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti a livello internazionale;
- Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso
- Proteggere le credenziali dell'identità digitale contro abusi e utilizzi non autorizzati, adottando le misure richieste dalla normativa,
- Definire, aggiornare e trasmettere a AgID il piano per la sicurezza del servizio SPID;
- Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato;
- Garantire la gestione sicura delle componenti riservate delle identità digitali, assicurando che non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata;
- Non mantenere alcuna sessione di autenticazione con l'utente in caso di utilizzo di credenziali SPID di livello 2;
- Effettuare un monitoraggio continuo, al fine di rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità di ciascun utente, procedendo alla sospensione della stessa in caso di attività sospetta;
- In caso di guasto o upgrade tecnologico, provvedere tempestivamente alla creazione di una credenziale nuova sostitutiva e alla revoca di quella sostituita;
- Effettuare, con cadenza almeno annuale, un'analisi dei rischi;
- 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 una apposita struttura interna all'Organizzazione;
- Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle

disposizioni previste dalla normativa, assicurando l'adeguamento in seguito all'aggiornamento della normativa;
- Sottoporsi, con cadenza almeno biennale, a una verifica di conformità alle disposizioni vigenti;
- Inviare all'AgID in forma aggregata i dati richiesti, a fini statistici;
- Tenere il Registro delle Transazioni, contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, integrità e inalterabilità e adottando idonee misure di sicurezza, oltre ad utilizzare meccanismi di cifratura;
- In caso di cessazione dell'attività, comunicarlo all'Agenzia e ai Titolari almeno 30 giorni prima, indicando gli eventuali gestori sostitutivi ovvero segnalando la necessità di revocare le identità digitali rilasciate. Revocare le identità rilasciate per le quali non si abbia avuto subentro;
- In caso di subentro a un gestore cessato, gestire le identità digitali prese in carico, conservandone le relative informazioni;
- Informare espressamente il Titolare in modo compiuto e chiaro sugli obblighi che assume, in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi.

3.2 Obblighi dei Titolari

Il **Titolare** dell'Identità Digitale è tenuto a adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (Art.32, comma 1 del CAD).

Il Titolare deve inoltre:
- Se richiesto dell'IdP, esibire i documenti necessari per l'emissione e gestione dell'identità digitale e delle credenziali connesse;
- Fornire all'atto dell'identificazione e della registrazione esclusivamente dati e documenti corretti e veritieri; in caso contrario (vale a dire in caso di dichiarazioni infedeli o mendaci) si assume le responsabilità previste dalla legislazione vigente;
- Verificare la correttezza dei dati registrati dall'IdP al momento dell'adesione, ed eventualmente segnalare tempestivamente inesattezze negli stessi;
- Comunicare tempestivamente all'IdP ogni variazione degli attributi;
- Mantenere aggiornati i contenuti dei seguenti attributi identificativi:
  - nel caso di *persona fisica*: estremi e immagine del documento di riconoscimento e relativa scadenza, numero di telefono (fisso o cellulare), email, domicilio fisico e digitale;
  - nel caso di *persona giuridica*: indirizzo sede legale, codice fiscale o partita IVA se uguale, rappresentante legale della società, numero di telefono (fisso o cellulare), email, domicilio fisico e digitale;
- Impiegare in via esclusivamente personale le credenziali connesse all'Identità Digitale, per le finalità specifiche per cui esse sono rilasciate (autenticazione informatica nello SPID), assumendo ogni eventuale responsabilità in caso di diverso utilizzo delle stesse;
- Non utilizzare le credenziali in maniera tale da creare danni alla rete e più in generale a terzi;
- Non violare leggi e regolamenti;
- Impiegare le dovute misure tecnico/organizzative volte a evitare danni a terzi;
- Custodire e conservare con la massima diligenza e sotto il proprio controllo esclusivo
  - le credenziali segrete utilizzate per l'accesso,
  - gli eventuali dispositivi su cui sono trasmesse le OTP,
  - le OTP stesse,

al fine di garantirne l'integrità e la riservatezza;
- Non violare diritti d'autore, marchi, brevetti o altri diritti derivanti da legge;
- Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali connesse all'Identità e chiedere immediatamente all'IdP la sospensione delle stesse;
- Assicurarsi dell'autenticità del Fornitore di servizi o del Gestore dell'Identità, nel momento in cui viene richiesto di utilizzare l'identità digitale;
- Nel caso in cui il Titolare conferma la volontà di accedere al servizio, è consapevole di autorizzare il Gestore a trasferire gli attributi dichiarati dal servizio al Fornitore del Servizio individuale o Aggregatore.
- Attenersi alle indicazioni fornite dal Gestore in merito a:
  - uso del sistema di autenticazione;
  - richiesta di sospensione o revoca dell'identità digitale
  - cautele da adottare per la conservazione e protezione delle credenziali;
- Chiedere immediatamente al Gestore la sospensione delle credenziali, in caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un soggetto terzo.

3.3 Obblighi dei richiedenti

Il **Richiedente,** che richiede il rilascio delle identità digitali, è tenuto ad attenersi a quanto disposto dal presente Manuale Operativo, di cui deve aver preso visione, e a tutte le istruzioni, le specifiche funzionali e le procedure indicate da Teamsystem sulla piattaforma www.teamsystem.com/store/firma-digitale/spid/ dedicata al servizio di Gestore SPID.

3.4 Tutela dei dati personali

Salvo espresso consenso, le informazioni relative al Titolare e al Richiedente (di cui il Gestore entra in possesso nell'esercizio della sua attività) sono da considerarsi riservate e non pubblicabili, ad eccezione di quelle esplicitamente destinate ad uso pubblico (in conformità alla normativa applicabile).
Tutti i personali vengono trattati dal Gestore in conformità al Regolamento Europeo 2016/679 (GDPR).

3.5 Risoluzione ai sensi dell'art. 1456 cc

L'inadempimento da parte del Richiedente o del Titolare degli obblighi descritti in questa sezione costituisce, ai sensi dell'art. 1456 c.c., inadempimento essenziale e pertanto mette il Gestore dell'Identità nella posizione di risolvere il contratto stipulato con suddetti soggetti.
La risoluzione opererà di diritto al semplice ricevimento di una comunicazione, inviata dal Gestore a mezzo raccomandata A.R. o posta elettronica certificata, contenente la contestazione dell'inadempienza e l'intendimento di avvalersi della risoluzione stessa.

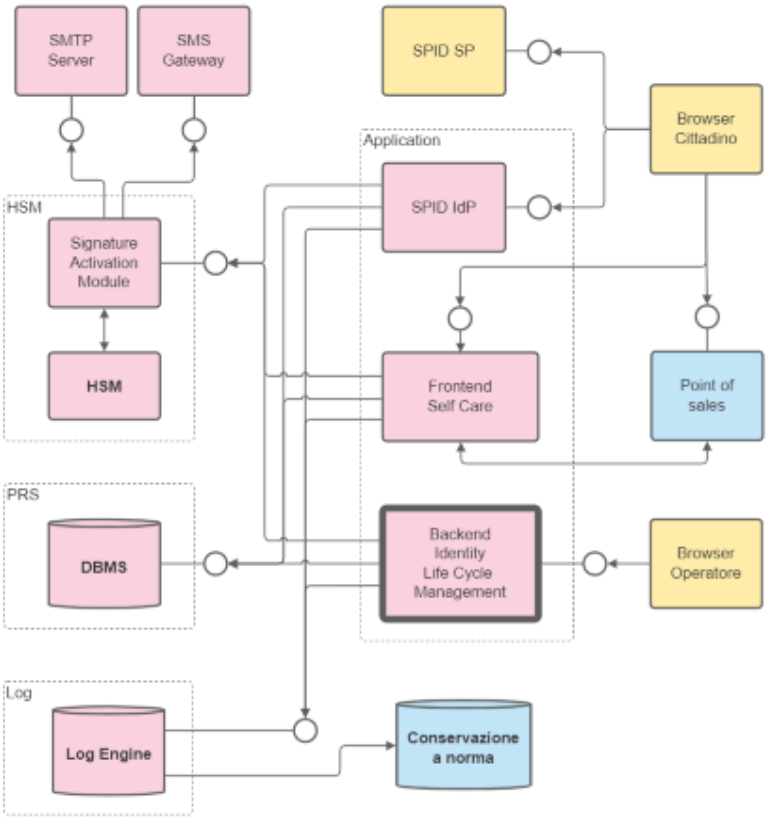
4. DESCRIZIONE DELL'ARCHITETTURA

4.1 Architettura di dispiegamento

La descrizione dell'architettura di dispiegamento è contenuta all'interno del piano della Sicurezza predisposto dal Gestore di Identità TeamSystem.

4.2 Architettura applicativa

In questa sezione si procede con la descrizione dell'architettura applicativa del sistema di gestione delle identità digitali SPID.
L'architettura applicativa del Gestore di Identità TeamSystem è composta da diverse componenti, che vengono rappresentate nel diagramma a seguire insieme agli attori principali coinvolti nel sistema di gestione delle identità digitali SPID:



Per una maggiore comprensione del diagramma, si riporta a seguire una descrizione sintetica delle componenti principali:

- **SPID IdP**: componente preposta alla ricezione delle richieste di autenticazione da parte dei Service Provider, mediante protocollo SAML v2.0
  È l'elemento che consente l'inserimento delle credenziali dell'utente, la relativa verifica, e ad autenticazione avvenuta invia l'asserzione al Service Provider, comunicando l'esito dell'autenticazione e gli attributi dell'utente.
- **Backend Identity Life Cycle Manager**: componente che cura il processo di identificazione

dell'utente, la generazione delle credenziali, la gestione del ciclo di vita degli utenti. Gestisce anche le sedi operative, i punti/autorità di registrazione e relativi operatori.

- **Frontend Self Care**: portale che espone ai titolari funzionalità per la gestione in self-service del ciclo di vita dell'identità.
- **Log Engine**: centralizzatore dei log provenienti dalle varie applicazioni che compongono l'architettura applicativa.
- **Authenticator Level 1/2 Manager**: modulo che realizza le specifiche di autenticazione SPID Livello 1 e 2. TeamSystem rende disponibile al Titolare i seguenti metodi di autenticazione denominati:
    - Basic Authentication (Livello SPID 1, LoA 2);
    - OTP via SMS/applicazione mobile (Livello SPID 2, LoA 3).

5. CICLO DI VITA DELLE IDENTITÀ DIGITALI SPID

5.1 Identificazione e rilascio dell'identità digitale

Il Gestore di Identità Digitali deve verificare con assoluta certezza l'identità del soggetto Richiedente alla prima richiesta di rilascio di un'Identità Digitale SPID, al fine di prevenire furti d'identità.
Tali operazioni sono svolte dall'IdP stesso o dai soggetti da lui delegati, in ottemperanza con quanto previsto dalla vigente normativa e secondo le modalità descritte nel seguito, il quale provvede all'identificazione degli utenti e all'emissione delle identità SPID.

Per i successivi rinnovi (nel caso di credenziali soggette a scadenza), sarà cura del soggetto Titolare mantenere aggiornati i propri dati e documenti, sulla pagina personale messa a disposizione su portale dedicato dal Gestore di Identità Digitali.

Nei paragrafi che seguono sono riportate le modalità di identificazione che l'IdP TeamSystem adotta nel il rilascio delle identità digitali SPID per persona fisica (SPID 1), SPID per la persona giuridica (SPID di tipo 2), SPID per la persona fisica ad uso professionale (SPID di tipo 3), e SPID per la persona giuridica ad uso professionale (SPID di tipo 4).

5.1.1 Registrazione del soggetto Richiedente

Nel caso in cui il soggetto Richiedente sia **una persona fisica** (Spid di tipo 1 per l'uso personale e 3 per l'uso professionale), i seguenti dati di registrazione sono necessari al rilascio dell'Identità SPID:

- Nome e Cognome;
- Data di nascita;
- Comune o stato estero di nascita;
- Codice fiscale;
- Sesso;
- Estremi del documento d'identità esibito;
- Estremi del Tesserino Sanitario.

Nel caso in cui il soggetto Richiedente sia invece **una persona giuridica**, è necessario fornire le seguenti informazioni:

- Denominazione/Ragione sociale della persona giuridica (organizzazione);
- Codice fiscale o Partita IVA (se uguale al C.F.) della persona giuridica (organizzazione);
- Sede legale della persona giuridica (organizzazione);
- Visura camerale (in alternativa atto notarile di procura legale) per attestare lo stato di rappresentante legale del richiedente l'identità per conto della persona giuridica (organizzazione);
- Estremi del documento di identità presentato dal rappresentante legale, per lo SPID di tipo 2;
- Estremi del Tesserino Sanitario presentato dal rappresentante legale, per lo SPID di tipo 2;
- In caso di richiesta di identità SPID per persona giuridica ad uso professionale (SPID di tipo 4), documento che attesti l'appartenenza del dipendente/collaboratore alla persona giuridica cui l'identità SPID farà riferimento;
- Estremi del documento di identità del dipendente/collaboratore a cui l'organizzazione intende richiedere il rilascio dello SPID di tipo 4;
- Estremi del Tesserino Sanitario del dipendente/collaboratore a cui l'organizzazione intende

richiedere il rilascio dello SPID di tipo 4.

Si evidenzia che nel caso in cui il soggetto Richiedente sia invece una persona fisica all'atto di richiedere l'identità per la **persona giuridica ad uso professionale (SPID di tipo 4)**, è necessario fornire le evidenze atte a confermare la titolarità a poter richiedere l'identità digitale per la persona giuridica (attestazione dell'organizzazione della persona giuridica)

In ogni caso, dovranno essere forniti al Gestore dell'Identità Digitale i seguenti attributi secondari:

- Numero di telefonia mobile;
- Indirizzo e-mail.

Tali attributi sono verificati dall'IdP nel corso del processo di identificazione, inviando un messaggio di posta all'indirizzo e-mail indicato contenente una URL (link) per la verifica e, al numero di telefonia mobile indicato, una OTP numerica di controllo, che va riportata in fase di identificazione.

Potranno infine essere richiesti dallo stesso Gestore:

- Domicilio fisico e/o digitale;
- Eventuali altri attributi individuati dall'AgID, funzionali alle necessarie comunicazioni.

Procedura per l'eventuale recupero del numero di telefonia mobile connesso all'Identità SPID

Il telefono cellulare costituisce un fattore di autenticazione in ambito SPID. Ad ogni modo, è possibile che si verifichi il caso per cui lo stesso numero di telefonia mobile sia già in uso per una diversa identità digitale nell'ambito dello stesso Identity Provider SPID.

Per evitare che si verifichi tale inconveniente, TeamSystem ha predisposto la seguente procedura applicabile nei casi di

- iscrizione al servizio,
- modifica del numero di telefonia mobile associato all'identità SPID dell'utente Titolare.

In caso di inserimento di un numero di telefonia mobile già utilizzato per un'altra identità digitale SPID, viene mostrato un messaggio di errore ad indicare all'utente la non disponibilità del numero stesso.

Nel caso egli volesse quindi rivendicarne la proprietà, dovrà contattare il servizio di Help Desk dell'IdP TeamSystem.

In tal caso, il flusso di comunicazioni/verifiche attuato è il seguente:

- Il richiedente apre un ticket presso l'Help Desk di TeamSystem, indicando il numero di telefonia mobile che risulta "non disponibile";
- L'ufficio SPID dell'IdP contatta quindi telefonicamente l'utente al numero di cellulare di cui rivendica il possesso, tramite due chiamate distinte e intervallate da un periodo compreso tra le 24 e le 48 ore.
- Allo stesso tempo, l'ufficio SPID dell'IdP effettua una verifica analoga, contattando via e-mail l'attuale assegnatario del numero di telefonia mobile, con l'invito a contattare l'Help Desk per verificare il possesso del numero o modificare lo stesso.

In base ai risultati ottenuti dal flusso descritto:

a. se l'attuale assegnatario dimostra di essere in possesso del numero di telefonia mobile in esame, la richiesta dell'utente che ne rivendicava il possesso viene di conseguenza rigettata.
b. se l'utente che effettua la richiesta dimostra invece di essere il possessore del numero di telefonia e l'attuale assegnatario non ha provveduto ad aggiornare lo stesso o a dimostrarne il possesso, si sospende l'identità digitale dell'attuale assegnatario. Trascorsi poi quindici giorni, in assenza di ulteriori contatti, si procede con la revoca dell'Identità SPID dello stesso.

5.1.2 Identificazione del soggetto Richiedente

Vengono descritte di seguito le modalità di identificazione del Richiedente previste dal Gestore di Identità Digitali TeamSystem.

Identificazione "de visu"

L'attività di identificazione "***de visu" (a vista) in presenza fisica*** del soggetto Richiedente viene effettuata:

a) dal Gestore di Identità Digitali, attraverso il personale preposto all'operazione presso gli uffici del Gestore stesso;
b) dalle Registration Authority o Uffici di Registrazione (RAO) di cui l'Identity Provider si avvale sul territorio nazionale, mediante i propri Incaricati alla Registrazione IR.

La persona che fa richiesta di rilascio dell'Identità Digitale comunica all'Incaricato alla Registrazione nominato dall'IdP TeamSystem la volontà di richiedere un'identità SPID ad uso privato o professionale, a seguito di tale scelta la persona viene identificata con certezza e viene inoltre archiviata la fotocopia di almeno un documento di identità ufficiale valido per lo Stato di appartenenza e della tessera sanitaria o del codice fiscale.

In caso il Richiedente sia una persona giuridica, oltre al documento, verrà altresì raccolta la visura camerale o una procura che attesti lo stato di rappresentante legale, per conto della società, al soggetto che sottoscrive e presenta la richiesta. In caso di richiesta di identità SPID per persona giuridica uso professionale (SPID di tipo 4), l'organizzazione dovrà produrre un documento che attesti l'appartenenza del soggetto medesimo alla persona giuridica cui l'identità SPID farà riferimento.

Saranno gli Operatori IR ad accertare l'Identità del Richiedente tramite la verifica della validità del documento di identità, della presenza sullo stesso di una foto e di una firma autografa, e che sia inoltre valido il codice fiscale mediante la verifica della tessera sanitaria o del codice fiscale.

Gli operatori IR potranno non accettare i documenti presentati se questi risultassero carenti delle caratteristiche indicate sopra, sospendendo il processo di iscrizione fino al momento in cui non verranno presentati documenti integri e validi.

Identificazione de visu da remoto

L'attività di identificazione ***a vista da remoto*** permette di avviare il processo di emissione dell'Identità Digitale SPID anche in quei casi in cui non sia possibile ottenere la presenza fisica di entrambe le parti (soggetto Richiedente e Personale del Gestore di Identità Digitali) per procedere con il riconoscimento a vista del richiedente.

Il servizio di identificazione de visu da remoto verrà gestito come descritto di seguito:

1) Il Richiedente, attraverso un dispositivo desktop o mobile (PC, smartphone o tablet) abilitato ad una connessione Internet e dotato di una webcam e di un sistema audio correttamente funzionante, si connette al sito del Gestore TeamSystem, dove vengono riportate tutte le istruzioni necessarie per eseguire gli step successivi e dove sono inoltre indicati i documenti necessari per la sua identificazione.
   Prima dell'avvio della registrazione della sessione video, l'operatore TeamSystem è tenuto a chiedere esplicitamente al Richiedente la conferma della sua volontà di procedere con la registrazione. In assenza di questo consenso, la sessione di riconoscimento deve essere interrotta.
   A tal proposito, è **fondamentale** la buona qualità del collegamento audio-video, per far sì che la procedura di identificazione possa essere effettuata con successo; nel caso, infatti, in cui si verificassero disturbi sulla linea e/o problemi che non rendessero possibile la verifica dell'identità del Richiedente con certezza, l'operatore dell'IdP **interromperà la sessione in corso**, invitando il soggetto Richiedente a fissare un successivo nuovo appuntamento, una volta risolti i problemi che sono stati riscontrati.

2) Il soggetto Richiedente compila sul sito un form, in cui è previsto vengano inserite tutte le informazioni utili al rilascio dell'Identità Digitale SPID;

3) Compilato il form, viene richiesto al soggetto Richiedente di:
   a. effettuare l'upload delle scansioni fronte/retro del proprio documento di identità (carta d'identità, patente, passaporto) in corso di validità;
   b. effettuare l'upload delle scansioni fronte/retro della Tessera Sanitaria.

4) Ultimata la fase di inserimento dati e upload delle scansioni dei documenti sarà possibile avviare la sessione di video-comunicazione remota, tramite funzionalità rese disponibili sul sito del Gestore;

5) Durante il processo di video-comunicazione l'operatore:
   - sarà libero di rifiutare la registrazione, nel caso emergano dubbi anche soggettivi circa l'effettiva identità del soggetto;
   - potrà chiedere all'utente, durante la registrazione, di compiere azioni estemporanee al fine di accertare la presenza reale alla postazione remota del Richiedente;
   - effettuerà le verifiche opportune per accertare la veridicità delle informazioni e dei documenti forniti dal Richiedente, ricorrendo, peraltro, a verifiche su fonti autoritative istituzionali, così come descritte al par. 5.1.3.

6) Al termine della sessione, i dati di registrazione costituiti da file audio-video, immagini e metadati strutturati in formato elettronico, vengono conservati e trattati in base a quanto previsto dalla normativa applicabile.

L'intera sessione è registrata in modalità audio e video, la registrazione della sessione deve necessariamente essere di qualità buona, con immagine a colori, riprese con definizione chiara e a fuoco, luminosità e contrasto adeguati, ripresa del testo eventualmente inquadrato correttamente distinguibile. Inoltre, l'intera sessione deve necessariamente essere fluente e continua, senza alcuna interruzione.

Identificazione informatica tramite CNS
In questo caso, l'identificazione avviene tramite verifica dei documenti digitali che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, come la tessera sanitaria-carta nazionale dei servizi (TS-CNS), la carta CNS o carte ad essa conformi.

Il gestore dell'identità digitale deve garantire che la richiesta di rilascio dell'identità digitale sia riconducibile all'utilizzo degli strumenti di cui al presente articolo, conservando la prova dell'identificazione avvenuta mediante CNS.

Identificazione informatica tramite firma elettronica qualificata o firma digitale
In questo caso si procede con l'acquisizione del modulo di richiesta di adesione in formato digitale, messo a disposizione in rete dal gestore dell'identità digitale, compilato e sottoscritto con firma elettronica qualificata o con firma digitale. L'identificazione avviene tramite la verifica della firma elettronica qualificata o firma digitale apposta sulla richiesta. Anche in questo caso il gestore delle identità digitali, considera che la fase di identificazione sia stata correttamente espletata dal fornitore di firma elettronica qualificata o digitale.

5.1.3 Verifica dell'identità dichiarata dal soggetto Richiedente

La verifica dell'identità dichiarata rafforza il livello di attendibilità degli attributi di identità raccolti in fase di identificazione e viene compiuta attraverso accertamenti effettuati tramite fonti autoritative istituzionali, in grado di confermare della veridicità dei dati raccolti.
L'IdP si avvale quindi di servizi di verifica del codice fiscale e dei dati anagrafici forniti da fonti autoritative.
Il personale preposto alla verifica dell'identità del soggetto Richiedente si connette al servizio di verifica dell'anagrafica e confronta le informazioni fornite dal soggetto Richiedente con quelle memorizzate negli archivi pubblici.
In particolare, l'operatore IR preposto alla verifica dell'identità del soggetto Richiedente può utilizzare i seguenti servizi:

- Servizio di verifica del codice fiscale (Agenzia Entrate): https://telematici.agenziaentrate.gov.it/VerificaCF/Scegli.jsp
- Servizio di verifica della partita IVA (Agenzia Entrate): https://telematici.agenziaentrate.gov.it/VerificaPIVA/Scegli.jsp
- Verifica e corrispondenza tra il codice fiscale e i dati anagrafici di una persona fisica (Agenzia Entrate): https://telematici.agenziaentrate.gov.it/VerificaCF/Scegli.do?parameter=verificaCfPf
- Servizio di verifica dello status di documento smarrito o rubato (Ministero dell'Interno): https://crimnet.dcpc.interno.gov.it/crimnet/ricerca-documenti-rubati-smarriti

In merito al processo di verifica a seguito degli accessi alle fonti autoritative, l'Identity Provider conserva tutti i riscontri ottenuti.

Nel caso di Identità Digitale per **persona giuridica ad uso professionale** (Spid di tipo 4), viene verificata l'appartenenza della persona fisica (dipendente-collaboratore) alla richiesta di questo tipo di identità. Tale titolarità viene verificata mediante la raccolta del consenso mediante trasmissione, da parte della persona giuridica, di una attestazione firmata.
La trasmissione dell'attestazione dovrà essere protetta da meccanismi tali da garantire l'integrità e la provenienza dei dati inviati dalla persona giuridica.
Il meccanismo percorribile è rappresentato dal documento attestazione sigillato elettronicamente tramite Sigillo Elettronico Qualificato o firmato elettronicamente tramite Firma Elettronica Qualificata rilasciata al legale rappresentante della persona giuridica.

Nel caso in cui venga presentato dall'IR, mediante il portale del Gestore, la copia scansionata dell'attestazione sottoscritta con firma autografa dal rappresentante legale dell'organizzazione, è obbligo dell'Incaricato alla Registrazione e sua esclusiva responsabilità conservare per venti anni l'originale cartaceo ed esibirlo su richiesta.

5.1.4 Emissione dell'identità digitale SPID

Compiute con successo tutte le attività di identificazione e verifica previste dalle fasi precedenti, l'identità digitale SPID viene creata e rilasciata dall'Identity Provider.

La suddetta identità è costituita da:

- attributi identificativi, come specificato nel DPCM 24 ottobre 2014, comma 1, lettera c);
- attributi secondari, come specificato nel DPCM 24 ottobre 2014, comma 1, lettera d);
- codice identificativo, come specificato nel DPCM 24 ottobre 2014, comma 1, lettera d);
- identificativo utente Titolare.

Il codice identificativo, univoco in ambito SPID, viene assegnato dall'IdP ed è definito dalla regola:
<codice Identificativo> = <cod_IdP><nr. unico>,

dove:
• < *cod_IdP* >: codice di 4 lettere, ad identificare il Gestore di Identità Digitali;
• < *nr. unico* >: codice alfanumerico di 10 caratteri, univoco nel dominio dell'IdP.

5.1.5 Creazione delle credenziali SPID

Il processo di creazione delle credenziali SPID comprende le operazioni necessarie a dare origine ad una credenziale o ai mezzi per produzione della stessa, con metodi differenti a seconda del livello di sicurezza associato alla credenziale.

Creazione credenziali di Livello 1 SPID

In caso di livello 1 di credenziali *SPID* (corrispondente al Level Of Assurance 2 dello standard ISO-IEC 29115), il Gestore di Identità Digitali fornirà al soggetto Richiedente una credenziale a singolo fattore, in particolare costituita da una password.
Per ottenere password difficilmente attaccabili e di complessità elevata, si raccomanda di adottare almeno i seguenti accorgimenti:

- 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 speciale, ad es. #, $,% ecc.

Le password devono avere una durata massima non superiore a 180 giorni, con l'impossibilità di riutilizzo o di avere password simili prima di cinque variazioni e comunque non prima di diciotto mesi.

Il Gestore adotta una procedura di sollecito per invitare il Titolare a modificare la propria password, con frequenza periodica.

Creazione credenziali di Livello 2 SPID
In caso di livello 2 di credenziali SPID (corrispondente al Level Of Assicurance 3 dello standard ISO-IEC 29115), il Gestore fornirà al soggetto Richiedente una credenziale a singolo fattore, ossia una password, abbinata all'adozione di una OTP inviata al cellulare dell'utente.
Per la creazione della credenziale OTP, viene generato un seed segreto, dal quale viene calcolato di volta in volta il codice OTP temporaneo, attraverso le logiche di generazione proprie del sistema che viene adottato.
In particolare, il seed viene generato utilizzando una chiave base salvata su HSM e una chiave di derivazione specifica della singola OTP e ottenuta tramite hashing di quantità che caratterizzano il token OTP stesso.
Le due chiavi sono soggette ad un processo di derivazione e decimalizzazione attraverso algoritmi standard di generazione del segreto, ossia della quantità che è utilizzata per la generazione degli OTP e/o la verifica della loro validità.

5.1.6 Consegna delle credenziali SPID

La complessità del processo di consegna delle credenziali dipende dal livello di sicurezza SPID associato alle stesse. Tale consegna va operata con modalità e strumenti che assicurino che essa sia effettuata al destinatario legittimo, con criteri adeguati di riservatezza che ne salvaguardino il contenuto.
In ogni caso, l'Identity Provider garantisce che:

- il Richiedente, tramite una specifica informativa consegnata in fase di rilascio dell'Identità Digitale SPID, sia stato espressamente e chiaramente informato su:
  - obblighi assunti dallo stesso, riguardo alla protezione della segretezza delle credenziali;
  - procedura di autenticazione e requisiti tecnici necessari ad accedervi;
- il proprio sistema di sicurezza dei dati risponda alle misure di sicurezza relative al trattamento dei dati personali, secondo quanto previsto dal Regolamento (UE) 679/2016 (GDPR) [1].

Consegna credenziali Livello 1 SPID
In caso di livello 1 di sicurezza SPID, composto da una credenziale a singolo fattore (*password*), visto che in fase di richiesta di rilascio dell'Identità Digitale è il Richiedente a scegliere la password da adottare come credenziale SPID, il processo si considera concluso in automatico al termine del processo di rilascio dell'Identità Digitale.

Consegna credenziali Livello 2 SPID
In caso di livello 2 di sicurezza SPID (livello significativo), essendo questo costituito da una *password* e da una *One-Time Password*:

a) la password viene consegnata in maniera analoga a quanto descritto al paragrafo precedente per il livello 1;
b) la One-Time Password, inviata su un telefono cellulare, non prevede invece la consegna della credenziale al termine del processo di rilascio dell'Identità Digitale SPID. Tale momento è invece prorogato nel momento in cui la credenziale per l'accesso ad un servizio offerto da un Service Provider viene utilizzata, quando l'Identity Provider provvederà ad inviare al cellulare dell'utente la OTP per la sessione corrente.

5.1.7 Attivazione delle credenziali

L'attivazione delle credenziali SPID è il processo durante il quale le credenziali SPID, o i mezzi usati per produrle, vengono effettivamente rese operative e pronte all'uso.

Attivazione credenziali Livello 1 SPID

Le credenziali di livello 1 di sicurezza SPID, analogamente alla fase di consegna, non prevedono una fase di attivazione per loro natura, in quanto sono considerate già attive al momento del loro primo rilascio e in caso di riattivazione in seguito a sospensione.

Attivazione credenziali Livello 2 SPID

In caso di credenziali di livello 2 di sicurezza SPID:

- la password è soggetta alle stesse condizioni descritte al paragrafo precedente per il livello di sicurezza 1;
- per la One-Time Password, data la volatilità della credenziale, le fasi di prima attivazione e riattivazione in seguito a sospensione non vengono previste. Per definizione, infatti, la credenziale è valida solo per la sessione di autenticazione in corso, per cui è già attivata nel momento in cui viene inviata al cellulare del Richiedente.

5.1.8 Conservazione e registrazione dei documenti

Il processo di conservazione e registrazione dei documenti completa la fase di emissione di un'identità SPID ad un soggetto. La documentazione soggetta a conservazione include i documenti e le informazioni raccolte nel corso della registrazione.
Il Gestore, per poter documentare la corretta esecuzione di ogni processo precedenti, ne conserva i relativi riscontri.

In particolare, riguardo al processo di **richiesta e identificazione** del soggetto Richiedente, vanno conservati:

- In caso di identificazione da remoto tramite CNS/FEQ: copia di tutta la documentazione esibita (documento d'identità e codice fiscale per persone fisiche, visura per persone giuridiche) e modulo di richiesta elettronicamente sottoscritto;
- In caso di identificazione de visu da remoto: le informazioni di registrazione, nonché l'esplicita volontà del soggetto di dotarsi di identità digitale SPID, sono memorizzate in specifici file audio/video, immagini e metadati strutturati in formato elettronico. In particolare, la documentazione che verrà conservata comprenderà:
    - contratto di identità digitale sottoscritto;
    - scansione fronte/retro del documento di identità;
    - scansione fronte/retro del tesserino sanitario;
    - dichiarazione di riconoscimento firmata dall'IR;
    - streaming audiovideo della sessione di riconoscimento;
- In caso di identificazione de visu: copia di tutta la documentazione esibita (documento d'identità e codice fiscale per persone fisiche, visura per persone giuridiche) e modulo di richiesta cartaceo sottoscritto.

Riguardo al processo di **verifica**, vanno conservati i riscontri ottenuti per le operazioni di verifica, a seguito

degli accessi alle fonti autoritative.

Tutte le informazioni e i documenti indicati vengono conservati a norma per un periodo di venti anni:

- per la documentazione cartacea, essa viene conservata in ambiente protetto, nel rispetto della normativa vigente;
- per le informazioni in formato digitale, esse vengono inserite in un archivio informatico e conservate secondo le normative vigenti.

L'Identity Provider, su richiesta dell'utente, segnala via e-mail alla casella indicata dall'utente Titolare, ogni avvenuto utilizzo delle proprie credenziali di accesso.

5.2 Sospensione o revoca dell'identità digitale SPID

La **sospensione** è associata ad un processo di annullamento temporaneo delle credenziali SPID di un titolare.

La **revoca**, invece, è il processo che annulla definitivamente la validità delle credenziali del Titolare ed è disposta in caso di:

1) smarrimento, furto o altre compromissioni/danni (con formale denuncia, presentata dal Titolare all'autorità giudiziaria);
2) uso per scopi non autorizzati, fraudolenti o abusivi, da parte di un soggetto terzo;
3) rilascio di una nuova credenziale, in sostituzione di una già in possesso del Titolare;
4) rilascio di una nuova credenziale, in sostituzione di una del Titolare scaduta.

Nel caso 1), il Titolare deve richiedere immediatamente la sospensione/revoca delle credenziali. La richiesta dev'essere effettuata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata ed inviata agli estremi di contatto dell'Identity Provider.

L'IdP sospende tempestivamente l'identità SPID per un periodo massimo di trenta giorni, informando l'utente che ha effettuato la richiesta. In questo periodo, può accadere che:

a) il soggetto richiedente annulla la richiesta e quindi l'identità digitale viene ripristinata (ad es. in caso di ritrovamento);
b) il soggetto richiedente formalizza la richiesta, presentando una copia della denuncia che è stata presentata all'autorità giudiziaria: in questo caso, l'identità digitale SPID viene revocata.

In assenza di quanto riportato ai punti a) o b), l'identità SPID verrà ripristinata in automatico, scaduto il periodo di trenta giorni dalla data di presentazione della richiesta.

Nel caso 2), anche a seguito di segnalazioni effettuate ai sensi dell'articolo 8, comma 4, del DPCM [10], l'utente Titolare richiede la sospensione immediata dell'identità digitale all'Identity Provider.

Modalità di sospensione o revoca dell'Identità SPID

Ai sensi dell'articolo 8, comma 3 e dell'articolo 9 del DPCM [10], 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 documento identità.

Nel caso previsto dai punti 1 e 6, il gestore dell'identità digitale revoca di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca all'utente, con avvisi ripetuti (90, 30 e 10 giorni nonché il giorno precedente la revoca definitiva), utilizzando l'indirizzo di posta elettronica e il recapito di telefonia mobile (attributi secondari essenziali forniti per la comunicazione).
Nei casi previsti dai punti 2 e 3, il gestore dell'identità digitale procede alla revoca dell'identità digitale, previo accertamento operato anche utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM. In assenza di disponibilità dei predetti servizi, dovrà essere cura dei rappresentanti del soggetto utente (eredi o procuratore, amministrazione, società subentrante) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'identità digitale. Il gestore, una volta in possesso della documentazione suddetta, dovrà procedere tempestivamente alla revoca.

Nel caso previsto dal punto 7, il gestore dell'identità digitale sospende di propria iniziativa l'identità, mettendo in atto meccanismi con i quali comunica 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:
a) richiesta al Gestore inviata via PEC all'indirizzo uff_teamsystemspid@pecteamsystem.com;
b) richiesta, in formato elettronico e sottoscritta con firma digitale o elettronica, inviata tramite la casella PEC appositamente predisposta dal Gestore;
c) richiesta tramite portale web dedicato all'utente https://spid.teamsystem.com/.

Il Gestore deve fornire esplicita evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.
Contestualmente l'utente potrà richiedere al Fornitore dei servizi presso il quale ritiene che la propria identità sia stata utilizzata fraudolentemente il blocco all'accesso della propria identità inviando una richiesta in tal senso con le stesse modalità sopra previste ad una casella di posta appositamente predisposta dal fornitore di servizi.
Trascorsi trenta giorni dalla suddetta sospensione, il gestore provvede al ripristino dell'identità precedentemente sospesa qualora non riceva copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione. In caso contrario l'identità digitale viene ripristinata.

Nel caso previsto dal punto 5, l'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione o la revoca della propria identità digitale seguendo modalità analoghe a quelle previste dal precedente punto 4, ovvero attraverso:
a) richiesta al gestore inviata via PEC uff_teamsystemspid@pecteamsystem.com;
b) richiesta inviata tramite la casella di posta nota al gestore in formato elettronico e sottoscritta con firma digitale o elettronica;
c) richiesta tramite portale web dedicato all'utente https://spid.teamsystem.com/.

Nel caso di richiesta di sospensione, trascorsi trenta giorni dalla suddetta sospensione, il gestore provvede al ripristino dell'identità precedentemente sospesa qualora non pervenga con le modalità sopra indicate una richiesta di revoca.

La revoca di una identità digitale comporta conseguentemente la revoca delle relative credenziali.
Il Gestore dell'identità digitale conserva la documentazione inerente il ciclo di vita dell'identità digitale per un periodo pari a venti anni decorrenti dalla revoca dell'identità digitale

6. MISURE ANTICONTRAFFAZIONE

TeamSystem, in qualità di Gestore dell'Identità Digitale, attua una serie di misure anticontraffazione, al fine di evitare qualunque **furto d'identità**, inteso come:

a) impersonificazione totale, ossia l'occultamento totale di identità, attraverso l'impiego indebito di informazioni relative a un altro soggetto, che sia esso in vita o deceduto;
b) impersonificazione parziale, ossia l'occultamento parziale di identità, attraverso l'impiego combinato di informazioni relative ad un altro soggetto, utilizzate in maniera indebita, e informazioni relative alla propria persona.

TeamSystem attua tutti i processi finalizzati a garantire la protezione delle credenziali SPID dei Titolari contro abusi e utilizzi non autorizzati, ossia ad assicurare la sicurezza della conservazione delle stesse o dei mezzi utilizzati per loro produzione.

A causa della diversa natura tecnologica che caratterizza le credenziali SPID, per ogni livello di sicurezza possibile vengono adottate differenti misure anticontraffazione.

Qualunque sia il livello di sicurezza SPID associato alla credenziale richiesta, TeamSystem attua come prima misura la verifica dei dati forniti, attraverso accertamenti effettuati con fonti autoritative istituzionali, in grado di dare conferma della veridicità delle informazioni raccolte.

TeamSystem usufruisce, mediante apposite convenzioni stipulate, del servizio di verifica del codice fiscale e dell'anagrafica degli utenti, fornito dall'Agenzia delle Entrate stessa.

Inoltre, le procedure di identificazione prevedono ulteriori meccanismi di controllo, attuati dall'operatore IR che esegue il riconoscimento.
In particolare, quest'ultimo:

- deve rispettare tutte le direttive ricevute dal Gestore;
- deve rispettare le disposizioni dei Regolamenti AgID e degli Avvisi AgID;
- non ammette documenti in fotocopia, ma solo in originale;
- confronta i connotati del Richiedente con quanto riportato sul documento di riconoscimento presentato;
- controlla la congruenza tra la data di emissione e quella di scadenza dei documenti, in base alla normativa di riferimento;
- effettua controlli specifici sui documenti che il Richiedente presenta, in particolare sulle misure di sicurezza in essi contenute. Ad esempio, alcuni controlli antifrode che gli operatori effettuano, a fronte di debita formazione, sono:
    - il font del numero di serie per la Carta di Identità;
    - l'allineamento della stampa dei dati anagrafici per la patente di guida;

- l'araldica del timbro sui documenti cartacei, corrispondente all'autorità emettitrice, ecc.

L'immagine della documentazione raccolta è conservata a norma di legge e in maniera non modificabile.

Le misure anticontraffazione si basano infine anche su *elementi tecnologici*, come l'utilizzo di algoritmi crittografici robusti per garantire riservatezza e integrità dei dati, sulla base di quanto prescritto normativamente e allineato con le best practice internazionali e per la generazione e protezione delle One-Time Password per il livello 2 di SPID.

6.1 Misure anticontraffazione Livello 1 SPID

La principale misura anticontraffazione della password che costituisce la credenziale SPID di livello 1 è rappresentata dalla riservatezza di conservazione da parte del Titolare dell'identità SPID.

Al fine di aumentare il grado di sicurezza ed evitare il rischio di utilizzi non autorizzati dell'identità:

- i file che contengono le credenziali sono protetti da un sistema di controllo, in modo da limitare l'accesso esclusivo agli amministratori e alle applicazioni autorizzate;
- le credenziali vengono processate, all'atto del salvataggio, applicando tecniche di hashing, al fine di garantire maggior sicurezza contro attacchi di tipo dizionario o forza bruta.

6.2 Misure anticontraffazione Livello 2 SPID

Il livello 2 SPID aggiunge alla sicurezza della password quella data dal possesso di un dispositivo mobile fisico cui viene inviata una seconda credenziale dinamica e di durata limitata.

Il sistema di *One Time Password* (OTP) adottato da TeamSystem fornisce una sicurezza maggiore, basandosi sul presupposto che l'utente Titolare, oltre a conoscere la *password*, abbia l'accesso esclusivo al telefono cellulare verificato in fase di registrazione.

L'architettura dell'autenticazione con One-Time Password permette di generare codici di autenticazione a valore variabile e di durata limitata a sessanta secondi, il che rende la singola credenziale OTP non utilizzabile, trascorso tale periodo di tempo.

La contraffazione di credenziali di livello 2 SPID risulta quindi estremamente complessa, perché richiederebbe di entrare in possesso sia della password (credenziale di livello 1) che della password temporanea (e quindi del cellulare dell'utente), andando in contrasto con l'obbligo a cui è soggetto il Titolare relativo all'obbligo di conservazione sicura delle credenziali ricevute.

7. TRACCIATURE

Secondo quanto specificato dal DPCM del 24 ottobre 2014 (rif. [10]), un Identity Provider SPID ha l'obbligo di conservazione delle informazioni riguardanti l'intero ciclo di vita di un'Identità Digitale.

A tal fine, TeamSystem S.p.A. mantiene quindi traccia, per un periodo di tempo adeguato e conforme alle norme vigenti, di:

- tutte le **operazioni svolte da e per i Titolari** delle identità digitali, registrando su di un apposito log tutta una serie di informazioni relative all'utilizzo dell'identità stessa;
- ogni **evento di sistema** e **operazioni di utenti amministratore/operatore**, al fine di consentire una precisa ricostruzione delle attività in caso di necessità.

Sono inoltre registrate anche le evidenze documentali a corredo della richiesta di identità e conservate a norma nel sistema di conservazione documentale elettronica certificato:

- contratto di identità digitale sottoscritto;
- scansione fronte/retro del documento di identità;
- scansione fronte/retro del tesserino sanitario;
- in caso di riconoscimento de visu da remoto:
  - dichiarazione di riconoscimento firmata dall'IR;
  - streaming audiovideo della sessione di riconoscimento.

I dati provenienti dai differenti servizi:

- sono mantenuti secondo quanto dettato dalle normative e nel rispetto del Regolamento UE 2016/679 (General Data Protection Regulation - GDPR) e del Codice della Privacy, garantendone l'accesso esclusivamente al personale incaricato;
- vengono archiviati a norma e resi disponibili ai titolari dell'identità digitale su richiesta, che potranno utilizzarle per gli usi consentiti dalla legge;
- costituiscono la base per le elaborazioni statistiche e le misurazioni del livello di servizio.

7.1 Classificazione delle tracciature

Nei prossimi paragrafi, verranno elencate le diverse tipologie di eventi tracciati dal sistema, suddivise a seconda del relativo processo oggetto delle operazioni dell'IdP.

7.1.1 Richiesta ed emissione dell'identità digitale

Al fine di poter tracciare il corretto rilascio di una Identità Digitale, vengono registrati, in appositi log, tutti gli eventi relativi alla richiesta dell'identità SPID, funzionali alla tipologia di registrazione e contrattualizzazione utilizzata:

- Accesso applicazione da parte del personale;
- Verifica dell'anagrafica del Richiedente presso le fonti autoritative di verifica;
- Processo di richiesta dell'identità digitale;
- Processo di identificazione remota dell'utente (se applicabile);
- In caso di identificazione informatica dell'utente, i tracciamenti delle transazioni;
- Verifica numero di cellulare/e-mail;
- Tracciamenti dei processi relativi all'emissione dell'identità digitale.

Tali informazioni, relative al processo di adesione, vengono mantenute per un periodo pari a 20 (venti) anni, decorrenti dalla scadenza o dalla revoca dell'identità digitale, nel rispetto dell'art. 7, comma 5 del già citato DPCM del 24 ottobre 2014 (rif. [10]).

7.1.2 Gestione del ciclo di vita dell'Identità Digitale

Nel rispetto dell'art. 21 del "Regolamento AgID recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014)" (rif. [13]), devono essere conservate adeguate evidenze per tutto il ciclo di vita di un'identità digitale SPID.

Viene quindi tracciato e mantenuto da TeamSystem, in maniera opportuna, ogni sottoprocesso del processo di gestione dell'identità, nel pieno rispetto della normativa in materia di protezione dei dati personali di cui Regolamento UE 2016/679 (General Data Protection Regulation - GDPR) e al decreto legislativo 30 giugno 2003, n. 196.

In particolare, vengono mantenuti:

- i log relativi alla modifica di attributi;
- i log relativi alla modifica delle credenziali;
- i log per ciascun processo di sospensione, revoca e rinnovo delle credenziali.

7.1.3 Accessi al servizio

TeamSystem, in aderenza alle "Regolamento recante le regole tecniche SPID" (rif. [14]), emanato in attuazione dell'art. 4, comma 2 del DPCM 24 ottobre 2014 (rif. [10]), mantiene un *Registro delle transazioni*, contenente l'insieme dei log delle richieste di autenticazione gestite negli ultimi 24 mesi e che coinvolgono le Identità Digitali SPID.

Come descritto all'art. 29 del "Regolamento AgID recante le modalità attuative per la realizzazione dello SPID (art. 4, comma 2, DPCM 24 ottobre 2014)" (rif. [10]), tali informazioni sono necessarie a imputare alle singole identità digitali le operazioni effettuate sui sistemi e sono costituite da registrazioni composte dal messaggio SAML di richiesta di autenticazione e della relativa asserzione emessa dal gestore delle identità.

I messaggi suddetti riportano identificativi e date di emissione e sono firmati, rispettivamente, dal *Fornitore di Servizi (Service Provider – SP)* e dallo stesso *Gestore dell'Identità Digitale* ed è quest'ultima caratteristica che fornisce le necessarie garanzie di integrità e non ripudio, secondo quanto previsto dalle regole tecniche di cui all'art. 4 del DPCM già citato (rif. [10]).

Caratteristiche dei log di autenticazione

Le registrazioni degli accessi al servizio devono avere caratteristiche di riservatezza, inalterabilità e integrità e sono conservate adottando idonee misure di sicurezza, ai sensi dell'articolo 31 del decreto legislativo 30 giugno 2003, n. 196 e ss.cc.ii (rif. [2]), sotto la responsabilità del titolare del trattamento.

Esse garantiscono infatti il collegamento per ogni transazione tra codice identificativo dell'Identità Digitale, richiesta di autenticazione generata dal Service Provider e relativa risposta generata dall'Identity Provider, in seguito all'autenticazione dell'utente, mediante le credenziali fornite in fase di rilascio dell'Identità

Digitale.

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

Il log certificato è un file prodotto dall'applicativo che gestisce il processo di autenticazione e dialogo con i Service Provider. Tali log sono salvati quindi in maniera persistente e nel rispetto del codice della privacy, utilizzando meccanismi di cifratura dei dati (come richiesto dall'art. 29 del "Regolamento recante le modalità attuative SPID", rif.13).

Formato dei log eventi
In accordo con quanto richiesto nonché suggerito nelle regole tecniche SPID (rif. [14]), per ogni transazione di autenticazione SAML utente, viene memorizzato sul sistema un record denominato "**log di accesso al servizio di autenticazione**", contenente le seguenti informazioni:

- codice Identificativo dell'identità digitale SPID (**spidCode**) attribuito al momento del rilascio dell'identità stessa;
- richiesta di autenticazione SAML (**<AuthnRequest>**), conforme ai protocolli definiti dalle Regole tecniche, emessa dal Fornitore di Servizi;
- asserzione di risposta SAML (**<Response>**) alla richiesta di autenticazione, emessa dal Gestore dell'Identità;
- codice identificativo della richiesta di autenticazione emessa dal Fornitore di servizi;
- data e ora (timestamp) della richiesta di autenticazione emessa dal Fornitore di servizi;
- l'entityID dell'SP (fornitore di servizi) che ha sottoposto la richiesta di autenticazione (**issuer richiesta**);
- codice identificativo della risposta fornita dal Gestore dell'Identità;
- data e ora (timestamp) della risposta fornita dal Gestore dell'Identità;
- l'entityID di TeamSystem (gestore dell'identità autenticante) che ha fornito la risposta (**issuer risposta**);
- codice identificativo (**<Assertion>**) della asserzione di risposta SAML alla richiesta di autenticazione, emessa dal Gestore dell'Identità;
- soggetto (**subject**) dell'asserzione di risposta che si è autenticato.

7.2 Accesso ai log e modalità di richiesta

Nel rispetto dell'art. 29 del "Regolamento recante le modalità attuative SPID" (rif. [13]), l'**accesso** in lettura e scrittura ai sistemi che custodiscono i log è riservato al solo personale tecnico dell'IdP espressamente autorizzato e incaricato del trattamento dei dati personali.

In caso di richiesta di accesso ai log **da parte delle autorità**, le modalità di acquisizione dei log prevedono il coinvolgimento tecnico dell'IdP ed il recupero di una versione dei log relativamente piccola, indicizzata e adatta ad una rapida identificazione di utente, operazione e riferimento orario.
Resta sempre garantita la possibilità di accesso ad una versione più ricca di informazioni.

L'utente **Titolare** di un'Identità Digitale può invece richiedere in qualunque momento una copia delle informazioni, contenute nel log certificato, relative all'utilizzo della propria identità SPID.

Per far questo, potrà essere utilizzata dallo stesso una delle modalità descritte di seguito.

Si intende precisare che le attestazioni rilasciate potranno essere utilizzate dal Titolare solo per gli usi consentiti dalla legge.

7.2.1 Richiesta via PEC o raccomandata postale

Per inviare la richiesta via PEC o raccomandata postale, il Titolare compila l'apposito modulo, fornito su richiesta dal Gestore utilizzando gli appositi canali, indicando i seguenti dati:

- dati anagrafici del Titolare;
- intervallo di date del quale si richiedono i log;
- ulteriori dettagli circa la tipologia di azione interessata dalla richiesta del Titolare;
- motivazione della richiesta;
- autorizzazione relativa alla normativa sulla privacy;
- modalità di invio dei dati di log (Posta Elettronica Certificata – PEC o raccomandata postale);
- recapito del Titolare da utilizzare nell'invio.

Il modulo compilato e sottoscritto dovrà essere inviato al Gestore, corredato di copia fronte/retro del documento di identità:
• tramite PEC all'indirizzo: *uff_teamsystemspid@pecteamsystem.com*;
• tramite raccomandata postale all'indirizzo riportato in apertura di documento

TeamSystem verificherà la correttezza della richiesta e provvederà alla raccolta di quanto richiesto e alla produzione dell'attestazione richiesta dal Titolare.

I dati verranno quindi inviati al Titolare entro **30** giorni lavorativi dalla ricezione della richiesta, in modalità digitale. Il log viene inoltre firmato digitalmente dal Legale Rappresentante di TeamSystem S.p.A. o da chi per questo delegato, con i dati minimi di riferimento come previsto dalla normativa.

7.2.2 Richiesta da portale di gestione dell'identità (area Self)

Per inviare la richiesta online, il Titolare accede con le proprie credenziali, al portale di gestione dell'identità (o area self-care) e da qui seguire le indicazioni per effettuare la richiesta, indicando l'intervallo temporale per cui intende ricevere le informazioni.

La richiesta dovrà essere validata mediante l'inserimento delle credenziali SPID di livello 2, ovvero con l'inserimento di una OTP ricevuta dal Titolare.

TeamSystem provvederà alla raccolta di quanto richiesto e alla produzione dell'attestazione richiesta dal Titolare, che quest'ultimo potrà scaricare dal portale di gestione dell'identità.

8. MONITORAGGIO

Gli Identity Provider SPID rendono disponibile all'Agenzia per l'Italia Digitale:

a) il livello di soddisfazione dei propri clienti;
b) le caratteristiche di eventuali servizi aggiuntivi offerti dall'IdP;
c) le informazioni relative agli eventuali disservizi. In particolare, il Gestore di Identità Digitali ha l'obbligo di comunicare all'AgID il codice del disservizio, come indicato nel Regolamento recante le modalità attuative SPID, entro uno SLA trenta minuti o due ore, a seconda della classificazione del disservizio effettuata [13].

Il Gestore dovrà comunicare inoltre all'Agenzia, con cadenza almeno bimestrale, i dati statistici relativi all'utilizzo del sistema SPID e le metriche qualitative e quantitative concordate.

Per un monitoraggio costante dello stato di tutti i servizi offerti, l'Identity Provider ha predisposto una piattaforma di monitoraggio, in grado di rilevare anomalie o disservizi in tempo reale e di segnalare gli stessi con differenti livelli di gravità alle strutture preposte alla loro gestione operativa.

Le funzionalità principali disponibili all'interno della piattaforma sono:

- monitoraggio dell'intera infrastruttura tecnologica (sistemi hardware, networking, occupazione di storage, ecc.);
- sonde di monitoraggio e controllo dei vari processi automatici;
- correlazione degli indicatori applicativi e di quelli infrastrutturali;
- implementazione e modifica di regole di gestione di allarmi;
- gestione reportistica (KPI/SLA).

APPENDICE A - DESCRIZIONE DEI CODICI E FORMATI DEI MESSAGGI DI ANOMALIA

Il sistema di gestione delle identità digitali segnala eventuali anomalie riscontrate sia relativamente ai protocolli che ai dispositivi di autenticazione utilizzati.
L'IdP ha recepito la tabella degli errori indicata sul sito dell'AgID e che viene riportata a seguire:

Autenticazione corretta

ERROR CODE:	**1 (AUTENTICAZIONE CORRETTA)**
Binding:	HTTP-POST, HTTP-Redirect
HTTP status code:	200
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Success`
Destinatario notifica:	Fornitore del servizio (SP)

Anomalie del sistema

ERROR CODE:	**2 (INDISPONIBILITÀ SISTEMA)**
Binding:	HTTP-POST
Destinatario notifica:	Utente
Schermata IdP:	Messaggio di errore generico
Troubleshooting utente:	Ripetere l'accesso al servizio più tardi

ERROR CODE:	**3 (ERRORE DI SISTEMA)**
Binding:	HTTP-Redirect
HTTP status code:	500
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio "Sistema di autenticazione non disponibile - Riprovare più tardi"
Troubleshooting utente:	Ripetere l'accesso al servizio più tardi

ERROR CODE:	**3 (ERRORE DI SISTEMA)**
Note:	Tutti i casi di errore di sistema in cui è possibile mostrare un messaggio informativo all'utente

Anomalie delle richieste

ERROR CODE:	**4 (FORMATO BINDING NON CORRETTO)**
Binding:	HTTP-Redirect, HTTP-POST
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Formato richiesta non corretto - Contatare il gestore del servzio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta
Parametri obbligatori:	• `SAMLRequest` • `SigAlg` (solo per HTTP-Redirect)

ERROR CODE:	**4 (FORMATO BINDING NON CORRETTO)**
	• `Signature` (solo per HTTP-Redirect)
Parametri non obbligatori:	• `RelayState`
ERROR CODE:	**5 (VERIFICA DELLA FIRMA FALLITA)**
Binding:	HTTP-Redirect
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Impossibile stabilire l'autenticità della richiesta di autenticazione - Contattare il gestore del servizio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare certificato o modalità di apposizione firma
Note:	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

ERROR CODE:	**6 (BINDING SU METODO HTTP ERRATO)**
Binding:	HTTP-Redirect, HTTP-POST
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Formato richiesta non ricevibile - Contattare il gestore del servizio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare metadata Gestore dell'identita (IdP)
Note:	Invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell'identity, oppure invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity
ERROR CODE:	**7 (ERRORE SULLA VERIFICA DELLA FIRMA DELLA RICHIESTA)**
Binding:	HTTP-POST
HTTP status code:	403

ERROR CODE:	**7 (ERRORE SULLA VERIFICA DELLA FIRMA DELLA RICHIESTA)**
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Formato richiesta non corretto - Contattare il gestore del servizio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare certificato o modalità di apposizione firma
Note:	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
ERROR CODE:	**8 (FORMATO DELLA RICHIESTA NON CONFORME ALLE SPECIFICHE SAML)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML StatusMessage:	ErrorCode nr08
Destinatario notifica:	Fornitore del servizio (SP)

ERROR CODE:	**8 (FORMATO DELLA RICHIESTA NON CONFORME ALLE SPECIFICHE SAML)**
Troubleshooting SP:	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente
Note:	Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente alla verifica positiva della firma
ERROR CODE:	**9 (PARAMETRO VERSION NON PRESENTE, MALFORMATO O DIVERSO DA `2.0`)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:VersionMismatch`
SAML StatusMessage:	ErrorCode nr09
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente
ERROR CODE:	**10 (ISSUER NON PRESENTE, MALFORMATO O NON CORRISPONDETE ALL'ENTITÀ CHE SOTTOSCRIVE LA RICHIESTA)**
Binding:	HTTP-Redirect, HTTP-POST

ERROR CODE:	**10 (ISSUER NON PRESENTE, MALFORMATO O NON CORRISPONDETE ALL'ENTITÀ CHE SOTTOSCRIVE LA RICHIESTA)**
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Formato richiesta non corretto - Contattare il gestore del servizio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare formato delle richieste prodotte
ERROR CODE:	**11 (ID NON PRESENTE, MALFORMATO O NON CONFORME)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML StatusMessage:	ErrorCode nr11

ERROR CODE:	**11 (ID NON PRESENTE, MALFORMATO O NON CONFORME)**
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente
Note:	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata s olo a seguito di una positiva verifica della firma.
ERROR CODE:	**12 (`REQUESTAUTHNCONTEXT` NON PRESENTE, MALFORMATO O NON PREVISTO DA SPID)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:NoAuthnContext`
SAML StatusMessage:	ErrorCode nr12
Destinatario notifica:	Fornitore del servizio (SP)

ERROR CODE:	**12 (`REQUESTAUTHNCONTEXT` NON PRESENTE, MALFORMATO O NON PREVISTO DA SPID)**
Schermata IdP:	Pagina temporanea con messaggio di errore: *"Autenticazione SPID non conforme o non specificata"*
Troubleshooting SP:	Informare l'utente
Note:	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata s olo a seguito di una positiva verifica della firma.
ERROR CODE:	**13 (`ISSUEINSTANT` NON PRESENTE, MALFORMATO O NON COERENTE CON L'ORARIO DI ARRIVO DELLA RICHIESTA)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:RequestDenied`
SAML StatusMessage:	ErrorCode nr13
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente

ERROR CODE:	**14 (`DESTINATION` NON PRESENTE, MALFORMATA O NON COINCIDENTE CON IL GESTORE DELLE IDENTITÀ RICEVENTE LA RICHIESTA)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported`
SAML StatusMessage:	ErrorCode nr14
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente

ERROR CODE:	**15 (ATTRIBUTO `ISPASSIVE` PRESENTE E ATTUALIZZATO AL VALORE TRUE)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:NoPassive`

ERROR CODE:	**15 (ATTRIBUTO `ISPASSIVE` PRESENTE E ATTUALIZZATO AL VALORE TRUE)**
SAML StatusMessage:	ErrorCode nr15
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente
ERROR CODE:	**16 (`ASSERTIONCONSUMERSERVICE` NON CORRETTAMENTE VALORIZZATO)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported`
SAML StatusMessage:	ErrorCode nr16
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente

ERROR CODE:	**16 (`ASSERTIONCONSUMERSERVICE` NON CORRETTAMENTE VALORIZZATO)**
Note:	• `AssertionConsumerServiceIndex` presente e attualizzato con valore non riportato nei metadata • `AssertionConsumerServiceIndex` riportato in presenza di uno od entrambi gli attributi `AssertionConsumerServiceURL` e `ProtocolBinding` • `AssertionConsumerServiceIndex` non presente in assenza di almeno uno attributi `AssertionConsumerServiceURL` e `ProtocolBinding` • La response deve essere inoltrata presso `AssertionConsumerService` di default riportato nei metadata
ERROR CODE:	**17 (ATTRIBUTO `FORMAT` DELL'ELEMENTO `NAMEIDPOLICY` ASSENTE O NON VALORIZZATO SECONDO SPECIFICA)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported`
SAML StatusMessage:	ErrorCode nr17
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente
Note:	Nel caso di valori diversi dalla specifica del parametro opzionale `AllowCreate` si procede con l'autenticazione senza riportare errori

ERROR CODE:	**18 (`ATTRIBUTECONSUMERSERVICEINDEX` MALFORMATO O CHE RIFERISCE A UN VALORE NON REGISTRATO NEI METADATI DI SP)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported`
SAML StatusMessage:	ErrorCode nr18
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Riformulare la richiesta con un valore dell'indice presente nei metadati

Anomalie derivanti dall'utente

ERROR CODE:	**19 (AUTENTICAZIONE FALLITA PER RIPETUTA SOTTOMISSIONE DI CREDENZIALI ERRATE - SUPERATO NUMERO TENTATIVI SECONDO LE POLICY ADOTTATE)**
Binding:	HTTP-Redirect, HTTP-POST

ERROR CODE:	**19 (AUTENTICAZIONE FALLITA PER RIPETUTA SOTTOMISSIONE DI CREDENZIALI ERRATE - SUPERATO NUMERO TENTATIVI SECONDO LE POLICY ADOTTATE)**
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr19
Destinatario notifica:	HTTP POST/HTTP Redirect
Schermata IdP:	Messaggio di errore specifico ad ogni interazione prevista
Troubleshooting utente:	Inserire credenziali corrette
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
Note:	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.

ERROR CODE:	**20 (UTENTE PRIVO DI CREDENZIALI COMPATIBILI CON IL LIVELLO RICHIESTO DAL FORNITORE DEL SERVIZIO)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr20
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting utente:	Acquisire credenziali di livello idoneo all'accesso al servizio richiesto
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto

ERROR CODE:	**21 (TIMEOUT DURANTE L'AUTENTICAZIONE UTENTE)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`

ERROR CODE:	**21 (TIMEOUT DURANTE L'AUTENTICAZIONE UTENTE)**
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr21
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting utente:	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinato periodo di tempo
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto

ERROR CODE:	**22 (UTENTE NEGA IL CONSENSO ALL'INVIO DI DATI AL SP IN CASO DI SESSIONE VIGENTE)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr22

ERROR CODE:	**22 (UTENTE NEGA IL CONSENSO ALL'INVIO DI DATI AL SP IN CASO DI SESSIONE VIGENTE)**
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting utente:	Dare consenso
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richies to
Note:	Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1.

ERROR CODE:	**23 (UTENTE CON IDENTITÀ SOSPESA/REVOCATA O CON CREDENZIALI BLOCCATE)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr23
Destinatario notifica:	Fornitore del servizio (SP)

ERROR CODE:	**23 (UTENTE CON IDENTITÀ SOSPESA/REVOCATA O CON CREDENZIALI BLOCCATE)**
Schermata IdP:	Pagina temporanea con messaggio di errore: "Credenziali sospese o revocate"
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto

ERROR CODE:	**24 (RISERVATO)**

ERROR CODE:	**25 (PROCESSO DI AUTENTICAZIONE ANNULLATO DALL'UTENTE)**
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr25
Destinatario notifica:	Fornitore del servizio (SP)

ERROR CODE:	**25 (PROCESSO DI AUTENTICAZIONE ANNULLATO DALL'UTENTE)**
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto