MANUALE OPERATIVO

SIELTE ID

Servizio di Gestione Sistema Pubblico dell'Identità Digitale (SPID)

File/Oggetto	**Manuale Operativo**		
Redatto da	**Development Management**		
Verificato da	**Delivery, Quality, Security**		
Approvato da	**CIO**		
Archivio	**Qualità e Amministrazione**		
Stato	**Bozza** ☐	**In fase di Approvazione** ☐	**Pubblicato** ☒

LISTA DI DISTRIBUZIONE

Classificazione	Riservato (ambito reparto) ☐	Riservato (ambito azienda) ☐	Riservato (azienda - cliente) ☐	Pubblico ☒
Distribuzione a	Nominativo:		Funzione/Azienda	
			AgID	
N. Copie Distribuite	1			

STATO DELLE REVISIONI DEL MANUALE OPERATIVO

REV.	CAP.	DESCRIZIONE MOTIVO	DATA
00	TUTTI	EMISSIONE MANUALE OPERATIVO	10/2015
01	TUTTI	REVISIONE GENERALE	04/2016
02	6	MODIFICHE DELLE PROCEDURE DI RILASCIO DELL'IDENTITA' DIGITALE / MODIFICHE ALLEGATO A	09/2016
03	5	AGGIUNTA DESCRIZIONE RIGUARDO LA SICUREZZA DEI DATI, GLI ALGORITMI DI CRITTOGRAFIA ADOTTATI E GENERAZIONE OTP	03/2017
04	5	AGGIUNTO NUOVO PROFILO E SVILUPPO SU UNIVERSAL WINDOWS PLATFORM	05/2017
05	5.4	TOUCH ID SU ANDROID	06/2017
06	1.3, 2.2, 5.7, 7	ESTENSIONE SPID; REVISIONE PROFILO	10/2017
07	TUTTI	PROCEDURE DI RECUPERO CREDENZIALI, GESTIONE CREDENZIALI DI LIVELLO 1 E 2, AMPLIAMENTO DELLE CONVENZIONI DI LETTURA, INTRODUZIONE DI SCIPAFI PER LA VERIFICA DEL CODICE FISCALE, REVISIONE REGISTRAZIONE E GESTIONE IMPRESE, REVISIONE GENERALE DEL DOCUMENTO	04/2018

Sommario

1 GENERALITÀ

1.1 Scopo del documento

Questo documento, denominato “Manuale Operativo”, contiene le regole e le procedure operative utilizzate per fornire il servizio di Identità Digitale (Identity Provider) 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 Convenzioni di lettura

Nel resto del documento, l’azienda Sielte S.p.A., erogatrice del servizio di gestore dell’identità digitale qui descritto e disciplinato, è indicata semplicemente con “Sielte”.

Col termine “Manuale Operativo” si intende sempre fare riferimento alla versione corrente del Manuale Operativo (vedere la sezione *Versione del manuale operativo*).

I riferimenti alla normativa e agli standard sono riportati tra parentesi quadre.

Affinché vengano rispettati i parametri RID previsti dalla norma UNI EN ISO 27001:2013, la distribuzione dei documenti prodotti da Sielte S.p.A. è controllata; i documenti e le loro successive emissioni vengono comunicate ai fruitori autorizzati, poiché direttamente coinvolti nelle attività oggetto dei documenti.

In questo specifico caso, essendo il documento classificato in ambito di riservatezza come “Pubblico”, esso deve essere reso disponibile a tutti. Nel momento in cui il presente documento viene distribuito al di fuori del contesto aziendale, Sielte S.p.A. non è più responsabile del monitoraggio delle copie distribuite.

1.3 Riferimenti normativi

[1] Decreto del Presidente della Repubblica (DPR) 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.

[2] Decreto del Presidente del Consiglio (DPCM) 24 ottobre 2014 "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di azione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese", pubblicato sulla Gazzetta Ufficiale del 9 dicembre 2014, n.285

[3] Decreto Legislativo (DLGS 196) 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n. 123 della Gazzetta Ufficiale n. 174, 29 luglio 2003

[4] Decreto Legislativo (CAD) 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale", pubblicato nella Gazzetta Ufficiale n.112 del 16 maggio 2005.

[5] Decreto Legislativo (DLGS 69) 21 giugno 2013, n. 69, convertito con modificazioni dalla legge del 9 agosto 2013, n. 69 che "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese".

[6] Regolamento UE n.910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, pubblicato nella Gazzetta Ufficiale dell'Unione Europea – serie L 257 del 28 agosto 2014.

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

[8] ISO EN UNI 9001:2008 – Sistema Qualità

[9] ISO/IEC 27001:2013 – Sistema di Gestione della Sicurezza delle Informazioni

[10] ISO/IEC 20000-1:2011 – Sistema Di Gestione Dei Servizi IT

[11] Regolamenti eIDAS [electronic IDentification Authentication and Signature – ETSI EN 319 401:2016 e, in aggiunta ETSI EN 319 411-1:2016 – ETSI EN 319 411-2:2016 – ETSI EN 319 421:2016]

1.4 Definizioni ed acronimi

AES	Advanced Encryption Standard
AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
CNS	Carta Nazionale dei Servizi
CODICE/CODICE DELLA PRIVACY	Codice in materia di protezione dei dati personali
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAAS	Infrastructure As A Service
ICT	Information and Communications Technology
IDP	Identity Provider
IETF	Internet Engineering Task Force
ISO/OSI	International Standards Organization Open Systems Interconnection
LOA	Level of Assurance – Livello di Sicurezza
OASIS	Organization for the Advancement of Structured Information Standards
OTP	One Time Password
PDF	Portable Document Format
PEC	Posta Elettronica Certificata

PIN	Personal Identification Number
REGOLAMENTO	Regolamento recante le modalità attuative per la realizzazione dello SPID
RFC	Request For Comments
RSI	Responsabile della Sicurezza delle Informazioni Sielte
SAML	Security Assertion Markup Language
SMS	Short Message Service
SP	Service Provider
SSO	Single Sign-On
TOTP	Time-based One-Time Password
XML	eXtensible Markup Language
UWP	Universal Windows Platform

- **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).

- **Riservatezza:** garanzia che le informazioni siano accessibili solo da parte delle persone autorizzate.
- **Integrità:** salvaguardia dell'esattezza e della completezza dei dati e delle modalità di processo.
- **Disponibilità:** garanzia che le informazioni siano accessibili a coloro che le richiedono e ne hanno il diritto.
- **Autorizzazione:** atto che conferisce la capacità di esercitare un diritto.
- **Autenticazione:** garanzia della corretta identità dichiarata da un'entità.
- **Definizione del rischio:** processo di individuazione, riconoscimento e descrizione del rischio.
- **Analisi dei rischi:** processo di comprensione della natura del rischio e di determinazione del livello di rischio.
- **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.
- **Criteri di rischio:** valori di riferimento rispetto ai quali è ponderato il rischio.
- **Gestione del rischio:** attività coordinate per dirigere e controllare una organizzazione in merito al rischio o ai rischi esistenti.
- **Trattamento del rischio:** processi di selezione e implementazione di attività volte a diminuire o comunque modificare il rischio presente.
- **Valutazione del rischio**: processo complessivo di identificazione, analisi e ponderazione del rischio.

2 DATI IDENTIFICATIVI

2.1 Dati identificativi del gestore

Ragione sociale	Sielte S.p.A.
Sede legale	Via Cerza, n.4 - 95027 S. Gregorio di Catania
Direzione generale	Via Valle di Perna, 1/a – 00128 Roma
Legale Rappresentate	Salvatore Turrisi
Codice Fiscale	00941910788
Partita IVA	03600700870
Telefono	+39 095 724 11 11
Sito web ufficiale	https://www.sielte.it
Sito web ufficiale progetto SPID	https://www.sielteid.it
E-mail	info@sielte.it
PEC	direzione.sielte@legalmail.it

Sielte nasce nel 1925 a Genova come Società Impianti Elettrici Telefonici Ericsson Italiana. Oggi vanta novant'anni di esperienza nei settori delle Telecomunicazioni, dei Sistemi Tecnologici per Trasporti & Infrastrutture e dei Servizi ICT orientati al Cloud Computing, un gruppo con un volume d'affari complessivo di oltre 400 milioni di euro, è oggi riconosciuta sul mercato come uno dei maggiori partner italiani con cui intraprendere importanti progetti di integrazione rappresentando una realtà, che opera su tutto il territorio nazionale con 30 sedi in Italia e circa 20 all'estero. Con sede legale a Catania e Direzione Generale a Roma, Sielte ha un capitale sociale di 28 milioni di euro, una squadra di oltre 3.000 persone,

costantemente impegnata in importanti percorsi di certificazione e di specializzazione. Particolare impegno è rivolto allo sviluppo delle giovani risorse assunte negli ultimi anni, attraverso progetti di formazione mirati, con lo scopo di migliorare know-how e competenze al fine di offrire System Engineer altamente qualificati, Team Leader e Project Manager certificati per l'uso di metodologie standard e internazionali.

Una spiccata vocazione per l'innovazione e le caratteristiche del proprio business spingono Sielte a investire continuamente in Ricerca & Sviluppo. Tale strategia permette di offrire continuamente nuovi servizi attraverso la scelta di tecnologie di ultima generazione al fine di offrire soluzioni perfettamente integrate e all'avanguardia nel proprio mercato di riferimento.

Sielte trasferisce valore ai propri Clienti attraverso:

- Competenza nel recepire i requisiti del cliente e tradurli in soluzione
- Conoscenza dei migliori prodotti e soluzioni disponibili sul mercato dell'ICT sia Enterprise sia Open Source
- Capacità di Project Management e relazioni con i committenti ed i propri partner tecnologici
- Corretta gestione dei tempi, dei costi e della qualità della fornitura di servizi, prodotti e soluzioni.

Sielte S.p.A. è una Società di Ingegneria, Progettazione, Costruzione e Manutenzione di:

- Reti di Telecomunicazioni
- Sistemi Tecnologici per Trasporti e Infrastrutture
- Servizi ICT & Cloud Computing
- Sistemi Satellitari
- Sistemi Energetici
- Impianti Oil & Gas

SielteCloud è la Business Unit riconosciuta sul mercato con il ruolo di Cloud Service Provider, dispone di un importante infrastruttura di proprietà caratterizzata da tre Data Center dislocati sul territorio nazionale con oltre 500 server fisici in configurazione ad altissima affidabilità, un teleporto satellitare direttamente interconnesso ad una rete MPLS a larga banda 10Gbit/s con oltre 150 nodi fornita dai più importanti operatori internazionali e propri firewall di protezione firmati Palo Alto Networks. I servizi sono affidati ad un service desk interno che dispone di competenze tecniche di I, IIe IIIlivello, risponde ad un unico numero verde (+ 800 11 33 22) operativo dal lunedì al sabato dalle 09:00 alle 18:00, al fine di offrire ai propri Clienti una piattaforma servizi completa, affidabile ed interventi on-site.

Negli ultimi anni Sielte ha sviluppato forti competenze nel settore dell'ICT (Information and Communication Technology) basando l'offerta sull'integrazione di proprie soluzioni con le più comuni piattaforme tecnologiche ad oggi presenti sul mercato per Aziende e Pubbliche Amministrazioni. Servizi di assistenza, manutenzione, progettazione e sviluppo software permettono di offrire ed erogare soluzioni innovative ed affidabili che risiedono sia sui propri data center certificati sia sulle infrastrutture dei clienti gestite. Il mercato di riferimento è oggi rappresentato, oltre che da Operatori della Telefonia, dalle Grandi Infrastrutture, dalle Pubbliche Amministrazioni, dalle Banche e dai Broadcaster. Un portafoglio clienti, tra cui spiccano referenze quali Telecom Italia, Vodafone, Fastweb, Telefonica di Spagna, Nokia Siemens, Ferrovie dello Stato, Infratel Italia, Aem, Aeroporti, Amministrazioni Pubbliche Centrali e Locali, Cloud for Europe, Regioni, Autostrade, Jazztel, Enel, H3G, Tiscali, Wind, Lepida e Teletu.

2.2 Standard e certificazioni

Tutti i processi operativi del Gestore descritti in questo Manuale Operativo, come ogni altra attività del Gestore, sono conformi agli standard. Sielte possiede le seguenti certificazioni:

- **ISO 9001:2008** [Gestione della qualità – EA: 28, 34, 33, 22b]
    - Progettazione, realizzazione e manutenzione di reti. Sviluppo tecnico, progettazione e ingegnerizzazione dei processi produttivi per innovazione

tecnologica e supporto ai clienti pubblici e privati. Progettazione e costruzione di impianti di segnalamento e tecnologie ferroviarie, e servizi di manutenzione di mezzi d'opera circolanti su rotaia. Erogazione servizi di Data Center (Cloud Computing, Housing e Hosting) e relativa assistenza specialistica tramite Help Desk. Erogazione del servizio SielteID, in qualità di Identity Provider, aderente al Sistema Pubblico per la gestione dell'Identità Digitale (SPID), accreditato da AgID e conforme ai sensi del DPCM del 24 ottobre 2014, del CAD e del DPR n. 445.

- **ISO/IEC 27001:2013** [Gestione della sicurezza delle informazioni – IAF: 19,33]
    - Erogazione Servizi Data Center (Cloud Computing, Hosting e Housing) con relativo supporto tecnico attraverso Service Desk. Progettazione e sviluppo software. Erogazione del servizio SielteID, in qualità di Identity Provider, aderente al Sistema Pubblico per la gestione dell'Identità Digitale (SPID), accreditato da AgID e conforme ai sensi del DPCM del 24 ottobre 2014, del CAD e del DPR n. 445.
- **ISO/IEC 20000-1:2011** [Gestione dei servizi IT – IAF: 33]
    - Erogazione del servizio di Identity Provider aderente al sistema SPID (Sistema Pubblico Identità Digitale). Gestione Servizi ICT con supporto di Service Desk, Progettazione, Erogazione, Manutenzione ed Assistenza tecnica.
- **ISO 14001** [Gestione ambientale – EA 19, 28]
    - Progettazione, realizzazione e manutenzione di reti. Sviluppo tecnico, progettazione e ingegnerizzazione dei processi produttivi per innovazione tecnologica e supporto ai clienti pubblici e privati. Progettazione e costruzione di impianti di segnalamento e tecnologie ferroviarie. Attività di ufficio della direzione generale di Roma.
- **ISO 18001** [Gestione salute e sicurezza – EA: 28, 34, 33, 22b]

- Progettazione, realizzazione e manutenzione di reti. Sviluppo tecnico, progettazione e ingegnerizzazione dei processi produttivi per innovazione tecnologica e supporto ai clienti pubblici e privati. Progettazione e costruzione di impianti di segnalamento e tecnologie ferroviarie, e servizi di manutenzione di mezzi d'opera circolanti su rotaia.

- **SOA** [Attestazione di qualificazione alla esecuzione di lavori pubblici]
  - Categorie: OG1, OG3, OG9, OG10, OG11, OS1, OS5, OS9, OS17, OS19, OS27, OS30, OS25

- **Regolamenti eIDAS** [electronic IDentification Authentication and Signature – ETSI EN 319 401:2016 e, in aggiunta ETSI EN 319 411-1:2016 – ETSI EN 319 411-2:2016 – ETSI EN 319 421:2016].

2.3 Versione del manuale operativo

Il presente Manuale Operativo è di proprietà di Sielte S.p.A., tutti i diritti sono ad essa riservati. Questo documento è la versione del Manuale Operativo per il Servizio di Gestore di Identità Digitale erogato da Sielte ai sensi del [CAD] e del "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" emanato dall'Agenzia per l'Italia Digitale.

Il codice interno di questo documento è riportato su frontespizio.

Questo documento è pubblicato sul sito web del servizio di gestore delle identità digitali https://www.sielteid.it ed è quindi consultabile telematicamente.

Come versione corrente del Manuale Operativo si intenderà esclusivamente la versione in formato elettronico disponibile sul sito web del servizio di gestore delle identità digitali https://www.sielteid.it oppure quella pubblicata sul sito web dell'AgID.

Il documento è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.

2.4 Responsabile del manuale operativo

Le comunicazioni riguardanti il presente documento possono essere inviate alla cortese attenzione di:

Sielte S.p.A.	
Responsabile del Servizio di Identità Digitale	
Indirizzo	Via Cerza, n.4 - 95027 S. Gregorio di Catania (CT)
Fax	+39 095 7241 573
Call Center	+800 11 33 22
PEC	sistemi.sielte@legalmail.it
Web	https://www.sielteid.it

3 OBBLIGHI E RESPONSABILITÀ

Sulla base della normativa vigente, nel presente paragrafo sono sinteticamente riassunti:

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

Nella documentazione contrattuale del servizio che il Gestore sottoporrà all'Utente nell'ambito delle operazioni necessarie per il rilascio dell'Identità Digitale, sono indicati gli ulteriori elementi di natura contrattuale derivanti dal rapporto di erogazione del servizio. La documentazione contrattuale, unitamente alle sue successive versioni, sarà resa disponibile all'interno del portale https://www.sielteid.it.

3.1 Obblighi del Gestore delle Identità Digitali

Di seguito vengono elencanti gli obblighi a cui il gestore Sielte, nella figura di gestore delle Identità Digitali, si fa carico:

- Rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta.
- Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale.
- Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione *de visu.*
- Conservare copia del log della transazione nei casi di identificazione tramite documenti digitali di identità, identificazione informatica tramite altra identità digitale SPID o altra identificazione informatica autorizzata.
- Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso di identificazione tramite firma digitale.

- Verifica degli attributi identificativi del richiedente.
- Consegnare in modalità sicura le credenziali di accesso all'utente.
- Conservare la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale.
- Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale.
- Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.
- Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione.
- Effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso.
- Revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica.
- Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente.
- Verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata).
- Fornire all'utente che l'ha inviata conferma della ricezione della richiesta di sospensione.
- Sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni ed informarne il richiedente.
- Rispristinare o revocare l'identità digitale sospesa, nei casi previsti.

- Revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione.
- Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale.
- Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso.
- Effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta.
- Effettuare con cadenza almeno annuale un'analisi dei rischi.
- Definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID.
- Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato.
- Condurre con cadenza almeno semestrale il *Penetration Test.*
- Garantire la continuità operativa dei servizi afferenti allo SPID.
- Effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna.
- Garantire la gestione sicura delle componenti riservate delle identità digitali assicurando non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata.
- Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa.
- Sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti.

- Informare tempestivamente l'AgID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali.
- Adeguare i propri sistemi a seguito dell'aggiornamento della normativa.
- Inviare all'AgID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici.
- In caso intendesse cessare la propria attività, comunicarlo all'AgID "e ai titolari" almeno 30 giorni prima della data di cessazione, indicando gli eventuali gestori sostitutivi, ovvero segnalando la necessità di revocare le identità digitali rilasciate.
- In caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e ne conserva le informazioni.
- In caso di cessazione dell'attività, scaduti i 30 giorni, revocare le identità digitali rilasciate e per le quali non si è avuto subentro.
- Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi.
- Se richiesto dall'utente, segnalargli via email o via sms ogni avvenuto utilizzo delle proprie credenziali di accesso.
- Notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale.
- Nel caso l'identità digitale risulti non attiva per un periodo superiore a 24 mesi o il contratto sia scaduto, revocarla e informarne l'utente via posta elettronica e numero di telefono mobile.
- In caso di decesso del titolare (persona fisica) o di estinzione della persona giuridica, revocare previo accertamento l'identità digitale.

- Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale.
- Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione.
- Nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale.
- Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.
- In caso di richiesta di revoca dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.
- Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa.
- All'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta.
- In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.
- Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID.

- Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, adottando idonee misure di sicurezza (art. 31 D.LGS 196/2003) ed utilizzando meccanismi di cifratura.

3.2 Obblighi del Proprietario dell'Identità Digitale

Di seguito vengono elencanti gli obblighi a cui il proprietario dell'Identità Digitale si fa carico:

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

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

- In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali.

3.3 Responsabilità

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

- Attribuisce l'Identità Digitale e rilascia le credenziali connesse attenendosi alle Regole Tecniche emanate dall'AgID.
- Si attiene alle misure di sicurezza previste dal "Codice in materia di protezione dei dati personali" ai sensi del D.Lgs. n.196 del 30.06.2003 e s.m.i. nonché alle indicazioni fornite nell'informativa pubblicata sul sito https://www.sielteid.it.
- Procede alla sospensione o revoca delle credenziali in caso di richiesta avanzata dall'utente per perdita del possesso o compromissione della segretezza, per provvedimento dell'AgID o su propria iniziativa per acquisizione della conoscenza di cause limitative della capacità dell'utente, per sospetti di abusi o falsificazioni.

4 CARATTERISTICHE GENERALI

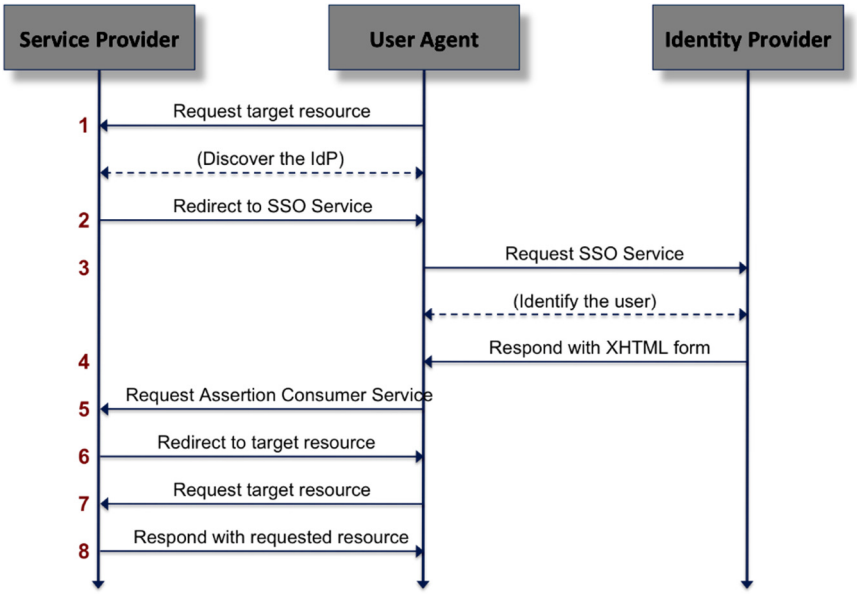
L' Identity Management (IDM) consiste nella gestione e verifica dell'identità degli utenti che operano on-line. In particolare, un sistema sviluppato in ambito IDM provvede all'autenticazione ed all'autorizzazione di un individuo fisico al fine di utilizzare specifiche applicazioni o servizi offerti da un Ente o da un'azienda. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte di AgID, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni.

Nell'ambito del sistema SPID vengono individuati i seguenti soggetti:

- **Gestore dell'identità digitale** (detto Identity Provider) – gestisce le identità digitali e provvede a tutti i meccanismi di autenticazione e autorizzazione di un utente.
- **Fornitore dei servizi** (detto Service Provider) – fa uso del gestore dell'identità digitale (IdP) per autenticare e autorizzare l'accesso agli utenti, detti User Agent (UAs), alle proprie aree dei servizi riservati.
- **Utente (**detto User Agent) – richiede e dispone di una o più identità digitali, che contengono le informazioni necessarie all'identificazione da parte del fornitore di servizi (Service Provider), come ad esempio il sito dell'Agenzia delle Entrate o quello dell'INPS.

Lo scopo è quello di mettere in relazione i suddetti soggetti per le attività necessarie alla richiesta e fruizione di un servizio online, erogato da un Fornitore dei servizi a seguito della richiesta da parte di un utente.

Lo schema generale del processo di autenticazione viene illustrato nella seguente figura:



L'utente, tramite il sito web del fornitore dei servizi (Service Provider), chiede l'accesso alle funzioni per le quali è necessaria l'autenticazione e gli viene proposto di scegliere il proprio gestore delle identità (Identity Provider) (passi 1 e 2 della figura). Dopo aver effettuato la scelta, il browser dell'utente viene re-diretto sul sito dell'Identity Provider con la richiesta di autenticazione, il livello di sicurezza ed il set di dati richiesti (passi 2 e 3 della figura). L'utente inserisce le proprie credenziali in funzione del livello di sicurezza richiesto e, se le credenziali vengono verificate correttamente, viene re-diretto nuovamente sul sito del Service Provider, dove può avere accesso alle funzioni (pass 4 e 5 della figura). Infine, il Service Provider può richiedere all'Identity Provider una serie di attributi qualificati necessari per l'elaborazione delle richieste.

I servizi forniti da Sielte fanno riferimento al rilascio e alla gestione delle Identità Digitali SPID (Sistema Pubblico dell'identità Digitale) con il ruolo di Identity Provider.

4.1 Livelli di servizio garantiti

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

ID	Indicatore di qualità	Modalità di Funzionamento	Valore limite
IQ-01	Disponibilità del sotto servizio di registrazione identità	*Erogazione automatica*	>= 99,0%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-02	Tempo di risposta del sotto servizio di registrazione identità		<= 24h (ore lavorative)
IQ-03	Disponibilità del sotto servizio di gestione rilascio credenziali	*Erogazione automatica*	>= 99,0%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-04	Tempo di rilascio credenziali		<= 5 giorni lavorativi
IQ-05	Tempo riattivazione delle credenziali		<= 2 giorni lavorativi
IQ-06			>= 99,0%

	Disponibilità del sotto servizio di sospensione e revoca delle credenziali		Singolo evento di indisponibilità < =6 ore
IQ-07	Tempo di sospensione delle credenziali		< =30 minuti
IQ-08	Tempo di revoca delle credenziali		<= 5 giorni lavorativi
IQ-09	Disponibilità del sotto servizio di rinnovo e sostituzione delle credenziali	*Erogazione automatica*	>= 99,0%
		Erogazione in presenza	>= 98,0%
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		<= 5 giorni lavorativi
IQ-11	Disponibilità del sotto servizio di autenticazione		>= 99,0%
			Singolo evento indisponibilità <= 4 ore
IQ-12	Tempo di risposta del sotto servizio di autenticazione		Tempo di risposta <=3 sec almeno nel 95,0% delle richieste

IQ-13	RPO sotto servizio registrazione e rilascio delle identità		1 ora
IQ-14	RTO sotto servizio registrazione e rilascio delle identità		8 ore
IQ-15	RPO sotto servizio di sospensione e revoca delle credenziali		1 ora
IQ-16	RTO sotto servizio di sospensione e revoca delle credenziali		8 ore
IQ-17	RPO sotto servizio di Autenticazione		1 ora
IQ-18	RTO sotto servizio di Autenticazione		8 ore

Il Gestore, oltre a quanto sopra riportato, si impegna a garantire l'integrità e la disponibilità delle tracciature relative alle transazioni di autenticazione già concluse.

Il titolare dell'Identità Digitale può visualizzare direttamente i contenuti delle tracciature delle transazioni di autenticazione ad essa relative collegandosi al Portale del Gestore. Eventuali richieste al di fuori dei termini previsti dal Portale e relative alle transazioni degli ultimi 24 mesi (Registro delle transazioni del Gestore, ([Modalità Attuative] art.29, terzo capoverso) degli ultimi possono essere richieste dal titolare a mezzo di documento cartaceo inviato per raccomandata A/R o a mezzo di documento informatico (firmato con firma elettronica qualificata o con firma digitale) inviato per Posta Elettronica Certificata.

4.2 Misure anti-contraffazione

Le misure di anti contraffazione delle identità digitali, messe in atto da Sielte in qualità di gestore di identità, sono di fondamentale importanza per prevenire il verificarsi del furto d'identità. Queste ci assicurano un'identità certa per l'accesso ai servizi telematici che fanno utilizzo di SPID nel rispetto delle norme e sfruttando gli standard tecnologici presenti nel mercato. Vale la pena sicuramente precisare che l'**identità digitale** non è esattamente la corrispondenza dell'**identità fisica** in quanto ci sono aspetti della personalità che ne contraddistinguono l'univocità. Questo concetto evidenzia che per accedere a dei servizi telematici attraverso un'identità digitale è necessario rispettare la tutela della privacy, con rifermento al personale ed essere certi dell'identità di chi si sta autenticando.

La norma che più si avvicina ed affronta queste tematiche è la ISO/IEC 29115; pertanto, per combattere possibili sistemi di contraffazione, le procedure più certe sono:

- l'identificazione a vista, ovvero l'accertamento dell'identità fisica;
- l'identificazione remota, ovvero l'accertamento dell'identità tramite strumenti audio/video remoti;
- la firma digitale, ovvero la ricezione delle richieste di iscrizione, sospensione e revoca firmate digitalmente con certificati emessi da certificatori accreditati a livello nazionale.

La verifica dell'identità viene compiuta attraverso l'accesso alle fonti autoritative, effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM.

I controlli effettuati da Sielte si basano sull'utilizzo del sistema SCIPAFI, Sistema pubblico di prevenzione, che consente il riscontro dei dati contenuti nei principali documenti d'identità e riconoscimento con quelli registrati nelle banche dati degli enti di riferimento. Il riscontro si configura, quindi, come efficace strumento di prevenzione per i furti d'identità sia totali che parziali.

Nell'attesa che i gestori di identità digitale ottengano le autorizzazioni all'accesso alle fonti autoritative, Sielte esegue una serie di controlli manuali accedendo ai sistemi pubblici resi disponibili dagli Enti competenti. I controlli possono essere eseguiti dall'operatore nel caso di riconoscimento a mezzo webcam oppure direttamente nelle sedi di Sielte.

I controlli eseguiti durante il processo di identificazione sono i seguenti:

- il codice fiscale viene verificato tramite il servizio messo a disposizione dall'Agenzia delle Entrate sul suo portale;
- il codice del documento presentato viene verificato presso il servizio presente sul portale della Polizia di Stato per verifica e smarrimento, furto e contraffazione del documento di identità;
- il numero della tessera sanitaria viene verificato mediante ricorso a SCIPAFI.

Inoltre, le procedure di identificazione prevedono ulteriori livelli di controllo:

- l'operatore che esegue il riconoscimento a mezzo webcam o di presenza, non ammette documenti in fotocopia, ma solo documenti in originale;
- l'immagine della documentazione raccolta è conservata a norma di legge in maniera non modificabile;
- il riconoscimento a mezzo webcam è accessibile solamente ai Titolari che dichiarano di voler presentare i documenti maggiormente diffusi (patente, carta di identità e passaporto), le cui caratteristiche sono riscontrabili anche da remoto. Per gli altri tipi di documenti ammessi dal DPR 445/2000 (patente nautica, porto d'armi, tesserini ministeriali, patentino di conduzione impianti termici, ecc.), stante la minore diffusione che ne comporta una minore conoscenza delle caratteristiche essenziali, l'identificazione può essere eseguita solamente di presenza, per accertare la bontà del documento con l'analisi della materialità dello stesso.

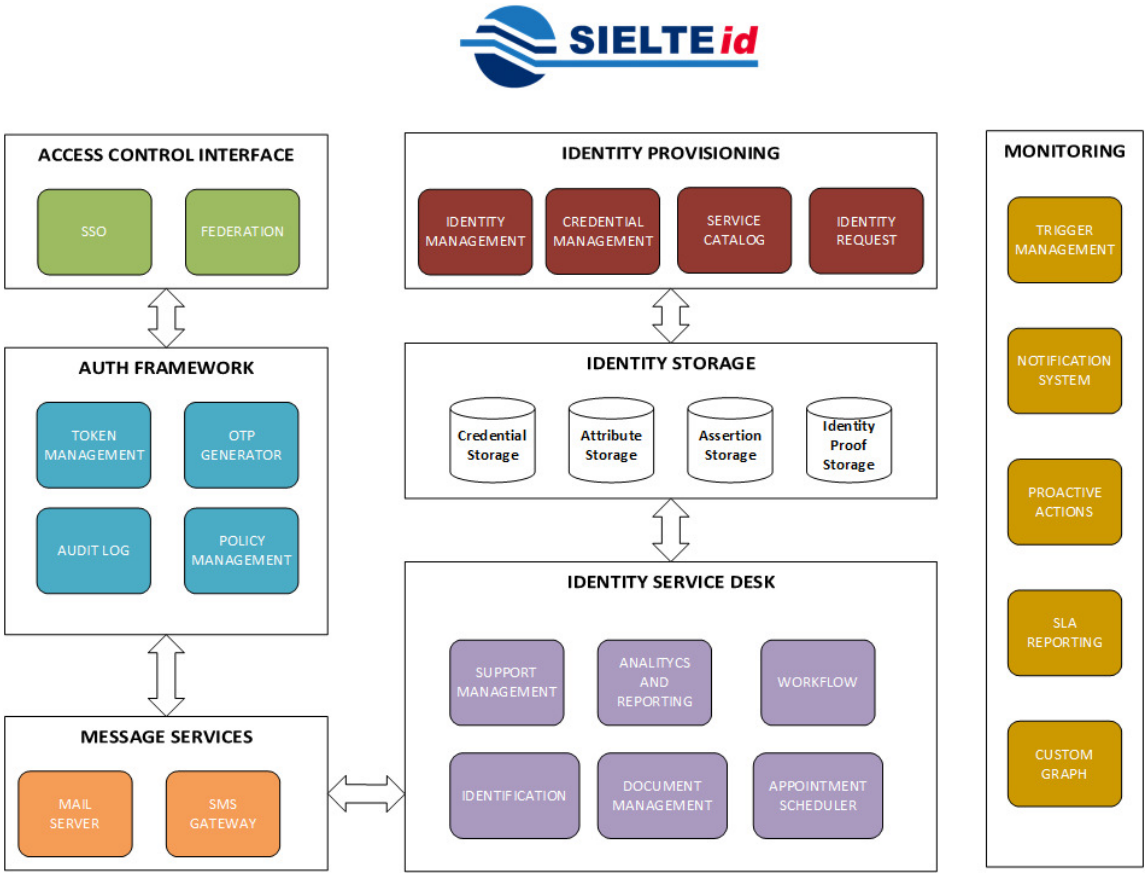
Le misure anticontraffazione si avvalgono anche di elementi tecnologici:

- sono utilizzati algoritmi crittografici robusti per garantire riservatezza e integrità dei dati, sulla base di quanto prescritto normativamente e allineato con le linee guida internazionali e per la generazione e protezione dei codici OTP;
- la firma digitale, ove utilizzata, deve essere basata su certificati emessi da un certificatore qualificato.

5 ARCHITETTURA LOGICA

Sielte adotta una suite di prodotti per implementare la migliore soluzione utile a realizzare la propria piattaforma di Identity Provider per il sistema di autenticazione SPID. Nel presente capitolo sono descritte le architetture, applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche del DPCM.

L'architettura della piattaforma IdP per SPID, che Sielte mette a disposizione, è basata su l'integrazione di prodotti e tecnologie di tipo Open Source con componenti di livello Enterprise. In figura è possibile visualizzare i componenti dell'architettura dell'infrastruttura utilizzata per la gestione delle identità digitale.



Il servizio di Identity Management mette a disposizione una serie di funzionalità per l'amministrazione delle identità degli utenti e il loro provisioning.

Come si evince dallo schema in figura, i blocchi sono separati tra di loro al fine di garantirne i migliori livelli di sicurezza. Di seguito viene riportata una sintetica descrizione degli elementi che compongono l'infrastruttura:

- **Identity Management –** contiene un'applicazione web sviluppata da Sielte per il rilascio dell'identità digitale e per la gestione delle relative credenziali. Tramite questo elemento l'utente ha la possibilità di gestire sia la fase di richiesta che il ciclo di vita dell'identità digitale. In particolare sono disponibili le funzioni di richiesta dell'identità digitale ed accettazione delle Condizioni Generali del Servizio, modifica degli attributi e gestione delle credenziali.
- **Identity Storage –** questi sono identificati come i contenitori, ridondati e sicuri, di tutte le informazioni che riguardano:
    - Identità Digitale
    - Attributi primari e attributi secondari
    - Documentazione
    - Credenziali
- **Authentication Framework –** contiene una soluzione modulare per autenticazione a singolo fattore e a due fattori, in particolare con i token OTP. Il prodotto utilizzato in questo caso è **PrivacyIDEA**. Grazie alla struttura modulare è stato adattato e migliorato per l'implementazione dell'architettura SPID. Si integra facilmente con la piattaforma di Identity Management e con i database sul componente Identity Storage.
- **Identity Provider Interface –** contiene il servizio di **Single Sign-On (SSO)**, che offre un accesso sicuro con unica login all'interno di una rete di più fornitori di servizi. Il servizio di SSO è basato su standard internazionali e di mercato e in particolare rispetta le regole specificate nel regolamento tecnico di SPID.

- **Service Desk –** Strumento utilizzato dagli utenti per segnalare eventuali anomalie riscontrate e dagli operatori Sielte per fornire servizio di assistenza sulle identità digitali. Nel caso specifico, il software utilizzato per il servizio di Service Desk è **OTRS**.
- **Message Services –** servizio utilizzato internamente per l'invio e la ricezione di posta elettronica agli utenti e per i servizi di invio SMS in fase di registrazione/identificazione.
- **Monitoring –** i servizi di monitoraggio notificano eventuali interruzioni di servizio e tengono traccia delle prestazioni dell'intera infrastruttura. In questo modo si riducono i tempi di risoluzione di eventuali disservizi grazie alle funzionalità di analisi e a misure correttive automatiche. Nel caso specifico il software utilizzato per il servizio di monitoraggio è **Zabbix**.

5.1 Servizi

Analizzando in dettaglio gli aspetti inerenti l'Identity Provider si possono definire tre diversi componenti:

- **Servizi di autenticazione**: forniscono i servizi necessari per poter usufruire dei flussi di autenticazione e gestire le credenziali necessarie per ogni utente registrato al sistema. Questo si integra e interagisce con i processi di autenticazione informatica rivolta all'utente finale, che interagendo con l'utente, ne verifica l'identità.
- **Servizi di gestione delle identità**: forniscono i servizi necessari per poter usufruire della base dati delle identità (attributi principali, attributi secondari e stato dell'identità digitale) e delle credenziali associate ad ogni utente.
- **Servizi di federazione**: forniscono i servizi necessari per poter generare i token di autenticazione sulla base delle caratteristiche definite dallo SPID per l'utilizzo da parte del Fornitore di Servizi.

Il front-end applicativo fornisce all'utente finale una specifica interfaccia di autenticazione. L'applicazione utilizza le informazioni della richiesta SAML emessa dal Fornitore di Servizi (*AuthNRequest*) e proveniente tramite re-direzione del browser dell'utente, per determinare il livello di autenticazione richiesto dalle specifiche SPID (*AuthnContextClassRef*). A questo punto, verrà attivato il flusso di autenticazione che corrisponde al livello di autenticazione richiesto.

Sulla base della scelta dell'utente, l'applicazione avrà accesso alla componente, che creerà una sessione autenticata, necessaria ad accedere ai servizi di federazione e ala componente di persistenza delle credenziali per interagire con le credenziali dell'utente. Inoltre, l'applicazione dispone delle interfacce essenziali per poter inviare eventuali SMS o e-mail all'utente associato all'identità digitale.

Quindi, l'utente avrà ottenuto una sessione di autenticazione valida per l'accesso ai servizi configurati nella federazione con il fornitore di servizi, come da specifiche dello SPID. Tale sessione è rappresentata da un cookie cifrato salvato sul browser dell'utente.

5.2 Livelli di sicurezza

Il sistema SPID prevede tre livelli di sicurezza, che sono specificati nella ISO-IEC 29115. Nel caso di Sielte, i flussi di autenticazione implementati sono:

- **Livello 1 SPID** – basato su un singolo fattore di autenticazione, è implementato attraverso il controllo di una parola segreta (password), associata ad un codice identificativo utente, che rispetta determinate politiche di sicurezza.
- **Livello 2 SPID** – basato su un un'autenticazione a due fattori, è implementato tramite il controllo di una parola segreta (password), con le stesse caratteristiche del Livello 1 SPID, combinato alla verifica di un codice One Time Password, inviato tramite un SMS o alla verifica di un codice TOTP (Time based One Time Password), generato attraverso l'applicazione *MySielteID* per dispositivi mobile Android, iOS e UWP.

Il codice One Time Password viene inviato al numero di telefono cellulare associato alla propria identità digitale e fornito in fase di registrazione. Questo sistema è chiamato ***Token out of band***, cioè un dispositivo (token), indirizzabile in modo univoco, che può ricevere un codice/segreto, selezionato dal gestore dell'identità, per essere usato, una sola volta, durante la sessione di servizio.

5.3 Generazione OTP

Il metodo di generazione dell'OTP è basato sull'algoritmo TOTP, che rispetta le specifiche RFC 6238 dell'IETF, ed è un algoritmo che, a partire da una chiave segreta condivisa e dall'ora corrente, calcola tramite una funzione *hash* crittografica una one-time password.

La chiave segreta dell'utente, associata al token (seme), è condivisa tra l'IdP e l'App e lo scambio della chiave avviene solamente una volta, durante la fase di inizializzazione dell'App.

Il seme viene memorizzato all'interno dell'App ed è cifrato, utilizzando l'algoritmo di crittografia AES a 256 bit per ragioni legate alla sicurezza.

5.4 Sicurezza dei dati

Per quanto concerne la sicurezza dei dati memorizzati, è stato implementato un meccanismo ad hoc, basato sull'algoritmo di crittografia AES (*Advanced Encryption Standard*, a chiave simmetrica, operante su 256 bit di lunghezza finita, organizzati in un blocco di dimensione fissa di 128 bit), in cui la chiave di cifratura adoperata consiste in una coppia di valori, di cui il primo elemento è il codice di sicurezza, scelto ed inserito dall'utente, e il secondo elemento è il '*salt'* (una sequenza di byte), che viene concatenata in una stringa, data in input alla funzione crittografica di *hash* SHA-256; quest'ultima funzione produce come risultato la chiave di sicurezza, utilizzata per cifrare il file, in cui sono memorizzati i dati in maniera sicura. Tale meccanismo è adottato su tutti i sistemi operativi per i quali è stata progettata l'applicazione: Android, UWP e iOS.

Un ulteriore strumento adottato, per garantire una sicurezza elevata, è il lettore di impronte digitali presente sui dispositivi (Touch ID per iOS e Fingerprint per Android). Il meccanismo di rilevamento delle impronte digitali utilizza *l'iOS Keychain* su dispositivi con sistema operativo iOS e *l'Android Keystore System* per dispositivi con sistema operativo Android.

5.5 Lettore di impronta digitale e riconoscimento facciale

Durante la configurazione dell'App l'utente può associare la propria impronta digitale (se disponibile ed abilitato sul dispositivo il lettore d'impronta), come codice di protezione per potervi accedere. Nel caso di iPhone X è possibile abilitare il riconoscimento facciale tramite la funzionalità Face ID.

Tale associazione è possibile da apparato mobile Android, iOS 9 o superiore con lettore d'impronta digitale o di riconoscimento facciale integrato.

L'utente può, in qualunque momento, abilitare e disabilitare l'impronta digitale (o riconoscimento facciale), tramite l'apposita funzionalità disponibile nell'app MySielteID.

Sielte non effettua alcun trattamento dei dati personali biometrici, relativi all'impronta digitale, che vengono acquisiti dall'apparato mobile utilizzato dall'utente, e, pertanto, non può essere ritenuta responsabile di eventuali danni, diretti o indiretti, derivanti dal non corretto utilizzo da parte dell'utente o da eventuali compromissioni del sensore di rilevamento e dei relativi servizi di gestione dell'apparato mobile.

5.6 Codici e formati di messaggi di anomalia

Durante il processo di autenticazione con il gestore delle identità potrebbero verificarsi degli errori, presentati all'utente che sta tentando di utilizzare il servizio. In allegato a questo Manuale Operativo viene inserita la tabella degli errori indicata dall'Agenzia e disponibile come Allegato A.

Sielte, nel rispetto delle indicazioni dell'Agenzia, si impegna a implementare e gestire per la piattaforma *SielteID* tutte le anomalie previste secondo quanto riportato nella tabella dell'Allegato A.

5.7 Sistema di monitoraggio

Il sistema di monitoraggio utilizzato da Sielte offre una serie di strumenti avanzati e flessibili, che consentono di monitorare le funzionalità e l'integrità dei server fisici e virtuali in Cloud, della rete e dei servizi attraverso meccanismi visuali (mappe e grafici avanzati), utilizzando sistemi di notifica basati su email, SMS, e messaggistica in generale.

I parametri che vengono verificati all'interno dell'infrastruttura Cloud Privato e della piattaforma SPID sono:

- raggiungibilità sistemi;
- memoria RAM utilizzata;
- CPU utilizzate;
- raggiungibilità device di rete;
- spazio disco singoli sistemi;
- stato dei volumi/disponibilità storage;
- raggiungibilità di rete esterna /interna;
- tempo di accensione e orario di sistema.

Attraverso l'utilizzo di agenti nativi si riesce a garantire una maggiore velocità nelle interrogazioni sullo stato dei controlli ed una maggiore compatibilità per i diversi sistemi. Tramite l'utilizzo di protocolli standard (Agent, Agent-less, SNMP v1/v2/v3 poll & trap, Log parsing, ODBC, Java, SSH, Telnet, custom script ecc.…) riusciamo a monitorare ed intervenire tempestivamente su qualsiasi elemento ICT.

Il sistema è configurato per rilevare anomalie ai sistemi attraverso due modalità:

- **Polling** – vengono interrogati ciclicamente tutti i server per verificare il loro stato;
- **Trapping** – il server informa la piattaforma di monitoraggio circa il verificarsi di una eccezione.

5.8 Sistemi di autenticazione

Sielte mette a disposizione del titolare dell'Identità Digitale dei sistemi di autenticazione:

1. *Basic Authentication* (Livello SPID 1, LoA2)
2. *Token out of Band* (Livello SPID 2, LoA3)
3. *Token crittografico software multi-fattore* (Livello SPID 2, LoA3)

Nei due paragrafi successivi vengono descritte le caratteristiche di tutti i sistemi.

5.8.1 *Basic Authentication*

Il sistema di autenticazione *Basic Authentication* prevede l'utilizzo di credenziali a singolo fattore, ovvero la coppia (username, password) scelta dal titolare dell'Identità Digitale in fase di creazione della stessa.
Al fine di garantire un alto livello di sicurezza, tutte le password devono soddisfare una serie di policy di sicurezza e non vengono mai memorizzate in chiaro, bensì cifrate attraverso algoritmi di *hashing*, nello specifico SHA256. Inoltre, al fine di garantire un livello di sicurezza maggiore, *SielteID* obbliga i titolari delle Identità Digitale a cambiare le proprie password ogni 6 mesi. Opportuni sistemi proattivi per la gestione della scadenza della password provvedono ad informare l'utente, con un certo preavviso, attraverso messaggi inviati ai recapiti associati al profilo.
L'autenticazione con *SielteID* avviene attraverso uno scambio di messaggi di richiesta e risposta, secondo il documento delle regole tecniche di SPID definito da *AgID*.

Il processo di autenticazione avviene attraverso le seguenti fasi:

1. l'utente richiede l'accesso ad un servizio protetto sul sito del fornitore dei servizi (*Service Provider*).
2. il fornitore di servizi (*Service Provider*) genera una richiesta di autenticazione e la inoltra a *SielteID* (*Identity Provider*) attraverso il browser dell'utente, mentre quest'ultimo viene reindirizzato alla pagina di login di *SielteID*.
3. l'utente inserisce il proprio codice fiscale e la propria password nel form di login.
4. *SielteID* avvia una query all'*Identity Storage* per determinare la entry associata all'username fornito.
5. l'*hash* della password inserita dall'utente viene confrontato con quello memorizzato nella entry.
6. se l'esito del confronto al punto precedente è positivo e la password non risulta scaduta o bloccata, l'autenticazione si conclude con successo.
7. sul browser dell'utente viene installato un cookie, che serve per identificare la sessione di SSO attivata.
8. l'utente viene reindirizzato alla pagina del servizio richiesto sul sito del Service Provider.

5.8.2 *Token out of Band*

Il sistema di autenticazione *Token out of Band* prevede l'utilizzo delle credenziali a singolo fattore della *Basic Authentication*, affiancato all'utilizzo di un codice OTP (*One Time Password*) casuale e con validità limitata, inviato tramite SMS al numero di cellulare verificato in possesso del titolare dell'Identità Digitale.
Il processo di autenticazione avviene in maniera del tutto analoga alla *Basic Authentication* fino alla verifica delle credenziali utente di Livello SPID 1.

Da qui, il processo di autenticazione procede attraverso le seguenti fasi:

1. se le credenziali di Livello 1 inserite dall'utente sono corrette e la password non risulta scaduta o bloccata, *PrivacyIDEA* provvede a generare un codice OTP casuale della validità di 5 minuti dando inizio ad una *Challenge di autenticazione*.
2. viene memorizzata la chiave segreta con cui il codice OTP viene generato e successivamente verificato ed inviato all'utente via SMS tramite *l'SMS Gateway*.
3. l'utente viene reindirizzato alla pagina preposta all'inserimento del codice OTP.
4. l'utente inserisce il codice OTP ricevuto.
5. il codice OTP inserito viene confrontato con quello memorizzato nel database.
6. se il codice è corretto e la *Challenge di autenticazione* non è ancora scaduta, l'autenticazione si conclude con successo.
7. l'utente viene reindirizzato alla pagina del servizio richiesto sul sito del Service Provider, senza che venga creata alcuna sessione di autenticazione.

5.8.3 *Token crittografico software multi-fattore (MF)*

Il sistema di autenticazione *Token crittografico software multi-fattore* prevede l'utilizzo delle credenziali a singolo fattore della Basic Authentication, affiancato all'utilizzo di un codice OTP (One Time Password) generato tramite applicazione installata sul dispositivo dell'utente.

L'applicazione, prima di essere utilizzata, deve essere inizializzata da parte dell'utente. Il processo di attivazione prevede che l'utente esegua le seguenti istruzioni:

- accede alla pagina del profilo, con autenticazione di Livello 2 SPID, disponibile tramite l'indirizzo https://profilo.sielteid.it.
- richiede l'inizializzazione di un nuovo dispositivo tramite la voce "Aggiungi dispositivo". Viene mostrato un codice QR Code temporaneo, con una durata di 10 minuti, da utilizzare all'interno dell'applicazione.

- sul dispositivo mobile viene avviata l'applicazione MySielteID. A questo punto vengono richieste le credenziali di accesso SPID e, se validate con successo, viene effettuata la lettura del QR Code generato dal profilo.
- completata la validazione del QR Code, viene invitato l'utente a scegliere un PIN segreto, che abilita l'applicazione alla generazione del codice OTP da utilizzare in fase di autenticazione.

Il processo di autenticazione avviene in maniera del tutto analoga alla *Basic Authentication* fino alla verifica delle credenziali utente di Livello SPID 1.

Successivamente, se l'utente ha attivato l'applicazione, verrà richiesta l'apertura dell'applicazione sul proprio dispositivo, da sbloccare inserendo il codice personal segreto inserito in fase di inizializzazione, e verrà generato il codice OTP, valido solo 60 secondi, da inserire durante l'autenticazione di Livello SPID 2.

Se il codice è corretto e la Challenge di autenticazione non è ancora scaduta, allora l'autenticazione si conclude con successo. Infine, l'utente viene reindirizzato alla pagina del servizio richiesto sul sito del Service Provider, senza che venga creata alcuna sessione di autenticazione.

6 RILASCIO IDENTITÀ DIGITALE

Il processo di rilascio dell'identità digitale implementato da Sielte come Gestore delle Identità Digitali prevede le seguenti fasi:

In ogni elemento del processo vengono adottate delle procedure per garantire la sicurezza delle informazioni e mitigare i rischi, tra cui quello ad impatto maggiore, il tentativo di furto di una identità da parte di estranei.

Il Richiedente si appresta ad effettuare la registrazione e scegliere una delle modalità di identificazione. Durante questa fase l'IdP effettuerà le prime verifiche.

L' IdP deve verificare l'identità del Titolare delle informazioni prima di procedere al rilascio dell'ID.

La procedura di identificazione comporta che l'Utente Titolare sia identificato, prima del rilascio della ID, secondo una delle procedure di seguito specificate.

I processi di rilascio della ID prevedono che:

1. la fase di identificazione sia eseguita prima della contrattualizzazione del servizio;
2. il Richiedente sottoscriva il contratto di adesione al servizio con una delle modalità previste nelle procedure di rilascio.
3. il Richiedente riceve dall'IdP userID e password temporanea, che provvede a modificare obbligatoriamente al primo accesso al portale per l'attivazione dell'ID.

L'identità del soggetto Richiedente viene accertata dall'IdP secondo le seguenti modalità:

1. identificazione informatica, grazie all'utilizzo di una firma digitale o una firma elettronica qualificata in possesso del Richiedente;
2. identificazione informatica, grazie all'utilizzo di una carta CIE, CNS o TS-CNS in possesso del Richiedente;
3. da remoto, grazie a una sessione webcam con un Incaricato dell'IdP;
4. in presenza presso un Incaricato dell'IdP.

Di seguito verranno descritti tutti i processi, che sono utilizzati da Sielte per il rilascio delle identità digitali.

6.1 Richiesta Identità

L'utente che desidera richiedere l'identità digitale da utilizzare all'interno di SPID può connettersi al sito web https://www.sielteid.it ed effettuare la Registrazione tramite il Modulo di Adesione elettronico, oppure recarsi presso gli uffici preposti e compilare il Modulo di Adesione Cartaceo, in presenza di un Operatore IdP Sielte.

6.1.1 *Registrazione tramite Modulo di Adesione elettronico*

Durante tutta la fase di Registrazione, sulla sezione destra di ogni pagina, il richiedente visualizza:

- ✓ Il Tempo Medio per completare la fase corrente.
- ✓ Le Informazioni Necessarie, ovvero un elenco dei dati che verranno richiesti per la registrazione; man mano che proseguirà con la registrazione il Richiedente vedrà la spunta in verde in corrispondenza dei dati già inseriti.
- ✓ Le Attività da svolgere durante quella sezione.

Il processo si compone nelle fasi descritte di seguito:

1. il Richiedente compila il modulo di richiesta elettronico, inserendo i propri dati anagrafici, gli estremi del documento di identità prescelto per l'identificazione (i documenti di riconoscimento ammessi per l'identificazione sono tutti quelli ammessi dal DPR 445/2000, art. 35)[1], il proprio indirizzo mail ed il numero di telefono cellulare

[1] DPR 445/2000, Art. 35 Documenti di identità e di riconoscimento

1. In tutti i casi in cui nel presente testo unico viene richiesto un documento di identità, esso può sempre essere sostituito dal documento di riconoscimento equipollente ai sensi del comma 2.

2. Sono equipollenti alla carta di identità il passaporto, la patente di guida, la patente nautica, il libretto di pensione, il patentino di abilitazione alla conduzione di impianti termici, il porto d'armi, le tessere di riconoscimento, purché' munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato.

3. Nei documenti d'identità e di riconoscimento non è necessaria l'indicazione o l'attestazione dello stato civile, salvo specifica istanza del richiedente.

e presta il consenso, qualora necessario, all'Informativa ai sensi del D.L.vo n. 196/2003 per il trattamento dei dati effettuato nell'ambito dei Servizi Sielte .

In questa fase Sielte, tramite il sistema, effettua una verifica della veridicità e univocità in ambito Sielte del codice fiscale (tramite i dati Nome, Cognome, Data e Comune di Nascita) e dell'indirizzo mail.

In particolare, in fase di compilazione, il richiedente sceglie la tipologia di profilo con cui registrarsi. In SPID vengono identificati due tipologie di utente: **persona fisica** e **persona giuridica**.

Per le persone fisiche sono obbligatori i seguenti attributi:

- Dati di contatto: Indirizzo mail e numero di cellulare
- Dati Personali/Anagrafici: Nome, Cognome, Codice Fiscale, Sesso, Data e Luogo di nascita, Indirizzo di Residenza
- Estremi di un valido documento di identità: Tipo, Numero, Ente di Rilascio, Data di Rilascio, Data di Scadenza.

Per le persone giuridiche si aggiungono i seguenti attributi obbligatori:

- Denominazione/ragione sociale
- Codice fiscale o P.IVA (se uguale al codice fiscale)
- Sede legale
- Visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società (in alternativa atto notarile di procura legale), firmata digitalmente dal richiedente
- I Dati personali e gli estremi del documento di identità devono essere quelli del Rappresentante Legale.

Per entrambi i profili il richiedente ha facoltà di inserire anche altre informazioni aggiuntive così come l'indirizzo PEC, gestite come Attributi Secondari, i quali sono

associati all'identità digitale, ma non utilizzati nel contesto di erogazione dei servizi da parte di Sielte.

Effettua la verifica Captcha e procede con la registrazione.

2. Il Richiedente visualizza il riepilogo dei dati inseriti, può tornare alla pagina precedente per modificarli, prendere visione ed accettare le Condizioni Generali Contrattuali e del Manuale Operativo.
3. Il richiedente riceve una email contenente in allegato il Modulo di Adesione compilato, il proprio codice fiscale (username),una password temporanea ed un link su cui deve cliccare per validare il proprio indirizzo mail. In questo modo Sielte si accerta che l'indirizzo fornito corrisponda ad una reale casella di posta elettronica, così come previsto dall'Art. 5 e dall'Art.8, comma g) del Regolamento.
4. Richiede il codice OTP all'interno della pagina su cui viene reindirizzato cliccando il link di verifica; contestualmente riceve una OTP sul proprio telefono, che deve inserire, sempre all'interno della pagina su cui si trova, nel campo di testo dedicato, al fine di certificare l'esistenza e la proprietà del numero di telefono (come previsto dall'Art.5 e dall'Art.8, comma g) del Regolamento). Nel caso in cui immette il codice errato, può riprovare solo altre due volte. Procede alla fase successiva immettendo il codice OTP corretto.
5. Viene richiesto di allegare foto o scansione del fronte e del retro del documento di riconoscimento (del quale ha precedentemente inserito gli estremi) e della tessera sanitaria (in formato PDF o JPG) in corso di validità.

   Se persona giuridica, viene richiesto di caricare la Visura Camerale della società (o in alternativa atto notarile di procura legale), firmata digitalmente dal richiedente, della quale ha inserito precedentemente nel modulo gli estremi.

   Dopo aver caricato i documenti, il richiedente clicca su Procedi. Il sistema gli richiede un ulteriore conferma, informandolo che non potrà modificare i documenti.

6. Il richiedente sceglie la modalità di identificazione, tra:

   a. ***Modalità Webcam***: il richiedente viene informato che per questa modalità di identificazione deve disporre di un PC o di uno Smartphone o di un Tablet, dotati di Webcam. In questa fase può annullare o confermare la sua scelta. Il Richiedente, per fissare l'appuntamento e procedere con l'identificazione tramite videochiamata da effettuare con l'operatore IdP Sielte, sceglie la data e l'ora tra quelle indicate come disponibili da Sielte, e la modalità/tecnologia per effettuare la videochiamata. Può scegliere tra 4 opzioni: Messenger.com, Hangouts, Skype o Cisco WebEx. Per le prime 3, dovrà inserire un recapito (indirizzo mail o account) per essere contattato e procedere con l'identificazione.

      Riceve una mail di conferma che riepiloga la data, l'ora e la tecnologia prescelta per l'appuntamento della videochiamata.

      Nel caso in cui scelga la tecnologia Cisco WebEx all'interno della mail, troverà un link per scaricare l'applicazione necessaria per la videoregistrazione.

   b. ***Modalità Di Persona:*** il richiedente viene informato che per questa modalità di identificazione deve stampare e firmare il modulo ricevuto via mail durante la prima fase del procedimento e fissare un appuntamento, scegliendo la sede dove recarsi per procedere con la fase di identificazione. In questa fase può annullare o confermare la modalità scelta.

      Confermando la modalità potrà scegliere la sede presso cui identificarsi e la data dell'appuntamento e Procede.

      Il Richiedente viene informato che i documenti sono stati caricati con successo e visualizza i dettagli dell'appuntamento; gli stessi vengono comunicati via mail per conferma e promemoria.

   c. ***Modalità Firma Digitale:*** il richiedente viene informato che per questa modalità di identificazione deve disporre di una Smart Card e lettore. In questa fase può annullare o confermare la modalità scelta.

Confermando la modalità gli vengono fornite le seguenti istruzioni: deve scaricare il Modulo di Richiesta ricevuto tramite mail, firmarlo digitalmente e caricarlo in questa sezione.

Il sistema informa il richiedente che il Documento è stato caricato con successo e di attendere una mail di conferma dell'avvenuta identificazione (che riceverà dopo la verifica del documento da parte di un Operatore IdP).

d. ***Modalità CIE/CNS (Smart Card e PIN):*** Il Richiedente viene informato che per questa modalità di identificazione deve disporre della Carta di Identità Elettronica o della Carta Nazionale dei Servizi e di un lettore di Smart Card. In questa fase può annullare o confermare la modalità scelta.

   Confermando la modalità, il Richiedente inserisce la CIE o CNS nel lettore collegato al PC, inserisce il PIN richiesto e se corretto viene identificato.

   Il Richiedente riceve una mail con i codici utente del servizio SPID e un link da cliccare per attivare l'identità.

Qualora il Richiedente, dopo la prima fase di registrazione, ovvero dopo la compilazione del Modulo e la ricezione della mail di verifica con username e password temporanea, debba interrompere la procedura per qualunque motivo (mancanza di rete, mancanza di disponibilità, ecc.), può in ogni momento riprendere dal punto in cui aveva lasciato, collegandosi al sito, cliccando su "Riprendi Registrazione" ed inserendo le proprie credenziali.

6.1.2 *Registrazione a vista tramite Modulo di Adesione Cartaceo*

Il Richiedente ha la possibilità di ottenere la sua identità digitale attraverso la compilazione del Modulo di adesione in forma cartacea , optando per la ***Registrazione ed Identificazione a vista tramite modulo cartaceo***.

Il Richiedente si reca in uno degli uffici preposti, consultabili tramite la mappa all'interno del sito www.sielteid.it, compila il Modulo di Adesione, prende visione e presta il consenso

dell'Informativa al trattamento dei dati ed alle Condizioni Generali del Servizio, e firma il Modulo.

Il Richiedente deve esibire all'Operatore IdP preposto il documento di riconoscimento, i cui estremi sono stati inseriti all'interno del modulo, integro, con fotografia e firma autografa ed in corso di validità e la tessera sanitaria in corso di validità.

L'Operatore IdP, ne verifica l'idoneità e ne acquisisce copia. Il richiedente completerà la sua fase di identificazione solo dopo un'ulteriore fase di verifica, che effettuerà l'Operatore IdP, dei documenti e dell'indirizzo mail e numero di telefono (questa fase di identificazione verrà descritta nel paragrafo 6.2.2.2.2 Identificazione a vista tramite modulo di adesione cartaceo).

6.2 Identificazione

Il processo di identificazione di un'identità (*Identity Proofing*) si compone dei seguenti passi:

- **Verifica** – accertamento della corretta validità delle informazioni tramite strumenti interni o esterni.
- **Dimostrazione** – acquisizione e accertamenti delle informazioni utili ad identificare una persona per uno specifico livello di sicurezza.

Sielte, per ulteriore tutela e sicurezza dei dati, predispone le misure di cifratura adottate dall'Organizzazione per tutti i documenti digitalizzati[2] e per i files audio, video, inviati o recapitati in loco, in conservazione e garantisce che la registrazione di tale documentazione ed in particolare del flusso audio/video sia limitata alla documentazione della reale volontà del richiedente di ottenere l'identità digitale, al fine di renderla strettamente correlata alle esigenze di riconoscimento e di documentazione previste dalla normativa di settore.

[2] Documenti cartacei acquisiti in forma digitale

Nel caso in cui vengano riscontrate anomalie, il personale di Sielte addetto all'identificazione è autorizzato a rifiutare il processo di identificazione.

6.2.1 *Verifica e Validazione dei dati*

Il personale addetto all'identificazione effettua le verifiche necessarie a validare i documenti e a verificare la stessa identità del richiedente attraverso l'accesso alle fonti autoritative effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM, principalmente attraverso l'utilizzo del sistema SCIPAFI, il quale consente il riscontro dei dati contenuti nei principali documenti d'identità e riconoscimento con quelli registrati nelle banche dati degli enti di riferimento. Il riscontro si configura, quindi, come efficace strumento di prevenzione per i furti d'identità sia totali che parziali.

Ogni richiesta viene presa in carico e gestita da un Operatore IdP Sielte.

Per la verifica del furto o smarrimento del documento l'operatore si avvale del servizio online disponibile sul sito della Polizia di Stato[3].

Per la verifica del codice fiscale l'operatore ricorre alla piattaforma SCIPAFI.

Inoltre l'Operatore IdP verifica che il documento di riconoscimento sia integro ed in corso di validità, rilasciato da un'Amministrazione dello Stato, munito di fotografia e firma autografa dello stesso e controlla la validità del codice fiscale/tessera sanitaria.

Sielte è responsabile della valutazione in merito alla veridicità delle informazioni relative all'identità, quindi l'operatore preposto all'attività, in caso di verifiche negative o per mancanza parziale o totale della documentazione richiesta, non avvia la fase di identificazione e quindi di attivazione dell'ID, bensì contatta il Richiedente tramite mail chiedendo di caricare la documentazione valida in sostituzione a quella presentata, piuttosto che caricare quella mancante.

[3] https://www.crimnet.dcpc.interno.gov.it/crimnet/ricerca-documenti-rubati-smarriti

Il richiedente può caricare i documenti richiesti nella form preposta, che visualizza cliccando il link all'interno della mail inviatagli. L'Operatore IdP verificherà nuovamente i documenti inseriti. Se la verifica è positiva, si procede alla fase di identificazione ed al rilascio dell'identità digitale.

6.2.2 *Identificazione in base alla modalità prescelta dal Richiedente*

6.2.2.1 IDENTIFICAZIONE A VISTA DA REMOTO

6.2.2.1.1 IDENTIFICAZIONE A VISTA DA REMOTO MEZZO WEBCAM

L'Operatore IdP ha in carico la Richiesta e, così come descritto all'interno del paragrafo 6.2.1 Verifica e Validazione dei dati, ha già effettuato le verifiche necessarie.

La Richiesta mostra all'Operatore IdP la tecnologia prescelta dall'utente in fase di registrazione per il contatto via Webcam (Messenger, Skype, Hangouts o Cisco WebEx), l'account e la fascia oraria di preferenza.

L'Operatore contatta il Richiedente secondo data e ora prescelte da quest'ultimo per l'appuntamento e, se disponibile, procede con l'identificazione a mezzo *Webcam;* l'operatore incaricato procede ad identificare il Richiedente grazie ad una sessione video registrata, seguendo il processo indicato sotto.

Se il Richiedente non è disponibile, viene concordato un ulteriore Appuntamento, secondo gli slot liberi e disponibili e verrà ricontattato successivamente dall'Operatore IdP.

Quindi, l'Operatore contatta il Richiedente ed avvia la videochiamata (non registrando ancora).

Sielte è responsabile della valutazione in merito alla sussistenza delle condizioni idonee della sessione (esplicitate nel flow chart), quindi l'Operatore preposto all'attività, nel caso in cui queste non si verifichino, può in ogni momento sospendere o non avviare il processo di identificazione (come previsto dall'Art. 8 del Regolamento).

L'Operatore avvia la registrazione, dichiara i propri dati identificativi e chiede al Richiedente se acconsente al trattamento dei dati personali contenuti nella registrazione audio/video e lo informa che la registrazione sarà conservata per 20 anni in modalità protetta ed i dati trattati in base all'articolo 7, commi 8 e 9 del DPCM (come previsto dall'Art. 8, commi a) e b) del Regolamento).

Il Richiedente acconsente e l'Operatore chiede conferma dei seguenti dati: generalità, data ed orario della videochiamata, volontà del Richiedente di dotarsi dell'identità digitale, dati inseriti nel Modulo di Adesione, numero di cellulare ed indirizzo di posta elettronica (come previsto dall'Art. 8, commi c), d), e) e f) del).

Il Richiedente dovrà rispondere alle domande di conferma di cui sopra, che l'Operatore in modo casuale gli porrà in modo diretto, indicando chiaramente e specificatamente i dati richiesti, evitando risposte affermative o non sufficientemente esaustive onde evitare la non ammissibilità della sessione.

L'Operatore chiede al Richiedente di mostrare il fronte e retro del documento di riconoscimento e codice fiscale/tessera sanitaria (come previsto dall'Art. 8, commi i) e j) del Regolamento). I documenti devono essere gli originali delle copie che il Richiedente ha inserito in fase di Registrazione.

L'Operatore chiede e ottiene conferma dal soggetto di aver preso visione ed accettare le condizioni contrattuali (come previsto dall'Art. 8, comma k) del Regolamento), disponibili sul sito web ed in fase di registrazione.

L'Operatore comunica che la fase di identificazione è andata a buon fine.

Termina la registrazione ed informa il Richiedente circa la tipologia di credenziali di cui disporrà per l'accesso ai servizi in rete e che riceverà una mail per attivare la sua Identità Digitale (come previsto dall'Art. 8, comma h) del Regolamento).

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

Al termine della sessione l'IdP considera identificato il Richiedente, il quale procederà, secondo quanto esplicitato successivamente, con l'attivazione dell'ID.

6.2.2.2 IDENTIFICAZIONE A VISTA

6.2.2.2.1 IDENTIFICAZIONE A VISTA TRAMITE MODULO DI ADESIONE ELETTRONICO

In caso di scelta di identificazione *a vista* il Richiedente incontra l'incaricato dell'IdP, recandosi negli uffici preposti, secondo Appuntamento stabilito in fase di Registrazione. Viene identificato di persona tramite esibizione di:

- Un valido documento di identità rilasciato da un'autorità Italiana, inserito già in fase di registrazione.
- Codice Fiscale utilizzato durante la fase di registrazione.

Tra i documenti validi riconosciuti da Sielte vi sono (i documenti di riconoscimento ammessi per l'identificazione sono tutti quelli ammessi dal DPR 445/2000, art. 35):

- **Carta d'identità** – deve essere INTEGRA ed in condizioni tali da potere leggere tutti i dati sopra scritti, nonché di poter identificare la persona che la presenta come titolare (foto perfetta) e la validità scritta sempre sul documento (10 anni dalla data del rilascio). Nel caso in cui l'operatore avesse qualche dubbio sulla validità del documento provvede a contattare l'Ufficio Anagrafe del comune di riferimento, oppure la Questura verificando i dati scritti sopra il documento.
- **Passaporto** – deve essere rilasciato dallo Stato Italiano, deve essere in perfette condizioni e contenere tutte le informazioni del richiedente. Tutte le pagine pari sono illustrate col disegno della pavimentazione della Piazza del Campidoglio e della statua equestre di Marco Aurelio. Quelle dispari sempre della pavimentazione della piazza e dal rosone del Duomo di Orvieto, insieme a uno o due monumenti architettonici nazionali.

L'Incaricato IdP acquisisce il Modulo di adesione firmato e, solo nel caso in cui il Richiedente in fase di registrazione non abbia inserito copia dei documenti, acquisisce una copia per immagine della documentazione di identificazione presentata dall'utente.

L'Incaricato informa il Richiedente circa la tipologia di credenziali di cui disporrà per l'accesso ai servizi in rete e che riceverà una mail per attivare la sua Identità Digitale.

L'Operatore IdP, conclusa positivamente l'identificazione, considera identificato il Richiedente, il quale procederà secondo quanto esplicitato successivamente con l'attivazione dell'ID.

Se il Richiedente è una persona giuridica, oltre al documento di riconoscimento e codice fiscale, deve fornire la visura camerale, firmata digitalmente dal richiedente, attestante i poteri di rappresentanza conferiti alla persona fisica, che sottoscrive e presenta l'istanza.

6.2.2.2.2 IDENTIFICAZIONE A VISTA TRAMITE MODULO DI ADESIONE CARTACEO

Il Richiedente si reca negli uffici preposti senza previa compilazione del modulo di richiesta elettronico e gli vengono forniti i seguenti moduli:

- Modulo di richiesta cartaceo, che il Richiedente dovrà compilare allo stesso modo di quello elettronico, come sopra descritto.
- L'informativa sul trattamento dei dati personali; il Richiedente ne prende visione e sottoscrive.
- Documento con le condizioni contrattuali relative al servizio; il Richiedente ne prende visione e sottoscrive.

L'Operatore procede con l'identificazione così come descritto nel paragrafo 6.1.2.

L'Incaricato IdP acquisisce il Modulo di adesione firmato ed una copia per immagine della documentazione di identificazione presentata dall'utente.

Segue una fase di Verifica e Validazione dei dati da parte dell'Operatore IdP, che segue il procedimento descritto nel paragrafo 6.2.1.

Il richiedente riceve una email contenente la propria Username ed una Password temporanea ed un link su cui deve cliccare per validare il proprio indirizzo mail. In questo modo Sielte si accerta che l'indirizzo fornito corrisponda ad una reale casella di posta elettronica.

Richiede il codice OTP all'interno della pagina su cui viene reindirizzato, cliccando sul link di verifica; contestualmente riceve un codice OTP sul proprio telefono, che deve inserire, all'interno della pagina su cui si trova, nel campo di testo dedicato, al fine di certificare l'esistenza e la proprietà del numero di telefono. Nel caso in cui immette il codice errato, può riprovare fino ad altre due volte. Procede alla fase successiva immettendo il codice OTP corretto.

L'Operatore IdP, se le verifiche dei dati sono positive, tra cui le verifiche riguardanti indirizzo mail e numero di telefono, considera identificato ed attivato il Richiedente.

6.2.2.3 IDENTIFICAZIONE TRAMITE FIRMA DIGITALE E FIRMA ELETTRONICA QUALIFICATA

In caso di scelta della modalità *Firma digitale o Firma elettronica qualificata*, il Richiedente sottoscrive il modulo di richiesta del servizio con il dispositivo di firma digitale rilasciato da un certificatore di firma digitale accreditato dall'AgID. (https://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi), lo carica nella form preposta e lo invia alla casella di posta spid@sielte.it. Sielte riceve il documento e verifica le informazioni sulla firma digitale. Nello specifico, il personale addetto all'identificazione provvede a verificare l'identità dell'utente, consultando la scheda di registrazione. Inoltre, viene verificata anche l'autorità di certificazione, che ha rilasciato il certificato per la firma. In particolar modo, viene effettuata una verifica sulla CRL (**C**ertificate **R**evocation **L**ist), che contiene la lista dei certificati revocati. Il personale Sielte addetto all'identificazione è autorizzato a richiedere ulteriori informazioni riguardo all'identificazione e a concludere negativamente la procedura di identificazione e rilascio. L'Operatore IdP, qualora le verifiche risultassero positive, considera identificato il Richiedente, il quale procederà secondo quanto esplicitato successivamente con l'attivazione dell'ID.

6.2.2.4 IDENTIFICAZIONE TRAMITE CIE/CNS/TS-CNS

In caso di scelta di identificazione tramite CIE/CNS/TS-CNS, il Richiedente compila il modulo di adesione inserendo i dati necessari all'identificazione. Alla fine della fase di compilazione, viene presentato un riepilogo dei dati inseriti e viene domandato al richiedente di autenticarsi con la carta in suo possesso ed il PIN associato ad essa. Sielte considera identificato il Titolare con questa modalità. Tale modalità di identificazione si basa su una presunzione di correttezza relativa al processo di identificazione espletato dal gestore che ha precedentemente rilasciato un documento digitale di identità. Il Richiedente procede successivamente con l'attivazione dell'ID.

6.3 Attivazione dell'ID

In caso di verifiche positive, viene inviata una e-mail all'indirizzo del Richiedente, contenente una User Id, ed un PIN temporaneo di accesso, i quali costituiscono lo strumento di autenticazione nel sistema di comunicazione sicuro tra Sielte ed il richiedente.

Quest'ultimo accede al portale Sielte con le credenziali che ha ricevuto; deve obbligatoriamente cambiare il suo PIN, inserendo una password a sua scelta (seguendo determinate regole di password sicura dettate dal Regolamento delle modalità attuative, art. 14). Il sistema procede così all'attivazione dell'identità digitale.

6.4 Rilascio dell'identità

Nella fase di rilascio dell'identità digitale vengono fornite le seguenti informazioni:

- **Estremi dell'identità digitale** – contiene, oltre al codice identificativo dell'utente, tutte le informazioni che sono state utilizzate.
- **Credenziali** – in funzione del livello di sicurezza scelto, vengono consegnate la password e il dispositivo OTP utilizzato per l'autenticazione.
- **Codici operativi per l'utilizzo dell'identità digitale** – i codici operativi (es. quello per la sospensione dell'identità digitale) che servono per la gestione dell'identità digitale e delle credenziali.

- **Data scadenza credenziali** – viene fornita anche la durata delle credenziali.
- **Manuale di utilizzo delle identità digitali** – all'interno del manuale vengono inserite le corrette indicazioni per l'utilizzo dell'identità digitale.
- **Manuale di utilizzo dei servizi** – all'interno del manuale, disponibile anche sul sito https://www.sielteid.it, vengono inserite tutte le informazioni per utilizzare il servizio SielteID e le istruzioni su come accedere ai servizi di Service Desk.

6.5 Attivazione delle credenziali di Livello 1 e 2

L'attivazione delle credenziali avviene nelle seguenti modalità:

- **Credenziali con sicurezza di Livello 1 SPID** – in questo caso viene creata una password temporanea, che viene inviata all'utente via posta elettronica insieme ad un link per l'attivazione delle credenziali. Successivamente, l'utente dovrà necessariamente impostare una nuova password con gli stessi criteri di protezione di quella generata automaticamente; quindi viene guidato su come cambiare la password inserendo prima il codice di attivazione temporaneo ricevuto via e-mail e dopo la nuova password (due volte per conferma). Effettuato il cambio della password, l'utente può visualizzare i propri dati e richiedere l'attivazione delle credenziali.
- **Credenziali con sicurezza di Livello 2 SPID** – in questo caso viene utilizzato lo stesso meccanismo per il rilascio delle credenziali di Livello 1 SPID. In aggiunta, è necessario associare un dispositivo smartphone o tablet con sistema operativo Android, iOS o Windows Phone (o anche desktop, nel solo caso Windows), con installata l'app MySielteID per generare un codice OTP da utilizzare in accoppiata alle credenziali di Livello 1. L'operazione per attivare le credenziali di Livello 2 è disponibile dalla pagina del proprio profilo SielteID su Aggiungi Dispositivo.

7 CICLO DI VITA DELL'IDENTITÀ DIGITALE

Il gestore dell'identità digitale assicura la manutenzione dell'identità attraverso tutto il suo ciclo di vita.

La gestione del ciclo di vita dell'identità digitale si articola nei seguenti processi:

- Sospensione e revoca dell'identità digitale.
- Conservazione delle credenziali.
- Rinnovo e sostituzione delle credenziali.
- Gestione utente dell'identità digitale, compreso il processo di recupero delle credenziali.

Di seguito vengono descritti nel dettaglio i processi afferenti ad ogni punto della precedente lista.

7.1 Sospensione e revoca dell'identità digitale

La sospensione dell'identità digitale può essere richiesta dall'utente accedendo al proprio profilo sul sito web https://www.sielteid.it tramite l'operazione **"Sospendi Identità"** ed effettuando un accesso di livello 2.

Successivamente deve compilare una form, inserendo le seguenti informazioni:

- la data fino a cui si desidera sospendere il proprio account SPID;
- la password;
- il codice di sospensione ricevuto in fase di attivazione delle credenziali;
- la motivazione della richiesta della sospensione (furto, smarrimento, sospetto uso abusivo, o altro).

Quando l'utente conferma la richiesta di sospensione, il sistema verifica la validità delle informazioni inserite e, in caso positivo, presenta un messaggio di conferma della sospensione dell'identità digitale.

Automaticamente anche le credenziali associate verranno aggiornate in modalità "sospese".

La richiesta di sospensione può essere allo stesso modo annullata utilizzando lo stesso servizio disponibile sul sito web.

Per effettuare la richiesta di sblocco sospensione l'utente deve:

- accedere al profilo personale www.sielteid.it
- scegliere dal menu a tendina l'operazione "Riattiva Identità";
- accedere tramite OTP (livello 2)
- inserire la password personale
- inserire il codice di riattivazione ricevuto in fase di attivazione delle credenziali;

Quando l'utente conferma l'operazione, il sistema verifica la validità delle informazioni inserite e, in caso positivo, presenta un messaggio di conferma dello sblocco sospensione dell'identità digitale.

La revoca dell'identità digitale può essere richiesta dall'utente attivo.

Per effettuare la richiesta di revoca dell'identità digitale l'utente deve:

- accedere al profilo personale www.sielteid.it;
- scegliere dal menu a tendina l'operazione **"Revoca Identità"**;
- allegare un documento di riconoscimento valido o una copia della denuncia nel caso di smarrimento/furto;
- inserire il codice segreto di revoca, ricevuto in fase di registrazione;
- inserire la motivazione della richiesta di revoca.

Il personale addetto di Sielte, che riceve la richiesta di revoca, provvede a verificare tutta la documentazione ricevuta, se l'identità digitale è stata precedentemente sospesa e la validità

della denuncia consegnata. Nel caso ci siano dei dati errati o la documentazione non sia valida, l'operatore provvede a contattare l'utente al fine di individuare e correggere il problema ed eventualmente rigettare la revoca.

Altrimenti, nel caso in cui tutta la documentazione fornita per la revoca dell'identità digitale sia corretta, l'utente riceve presso il proprio indirizzo email una notifica di conferma di avvenuta revoca dell'identità digitale.

7.2 Conservazione delle credenziali

La conservazione delle credenziali è il processo che riguarda le modalità di memorizzazione e i mezzi usati per la produzione delle credenziali, in modo da garantirne la protezione contro abusi ed usi non autorizzati.

A livello 1 SPID, le credenziali sono memorizzate all'interno di una base dati dedicata e sono protetti da un sistema di controllo che limita l'accesso soltanto agli amministratori e alle applicazioni autorizzate. In particolare, vengono utilizzati algoritmi di *salt* e *hashing*, definiti a livello di standard internazionali, che permettono di schermare (non in chiaro) la password e di renderla inattaccabile dall'esterno.

A livello 2 SPID, vengono utilizzate le stesse tecniche a cui si ricorre per il livello 1 insieme agli algoritmi standard per la generazione di codici OTP di tipo *token out of band*.

7.3 Rinnovo e sostituzione delle credenziali

Le credenziali hanno una valenza di sei mesi a partire dalla data di attivazione. L'utente viene avvisato preventivamente tramite mail quando stanno per scadere, affinché possa modificarle; queste infatti, se non modificate, a partire dalla data di scadenza non possono più essere utilizzate e quindi l'utente deve eseguire il rinnovo delle proprie credenziali.

L'utente può effettuare la modifica o sostituzione delle proprie credenziali in qualsiasi momento, accedendo al proprio profilo sul sito web https://www.sielteid.it con autenticazione di livello 2 e cliccando sull'operazione **"Cambia password"**.

Quando l'utente conferma la richiesta di sostituzione delle credenziali, il sistema verifica la validità delle informazioni inserite e, in caso positivo, presenta un messaggio di conferma.

7.4 Gestione utente dell'identità digitale

L'utente titolare di un'identità digitale ha la possibilità, accedendo al proprio profilo, tramite il sito web https://www.sielteid.it, di visualizzare i propri dati personali (attributi qualificati) e di modificare quelli non identificativi.

Per ogni operazione di modifica sugli attributi relativi ad un'identità digitale viene eseguita una validazione da parte del personale addetto di Sielte in modo da garantire la validità delle informazioni. Inoltre, l'utente viene notificato via email dell'aggiornamento degli attributi.

In questo stesso contesto l'utente può anche richiedere supporto a Sielte tramite un help desk dedicato oppure utilizzando la casella di posta spid@sielte.it per quanto riguarda le informazioni legate all'uso e al funzionamento dell'identità digitale.

7.4.1 *Processo di recupero delle credenziali*

L'utente titolare di un'identità digitale ha la possibilità di poter recuperare le proprie credenziali di accesso al profilo SielteID, in base agli attributi in possesso, richiedendo il cambio password, tramite la voce **"Ho dimenticato la mia password"**, dalla login box di accesso.

Nel caso di possesso dell'indirizzo email e del numero di cellulare inseriti in fase di registrazione, riceverà su ciascuno di essi, un codice OTP da inserire; validati i due codici OTP, potrà procedere all'inserimento di una nuova password.

Nel caso di solo possesso dell'indirizzo email e non del numero di cellulare, dovrà rispondere a tre domande personali, o ad una domanda segreta, qualora l'abbia impostata

precedentemente; rispondendo correttamente, riceverà un codice OTP all'indirizzo email inserito in fase di registrazione; validato il codice OTP, ricevuto via email, potrà inserire un nuovo numero di cellulare, sul quale riceverà un altro codice OTP, utile a validarlo; infine, potrà procedere all'inserimento di una nuova password.

Nel caso di solo possesso del numero di cellulare e non dell'indirizzo email, dovrà rispondere a tre domande personali, o ad una domanda segreta, qualora l'abbia impostata precedentemente; rispondendo correttamente, riceverà un codice OTP al numero di cellulare inserito in fase di registrazione; validato il codice OTP, potrà inserire un nuovo indirizzo email, sul quale riceverà un codice OTP, utile a verificarlo; infine, potrà procedere all'inserimento di una nuova password.

Nel caso in cui non sia in possesso di nessuno dei due attributi inseriti in fase di registrazione, indirizzo email e numero di cellulare, l'utente dovrà compilare un form, in cui dovrà rispondere ad un set di domande personali e, qualora l'avesse impostata, anche ad una domanda segreta, ed inserire il nuovo indirizzo email e il nuovo numero di cellulare, su ciascuno dei quali riceverà un codice OTP, utile a verificarli. Se la validazione dei codici si concluderà con successo, verrà inviata una richiesta al supporto dedicato, con i dati inseriti. Validata la richiesta da un operatore, l'utente riceverà via email una password temporanea con la quale potrà accedere al profilo e poter procedere all'inserimento di una nuova password.

8 SICUREZZA DEL SERVIZIO

8.1 Conservazione della documentazione relativa al ciclo di vita di un'identità digitale

Secondo quanto specificato dal DPCM del 24 ottobre 2014, Sielte ha l'obbligo di conservazione delle informazioni e della documentazione raccolta durante l'intero ciclo di vita di un'identità digitale.

8.2 Tracciatura delle informazioni del servizio

Ai fini della tracciatura, ogni transazione di autenticazione viene marcata temporalmente e registrata all'interno di un log certificato, contenente i record delle transazioni gestite negli ultimi 24 mesi, nel rispetto dell'art. 4 del DPCM del 24 ottobre 2014. Le tracciature, sono salvate in maniera persistente e nel rispetto del codice della privacy, utilizzando meccanismi di cifratura dei dati e sistemi di basi di dati (DBMS), al fine di garantirne l'integrità, il non ripudio e la disponibilità.

8.2.1 *Formato dei log*

In accordo con quanto suggerito nel documento delle regole tecniche di SPID, per ogni transazione di autenticazione viene memorizzato un record contenente le seguenti informazioni:

- l'identificativo dell'identità digitale (*spidCode*) interessata dalla transazione;
- la richiesta SAML (*<AuthnRequest>*) emessa dall'SP;
- la risposta SAML (*<Response>*) ricevuta da *SielteID*;
- l'identificativo della richiesta;
- l'identificativo della risposta;

- il timestamp della richiesta;
- il timestamp della risposta;
- l'entityID del SP (issuer della richiesta);
- l'entityID di *SielteID* (issuer della risposta);
- l'ID dell'asserzione di risposta SAML (<*Assertion*>);
- il soggetto dell'asserzione di risposta.

8.3 Procedura per la richiesta del log certificato

L'utente titolare di una Identità Digitale ha facoltà di richiedere in qualunque momento una copia delle informazioni contenute nel log certificato relative alle proprie credenziali SPID. Deve accedere, con le proprie credenziali, al portale di gestione dell'identità e da qui effettuare un'apposita richiesta indicando l'intervallo di date per cui intende ricevere le informazioni sull'utilizzo delle proprie credenziali SPID. La richiesta deve essere validata attraverso l'inserimento delle credenziali SPID di livello 2, ovvero con l'inserimento dell'OTP. Sielte provvede alla raccolta delle informazioni richieste e alla produzione di un report, che viene quindi messo a disposizione per il download sul portale di gestione dell'identità.

9 REGISTRI

Il gestore delle identità ha l'obbligo di conservazione delle informazioni e della documentazione raccolta durante la fase di registrazione, le informazioni sul processo di verifica delle informazioni di identità, i messaggi generati durante il processo di autenticazione e altri dati pertinenti.

Sielte conserva i dati utilizzati per la verifica dell'identità personale di ciascun utente, in particolare:

- documentazione utilizzata per l'identificazione dell'utente;

- modulo di richiesta firmato digitalmente;
- email inviate/ricevute da caselle di posta elettronica;
- SMS inviati/ricevuti;

Appropriate registrazioni vengono conservate per tutto il ciclo di vita di una credenziale.

I registri sono mantenuti per documentare le seguenti informazioni:

a) creazione di una credenziale;

b) identificativo della credenziale;

c) soggetto (persona fisica o giuridica) al quale è stata rilasciata la credenziale;

d) stato della credenziale.

In merito alla conservazione dei documenti è previsto un'archiviazione di tutta la documentazione in appositi fascicoli. Il fascicolo contiene tutta la pratica della gestione delle identità digitale. All'interno della documentazione si trova la copia del documento d'identità ed il modulo di richiesta dell'identità digitale. Tutta la documentazione viene conservata secondo i termini di legge, trasferendola all'AgID alla scadenza del contratto.

10 SERVICE DESK

Sielte mette a disposizione un canale di contatto diretto verso i propri utenti, tramite il servizio di Service Desk con operatore disponibile dal lunedì al sabato, dalle ore 09:00 alle ore 18:00, accessibile tramite il Numero Verde gratuito 800 11 33 22.

Gli utenti possono richiedere informazioni anche tramite mail all'indirizzo spid@sielte.it.

11 PRIVACY E PROTEZIONE DEI DATI PERSONALI

Forte interesse viene attribuito in Sielte alla gestione ed alle tematiche relative al trattamento dei dati personali nel rispetto delle attuali leggi e del codice etico e professionale.

Le misure messe in atto per la gestione e la protezione dei dati personali sono in linea con quanto previsto dal Codice per la Protezione dei Dati Personali (DL 196/03).

Le caratteristiche più importanti del sistema si riferiscono al personale dipendente che ha ricevuto la nomina ai sensi dell'art.30 del DL 196/03 e pertanto è in possesso delle conoscenze per gestire i dati e mette in atto tutte le misure di sicurezza nella gestione di questi. Il trattamento dei dati personali avviene sempre con una supervisione da parte di un responsabile, che verifica e controlla la messa in pratica delle norme e delle procedure operative.

L'art.13 D.Lgs. n. 196/2003, che tratta il "Codice in materia di protezione dei dati personali", si riferisce ai dati che l'utente finale o l'azienda daranno al gestore delle identità e formano l'oggetto di trattamento, nel rispetto della normativa sopra citata, da parte di Sielte. Il trattamento dei dati viene effettuato in modo lecito, secondo correttezza e in conformità alla normativa sopra citata, mediante strumenti idonei a garantirne la sicurezza e la riservatezza e potrà essere effettuato anche attraverso strumenti automatizzati, atti a memorizzare, gestire e trasmettere i dati stessi.

I criteri di sicurezza seguiti e le eventuali azioni da intraprendere in materia di sicurezza ICT riflettono una visione ad ampio raggio dell'argomento privacy e protezione dei dati. Infatti, devono essere necessariamente previste misure da adottare al fine di garantire la segretezza dei dati e delle informazioni, l'accesso controllato ai sistemi informatici, la salvaguardia dell'integrità e coerenza dei dati gestiti e contenuti nei sistemi informativi, ecc.

Per implementare tali politiche di sicurezza è quindi necessario garantire i seguenti requisiti minimi:

- **Identificazione** (identification), il cui scopo è stabilire univocamente l'identità di chi sta richiedendo il servizio.
- **Autenticazione** (authentication): per stabilire che l'identità dichiarata da chi sta richiedendo il servizio è quella vera. Le tecniche di autenticazione sono basate sull'utilizzo della firma digitale.

- **Integrità** (integrity): per garantire che i dati inviati non siano corrotti o modificati e le transazioni non siano state alterate. L'integrità può essere realizzata mediante l'uso di crittografia asimmetrica (a chiave pubblica) o simmetrica (a chiave privata).
- **Confidenzialità e Privacy** (confidentiality): per garantire che solo le entità direttamente coinvolte nell'erogazione e nella fruizione del servizio abbiano accesso ai dati trasmessi. La confidenzialità e privatezza dei dati è realizzata mediante meccanismi di crittografia, basati su schema asimmetrico (a chiave pubblica) o simmetrico (a chiave privata). Coerentemente con quanto disposto dalla legge n.196/2003, ai fini della registrazione sul sito e del corretto svolgimento delle procedure on-line, gli utilizzatori del sistema dovranno autorizzare l'Amministrazione al trattamento dei dati personali secondo le norme vigenti e per le finalità di cui all'informativa, che dovrà essere pubblicata sul sito.
- **Accesso alle aree riservate**: tale accesso è subordinato all'accettazione delle informative mostrate all'utente in sede di abilitazione e/o registrazione, nonché il rilascio del consenso per i trattamenti, ove questo occorra, per finalità legate alla comunicazione e diffusione dei dati.
- **Tracciamento** (audit): per permettere di tracciare i principali eventi legati all'erogazione/fruizione del servizio.
- **Non ripudio** (non-repudiation): per evitare che chi ha inviato dati o eseguito una transazione neghi di averlo fatto. È realizzato mediante firma digitale e meccanismi di reliability della messaggistica. Il non-ripudio è un servizio di sicurezza critico in ogni applicazione in cui si negoziano obblighi legali o contrattuali.
- **Protezione fisica dei dati:** al fine di garantire l'integrità delle informazioni (ed in particolare, degli archivi) attraverso la predisposizione di meccanismi e procedure di Backup & Recovery.

Sielte mette in campo tutte le soluzioni tecniche ed organizzative per la protezione e la conservazione dei dati, utilizzando strumenti informatici, che permettono di avere i sistemi in alta disponibilità, sicuri, aggiornati e distribuiti. La protezione non si ferma agli aspetti

informatici, ma viene estesa anche ai punti di accesso della rete aziendale ed alle strutture fisiche. Un punto di forza di Sielte è il supporto tecnico, il call center ed il monitoraggio di tutta l'infrastruttura fisica e virtuale.

Le politiche di Sicurezza non possono prescindere da un'analisi dettagliata dei rischi sulla sicurezza, identificando tutte le misure necessarie per realizzare un sistema, che sia il più possibile protetto da eventi imprevisti. Tale approccio sarà quindi adottato nella fase di progettazione architetturale di dettaglio, al fine di realizzare un sistema che sia garantito dal punto di vista della sicurezza.

12 ALLEGATO A

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
1	Autenticazione corretta	HTTP POST HTTP Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)	n.a.	n.a.	n.a.	
Anomalie di Sistema									
2	Indisponibilità sistema	HTTP POST	n.a.	n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio più tardi	n.a.	

3	Errore di sistema	HTTP Redirect	HTTP 500	n.a.	Utente	Pagina di cortesia con messaggio "Sistema di autenticazione non disponibile - Riprovare più tardi"	Ripetere l'accesso al servizio più tardi	n.a.	Tutti i casi di errore di sistema in cui è possibile mostrare un messaggio informativo all'utente
Anomalie delle richieste									
Anomalie sul binding									
4	Formato binding non corretto	HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il	Contattare il gestore del servizio	Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta	Parametri obbligatori: SAMLRequest SigAlg Signature Parametri non obbligatori: RelayState

		HTTP POST				gestore del servizio"			Parametri obbligatori: SAMLRequest Parametri non obbligatori: RelayState
5	Verifica della firma fallita	HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Impossibile stabilire l'autenticità della richiesta di autenticazione - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati
6	Binding su metodo HTTP errato	HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non ricevibile - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare metadata Gestore dell'identità (IdP)	Invio richiesta in HTTP-Redirect su entry point HTTP-POST dell'identità
		HTTP POST							Invio richiesta in HTTP-POST su entry point HTTP-Redirect dell'identità

Anomalie sul formato della AuthnReq									
7	Errore sulla verifica della firma della richiesta	HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati
8	Formato della richiesta non conforme alle specifiche SAML	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr08	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia	Non conforme alle specifiche SAML - il controllo deve essere operato successivamente alla verifica positiva della firma
9	Parametro *version* non presente, malformato o diverso da '2.0'	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch ErrorCode nr09	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente	
10	Issuer non presente, malformato o non corrispondente all'entità che sottoscrive la richiesta	HTTP POST / HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il	Contattare il gestore del servizio	Verificare formato delle richieste prodotte	

						gestore del servizio"			
11	Identificatore richiesta(ID) non presente, malformato o non conforme	HTTO POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr11	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	Identificatore necessario per la correlazione con la risposta
12	RequestAuthnContext non presente, malformato o non previsto da SPID	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:statuss:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Autenticazione SPID non conforme o non specificata"		Informare l'utente	AUTH livello richiesto diverso da: urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3
13	IssueInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
14	destination non presente, malformata o non coincidente con il Gestore delle identità ricevente la richiesta	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	

15	attributo isPassive presente e attualizzato al valore true	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
16	AssertionConsumerService non correttamente valorizzato	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr16	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	AssertionConsumerServiceIndex presente e attualizzato con valore non riportato nei metadata AssertionConsumerServiceIndex riportato in presenza di uno od entrambi gli attributi AssertionConsumerServiceURL e ProtocolBinding AssertionConsumerServiceIndex non presente in assenza di almeno un attributo AssertionConsumerServiceURL e ProtocolBinding
17	Attributo Format dell'elemento NameIDPolicy assente o non valorizzato secondo specifica	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr17	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	Nel caso di valori diversi dalla specifica del parametro opzionale AllowCreate si procede con l'autenticazione senza riportare errori

18	AttributeConsumerServiceIndex malformato o che riferisce a un valore non registrato nei metadati di SP	HTTO POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18	Fornitore del servizio (SP)	n.a.	n.a.	Riformulare la richiesta con un valore dell'indice presente nei metadati	
Anomalie derivanti dall'utente									
19	Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero di tentativi secondo le policy adottate)	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19	HTTP POST / HTTP Redirect	Messaggio di errore specifico ad ogni interazione prevista	Inserire credenziali corrette	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Si danno indicazioni specifiche e puntuali all'utente per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi di determinate condizioni legate alle policy di sicurezza aziendali, ad esempio dopo 3 tentativi falliti, si risponde al SP

20	Utente privo di credenziali compatibili con il livello richiesto dal fornitore del servizio	HTTO POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20	Fornitore del servizio (SP)	n.a.	Acquisire credenziali di livello idoneo all'accesso al servizio richiesto	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
21	Timeout durante l'autenticazione utente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21	Fornitore del servizio (SP)	n.a.	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinato periodo di tempo	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
22	Utente nega il consenso all'invio di dati al SP in caso di sessione vigente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22	Fornitore del servizio (SP)		Dare consenso	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1

23	Utente con identità sospesa/revocata o con credenziali bloccate	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Credenziali sospese o revocate"		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
25	Processo di autenticazione annullato dall'utente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr25	Fornitore di servizi	non applicabile	non applicabile	Notificare l'avvenuto annullamento del processo autenticazione e ripristinare lo stato dell'interazione utente al momento della richiesta	