MANUALE OPERATIVO

SIELTE ID

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

IL PRESENTE DOCUMENTO È DI PROPRIETÀ DELLA **SIELTE S.p.A.** È VIETATA LA RIPRODUZIONE PARZIALE O TOTALE O LA DIVULGAZIONE SENZA PREVENTIVA AUTORIZZAZIONE DELLA **SIELTE S.p.A.**

File/Oggetto	**Manuale Operativo**		
Redatto da	**Development Management**		
Verificato da	**Compliance Manager**		
Approvato da	**SPID Service Manager**		
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			

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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, REVISIONE REGISTRAZIONE E GESTIONE IMPRESE, REVISIONE GENERALE DEL DOCUMENTO	04/2018
08	3.2 6.1.1 7.5, 5.8.3	OBBLIGHI E RESPONSABILITÁ DEGLI UFFICI DI REGISTRAZIONE REINGEGNERIZZAZIONE REGISTRAZIONE RINNOVO IDENTITÁ NOTIFICHE	10/2018
09	6.1.1.1 6.1.1.2	INSERIMENTO SOTTOPARAGRAFO SU REGISTRAZIONE IDENTITÀ PREGRESSA CON MIGRAZIONE ASSISTITA E SU REGISTRAZIONE IDENTITÀ PREGRESSA	11/2018
09.1	6.1.3	AGGIORNAMENTO NUMERO DEL CONTACT CENTER, PROCESSO RECUPERO PASSWORD, AGGIUNTA PARAGRAFO IN RIFERIMENTO AI RAO, AGGIORNAMENTO ALLEGATO A	09/2019

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

09.2	7.4 7.5 12	AGGIORNAMENTO PROCESSO DI RECUPERO DELLE CREDENZIALI AGGIORNAMENTO PARAGRAFO GESTIONE E RINNOVO DELL'IDENTITÀ DIGITALE AGGIORNAMENTO ALLEGATO A CON ERRORE N.30	02/2020
10	5.2 5.8.4 6 6.4	INSERIMENTO NUOVA MODALITÀ DI RILASCIO IDENTITÀ DIGITALE CON CIE 3.0 AGGIUNTA RIFERIMENTI ALL'ATTIVAZIONE DI SPID LIV 3 MODIFICHE AL CAPITOLO SUL RILASCIO DELL'IDENTITÀ DIGITALE	03/2020
11	7.6 6.1.1.3	INSERIMENTO PARAGRAFO SU SERVIZIO CREDITI SMS INSERIMENTO DESCRIZIONE NUOVA MODALITÀ DI IDENTIFICAZIONE MEDIANTE SPORTELLO PUBBLICO	12/2020
12	6.1.1 6.2.2.1 7.7 7.8	AGGIORNAMENTO PARAGRAFO RELATIVO ALLE MODALITÀ D'IDENTIFICAZIONE; AGGIUNTA PRIORITY WEBCAM AGGIORNAMENTO PIATTAFORME DI CONTATTO, MESSAGING E VIDEOCALL. AGGIUNTO PARAGRAFO "SERVIZIO PRIORITY WEBCAM" AGGIUNTO PARAGRAFO "RICHIESTE DI RIMBORSO PER I SERVIZI PRIORITY WEBCAM E PACCHETTO SMS PER SPID LIVELLO 2"	05/2021
12.1	5.8.1	INSERIMENTO INIBIZIONE RIUTILIZZO PASSWORD, IN CONFORMITÀ AL REGOLAMENTO DELLE MODALITÀ ATTUATIVE	08/2021
12.2	6.2.2 7.6	TRATTAMENTO DATI DURANTE LE VIDEOCHIAMATE CON PIATTAFORME TERZE DI CONTATTO E CIFRATURA DI TALI CANALI DI COMUNICAZIONE AGGIORNAMENTO CAPITOLO SERVIZIO CREDITI SMS SIELTEID	12/2021

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

13	TUTTI	AGGIORNAMENTO MODALITÀ DI IDENTIFICAZIONE WEBCAM E DE VISU AGGIORNAMENTO PARAGRAFO CUSTOMER CARE AGGIORNAMENTO POLICY UTILIZZO SMS DISMISSIONE APP MYSIELTEID PER WINDOWS REVISIONE INTERO DOCUMENTO	10/2022
13.1	1.3 2.1 2.4 11 5.8.3 6.4	INSERIMENTO RIFERIMENTO NORMATIVO DPCM DEL 19 OTTOBRE 2021, CHE MODIFICA IL DPCM DEL 24 OTTOBRE 2014 NEI SEGUENTI ARTICOLI: 7,10,12,16 MODIFICA CAPITOLO CUSTOMER CARE AGGIORNAMENTO PARAGRAFO ATTIVAZIONE DELLE CREDENZIALI AGGIORNAMENTO PARAGRAFO TOKEN CRITTOGRAFICO SOFTWARE MULTI-FATTORE (MF) AGGIORNAMENTO PARAGRAFO ATTIVAZIONE DELLE CREDENZIALI DI LIVELLO 1, 2 E 3	03/2023
14	TUTTI	AGGIORNAMENTO MENU DEL PROFILO AGGIORNAMENTO PARAGRAFO SOSPENSIONE E REVOCA DELL'IDENTITÀ DIGITALE	09/2023
15	8	INSERIMENTO PARAGRAFO IDENTITA' DIGITALE PER MINORENNI	11/2023
16	3.2 4 6.1.1 14	AGGIORNAMENTO PARAGRAFI IDENTIFICAZIONE MEDITANTE RA E MISURE ANTI-CONTRAFFAZIONE REVISIONE TERMINOLOGIE NELL'AMBITO DEL SISTEMA SPID REVISIONE CAPITOLO ALLEGATO A	01/2024
16.1	6.1.1 6.2.2.3	AGGIORNAMENTO PARAGRAFO REGISTRAZIONE MODULO DI ADESIONE ELETTRONICO E IDENTIFICAZIONE TRAMITE CIE/CNS/TS-CNS	07/2024

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

17	5.2 5.8.4 6.1 6.1.1.3 6.2.2.3	DETTAGLIATO MAGGIORMENTE IL LIVELLO 3 DETTAGLIATO MAGGIORMENTE PARAGRAFO SUL LIVELLO 3 AGGIORNATO CARICAMENTO DOCUMENTI IN FASE DI REGISTRAZIONE AGGIORNAMENTO REGISTRAZIONE TRAMITE SPORTELLO PUBBLICO AGGIORNAMENTO PARAGRAFO PER L'IDENTIFICAZIONE CIE 3.0	10/2024

Sommario

1 GENERALITÀ 9

1.1 Scopo del documento 9

1.2 Convenzioni di lettura 9

1.3 Riferimenti normativi 10

1.4 Definizioni ed acronimi 12

2 DATI IDENTIFICATIVI 15

2.1 Dati identificativi del gestore 15

2.2 Standard e certificazioni 18

2.3 Versione del manuale operativo 21

2.4 Responsabile del manuale operativo 21

3 OBBLIGHI E RESPONSABILITÀ 22

3.1 Obblighi del Gestore delle Identità Digitali 22

3.2 Obblighi e Responsabilità degli Uffici di Registrazione [Non operativo] 27

3.3 Obblighi del Proprietario dell'Identità Digitale 28

3.4 Responsabilità 30

4 CARATTERISTICHE GENERALI 30

4.1 Livelli di servizio garantiti 32

4.2 Misure anti-contraffazione 35

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

5 ARCHITETTURA LOGICA 37

5.1 Servizi 40

5.2 Livelli di sicurezza 41

5.3 Generazione OTP 41

5.4 Sicurezza dei dati 42

5.5 Lettore di impronta digitale e riconoscimento facciale 42

5.6 Codici e formati di messaggi di anomalia 43

5.7 Sistema di monitoraggio 43

5.8 Sistemi di autenticazione 44

5.8.1 Basic Authentication 44

5.8.2 Token out of Band 46

5.8.3 Token crittografico software multi-fattore (MF) 47

5.8.4 Dispositivo Crittografico multi-fattore (MF) 48

6 RILASCIO IDENTITÀ DIGITALE 49

6.1 Richiesta Identità 50

6.1.1 Registrazione tramite Modulo di Adesione elettronico 51

6.1.2 Registrazione tramite RA [Non operativo] 58

6.2 Identificazione 60

6.2.1 Verifica e Validazione dei dati 60

6.2.2 Identificazione in base alla modalità prescelta dal Richiedente 62

6.3 Attivazione dell'ID 65

6.4 Attivazione delle credenziali di Livello 1, 2 e 3 66

7 CICLO DI VITA DELL'IDENTITÀ DIGITALE 67

7.1 Sospensione e revoca dell'identità Digitale 67

7.2 Conservazione delle credenziali 70

7.3 Rinnovo e sostituzione delle credenziali 71

7.4 Processo di recupero delle credenziali 71

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

7.4.1 Recupero Password. 71
7.4.2 Recupero Password e cellulare. 71
7.4.3 Recupero Password ed e-mail. 72
7.4.4 Recupero Password, e-mail e cellulare. 72

7.5 Gestione e rinnovo dell'Identità Digitale 74

8 IDENTITA' DIGITALE PER MINORENNI 74

8.1 Rilascio spid Minori 75
8.1.1 Richiesta Identità da parte del Genitore/Tutore 75
8.1.2 Registrazione da parte del Minore 77
8.1.3 Verifica e validazione dati 78
8.1.4 Identificazione 78
8.1.5 Attivazione identità 79

8.2 Utilizzo spid minori 79

8.3 Gestione dell'identità digitale del minore 80

8.4 Identità del genitore/tutore sospesa o revocata 81

8.5 Dissociazione dal genitore al compimento dei 18 anni 82

9 SERVIZI 83

9.1 Servizio Crediti SMS SielteID 83

9.2 Servizio Priority Webcam 86

9.3 Richieste di rimborso per i servizi Webcam e Pacchetto SMS per SPID Livello 2 86

10 SICUREZZA DEL SERVIZIO 87

10.1 Conservazione della documentazione relativa al ciclo di vita di un'Identità Digitale 87

10.2 Tracciatura delle informazioni del servizio 88
10.2.1 Formato dei log 88

10.3 Procedura per la richiesta del log certificato 88

11 REGISTRI 89

12 CUSTOMER CARE 90

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

12.1 Registrazione de visu (casi eccezionali) 90

13 PRIVACY E PROTEZIONE DEI DATI PERSONALI 90

14 ALLEGATO A 93

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 e ai sensi del DPCM del 19 ottobre 2021, pubblicato sulla Gazzetta Ufficiale del 14/01/2021 n. 296, che modifica il DPCM del 24 ottobre 2014 nei seguenti articoli: 7,10,12,16.

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

USO PUBBLICO

Le informazioni contenute all’interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale, e, in particolare, l'articolo 64 che prevede l'istituzione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (di seguito: SPID);

[2] 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.

[3] 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

[4] DPCM del 19 ottobre 2021, pubblicato sulla Gazzetta Ufficiale del 14/01/2021 n. 296, che modifica il DPCM del 24 ottobre 2014 nei seguenti articoli: 7,10,12,16.

[5] 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

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

[7] 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

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese".

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

[9] Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

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

[11] Regolamento recante le modalità attuative per la realizzazione dello Spid (articolo 4, comma 2, DPCM 24 ottobre 2014).

[12] Linee Guida per la realizzazione di un modello di RAO Pubblico, emesse ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n.82 e successive modifiche e integrazioni e ai sensi dell'articolo 3, comma 2, del DPCM 24 ottobre 2014.

[13] Determinazione AgID n.133 dell'11 maggio 2022.

[14] ISO EN UNI 9001:2015 – Sistema Qualità

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

[16] ISO/IEC 20000-1:2018 – Sistema Di Gestione Dei Servizi IT

[17] ISO/IEC 29115:2015 – Tecnologie Informatiche- Tecniche per la sicurezza- Quadro di riferimento per la garanzia dell'autenticazione delle entità

[18] 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]

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

[19] Linee Guida operative per la fruizione dei servizi SPID da parte dei minori, con determinazione n.133/2022

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
GDPR	General Data Protection Regulation- Regolamento Generale sulla Protezione dei Dati
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
NFC	Near Field Communication

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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
RA	Registration Authority
RAO	Registration Authority Officer
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
SP-IP	Service Provider Identità Pregresse
SSO	Single Sign-On
TOTP	Time-based One-Time Password
XML	eXtensible Markup Language
UE	Unione Europea
UWP	Universal Windows Platform

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- **Dati personali**: 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 ed ai sensi dell'art.4, comma 1 del Regolamento UE 2016/679- GDPR).
- **Dati Particolari:** sono quei " dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (art. 9 del Regolamento Generale sulla Protezione dei Dati, GDPR).
- **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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- **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 Rappresentante	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

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

E-mail	info@sielte.it
PEC	sistemi.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. 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

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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

Sielte è 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, II e III livello (maggiori informazioni sono presenti all'interno della Carta dei servizi Service Desk), al fine di offrire ai propri Clienti una piattaforma servizi completa, affidabile ed interventi on-site H24x7x365.

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

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 9001:2015** [Gestione della qualità – IAF: 28, 34, 33, 22, 35]
    - Progettazione, realizzazione e manutenzione di reti di telecomunicazioni e trasmissione dati. 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, Hosting, Disaster Recovery, inclusa progettazione e sviluppo software) e relativa assistenza specialistica tramite Help Desk. Servizio di Identity Provider aderente al Sistema SPID (Sistema Pubblico Identità Digitale). Progettazione, realizzazione e manutenzione di impianti elettrici, di reti di trasporto e distribuzione di energia elettrica. Progettazione, installazione, assistenza e manutenzione di sistemi di videosorveglianza. Progettazione, realizzazione ed erogazione di servizi di Call Center, Contact Center e Help Desk Tecnico.
- **ISO/IEC 27001:2013** [Gestione della sicurezza delle informazioni – IAF: 33]
    - Erogazione Servizi Data Center: Cloud Computing (in modalità IaaS-PaaS-SaaS con l'utilizzo delle linee guida ISO/IEC 27017 e ISO/IEC 27018) Hosting e Housing, Disaster Recovery con relativo supporto tecnico attraverso Service Desk. Progettazione, sviluppo, manutenzione e assistenza software. Servizio di Identity Provider aderente al sistema SPID (Sistema Pubblico Identità Digitale).

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- **ISO/IEC 20000-1:2018** [Gestione dei servizi IT – IAF: 33]
    - Erogazione del servizio di Identity Provider aderente al sistema SPID (Sistema Pubblico Identità Digitale). Erogazione servizi di gestione e manutenzione di sistemi ICT.
- **ISO 14001:2015** [Gestione ambientale – IAF: 28, 34, 33, 22, 35]
    - Progettazione, realizzazione e manutenzione di reti di telecomunicazioni e trasmissione dati. 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 rotaie. Erogazione servizi di Data Center (Cloud Computing, Housing, Hosting, Disaster Recovery, inclusa progettazione e sviluppo software) e relativa assistenza specialistica tramite Help Desk. Progettazione, realizzazione e manutenzione di impianti elettrici, di reti di trasporti e distribuzione di energia elettrica. Progettazione, realizzazione, assistenza e manutenzione di sistemi di videosorveglianza. Progettazione, realizzazione ed erogazione di servizi di Call Center, Contact Center, Help Desk tecnico.
- **ISO 45001:2018** [Gestione salute e sicurezza sul lavoro – IAF: 28, 34, 33, 22, 35]
    - Progettazione, realizzazione e manutenzione di reti di telecomunicazioni e trasmissione dati. 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, Hosting, Disaster Recovery, inclusa progettazione e sviluppo software) e relativa assistenza specialistica tramite Help Desk. Progettazione, realizzazione e manutenzione di impianti elettrici, di reti di trasporti e distribuzione di energia elettrica. Progettazione, realizzazione, assistenza e manutenzione di sistemi

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

di videosorveglianza. Progettazione, realizzazione ed erogazione di servizi di Call Center, Contact Center, Help Desk tecnico.

- **ISO 50001:2018** [Gestione dell'energia]
    - Progettazione, realizzazione e manutenzione di reti di telecomunicazioni e trasmissione dati. 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, Hosting, Disaster Recovery, inclusa progettazione e sviluppo software) e relativa assistenza specialistica tramite Help Desk. Servizio di identity provider aderente al sistema SPID (Sistema Pubblico di Identità Digitale). Progettazione, realizzazione e manutenzione di impianti elettrici, di reti di trasporti e distribuzione di energia elettrica. Progettazione, realizzazione, assistenza e manutenzione di sistemi di videosorveglianza. Progettazione, realizzazione ed erogazione di servizi di Call Center, Contact Center, Help Desk tecnico.
- **ISO 37001:2016** [Gestione per la prevenzione della corruzione]
    - Progettazione, realizzazione e manutenzione di reti di telecomunicazioni e trasmissione dati. 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, Hosting, Disaster Recovery, inclusa progettazione e sviluppo software) e relativa assistenza specialistica tramite Help Desk. Servizio di identity provider aderente al sistema SPID (Sistema Pubblico di Identità Digitale).
- **SOA** [Attestazione di qualificazione alla esecuzione di lavori pubblici]

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- Categorie: OG1, OG3, OG9, OG10, OG11, OS1, OS5, OS9, OS17, OS19, OS27, OS30, OS35.

- **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.

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 558
Call Center	095 2291712

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

PEC	sistemi.sielte@legalmail.it
Mail	spid@sielte.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 firmato, nel caso di identificazione *de visu.*

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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.
- Verificare gli 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 revoca dell'identità digitale.
- Cancellare la documentazione inerente al processo di adesione trascorsi venti anni 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 ed ai sensi del Regolamento UE 2016/679- GDPR.
- 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).

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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, nei casi di smarrimento, furto o altri danni/compromissioni.
- Ripristinare o revocare l'identità digitale sospesa, nei casi previsti dal regolamento delle modalità attuative.
- 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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 e-mail 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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, revocare 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.
- 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livello 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 e Regolamento UE 2016/679- GDPR) ed utilizzando meccanismi di cifratura.

3.2 Obblighi e Responsabilità degli Uffici di Registrazione [Non operativo]

I RA o Uffici di Registrazione Autorizzati sono soggetti incaricati dal Gestore delle Identità Digitali che, a seguito di sottoscrizione di apposite convenzioni, hanno il mandato di espletare il processo di registrazione, identificare coloro che richiedono le credenziali SPID e rilasciare le medesime credenziali. Il Distributore, che funge da Ufficio di Registrazione, è tenuto a:

- Informare il Richiedente sulle procedure SPID relative all'identificazione e al rilascio e sulle caratteristiche tecniche necessarie.
- Informare il Richiedente circa gli obblighi di riservatezza e segretezza delle credenziali SPID, in modo da garantirne la massima integrità.
- Informare il Richiedente in merito agli obblighi da assumere per la conservazione della credenziale OTP, laddove venisse fornita.
- Informare il Richiedente sulla normativa vigente in materia di protezione dei dati personali.
- Verificare accuratamente che i documenti di riconoscimento presentati dal Richiedente per il riconoscimento *webcam* e *de visu* siano integri, con firma autografa e in corso di validità.
- Verificare tempestivamente l'identità del Richiedente, registrare i dati e avviare la procedura di identificazione (secondo quanto previsto dal presente Manuale Operativo), inviare al Gestore delle Identità Digitali la documentazione in originale e

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

comunicargli i dati acquisiti, al fine di avviare il prima possibile la procedura di rilascio dell'Identità Digitale.

- Accertarsi che il Richiedente abbia compreso le disposizioni relative al servizio SPID, contenute all'interno del presente Manuale.

Gli Uffici di Registrazione Autorizzati svolgono sostanzialmente il ruolo di interfaccia tra il Gestore delle Identità Digitali e il Richiedente, sulla base degli accordi precedentemente presi. Il personale addetto, ovvero gli Incaricati alla Registrazione o Operatori IdP RAO, viene adeguatamente formato ed è soggetto a verifiche da parte del Gestore delle Identità Digitali in merito alla correttezza delle procedure attuate. Il Gestore delle Identità Digitali rimane responsabile verso terzi delle attività svolte dal RA.

3.3 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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.

USO PUBBLICO

Le informazioni contenute all’interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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.

3.4 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 ed ai sensi del Regolamento UE 2016/679-GDPR per il trattamento dei dati personali, 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

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 utilizzate le seguenti terminologie:

- **Identity Provider o Gestore dell'identità digitale** – gestisce le identità digitali e provvede a tutti i meccanismi di autenticazione e autorizzazione di un utente.
- **Service Provider o Fornitore dei servizi** – fa uso del gestore dell'identità digitale (IdP) per autenticare e autorizzare l'accesso agli utenti alle proprie aree dei servizi riservati.
- **Utente** – 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.
- **User Agent** – è il browser attraverso il quale l'utente richiede l'accesso al servizio.

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:

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

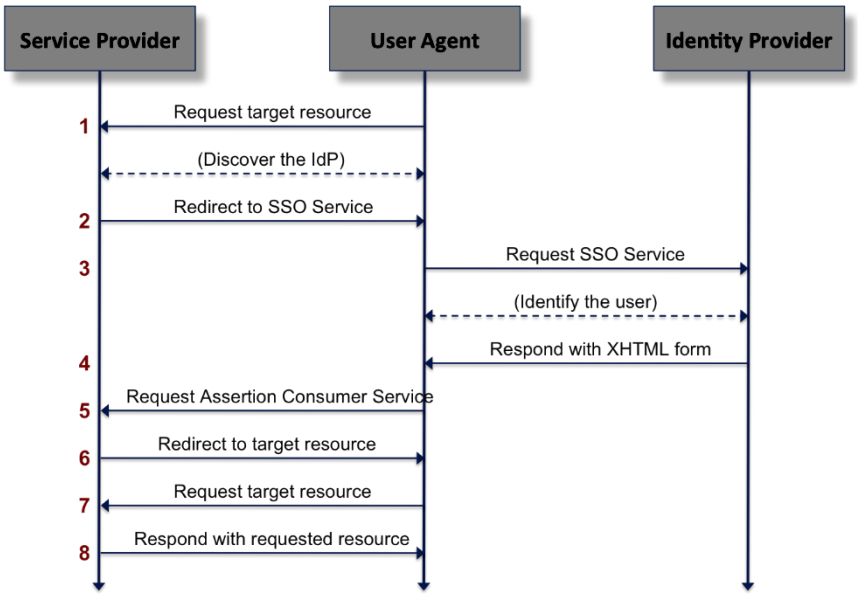

Figura 1

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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

ID	Indicatore di qualità	Modalità di Funzionamento	Valore limite
IQ-01	Disponibilità del sottoservizio di registrazione identità	*Erogazione automatica*	>= 99,0%
			Singolo evento di indisponibilità < =6 ore
		Erogazione in presenza	>= 98,0%
IQ-02	Tempo di risposta del sottoservizio di registrazione identità		<= 24h (ore lavorative)
IQ-03	Disponibilità del sottoservizio 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	Disponibilità del sottoservizio di sospensione e revoca delle credenziali		>= 99,0%
			Singolo evento di indisponibilità < =6 ore
IQ-07	Tempo di sospensione delle credenziali		< =30 minuti

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

IQ-08	Tempo di revoca delle credenziali		<= 5 giorni lavorativi
IQ-09	Disponibilità del sottoservizio 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 sottoservizio di autenticazione		>= 99,0%
			Singolo evento indisponibilità <= 4 ore
IQ-12	Tempo di risposta del sottoservizio di autenticazione		Tempo di risposta <=3 sec almeno nel 95,0% delle richieste
IQ-13	RPO sottoservizio registrazione e rilascio delle identità		1 ora
IQ-14	RTO sottoservizio registrazione e rilascio delle identità		8 ore
IQ-15	RPO sottoservizio di sospensione e revoca delle credenziali		1 ora

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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

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) 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, sviluppate e messe in atto da Sielte in qualità di gestore di identità, sono di fondamentale importanza per prevenire il verificarsi del furto d'identità, inteso o come impersonificazione totale (utilizzo indebito di dati appartenenti ad un altro soggetto) sia come impersonificazione parziale (utilizzo parziale di dati relativi alla propria persona combinati con alcuni dati appartenenti ad un altro soggetto).

Le misure anti-contraffazione 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 sul mercato. Vale la pena sicuramente precisare che l'**identità digitale** non è l'esatta corrispondenza dell'**identità fisica** in quanto ci sono aspetti della personalità che ne

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 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 del 24 ottobre 2014.

I controlli effettuati da Sielte per la validazione dell'autenticità dei dati si basano sull'utilizzo di sistemi quali Crimnet, SCIPAFI (Sistema pubblico di prevenzione), sito dell'Agenzia delle Entrate. 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 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 e tramite il sistema SCIPAFI;
- i dati anagrafici e dei documenti vengono verificati tramite il Sistema Pubblico di Prevenzione della Frode SCIPAFI (soltanto webcam);

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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.

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

- l'Operatore IdP 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 di guida, carta di identità e passaporto emessi da autorità italiane), le cui caratteristiche sono riscontrabili anche da remoto.

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 del 24 ottobre 2014 e del DPCM del 19 ottobre 2021, pubblicato sulla Gazzetta Ufficiale del 14/01/2021 n. 296, che modifica il DPCM del 24 ottobre 2014 nei seguenti articoli: 7,10,12,16.

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

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Enterprise. In figura è possibile visualizzare i componenti dell'architettura dell'infrastruttura utilizzata per la gestione delle identità digitali.

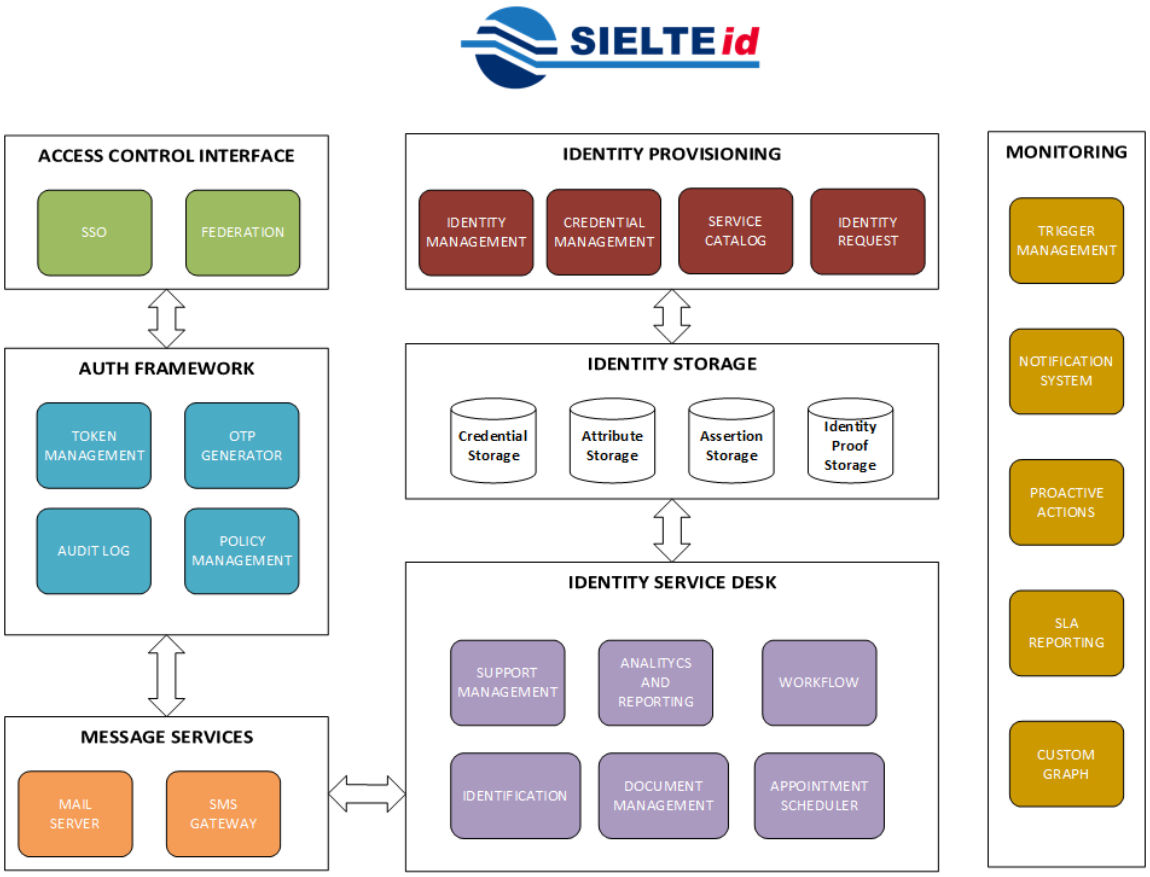

Figura 2

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

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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.
- **Access Control Interface –** contiene il modulo che esegue la logica di autenticazione interfacciandosi con i dati dell'identity storage per verificare lo stato e validità dell'identità e la correttezza delle credenziali.
- **Service Desk –** Strumento utilizzato per segnalare eventuali anomalie riscontrate dagli utenti 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

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 all'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 alla 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 29115:2015. 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'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.
- **Livello 3 SPID –** basato su un'autenticazione multi-fattore, è implementato tramite il controllo di una parola segreta (password), con le stesse caratteristiche del Livello 1 SPID, combinato alla verifica dei certificati di autenticazione contenuti nelle CIE 3.0 in corso di validità.

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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 e-mail, 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;

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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.

Le password hanno una durata massima non superiore a 180 giorni (6 mesi) e non possono essere riutilizzate prima di cinque variazioni e comunque non prima di 15 mesi, secondo quanto previsto dalla normativa in materia di protezione dei dati personali (D.Lgs. 196/2003 e Regolamento Europeo 2016/679- GDPR) e dall'art. 15 del *Regolamento modalità attuative SpID (art. 4 c. 2 DPCM 24 ottobre 2014).*

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 nella 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;

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

7. sul browser dell'utente viene installato un cookie, che serve per identificare la sessione di autenticazione 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 di configurazione:

- sul dispositivo mobile viene avviata l'applicazione MySielteID, successivamente vengono richieste le credenziali di accesso SPID;
- se validate con successo, l'utente validerà nel campo richiesto l'OTP inviato automaticamente tramite SMS;
- Completata la validazione dell'SMS, l'utente viene invitato a scegliere un PIN segreto. Configurato il codice, sui dispositivi con sistema operativo iOS e Android che ne sono provvisti, viene chiesto all'utente se abilitare o meno l'impronta digitale, utile per poter accedere all'app senza la necessità di dover inserire il codice di sicurezza. L'applicazione risulta così configurata 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 personale segreto inserito in fase di inizializzazione, e verrà generato il codice OTP temporaneo da inserire durante l'autenticazione di Livello SPID 2.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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.

Un ulteriore strumento di autenticazione di Livello SPID 2 è la generazione di un token tramite notifiche push. L'utente, che ha già attivato l'App sul suo smartphone ed ha dato il permesso di ricevere notifiche sull'App MySielteID, riceverà una notifica che lo inviterà ad accettare o a negare l'accesso di secondo livello. Se l'utente approva la richiesta ricevuta tramite notifica l'autenticazione si conclude con successo (se risponde entro il limite di tempo di un minuto, oltre il quale verrà visualizzato il messaggio di "Richiesta scaduta").

Nel caso di Android, è adoperata la tecnologia Firebase Cloud Messaging (FCM), che genera una chiave segreta alla prima configurazione dell'App. Al momento dell'invio della notifica, il messaggio viene codificato con la chiave segreta così che, al momento della ricezione della notifica all'interno dell'App, il token generato dal dispositivo viene validato.

Alla base delle notifiche push in iOS, invece, c'è Apple Push Notification Gateway (APNS). Si tratta di un servizio fornito da Apple che funge da tramite per trasmettere le notifiche da un application server ai dispositivi iOS. Il dispositivo, dopo aver generato il token, comunica con l'APNS, che decodifica il token e lo convalida con il certificato con cui è stata pubblicata l'App. Le notifiche inviate al device saranno codificate e decodificate dall'APNS attraverso la chiave segreta.

5.8.4 Dispositivo Crittografico multi-fattore (MF)

Il sistema di autenticazione Dispositivo Crittografico multi-fattore prevede l'utilizzo delle credenziali a singolo fattore della Basic Authentication, affiancato all'utilizzo di un dispositivo digitale appoggiando la CIE 3.0 contenente il certificato di autenticazione in corso di validità che richiedono l'attivazione attraverso un secondo fattore di autenticazione. Il processo di attivazione del dispositivo prevede che l'utente esegua le seguenti istruzioni di configurazione:

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- accede alla pagina del profilo, con autenticazione di Livello 2 SPID, disponibile tramite l'indirizzo https://profilo.sielteid.it;
- richiede l'attivazione della credenziale di tipo SPID Liv3 tramite la voce "Gestione SPID" nella sezione Spid Liv3 – Smartcard accedendo con il livello 2. Viene mostrata una mini-giuda utente su come associare il dispositivo;
- dopo aver collegato il dispositivo digitale con la CIE 3.0 viene richiesto di inserire il PIN della CIE e, se validato con successo, l'utente sceglie un alias da associare al suo certificato;
- completata la validazione del certificato, Spid Liv3 sarà attivo e il certificato risulterà nella lista dei certificati associati al profilo presenti nella sezione stessa.

6 RILASCIO IDENTITÀ DIGITALE

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

Richiesta identità
- Acquisizione dei dati per la creazione del profilo

Identificazione
- Esame e verifica dell'identità del richiedente

Emissione e consegna delle credenziali
- Emissione e consegna delle credenziali

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 un'identità da parte di estranei.

Il Richiedente si appresta ad effettuare la registrazione e a 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

La procedura di identificazione comporta che l'Utente Titolare sia identificato, prima del rilascio dell'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 CIE 3.0 in possesso del Richiedente;
3. da remoto, grazie a una sessione webcam con un Incaricato dell'IdP;
4. in presenza presso un Operatore incaricato.

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 nell'ambito del servizio SPID può connettersi al sito web https://www.sielteid.it ed effettuare la Registrazione tramite il Modulo di Adesione elettronico.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

6.1.1 Registrazione tramite Modulo di Adesione elettronico

Il processo si compone nelle fasi descritte di seguito:

1. Il Richiedente sceglie la tipologia di profilo con cui registrarsi. In SPID vengono identificati due tipologie di utente: **persona fisica** e **persona giuridica**.
2. Il Richiedente sceglie la modalità di identificazione, tra:
   a. ***Modalità Carta d'Identità Elettronica CIE 3.0:*** il Richiedente che dispone di una Carta d'Identità Elettronica CIE 3.0 e di un PIN associato alla CIE può scegliere questa modalità, identificandosi mediante l'App Sielte *Identifica* disponibile negli store digitali per smartphone con tecnologia NFC attiva.
   b. ***Modalità Webcam***: il Richiedente viene informato che per questa modalità di identificazione deve disporre di un PC, di uno Smartphone o di un Tablet dotati di webcam. Il Richiedente può scegliere tra due opzioni descritte di seguito:
      - ***Standard:*** permette di ottenere un appuntamento entro **5 giorni lavorativi** dalla richiesta. In caso di esito negativo delle verifiche sui documenti caricati, il Richiedente ha tempo fino a 60 minuti prima dell'appuntamento per caricare i documenti corretti, altrimenti perderà lo slot pianificato e dovrà schedulare un nuovo appuntamento.
      - ***Priority:*** permette di ottenere un appuntamento con "precedenza assoluta" entro un **massimo** di **4 ore lavorative** dalla richiesta. In caso di esito negativo delle verifiche sui documenti caricati, il Richiedente ha tempo fino al momento dell'appuntamento per caricare i documenti corretti o decidere di schedulare un nuovo appuntamento.

   Il Richiedente dovrà scegliere una delle due opzioni disponibili. Su ognuna di esse saranno presenti i dettagli del primo appuntamento disponibile per effettuare la videochiamata di riconoscimento.

   Il sistema riserva al Richiedente il primo appuntamento disponibile per l'opzione di identificazione webcam selezionato e concede 15 minuti di tempo

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

per completare l'inserimento dei dati richiesti e confermare l'appuntamento riservato; il Richiedente può in ogni caso modificare l'appuntamento riservato, in base alle sue esigenze, dopo aver caricato i documenti. Il pagamento relativo all'opzione scelta è eseguito tramite una piattaforma di pagamenti online semplice e sicura.

c. ***Modalità Sportello Pubblico:*** il Richiedente per questa modalità di identificazione deve recarsi presso un Comune abilitato e riceverà il pacchetto di attivazione via e-mail e il codice di attivazione suddiviso in due parti, una parte in modalità cartacea e l'altra all'indirizzo e-mail fornito dal Richiedente stesso. Tale modalità viene approfondita al par. 6.1.1.3.

d. ***Modalità Firma Digitale:*** il Richiedente per questa modalità di identificazione deve disporre di una Smart Card e di un lettore o di una chiavetta usb. Nel caso di persona giuridica è disponibile soltanto questa modalità di identificazione. Confermando tale modalità gli verranno fornite le istruzioni per scaricare il Modulo di Richiesta ricevuto tramite mail, firmarlo digitalmente e caricarlo sul sistema.

e. ***Modalità Carta Nazionale dei Servizi (CNS) [Non operativo]:*** il Richiedente per questa modalità di identificazione deve disporre di una Carta Nazionale dei Servizi (CNS), di un PIN, di un PC e di un lettore Smart Card.

3. Il Richiedente dichiara di:

- prendere visione dell'Informativa sul trattamento dei dati personali ai sensi del Regolamento UE 2016/679 per il trattamento dei dati effettuato nell'ambito dei Servizi Sielte
- Prendere visione della documentazione contrattuale (Condizioni Generali Contrattuali, Manuale Operativo, Guida Utente e Guida alla sicurezza dell'identità).

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

4. In seguito, il Richiedente passa alla verifica del proprio indirizzo e-mail; in questa fase il sistema effettua una verifica dell'univocità dell'indirizzo inserito, inviando un codice di verifica alla mail indicata per verificarne la validità.

   In questo modo Sielte si accerta che l'indirizzo fornito corrisponda ad una reale casella di posta elettronica, così come previsto dall'Art. 5 del Regolamento, e che l'indirizzo non sia già associato a un'altra identità.

5. Dopo aver verificato il proprio indirizzo e-mail, il Richiedente inserisce il numero di cellulare e richiede un codice di verifica che verrà inviato al numero stesso per verificarne la validità. Il codice OTP ricevuto dovrà essere inserito nel campo di testo dedicato, al fine di certificarne l'esistenza, l'univocità all'interno dei sistemi Sielte e la proprietà del numero di telefono (come previsto dall'Art.5 del Regolamento). Procede alla fase successiva immettendo il codice OTP corretto.

6. A questo punto, il Richiedente compila il Modulo di Richiesta elettronico, inserendo i propri dati anagrafici e i dati del domicilio. Nel caso di persona giuridica saranno presenti anche le sezioni riguardanti le informazioni aziendali e la sede legale.

   Consapevole che la falsa dichiarazione delle proprie generalità è un reato penale, per cui saranno effettuati controlli anche successivi alla fase di identificazione, dichiara sotto la propria responsabilità che le informazioni fornite corrispondono a verità.

   In questa fase, tramite il sistema, viene effettuata la verifica della veridicità e univocità in ambito Sielte del codice fiscale (tramite i dati Nome, Cognome, Data e Comune di Nascita).
   Nel caso di persona giuridica sono presenti anche le sezioni riguardanti le informazioni aziendali e la sede legale.

   Inseriti correttamente i dati personali, riceve la mail di benvenuto con le credenziali per l'accesso nel caso in cui debba sospendere la registrazione.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

7. Successivamente, viene richiesto di inserire gli estremi del documento di identità prescelto per l'identificazione (i documenti di riconoscimento ammessi per l'identificazione sono: Carta d'identità, Patente versione tessera e Passaporto). Nel caso di identificazione "Webcam" e "Firma Digitale" il Richiedente deve allegare foto o scansione del fronte e del retro del documento di riconoscimento e della tessera sanitaria o, nel caso di soggetti sprovvisti di Tessera Sanitaria, il tesserino del codice fiscale o equipollenti certificati sostituitivi.

   Se persona giuridica, viene richiesto di caricare anche la Visura Camerale della società e i documenti di riconoscimento caricati corrispondono a quelli del Legale Rappresentante.

8. Dopo aver confermato l'appuntamento e selezionato la piattaforma con cui effettuare la videochiamata, dovrà procedere confermando il riepilogo ordine e saldando il corrispettivo dovuto, tramite la procedura guidata.

9. Confermando i dati dal riepilogo, il Richiedente riceve una e-mail contenente in allegato il Modulo di Richiesta compilato con i dati precedentemente inseriti.

   - Se ha scelto la modalità "Firma digitale", l'utente firma digitalmente con un software di firma digitale il Modulo di Adesione e lo carica sul sistema. Il sistema informa il Richiedente che il documento è stato caricato con successo e di attendere una mail di conferma circa l'avvenuta identificazione (che riceverà dopo la verifica da parte di un Operatore IdP della validità della firma digitale apposta sul documento).
   - **[Non operativo]** Se ha scelto la modalità CNS (Carta Nazionale dei Servizi), il Richiedente inserisce la smartcard ed il pin e il sistema lo valida, identificandolo istantaneamente.
   - Infine, se possiede una Carta d'Identità Elettronica 3.0, il Richiedente può identificarsi tramite l'app di Sielte *Identifica*, disponibile negli store digitali per dispositivi dotati di tecnologia NFC.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Qualora il Richiedente debba sospendere per qualunque motivo (mancanza di rete, mancanza di disponibilità, ecc.) la fase di Registrazione, può in qualsiasi momento riprendere la registrazione dal punto lasciato in sospeso ricollegandosi al sito, cliccando su *Riprendi Registrazione* ed inserendo le credenziali: username (codice fiscale) e password temporanea, ricevute nella e-mail di Benvenuto, dopo aver compilato i suoi dati anagrafici.

6.1.1.1 REGISTRAZIONE IDENTITÀ PREGRESSA CON MIGRAZIONE ASSISTITA

Il Richiedente ha la possibilità di ottenere la sua identità digitale tramite l'SP-Ip presso cui ha un account; il profilo viene trasferito all'Identity Provider scelto dal titolare, in cui dovrà completare la registrazione.

Sarà necessario, dunque, che l'utente sia autenticato sull' SP presso cui ha l'account.

L'asserzione generata dovrà essere firmata e i dati dovranno essere criptati dall'SP.

Lo scenario prevede che l'utente, obbligatoriamente autenticato, possa essere reindirizzato su sua richiesta verso un IdP, in cui troverà la maschera di registrazione precompilata con i dati forniti obbligatoriamente dal SP: Nome, Cognome e Codice Fiscale.

L'utente può effettuare la procedura di richiesta dell'Identità Digitale completando la registrazione secondo quanto descritto nel paragrafo 6.1.1 e la fase di identificazione in base alla modalità prescelta secondo quanto descritto nel paragrafo 6.1.1.

6.1.1.2 REGISTRAZIONE IDENTITÀ PREGRESSA

Il Richiedente ha la possibilità di ottenere la sua Identità Digitale tramite l'SP presso cui ha già un'identità; il profilo viene trasferito presso l'IdP scelto dal titolare che dovrà completare la registrazione con le altre informazioni necessarie per ottenere l'Identità Digitale SPID. L'utente, dopo aver effettuato l'autenticazione sul servizio dell'SP con un livello equivalente al livello SPID 2 (LoA3), clicca sul pulsante *Ottieni SPID*; a quel punto l'SP trasmette i dati obbligatori all'IdP scelto dall'utente (Nome, Cognome e Codice Fiscale), e completa la registrazione secondo quanto sotto riportato:

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- Il Richiedente prende visione dell'informativa ai sensi del D.L.vo n. 196/2003 ed ai sensi del Regolamento UE 2016/679 per il trattamento dei dati personali nell'ambito dei Servizi Sielte; prende, inoltre, visione delle documentazioni (Condizioni Generali Contrattuali, il Manuale Operativo, il Manuale Utente e la Guida alla sicurezza dell'identità) e clicca sul pulsante "Avanti".
- In seguito, il Richiedente passa alla verifica dell'indirizzo e-mail e del numero di cellulare così come descritto nel paragrafo 6.1.1.
- Il Richiedente compila il Modulo di Richiesta elettronico, inserendo i propri dati anagrafici e i dati del domicilio. Inseriti correttamente i dati personali, riceve la mail di benvenuto insieme alla password temporanea. Inseriti correttamente i dati personali, riceve la mail di benvenuto con le credenziali per l'accesso nel caso in cui debba sospendere la registrazione.
- Successivamente, gli viene richiesto di inserire gli estremi del documento di identità.
- Procedendo, visualizza il Riepilogo dei dati inseriti dove può modificarli.
- Confermando i dati, il Richiedente riceve un'e-mail contenente in allegato il Modulo di Richiesta compilato, che presenta i dati inseriti ed il link per attivarsi.

Una volta attivato, sarà compito dell'IdP comunicare all'SP da cui proviene l'utente l'avvenuta attivazione.

6.1.1.3 REGISTRAZIONE TRAMITE SPORTELLO PUBBLICO

L'IdP si avvale della procedura di identificazione effettuata presso lo sportello da un RAO (Registration Authority Officer) Pubblico, cioè un operatore che è un pubblico ufficiale espressamente incaricato da una Pubblica Amministrazione per l'espletamento dell'attività di identificazione.

L'operatore di uno sportello pubblico effettua l'identificazione dell'utente, accertando l'identità del Richiedente tramite la verifica di un documento di riconoscimento integro e in

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

corso di validità, munito di fotografia e firma autografa dello stesso, e controlla la validità del codice fiscale, verificando che anche la tessera sanitaria sia in corso di validità.

Se i documenti presentati dal Richiedente risultano carenti delle caratteristiche di cui sopra, il processo di identificazione viene sospeso fino all'esibizione di documenti validi ed integri.

L'operatore, effettuato il riconoscimento, compila a sistema la scheda anagrafica con i seguenti dati dell'utente:

- Nome e Cognome
- Luogo e Data di nascita
- Sesso
- Codice Fiscale
- Estremi del documento d'identità in corso di validità utilizzato ai fini dell'identificazione
- Numero di cellulare
- Indirizzo di posta elettronica
- Domicilio

Il sistema permette la generazione del codice di attivazione e consente la creazione del token, necessari per concludere con esito positivo le procedure di identificazione e attivazione.

L'operatore consegna all'utente metà del codice di attivazione in modalità cartacea e l'altra metà viene inviata all'indirizzo e-mail fornito dall'utente, unitamente al token.

La lunghezza del codice di attivazione è di 12 caratteri, generati in maniera casuale, e deve contenere almeno una lettera maiuscola, una lettera minuscola, un carattere numerico e un carattere speciale. Come sopra detto, ai fini del processo, il codice di attivazione è diviso in due parti da 6 caratteri ciascuno.

Il token ha validità di 30 giorni, periodo in cui l'utente, a cui fanno riferimento le informazioni contenute nel token, può utilizzarlo per ottenere l'Identità Digitale.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

L'utente si collega al sito https://www.sielteid.it e seleziona la modalità "Sportello Pubblico". Viene richiesto l'inserimento del Codice Fiscale, segue l'upload del token e gli viene quindi richiesto l'inserimento del codice di attivazione (prima parte cartacea e seconda parte ricevuta tramite mail).

L'utente ha a disposizione 5 tentativi, superati i tentativi errati di inserimento del codice di attivazione, il token non viene più accettato dall'IdP, di conseguenza l'utente dovrà recarsi nuovamente allo sportello pubblico.

Se l'inserimento del codice di attivazione va a buon fine prosegue accettando l'informativa, conferma l'indirizzo mail e numero di cellulare, comunicati precedentemente all'operatore dello sportello, tramite verifica OTP. L'utente visualizza il Riepilogo con la possibilità di modificare le informazioni e conferma i propri dati. Se la conferma dei dati ha avuto esito negativo la pagina presenterà a video un messaggio per informare il Richiedente che la sua pratica è in fase di ulteriori controlli da parte di un Operatore IdP e che riceverà aggiornamenti sullo stato della pratica via e-mail.

Se la conferma dei dati ha avuto esito positivo conclude la fase di Identificazione effettuando il cambio password e scegliendo la domanda segreta. Il profilo è così attivo.

I RAO Pubblici si assumono la responsabilità della corretta verifica dell'identità personale dell'utente e sono tenuti a mantenere le evidenze per individuare il singolo operatore che ha effettuato il riconoscimento.

6.1.2 Registrazione tramite RA [Non operativo]

Il Richiedente ha la possibilità di ottenere la sua Identità Digitale recandosi in uno degli uffici preposti RA convenzionati con Sielte visionabili tramite questo link https://www.sielteid.it/lra.html. L'Operatore RAO, supportando il Richiedente attraverso la compilazione del modulo di adesione, effettua l'identificazione a vista secondo quanto successivamente descritto.

Il richiedente viene identificato di persona tramite esibizione di:

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- Un valido documento di identità rilasciato da un'autorità italiana;
- Tessera sanitaria o, nel caso di soggetti sprovvisti di Tessera Sanitaria, il tesserino del codice fiscale o equipollenti certificati sostituitivi.

Tra i documenti validi riconosciuti da Sielte vi sono alcuni fra i documenti di riconoscimento ammessi per l'identificazione secondo il DPR 445/2000, art. 35 ovvero quelli equipollenti alla carta di identità come il passaporto e la patente di guida, purché munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato.

L'Incaricato RAO, dopo aver inserito a sistema i dati del richiedente, acquisisce una copia digitale e carica a sistema il documento di riconoscimento e la tessera sanitaria utilizzati per identificare il Cittadino. Generata l'anagrafica con relativo Modulo di Adesione del Richiedente, l'Operatore RAO provvede a stampare il suddetto modulo, facendolo firmare al Richiedente e caricandolo successivamente in piattaforma.

Segue una fase di Verifica e Validazione dei dati da parte dell'Operatore RAO, secondo il procedimento descritto al paragrafo 6.2.1. Se le verifiche hanno generato esito positivo, l'Operatore provvede a identificare il Richiedente.

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.

Il Richiedente riceve quindi una e-mail contenente la propria Username, una Password temporanea ed un link sul quale deve cliccare per prendere visione della documentazione (Condizioni Generali Contrattuali, il Manuale Operativo, il Manuale Utente e la Guida alla sicurezza dell'identità).

Il Richiedente valida successivamente 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; contestualmente, riceve un OTP sul proprio telefono, che deve inserire, sempre all'interno della pagina in cui si trova, nel campo di testo dedicato, al fine di certificare l'esistenza e la proprietà del numero di telefono. Successivamente effettua il cambio password, sceglie la domanda segreta ed

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

attiva la propria identità digitale, ricevendo contestualmente una mail con i codici di sospensione, revoca e sblocco sospensione e i relativi link alla documentazione.

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 a 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[1] 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.

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

6.2.1 Verifica e Validazione dei dati

L'operatore Idp 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 del 24 ottobre 2014, principalmente attraverso l'utilizzo di sistemi di controllo. Il riscontro si configura, quindi, come efficace strumento di prevenzione per i furti d'identità sia totali che parziali.

Per ogni richiesta vengono eseguite le seguenti verifiche:

---

[1] Documenti cartacei acquisiti in forma digitale

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- **furto o smarrimento del documento** tramite il servizio online disponibile sul sito della Polizia di Stato (Crimnet)[2], assicurandosi che non ci siano denunce di furto o smarrimento;
- **corrispondenza tra il codice fiscale e i dati anagrafici di una persona** tramite il servizio online sul sito dell'Agenzia delle Entrate;
- **verifica generale dei dati e dei documenti** tramite il sistema pubblico di prevenzione delle frodi SCIPAFI.

Inoltre, in caso di identificazione *Webcam* o *Di Persona*, gli Operatori verificano che il documento di riconoscimento caricato 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.

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.

Nel caso di persone giuridiche, oltre alla verifica dei documenti, viene controllato anche che il documento di visura camerale non sia più vecchio di sei mesi e firmato digitalmente dal legale rappresentante dell'azienda; tale controllo viene effettuato attraverso il sito registroimprese.it. Inoltre, viene verificato che il Richiedente figuri attestante dei poteri di rappresentanza all'interno della Visura.

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

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

6.2.2 Identificazione in base alla modalità prescelta dal Richiedente

6.2.2.1 IDENTIFICAZIONE A VISTA DA REMOTO

L'Operatore IdP che ha in carico la Richiesta procede con la fase di identificazione dopo le verifiche effettuate.

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

Effettuando la videochiamata tramite piattaforme terze di contatto, messaging e video call, i dati e le interazioni sono soggette alle impostazioni privacy dell'account del Richiedente associato alle piattaforme. I dati correlati all'account del Richiedente vengono temporaneamente inseriti dall'Operatore IdP nell'elenco dei contatti, con la finalità di effettuare la videochiamata. Al termine della sessione audio/video l'account del Richiedente verrà eliminato dal suddetto elenco. La relazione instauratasi tramite piattaforme terze di contatto, messaging e video call sarà utilizzata solo ed esclusivamente e per il tempo necessario per effettuare la procedura di video identificazione; inoltre è garantita la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati alla versione più recente. I canali di video piattaforma sono infatti stati selezionati perché crittografati end-to-end.

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 a identificare il Richiedente grazie ad una sessione video registrata, seguendo il processo sottoindicato.

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).

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Sielte è responsabile della valutazione in merito alla sussistenza delle condizioni idonee della sessione, 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 e pone al Richiedente in modo casuale delle domande sulle sue generalità. Chiede quindi conferma di data ed orario della videochiamata, di numero di cellulare ed indirizzo di posta elettronica (come previsto dall'Art. 8 del Regolamento).

Il Richiedente deve rispondere alle domande di conferma di cui sopra, che l'Operatore in modo casuale gli pone 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 fronte/retro del documento di riconoscimento e tessera sanitaria (come previsto dall'Art. 8, commi i) e j) del Regolamento) o, nel caso di soggetti sprovvisti di Tessera Sanitaria, il tesserino del codice fiscale o equipollenti certificati sostituitivi. I documenti devono essere gli originali delle copie che il Richiedente ha inserito 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

6.2.2.2 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) e lo carica nella form. 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.

6.2.2.3 IDENTIFICAZIONE INFORMATICA TRAMITE DOCUMENTI DIGITALI DI IDENTITÀ

In caso di scelta di identificazione tramite la suddetta modalità, il Richiedente compila il Modulo di Adesione inserendo i dati necessari all'identificazione. Il Richiedente può identificarsi con:

- ***Carta Identità Elettronica CIE 3.0:*** se possiede carta di identità elettronica con CIE 3.0 scarica l'app di Sielte *Identifica*, funzionante solo su dispositivi dotati di NFC. Dopo aver installato l'app, inserisce le credenziali temporanee ricevute nella e-mail di Benvenuto, digita il PIN richiesto, avvicina la CIE 3.0 allo smartphone per l'identificazione tramite NFC, per attivare la lettura dei dati. Se il PIN precedentemente inserito è corretto e la carta viene riconosciuta, il Richiedente viene identificato. Diversamente, se la verifica non va a buon fine, l'app presenterà a video un messaggio per informare il Richiedente che la sua pratica è in fase di ulteriori

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

controlli da parte di un Operatore IdP e che riceverà aggiornamenti sullo stato della pratica via e-mail.

- ***CNS (Carta Nazionale dei Servizi) [Non operativo]:*** se possiede una CNS (carta nazionale dei servizi) inserisce la carta nel lettore Smart Card collegato al PC, insieme al PIN richiesto e, se corretto, viene identificato.

Sielte considera identificato il Richiedente con queste modalità. Tali modalità di identificazione si basano 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. Il Richiedente riceve una mail con un link da cliccare per attivare l'identità e dopo l'attivazione riceverà un'altra mail con i codici utente del servizio SPID.

6.3 Attivazione dell'ID

In caso di verifiche positive, viene inviata una e-mail all'indirizzo del Richiedente, contenente un link per l'attivazione dell'ID, 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 nella mail di benvenuto; deve obbligatoriamente cambiare la password temporanea, inserendo una password a sua scelta (seguendo determinate regole di password sicura dettate dal Regolamento delle modalità attuative, art. 14) e viene scelta la domanda segreta. Il sistema procede così all'attivazione dell'Identità Digitale.

Nella fase di rilascio dell'Identità Digitale viene mandata una mail con le seguenti informazioni:

- **Codici segreti per l'utilizzo dell'Identità Digitale** – i codici segreti (codice di sospensione, revoca e sblocco sospensione) che servono per la gestione dell'Identità Digitale e delle relative credenziali.
- **Documentazione contrattuale** – Condizioni Generali del Contratto, Manuale Operativo, Informativa Privacy, Guida alla Sicurezza dell'Identità e Manuale Utente.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

6.4 Attivazione delle credenziali di Livello 1, 2 e 3

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, durante la fase di registrazione nella mail di Benvenuto. Successivamente, l'utente dovrà necessariamente impostare una nuova password con i seguenti criteri di protezione: lunghezza minima di 8 caratteri e lunghezza massima di 16 caratteri, che contiene caratteri maiuscoli e minuscoli, contiene almeno un carattere numerico, non contiene più di due caratteri identici consecutivi e contiene almeno un carattere speciale (#, $, %, ecc.). Effettuato il cambio della password, l'utente può impostare la domanda segreta e quindi visualizzare i propri dati.
- **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 installare e configurare l'App MySielteID su un dispositivo smartphone o tablet con sistema operativo Android, iOS o HarmonyOS. L'app servirà a generare un codice OTP da utilizzare in accoppiata alle credenziali di Livello 1. È possibile configurare il Liv2 dall'app stessa tramite SMS. SielteID mette altresì a disposizione dell'utente il Servizio "Crediti SMS" per gli accessi con Livello di sicurezza 2 con OTP consegnato via SMS: l'utente che aderisce a tale servizio ha a sua disposizione un credito costituito da un tot di SMS. Quando l'utente effettua un accesso di Livello 2 consuma un SMS e può ricaricare sul proprio profilo la quantità di SMS a sua disposizione ogni qualvolta che lo desidera.
- **Credenziali con sicurezza di Livello 3 SPID** - in questo caso viene utilizzato lo stesso meccanismo per il rilascio delle credenziali di Livello 1 SPID. In aggiunta, è necessario un dispositivo digitale che richiede di appoggiare la

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

CIE 3.0 contenente il certificato di autenticazione in corso di validità per accedere ai servizi di Livello 3. L'operazione per attivare le credenziali di Livello 3 è disponibile dalla pagina del proprio profilo SielteID su "Gestione SPID" nella sezione Spid Liv3 - Smartcard.

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 dopo l'attivazione delle credenziali;

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- 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 dopo l'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.

Nel caso in cui Sielte dovesse rilevare anomalie o irregolarità su un'Identità Digitale rilasciata, o dovesse avere dei sospetti, oltre ad eseguire le dovute verifiche del caso, provvederà a contattare l'utente mediante il recapito telefonico fornito, al fine di confermare l'identità del richiedente. Qualora il contatto non andasse a buon fine per irraggiungibilità del canale telefonico su più tentativi, Sielte provvederà alla cautelativa sospensione dell'identità, riattivandola dopo aver rettificato/chiarito le presunte irregolarità o sospetti.

La revoca dell'Identità Digitale può essere richiesta dall'utente attivo.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 dopo l'attivazione delle credenziali;
- inserire la motivazione della richiesta di revoca.

L'operatore IdP, che riceve la richiesta di revoca, provvede a verificare tutta la documentazione ricevuta. 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.

Nel caso in cui tutta la documentazione fornita per la revoca dell'Identità Digitale sia corretta, quindi, l'utente riceve presso il proprio indirizzo e-mail una notifica di conferma di avvenuta revoca dell'Identità Digitale.

SIELTE revoca in autonomia l'Identità Digitale all'UTENTE nei casi in cui:

- l'Identità Digitale non è stata rilasciata secondo quanto previsto dalla vigente normativa e dal Manuale Operativo;
- in fase di identificazione viene a mancare almeno uno dei prerequisiti previsti;
- i dati immessi dall'UTENTE al momento della registrazione vengono modificati.

L'Identità Digitale va inoltre revocata se viene riscontrata l'inattività per un periodo superiore ai 24 mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica.
SIELTE, nel pieno rispetto della normativa vigente, si riserva la facoltà di procedere alla revoca dell'Identità Digitale in quei casi in cui, a proprio insindacabile giudizio, ritenesse venute meno le condizioni di sicurezza per l'espletamento dell'attività di Identity Provider.
In ogni caso, qualora l'utente volesse usufruire del servizio SPID, dopo la revoca, potrà effettuare una nuova registrazione e procedere ad una nuova identificazione.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Nel caso in cui l'utente attivo non ricordi le sue credenziali (password, mail, cellulare e domanda segreta), lo stesso dovrà inoltrare la richiesta di revoca all'indirizzo sistemi.sielte@legalmail.it per mezzo PEC allegando il Modulo Richiesta Revoca (comprensivo dei documenti richiesti dal modulo) – scaricabile dal sito istituzionale www.sielteid.it (sezione Documentazione) o dal profilo personale dell'UTENTE (sezione Documenti), debitamente compilato in tutte le sue parti e firmato tramite firma autografa o digitale. Nel caso di firma digitale, non sarà necessario inviare la richiesta tramite una casella PEC, potrà quindi essere inoltrata tramite una normale casella e-mail all'indirizzo sistemi.sielte@legalmail.it.

Gli utenti che dovessero far pervenire a mezzo PEC la richiesta di revoca verranno contattati dal Customer Care del Gestore, al fine confermare la reale volontà dell'utente e la sua identità. Confermate tali informazioni, insieme alle verifiche standard di processo sulla documentazione inoltrata, l'Operatore procede a revocare l'Identità Digitale come da richiesta pervenuta.

Qualora l'utente non fosse in possesso di un indirizzo PEC o di una firma digitale sarà necessario attendere la Revoca automatica dopo due anni di inutilizzo dell'identità.

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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 recupero delle proprie credenziali, come spiegato nel paragrafo 7.4.

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 dalla sezione Profilo su **"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 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 **"Recupero password"**, dalla login box di accesso.

7.4.1 Recupero Password.

Nel caso in cui l'utente non ricordi la propria password personale e risulti in possesso dell'indirizzo e-mail e del numero di cellulare associati al proprio profilo SPID, riceverà su ciascuno di essi, un codice OTP da inserire; validati i due codici OTP, potrà procedere all'inserimento di una nuova password.

7.4.2 Recupero Password e cellulare.

Nel caso in cui l'utente non ricordi la propria password e risulti in possesso soltanto dell'indirizzo e-mail e non del numero di cellulare, dovrà rispondere ad un set di domande

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

personali o alla domanda segreta precedentemente impostata; se non risponde correttamente alla domanda avrà un numero massimo di tre tentativi giornalieri, rispondendo invece correttamente riceverà un codice OTP all'indirizzo email associato al proprio profilo SPID per verificare l'identità; validato il codice OTP ricevuto via email potrà inserire un nuovo numero di cellulare, sul quale riceverà un altro codice OTP di conferma, utile a validarlo; infine, potrà procedere all'inserimento di una nuova password.

7.4.3 Recupero Password ed e-mail.

Nel caso in cui l'utente non ricordi la sua password e risulti essere in possesso soltanto del numero di cellulare e non dell'indirizzo e-mail, dovrà rispondere ad un set di domande personali o alla domanda segreta precedentemente impostata; se non risponde correttamente alla domanda avrà un numero massimo di tre tentativi giornalieri, rispondendo invece correttamente riceverà un codice OTP al numero di cellulare associato al proprio profilo SPID per verificare l'identità; validato il codice OTP ricevuto tramite sms potrà inserire un nuovo indirizzo e-mail, sul quale riceverà un codice OTP di conferma, utile a verificarlo; infine, potrà procedere all'inserimento di una nuova password.

7.4.4 Recupero Password, e-mail e cellulare.

Nel caso in cui l'utente non ricordi la sua password e non risulti essere in possesso di nessuno dei due attributi associati al proprio profilo SPID (indirizzo e-mail e numero di cellulare), l'utente dovrà compilare una form in cui dovrà rispondere ad un set di domande personali relative alla sua identità digitale quali:

- modalità di identificazione effettuata;
- numero di cellulare inserito in fase di registrazione;
- indirizzo mail inserito in fase di registrazione;
- tipo, numero e data di scadenza del documento di identità inserito in fase di registrazione;

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- numero identificativo e data di scadenza della tessera sanitaria (o numero identificativo del tesserino del codice fiscale nel caso di soggetti sprovvisti di tessera sanitaria) inserito in fase di registrazione;
- domanda segreta precedentemente impostata.

Successivamente dovrà inserire il nuovo indirizzo e-mail e il nuovo numero di cellulare da associare alla propria identità, 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, sotto forma di *Richiesta di Recupero*.

La richiesta verrà controllata e verificata dall'operatore che, dopo un primo check da parte del sistema che ha validato le risposte inserite dall'utente in fase di richiesta, controllerà le risposte date confrontando anche i documenti caricati dall'utente in fase di registrazione decidendo se approvarla o rifiutarla. In entrambi i casi l'utente riceverà una mail con l'esito della richiesta. Se la richiesta viene approvata l'utente riceverà una mail con una password temporanea con la quale potrà accedere al profilo e procedere all'inserimento di una nuova password.

Se l'operatore rigetta la Richiesta di Recupero, l'utente riceverà una mail in cui è specificato che la richiesta è stata respinta, di conseguenza dovrà ripetere la procedura, rispondendo correttamente a tutte le domande. L'operatore al terzo tentativo rigettato sospende l'identità per motivi di sicurezza.

Di conseguenza l'utente che ha effettuato la *Richiesta di Recupero* non ha soddisfatto i requisiti utili per effettuare il recupero delle credenziali; pertanto, dovrà provvedere ad inviare una richiesta di revoca tramite pec all'indirizzo sistemi.sielte@legalmail.it allegando, oltre alla richiesta, copia dei documenti di riconoscimento. Qualora l'utente volesse usufruire del servizio SPID, dopo la revoca, potrà effettuare una nuova registrazione per procedere ad una nuova identificazione.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

7.5 Gestione e rinnovo 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 eseguito un accesso di livello 2.

L'utente riceverà per mail una comunicazione che gli ricorderà la data di scadenza della propria identità digitale.

Al momento della scadenza, l'Identità Digitale sarà rinnovata per due anni in automatico.

L'utente può anche richiedere di non rinnovare automaticamente l'identità tramite una comunicazione da inviare all'indirizzo pec sistemi.sielte@legalmail.it. La comunicazione deve pervenire almeno trenta giorni prima, indicando la data a decorrere dalla quale si richiede la cessazione del servizio.

Qualora l'utente volesse usufruire nuovamente del servizio SPID dopo il recesso, dovrà effettuare una nuova registrazione per procedere poi ad una nuova identificazione.

8 IDENTITA' DIGITALE PER MINORENNI

Il servizio SielteID, in conformità a quanto previsto dalle *Linee guida operative per la fruizione dei servizi SPID da parte dei minori* emanate da AgID, rende disponibile il rilascio e gestione dell'identità digitale per i minori.

I minori possono ottenere la propria identità digitale e fruire autonomamente di servizi online, richiedendo, nei casi previsti, l'autorizzazione all'accesso da parte di chi ne esercita la responsabilità genitoriale.

Il rilascio Spid ai minori deve essere richiesto da parte dell'esercente la responsabilità genitoriale, avente già una identità SielteID attiva; segue poi una fase di registrazione del minore, di controllo e di identificazione.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Sono richiesti documenti specifici al fine del rilascio dell'identità, sia relativi al minore sia relativi all'esercente la responsabilità genitoriale.

8.1 Rilascio spid Minori

8.1.1 Richiesta Identità da parte del Genitore/Tutore

La richiesta di un'identità digitale SPID per un minore deve essere avviata da chi esercita la responsabilità genitoriale ed è titolare di un'identità digitale SielteID attiva.

Spid minori può essere rilasciato a minori in età compresa tra i 5 e 17 anni.

Il Richiedente avente la responsabilità genitoriale può avviare la richiesta dell'identità digitale del minore dalla sua area riservata, sul sito https://www.sielteid.it, accedendo al proprio profilo personale, nella sezione "Identità Minore", e compilando la richiesta di nuova identità minore.

La richiesta prevede i seguenti dati anagrafici del minore:

- nome e cognome
- codice fiscale
- data di nascita
- luogo di nascita
- provincia di nascita
- sesso

Il Richiedente dichiara la propria qualità di esercente la responsabilità genitoriale sul minore scegliendo tra le opzioni:

- genitore
- genitore affidatario
- tutore legale

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Nel caso in cui viene selezionato l'opzione **"genitore**", se nel documento del minore non è presente il nome e cognome del Richiedente, quest'ultimo deve allegare il certificato di stato di famiglia.

Nel caso in cui viene selezionato l'opzione **"genitore affidatario" o "tutore legale"**, il Richiedente deve allegare il decreto del giudice tutelare o del Tribunale dei minorenni, attestante la nomina del tutore o l'affidamento del minore.

Il Richiedente dichiara, con assunzione di responsabilità, ai sensi dell'art.47 del DPR 445/2000:

- se esiste **un secondo** soggetto con responsabilità genitoriale sul minore, e di essere stato autorizzato alla gestione dell'identità del minore. Viene richiesto copia di un documento di identità del secondo soggetto.
- se è l'unico esercente la responsabilità genitoriale sul minore e di darne prova con un documento che attesti tale condizione (*ad esempio:* stato di morte dell'altro genitore, nomina in qualità di tutore, ecc.)

Infine, viene chiesta la presa visione e accettazione dei seguenti documenti:

- informativa sul trattamento dei dati personali del minore per il rilascio e la gestione dell'identità digitale, ai sensi degli art. 12 e ss. del GDPR
- ricezione di notifiche da parte dell'IdP per l'autorizzazione all'utilizzo di SPID da parte del minore.
- condizioni generali del contratto.

Completato l'inserimento dei dati, il Richiedente passa al pagamento una tantum della videochiamata di identificazione del minore.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

L'utente viene informato dell'invio di una e-mail contenente il *codice di verifica*, il quale ha una durata di validità di 30 giorni e deve essere comunicato al minore per procedere con la registrazione online e rilascio dell'identità digitale.

La richiesta di rilascio identità minore segue un flusso di avanzamento stati fino al rilascio dell'identità. Il Richiedente può verificare lo **stato** di avanzamento della richiesta dalla propria area personale dell'identità digitale dedicata alla gestione delle identità minore:

8.1.2 Registrazione da parte del Minore

Una volta ricevuto il codice di verifica dal Richiedente, il minore deve eseguire la registrazione sul sito https://www.sielteid.it selezionando l'opzione "**Cittadino Minorenne**".

Il minore compila i campi richiesti iniziando dal **"codice fiscale"** e **"codice di verifica"** precedentemente comunicato dal genitore/tutore.

Il minore dichiara di:

- prendere visione dell'Informativa sul trattamento dei dati personali ai sensi del Regolamento UE 2016/679 per il trattamento dei dati effettuato nell'ambito dei Servizi Sielte.
- Prendere visione della documentazione contrattuale (Condizioni Generali Contrattuali, Manuale Operativo, Guida Utente e Guida alla sicurezza dell'identità).

In seguito, il minore inserisce i seguenti dati

- indirizzo e-mail, sul quale riceve il codice di verifica per validare l'indirizzo;
- numero di cellulare (facoltativo)

  nel caso in cui il minore non sia in possesso di un numero di cellulare, al fine di garantire specifiche funzionalità come la procedura di recupero delle credenziali, il sistema assocerà in automatico il numero di cellulare del Richiedente che NON può essere utilizzato per l'accesso di secondo livello.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- indirizzo di domicilio
- documento d'identità in corso di validità
- tessera sanitaria

A questo punto il minore sceglie l'appuntamento per la identificazione e modalità di connessione.

8.1.3 Verifica e validazione dati

Gli Operatori IdP verificano i dati della richiesta compilata dal genitore/tutore, secondo le consuete modalità.

Se la verifica è negativa, viene inviata un'e-mail al genitore/tutore per indicare i dati e/o documenti da correggere e riallegare.

Gli Operatori IdP verificano successivamente i dati della registrazione compilata dal minore secondo la modalità di verifica indicata nel capitolo Verifica e Validazione dei dati.

Completate le verifiche di tutti i dati, si procede alla identificazione del minore tramite video identificazione, dove non sono ammessi documenti in fotocopia ma solo in originale.

*Si evidenzia che se non si procede con il completamento della richiesta o identificazione, in **30 giorni** la registrazione del minore viene annullata e dopo **60 giorni** viene cancellata (come previsto dal normale flusso di una registrazione abbandonata).*

8.1.4 *Identificazione*

La procedura di identificazione del minore viene eseguita tramite video identificazione secondo le modalità già indicate nel paragrafo *Identificazione a vista da remoto* e prevede, in aggiunta, l'affiancamento del genitore/tutore che ne ha richiesto l'identità digitale.

Il genitore/tutore deve confermare la propria identità e di esercitare la responsabilità genitoriale del minore, mostrando un documento di identità originale.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

L'Operatore pone al minore delle domande sulle sue generalità e chiede conferma di data ed orario della videochiamata, del numero di cellulare ed indirizzo di posta elettronica (come previsto dall'Art. 8 del Regolamento).

L'Operatore chiede al minore di mostrare fronte/retro del documento di riconoscimento e tessera sanitaria in originale.

Il minore può essere assistito dal genitore/tutore nelle suddette operazioni (*esempio se il minore è troppo piccolo, esempio di meno di dieci anni, e/o presenta difficoltà nel rispondere o ricordare i dati).*

8.1.5 Attivazione identità

Se la procedura di identificazione si conclude con successo, viene inviata una e-mail al minore e genitore/tutore con le istruzioni per attivare l'identità secondo quanto descritto nel capitolo *Attivazione dell'ID* e *Attivazione delle credenziali di Livello 1, 2 e 3*.

8.2 Utilizzo spid minori

Dopo aver attivato l'identità digitale, il minore può utilizzarla per accedere ai servizi online pubblici e privati indirizzati ad utilizzo per i minori.

Nel caso di minori, l'accesso ai Service provider prevede la verifica da parte dell'IDP che l'identità del minore soddisfi i requisiti di età indicati dal Service Provider e sia richiesta o meno l'autorizzazione del genitore/tutore.

Se il requisito d'età è soddisfatto, nel caso in cui è necessario l'autorizzazione del genitore/tutore per l'accesso al servizio, viene inviata una notifica di autorizzazione al genitore/tutore se il minore accetta di proseguire. Il genitore/tutore ha 24 ore per poter accettare la richiesta.

Se il genitore/tutore non ha l'App MySielteID configurata, la notifica di autorizzazione all'accesso al servizio viene inviata tramite e-mail e deve essere gestita dall'area personale della propria identità digitale, nella sezione *Identità Minore*.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Se il genitore/tutore ha l'App MySielteID configurata, la notifica viene inviata all'app e può essere gestita direttamente dall'app stessa.

Per ogni richiesta di autorizzazione, il genitore/tutore può negarla o autorizzarla:

- Se la richiesta è negata, il minore riceve una e-mail con esito negativo e non gli sarà permesso di accedere al servizio.
- Se la richiesta è autorizzata, il minore riceve una e-mail con esito positivo e potrà accedere al servizio. L'autorizzazione prevede anche una durata, in giorni, entro la quale il minore potrà accedere allo specifico servizio senza richiedere ulteriori autorizzazioni.

Dopo aver verificato i requisiti precedentemente descritti ed in caso di autorizzazione concessa, se il Service Provider richiede un **accesso di livello 1** (codice fiscale e password), il minore può accedere al servizio.

Se il Service Provider richiede un **accesso di livello 2** (codice fiscale, password e codice OTP), il minore deve inserire un codice OTP ottenibile secondo una delle modalità indicate sotto:

- Ricezione notifica sull'app MySielteID *(se il minore ha configurato l'app)*
- Copia OTP dall'app MySielteID *(se il minore ha configurato l'app)*
- SMS *(opzione disponibile se il minore ha inserito il proprio numero cellulare)*
- E-mail *(se il minore non ha inserito il proprio cellulare)*

8.3 Gestione dell'identità digitale del minore

La gestione dell'identità del minore prevede operazioni disponibili sia per il minore, con delle limitazioni in base alla sua età, sia operazioni disponibili per il genitore/tutore in qualità di custode della identità stessa e secondo le indicazioni previste dalle Linee Guida AgID.

Le operazioni disponibili al genitore/tutore per la gestione dell'identità del minore possono essere svolte accedendo alla propria area personale sul sito https://www.sielteid.it entrando nella scheda *Identità Minore* dall'area personale, e sono di seguito descritte:

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- Sospendere l'identità del minore:

  il genitore/tutore può sospendere per un l'intervallo di tempo della sospensione.

- Riattivare l'identità del minore

  In seguito alla sospensione eseguita da parte del genitore/tutore o dal minore stesso, il genitore/tutore può riattivare l'identità sospesa.

- Revocare l'identità del minore:

  In seguito alla revoca dell'identità viene inviata una notifica via e-mail al genitore/tutore e minore.

Si precisa che la revoca dell'identità del minore può essere anche richiesta dal secondo tutore/genitore, inserito nella richiesta di rilascio di identità, inviando una richiesta di revoca tramite raccomandata o pec, includendo copia di un documento d'identità proprio e del minore, e documento che attesti la responsabilità genitoriale.

Il minore può gestire la propria identità accedendo alla sua area personale; le operazioni indicate di seguito sono disponibili a partire dal quattordicesimo anno:

- Visualizzare accessi spid
- Sospendere/attivare l'identità
- Revocare l'identità
- Acquistare SMS

8.4 Identità del genitore/tutore sospesa o revocata

L'identità del minore è connessa a quella del genitore/tutore, per cui la sospensione o revoca dell'identità di quest'ultimo comporterà delle azioni su quella del minore come descritto di seguito:

- In caso di sospensione dell'identità digitale del genitore/tutore:

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

il genitore/tutore non potrà più gestire l'identità del figlio dal suo profilo personale né autorizzare nuove richieste di accesso; le richieste di accesso precedentemente autorizzate ed ancora valide saranno sospese. Il minore può continuare ad utilizzare i soli servizi che **non** richiedono l'autorizzazione del genitore

- In caso di revoca dell'identità digitale del genitore/tutore:

  tutte le autorizzazioni all'accesso concesse al minore decadono; il minore può continuare ad utilizzare i soli servizi che **non** richiedono l'autorizzazione del genitore.

  In caso di richiesta di accesso con autorizzazione, il minore visualizza una pagina di errore che lo invita a verificare lo stato dell'identità del genitore/tutore.

  Se il minore non ha fornito un numero di cellulare proprio (facoltativo), la sua identità viene inoltre sospesa fino a quando non fornisce un numero di cellulare personale accedendo alla funzione "Cambia cellulare" presente all'interno del suo profilo.

8.5 Dissociazione dal genitore al compimento dei 18 anni

Come previsto dalle Linee Guida AgID, al compimento del diciottesimo anno di età del minore la sua identità deve essere svincolata da quella del genitore/tutore ed osservare le logiche operative di uno spid per maggiorenni.

Il giorno del compimento del diciottesimo compleanno l'identità del neomaggiorenne viene sospesa e viene inviata una e-mail di notifica di svincolo dell'identità da quella del genitore/tutore ed istruzioni per procedere con la riattivazione o revoca dell'identità. L'email contiene inoltre nuovi Codici Utente di sicurezza personali (codice di sospensione, codice di riattivazione e codice di revoca) che andranno conservati accuratamente perché serviranno per gestire operazioni di sicurezza.

Per riattivare l'identità il neomaggiorenne deve accedere al profilo personale, e riattivare la sua identità usando il codice di riattivazione ricevuto.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Prima della riattivazione, sarà validato il numero di cellulare usato dal minorenne e nel caso in cui **il minore non disponeva di un numero di cellulare** personale deve associare un proprio numero di cellulare e seguire la procedura di verifica del numero inserito.

Il neomaggiorenne deve prendere visione dell'informativa, delle condizioni generali di contratto, del manuale operativo, del manuale utente e della guida alla sicurezza dell'identità.

A questo punto, l'identità del neomaggiorenne viene attivata senza i precedenti limiti.

Se il neomaggiorenne non esegue nessuna azione l'identità rimane sospesa, ed in caso di inattività per un periodo superiore ai 24 mesi l'identità digitale è automaticamente revocata.

9 SERVIZI

9.1 Servizio Crediti SMS SielteID

Gli utenti che effettuano l'accesso ai servizi offerti dalla Pubblica Amministrazione tramite credenziali di Livello 2 devono inserire codice fiscale e password e approvare la richiesta di secondo livello scegliendo uno dei tre metodi sottoelencati:

- notifica dall'app MySielteID;
- inserimento di un codice OTP generato tramite App MySielteID;
- inserimento di un codice OTP inviato tramite SMS.

SielteID mette a disposizione il servizio *Crediti SMS* per gli accessi con Livello di sicurezza 2 con OTP via SMS.

Ogni utente che attiva la propria identità ha a disposizione un bonus gratuito di 7 SMS all'anno che verrà decrementato ad ogni accesso ai servizi che richiedono credenziali di Livello 2.

Il rinnovo annuale del bonus di 7 SMS avverrà ad un anno dalla data del precedente accredito bonus ed al primo accesso ai servizi.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

Finiti i 7 sms di bonus l'utente, qualora volesse mantenere gli accessi di Livello 2 tramite SMS, potrà in qualsiasi momento acquistare un pacchetto aggiuntivo di OTP via SMS tramite la pagina del proprio profilo personale o attendere il rinnovo annuale del bonus.

Gli utenti che hanno attivato le credenziali SPID prima dell'avvio del servizio *Crediti SMS* riceveranno il bonus di 7 SMS al momento del primo acquisto di un pacchetto di OTP via SMS.

L'utente può visionare e gestire il credito SMS tramite la pagina del proprio profilo personale.

L'Operatore IdP può effettuare le seguenti operazioni relativamente al credito dell'utente:

Figura 3- Operazioni Operatore IdP

- **Movimenti SMS**: l'Operatore IdP può visualizzare tutti i movimenti relativi ai crediti SMS dell'utente.
- **Cronologia Acquisti**: l'Operatore IdP può visualizzare gli acquisti effettuati mediante la piattaforma.
- **Operazione di Storno**: questa operazione permette all'Operatore IdP di ricaricare il credito dell'utente.

All'interno della scheda dell'utente, l'Operatore IdP può visualizzare la lista dei movimenti dei crediti SMS, lo storico di tutti gli acquisti e il credito residuo.

Relativamente ai movimenti dei crediti SMS, l'Operatore IdP può visualizzare le seguenti informazioni:

- **Data e ora del movimento**.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

- **Operazione:** può essere una ricarica credito, un consumo, uno storno da parte dell'operatore.
- **Quantità** di SMS utilizzati per il movimento.
- **Esito** dell'operazione.
- **Origine** del movimento: profilo, accesso con SPID, Servizio clienti (Back Office).

L'Operatore IdP può inoltre visualizzare tutti gli acquisti effettuati dall'utente e le informazioni sui singoli acquisti, quali:

- **Intestato a:** indica l'intestatario dell'acquisto, informazione inserita durante la conferma dei dati di fatturazione.
- **Pagamento:** indica il prezzo pagato per il servizio.
- **Acquisto:** indica il numero di crediti acquistati.
- **Data acquisto:** indica la data di acquisto dei crediti SMS.
- **Scadenza articolo:** indica la validità dell'articolo acquistato.
- **P. IVA:** qualora l'intestatario fosse una persona giuridica, viene inserita questa informazione.
- **Stato:** riporta lo status dell'acquisto, cioè "pagato" o "da pagare".
- **Ricevuta:** operazione che permette il download in formato PDF della fattura generata dalla piattaforma *Stripe.* La fattura viene generata dalla piattaforma *Stripe* dopo un pagamento.

In merito all'Operazione di Storno, l'Operatore IdP ha la possibilità di aggiungere/ricaricare credito all'utente nel caso sia necessario, provvedendo ad inserire il credito che va ricaricato e una nota obbligatoria come causale dello storno, prima di procedere con la Conferma.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

9.2 Servizio Priority Webcam

Il Richiedente può decidere, secondo le proprie esigenze, di identificarsi in maniera prioritaria e quindi ottenere lo SPID in modo più rapido rispetto alla modalità classica.

Per procedere in tal senso, il Richiedente dovrà effettuare una normale registrazione e scegliere il servizio priority nell'ambito della modalità di identificazione webcam.

L'operatore IdP, tramite l'operazione *Cronologia Acquisti* presente sull'anagrafica, potrà visualizzare:

- **Intestato a:** indica l'intestatario dell'acquisto, informazione inserita durante la conferma dei dati di fatturazione.
- **Prodotto Acquistato:** Webcam Prioritaria.
- **Data Acquisto:** che indica la data di acquisto della webcam.
- **Stato:** riporta lo status dell'acquisto, cioè "pagato" o "da pagare".
- **Ricevuta** riepilogativa di tutti i dati, scaricabile in formato PDF.
- **Pulsante relativo al rimborso** (vedi sottoparagrafo 7.7.1).

9.3 Richieste di rimborso per i servizi Webcam e Pacchetto SMS per SPID Livello 2

Il Cliente può attivare una richiesta di rimborso per i servizi webcam e pacchetto SMS per SPID secondo livello.

Si elencano i soli scenari in cui la richiesta di rimborso può essere accettata dall'Operatore IdP insieme al dettaglio della tempistica entro cui il Cliente può inviare una richiesta:

- Mancato appuntamento da parte dell'operatore, opzione selezionabile entro e non oltre le 24 ore successive alla data dell'appuntamento.
- Impossibilità ad effettuare il riconoscimento tramite webcam per motivi imputabili al Cliente stesso, come ad esempio mancata presentazione di valido documento di riconoscimento e/o videochiamata in presenza di soggetti terzi oltre al Cliente;

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

opzione selezionabile entro e non oltre le 48 ore successive alla data dell'appuntamento.

- Ripensamento, opzione selezionabile entro e non oltre le 24 ore successive alla data di acquisto.
- Malfunzionamento del sistema di registrazione e gestione degli appuntamenti di SielteID, opzione selezionabile entro e non oltre le 24 ore successive alla rilevazione del disservizio.

Per quest'ultimo caso si richiede inoltre di allegare al Modulo di Richiesta Rimborso evidenza del suddetto malfunzionamento, come mail di richiesta precedentemente inviata al Supporto SielteID per segnalare il malfunzionamento.

Il rimborso verrà eseguito utilizzando lo stesso metodo di pagamento a cui è ricorso il Cliente per l'acquisto del servizio.

Il Cliente può richiedere il rimborso del costo del servizio inviando, dalla casella con la quale si è registrato, un'e-mail avente per oggetto *Rimborso,* all'indirizzo spid@sielte.it con allegato il "Modulo di Richiesta Rimborso" debitamente compilato e sottoscritto in ogni sua parte.

Il "Modulo di Richiesta Rimborso" è disponibile nella sezione "Documentazione" del sito www.sielteid.it oppure è accessibile dal profilo personale dell'utente.

L'Operatore IdP, una volta ricevuta la richiesta, procede a verificare che quest'ultima rientri nelle politiche di rimborso previste; se così fosse procede ad eseguire rimborso.

Effettuato il rimborso, l'Operatore avverte l'utente del corretto espletamento della richiesta.

10 SICUREZZA DEL SERVIZIO

10.1 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

10.2 Tracciatura delle informazioni del servizio

Ai fini della tracciatura, ogni transazione di autenticazione viene 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.

10.2.1 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.

10.3 Procedura per la richiesta del log certificato

L'utente titolare di un'Identità Digitale ha facoltà di richiedere in qualunque momento una copia delle informazioni contenute nel log certificato relative alle proprie credenziali SPID.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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.

11 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;
- e-mail 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

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

dell'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.

12 CUSTOMER CARE

Sielte mette a disposizione dei propri utenti diversi canali di contatto. Per informazioni circa le modalità e i canali di assistenza, è possibile visitare la pagina web https://www.sielteid.it/contact.php.

12.1 Registrazione de visu (casi eccezionali)

Nell'ottica di poter venire incontro, ove possibile, a particolari necessità o condizioni dell'utente, il Richiedente può richiedere di identificarsi tramite modalità *de visu* presso le sedi del Gestore. L'utente è tenuto a contattare il Customer Care al numero soprariportato, esponendo la particolare casistica che richiederebbe un'identificazione di persona; successivamente alla richiesta, il Gestore effettua delle valutazioni di casistica e disponibilità, fornendo relativo feedback all'utente.

13 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 (D.Lgs. 196/03) e dal Regolamento UE 2016/679 noto come GDPR.

Le caratteristiche più importanti del sistema si riferiscono al personale dipendente che ha ricevuto la nomina ai sensi dell'art.30 del D.Lgs. 196/03 e ai sensi del Regolamento UE 2016/679 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 e dal Regolamento UE 2016/679, ai fini della registrazione sul sito e del

Le informazioni contenute all’interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

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 alla presa visione 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.

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.

14 ALLEGATO A

SPID – Tabella messaggi di anomalia V1.4

https://www.agid.gov.it/sites/default/files/repository_files/tabella-messaggi-spid-v1.4.pdf

USO PUBBLICO

Le informazioni contenute all'interno del presente documento, di proprietà di Sielte S.p.A., sono di dominio pubblico. Una volta che il documento viene divulgato al di fuori del contesto aziendale, Sielte S.p.A. non detiene più la responsabilità della riproduzione e del monitoraggio delle copie distribuite.