



lepida

LepidaID
Manuale operativo



lepida

1. Introduzione	4
1.1. Storia del documento	4
1.2. Scopo del documento	7
1.3. Acronimi e abbreviazioni	7
1.4. Riferimenti normativi	7
2. Dati identificativi del Gestore	9
3. Dati identificativi della versione del manuale	9
4. Responsabile del Manuale Operativo	9
5. Descrizione del servizio di Gestione delle Identità	10
5.1. Architetture applicative e di dispiegamento	10
5.2. Architetture dei sistemi di autenticazione e delle credenziali	12
5.3. Descrizione dei codici e dei formati dei messaggi di anomalia	14
5.4. Livelli di servizio	14
5.5. Tracciature	16
5.5.1. Tracciature accessi	16
5.5.2. Registro delle transazioni	17
5.5.3. Modalità di accesso ai log	18
5.6. Servizi aggiuntivi	19
6. Guida utente	19
7. Processi e procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali SPID	19
7.1. Richiesta dell'Identità Digitale ad uso privato	19
7.2. Identificazione del soggetto richiedente	22
7.3. Esame e verifica del richiedente	25
7.4. Emissione e creazione delle credenziali	26
7.5. Richiesta dell'Identità Digitale ad uso professionale per persona fisica e per persona giuridica	27
8. Revoca o sospensione o riattivazione dell'Identità Digitale	28
9. Gestione dei rapporti con gli utenti	31
10. Descrizione generale delle misure anti-contraffazione	32
10.1. Livello 1 SPID	32
10.2. Livello 2 SPID	33
11. Descrizione generale del sistema di monitoraggio	34
12. Obblighi del Gestore e dei Titolari dell'Identità Digitale	34



12.1. Obblighi del Gestore dell'Identità Digitale	34
12.2. Obblighi del Titolare dell'Identità Digitale	38
12.3. Responsabilità	39
13. Documentazione	39
14. Cessazione IdP	39
15. Appendice A - Codici e Messaggi di anomalia	40



1. Introduzione

1.1. Storia del documento

VERSIONE	DATA	CAMBIAMENTI APPORTATI
1.0	30/11/2017	Prima stesura
1.1	19/02/2018	Seconda stesura
1.2	23/03/2018	<ul style="list-style-type: none"> • Aggiornamento paragrafo 9: "Gestione dei rapporti con utenti" • Aggiornamento paragrafo 8 "Revoca e Sospensione dell'Identità Digitale" • Inserimento della modalità di "Identificazione a vista del soggetto richiedente" e di "Identificazione a vista da remoto" in una fase successiva all'avvio del servizio • Aggiornamento paragrafo 5.5 "Tracce"
1.3	15/05/2018	<ul style="list-style-type: none"> • Aggiornamento paragrafo 4 "Responsabile del Manuale Operativo": Esplicitata la responsabilità del Manuale Operativo. • Aggiornamento paragrafo 7.1 "Richiesta dell'identità digitale" : Inserimento della PEC come attributo opzionale ed esplicita evidenza della conservazione della scansione del documento d'identità e della tessera sanitari. • Aggiornamento paragrafo 8 "Revoca e sospensione della identità digitale" : Aggiunta del canale alternativo in caso di indisponibilità dei canali di comunicazione previsti. • Aggiornamento paragrafo 5.1.3 "Modalità di accesso ai log" • Aggiornamento paragrafo 5.4 "Livelli di servizio"
1.4	15/06/2018	<ul style="list-style-type: none"> • Aggiornamento paragrafo 10.2 "Livello 2 SPID" • Aggiornamento paragrafo 7.3 "Esame e verifica del richiedente": precisate le motivazioni di una mancata concessione di una identità digitale • Aggiornamento paragrafo 7.2: "Identificazione del soggetto richiedente": precisate la non necessità della presenza fisica del richiedente l'identità digitale
1.5	11/07/2018	<ul style="list-style-type: none"> • Aggiornato paragrafo 7.1 "Richiesta dell'Identità Digitale": eliminazione della generazione dell'OTP via Google Auth • Aggiornato paragrafo 10.2 "Livello 2 SPID": eliminazione della generazione dell'OTP via Google Auth • Aggiornato nome Responsabile Manuale Operativo



1.6	11/10/2019	<ul style="list-style-type: none"> • Aggiornamento paragrafo 8 "Revoca e sospensione della identità digitale" : Aggiunta della possibilità di porre una firma autografa al modulo di revoca • Aggiornamento paragrafo 7 "Processi e procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali" : Aggiunta della modalità di registrazione "assistita" e della possibilità di utilizzare la APP LepidaID per l'autenticazione a due fattori • Aggiornato paragrafo 10.2 "Livello 2 SPID": aggiunta della generazione dell'OTP via app LepidaID
1.7	23/12/2019	<ul style="list-style-type: none"> • Aggiornamento paragrafo 7.1 "Richiesta dell'identità digitale": eliminati riferimenti alla domanda e risposta segreta per recuperare la password • Aggiornato paragrafo 7.4 "Emissione e creazione delle credenziali": precisata la lunghezza massima della password • Aggiornato paragrafo 10.1 "Livello 1 SPID": precisata la lunghezza massima della password
1.8	16/03/2020	<ul style="list-style-type: none"> • Aggiornato paragrafo 7.2 "Identificazione del soggetto richiedente": viene resa disponibile la modalità di riconoscimento a vista da remoto
1.9	10/10/2020	<ul style="list-style-type: none"> • Aggiornato paragrafi 7.1 "Richiesta dell'identità digitale" e 7.2 "Identificazione del soggetto richiedente": vengono introdotte le nuove modalità di identificazione con registrazione audio/video e bonifico e con CIE 3.0. • Introdotta la gestione dell' 'attributo del domicilio fisico • Aggiornato il capitolo 9 "Gestione rapporti con gli utenti" • Aggiornata la possibilità di utilizzare il tesserino del codice fiscale al posto del tesserino della tessera sanitaria • Aggiornamenti minori
2.0	27/04/2021	<ul style="list-style-type: none"> • Aggiornato nome Responsabile Manuale Operativo • Aggiunto come "Servizio Aggiuntivo" il servizio di Firma con SPID: inserito paragrafo 5.6 • Aggiunta l'autenticazione di livello 2 con QR Code: aggiornamento del paragrafo 7.1 e inserito paragrafo 10.2
2.1	08/06/2021	<ul style="list-style-type: none"> • Aggiornato il paragrafo 5.5.3 Modalità di accesso ai log, con precisazioni relative reperire il modulo da utilizzare • Aggiornato il paragrafo 7.4 e il paragrafo 10.2 con la descrizione del PIN impostato dall'utente sulla APP LepidaID
2.2	24/06/2021	<ul style="list-style-type: none"> • Aggiornato il paragrafo 7.4 e il paragrafo 10.2 con la descrizione del PIN impostato dall'utente sulla APP LepidaID



2.3	05/10/2021	<ul style="list-style-type: none"> Aggiornato il paragrafo 7.4 e il paragrafo 10.2 con l'indicazione che il PIN impostato dall'utente sulla APP LepidaID può essere alfanumerico o numerico
2.4	29/11/2021	<ul style="list-style-type: none"> Aggiornato il paragrafo 7.1 e il paragrafo 10.2 con l'autenticazione di livello 2 mediante notifiche push
2.5	30/12/2021	<ul style="list-style-type: none"> Introdotta l'identità digitale ad uso professionale per persona fisica e giuridica (paragrafo 7.5). Aggiornato il capitolo 4 con il nuovo numero di assistenza telefonica. Aggiornato il capitolo 8 con il link alla pagina di assistenza
2.6	23/08/2022	<ul style="list-style-type: none"> Aggiornato logo Lepida ScpA, stile e impaginato Aggiornato paragrafo 3 con riferimenti normative attuali Aggiornato paragrafo 9 con il link dell'assistenza Aggiornata immagine paragrafo 9 Corretti refusi e adeguate maiuscole/minuscole
2.7	07/12/2022	<ul style="list-style-type: none"> Aggiornati i riferimenti normativi (inserite LLGG SPID minori)i Introdotta il protocollo OpenID Connect (aggiornati paragrafi 5.1, 5.2, 5.5.2, 11.1) Introdotta la possibilità di rilascio delle identità digitali LepidaID ai cittadini della Repubblica di San Marino (aggiornati paragrafi 7.2, 7.3) Introdotta la possibilità di rilascio delle identità digitali LepidaID ai minori (inserito capitolo 8 e aggiornato capitolo 9) Aggiornato paragrafo 5.1 a seguito dell'introduzione del nuovo sito informativo di LepidaID;
2.8	06/06/2023	<ul style="list-style-type: none"> Aggiornamento responsabili manuale operativo Aggiornamento policy password con rimozione della lunghezza massima
2.9	25/10/2023	<ul style="list-style-type: none"> Aggiornato paragrafo 5.5.3 con aggiunta della modalità di accesso civico. Aggiornato paragrafo 7.2 con aggiunta della necessaria accettazione del modulo di adesione e della documentazione informativa nella fase di identificazione Aggiornato paragrafo 7.3 con aggiunta dei controlli con Scipafi Aggiornato paragrafo 9 con aggiunta della revoca della identità in caso di perdita dell'accesso a mail o cellulare e aggiunta dell'obbligo di ricezione della richiesta di revoca/sospensione e riattivazione via PEC a partire solo dalla PEC associata al titolare di identità;

		<ul style="list-style-type: none"> Aggiornato capitolo 11, con aggiunta l'indicazione che gli attributi secondari sono modificabili solo dal soggetto titolare di identità;
3.0	27/03/2025	<ul style="list-style-type: none"> Aggiornato logo Aggiornato cap. 7 e sottoparagrafi Inserite precisazioni e sistemati refusi Aggiornato logo e precisazioni derivanti dall'introduzione dei controlli sul documento del codice fiscale previsti dall'Avviso 7v2 di AgID
3.1	19/12/2025	<ul style="list-style-type: none"> Eliminato cap. 8 e relativi sottoparagrafi Aggiornati capp. 1.4, 2, 4, 5.1, 5.2, 5.4, 5.5.1, 5.5.2, 5.5.3, 7.1, 7.2, 7.3, 7.4, 7.5, 9, 11, 11.2, 13.1

Versione	Redatto	Verificato	Approvato
3.1	Dipartimento Software e Piattaforme	Direttori Dipartimento Software e Piattaforme	Direttori Dipartimento Software e Piattaforme

1.2. Scopo del documento

Il presente manuale illustra l'architettura, le modalità, le procedure adottate dal Gestore Lepida ScpA, di seguito Lepida, per l'erogazione del servizio di Gestione di Identità SPID, come indicato nel DPCM 24 ottobre 2014.

1.3. Acronimi e abbreviazioni

- **AgID** – Agenzia per l'Italia Digitale
- **SPID** – Sistema Pubblico per la gestione dell'Identità Digitale
- **IdM** – Identity Manager
- **IdP** – Identity Provider
- **SP** – Service Provider

1.4. Riferimenti normativi



DLgs 82/2005	Codice dell'amministrazione digitale
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 adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese https://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/dpcm_24_ottobre_2014a.pdf
Dlgs 30 giugno 2003 n.196	Codice in materia di protezione dei dati personali http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1311248
Modalità attuative SPID (art.4, DPCM 24 ottobre 2014)	Regolamento recante le modalità attuative per la realizzazione dello SPID https://www.agid.gov.it/sites/default/files/repository_files/regolamento_modalita_attuative_spid_2.0.pdf
Regole tecniche (art.4, comma 2 DPCM 24 ottobre 2014)	Regolamento recante le regole tecniche https://docs.italia.it/italia/spid/spid-regole-tecniche/it/stabile/index.html
Accreditamento Gestori (art.1, comma 1, lettera I DPCM 24 ottobre 2014)	Regolamento recante le modalità per l'accreditamento e la vigilanza dei Gestori dell'identità digitale https://www.agid.gov.it/sites/default/files/repository_files/regolamento_accreditamento_idp-spip_2.0.pdf
Approvazione di AgID del 26/09/2019 degli aggiornamenti sulle procedure utilizzate per la verifica dell'identità degli utenti, per il rilascio delle credenziali e documentazione sulla nuova applicazione mobile della società Lepida S.p.A., accreditata in qualità di gestione dell'identità digitale SPID (articolo 1, comma 1, lettera I), DPCM 24 ottobre 2014).	
Linee Guida per il rilascio dell'identità digitale per uso professionale	https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_identita_digitale_per_uso_professionale_v.1.0_0.pdf



2. Dati identificativi del Gestore

Denominazione sociale	Lepida ScpA
indirizzo della sede legale	Via della Liberazione, 15 - 40128 Bologna (BO)
Legale Rappresentante	Davide Conte
N° iscrizione al Registro delle imprese	N° REA: 466017
N° Partita IVA	02770891204
E-mail PEC	segreteria@pec.lepida.it
Sito web generale (informativo ITA/ENG)	https://www.lepida.net
Sito web dedicato al servizio IDP Lepida ScpA	https://id.lepida.it

3. Dati identificativi della versione del manuale

Il presente Manuale Operativo è pubblicato ed è consultabile sul sito web del Gestore Lepida a questo indirizzo: <https://id.lepida.it>.

Per versione aggiornata del presente documento si intende unicamente quella consultabile e scaricabile dal sito web dedicato del Gestore delle Identità Digitali Lepida <https://id.lepida.it> e sul sito web di AgiD.

4. Responsabile del Manuale Operativo

Il Responsabile del Manuale Operativo cura gli aggiornamenti e la pubblicazione del presente documento.

Eventuali comunicazioni e suggerimenti possono essere inviati all'attenzione dei Responsabili del Manuale Operativo:

Lorenzo Fabricatore, Giuseppe Sberlati
 Indirizzo: Via della Liberazione, 15 - 40128 Bologna (BO)
 Centralino e Segreteria: +39 051 63388 00
 Fax: +39 051 4208511



Numero Verde: **800 77 90 77**

Indirizzo PEC: segreteria@pec.lepida.it

Sito web: <https://id.lepida.it>

5. Descrizione del servizio di Gestione delle Identità

5.1. Architetture applicative e di dispiegamento

L'architettura applicativa del Gestore di Identità SPID Lepida è composta dai seguenti principali componenti, denominati come segue:

- Landing page: sito informativo del servizio LepidaID;
- Identity Manager (IdM): componente applicativo che si occupa del processo di identificazione dell'utente, generazione delle credenziali, gestione del ciclo di vita delle utenze, gestione delle sedi operative e dei relativi operatori.
- Identity Provider (IdP): componente che si occupa del processo di autenticazione utilizzando il protocollo SAML v2.0: riceve le richieste di autenticazione dai Service Provider integrati, permette l'immissione delle credenziali dell'utente, la verifica, e ad autenticazione avvenuta invia l'asserzione al Service Provider, comunicando l'esito dell'autenticazione e gli attributi dell'utente.

I due componenti (IdM e IdP), per quanto distinti sia nell'architettura sia dal punto di vista funzionale, presentano come unico punto in comune la condivisione della stessa base dati contenente le identità degli utenti interessati. La landing page, ovvero il sito informativo del servizio LepidaID, ha invece un'architettura e una base dati distinta dagli altri due componenti.

Di seguito i diagrammi logici dei componenti del servizio di Gestione di Identità Lepida e del flusso di gestione delle Identità Digitali.

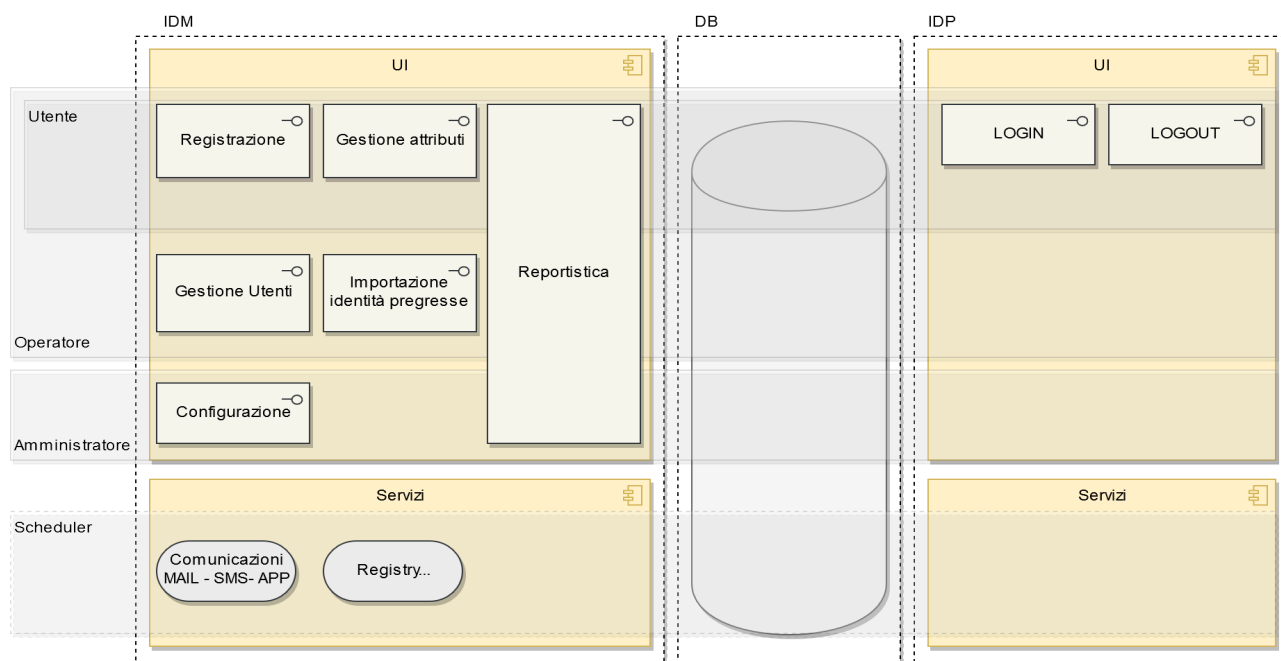
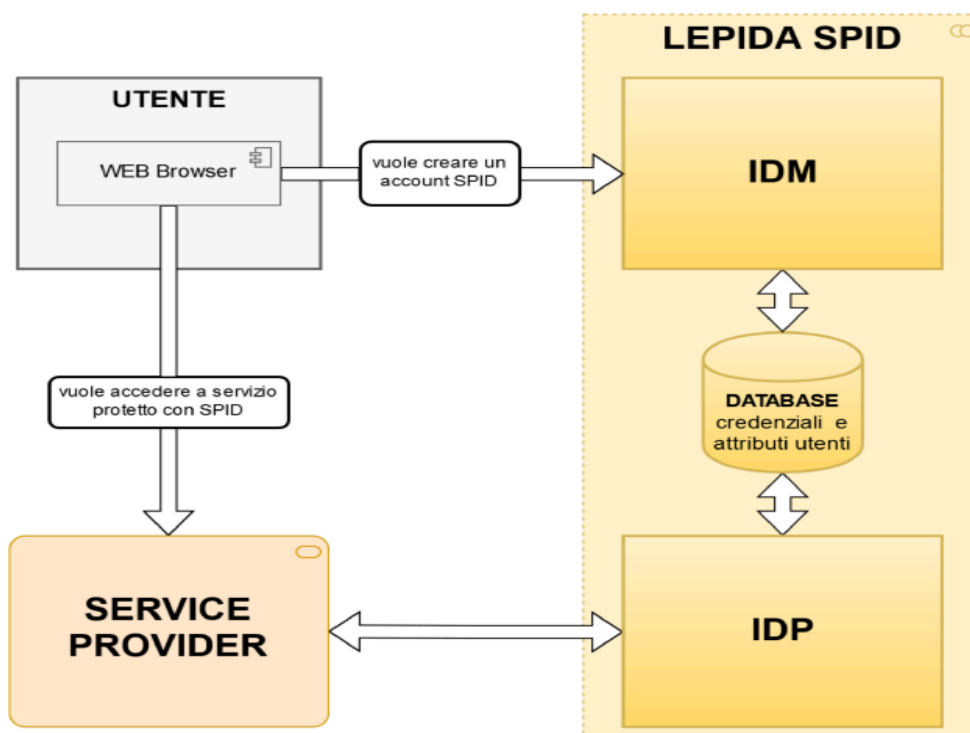


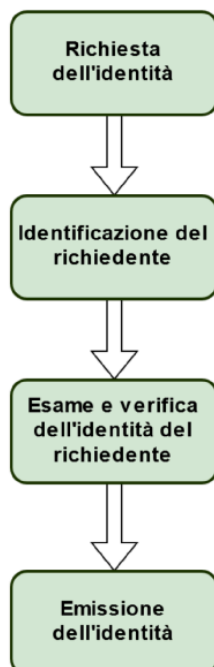
Diagramma logico del Gestore di Identità Lepida



Flusso di gestione Identità Digitale



Il seguente diagramma presenta i singoli passaggi per il rilascio di una Identità Digitale, gestito interamente dalla componente IdM. Al termine di questi passaggi, l'Identità risulta rilasciata ed è possibile avviare la fase di autenticazione gestita dall'IdP.



Flusso di rilascio Identità Digitale gestita dalla componente IdM

Per la descrizione dell'architettura di dispiegamento, si rimanda al manuale di sicurezza del Gestore di Identità Lepida.

5.2. Architetture dei sistemi di autenticazione e delle credenziali

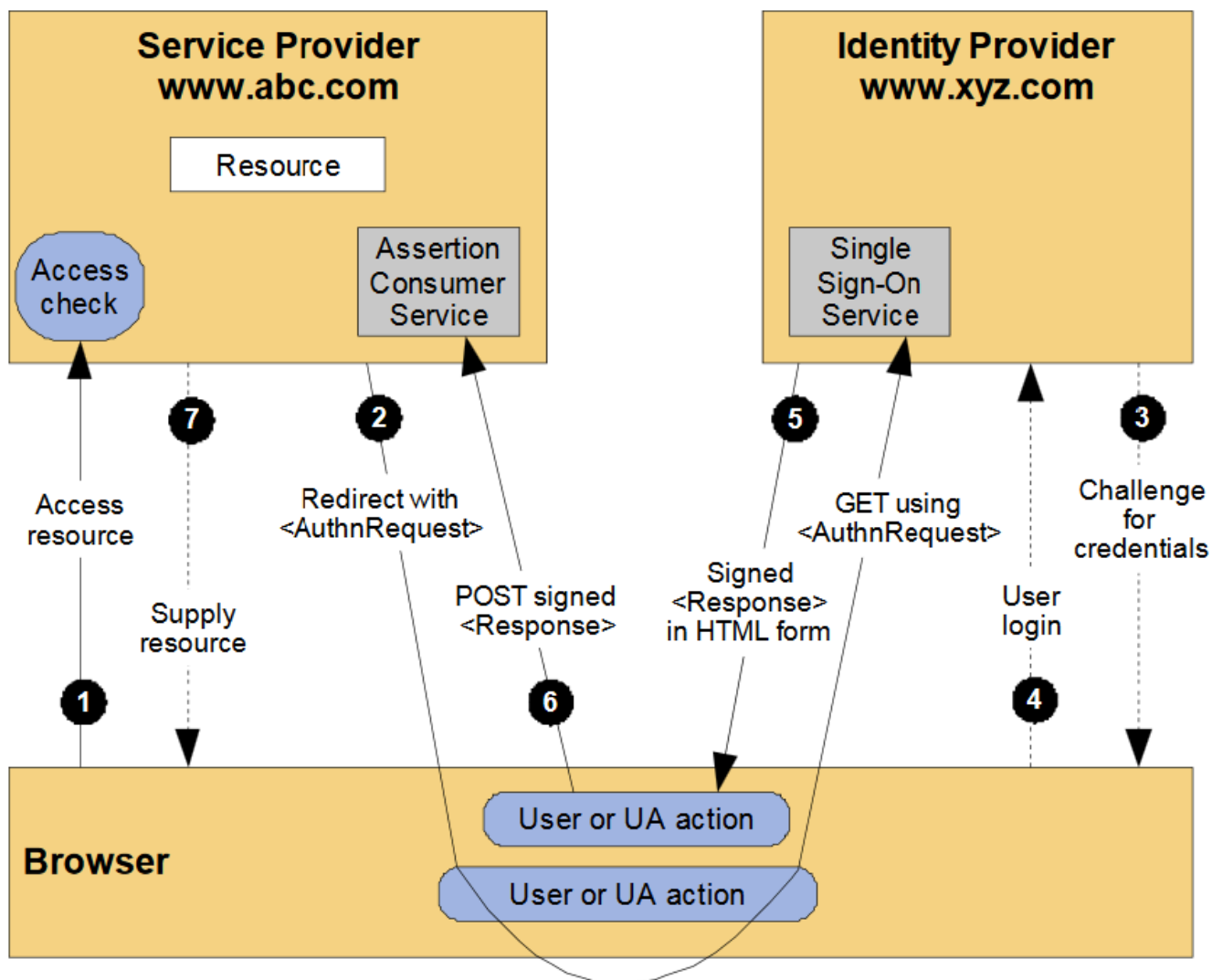
Il sistema di autenticazione del Gestore di Identità SPID prevede meccanismi di autenticazione dell'identità secondo i livelli di sicurezza SPID 1 e 2 come descritto nei paragrafi successivi.

Il processo di autenticazione prevede i seguenti soggetti che concorrono al servizio di autenticazione informatica:

- Utente, titolare della Identità Digitale, che richiede l'accesso al servizio online
- Fornitore del servizio
- Gestore di Identità.



Nel caso del protocollo SAML, il flusso di autenticazione è rappresentato dallo schema seguente:



Flusso di autenticazione con SAML 2.0

I passaggi previsti sono:

1. L'utente chiede l'accesso ad un servizio online collegandosi telematicamente al portale del fornitore del servizio
2. Il fornitore del servizio chiede allo stesso utente di individuare il Gestore di Identità presso il quale ha ottenuto l'Identità Digitale da un elenco riportante tutti i Gestori aderenti a SPID
3. Il fornitore del servizio indirizza il soggetto titolare dell'Identità Digitale, scelto dall'utente, richiedendo l'autenticazione con il livello SPID maggiore di quello minimo definito dal servizio



4. Il Gestore di Identità verifica l'identità del soggetto sulla base delle credenziali fornite dallo stesso. Se tale verifica ha esito positivo, il Gestore di Identità emette una asserzione di autenticazione SAML attestante gli attributi eventualmente richiesti
5. Il titolare dell'Identità Digitale viene quindi re-indirizzato, portando con sé l'asserzione prodotta, verso il fornitore dei servizi
6. Il fornitore di servizi verifica le policy di accesso al servizio richiesto e decide se accettare o meno la richiesta.

5.3. Descrizione dei codici e dei formati dei messaggi di anomalia

Come indicato dalla normativa fornita da AgID, il Gestore di Identità Lepida adotta i messaggi di anomalia, a seguito di errori in fase di autenticazione da parte dell'utente, riportati nell'Appendice A - Codici e Messaggi di anomalia del presente documento.

5.4. Livelli di servizio

Il Gestore garantisce la continuità operativa dei servizi di sua competenza afferenti allo SPID, conformemente agli indicatori di qualità e livelli di servizio allegati alla convenzione per l'adesione a SPID.

Nella tabella seguente sono elencati gli indicatori di qualità (Service Level Agreement) previsti per il Gestore di identità Lepida.

ID	Indicatore di qualità	Modalità di funzionamento	Valore limite
IQ-01	Disponibilità del sottoservizio di registrazione identità	Erogazione automatica	≥ 99,5%
			Singolo evento di indisponibilità ≤ 6 ore
		Erogazione presenza in	≥ 98,0%
IQ-02	Tempo di risposta del sottoservizio di registrazione identità		≤ 12h (ore lavorative) per il 95% di richieste registrazione utente
IQ-03	Disponibilità del sottoservizio di gestione rilascio credenziali	Erogazione automatica	≥ 99,5%
			Singolo evento di indisponibilità ≤ 6 ore



ID	Indicatore di qualità	Modalità di funzionamento	Valore limite
		Erogazione in presenza	≥ 98,0%
IQ-04	Tempo di rilascio credenziali	Erogazione da remoto	≤ 5 giorni lavorativi
		Erogazione in presenza	≤ 3 giorni lavorativi
IQ-05	Tempo riattivazione delle credenziali		≤ 2 giorni lavorativi
IQ-06	Disponibilità del sottoservizio di sospensione revoca delle credenziali		≥ 99,5%
			Singolo evento di indisponibilità ≤ 6 ore
IQ-07	Tempo di sospensione delle credenziali	Erogazione automatica	≤ 1 minuto
		Erogazione in presenza	≤ 10 minuti
IQ-08	Tempo di revoca delle credenziali successiva alla sospensione		≤ 5 giorni lavorativi
IQ-09	Disponibilità del sottoservizio di rinnovo e sostituzione delle credenziali	Erogazione automatica	≥ 99,5%
			Singolo evento di indisponibilità ≤ 6 ore
		Erogazione in presenza	≥ 98,0%
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		≤ 2 giorni lavorativi
IQ-10-bis ¹	Tempo di dispiegamento/aggiornamento metadata		≤ 2 giorno lavorativi
IQ-11	Disponibilità del sottoservizio di autenticazione		≥ 99,5%
			Singolo evento di indisponibilità ≤ 6 ore
			Coefficiente moltiplicativo = 300 300: tot. eID nazionale = x : tot. eID gestore



ID	Indicatore di qualità	Modalità di funzionamento	Valore limite
IQ-12	Tempo di risposta del sottoservizio di autenticazione		$300 \times \text{tot. eID gestore}$ $x =$ $\text{tot. eID nazionali}$ $x =$ numero effettivo di richieste di autenticazioni al secondo (auth sec) correlate alle identità rilasciate dal gestore. Se $x < 100$, il gestore deve garantire almeno 100 auth sec. Tempi di risposta ≤ 2 sec per il 98% delle richieste di autenticazione Per un numero di richieste di auth sec superiore al coefficiente moltiplicativo, lo SLA andrà concordato in anticipo tra AgID e gestori.
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
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

5.5. Tracciatore

5.5.1. Tracciatore accessi

Le tipologie di eventi tracciati sono:

- Richiesta, attivazione e gestione identità
- Autenticazioni
- Ciclo di vita dell'identità
- Operazione degli operatori



- Operazioni degli amministratori
- Operazioni dello scheduler.

Per tutte le tipologie di eventi vengono indicati i riferimenti temporali e, in aggiunta:

- Per gli eventi di autenticazione vengono inoltre indicati il SP e il livello SPID utilizzato
- Per gli eventi di variazione dati vengono indicati se effettuati da operatore o dall'utente stesso.

Qualora la modifica sia stata effettuata da un operatore, oltre all'identificativo dell'operatore stesso viene inserito il link all'eventuale documentazione giustificativa dell'intervento eventualmente caricata:

- Per quanto riguarda le variazioni di stato (sospensione, revoca, ecc.) viene indicato l'eventuale operatore autore della transizione e il link all'eventuale documentazione giustificativa
- Per gli eventi di validazione viene indicato il riferimento a tipologia e valore del contatto validato
- Per gli eventi generati dallo scheduler viene indicata la tipologia di evento verificatosi e l'eventuale azione intrapresa (es: evento di scadenza documento con azione di segnalazione all'utente tramite email).

I record di log vengono salvati su database e sono consultabili per almeno 24 mesi secondo le modalità descritte nelle modalità attuative SPID.

5.5.2. Registro delle transazioni

Ai fini della tracciatura il Gestore di Identità Lepida mantiene un Registro delle transazioni contenente i tracciati delle richieste di autenticazione con protocollo SAML 2.0 servite negli ultimi 24 mesi.

Per ogni singola transazione vengono memorizzate in particolare le seguenti informazioni:

- Timestamp: Timestamp di ricezione della richiesta da parte del SP
- IpAddress: Indirizzo ip dell'utente
- AuthnRequest: Authentication request arrivata dal SP, codificata in formato base64 e compressa con algoritmo deflate
- AuthnRequestID: Attributo "ID" contenuto nell'authentication request arrivata dal SP
- AuthnRequestIssuer: Tag "Issuer" presente nell'authentication request arrivata dal SP



- AuthnRequestIssueInstant: Attributo "IssueInstant" presente nell'authentication request originale arrivata dal SP
- AuthnRequestBinding: Binding HTTP utilizzato dal SP per inviare l'authentication request, valorizzata con "HTTP-REDIRECT" o con "HTTP-POST"
- Response: Response generata dall'IdP, codificata in formato base64 e compressa con algoritmo deflate
- ResponseID: Attributo "ID" presente nella response generata dall'IdP
- ResponseIssueInstant: Attributo "IssueInstant" presente nella response generata dall'IdP
- SpidCode: Attributo utente "spidCode"
- AssertionID: Attributo "ID" del tag "Assertion" presente nella response generata dall'IdP
- AssertionSubjectNameID: Tag "NameID", sottonodo del tag "Subject" (a sua volta sottonodo del tag "Assertion") presente nella response generata dall'IdP.

Il registro viene mantenuto su file csv e aggiornato in tempo reale contestualmente alle attività degli utenti sul sistema. Il contenuto del file risulta protetto dagli accessi non autorizzati mediante opportune politiche di offuscamento. Il file di registro, come da normativa, contiene i log delle attività degli ultimi 24 mesi. Uno specifico job si occupa di eliminare dal file i contenuti via via divenuti obsoleti.

5.5.3. Modalità di accesso ai log

I soggetti aventi diritto possono richiedere di ricevere le informazioni inerenti le transazioni, inviando un apposito modulo di richiesta compilato e sottoscritto, corredato di copia fronte/retro del documento di identità, da inviare al Gestore di Identità Lepida tramite PEC all'indirizzo segreteria@pec.lepida.it. Il modulo per l'esercizio di diritti in materia di protezione dei dati personali è presente sul sito di Lepida nella sezione relativa alla ["Protezione delle persone fisiche con riguardo al trattamento dei dati personali"](#).

Il Gestore di Identità effettua le verifiche della correttezza della richiesta e recupera le informazioni dal registro mediante l'accesso al sistema presso il quale si reperiscono i log. In particolare, recupera le evidenze, raggruppando le informazioni per il periodo temporale, formatta il documento di presentazione delle stesse e trasmette il documento all'interessato. Le regole e procedure adottate al fine di fornire riscontro, nei tempi e nei modi previsti dalla legge, ai soggetti che esercitano i diritti di cui agli artt. 15-23 del Regolamento UE n. 2016/679 sono indicate nel documento "Disciplinare riguardante l'esercizio dei diritti dell'interessato" presente sul sito di Lepida nella sezione relativa alla ["Protezione delle persone fisiche con riguardo al trattamento dei dati personali"](#).



L'utente, titolare della Identità Digitale, ha a disposizione una sezione specifica nel proprio profilo utente per la visualizzazione delle proprie autenticazioni. L'accesso avviene con LIV 2 SPID.

Si precisa che AgID può richiedere l'accesso ai log direttamente a Lepida.

5.6. Servizi aggiuntivi

Lepida offre il servizio di sottoscrizione elettronica di documenti attraverso l'utilizzo dell'Identità Digitale SPID LepidaID ai sensi dell'art. 20 del CAD, la cosiddetta "Firma con SPID". Il processo attuato è stato realizzato sulla base delle linee guida [Regole Tecniche per la sottoscrizione elettronica di documenti](#).

6. Guida utente

Per la Guida Utente si fa riferimento al relativo documento denominato "LepidaID - Guida Utente".

7. Processi e procedure utilizzate per la verifica dell'identità degli utenti e per il rilascio delle credenziali SPID

Lepida è un Gestore di Identità Digitali SPID (LepidaID) che fornisce e gestisce:

- Identità digitale della persona fisica (veicola solo i dati della persona fisica) - di seguito identità digitale ad uso privato
- Identità digitale ad uso professionale della persona fisica (veicola solo i dati della persona fisica)
- Identità digitale ad uso professionale per la persona giuridica (veicola solo i dati della persona fisica e della persona giuridica).

In tutti i casi le identità sono fornite a utenti maggiorenni.

7.1. Richiesta dell'Identità Digitale ad uso privato

Lepida prevede che la richiesta di adesione avvenga soltanto in formato digitale tramite modalità informatiche. Tuttavia è possibile effettuare la richiesta di adesione in modalità assistita, ossia con il supporto di un operatore, presso gli sportelli LepidaID abilitati a tale servizio.

Il servizio LepidaID, per le sole persone fisiche, prevede il seguente set di informazioni:



- Email
- Password
- Cognome e nome
- Sesso
- Data di nascita
- Nazione di nascita
- Provincia di nascita
- Luogo di nascita
- Codice fiscale
- Estremi di un valido documento di identità
- Domicilio fisico
- Telefono cellulare
- PEC (opzionale).

Nel caso di **richiesta di adesione online** da parte del soggetto richiedente, all'indirizzo <https://id.lepida.it/>, la procedura prevede i seguenti passi:

- Identificazione del soggetto richiedente
- Verifica dei dati e dell'identità dichiarata
- Attivazione dell'Identità Digitale.

Nel caso di **richiesta di adesione in modalità assistita** (disponibile solo per le Identità Digitali ad uso privato), ossia con il supporto di un operatore, presso gli sportelli LepidaID abilitati a tale servizio la procedura prevede, attraverso apposita funzione del sistema, i seguenti passi:

- l'identificazione a vista del cittadino (soggetto richiedente)
- il supporto all'inserimento, sul sistema id.lepida.it, della richiesta
- la verifica dei dati inseriti e la successiva attivazione dell'Identità Digitale.

La **richiesta di adesione (registrazione)** online consiste nell'inserimento da parte del cittadino delle informazioni necessarie per richiedere una Identità Digitale SPID. Tale processo consiste in più step: il primo passo è rappresentato dall'inserimento dei dati accesso, il secondo dall'inserimento della propria anagrafica e del domicilio fisico, il terzo dall'inserimento degli estremi del documento d'identità, del documento del codice fiscale e dal caricamento di una scansione fronte/retro del documento di identità e del documento del codice fiscale (tessera sanitaria o equipollenti, previsti dalla normativa AgID), il quarto rappresenta una sezione nella quale l'utente valida i propri contatti elettronici (email, cellulare ed eventualmente PEC), terminando con l'ultimo step durante il quale l'utente seleziona la modalità di riconoscimento.



La **richiesta di adesione in modalità assistita** consiste nel supporto al soggetto richiedente da parte di un operatore di sportello abilitato nella registrazione che svolge al tempo stesso l'identificazione a vista del soggetto richiedente. Nello specifico:

- Il cittadino si reca in uno sportello LepidaID abilitato alla funzione di "supporto alla registrazione" oltre a quella di base di "identificazione/attivazione"
- Il cittadino viene riconosciuto de visu da un Operatore di sportello esibendo un documento di identità e il documento del codice fiscale (tessera sanitaria o equipollenti, previsti dalla normativa AgID), in corso di validità
- Il cittadino viene supportato dall'operatore di sportello nella compilazione dei dati e validazione del numero cellulare (inclusa la scansione dei documenti e relativo caricamento nel sistema)
- L'operatore di sportello effettua le verifiche previste dalle procedure LepidaID sui documenti.

Al termine di entrambe le modalità di richiesta, LepidaID invia una mail al titolare di identità per completare, durante la fase di riconoscimento, le ultime azioni a proprio carico:

- accesso attraverso autenticazione con username e password ad un link personalizzato univoco e associato alla identità per effettuare la verifica della mail;
- validazione del cellulare comunicato in fase di registrazione;
- presa visione e accettazione del modulo di adesione, informativa della privacy, documento di informativa sui rischi derivanti dal possesso dell'identità SPID e le condizioni di utilizzo del servizio.

Il completamento della registrazione da parte del cittadino deve avvenire entro 15 minuti dal termine delle attività di verifica svolte dall'operatore.

Solo a seguito di tutte le azioni sopra indicate, l'identità sarà attiva e utilizzabile per l'accesso ai servizi della federazione SPID.

Lepida prevede la gestione di due livelli di autenticazioni: Livello 1 SPID e Livello 2 SPID.

Per il livello 1 SPID (corrispondente al LoA2 dell'ISO-IEC 29115) sono accettabili credenziali composte da un singolo fattore (ad es. password), mentre per il livello 2 SPID (corrispondente al LoA3 dell'ISO-IEC 29115), il Gestore di Identità Digitali rende disponibili sistemi di autenticazione informatica a due fattori, non necessariamente basati su certificati digitali.

Per il livello 2 SPID, l'autenticazione a due fattori, il Gestore di Identità Lepida prevede cinque modalità:



- Username/password e codice OTP, generato da LepidaID e inviato via SMS al numero di telefono cellulare associato all'identità digitale dell'utente e verificato in fase di registrazione
- Username/password, codice OTP generato tramite APP LepidaID e PIN o riconoscimento biometrico
- Lettura, tramite APP LepidaID del QR Code visualizzato sulla pagina web di login e PIN o riconoscimento biometrico
- Ricezione di una notifica push tramite APP LepidaID e PIN o riconoscimento biometrico
- Inserimento di un codice OTP generato da LepidaID e inviato tramite e-mail all'indirizzo associato all'identità digitale dell'utente (opzione riservata esclusivamente alle identità digitali ad uso professionale per la persona giuridica).

Durante la registrazione l'utente non può scegliere il proprio nome utente che si assume essere coincidente con l'indirizzo email (il sistema ne verifica l'unicità al termine della digitazione impedendo il proseguimento in caso di nome utente/email già presenti nel sistema) ma deve inserire la propria password. La password digitata deve rispettare un set di vincoli al fine di evitare formati facilmente individuabili da terzi.

Al termine della procedura di registrazione sarà subito possibile effettuare accesso alla propria area riservata utilizzando le credenziali di LIV2 SPID, anche se l'identificazione e il conseguente rilascio dell'identità non sono ancora avvenuti.

7.2. Identificazione del soggetto richiedente

Lepida rende disponibile un servizio base gratuito per tutti i cittadini con documenti di identità rilasciati da un'autorità italiana (carta d'identità, passaporto, patente) oppure carta di identità o passaporto rilasciato dalla Repubblica di San Marino. Sono disponibili tre modalità di identificazione informatica:

- **Identificazione informatica tramite documenti digitali di identità.** Nel caso di identificazione informatica tramite documenti digitali di identità, l'identificazione avviene tramite verifica dei documenti digitali rilasciati con un meccanismo che prevede il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui la Carta di Identità Elettronica (CIE 3.0, versione contactless).

Nel caso di identificazione informatica tramite CIE 3.0, il sistema avvia una specifica procedura che consente l'accesso mediante l'utilizzo della CIE 3.0, interfacciandosi con il sito del Ministero dell'Interno.



Terminata la procedura di verifica, sono salvati a sistema gli estremi della sessione di log come dimostrazione dell'avvenuta identificazione.

- **Identificazione informatica tramite firma elettronica qualificata o firma digitale.** Nel caso di identificazione informatica tramite firma elettronica qualificata o firma digitale si procede con l'acquisizione del modulo di richiesta di adesione in formato digitale, messo a disposizione in rete dal Gestore dell'Identità Digitale, compilato e sottoscritto con firma elettronica qualificata o con firma digitale. L'identificazione avviene tramite la verifica della firma elettronica qualificata o firma digitale apposta sulla richiesta. La verifica viene fatta dall'operatore che, dopo aver verificato la validità della firma (anche come data di scadenza) apposta sul documento, provvede a confrontare il codice fiscale associato con quello dell'utente soggetto ad identificazione. Il documento firmato digitalmente viene salvato nel sistema come attestazione dell'avvenuta identificazione.
- **Identificazione informatica tramite altra identità SPID LepidaID** (disponibile solo per richieste di identità ad uso professionale per persona fisica per utenti che hanno identità SPID LepidaID ad uso privato). Nel caso di identificazione informatica tramite altra identità SPID LepidaID l'identificazione avviene attraverso l'accesso, utilizzando credenziali SPID LepidaID ad uso privato di livello di sicurezza 2, ad un servizio reso disponibile allo scopo da parte dal Gestore dell'Identità Digitale. Qualora l'utente desideri utilizzare le medesime credenziali, l'identità ad uso professionale per persona fisica è un upgrade della identità ad uso privato utilizzata per l'identificazione informatica; in caso contrario, le due identità sono distinte.

Inoltre, Lepida rende disponibile anche la possibilità di effettuare:

- **identificazione a vista del soggetto richiedente in presenza** presso sportelli preposti al rilascio delle Identità Digitali LepidaID. Il soggetto richiedente si presenta fisicamente presso le sedi preposte al rilascio delle Identità Digitali messe a disposizione di Lepida, esibendo un documento di identità e il documento del codice fiscale (tessera sanitaria o equipollenti, previsti dalla normativa AgID) in corso di validità. L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento integro e in corso di validità rilasciato da un'Amministrazione dello Stato Italiano e della Repubblica di San Marino, munito di fotografia e firma autografa dello stesso e controlla il documento del codice fiscale che costituiscono ulteriori elementi a supporto del processo di verifica dell'identità. A dimostrazione dell'avvenuta identificazione a vista devono essere caricate sul sistema la scansione fronte/retro del documento di identità e del documento del codice fiscale qualora non fosse già stato fatto dall'utente durante la fase di registrazione.



L'identificazione a vista del soggetto richiedente deve avvenire sia nel caso di richiesta di adesione online con "riconoscimento de visu" che nel caso di richiesta di adesione in "modalità assistita".

- **Identificazione a vista da remoto (videocomunicazione con operatore)** del soggetto richiedente un'identità SPID LepidaID. Viene effettuata da remoto tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196. Lepida rende disponibili tutte le informazioni necessarie per l'utilizzo, ivi compresi requisiti tecnici minimi necessari per la postazione dell'utente. Si fa presente che l'identificazione a vista da remoto avviene a seguito della registrazione online del soggetto richiedente che prevede il caricamento dei documenti previsti (copia per immagine, ovvero foto o scannerizzazione, fronte/retro del documento di identità e del documento del codice fiscale).

Si precisa che sia per l'identificazione a vista che per quella a vista da remoto, il soggetto richiedente deve procedere all'identificazione entro un tempo massimo di 30 giorni pena la decadenza della richiesta.

Lepida può richiedere l'integrazione della documentazione presentata dall'utente al momento della richiesta. Il richiedente deve provvedere entro 30 giorni, oltre i quali la richiesta decade.

Viene resa disponibile una ulteriore modalità:

- **Identificazione con registrazione audio/video e bonifico** dell'utente richiedente un'identità SPID LepidaID. Viene effettuata da remoto tramite strumenti di registrazione audio/video nel rispetto del decreto legislativo 30 giugno 2003, n.196. La registrazione online del soggetto richiedente prevede il caricamento dei documenti previsti (copia per immagine, ovvero foto o scannerizzazione, fronte/retro del documento di identità e del tesserino della tessera sanitaria o del documento del codice fiscale). Al passo finale della registrazione l'utente è invitato a effettuare una registrazione audio/video in maniera autonoma, seguendo le istruzioni fornite dal sistema. Il rilascio dell'Identità Digitale SPID LepidaID è subordinata alla ricezione da parte di Lepida di un bonifico di valore simbolico, necessario per completare l'identificazione, che deve essere ricevuto entro 10 giorni, e all'esito delle verifiche previste dalle normative.

Si fa notare che nel caso di identificazione con registrazione audio/video e bonifico, qualora la ricezione del bonifico non avvenga nei 10 giorni successivi alla registrazione, la richiesta di Identità Digitale decade.



Gli operatori di Lepida, nella propria Area Riservata, a cui accedono esclusivamente tramite le proprie credenziali SPID con autenticazione di livello 2, hanno a disposizione la lista degli utenti che hanno effettuato richiesta di un'Identità Digitale. Per ognuna di essi hanno evidenza della modalità di identificazione richiesta (nel caso di identificazione a vista, da remoto del soggetto richiedente o con registrazione audio/video più bonifico) o già effettuata al momento dell'invio della richiesta (nel caso di identificazione tramite smartcard, documento firmato digitalmente e CIE 3.0). Nel caso di identificazione a vista o da remoto del soggetto richiedente, hanno anche evidenza di un'eventuale richiesta di appuntamento per procedere con la fase di identificazione che devono confermare (l'operazione verrà notificata all'utente attraverso email e SMS), con la possibilità di contattare l'utente per suggerire la modifica della data dell'appuntamento; l'utente visualizza il contatto all'interno della propria area riservata. Gli operatori di Lepida hanno inoltre la possibilità di visionare la documentazione presentata nell'invio della richiesta, e validarla al fine di attivare l'Identità Digitale.

7.3. Esame e verifica del richiedente

Sulla base del regolamento attuativo SPID, le attività atte alla verifica dell'Identità Digitale consistono nel rafforzamento del livello di attendibilità degli attributi di identità, raccolti in fase di identificazione.

Sia il processo di identificazione sia il processo di verifica sono eseguiti allo scopo di ottenere un adeguato grado di affidabilità dei dati e delle informazioni forniti dall'utente in fase di registrazione.

Lepida, in qualità di Gestore dell'Identità, effettua l'accesso alle fonti autoritative per le attività di verifica nel rispetto delle Modalità Attuative (Versione 2) per la realizzazione dello SPID con particolare riferimento all'Articolo 12.

Indipendentemente dalle modalità di riconoscimento sopra citate, l'operatore deve verificare che il documento di identità e documento del codice fiscale, caricati sul sistema, siano integri e in corso di validità. Il documento di identità deve essere rilasciato da un'amministrazione dello Stato Italiano o della Repubblica di San Marino, munito di fotografia ben visibile e firma autografa dello stesso.

Le verifiche si basano sulle fonti autoritative quali ad esempio:

- Il servizio dell'Agenzia delle Entrate per la validità dei codici fiscali
- Crimnet messo a disposizione dal Ministero dell'Interno
- Il sistema pubblico SCIPAFI (Sistema pubblico di prevenzione delle frodi nel settore del credito al consumo con specifico riferimento al Furto d'identità).



Viene verificata anche la corrispondenza dei dati caricati online sul profilo dell'utente e presenti sui documenti presentati. Gli operatori di Lepida hanno a disposizione una lista degli utenti in attesa di verifica. Terminate le procedure di verifica l'operatore ha a disposizione una specifica form per confermare l'attività svolta e attivare l'Identità Digitale.

Qualora siano scaduti i termini per l'identificazione oppure qualora una qualche verifica risulti negativa (ad esempio un documento logoro o non conforme) l'operatore può negare la richiesta di identità e inviare specifica comunicazione all'utente che ha facoltà di presentare nuova documentazione in sostituzione di quella già presentata, tramite la sua pagina profilo. Il processo rimane sospeso fino ad intervento che permetta la conclusione positiva della verifica precedentemente fallita. L'invio della comunicazione all'utente può avvenire tramite email o SMS da parte dell'operatore. Tali funzionalità possono essere utilizzate per qualsiasi genere di comunicazione durante tutta la vita dell'Identità Digitale.

Nel caso di negazione della richiesta di un'Identità Digitale, l'utente deve presentare una nuova domanda.

7.4. Emissione e creazione delle credenziali

A seguito delle verifiche descritte nel capitolo 7.3, LepidaID chiede al titolare di identità di completare, durante la fase di riconoscimento, le ultime azioni a carico dell'utente. In particolare, la presa visione e accettazione del modulo di adesione, informativa della privacy, documento di informativa dei rischi dal possesso di identità SPID e le condizioni del servizio LepidaID. Solo a seguito di questi passaggi, l'identità sarà attiva e utilizzabile per l'accesso ai servizi della federazione SPID. Il processo di creazione delle credenziali comporta attività necessarie a dare origine ad una credenziale sicura.

Per le autenticazione di livello 1, la credenziale a un fattore (password) viene prodotta dall'utente Titolare dell'Identità Digitale sulla base di regole sul formato, definite dalle modalità attuative SPID.

In particolare, la password deve avere i seguenti vincoli:

- Lunghezza minima di 8 caratteri
- Utilizzo di caratteri maiuscoli e minuscoli
- Inclusione di uno o più caratteri numerici
- Non deve contenere più di due caratteri identici consecutivi
- Inclusione di almeno un carattere speciale ad es #,\$,%, ecc.
- Vietato l'utilizzo di informazioni non segrete riconducibili all'utente



- Validità massima non superiore a 180 giorni
- Vietato il riutilizzo o elementi di similitudine prima di cinque variazioni e comunque non prima di 15 mesi.

Per l'implementazione del livello 2 SPID, Lepida oltre alla password composta come sopra indicato, si utilizza anche una password temporanea (OTP), cioè un codice la cui validità è limitata solo ad una transazione nell'ambito della sessione applicativa e per un tempo limitato. Tale codice temporaneo è inviato dal sistema tramite SMS sul cellulare verificato dell'utente oppure generato attraverso la APP LepidaID, precedentemente attivata dall'utente titolare dell'identità, con PIN o con riconoscimento biometrico.

Tramite la APP LepidaID è possibile generare il secondo fattore di autenticazione anche attraverso la generazione di una notifica push oppure la lettura del QR Code presente sulla pagina web di login, unitamente all'inserimento del PIN oppure riconoscimento biometrico.

Il PIN è un codice alfanumerico/numerico, scelto dall'utente titolare della Identità Digitale in fase di associazione della APP, che viene richiesto all'utente ad ogni utilizzo della APP LepidaID nel caso in cui non sia disponibile oppure l'utente non abbia attivato sul proprio dispositivo il riconoscimento biometrico.

7.5. Richiesta dell'Identità Digitale ad uso professionale per persona fisica e per persona giuridica

Per richiedere Identità Digitali ad uso professionale occorre rivolgersi direttamente a Lepida.

Gli utenti che desiderano dotarsi di una identità ad uso professionale per persona fisica dovranno contattare Lepida, e una volta finalizzata la contrattualizzazione, la richiesta di adesione online viene abilitata dal personale di Lepida. La procedura di rilascio si differenzia a seconda che il richiedente sia già dotato o meno di un'Identità Digitale LepidaID ad uso privato per persona fisica attiva. Nel secondo caso va effettuata la procedura di riconoscimento come per le Identità Digitale ad uso privato precedentemente descritta.

Gli utenti che desiderano dotarsi di una identità ad uso professionale per persona giuridica dovranno contattare Lepida S.c.p.A. facendo riferimento all'organizzazione di appartenenza. La persona giuridica, che coincide con l'organizzazione, deve stipulare un'apposita convenzione con Lepida per poter rilasciare credenziali LepidaID ad uso professionale per persona giuridica agli utenti appartenenti alla propria organizzazione. L'organizzazione nomina gli operatori (utenze di governo e di gestione), che, opportunamente formati da Lepida, provvederanno a raccogliere i nominativi dei soggetti eleggibili appartenenti all'organizzazione per rilasciare loro l'identità ad



uso professionale per persona giuridica esclusivamente mediante riconoscimento de visu e sulla base della procedura definita dalle “Linee guida per il rilascio dell’Identità Digitale per uso professionale” definite da AGID. Per avere maggiori informazioni in merito al rilascio di tali identità, l’organizzazione deve rivolgersi a Lepida.

L’identità ad uso professionale per la persona giuridica prevede lo stesso set di informazioni per l’identità per persona fisica più le seguenti:

- Ragione sociale della persona giuridica
- Sede legale della persona giuridica
- P. IVA della persona giuridica
- Codice fiscale della persona giuridica.

Per le sole identità digitali SPID LepidaID ad uso professionale per persona giuridica, è possibile ricevere il secondo fattore di autenticazione tramite e-mail all’indirizzo associato alla propria identità digitale.

8. Revoca o sospensione o riattivazione dell’Identità Digitale

La revoca dell’identità digitale rappresenta il processo che annulla definitivamente la validità delle Identità Digitali. La sospensione, invece, è un processo di annullamento temporaneo.

L’utente, titolare di Identità Digitale, può chiedere al Gestore dell’Identità Digitale, in qualsiasi momento e a titolo gratuito, la sospensione o la revoca a seguito di una sospensione della propria Identità Digitale attraverso una delle seguenti modalità:

- a) richiesta al Gestore LepidaID inviata via PEC all’indirizzo lepidaid@pec.lepida.it, qualora disponibile la PEC del titolare e sia associata alla identità del soggetto.
- b) richiesta al Gestore LepidaID inviata via posta elettronica all’indirizzo lepidaid@lepida.it utilizzando l’e-mail associata alla propria Identità Digitale SPID LepidaID.

Il modulo può essere trasmesso da un indirizzo diverso da quello associato all’identità digitale SOLO nel caso di richiesta di revoca dell’identità digitale per impossibilità di modificare in autonomia l’e-mail o la PEC associati alla propria identità digitale.

La richiesta al Gestore LepidaID deve includere il relativo “Modulo di richiesta revoca/sospensione/riattivazione” disponibile sul sito del servizio LepidaID (<https://id.lepida.it/>) nonché nell’Area Riservata dell’utente. Il modulo deve preferibilmente essere firmato

digitalmente. Qualora non si disponga di una firma digitale, si può inviare il modulo firmato con firma autografa e con allegato un documento di identità (se non scaduto, lo stesso documento che è stato utilizzato in fase di riconoscimento).

In caso di indisponibilità dei canali sopra indicati, l'utente può comunque richiedere la sospensione della propria Identità Digitale (ad esempio in caso di furto dell'identità) chiamando il numero verde indicato nella pagina di assistenza <https://id.lepida.it/assistenza> nelle more di invio delle informazioni previste per la revoca.

La revoca della Identità Digitale deve essere richiesta dall'utente nei seguenti casi:

- 1) Smarrimento, furto o altri danni/compromissioni (con obbligo di allegare la denuncia presentata alle autorità giudiziarie)
- 2) uso illecito dell'Identità Digitale
- 3) Volontà del titolare dell'Identità Digitale
- 4) Decesso della persona fisica titolare della Identità Digitale
- 5) Impossibilità di modificare in autonomia il cellulare, l'e-mail o la PEC associati alla propria identità digitale

Nel caso di smarrimento, furto o altri danni/compromissioni e uso illecito dell'Identità Digitale, ovvero nel caso in cui l'utente ritenga che la propria Identità Digitale sia stata utilizzata fraudolentemente, lo stesso può chiederne la sospensione nelle modalità sopra descritte. Per procedere alla revoca deve allegare la denuncia presentata alle autorità giudiziarie.

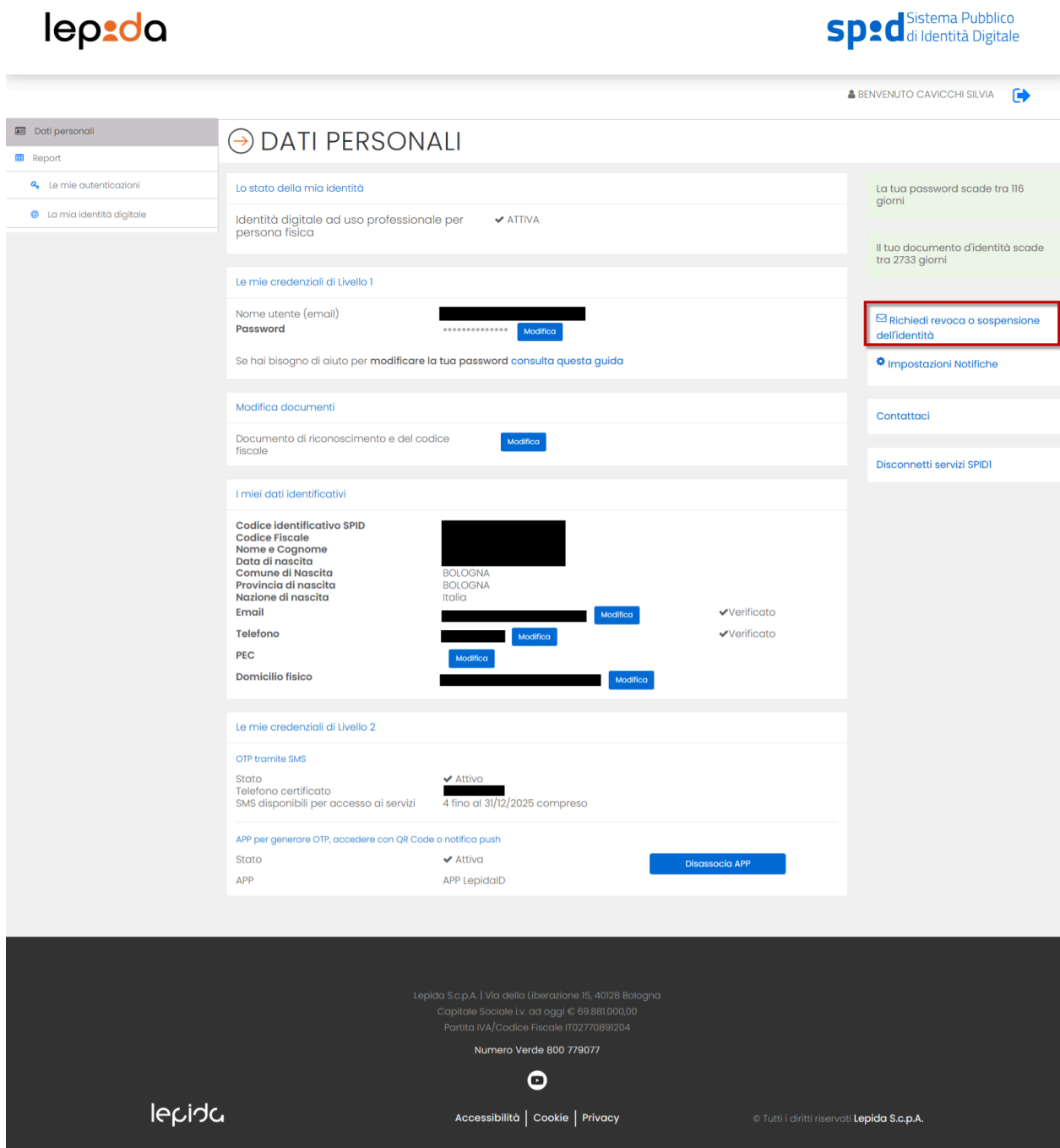
Nel caso di decesso della persona fisica titolare dell'Identità Digitale, i rappresentanti del soggetto titolare dell'identità deceduto (eredi o procuratore) devono presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'Identità Digitale.

Al fine di suddetto accertamento, oltre al modulo di richiesta di sospensione/revoca dell'Identità Digitale, e sempre nelle medesime modalità, si richiede la contestuale trasmissione di:

- Dichiarazione sostitutiva di atto notorio ex art. 47 DPR 445/2000 circa lo status di erede e il decesso del titolare delle credenziali SPID
- Copia del documento di identità del richiedente in corso di validità
- Copia del documento di identità del defunto titolare della Identità Digitale.

Nel caso di perdita della disponibilità del numero di cellulare o della email di contatto / nome utente e pertanto nell'impossibilità di modifica autonoma da parte del titolare di identità

attraverso le funzioni rese disponibili nella propria area personale, il titolare di identità deve richiedere la revoca della propria identità nelle modalità sopra indicate.



lepida **spid** Sistema Pubblico di Identità Digitale

BENVENUTO CAVICCHI SILVIA

DATI PERSONALI

[Lo stato della mia identità](#)

Identità digitale ad uso professionale per persona fisica **ATTIVA**

[Le mie credenziali di Livello 1](#)

Nome utente (email) **[REDACTED]**

Password **[REDACTED]** [Modifica](#)

Se hai bisogno di aiuto per [modificare la tua password consulta questa guida](#)

[Modifica documenti](#)

Documento di riconoscimento e del codice fiscale [Modifica](#)

[I miei dati identificativi](#)

Codice identificativo SPID **[REDACTED]**

Codice Fiscale **[REDACTED]**

Nome e Cognome **[REDACTED]**

Data di nascita **[REDACTED]**

Comune di Nascita **[REDACTED]**

Provincia di nascita **[REDACTED]**

Nazione di nascita **[REDACTED]**

Email **[REDACTED]** [Modifica](#) **✓ Verificato**

Telefono **[REDACTED]** [Modifica](#) **✓ Verificato**

PEC **[REDACTED]** [Modifica](#)

Domicilio fisico **[REDACTED]** [Modifica](#)

[Le mie credenziali di Livello 2](#)

[OTP tramite SMS](#)

Stato **Attivo**

Telefono certificato **[REDACTED]**

SMS disponibili per accesso ai servizi **4 fino al 31/12/2025 compreso**

[APP per generare OTP, accedere con QR Code o notifica push](#)

Stato **Attiva**

APP **APP LepidaID** [Disassocia APP](#)

[Richiedi revoca o sospensione dell'identità](#)

[Impostazioni Notifiche](#)

[Contattaci](#)

[Disconnetti servizi SPID](#)

Lepida S.p.A. | Via della Liberazione 15, 40128 Bologna
Capitale Sociale i.v. ad oggi € 69.881.000,00
Partita IVA/Codice Fiscale IT02770891204
Numero Verde 800 779077

lepida

[Accessibilità](#) | [Cookie](#) | [Privacy](#)

© Tutti i diritti riservati **Lepida S.p.A.**

Richiesta di revoca o sospensione dell'identità digitale



Il Gestore dell'Identità fornisce esplicita evidenza all'utente dell'avvenuta presa in carico della richiesta e procede alla immediata sospensione dell'Identità Digitale.

Il Gestore provvede alla revoca dell'identità nel momento in cui riceve la denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione oppure una richiesta di revoca.

La revoca di una Identità Digitale comporta conseguentemente la revoca delle relative credenziali. I Gestori dell'Identità Digitale conservano la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla revoca dell'identità digitale.

In caso di scadenza del documento identità associato all'Identità Digitale, il Gestore dell'Identità Digitale sospende di propria iniziativa l'identità, comunicando la causa e la data della sospensione all'utente, utilizzando l'indirizzo di posta elettronica associato al profilo dell'utente. Prima della scadenza del documento il sistema LepidaID informa automaticamente il titolare della identità, attraverso mail, invitandolo a caricare gli estremi del documento di identità attraverso una funzione resa disponibile all'interno della propria Area Riservata.

In caso di identità non attiva per un periodo superiore a 24 mesi, il Gestore di identità revoca di propria iniziativa, mettendo in atto meccanismi con i quali comunica la causa e la data della revoca all'utente, con avvisi ripetuti utilizzando l'indirizzo di posta elettronica associato al profilo utente.

In caso di sospensione delle credenziali, avvenuta a seguito di richiesta del titolare dell'identità oppure a seguito dell'inserimento della password sbagliata per più di 10 volte consecutive e ignoro della procedura per sblocco automatico, il titolare dell'identità digitale può richiederne la riattivazione utilizzando il "Modulo di richiesta revoca/sospensione/riattivazione" disponibile sul sito del servizio LepidaID (<https://id.lepida.it/>) nonché nella propria Area Riservata.

9. Gestione dei rapporti con gli utenti

Lepida mette a disposizione un servizio di helpdesk per supportare i Titolari di Identità Digitale SPID LepidaID sia al momento della registrazione al servizio sia al momento dell'utilizzo delle credenziali per l'accesso ai servizi.

Sono disponibili diversi canali di accesso al servizio di assistenza sul sito del servizio LepidaID al link <https://id.lepida.it/assistenza>.



Eventuali comunicazioni e avvisi di interventi o modifiche alle condizioni del servizio o alle modalità di erogazione del servizio sono pubblicate sul sito del servizio LepidaID (<https://id.lepida.it>) con adeguato anticipo.

10. Descrizione generale delle misure anti-contraffazione

Lepida mette in atto tutti i processi (tecnici e organizzativi) volti a garantire la protezione delle identità al fine di evitare abusi e usi non autorizzati ovvero ad assicurare la sicurezza della conservazione delle credenziali.

Per ogni livello di sicurezza SPID, vengono adottate diverse misure di anti-contraffazione.

10.1. Livello 1 SPID

Il livello di sicurezza SPID 1 è implementato attraverso l'utilizzo di credenziali di accesso composte da un singolo fattore (password).

La principale misura anti-contraffazione è determinata dalla riservatezza di conservazione e dall'utilizzo personale da parte dell'utente, titolare dell'Identità Digitale. Al fine di aumentare il livello di sicurezza e ridurre il pericolo di abusi ed uso improprio delle stesse, è prevista la seguente complessità di composizione delle credenziali:

- La password deve risultare compatibile alle comuni precauzioni sul formato e deve essere fortemente sconsigliato l'uso di informazioni non segrete riconducibili all'utente (ad es. codice fiscale, patente auto, sigle documenti, date, nomi, account-Id ecc.)
- Il formato della password deve prevedere una lunghezza minima di otto caratteri, l'uso di caratteri maiuscoli e minuscoli, l'inclusione di uno o più caratteri numerici e di almeno un carattere speciali ad es #, \$,% e non deve contenere più di due caratteri identici consecutivi
- La password deve avere una durata massima non superiore a 180 giorni e non possono essere riutilizzate, o avere elementi di similitudine, prima di cinque variazioni e comunque non prima di 15 mesi.

Per aumentare il grado di sicurezza delle password e al fine di evitare utilizzi impropri delle Identità Digitali, Lepida implementa anche le politiche di sicurezza nella gestione delle chiavi segrete associate alle Identità Digitali:

- Le password vengono salvate sulla base dati utilizzando tecniche di hashing robusti (Argon2ID) e tecniche di salt idonei al fine di garantire maggiore sicurezza contro attacchi



- L'accesso ai sistemi è limitato al personale autorizzato di Lepida secondo le modalità definite dai processi ISO27001 previsti nella stessa.

10.2. Livello 2 SPID

Il livello di sicurezza SPID 2 è implementato attraverso un sistema a due fattori: l'utilizzo della verifica di una password, con le stesse caratteristiche previste per il livello SPID 1, e l'adozione di una OTP (One Time Password) la cui validità è limitata solo ad una transazione nell'ambito della sessione applicativa. Il formato dell'OTP, che potrà essere utilizzata un'unica volta, è rigorosamente numerico (non è previsto l'utilizzo di lettere o simboli) e ha una lunghezza di 6 cifre e durata di validità di 5 minuti.

Lepida permette l'invio della OTP attraverso un messaggio SMS al numero di cellulare inserito in fase di registrazione oppure la generazione dell'OTP attraverso la APP LepidaID, associata all'account utente. Inoltre la ricezione del secondo fattore può avvenire sempre sul dispositivo mobile dell'utente titolare di identità attraverso una notifica push tramite APP LepidaID associata all'account utente. Quest'ultima modalità è implementata nelle versioni Android, IOS e Huawei.

Il livello di sicurezza SPID 2 è implementato anche attraverso la lettura, tramite APP LepidaID, del QR Code presentato sulla pagina web di login e PIN oppure riconoscimento biometrico. Il QR Code ha validità limitata (120 secondi), dopodiché non è più utilizzabile e ne viene generato uno nuovo. Il PIN è un codice alfanumerico/numerico, scelto dall'utente titolare della Identità Digitale in fase di associazione della APP LepidaID, che viene richiesto all'utente ad ogni utilizzo della APP LepidaID nel caso in cui non sia disponibile oppure l'utente non abbia attivato sul proprio dispositivo il riconoscimento biometrico.

Il PIN ha lunghezza fissa di 6 caratteri, può contenere sia lettere dell'alfabeto sia numeri, senza vincoli particolari di maiuscole e minuscole, non deve contenere sequenze alfabetiche e numeriche, le sequenze alfabetiche non devono contenere un nome proprio.

L'utilizzo di un dispositivo fisico di proprietà dell'utente per la ricezione del codice temporaneo, univoco per sessione, permette di garantire elevati requisiti di sicurezza.

L'utilizzo del codice di verifica OTP in aggiunta alla password annulla la vulnerabilità legata agli attacchi con replica, garantendo che il codice – anche se intercettato – non possa più essere riutilizzato per eseguire una autenticazione, in quanto valido solo per il determinato periodo temporale per il quale è stato emesso.

Gli attributi secondari, in particolare numero di cellulare e e-mail, possono essere modificati solo dal diretto interessato attraverso le funzioni rese disponibili nell'area personale del titolare di



identità. Qualora tali attributi non siano più nella disponibilità del titolare di identità, il titolare deve richiedere la revoca della propria identità.

11. Descrizione generale del sistema di monitoraggio

Il Gestore di Identità SPID deve rendere disponibili all'Agenzia per l'Italia Digitale sia informazioni statistiche che informazioni relative al servizio offerto.

Di seguito l'elenco delle tipologie di informazioni che il Gestore di Identità deve fornire:

- Gli incidenti di sicurezza rilevati
- Le informazioni circa il livello di soddisfazione dei clienti
- Le caratteristiche di eventuali servizi aggiuntivi offerti
- Le informazioni relative a disservizi.

I Gestori delle Identità Digitali inviano all'Agenzia, con cadenza definita congiuntamente, i dati statistici relativi all'utilizzo del sistema, le metriche quantitative e qualitative che saranno definite e concordate a valle dell'avvio in produzione del Gestore di Identità Lepida.

Al fine di monitorare il sistema, Lepida dispone di un sistema di monitoraggio in grado di rilevare in tempo reale anomalie o disservizi e di segnalarli alle strutture preposte alla gestione tecnica. Le funzioni del sistema di monitoraggio sono relative al controllo dell'intera infrastruttura tecnologica (rete, server, storage, applicazioni software). Attraverso sonde e simulazioni applicative vengono monitorati i principali indicatori applicativi e infrastrutturali che misurano il corretto funzionamento del servizio di Gestione delle Identità.

Le console di monitoraggio sono configurate per il continuo controllo, produzione di allarmi e periodicamente si produce la reportistica dei controlli effettuati.

12. Obblighi del Gestore e dei Titolari dell'Identità Digitale

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

- Gli obblighi che il Gestore Lepida assume in relazione alla propria attività
- Gli obblighi che il Titolare dell'Identità Digitale assume in relazione alla richiesta e all'utilizzo dell'Identità Digitale rilasciata dal Gestore, con indicazione dei rispettivi riferimenti normativi.

12.1. Obblighi del Gestore dell'Identità Digitale



Di seguito l'elenco degli obblighi del Gestore di Identità:

- Rilasciare l'identità su domanda dell'interessato e acquisire e conservare il relativo modulo di richiesta
- Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale
- Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione a vista
- 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 scadenza o dalla revoca dell'Identità Digitale
- Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'Identità Digitale
- Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al Regolamento UE n. 679/2016
- 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
- Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente
- Verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata)
- Fornire all'utente che l'ha inviata conferma della ricezione della richiesta di sospensione
- Sospendere tempestivamente l'Identità Digitale per un periodo massimo di trenta giorni e informarne il richiedente
- Ripristinare o revocare l'Identità Digitale sospesa, nei casi previsti
- Revocare l'Identità Digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione



- Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale
- Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso
- Effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'Identità Digitale di ciascun utente, procedendo alla sospensione dell'Identità Digitale in caso di attività sospetta
- Effettuare con cadenza almeno annuale un'analisi dei rischi
- Definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID
- Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato
- Condurre con cadenza almeno semestrale il Penetration Test
- Garantire la continuità operativa dei servizi afferenti allo SPID
- Effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna
- Garantire la gestione sicura delle componenti riservate delle Identità Digitali assicurando che non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata
- Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa
- Sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti
- Informare tempestivamente l'AGID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali
- Adeguare i propri sistemi a seguito dell'aggiornamento della normativa
- Inviare all'AGID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici
- In caso intendesse cessare la propria attività, comunicarlo all'AGID "e ai titolari" almeno 30 giorni prima della data di cessazione, indicando gli eventuali Gestori sostitutivi, ovvero segnalando la necessità di revocare le Identità Digitali rilasciate
- In caso di subentro ad un Gestore cessato, gestire le Identità Digitali che questi ha rilasciato dal Gestore cessato e ne conserva le informazioni
- In caso di cessazione dell'attività, scaduti i 30 giorni, revocare le Identità Digitali rilasciate e per le quali non si è avuto subentro



- Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi
- Se richiesto dall'utente, segnalargli via email, ogni avvenuto utilizzo delle sue credenziali di accesso
- Notificare all'utente la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua Identità Digitale
- Nel caso l'Identità Digitale risulti non attiva per un periodo superiore a 24 mesi o il contratto sia scaduto, revocarla e informare l'utente via posta elettronica. In caso di decesso del titolare (persona fisica), revocare previo accertamento l'Identità Digitale
- Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'Identità Digitale
- Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione
- Nel caso in cui l'utente richieda la sospensione o la revoca della propria Identità Digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'Identità Digitale
- Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente
- In caso di richiesta di revoca di dell'Identità Digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'Identità Digitale
- Proteggere le credenziali dell'Identità Digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa
- All'approssimarsi della eventuale scadenza dell'Identità Digitale, comunicare all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta
- In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita;
- Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID



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

12.2. Obblighi del Titolare dell'Identità Digitale

Di seguito l'elenco degli obblighi del Titolare d'Identità Digitale:

- 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
- L'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private
- Sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite
- Fornire/comunicare al Gestore dati e 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:
 - Estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale
- Conservare le credenziali e le informazioni per l'utilizzo dell'Identità Digitale in modo da minimizzare i rischi seguenti:
 - Divulgazione, rivelazione e manomissione



- Furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'Identità Digitale
 - Accertarsi dell'autenticità del fornitore di servizi o del Gestore dell'Identità Digitale quando viene richiesto di utilizzare l'Identità Digitale
- Attenersi alle indicazioni fornite dal Gestore in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele che da adottare per la conservazione e protezione delle credenziali
- In caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali
- In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto, richiedere immediatamente al Gestore la sospensione delle credenziali.

12.3. Responsabilità

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

- Attribuisce l'Identità Digitale e rilascia le credenziali connesse attenendosi alle Regole Tecniche emanate dall'AGID
- Si attiene alle misure di sicurezza previste dal "Codice in materia di protezione dei dati personali" ai sensi del D.lgs n.196 del 30.06.2003 e s.m.i. nonché alle indicazioni fornite nell'informativa pubblicata sul sito <https://id.lepida.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.

13. Documentazione

Tutte le informazioni relative al servizio sono disponibili sul sito web del Gestore dell'Identità Digitale Lepida <https://id.lepida.it>

14. Cessazione IdP

Lepida si impegna a comunicare con un preavviso di almeno 30 gg ad Agenzia e ai titolari l'eventuale cessazione della propria attività di Gestore di Identità Digitale, ai sensi di quanto previsto dalla Normativa SPID, indicando gli eventuali Gestori sostitutivi ovvero segnalando la



necessità di revocare le Identità Digitali rilasciate.

In caso di cessazione dell'attività, scaduti i 30 giorni, Lepida procede con la revoca delle Identità Digitali rilasciate e per le quali non si è avuto subentro.

15. Appendice A - Codici e Messaggi di anomalia

Per quanto riguarda il protocollo SAML, di seguito la tabella dei codici e dei messaggi di anomalie.

Error code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/ SubStatus/ StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
1	Autenticazione corretta	HTTP POST HTTP Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)	n.a	n.a	n.a	
Anomalie del sistema									
2	Indisponibilità sistema	HTTP POST	n.a.	n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio più tardi	n.a.	
3	Errore di sistema	HTTP Redirect	HTTP 500	n.a.	Utente	Pagina di cortesia con messaggio "Sistema di autenticazione non disponibile - Riprovare più tardi"	Ripetere l'accesso al servizio più tardi	n.a.	Tutti i casi di errore di sistema in cui è possibile mostrare un messaggio informativo all'utente
Anomalie delle richieste									
Anomalie sul binding									
4	Formato binding non	HTTP Redirect -----	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio	Contattare il gestore del servizio	Verificare la conformità con le regole	Parametri obbligati



	corretto	HTTP POST				"Formato richiesta non corretto - Contattare il gestore del servizio"		tecniche SPID del formato del messaggio di richiesta	ori: SAMLReq uest SigAlg Signatur e Paramet ri non obligat ori: RelaySta te ----- - Paramet ri obligat ori: SAMLReq uest Paramet ri non obligat ori: RelaySta te
5	Verifica della firma fallita	http:Re direc t	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Impossibile stabilire l'autenticità della richiesta di autenticazion e- Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente , corrotta, non conform e in uno dei paramet ri, con certificat o scaduto o con certificat o non associat o al corretto EntityID nei metadat



									i registrati
6	Binding su metodo HTTP errato	HTTP Redirect ----- - HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non ricevibileCont atare il gestore del servizio"	Contattare il gestore del servizio	Verificare metadata Gestore dell'identita (IdP)	invio richiesta in HTTP-Re direct su entrypoi nt HTTP-PO ST dell'ident ity ----- ----- ---- invio richiesta in HTTP-PO ST su entrypoi nt HTTP-Re direct dell'ident ity
Anomalie sul formato della AuthnReq									
7	Errore sulla verifica della firma della richiesta	HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente , corrotta, non conform e in uno dei paramet ri, con certificat o scaduto o non corrispo ndente ad un fornitore



									di servizi riconosciuti o non associati o al corretto EntityID nei metadati registrati
8	Formato della richiesta non conforme alle specifiche SAML	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr08	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente	Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente e alla verifica positiva della firma
9	Parametro versione non presente, malformato o diverso da '2.0'	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch ErrorCode nr09	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente	
10	Issuer non presente, malformato o non corrisponde all'entità	HTTP POST/HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare formato delle richieste prodotte	



	che sottoscrive la richiesta								
11	ID (Identificatore richiesta) non presente, malformato o non conforme	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr11	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata solo a seguito di una positiva verifica della firma.
12	Request AuthnContext non presente, malformato o non previsto da SPID	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Autenticazione SPID non conforme o non specificata"		Informare l'utente	Auth livello richiesto diverso da: urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2



									ses:SpidL3
13	IssueInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requesterurn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
14	destinatari non presenti, malformati o non coincidenti con il Gestore delle identità ricevente e la richiesta	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requesterurn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
15	attributo isPassive presente e e attualizzato al valore true	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requesterurn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
16	AssertionConsumerService non correttamente valorizzata	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requesterurn:oasis:names:tc:SAML:2.0:status:RequestUnsupported	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	AssertionConsumerServiceIndex presente e attualizzato



	to			ErrorCode nr16					ato con valore non riportato nei metadat a Assertio nConsu merServi celIndex riportato in presenz a di uno od entramb i gli attributi Assertio nConsu merServi ceURL e Protocol Binding Assertio nConsu merServi celIndex non presente in assenza di almeno uno attributi Assertio nConsu merServi ceURL e Protocol Binding La respons e deve essere inoltrata presso Assertio nConsu merServi
--	----	--	--	----------------	--	--	--	--	---



									ce di default riportato nei metadati
17	Attributo Format dell'elemento NameID Policy assente o non valorizzato secondo specifica	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr17	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	Nel caso di valori diversi dalla specifica del parametro opzionale AllowCreate si procede con l'autenticazione senza riportare errori
18	Attribute ConsumerServiceIndex malformato o che riferisce a un valore non registrato nei metadati di SP	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18	Fornitore del servizio (SP)	n.a.	n.a.	riformulare la richiesta con un valore dell'indice presente nei metadati	
Anomalie derivante dall'utente									
19	Autenticazione fallita per ripetuta sottomissione di	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19	HTTP POST/HTTP Redirect	Messaggi di errore specifico ad ogni interazione prevista	inserire credenziali corrette	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno	Si danno indicazioni specifiche e puntuali all'utente



	credenziali errate (superato numero tentativi secondo le policy adottate)							determinato il mancato accesso al servizio richiesto	e per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi di determinate condizioni legate alle policy di sicurezza aziendali, ad esempio dopo 3 tentativi falliti, si risponde al SP.
20	Utente privo di credenziali compatibili con il livello richiesto dal fornitore del servizio	HTTP POST HTTP Redirect	n.a	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20	Fornitore del servizio (SP)	n.a	acquisire credenziali di livello idoneo all'accesso al servizio richiesto	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
21	Timeout durante l'autenticazione utente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21	Fornitore del servizio (SP)	n.a.	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinato periodo di tempo	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	



22	Utente nega il consenso all'invio di dati al SP in caso di sessione vigente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22	Fornitore del servizio (SP)		Dare consenso	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Sia per autenticazione da fare, sia per sessione attiva di classe SpidLL.
23	Utente con identità sospesa /revocata o con credenziali bloccate	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Credenziali sospese o revoke"		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
24	Riservato								
25	Processo di autenticazione annullato dall'utente	HTTP POST	n.a.	ErrorCode nr25	Fornitore del servizio (SP)			Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
26	Processo di erogazione dell'identità digitale andata a buon fine	HTTP POST	n.a.	ErrorCode nr26	Fornitore del servizio (SP)		Identità Digitale erogata con successo		
27	Utente già	HTTP POST	n.a.	ErrorCode nr27	Fornitore del servizio (SP)		Utente già in possesso		



	presente						dell'Identità Digitale con il Fornitore di Identità Digitale selezionato		
28	Operazione annullata	HTTP POST	n.a.	ErrorCode nr28	Fornitore del servizio (SP)		Operazione di richiesta identità digitale annullata dall'utente		
29	Identità non erogata	HTTP POST	n.a.	ErrorCode nr29	Fornitore del servizio (SP)		Il fornitore non ha erogato l'identità digitale		

