LepidaID

Manuale Operativo

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**	**Versione aggiornata** • 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 "Tracciature"
1.3	**15/05/2018**	**Versione aggiornata** • 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**	• 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**	• 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**	• 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**	• 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**	• Aggiornato paragrafo 7.2 "Identificazione del soggetto richiedente": viene resa disponibile la modalità di riconoscimento a vista da remoto
1.9	**10/10/2020**	• 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**	• 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**	• 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**	• 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**	• 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**	• Aggiornato il paragrafo 7.1 e il paragrafo 10.2 con l'autenticazione di livello 2 mediante notifiche push

2.5	**30/12/2021**	• 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**	• 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**	• Aggiornati i riferimenti normativi (inserite LLGG SPID minori)i • Introdotto 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**	• Aggiornamento responsabili manuale operativo • Aggiornamento policy password con rimozione della lunghezza massima
2.9	**25/10/2023**	• 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;

		• Aggiornato capitolo 11, con aggiunta l'indicazione che gli attributi secondari sono modificabili solo dal soggetto titolare di identità;

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 l 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-spid_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 l), 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
Linee Guida operative per la fruizione dei servizi SPID da parte dei minori	https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2213514380300__OLinee+guida+operative+fruizione+SPID+minori+-+11+maggio+2022.pdf

2. Dati identificativi del Gestore

Denominazione sociale	Lepida ScpA
indirizzo della sede legale	Via della Liberazione, 15 - 40128 Bologna (BO)
Legale Rappresentante	Alfredo Peri
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 9525156
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.
  Nel caso di OpenID Connect, Il modello di flusso è l'"OpenID Connect Authorization Code Flow", che è l'unico flusso previsto da iGov. L'Authorization code flow restituisce al Relying Party un codice di autorizzazione che può essere utilizzato per ottenere un ID token e/o un access token necessario per le funzioni di accesso al servizio.

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.

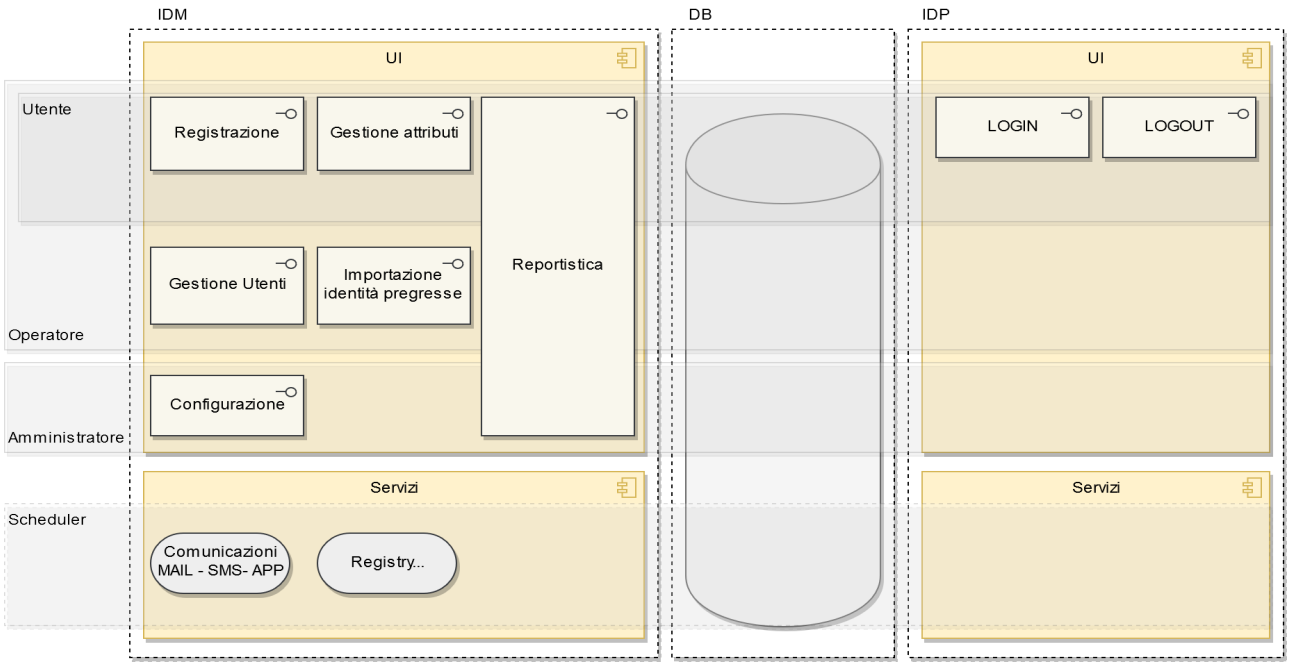
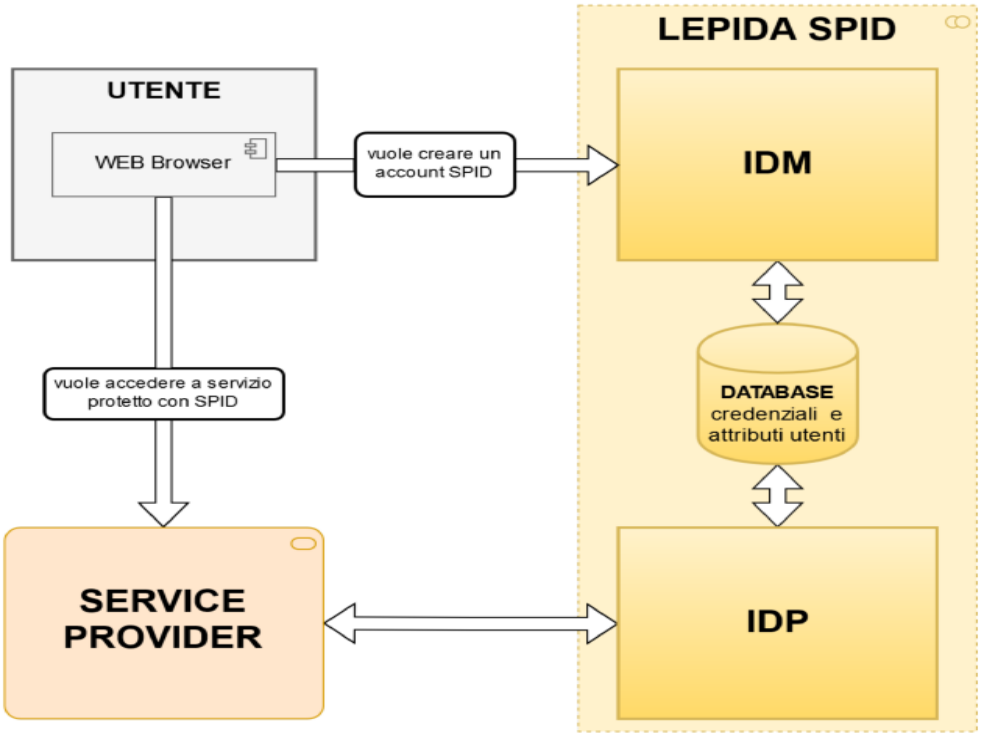
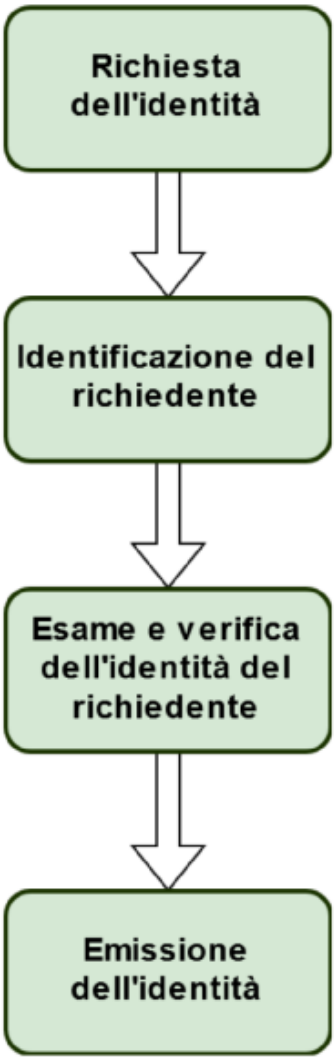


Diagramma logico del Gestore di Identità Lepida



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.

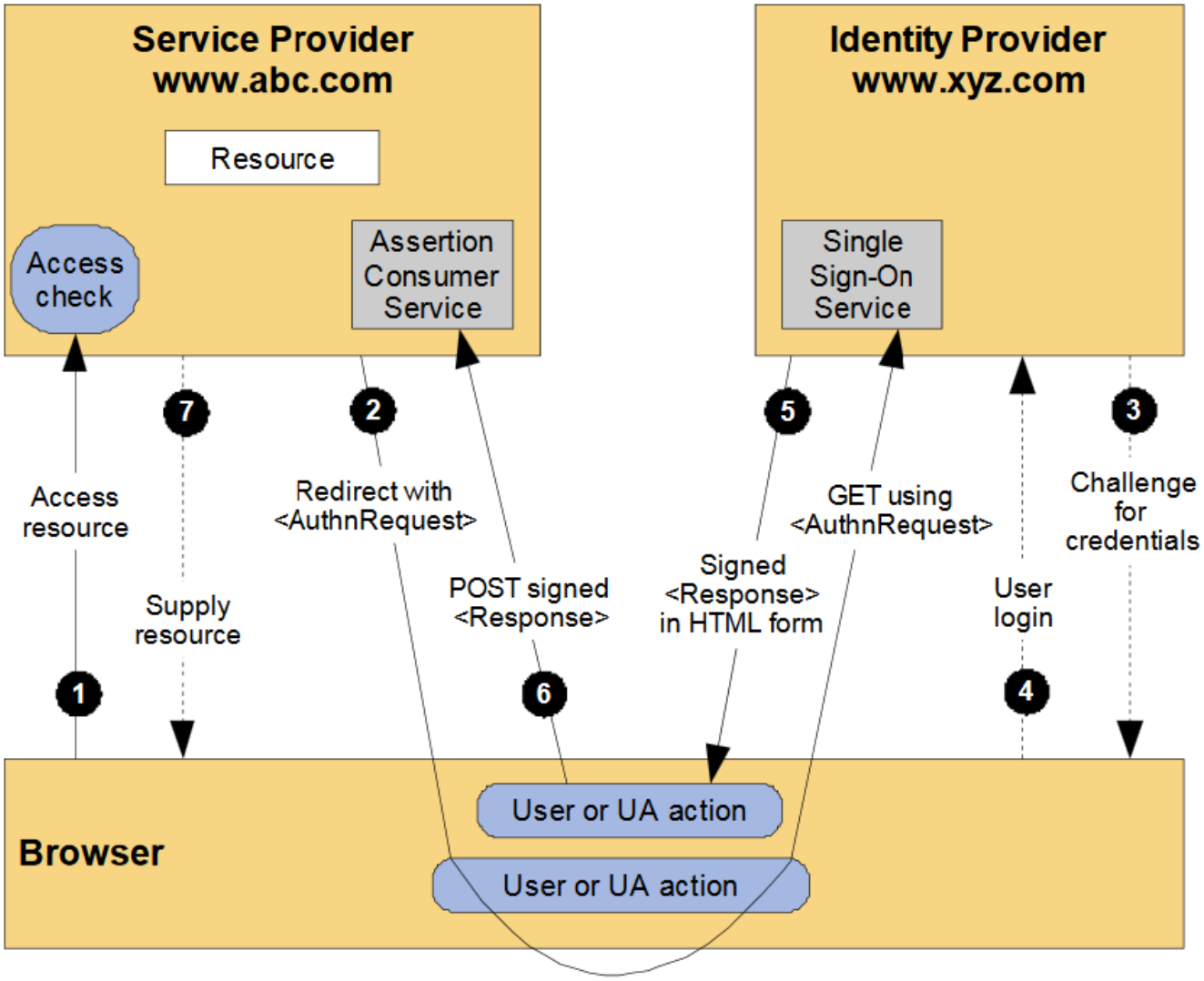
5.2. Architetture dei sistemi di autenticazione e delle credenziali

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:



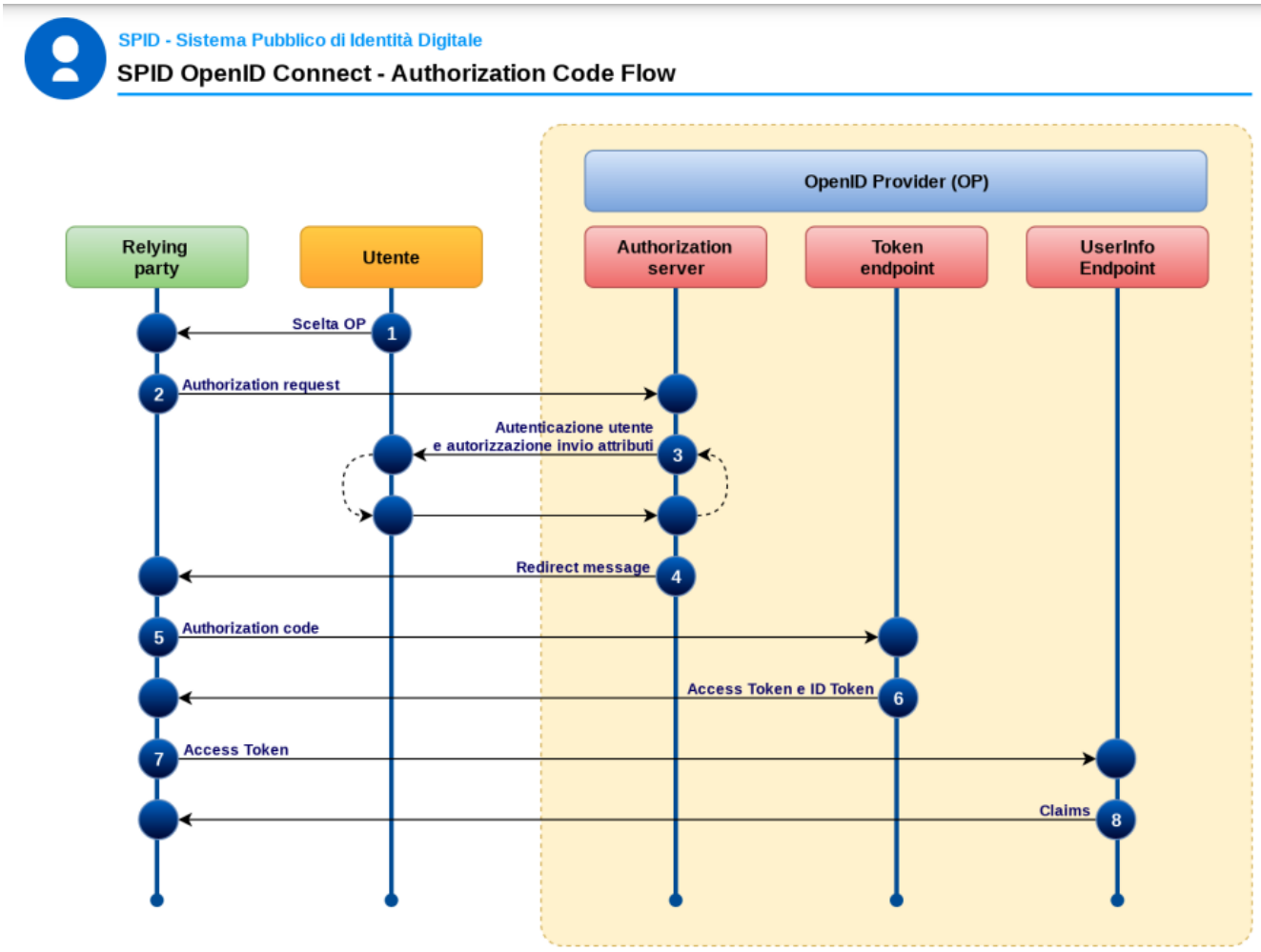
Flusso di autenticazione con SAML 2.0

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 se 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.

Nel caso del protocollo OpenID Connect, il flusso di autenticazione è rappresentato dall'"OpenID Connect Authorization Code Flow", illustrato nello schema seguente:



Flusso di autenticazione con OpenID Connect

I passaggi previsti sono:

1. L'Utente, nella pagina di accesso del Relying Party (RP), seleziona, sul pulsante SPID, l'OpenID Provider (OP) con cui autenticarsi;
2. Il Relying Party (RP) prepara un'authentication request e reindirizza l'user agent dell'utente con l'authentication request verso l'Authorization Endpoint dell'OpendID Provider (OP) selezionato dall'utente;
3. L'OpendID Provider (OP) richiede all'utente l'inserimento delle credenziali, secondo il livello SPID richiesto dal Relying Party (RP), all'utente a cui chiede, una volta autenticato, di autorizzare gli attributi richiesti dal Relying Party (RP);

4. L'OpenID Provider (OP) reindirizza l'utente verso il Redirect URI specificato dal Relying Party (RP), passando un authorization code;
5. Il Relying Party (RP) invia l'authorization code ricevuto al Token endpoint del OpendID Provider (OP);
6. L'OP Token endpoint rilascia un ID Token, un Access Token e se richiesto un Refresh token;
7. Il Relying Party (RP) riceve e valida l'Access Token e l'ID Token. Per chiedere gli attributi che erano stati autorizzati dall'utente al punto 3, invia una richiesta all'UserInfo endpoint utilizzando l'Access Token per l'autenticazione;

L'OpendID Provider (OP) rilascia gli attributi richiesti.

Per la descrizione dell'architettura del sistema di autenticazione si rimanda al Piano della sicurezza del Gestore di Identità Lepida per il servizio LepidaID.

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

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 sotto-servizio di registrazione identità	*Erogazione automatica*	>= 99,0%
			Singolo evento di indisponibilità <= 6 ore

		Erogazione in presenza	>= 98,0%
IQ-02	Tempo di risposta del sotto-servizio di registrazione identità		<= 24h (ore lavorative)
IQ-03	Disponibilità del 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 di riattivazione delle credenziali		<= 2 giorni lavorativi
IQ-06	Disponibilità del sotto-servizio di sospensione e revoca delle credenziali		>= 99,0%
			Singolo evento di indisponibilità <= 6 ore
IQ-07	Tempo di sospensione delle credenziali		<= 30 minuti
IQ-08	Tempo di revoca delle credenziali		<= 5 giorni lavorativi
IQ-09	Disponibilità del sotto-servizio di rinnovo e sostituzione delle credenziali	*Erogazione automatica*	>=99,0%
		Erogazione in presenza	>=98,0%
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		<= 5 giorni lavorativi

IQ-11	Disponibilità del sotto-servizio di autenticazione		>= 99,0 %
			Singolo evento di indisponibilità <= 4 ore
IQ-12	Tempo di risposta del sotto-servizio di autenticazione		Tempo di risposta <=3 sec almeno per il 95,0% delle richieste
IQ-13	RPO sotto-servizio registrazione e rilascio identità		1 ora
IQ-14	RTO sotto-servizio registrazione e rilascio identità		8 ore
IQ-15	RPO sotto-servizio sospensione e revoca delle credenziali		1 ora
IQ-16	RTO sotto-servizio sospensione e revoca delle credenziali		8 ore
IQ-17	RPO sotto-servizio di autenticazione		1 ora
IQ-18	RTO sotto-servizio di autenticazione		8 ore

5.5. Tracciature

5.5.1. Tracciature accessi

Si prevede di mantenere traccia di ogni evento di sistema al fine di consentire una precisa ricostruzione delle attività in caso di necessità. A tal fine vengono tracciate le seguenti tipologie di eventi:

- Autenticazioni
- Variazione dati utente
- Variazione stato
- 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.

Per quanto riguarda il protocollo OpenID Connect, viene mantenuto un Registro delle transazioni contenente i tracciati delle richieste di autenticazione, in particolare mantenendo le seguenti evidenze per:

- rilascio di ID e access token a fronte di autenticazione;
- rilascio di refresh token a fronte di autenticazione;
- rilascio di ID e access token a fronte di utilizzo del refresh token. Per ogni rilascio sono conservati JWT costituenti richiesta e risposta e sono tracciate le chiamate e le relative risposte effettuate verso ogni endpoint.

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 occuperà di eliminare dal file i contenuti via via divenuti obsoleti.

Inoltre, solo i log delle autenticazioni vengono mantenuti anche su un database senza considerare il limite temporale del 24 mesi in modo da consentire agli utenti autorizzati la possibilità di effettuare eventuali ricerche.

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" oppure attraverso le modalità previste dal procedimento di accesso civico previsto da Lepida ScpA.

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 entro 5 giorni lavorativi dalla ricezione della richiesta. Il log sarà prodotto in formato testo, firmato digitalmente dal Legale Rappresentante di Lepida con i dati minimi come previsto dalla normativa.

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 Digitali ad uso privato e Identità Digitali ad uso professionale, sia per persona fisica che per persona giuridica per utenti maggiorenni.

7.1. Richiesta dell'Identità Digitale ad uso privato

Lepida prevede che la richiesta di adesione possa avvenire soltanto in formato digitale tramite modalità informatiche. Tuttavia è possibile effettuare la richiesta di adesione in modalità assistita, ovvero 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/, da parte del soggetto richiedente, 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 attualmente solo per le Identità Digitali ad uso privato), ovvero 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 da parte dell'utente dei dati accesso, il secondo dall'inserimento della propria anagrafica e del domicilio fisico, il terzo dall'inserimento degli estremi del documento d'identità e dal caricamento di una scansione fronte/retro del documento di identità e del tesserino della tessera sanitaria o del codice fiscale, 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 scelta.

Al fine di verificare il possesso degli attributi secondari, il sistema provvede ad inviare apposite comunicazioni di verifica ai contatti inseriti durante la registrazione.

Per validare l'indirizzo email, l'indirizzo PEC e il numero di telefono, viene inviata una comunicazione rispettivamente via email, PEC o via cellulare contenente un codice casuale da inserire in una specifica form dell'Area Riservata.

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 tesserino della tessera sanitaria o del codice fiscale, 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 delle verifiche effettuate dall'operatore di sportello, LepidaID invia una mail al titolare di identità per completare, durante la fase di riconoscimento, le ultime azioni in carico all'utente:
    - accesso attraverso autenticazione con username e password ad un link personalizzato univoco e associato alla identità per effettuare la verifica della mail;
    - a seguito dell'accesso, validazione del cellulare comunicato in fase di registrazione;
    - a seguito dell'accesso, 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'indentità 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 quattro modalità:

- Username/password e codice OTP, generato da LepidaID e inviato via SMS al numero di telefono cellulare associato all'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 presentato sulla pagina web di login e PIN o riconoscimento biometrico
- Ricezione di una notifica push tramite APP LepidaID e PIN o riconoscimento biometrico.

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 al proprio profilo utilizzando le proprie 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 tre modalità di identificazione:

- **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 tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi

  Carta di Identità Elettronica (CIE 3.0, versione contactless). In caso di richiesta da parte dell'utente di identificazione tramite CNS, il sistema avvia una apposita procedura di verifica della carta in locale. 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 la tessera sanitaria 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 tesserino della tessera sanitaria o 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 scannerizzazione fronte/retro del documento di identità e il tesserino della tessera sanitaria o 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 tesserino della tessera sanitaria o del codice fiscale).

Si fa notare che sia per l'identificazione a vista che per quella a vista da remoto, il soggetto richiedente deve procedere all'identificazione, a seguito dell'invio della richiesta di emissione di una nuova Identità Digitale, entro un tempo massimo di 30 giorni pena la decadenza della richiesta.

Per tutte le identificazioni sopra citate, qualora il soggetto richiedente non completi la richiesta integrando la documentazione mancante che Lepida può sollecitare a seguito del controllo della documentazione presentata in fase di registrazione entro un tempo massimo di 30 giorni, 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 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 in fase di 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) o meno, con la possibilità di contattare l'utente per suggerire la modifica della data dell'appuntamento all'interno del proprio account personale. 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 che 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 il tesserino della tessera sanitaria o 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. Nel caso di identificazione tramite Smart Card viene verificata automaticamente la corrispondenza del Codice Fiscale dichiarato e quello contenuto nella carta.

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, 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.

Oltre alle modalità sopra indicate, la ricezione del secondo fattore può avvenire sempre sul dispositivo mobile dell'utente titolare di identità attraverso la ricezione di una notifica push tramite APP LepidaID installata e associata al sistema LepidaID e l'autenticazione si completa con PIN oppure riconoscimento biometrico.

Lepida implementa il Livello 2 SPID anche attraverso l'inquadramento tramite APP LepidaID del QR Code presente sulla pagina web di login e PIN oppure riconoscimento biometrico. Il QR Code mostrato sulla pagina di login 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, 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 alla 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 nominerà degli operatori, 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. L'organizzazione per avere maggiori informazioni in merito al rilascio di tali identità 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.

8. Identità Digitale per minori

In questo capitolo vengono descritte le modalità operative che il Gestore di identità digitali Lepida ha messo in atto come procedura per il rilascio, la gestione e l'utilizzo delle identità digitale SPID LepidaID per minori, sulla base delle rispettive linee guida emesse da AgID.

Con l'identità digitale dei minori si mira a garantire il raggiungimento dei seguenti obiettivi:

- consentire al minore di acquisire la propria identità digitale, previa richiesta da parte di chi esercita la responsabilità genitoriale;
- consentire al minore di fruire autonomamente di servizi online mediante la propria identità digitale, ferma restando - salvo casi specifici - la possibilità di autorizzazione e verifica da parte dell'esercente la responsabilità genitoriale;
- consentire ai fornitori di servizi in rete la selezione dei propri utenti in base all'età.

In questo caso i soggetti coinvolti sono:

- **Minore** - soggetto con età maggiore di 5 anni e minore di 18 anni;

- **Genitore richiedente** - soggetto che esercita la responsabilità genitoriale e richiede al gestore LepidaID il rilascio della identità SPID a favore del minore;
- **Genitore non richiedente** - soggetto che esercita la responsabilità genitoriale, ma non ha richiesto operativamente al gestore LepidaID il rilascio della identità SPID a favore del minore.

Richiesta di rilascio di identità a favore di un minore

Il genitore richiedente che desidera richiedere l'attivazione di una identità digitale SPID LepidaID a favore di un soggetto minore deve essere titolare di una identità digitale SPID LepidaID attiva.

Il genitore richiedente può richiedere una identità digitale SPID a favore del minore di cui esercita la responsabilità genitoriale accedendo con le proprie credenziali SPID LepidaID alla propria Area Riservata sul sito del servizio LepidaID (https://id.lepida.it/), utilizzando la voce di menù "Minori" > "Richiedi identità digitale", funzione disponibile solo per titolari di identità SPID LepidaID maggiorenni.

Il genitore richiedente deve inserire obbligatoriamente i seguenti dati anagrafici del minore per cui sta richiedendo credenziali SPID LepidaID:

- Codice fiscale;
- Nome;
- Cognome;
- Data di nascita.

Il sistema LepidaID controlla che i dati inseriti appartengano ad un soggetto con età di almeno 5 anni. In caso contrario, la procedura viene interrotta.

Il genitore richiedente deve

- dichiarare la propria qualità di esercente di responsabilità genitoriale sul minore, ai sensi dell'art. 46 comma 1, lett. u) del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.;

- dichiarare, ai sensi dell'art. 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i., di essere autorizzato a procedere con la richiesta dal genitore non richiedente oppure di essere l'unico esercente la responsabilità genitoriale e poter procedere in autonomia;
- autorizzare l'invio di notifiche via email da parte del sistema LepidaID per autorizzare l'utilizzo dell'identità SPID LepidaID al minore, qualora richiesto.

Tali dichiarazioni avvengono attraverso specifiche spunte da parte del genitore richiedente, e sono a tutti gli effetti dichiarazioni che il sistema LepidaID memorizza sui propri sistemi.

A conferma di quanto dichiarato nei passi precedenti, durante la richiesta online il genitore richiedente deve caricare i seguenti documenti:

- se il genitore richiedente non è l'unico esercente la responsabilità genitoriale dovrà caricare a sistema documento di identità e estremi dello stesso relativi al genitore non richiedente. Viene richiesto di caricare l'immagine fronte e retro della carta di identità o del passaporto o della patente di guida e di compilare i campi predisposti con numero di documento di identità, data di scadenza ed ente di emissione;
- se il genitore richiedente è l'unico esercente la responsabilità genitoriale, dovrà caricare a sistema un documento attestante tale condizione. In particolare, si richiede il caricamento di uno dei seguenti documenti:
    - Certificato di morte del genitore non richiedente. Viene richiesto il caricamento dell'immagine fronte e retro del documento e di indicare l'ente di emissione dello stesso;
    - Nomina in qualità di tutore del genitore richiedente. Viene richiesto il caricamento dell'immagine del documento e di indicare l'ente di emissione dello stesso.

Se il genitore richiedente non è indicato sul documento di identità del minore, occorre caricare alternativamente:

- il certificato di stato di famiglia con rapporti di parentela. Viene richiesto il caricamento dell'immagine del documento e di indicare l'ente di emissione dello stesso;

- il decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina del tutore o l'affidamento del minore. Viene richiesto il caricamento dell'immagine del documento e di indicare l'ente di emissione dello stesso;

Il genitore richiedente deve dichiarare la presa visione del documento di informativa privacy, dell'informativa dei rischi e delle condizioni di utilizzo del servizio.

A seguito delle azioni sopra citate, il sistema LepidaID genera e comunica al genitore richiedente (sia a video che tramite l'invio di email) il codice di verifica assegnato al minore, che il genitore richiedente dovrà comunicare a sua volta al minore, attraverso canali a sua scelta.

Registrazione di un minore

Il minore, una volta ricevuto il codice di verifica da parte del genitore richiedente, può procedere con la propria registrazione sul sito del servizio LepidaID (id.lepida.it) accedendo alla sezione "Registrati".

In fase di registrazione, nella sezione "Dati personali" l'utente deve inserire i propri dati, tra cui anche la data di nascita. Qualora il sistema LepidaID verifichi che si tratta di una registrazione di un minore, richiede all'utente anche l'inserimento del codice di verifica che il minore deve avere ricevuto dal genitore richiedente a seguito della sua richiesta. Quindi al momento della registrazione il minore deve essere in possesso del codice di verifica, che era stato fornito al genitore richiedente, ed inserirlo necessariamente per procedere.

Il sistema LepidaID verifica l'esistenza a sistema del codice di verifica inserito dal minore nonché la corrispondenza dei dati forniti dal minore con i dati precedentemente inseriti dal genitore richiedente: solo in caso di esito positivo su queste verifiche il sistema permette di procedere con i passi successivi per il completamento della registrazione. In caso di esito negativo il flusso si interrompe e viene restituito un messaggio di errore che ne esplicita anche la motivazione.

Nella procedura di registrazione del minore, l'attributo secondario "e-mail" è l'unico attributo obbligatorio, mentre i restanti attributi sono facoltativi, quali il domicilio fisico, il domicilio digitale (PEC) e il numero di telefono mobile.

Nei casi in cui il minore non sia in possesso di un numero di telefonia mobile e quindi tale numero non sia presente tra i dati forniti in fase di registrazione, durante il processo di autenticazione il sistema LepidaID trasmette il secondo fattore di autenticazione per il livello SPID 2 all'indirizzo di posta elettronica fornito dal minore, certificata dal minore stesso in fase di registrazione.

Inoltre, nei casi in cui il minore non sia in possesso di un numero di telefonia mobile, attraverso una "spunta" presente in fase di registrazione (modificabile anche successivamente se necessario) il minore può dichiarare di voler usare il numero di telefono mobile del genitore unicamente per le funzionalità di gestione della sicurezza della propria identità digitale (in realtà inizialmente usato solo per il cambio password), escludendo quindi l'utilizzo del numero di telefono mobile del genitore per l'invio del secondo fattore di autenticazione per il livello SPID 2 (OTP) del minore.

Qualora il minore abbia compiuto i 14 anni, nella fase di registrazione deve obbligatoriamente prendere visione delle condizioni di utilizzo del servizio, dell'informativa dei rischi e dell'informativa privacy.

Prima di concludere la registrazione, dopo il caricamento dei dati personali e dei documenti di identità e della tessera sanitaria e la validazione dei contatti secondari inseriti, nella sezione "Riconoscimento" l'utente minore seleziona una tra le modalità di riconoscimento tra quelle disponibili: riconoscimento a vista presso lo sportello oppure riconoscimento da remoto con un operatore.

Documentazione

Se il "genitore richiedente" è un genitore ed esiste il genitore non richiedente, la documentazione che deve essere presentata al gestore di credenziali SPID LepidaID è la seguente:

- se sul documento di riconoscimento del minore non è riportato il nome e cognome del genitore richiedente, il ***certificato di stato di famiglia*** **con rapporti di parentela** in cui siano riportati contemporaneamente il nome del genitore richiedente e quello del minore, *da caricare durante la procedura di richiesta e presentare in originale anche durante il riconoscimento*;

- documento di riconoscimento in originale in corso di validità del genitore non richiedente (carta di identità, patente o passaporto), *da caricare durante la procedura di richiesta e presentare in originale durante il riconoscimento*;
- tessera sanitaria o codice fiscale in corso di validità attestante il codice fiscale del minore, *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;
- documento di riconoscimento in corso di validità del minore (carta di identità o passaporto), *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;
- documento di riconoscimento in originale in corso di validità del genitore richiedente (carta di identità, patente o passaporto), *da presentare in originale durante il riconoscimento*.

Se il "genitore richiedente" è un genitore e non esiste il genitore non richiedente, la documentazione che deve essere presentata al gestore Lepida è la seguente:

- se sul documento di riconoscimento del minore non è riportato il nome e cognome del genitore richiedente, il ***certificato di stato di famiglia* con rapporti di parentela** in cui siano riportati contemporaneamente il nome del genitore richiedente e quello del minore, *da caricare durante la procedura di richiesta e presentare in originale anche durante il riconoscimento*;
- certificato di morte del secondo genitore oppure un eventuale provvedimento del tribunale oppure l'estratto di nascita del minore con indicazioni di maternità/paternità, *da caricare durante la procedura di richiesta e presentare in originale anche durante il riconoscimento*;
- tessera sanitaria o codice fiscale in corso di validità attestante il codice fiscale del minore, *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;
- documento di riconoscimento in corso di validità del minore (carta di identità o passaporto), *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;

- documento di riconoscimento in originale in corso di validità del genitore richiedente (carta di identità, patente o passaporto), *da presentare in originale durante il riconoscimento*..

Se il "genitore richiedente" è un tutore ed esiste il genitore non richiedente:

- decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina a tutore o l'affidamento del minore, *da caricare durante la procedura di richiesta e presentare in originale durante il riconoscimento*;
- documento di riconoscimento in originale in corso di validità del genitore non richiedente (carta di identità, patente o passaporto), *da caricare durante la procedura di richiesta e presentare in originale durante il riconoscimento*;
- tessera sanitaria o codice fiscale in corso di validità attestante il codice fiscale del minore, *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;
- documento di riconoscimento in corso di validità del minore (carta di identità o passaporto), *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;
- documento di riconoscimento in originale in corso di validità del soggetto che esercita la responsabilità genitoriale sul minore e che chiede il rilascio SPID con titolo diverso da quello di genitore, *da presentare in originale durante il riconoscimento*.

Se il richiedente è un tutore e non esiste il genitore non richiedente:

- decreto del giudice tutelare o del tribunale dei minorenni attestante la nomina COMPLETA a tutore o l'affidamento del minore, *da caricare durante la procedura di richiesta e presentare in originale durante il riconoscimento*;
- certificato di morte del secondo genitore oppure un eventuale provvedimento del tribunale, *da caricare durante la procedura di richiesta e presentare in originale anche durante il riconoscimento*;

- tessera sanitaria o codice fiscale in corso di validità attestante il codice fiscale del minore, *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;
- documento di riconoscimento in corso di validità del minore (carta di identità o passaporto), *da caricare durante la registrazione e presentare in originale anche durante il riconoscimento*;
- documento di riconoscimento in originale in corso di validità del soggetto che esercita la responsabilità genitoriale sul minore e che chiede il rilascio SPID con titolo diverso da quello di genitore, *da presentare in originale durante il riconoscimento*.

Modalità di riconoscimento

Per un utente minore sono disponibili le seguenti modalità di riconoscimento:

- identificazione a vista in presenza, presso uno sportello LepidaID abilitato;
- Identificazione a vista da remoto con colloquio via webcam con operatore;

In entrambi i casi, il minore deve sempre essere accompagnato dal genitore richiedente e il genitore richiedente deve presentare la medesima documentazione in originale caricata durante la fase di richiesta online ed elencata nel capitolo "Documentazione".

Al termine della procedura di identificazione, in caso di esito positivo il sistema LepidaID invia una e-mail per comunicare l'avvenuta attivazione dell'identità digitale, sia sull'indirizzo di contatto del minore che a quello del genitore richiedente. Nel caso in cui la richiesta sia stata negata, la negazione viene notificata anche via email.

In caso di negazione il genitore dovrà ripetere da capo la richiesta.

Riconoscimento a vista

Nel caso di identificazione a vista, Il minore e il genitore richiedente devono presentarsi fisicamente insieme presso uno sportello LepidaID preposto al rilascio delle identità digitali SPID. L'operatore richiede il documento di identità e la tessera sanitaria del

minore, precedentemente caricati a sistema, effettua i medesimi controlli previsti nelle procedure per il rilascio di identità SPID ad utenti maggiorenni (sia di corrispondenza dei dati caricati sia sugli appositi siti di verifica) e ne accerta l'identità.

Qualora sul documento del minore non sia presente il nome del genitore richiedente, l'operatore richiede anche il certificato di famiglia del minore, verificando che sia il medesimo caricato a sistema in fase di richiesta e che siano specificati i rapporti di parentela, pertanto nel certificato di famiglia devono essere presenti contemporaneamente i nominativi del genitore richiedente e del minore.

Qualora fosse necessario l'operatore può ricaricare a sistema la scansione dei documenti presentati dal genitore richiedente in fase di richiesta (ad esempio se la scansione originaria non rende leggibile il documento scansionato)

L'operatore che effettua l'identificazione del minore deve anche accertarsi della identità del genitore richiedente nonchè accompagnatore, per cui richiede al genitore di esibire un proprio documento di identità (carta d'identità, patente, passaporto). L'operatore accerta l'identità del genitore richiedente e la corrispondenza del documento con quello associato alla identità LepidaID dello stesso. In caso di esistenza di un secondo genitore, il genitore richiedente deve presentare anche il suo documento di identità in originale.

Qualora il secondo genitore non esista, l'operatore verifica il documento che attesta l'unico esercente la responsabilità genitoriale (es. stato di morte dell'altro genitore, nomina in qualità di tutore, ecc.), ne verifica la congruenza e la corrispondenza con il materiale caricato a sistema in fase di richiesta.

In caso di incoerenze, l'identità non può essere rilasciata e la richiesta viene negata.

Qualora i documenti presentati in fase di riconoscimento non corrispondano a quelli caricati in fase di richiesta, l'operatore richiede di esibire quelli caricati a sistema. Qualora il genitore richiedente non sia in grado di presentare tutti i documenti caricati a sistema, l'operatore non può completare il riconoscimento. La negazione annulla sia la

richiesta effettuata del genitore richiedente per il minore che la registrazione fatta a seguire dal minore.

Riconoscimento via webcam con operatore

Nel caso di identificazione a vista da remoto con operatore, la procedura di riconoscimento è la medesima utilizzata per un utente maggiorenne, ma durante il colloquio via webcam deve essere presente, oltre al minore, anche il genitore richiedente: nella prima parte della videochiamata, l'operatore richiede al genitore di esibire tutta la documentazione allegata in fase di richiesta.

Diversamente dalla modalità di riconoscimento di persona, in questa modalità l'operatore non può ricaricare a sistema una nuova scansione dei documenti presentati in fase di registrazione. Se i documenti caricati del genitore richiedente o dal minore non sono completi o leggibili la richiesta viene negata.

Ciclo di vita dell'identità digitale del minore

Gestione dell'identità del minore

Il genitore richiedente può gestire l'identità del minore accedendo alla propria Area Riservata..

Nell'Area Riservata di LepidaID del genitore richiedente è disponibile una sezione per la gestione della identità dei minori a lui associati, in cui fino al compimento del 18esimo anno il genitore può gestire il ciclo di vita dell'identità digitale SPID LepidaID di ciascun minore a lui associato e le relative richieste/autorizzazioni all'accesso ai servizi. In particolare il genitore può:

- accettare o rifiutare le autorizzazioni per le richieste in sospeso arrivate nelle ultime 24 ore dei minori a lui associati, definendone la durata;
- sospendere le autorizzazioni concesse ad uno dei minori a lui associati;
- riattivare le autorizzazioni sospese ad uno dei minori a lui associati;
- revocare le autorizzazioni sospese ad uno dei minori a lui associati;
- modificare alcuni dati delle identità digitali dei minori a lui associati;
- richiedere la sospensione delle identità digitali dei minori a lui associati;

- richiedere la riattivazione delle identità digitali dei minori a lui associati;
- richiedere la revoca delle identità digitali dei minori a lui associati;

Il minore ultraquattordicenne ha a disposizione la propria Area Riservata per la gestione autonoma della propria identità digitale dove può:

- modificare i dati della propria identità digitale;
- richiedere la sospensione della propria identità digitale;
- richiedere la riattivazione della propria identità digitale;
- richiedere la revoca della propria identità digitale;
- consultare in autonomia gli accessi effettuati presso i servizi utilizzati.

Il minore infraquattordicenne, invece, non ha accesso ad una propria Area Riservata. La sua identità SPID LepidaID viene gestita interamente dal genitore richiedente.

Le procedure di sospensioni, attivazione e revoca per l'identità digitale SPID LepidaID di un minore sono descritte nel relativo capitolo di questo manuale e sono disponibili per entrambi i genitori (richiedente e non richiedente).

Azioni al raggiungimento della maggiore età del minore

Quando il titolare minore raggiunge la maggiore età, il sistema LepidaID rimuove le limitazioni presenti nel caso di minore ed elimina i legami con la identità del genitore richiedente.

Al compimento dei 18 anni il sistema LepidaID invia una mail informativa al soggetto titolare dell'identità informandolo che è stato rimosso il controllo parentale e chiedendo a lui di valutare se mantenere attiva l'identità digitale SPID LepidaID o meno.

Qualora il titolare desideri revocare l'identità, deve richiedere esplicitamente la revoca attraverso la procedura prevista nel Manuale Operativo.

In caso contrario, per dichiarare la volontà di mantenere attiva l'identità digitale SPID LepidaID deve accedere alla propria Area Riservata per esplicitare, in fase di accesso, tale volontà. A questo punto il neo-maggiorenne deve obbligatoriamente inserire e validare il numero di telefono mobile, se non ancora presente.

Sino a quando il neo-maggiorenne non dichiara esplicitamente la propria volontà di continuare a usare la propria identità digitale SPID LepidaID, la fruizione dei servizi mediante accesso con SPID è totalmente preclusa e, trascorsi due anni dall'ultimo utilizzo, l'identità digitale SPID LepidaID verrà revocata, in ossequio alla regolamentazione SPID.

Azioni al raggiungimento dei quattordici anni del minore

Quando il titolare minore raggiunge i quattordici anni di età, LepidaID gli invia una mail informandolo della possibilità di gestione della identità da una propria Area Riservata. La stessa informazione viene comunicata anche al genitore richiedente.

Utilizzo dell'identità digitale di minori e fruizione dei servizi

Autenticazione del minore

Al momento dell'accesso ad un servizio con SPID il minore titolare di identità digitale SPID LepidaID deve poter disporre degli strumenti di autenticazione resi disponibili dal gestore di identità per procedere all'autenticazione.

Dal momento che per il minore titolare l'attributo "numero di cellulare" non è obbligatorio e neanche il possesso di un dispositivo dove installare la APP LepidaID, è stata prevista una modalità di autenticazione, disponibile solo ai minori che non hanno associato un numero di cellulare certificato in fase di registrazione che prevede la ricezione del codice temporaneo (OTP) via email.

Il processo di fruizione di un servizio da parte di un minore prevede due casi d'uso:

- fruizione di un servizio da parte di un minore nel caso in cui il servizio non richieda l'autorizzazione del genitore richiedente per l'età dell'utente;
- fruizione di un servizio da parte di un utente minore nel caso in cui il servizio richieda l'autorizzazione del genitore richiedente per l'età dell'utente;

Nel caso in cui il servizio non richiede l'autorizzazione del genitore:

- il minore chiede di accedere al servizio con SPID con gestore LepidaID;
- il fornitore di servizio invia al sistema LepidaID la richiesta di autenticazione;

- il sistema LepidaID effettua la procedura di autenticazione del minore, comprendente anche la verifica di congruenza tra l'età richiesta dal servizio e quella effettiva del minore. Qualora la verifica dia esito negativo, la procedura di autenticazione è interrotta con esito negativo; qualora invece la verifica dia esito positivo, il sistema LepidaID porta a termine il processo di autenticazione del minore presso il fornitore del servizio.

Nel caso in cui il servizio richiede l'autorizzazione del genitore:

- il minore chiede di accedere al servizio con SPID con gestore LepidaID;
- il fornitore di servizio invia al sistema LepidaID la richiesta di autenticazione;;
- il sistema LepidaID effettua la procedura di autenticazione del minore, comprendente anche le seguenti operazioni:
    - esegue la verifica di congruenza fra l'età richiesta dal servizio e l'età effettiva del minore: qualora la verifica dia esito negativo, la procedura di autenticazione è interrotta con esito negativo; qualora invece la verifica dia esito positivo, il sistema LepidaID continua la procedura di autenticazione;
    - se la verifica precedente ha avuto esito positivo, invia al minore la richiesta di conferma della sua volontà di chiedere al genitore richiedente l'autorizzazione all'accesso: qualora il minore non confermi tale volontà, la procedura di autenticazione è interrotta con esito negativo; qualora invece il minore confermi tale volontà, la procedura di autenticazione prosegue con i passaggi successivi;
    - se il minore ha confermato la sua volontà di chiedere al genitore l'autorizzazione all'accesso a quel servizio, invia al genitore richiedente una notifica contenente il nome e il cognome del minore, la denominazione del fornitore di servizio al cui servizio il minore ha chiesto di accedere, la data e l'ora della richiesta di accesso e la richiesta di autorizzazione all'accesso del minore; qualora il genitore richiedente non autorizzi l'accesso, la procedura di autenticazione è interrotta con esito negativo; qualora invece il genitore fornisca l'autorizzazione all'accesso, il sistema LepidaID porta a termine il processo di autenticazione del minore presso il fornitore di servizi.

Autorizzazione del genitore richiedente all'accesso ai servizi

Quando un minore accede con SPID ad un servizio per il quale è necessaria l'autorizzazione del genitore, il sistema LepidaID verifica se è già presente l'autorizzazione del genitore richiedente.

Nel caso in cui l'autorizzazione non sia presente (prima richiesta oppure già scaduta), il genitore richiedente riceve una richiesta di autorizzazione, tramite email, da parte del minore a lui associato per l'accesso al servizio di interesse; il genitore ha 24 ore per autorizzare l'accesso accedendo alla apposita funzione nella propria Area Riservata.

Qualora l'autorizzazione sia già stata fornita dal genitore richiedente e sia attiva, il sistema LepidaID verifica la presenza di autorizzazione, non chiede al genitore una nuova autorizzazione e permette direttamente l'accesso al minore.

L'autorizzazione all'accesso ad un servizio decade:

- su volontà esplicita del genitore richiedente;
- alla revoca della identità digitale SPID LepidaID del genitore richiedente;
- su richiesta del fornitore di servizi, ad esempio se cambiano le finalità del trattamento dei dati personali e/o le condizioni di erogazione dei servizi.

Effetti della cessazione dell'identità digitale di cui è titolare il genitore richiedente

In caso di decadenza (sospensione o revoca) dell'identità digitale SPID LepidaID del genitore richiedente, vengono automaticamente sospese le identità digitali SPID LepidaID associate al genitore richiedente, e decadono tutte le autorizzazioni attive per il minore / i minori a lui associate.

Il sistema LepidaID invia una comunicazione via email al minore / ai minori interessati per informarli dell'avvenuta sospensione della loro identità digitale SPID LepidaID e della relativa disabilitazione di tutte le autorizzazione in essere per l'accesso ai servizi.

9. Revoca o sospensione e riattivazione dell'Identità Digitale

In questo paragrafo vengono descritte le modalità con cui un utente può richiedere al Gestore di Identità Lepida la revoca e la sospensione della stessa.

La revoca rappresenta il processo che annulla definitivamente la validità delle Identità Digitali. Diversamente, la sospensione è associata ad 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 dall'indirizzo email utilizzato dall'utente per la registrazione.

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. Il modulo deve essere compilato e firmato digitalmente; qualora non si disponga di una firma digitale, si può porre una firma autografa al modulo di revoca o di sospensione, inviandolo a Lepida utilizzando uno dei due metodi sopra elencati, con allegato il documento di identità (lo stesso, se non scaduto, 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 eventuale denuncia presentata alle autorità giudiziaria)
2) Sospetto uso illecito dell'Identità Digitale

3) Volontà del titolare dell'Identità Digitale
4) Decesso della persona fisica titolare della Identità Digitale
5) Perdita della disponibilità del numero di cellulare o della email di contatto associato alla Identità Digitale
6) Altro.

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 dovrà allegare la denuncia presentata alle autorità giudiziarie.

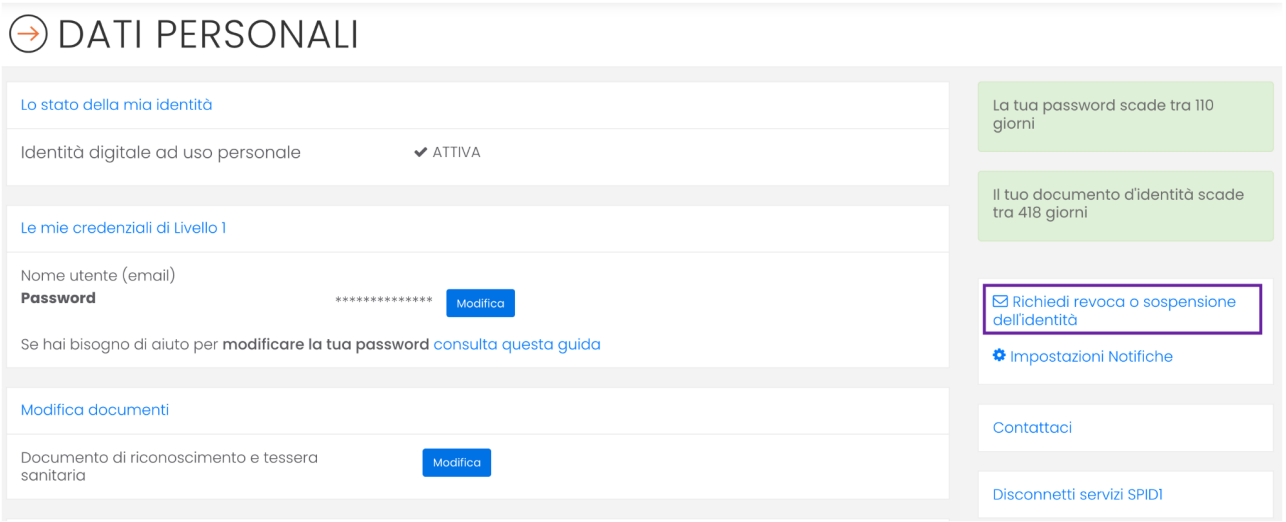
Nel caso di decesso della persona fisica titolare dell'Identità Digitale, i rappresentanti del soggetto titolare dell'identità deceduto (eredi o procuratore) devono presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'Identità Digitale.

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.

Nel caso dei minori, il genitore richiedente o il genitore non richiedente possono richiedere la sospensione o revoca della identità digitale del minore attraverso lo stesso modulo e allegando anche i documenti di identità, il proprio e quello del minore (gli stessi, se non scaduti, che sono stati utilizzati in fase di riconoscimento per l'attivazione dell'identità).



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.

Trascorsi trenta giorni dalla suddetta sospensione, il Gestore provvede al ripristino dell'identità precedentemente sospesa qualora non riceva copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione 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 e il recapito di telefonia mobile associati 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 e il recapito di telefonia mobile associati 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 nell'Area Riservata.

10. Gestione dei rapporti con gli utenti

Lepida mette a disposizione un servizio di helpdesk per supportare i Titolari di Identità Digitale SPID LepidaID sia in fase di registrazione al servizio che in fase di utilizzo e 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 verranno pubblicate sul sito del servizio LepdiaID (https://id.lepida.it) con adeguato anticipo.

11. 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.

11.1. 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 chiave segrete associate alle Identità Digitali:

- Le password vengono salvate sulla base dati utilizzando tecniche di hashing robusti (SHA-256, si SHA-512) 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.

Nell'ambito dell'utilizzo del protocollo OpenID Connect da parte del fornitore dei servizi online, è possibile mantenere attiva la sessione autenticazione su LepidaID per un massimo di 30 giorni, entro i quali il fornitore di servizi può richiedere al gestore di identità gli attributi ad ogni necessità, senza chiedere ulteriore autenticazione all'utente, ma un eventuale fattore di autenticazione locale oppure fattore biometrico, a discrezione del gestore di servizi stesso. Alla fine dei 30 giorni, la sessione verrà cancellata e sarà necessario richiedere all'utente di eseguire una nuova autenticazione.

L' instaurazione di una sessione lunga revocabile è attivabile da LepidaID su richiesta del fornitore di servizio ed è fornita informativa all'utente a valle della procedura di autenticazione. .

Le sessioni lunghe revocabili vengono revocate automaticamente a seguito del cambio password dell'identità digitale, a password scaduta, alla sospensione o revoca della identità.

Le sessioni lunghe revocabili possono essere gestite autonomamente dal titolare dell'identità LepidaID tramite una funzione "Disconnetti sessioni lunghe" disponibile nella propria Area Riservata. Il titolare visualizza le sessioni lunghe revocabili attive e può effettuare la revoca della sessione lunga attiva sullo specifico fornitore di servizi oppure la revoca massiva su tutti i fornitore di servizi, prima dei 30 giorni di naturale scadenza.

11.2. 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 inizialmente solo nelle versioni Android e IOS, successivamente anche nella versione 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 più di 2 caratteri identici consecutivi, 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.

12. 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.

13. 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.

13.1. 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 decreto legislativo 30 giugno 2003, n. 196

- Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione
- Effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'Identità Digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso
- Revocare l'Identità Digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona fisica
- 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 informarne l'utente via posta elettronicaIn 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, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta
- In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita;

- Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3 SPID
- Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, adottando idonee misure di sicurezza (art. 31 D.LGS 196/2003) ed utilizzando meccanismi di cifratura.

13.2. 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.

13.3. 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.

14. Documentazione

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

15. 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.

16. 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 corretto	HTTP Redirect ----- HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contatare il gestore del servzio"	Contattare il gestore del servizio	Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta	Parametri obbligatori: SAMLRequest SigAlg Signature Parametri non obbligatori: RelayState --------

									- Parametri obbligatori: SAMLRequest Parametri non obbligatori: RelayState
5	Verifica della firma fallita	http:Redirec t	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio “Impossibile stabilire l’autenticità della richiesta di autenticazione- Contatare il gestore del servzio”	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati
6	Binding su metodo HTTP errato	HTTP Redirect ------- - HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio “Formato richiesta non ricevibileCont	Contattare il gestore del servizio	Verificare metadata Gestore dell'identita (IdP)	invio richiesta in HTTP-Redirect su entrypoi

						atare il gestore del servzio"			nt HTTP-POST dell'identity ---------- invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity
Anomalie sul formato della AuthnReq									
7	Errore sulla verifica della firma della richiesta	HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Conttatare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o non corrispondente ad un fornitore di servizi riconosciuto o non associat

									o al corretto EntityID nei metadati registrat
8	Formato della richiesta non conforme alle specifiche SAML	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:RequesterErrorCode 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 alla verifica positiva della firma
9	Parametro version non presente, malformato o diverso da '2.0'	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch ErrorCode nr09	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente	
10	Issuer non presente, malformato o non corrispondete all'entità che	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	

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

16	AssertionConsumerService non correttamente valorizzato	HTTP POST/HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr16	Fornitore del servizio (SP)	n.a	n.a	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	AssertionConsumerServiceIndex presente e attualizzato con valore non riportato nei metadata AssertionConsumerServiceIndex riportato in presenza di uno od entrambi gli attributi AssertionConsumerServiceURL e Protocol Binding AssertionConsumerServiceIndex non presente in assenza di almeno uno attributi AssertionConsumerServi

									ceURL e Protocol Binding La respons e deve essere inoltrata presso AssertionConsumerService di default riportato nei metadata
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	AttributeConsumerServiceIn dex malformato o che riferisce a un	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	

	valore non registrato nei metadati di SP								
Anomalie derivante dall'utente									
19	Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero tentativi secondo le policy adottate)	HTTP POST HTTP Redirect	n.a	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19	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 determinato il mancato accesso al servizio richiesto	Si danno indicazioni specifiche e puntuali all'utente per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi di determinate condizioni legate alle policy di sicurezza aziendali, ad esempio dopo 3 tentativi falliti, si risponde al SP.
20	Utente privo di credenziali	HTTP POST HTTP Redirect	n.a	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:name	Fornitore del servizio (SP)	n.a	acquisire credenziali di livello idoneo all'accesso al	Fornire una pagina di cortesia notificando	

	compatibili con il livello richiesto dal fornitore del servizio			s:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20			servizio richiesto	all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
21	Timeout durante l'autenticazione utente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21	Fornitore del servizio (SP)	n.a.	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinati periodo di tempo	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
22	Utente nega il consenso all'invio di dati al SP in caso di sessione vigente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22	Fornitore del servizio (SP)		Dare consenso	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1.
23	Utente con identità sospesa /revocata o con credenziali bloccate	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Credenziali sospese o revocate"		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
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 presente	HTTP POST	n.a.	ErrorCode nr27	Fornitore del servizio (SP		Utente già in possesso 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		

Per quanto riguarda i codici dei messaggi di anomalie nel caso di protocollo OpenID Connect, si faccia riferimento alle relative regole tecniche pubblicate da AGID.