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

1.2 Scopo del documento

Il presente manuale illustra l’architettura, le modalità, le procedure adottate dal gestore Lepida ScpA 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 http://www.agid.gov.it/sites/default/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 http://www.agid.gov.it/sites/default/files/circolari/regolamento_modalita_attuative_spid_2.0.pdf
Regole tecniche (art.4, comma 2 DPCM 24 ottobre 2014)	Regolamento recante le regole tecniche http://www.agid.gov.it/sites/default/files/circolari/spid-regole_tecniche_v1.pdf
Accreditamento Gestori (art.1, comma 1, lettera I DPCM 24 ottobre 2014)	Regolamento recante le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale http://www.agid.gov.it/sites/default/files/circolari/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).	

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 ScpA 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 ScpA 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 del Responsabile del Manuale Operativo:

Kussai Shahin

Indirizzo Via della Liberazione, 15 - 40128 Bologna (BO)

Centralino e Segreteria +39 051 63388 00

Fax +39 051 9525156

Numero Verde 800 44 5500

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 ScpA è composta dai seguenti principali componenti, denominati come segue:

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

I due componenti (IdM e IdP), per quanto distinti sia nell'architettura sia dal punto di vista funzionale presentano come unico punto in comune la condivisione della stessa base dati contenente le identità degli utenti interessati.

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

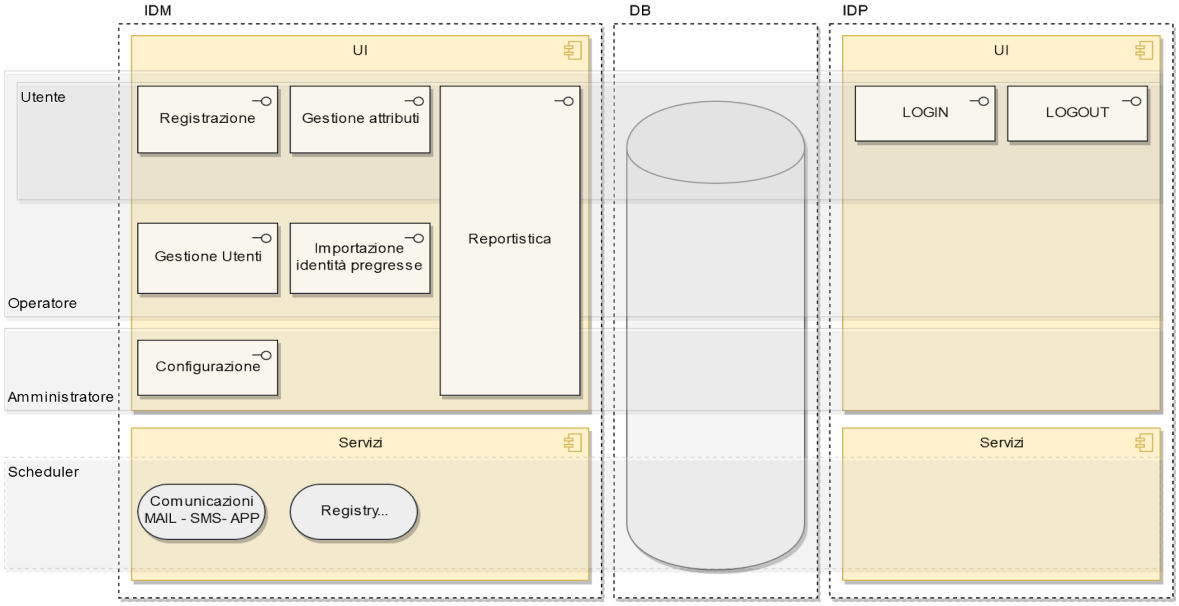
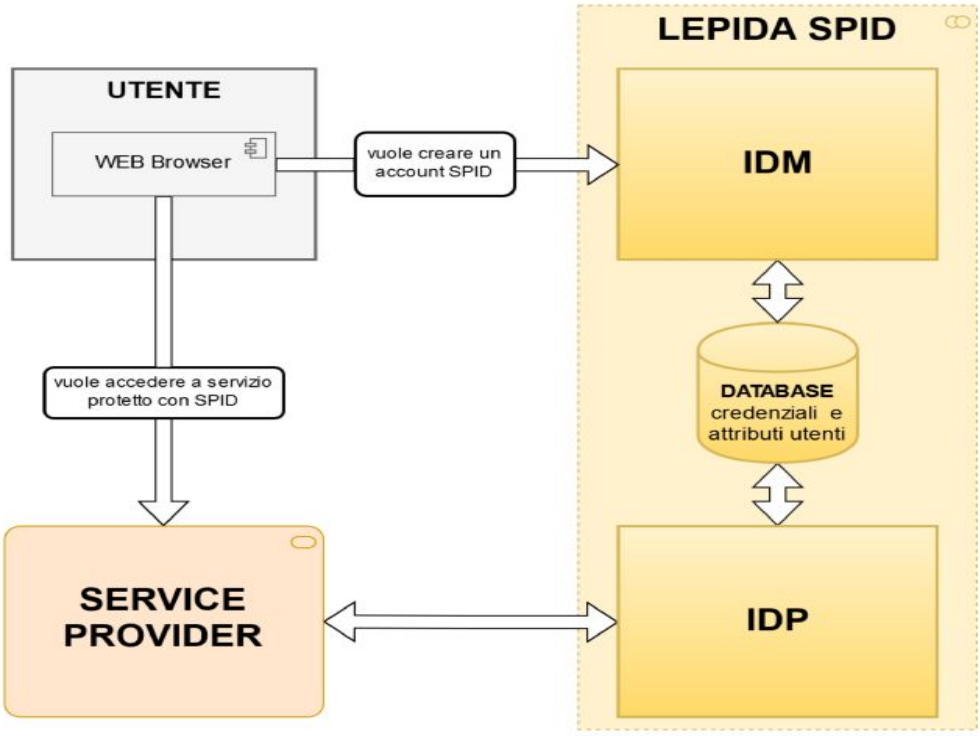
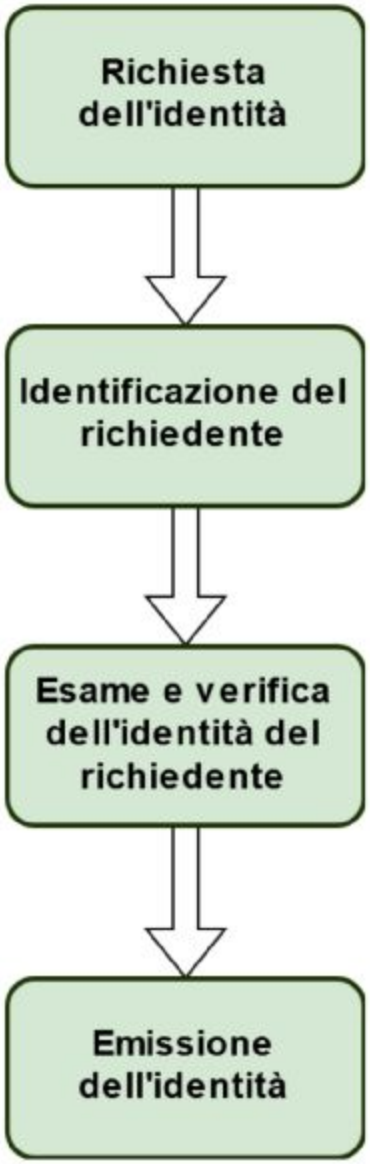


Diagramma logico del Gestore di Identità Lepida ScpA



Flusso di gestione identità digitale

Il diagramma seguente 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

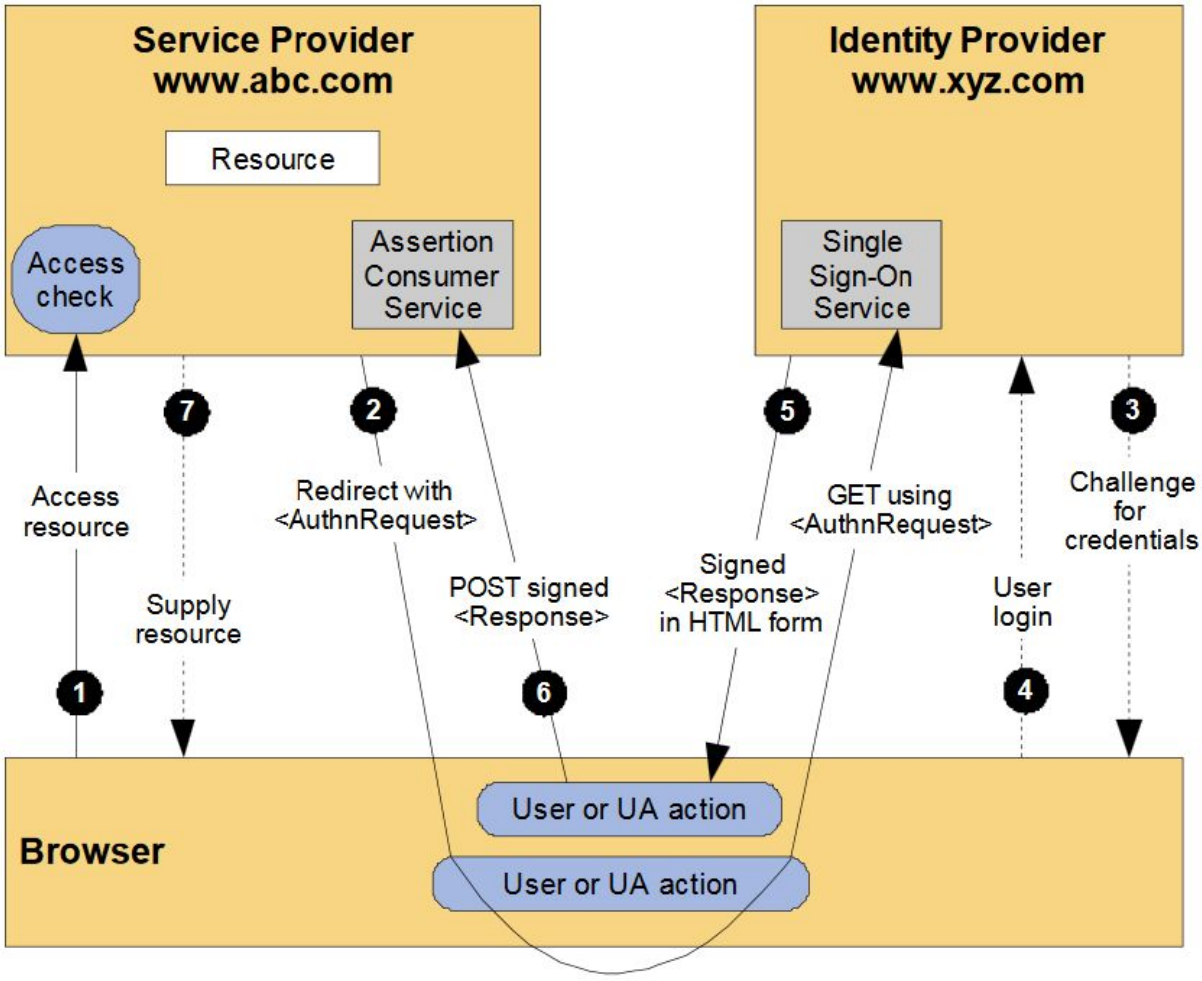
Per la descrizione dell'architettura di dispiegamento, si rimanda al manuale di sicurezza del Gestore di Identità Lepida ScpA.

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.



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.

Per la descrizione dell'architettura del sistema di autenticazione si rimanda al manuale di sicurezza del Gestore di Identità Lepida ScpA.

5.3 Descrizione dei codici e dei formati dei messaggi di anomalia

Come indicato dalla normativa fornita da AgID, il Gestore di Identità Lepida ScpA 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) dell' IDP di Lepida ScpA.

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 Tracciatura 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 mail).

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 ScpA mantiene un Registro delle transazioni contenente i tracciati delle richieste di autenticazione 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;
- *AuthnReques*t: Authentication request arrivata dal SP, codificata in formato base64 e compressa con algoritmo deflate;
- *AuthnRequestID*: Attributo "ID" contenuto nell'authentication request arrivata dal SP;
- *AuthnRequestIssue*r: Tag "Issuer" presente nell'authentication request arrivata dal SP;
- *AuthnRequestIssueInstant*: Attributo "IssueInstant" presente nell'authentication request originale arrivata dal SP;
- *AuthnRequestBinding*: Binding HTTP utilizzato dal SP per inviare l'authentication request, valorizzata con "HTTP-REDIRECT" o con "HTTP-POST";
- *Response*: Response generata dall'IdP, codificata in formato base64 e compressa con algoritmo deflate;
- *ResponseID*: Attributo "ID" presente nella response generata dall'IdP;
- *ResponseIssueInstant*: Attributo "IssueInstant" presente nella response generata dall'IdP;
- *SpidCode*: Attributo utente "spidCode";
- *AssertionID*: Attributo "ID" del tag "Assertion" presente nella response generata dall'IdP;
- *AssertionSubjectNameID*: Tag "NameID", sottonodo del tag "Subject" (a sua volta sottonodo del tag "Assertion") presente nella response generata dall'IdP.

Il registro viene mantenuto su file csv ed aggiornato in tempo reale contestualmente alle attività degli utenti sul sistema. Il contenuto del file risulta protetto dagli accessi non autorizzati mediante opportune politiche di offuscamento. Il file di registro, come da normativa, contiene i

log delle attività degli ultimi 24 mesi. Uno specifico job si occupa di eliminare dal file i contenuti via via divenuti obsoleti.

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 ScpA tramite PEC all'indirizzo lepidaid@pec.lepida.it .

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 ScpA 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 dei proprie autenticazioni. L'accesso avviene con LIV 2 SPID.

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

6 Guida Utente

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

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

7.1 Richiesta dell'identità digitale

Lepida ScpA 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, disponibile 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;
- telefono cellulare;
- pec (opzionale).

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

- l'identificazione del soggetto richiedente;
- verifica dei dati e dell'identità dichiarata;
- attivazione dell'identità digitale.

Nel caso di **richiesta di adesione assistita**, 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, il terzo dal caricamento di una scansione fronte/retro del documento di identità e della tessera sanitaria, 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 mail, pec o via cellulare contenente un codice casuale da inserire in una specifica form dell'area riservata.

La **richiesta di adesione assistita** consiste nel supporto al soggetto richiedente di un operatore di sportello abilitato nella registrazione svolgendo 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 la tessera sanitaria 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.
- Termina la prima fase.
- Il cittadino, in un momento successivo alla prima fase, accedendo al proprio profilo creato nella prima fase accedendo ad un link personalizzato, effettua la validazione dell'indirizzo di posta elettronica (passaggio ritenuto utile per le persone che non dispongono di uno smartphone ad esempio), effettua la validazione del numero di cellulare (se non era disponibile nella prima fase).
- Terminata la seconda fase, la registrazione è completata e il soggetto è automaticamente attivato in quanto tutte le verifiche necessarie sono già state effettuate nella prima fase.

Lepida ScpA 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 l'autenticazione a due fattori, il Gestore di Identità Lepida ScpA prevede due possibilità:

- la generazione di one time password (OTP) e l'invio via SMS al numero di telefono indicato e verificato in fase di registrazione;
- l'utilizzo della APP LepidaID installata sullo smartphone dell'utente.

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 ScpA rende disponibile un servizio base gratuito per tutti i cittadini con documenti di identità rilasciati da un'autorità italiana (carta d'identità, passaporto, patente) due 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. In caso di richiesta da parte dell'utente di identificazione tramite CNS, il sistema avvia una apposita procedura di verifica della carta. 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.

Inoltre, Lepida ScpA rende disponibile anche la possibilità di effettuare:

- **l'identificazione a vista del soggetto richiedente**, 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 ScpA, esibendo un documento di identità valido. 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, munito di fotografia e firma autografa dello stesso e controlla la validità del codice fiscale verificando la tessera sanitaria anch'essa in corso di validità. A dimostrazione dell'avvenuta identificazione a vista devono essere caricate sul sistema la scannerizzazione fronte/retro del documento di identità e della tessera sanitaria 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".

- **L'identificazione a vista da remoto 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 ScpA 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 della tessera sanitaria).

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.

Gli operatori di Lepida ScpA, nella propria area riservata, a cui accedono esclusivamente tramite le proprie credenziali SPID 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 o da remoto del soggetto richiedente) o già effettuata in fase di invio della richiesta (nel caso di identificazione tramite smartcard o documento firmato digitalmente). 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 ScpA 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 ScpA, 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 la tessera sanitaria, caricati sul sistema, siano integri e in corso di validità. Il documento di identità deve essere rilasciato da una amministrazione dello stato, 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, una volta disponibile.

Occorre verificare anche la corrispondenza dei dati caricati online sul profilo dell'utente e presenti sui documenti presentati. Si fa presente che in caso di identificazione tramite Smart Card viene verificata automaticamente la corrispondenza del Codice Fiscale dichiarato e quello contenuto nella carta.

Gli operatori di Lepida ScpA 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 o 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 dall'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

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 e massima di 16 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;

- sconsigliato 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 ScpA oltre alla password composta come sopra, adotta anche l'invio di 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.

8 Revoca e sospensione dell'identità digitale

In questo paragrafo vengono descritte le modalità con cui un utente può richiedere al Gestore di Identità Lepida ScpA 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, la revoca o la riattivazione a seguito di una sospensione della propria Identità digitale attraverso una delle seguenti modalità:

a) richiesta al gestore inviata via PEC all'indirizzo lepidaid@pec.lepida.it;

b) richiesta al gestore inviata via posta elettronica dall'indirizzo email utilizzato dall'utente per la registrazione.

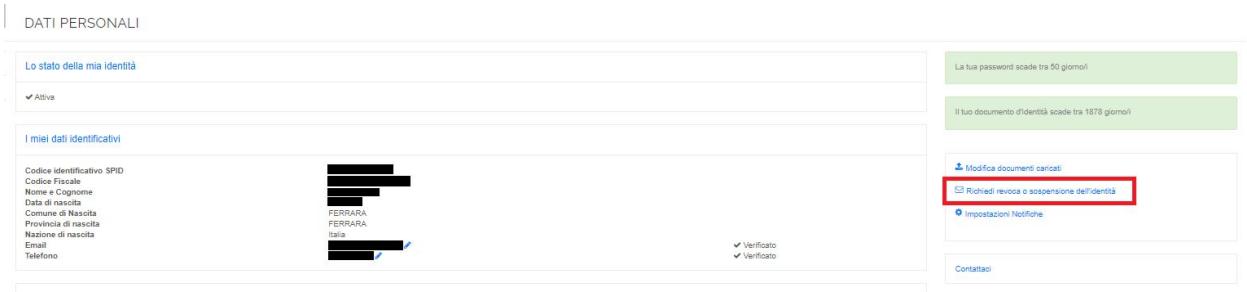
La richiesta deve includere il modulo di richiesta di sospensione e revoca disponibile sul sito https://id.lepida.it. Il modulo deve essere firmato digitalmente nel caso di invio via posta elettronica. Qualora non si disponga di una firma digitale, si può porre una firma autografa al modulo di revoca o di sospensione, inviandolo al Gestore di Identità Lepida ScpA 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 800.445500 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) uso illecito dell'identità digitale;
3) volontà dell' utente.

Nel casi previsti dai punti 1 e 2, 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.



Richiesta di revoca o sospensione dell'identità digitale

Il Gestore 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 decesso della persona fisica, il gestore dell'identità digitale procede alla revoca dell'identità digitale, previo accertamento operato anche utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM. In assenza di disponibilità dei predetti servizi, è cura dei rappresentanti del soggetto utente (erede o procuratore) presentare la documentazione necessaria all'accertamento della cessata sussistenza dei presupposti per l'esistenza dell'identità digitale. Il gestore, una volta in possesso della documentazione suddetta, procede tempestivamente alla revoca.

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.

In caso di identità non attiva per un periodo superiore a 24 mesi e scadenza contrattuale, 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.

9 Gestione dei rapporti con gli utenti

Lepida ScpA mette a disposizione un servizio di helpdesk per supportare i Titolari di Identità Digitale sia in fase di registrazione al servizio che in fase di utilizzo e accesso ai servizi.

Lepida ScpA mette a disposizione dell'utente tre diversi canali di accesso al servizio di assistenza:

- Via telefono attraverso il numero verde 800 445500
- Via email attraverso l'indirizzo email helpdesk@lepida.it
- Via web attraverso l'utilizzo del form online accessibile all'URL: https://id.lepida.it

Il servizio di helpdesk è disponibile dal lunedì a venerdì dalle ore 8:30 alle ore 18:30 e al sabato dalle ore 8:30 alle ore 13:30.

Eventuali comunicazioni e avvisi di interventi o modifiche alle condizioni del servizio o alle modalità di erogazione del servizio verranno pubblicate sul sito https://id.lepida.it con adeguato anticipo.

10 Descrizione generale delle misure anti-contraffazione

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

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

10.1 Livello 1 SPID

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

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

- La password deve risultare compatibile alle comuni precauzioni sul formato e deve essere vietato 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 e massima di 16 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 ed al fine di evitare utilizzi impropri delle identità digitali, Lepida ScpA 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 ScpA secondo le modalità definite dai processi ISO27001 previsti nella stessa;

10.2 Livello 2 SPID

Il livello di sicurezza SPID 2 è implementato attraverso un sistema a due fattori: l'utilizzo della verifica di una password , con le stesse caratteristiche previste per il livello SPID 1, e l'adozione di una OTP (One Time Password), la cui validità è limitata solo ad una transazione nell'ambito della sessione applicativa. Lepida ScpA permette l'invio della OTP attraverso un messaggio SMS al numero di telefono inserito in fase di registrazione oppure la relativa generazione attraverso la APP LepidaID, associata all'account utente.

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.

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.

11 Descrizione generale del sistema di monitoraggio

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

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

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

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

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

Le console di monitoraggio sono configurate per il continuo controllo, produzione di allarmi e

periodicamente si produce la reportistica dei controlli effettuati.

12 Obblighi del Gestore e dei Titolari dell'Identità Digitale

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

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

12.1 Obblighi del Gestore dell'Identità Digitale

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

- rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo modulo di richiesta;
- verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale;
- conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione 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;
- verifica degli attributi identificativi del richiedente;
- consegnare in modalità sicura le credenziali di accesso all'utente;
- conservare la documentazione inerente al processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale;
- cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale;
- trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;
- verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione;
- effettuare tempestivamente e a titolo gratuito su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso;
- revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona fisica;
- segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente;
- verificare la provenienza della richiesta di sospensione da parte dell'utente (escluso se inviata tramite PEC o sottoscritta con firma digitale o firma elettronica qualificata);
- fornire all'utente che l'ha inviata conferma della ricezione della richiesta di sospensione
- sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni ed informarne il richiedente;
- rispristinare o revocare l'identità digitale sospesa, nei casi previsti;
- revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione;
- utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo o internazionale;
- adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso;
- effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta;
- effettuare con cadenza almeno annuale un'analisi dei rischi;

- definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID;
- allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato;
- condurre con cadenza almeno semestrale il *Penetration Test;*
- garantire la continuità operativa dei servizi afferenti allo SPID;
- effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di un'apposita struttura interna;
- garantire la gestione sicura delle componenti riservate delle identità digitali assicurando 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 o via sms, 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 elettronica e numero di telefono mobile;
- in caso di decesso del titolare (persona fisica), revocare previo accertamento l'identità digitale;
- nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale;
- trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione;

- nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale;
- ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente;
- in caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale;
- proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure richieste dalla normativa;
- all'approssimarsi della eventuale scadenza dell'identità digitale, 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;

12.2 Obblighi del Titolare dell'Identità Digitale

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

- esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione;
- si obbliga all'uso esclusivamente personale delle credenziali connesse all'Identità Digitale;
- si obbliga a non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti. A tale proposito, si precisa che l'utente è tenuto ad adottare tutte le misure tecniche e organizzative idonee ad evitare danni a terzi;
- si obbliga a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine;
- deve garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi;
- l'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private;
- sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite;

- fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci;
- accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze;
- informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati;
- mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi:
    - estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale;
- conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i rischi seguenti:
    - divulgazione, rivelazione e manomissione;
    - furto, duplicazione, intercettazione, cracking dell'eventuale token associato all'utilizzo dell'identità digitale;
    - accertarsi dell'autenticità del fornitore di servizi o del gestore dell'identità digitale quando viene richiesto di utilizzare l'identità digitale;
- attenersi alle indicazioni fornite dal Gestore in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele che da adottare per la conservazione e protezione delle credenziali;
- in caso di smarrimento, furto o altri danni/compromissioni (con formale denuncia presentata all'autorità giudiziaria) richiedere immediatamente al Gestore la sospensione delle credenziali;
- in caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto richiedere immediatamente al Gestore la sospensione delle credenziali;

12.3 Responsabilità

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

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

13. Documentazione

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

14 Cessazione IDP

Lepida ScpA 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 ScpA procede con la revoca delle identità digitali rilasciate e per le quali non si è avuto subentro.

15. Appendice A - Codici e Messaggi di anomalia

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:Redirect	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 Redirec	HTTP 403	n.a.	Utente	Pagina di cortesia	Contattare il gestore del	Verificare metadata	invio richiesta in

	HTTP errato	t -------- HTTP POST				con messaggio “Formato richiesta non ricevibileContatare il gestore del servzio”	servizio	Gestore dell'identita (IdP)	HTTP-Redirect su entrypoint 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 associato 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:Requester ErrorCode nr08	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente	Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente 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	HTTP POST/ HTTP Redirec	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio	Contattare il gestore del servizio	Verificare formato delle richieste prodotte	

	corrispondente all'entità che sottoscrive la richiesta	t				“Formato richiesta non corretto - Contattare il gestore del servizio”			
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	RequestAuthnContext non presente, malformato o non previsto da SPID	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:statuss:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: “Autenticazione SPID non conforme o non specificata”		Informare l'utente	Auth livello richiesto diverso da: urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3
13	IssueInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP POST/ HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
14	destination non presente, malformata o non coincidente con ill Gestore	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	

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

	non valorizzato secondo specifica			upp orted ErrorCode nr17				all'utente	procede con l'autenticazione senza riportare errori
18	AttributeConsumerServiceIn dex malformato o che riferisce a un valore non registrato nei metadati di SP	HTTP POST HTTP Redirect	n.a	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18	Fornitore del servizio (SP)	n.a.	n.a.	riformulare la richiesta con un valore dell'indice presente nei metadati	
Anomalie derivante dall'utente									
19	Autenticazione fallita per ripetuta sottomissione di 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 compatibili con il livello richiesto dal fornitore del servizio	HTTP POST HTTP Redirect	n.a	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20	Fornitore del servizio (SP)	n.a	acquisire credenziali di livello idoneo all'accesso al servizio richiesto	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
21	Timeout durante l'autenticazione utente	HTTP POST HTTP Redirec	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names	Fornitore del servizio (SP)	n.a.	Si ricorda che l'operazione di autenticazione deve essere	Fornire una pagina di cortesia notificando	

		t		:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21			completata entro un determinati periodo di tempo	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	HTTP	n.a.	ErrorCode nr27	Fornitore		Utente già in		

	presente	POST			del servizio (SP		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		