Allegato Tecnico FedERa

release: 3
data: 10.11.2017

redazione documento: Vania Corelli Grappadelli
verifica documento: Kussai Shahin
approvazione documento: Gianluca Mazzini

Nota di lettura

LepidaSpA si riserva la facoltà di poter intervenire sulle misure tecniche e organizzative descritte nel presente documento, al fine di rendere il sistema conforme alle successive indicazioni normative che dovessero subentrare in argomento. Si riserva inoltre di intervenire per la correzione di meri errori materiali o refusi.

Si fa presente che LepidaSpA è impegnata, su mandato di Regione Emilia-Romagna, nella valorizzazione delle identità digitali FedERa attraverso l'evoluzione di LepidaSpA verso un IDP (Identity Provider) SPID (Sistema Pubblico Identità Digitale) accreditato secondo le normative previste.

1. Descrizione del servizio

1.1 Definizione e Acronimi

- Community Network dell'Emilia-Romagna (CNER): con la Delibera DGR 758/2013 è stata approvata la Nuova convenzione per il funzionamento, la crescita e lo sviluppo della Community Network Emilia-Romagna (CNER) per creare le condizioni organizzative per dare attuazione alle finalità e ai progetti contenuti nel Piano Telematico dell'Emilia-Romagna, ora AdER Agenda Digitale dell'Emilia-Romagna, è un'aggregazione territoriale su base regionale (Art. 30 TUEL), con propria sede (presso la sede della Regione Emilia-Romagna, cui è conferito potere di rappresentanza della CNER stessa), con una governance solida e partecipata, affidata al "Comitato Permanente di Indirizzo e Coordinamento con gli enti locali" (Art. 6, comma 4 LR 11/04), e con uno specifico ruolo attivo da parte della Società LepidaSpA;
- Comitato Permanente di Indirizzo e Coordinamento (CPI): il Comitato Permanente di Indirizzo e Coordinamento con gli Enti locali, istituito con la Legge Regionale n.11/2004 e successive modifiche e integrazioni, è organismo della Community Network dell'Emilia-Romagna;
- Comitato Tecnico (CT): il Comitato Tecnico, istituito dalla Legge Regionale n. 11/2004 e successive modifiche e integrazioni , la cui composizione è disciplinata con apposita delibera della Giunta regionale, opera a supporto delle attività del CPI;
- Utente: soggetto al quale viene rilasciata un'identità digitale con la quale potrà richiedere l'accesso ai servizi erogati dal Service Provider (SP); l'utente in tale contesto opera per il tramite del proprio browser;

- Service Provider (SP): soggetto che eroga un servizio all'utente che si sia autenticato per il tramite dell'identità digitale rilasciata dall'IdP (Identity Provider). Ai fini del D.lgs. 196/2003 Il Service Provider è titolare del trattamento dei dati di propria competenza effettuato per le proprie finalità istituzionali;
- Identity Provider (IdP): soggetto che nell'ambito della federazione FedERa o del sistema SPID è abilitato a rilasciare un'identità digitale all'utente e a verificarla; l'identità digitale consentirà all'utente di autenticarsi al Service Provider (SP) il quale nel rispetto delle proprie policy potrà consentire l'accesso ai propri servizi erogati e integrati in FedERa. Ai fini del D.lgs. 196/2003 l'IdP è titolare del trattamento dei dati di propria competenza effettuato per le proprie finalità istituzionali;
- identità digitale: la rappresentazione informatica della corrispondenza biunivoca tra un utente e suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale;
- autenticazione informatica: verifica effettuata dal gestore dell'identità digitale, su richiesta del fornitore di servizi, della validità delle credenziali di accesso presentate dall'utente al fine di convalidarne l'identificazione informatica;
- Gateway (GW): il sistema che permette il colloquio tra i service provider e gli identity provider per la verifica dell'identità per l'accesso ai servizi;
- Gestore del Gateway: soggetto che gestisce il Gateway (LepidaSpA); ai fini del D.lgs. 196/2003 il Gestore del gateway è titolare del trattamento dei dati di propria competenza effettuato per le proprie finalità istituzionali;
- Federazione: insieme dei soggetti, strumenti, regole e sistema di governo che intervengono nell'ambito di FedERa e finalizzata a fornire agli utenti accesso a servizi telematici, attraverso l'utilizzo di una credenziale elettronica unica (Identità digitale) riconosciuta come valida all'interno della federazione stessa;
- Soggetto Aderente a FedERa: il Soggetto Aderente – di natura pubblica e privata - può essere un IdP o un SP sottoscrittore del protocollo di adesione alla federazione;
- SPID: Sistema pubblico dell'identità digitale di cittadini e imprese, istituito ai sensi del Codice Amministrazione Digitale (CAD);
- Ente Aderente a SPID: Soggetto Aderente a SPID in virtù dell'adesione alla CNER e della Convenzione per l'adesione delle pubbliche amministrazioni a SPID stipulata in data 21 del mese di Aprile dell'anno 2016 stipulata tra AgID, Regione Emilia-Romagna e LepidaSpA (quest'ultimo in qualità di soggetto attuatore).

1.2 Descrizione generale

FedERa (Federazione degli Enti dell'Emilia-Romagna per l'Autenticazione) è l'infrastruttura tecnica ed organizzativa della CNER realizzata e gestita da LepidaSpA, su mandato di Regione Emilia-Romagna, sulla base della piattaforma tecnologica FedERa e dei relativi servizi.

In forza di quanto disposto dalla LEGGE REGIONALE 24 maggio 2004, n. 11 SVILUPPO REGIONALE DELLA SOCIETÀ DELL'INFORMAZIONE e ss.mm.e.ii. che all'art. 14 c.5 definisce: *"Le attività di nodo tecnico-informativo centrale possono essere svolte dalla società "LEPIDA" S.p.A. di cui all'articolo 10, che in tal caso è titolare autonomo del trattamento dei dati. Le informazioni acquisite sono utilizzate nel rispetto delle disposizioni vigenti, anche in materia di consultazione delle banche dati, osservando le misure di sicurezza ed i vincoli di riservatezza previsti dal decreto legislativo n. 196 del 2003."* il sistema fedERa è gestito da LepidaSpA .
Il governo della Federazione è demandato: alla Regione Emilia-Romagna, alla CNER, la quale opera anche per il tramite del proprio rappresentante; al CPI; al CT e a LepidaSpA.

Il servizio FedERa prevede due componenti principali:

- servizio di rilascio e gestione di identità digitali (credenziali) ai cittadini;
- servizio di GW che permette l'accesso ai servizi telematici esposti da SP utilizzando i servizi di autenticazione offerti dagli IdP fedERa e SPID.

1.2.1. Identità digitali

LepidaSpA sta predisponendo un aggiornamento dell'impianto tecnico ed organizzativo di FedERa per evolvere le identità digitali FedERa in identità digitali SPID attraverso l'accreditamento di LepidaSpA come un IDP SPID, secondo le modalità previste dalle normative, per la gestione delle identità digitali del territorio emiliano romagnolo. Il modello tecnico organizzativo prevede per gli enti il ruolo di sportello di Registration Authority (RA) presso la propria sede dove il cittadino può essere identificato e può ricevere le credenziali per utilizzare le propria identità digitale.

Le identità digitali (credenziali) FedERa sono rilasciate e gestite secondo un modello tecnico-organizzativo riportato in Appendice 1 che sarà oggetto di revisione ed evoluzione per garantire il rispetto dei requisiti e delle specifiche SPID.

1.2.2. Gateway FedERa

LepidaSpA ha provveduto all'integrazione della piattaforma regionale FedERa con SPID garantendo l'adesione di tutti gli Enti della regione Emilia-Romagna a SPID, attraverso una integrazione centralizzata unica per tutti gli Enti valorizzando il modello e la scelta tecnologica di FedERa adottata in Emilia-Romagna e l'esperienza consolidata di collaborazione tra gli Enti del territorio nell'ambito dell'Agenda Digitale dell'Emilia-Romagna.

Il Gateway FedERa garantisce infatti l'adesione di tutti gli Enti della Community Network a SPID attraverso l'integrazione centralizzata con gli IDP SPID accreditati per la verifica delle identità digitali necessaria per l'accesso ai servizi federati.

1.3 Privacy e trattamento dei dati: ruoli e responsabilità

In forza di quanto disposto dalla LEGGE REGIONALE 24 maggio 2004, n. 11 SVILUPPO REGIONALE DELLA SOCIETÀ DELL'INFORMAZIONE il sistema fedERa è gestito da LepidaSpA come nodo tecnico-informativo centrale in qualità di delegato degli enti federati appartenenti alla CNER a svolgere in maniera centralizzata il servizio di Gestore dell'Identità digitale oppure come servizio erogato agli Enti soci. In ogni caso agisce come delegato e condivide la co-titolarità dei dati relativi alle identità digitali con gli Enti.

Lo svolgimento di questa funzione prevede il trattamento di dati personali, nello specifico di quelli relativi agli utilizzatori del sistema e a quelli abilitati all'accesso al cruscotto di backend, secondo il relativo profilo. LepidaSpA nella sua funzione di gestore della piattaforma fedERa ha visibilità di tutte le attività registrate nel sistema relativamente ai servizi e per questo deve essere nominata da parte di ogni singolo Ente che utilizza fedERa quale responsabile esterno della verifica della conformità degli accessi nel rispetto di quanto definito nel presente documento, ma anche secondo i più generali principi contenuti nel d.lgs 196/03 (necessità, pertinenza e non eccedenza).

Il modello tecnico e organizzativo presentato in Appendice 1 non prevede alcuna comunicazione diretta di dati personali fra i Soggetti Aderenti alla federazione. È, invece, l'interessato che comunica i dati che lo riguardano a ciascuno dei Soggetti, configurandosi così solo uno scambio di dati fra titolare di trattamento e interessato. Nell'esecuzione della richiesta dell'utente, interessato, avvengono trattamenti da parte di tutti e tre i soggetti coinvolti nell'erogazione: provider del servizio, gestore del gateway, provider dell'identità. Ogni soggetto è titolare del trattamento dei dati di propria pertinenza collegati all'espletamento del servizio richiesto dall'utente e deve adempiere agli obblighi previsti dalla normativa.

1.4 Descrizione dei servizi offerti

I servizi offerti da LepidaSpA nell'ambito di FedERa vengono di seguito descritti.

1.4.1. Servizio di rilascio e gestione di identità digitali

Il servizio riguarda principalmente la gestione e il mantenimento della federazione degli IDP esistenti nelle more dell'evoluzione verso IDP SPID.
La federazione riguarda sistemi di gestione di identità in disponibilità degli Enti oppure l'utilizzo di un sistema di gestione utenti in modalità ASP messo a disposizione da LepidaSpA attraverso la piattaforma FedERa. In entrambi i casi l'Ente svolge il ruolo di Registration Authority (Gestore Identità) permettendo agli utenti l'accesso ai servizi federati, nel rispetto dei livelli di affidabilità e password policy definiti nell'ambito della federazione.

Nel caso dell'utilizzo del sistema di gestione utenti in modalità ASP, viene messa a disposizione dell'Ente una procedura informatica di rilascio e successiva gestione delle credenziali. Il sistema consente di gestire tramite un applicativo web un proprio dominio di utenti, identificato da un nome di dominio univoco. Gli operatori dell'ente possono registrare nuovi utenti e rilasciare ad essi credenziali di accesso del tipo username e password tramite le procedure previste nella federazione. Si fa presente che è possibile effettuare una procedura automatica di migrazione di utenti da una base dati di IdP esterno a fedERa, purché l'Ente sia in possesso degli attributi obbligatori associati all'identità digitale.

1.4.2. Servizio di GW per l'accesso ai servizi telematici esposti da SP

Il servizio permette l'accesso ai servizi telematici esposti dagli SP federati utilizzando i servizi di autenticazione offerti dagli IdP fedERa e SPID.
La federazione di un SP, ovvero di un Ente che dispone di un servizio online, può prevedere anche l'attivazione di una ACL (Access Control List), tramite la quale l'operatore SP può decidere i criteri secondo i quali permettere l'accesso al servizio, definendo quali valori devono assumere determinati attributi del profilo utente affinché venga concesso all'utente l'accesso al servizio offerto dall' SP. In questa maniera un SP può permettere l'accesso al servizio solo a determinati utenti (impostando ad esempio un criterio sull'attributo "CodiceFiscale", che deve corrispondere ad uno dei codici fiscali delle sole persone scelte), oppure soltanto ad una determinata categoria di utenti.
Si fa presente che nel caso di SPID gli attributi per ciascuno SP vengono definiti all'attivazione della federazione e non posso subire modifiche se non previa una procedura legata al funzionamento di SPID.
Si evidenzia che il sistema SPID prevede che, per ogni servizio telematico erogato delle pubbliche amministrazioni (SP), venga definito, a cura del SP, il livello di sicurezza SPID necessario per l'accesso al servizio. LepidaSpA fornisce supporto agli Enti per la determinazione del livello di sicurezza SPID per ciascun servizio coerentemente con le indicazioni nazionali. A tal fine, si ricorda che i livelli di sicurezza per l'autenticazione e l'accesso ai servizi in SPID sono tre: autenticazione a un fattore, ovvero password; autenticazione a due fattori non basati necessariamente su certificati digitali, ad esempio password e OTP (one time password); autenticazione a due fattori basati su certificati digitali, ad esempio smart card.

La piattaforma FedERa permette di federare anche sistemi di gestione di attributi e dispone inoltre di un meccanismo di gestione di attributi in modalità ASP, il tutto per permettere di definire attributi certificati associati alle identità digitali. Queste funzionalità dovranno evolvere a seconda dell'evoluzione delle modalità di gestione degli attributi in SPID.

2. Attivazione dei servizi

L'attivazione del servizio FedERa richiede la nomina da parte dell'Ente, e la comunicazione a LepidaSpA, di un proprio referente per il servizio FedERa che sarà il soggetto titolato a richiedere, attraverso le modalità nel seguito descritte, l'attivazione dei servizi e verificarne la corretta implementazione. L'Ente si impegna a comunicare il proprio referente al momento dell'adesione al servizio e a comunicare tempestivamente a LepidaSpA eventuale variazione del referente.

L'attivazione dei servizi di FedERa richiede come prerequisito tecnologico l'adozione del protocollo di autenticazione SAML2.0, da parte degli SP e degli IdP, per le comunicazioni con il GW fedERa e la predisposizione dei propri sistemi secondo il modello tecnico organizzativo di FedERa. Si fa presente che l'evoluzione di SPID, sia dal punto di vista tecnologico che tecnico-organizzativo, potrà richiedere ulteriori requisiti che saranno aggiornati e comunicati.

2.1 Processo di attivazione

L'Ente deve comunicare a LepidaSpA le informazioni complete necessarie per l'attivazione dei servizi FedERa secondo le procedure e le modalità di trasmissione previste da LepidaSpA. Le informazioni riguardano principalmente:

- tutti i dati dell'Ente, i dati del referente (nome, cognome, e-mail, telefono), i dati dei referenti tecnici e di supporto relativi ai servizi oggetto di integrazione con FedERa oltre a tutti i dettagli tecnici necessari per la configurazione e l'attivazione del servizio;
- tutti i dati degli operatori (ad esempio di RA) che l'Ente intende nominare specificando il ruolo e la responsabilità di ciascuno.

Tutte le comunicazioni relative al servizio FedERa e alle modalità di attivazione dei servizi devono essere inviate all'indirizzo email: piattaformecittadini@lepida.it .

L'attivazione del servizio, da parte di LepidaSpA, avviene attraverso la configurazione della piattaforma in ambiente di test e prevede una fase di verifica da parte del referente dell'Ente che dovrà comunicare esplicitamente a LepidaSpA il corretto funzionamento del servizio. Successivamente LepidaSpA effettua la configurazione in ambiente di produzione con una ulteriore verifica da parte del referente dell'Ente che dovrà comunicare esplicitamente a LepidaSpA il corretto funzionamento del servizio in produzione.

Si fa presente che rimane a carico di ciascun Ente la responsabilità delle soluzioni software che si intende integrare con FedERa e la relativa interoperabilità con FedERa oltre allo

svolgimento di eventuali verifiche delle integrazioni con gli ambienti di test messi a disposizione da LepidaSpA.

Si fa presente che eventuali modifiche successive all'attivazione rientrano nell'esercizio del servizio e pertanto l'Ente deve comunicare la richiesta secondo le modalità di seguito riportate, fornendo le informazioni complete necessarie per tali modifiche secondo le procedure e le modalità di trasmissione previste da LepidaSpA.

2.2 Livelli di servizio per l'attivazione

LepidaSpA garantisce i seguenti livelli di servizio (SLA) dal momento in cui LepidaSpA dispone di tutte le informazioni necessarie. I valori temporali indicati sono al netto del tempo necessario all'Ente per fornire ulteriori informazioni o chiarimenti su aspetti inizialmente non specificati e del tempo necessario ad AgID per l'attivazione su SPID.

Parametro	Valore	SLA (su base quadrimestrale)
Tempo di lavorazione di una richiesta di attivazione o modifica dell'Ente	10 giorni lavorativi	90% dei casi

3. Esercizio del servizio

3.1 Disponibilità del servizio

Il servizio è disponibile all'utenza H24 ad eccezione delle finestre temporali necessarie per eventuali manutenzioni e per cause non imputabili a LepidaSpA e alla piattaforma FedERa.

Parametro	Livello di Servizio
Tempo di disponibilità annuo	99.40%

LepidaSpA procede ad effettuare operazioni di manutenzione programmata, anche durante le ore di normale apertura degli uffici. Rientrano nelle attività di manutenzione programmata tutti gli aggiornamenti correttivi, funzionali e di sistema. Nel caso in cui la manutenzione programmata richieda l'indisponibilità del servizio, questa sarà preventivamente notificata per email ai referenti degli Enti. Nella comunicazione verranno forniti gli estremi temporali presunti del fermo, non vincolanti per LepidaSpA.

LepidaSpA garantisce i seguenti livelli di servizio (SLA) per la manutenzione programmata:

Parametro	Valore	SLA (su base quadrimestrale)
Tempo minimo di avviso in caso di disservizio per manutenzione programmata di competenza LepidaSpA	3 giorni solari	90% dei casi

3.2 Assistenza in esercizio

LepidaSpA fornisce due tipi di assistenza in esercizio:

- Servizio di help desk
- Gestione e manutenzione

Considerato che il servizio FedERa prevede l'integrazione con servizi degli Enti per la parte GW FedERa, si fa presente che rimane a carico di ciascun Ente la responsabilità dei servizi integrati, e da loro erogati, pertanto l'Ente deve effettuare la corretta diagnosi in caso di malfunzionamenti in modo da identificare con opportuno grado di precisione eventuali problemi dovuti al servizio FedERa. La segnalazione di eventuali malfunzionamenti da parte del referente dell'Ente, a seguito di un'accurata diagnosi nell'ambito del proprio dominio, sarà oggetto di analisi congiunta in modo da determinarne la natura e presa in carico da LepidaSpA qualora dovuta al servizio FedERa.
Inoltre si sottolinea che LepidaSpA fornisce servizio di Help desk ai cittadini per tutti gli aspetti inerenti l'utilizzo del servizio FedERa ad eccezione della natura o della correttezza delle informazioni pubblicate o provenienti dagli Enti.

3.2.1 Help Desk

La segnalazione di eventuali malfunzionamenti e per la richiesta di assistenza tecnica deve avvenire attraverso il servizio di Help Desk disponibile dal **lunedì al venerdì dalle ore 8:30 alle ore 18:30 ed il sabato dalle ore 8.30 alle ore 13.30**. I riferimenti dell'Help Desk sono:

Telefono	**800 445500**
e-mail	helpdesk@lepida.it
Web	http://www.lepida.it/servizi/help-desk

LepidaSpA non garantisce alcun livello di servizio per le segnalazioni inoltrate tramite canali diversi dall'Help Desk.

3.2.2 Gestione e manutenzione

LepidaSpA garantisce la gestione e manutenzione del servizio fornendo supporto agli Enti e ai cittadini e garantendone il funzionamento del rispetto di livelli di servizio previsti. In particolare, si precisa che per manutenzione correttiva si intendono gli interventi di correzione di malfunzionamenti del sistema che non possono essere risolti attraverso semplici operazioni di configurazione, ma necessitano di operazioni di modifica software oppure aggiornamento di una o più componenti del sistema, purché inerenti funzionalità già previste dal sistema.

3.2.3 Livelli di servizio

I valori di SLA, su base quadrimestrale, riportati di seguito si riferiscono alla finestra temporale disponibilità del servizio di Help Desk ed esclusivamente alle attività di competenza di LepidaSpA e relativamente al servizio FedERa.

Parametro	**Valore**	**Livello di servizio**
Tempo di presa in carico di un malfunzionamento dovuto al sistema FedERa	60 minuti	90% dei casi
Tempo di diagnosi e risoluzione, anche provvisoria, di malfunzionamenti bloccanti che non richiedono manutenzione correttiva	240 minuti	85% dei casi
Tempo di diagnosi risoluzione, anche provvisoria, di malfunzionamenti non bloccanti che non richiedono manutenzione correttiva	480 minuti	85% dei casi

Per la risoluzione dei malfunzionamenti rimangono esclusi cause non imputabili a LepidaSpA e alla piattaforma FedERa.

4. Documentazione tecnica

LepidaSpA rende disponibile sul proprio sito Internet la documentazione tecnica contenente le specifiche tecniche per l'integrazione con FedERa oltre ad altre informazioni utili.

Appendice 1: Linee guida della federazione

La presente appendice descrive le linee guida tecnico organizzative per la federazione vigente che saranno oggetto di evoluzione in relazione all'evoluzione di SPID in generale ed in particolare in relazione all'evoluzione dell'accreditamento di LepidaSpA come un IDP SPID.

1.1 Linee guida organizzative della federazione: soggetti, ruoli e responsabilità

I soggetti che compongono la federazione sono gli Identity Provider, i Service Provider, le Attribute Authority e il Gestore della federazione.

1.1.1 Identity Provider

Gli Identity Provider (IdP) sono i soggetti che rilasciano credenziali di autenticazione ai cittadini e consente loro l'accesso ai servizi online federati.
Gli IdP, per federarsi, devono rendere i loro sistemi conformi alle linee guida tecniche della federazione, ed in particolare devono:

- provvedere al riconoscimento della persona alla quale rilasciano le credenziali in conformità ad uno dei livelli di identificazione previsti nella federazione e definiti nel paragrafo 1.2 della presente appendice;
- implementare le politiche di gestione delle password in conformità ad uno dei livelli previsti nella federazione e definiti nel paragrafo 1.2 della presente appendice;
- autenticano gli utenti usando uno o più metodi di autenticazione previsti nella federazione e definiti nel paragrafo 1.2 della presente appendice.

A seguito di una richiesta di accesso da parte di un utente ad uno qualsiasi dei servizi federati, l'IdP presso cui l'utente si è registrato, ne verifica le credenziali.

1.1.1.1 Registration Authority

Un Ente, sprovvisto di un proprio sistema di identificazione utenti, può diventare Identity Provider all'interno della federazione utilizzando il software messo a disposizione dal servizio fedERa, che permette l'espletamento dei servizi di Registration Authority (RA). Si tratta di una procedura informatica di rilascio e successiva gestione delle credenziali utenti. A questo livello avviene l'associazione tra un identificativo username/password ed una persona fisica.

Tramite questo applicativo web gli operatori dell'ente (operatori RA) possono registrare nuovi utenti e rilasciare ad essi credenziali di accesso del tipo username e password, cercare, visualizzare le informazioni, rimuovere o sospendere utenti, e associare una nuova busta cieca (busta consegnata all'utente con password e puk, per il recupero della stessa). Il sistema mette inoltre a disposizione degli utenti una form di registrazione e una di login personalizzate con nome e logo dell'ente. L'operatore RA è l'operatore dell'Ente che identifica gli utenti e ne gestisce le identità digitali. Le funzionalità disponibili sono descritte nel relativo manuale di utilizzo del servizio di RA gestito da LepidaSpA.

1.1.2 Service Provider

I Service Provider (SP) sono i soggetti che mettono a disposizione degli utenti servizi web a seguito di una procedura di autenticazione federata. Gli SP provvedono a rendere i loro sistemi conformi alle linee guida tecniche della federazione, descritte nel paragrafo 1.2. Il SP, a seguito di una richiesta di accesso ad un servizio gestito, provvede a re-indirizzare l'utente al GW fedERa il quale a sua volta provvederà a re-indirizzarlo all'IdP per la verifica delle credenziali. Il SP, al quale il GW fedERa avrà re-indirizzato l'utente che ha superato la verifica di credenziali da parte dell'IdP, provvederà a completare la procedura di accesso al servizio secondo le proprie regole di accesso.

Con la federazione di un proprio SP, viene riconosciuta l'identità digitale rilasciata da un qualsiasi IdP federato, purchè l'utenza possieda livello di identificazione e password policy minimi richiesti dal servizio stesso e rispetti le regole definite dallo SPID.

L'operatore SP è l'operatore dell'Ente che definisce i criteri secondo i quali permettere l'accesso al servizio, indicando, ad esempio, quali valori devono assumere determinati attributi del profilo utente affinchè venga concesso all'utente l'accesso al servizio offerto dall' SP.

1.1.3 Attribute Authority

Le Attribute Authority sono i soggetti abilitati a certificare gli attributi qualificati contenuti nel profilo utente dell'Identità digitale. L'introduzione dell' Attribute Authority nello scenario della federazione permette di certificare un insieme degli attributi che vengono rilasciati al servizio.
Un Ente, sprovvisto di un proprio sistema di certificazione di attributi, può diventare Attribute Authority all'interno della federazione e fornire attributi qualificati, utilizzando il software messo a disposizione dal servizio fedERa.

1.1.4 Gestore della federazione

LepidaSpA, assumendosi il ruolo di Gestore della federazione perchè affidatogli dall'Ente Regione Emilia-Romagna come delegato all'interno della CNER o direttamente dall'Ente socio, provvederà a garantire:

- il funzionamento del gateway multiprotocollo e in generale dei sistemi di gestione della federazione nel suo complesso;
- l'aderenza agli standard della federazione da parte di tutti i soggetti coinvolti, al fine di consentire la corretta interazione tra gli stessi e l'espletamento dei servizi rivolti agli utenti;
- il necessario supporto in fase di adesione alla federazione anche relativamente alla integrazione di IdP e SP;
- il funzionamento e la disponibilità di servizi di help desk;
- gestione dell' albo dei soggetti federati, consultabile sul portale della federazione, per ciascuno dei quali viene indicato con quali funzioni il soggetto aderente si integra al sistema (IdP e/o SP).

1.2 Linee guida tecniche ed organizzative della federazione

Di seguito sono descritte le linee guida tecniche ed organizzative vigenti della federazione che saranno oggetto di evoluzione in relazione all'evoluzione SPID e del ruolo di LepidaSpA.

1.2.1 Rilascio delle identità digitali

Le procedure di rilascio delle credenziali sono conformi alle modalità previste dallo SPID. Le identità digitali sono rilasciate, su richiesta dell'interessato, dal gestore di identità del soggetto richiedente.

1.2.1.1 Livelli di identificazione dell'utente

L'identificazione è la procedura con cui un IdP associa una identità fisica ad una utenza, verificandone l'autenticità. Le identificazioni e le modalità di rilascio di credenziali sono conformi alle modalità previste da SPID, nello specifico:

- **Identificazione forte:** l'utente che richiede il rilascio di credenziali viene identificato in maniera certa e le credenziali vengono consegnate in maniera sicura. Di seguito si elencano le modalità previste:
    - l'utente si presenta presso la RA dell'IdP e richiede il rilascio di una identità digitale. L'operatore della RA verifica l'identità dell'utente con un documento di identità presentato a vista dall'utente e registra l'utenza nell' IdP. I documenti accettati sono Carta di Identità, Passaporto e Patente di Guida. Gli estremi del documento sono annotati, una fotocopia dello stesso viene conservata insieme al documento di riepilogo dei dati di identità firmato. Le credenziali sono consegnate mediante busta cieca all'atto della registrazione.

- l'utente si presenta presso la RA dell'IdP a seguito di una preregistrazione online, richiedendo l'identificazione tramite esibizione a vista di un valido documento di identità per ottenere una utenza con identificazione forte. L'operatore della RA controlla la corrispondenza dei dati inseriti nella preregistrazione online con quelli contenuti nel documento di identità. I documenti accettati sono Carta di Identità, Passaporto e Patente di Guida. Gli estremi del documento sono annotati, ed una fotocopia dello stesso viene conservata insieme al documento di riepilogo dei dati di identità firmato.
- L'utente effettua la preregistrazione online e richiede l'identificazione forte caricando il modulo di adesione a fedERa firmato digitalmente. L'operatore verifica la firma digitale e nel caso che la firma sia corretta, identifica in maniera forte l'utente.
- L'utente effettua la preregistrazione online e ottiene una identificazione forte attraverso l'utilizzo di una carta di autenticazione elettronica, CNS (carta nazionale dei servizi) o CIE (carta di identità elettronica).
- L'utente effettua la registrazione online con l'utilizzo della carta di identità elettronica, CIE e CNS.

Tutte le identità rilasciate in passato con modalità non coerenti con SPID dovranno essere oggetto di adeguamento, ove è possibile. Si riportano di seguito le modalità non più utilizzabili.

- Nessuna identificazione: non c'è nessun controllo da parte dell' Idp sulla veridicità dei dati inseriti dall'utente in fase di registrazione. L'Idp non ha alcun dato per risalire all'identità dell'utente. Tipicamente l'utente si registra compilando una form web e viene solo effettuato un controllo sulla corrispondenza del Codice Fiscale con i dati personali introdotti dall'utente.
- Identificazione debole: l'utente viene identificato in maniera debole/indiretta, dimostrando attraverso una procedura informatica di essere possessore di una SIM rilasciata da un gestore telefonico, previa identificazione. Gli utenti si registrano online presso il gestore di identità, inserendo e confermando il proprio numero di telefono cellulare. Non c'è alcun controllo sulla veridicità dei dati associati all'utenza, ma il cittadino è stato riconosciuto indirettamente dal soggetto terzo che ha rilasciato la SIM. L'Idp conserva il numero di SIM utilizzata durante la procedura di autenticazione.

1.2.1.2 Sicurezza della password

Per sicurezza della password si intende un set di regole sulla robustezza dell'account e della password scelta dall'utente, da applicare agli utenti identificati in maniera forte. Le regole dovranno essere adeguate alle regole SPID

Nella vigente federazione fedERa sono individuati tre livelli di sicurezza della password:

- Password minima: l'IdP richiede che la password scelta dall'utente abbia come unico vincolo una lunghezza minima pari a sei caratteri e non è prevista nessuna policy sull'account.
- Password per dati personali: L'IdP implementa regole di sicurezza delle password che consentono di operare su dati personali ai sensi del D.Lgs 196/2003. In particolare l'IdP implementa controlli che assicurano che le password siano lunghe almeno otto caratteri, con una certa composizione di caratteri e che siano cambiate almeno ogni sei mesi. In più l'account è disattivato dopo sei mesi dall'ultimo accesso.
- Password per dati sensibili: L'IdP implementa regole di sicurezza delle password che consentono di operare su dati sensibili ai sensi del D.Lgs 196/2003. In particolare l'IdP implementa controlli che assicurano che le password siano lunghe almeno otto caratteri, con una certa composizione di caratteri e che siano cambiate almeno ogni tre mesi. In più l'account è disattivato dopo sei mesi dall'ultimo accesso.

1.2.1.3 Rilascio di credenziali a soggetti minori

Un utente di età inferiore a 18 anni può ottenere una identità digitale con livello di affidabilità forte solo presentandosi presso lo sportello della registration authority, e facendone richiesta con particolare modulo. Il minore deve essere accompagnato dal genitore e/o da chi ne esercita la potestà genitoriale. L'operatore della RA deve effettuare l'identificazione tramite esibizione a vista di un valido documento d'identità del richiedente minore e dell'adulto esercitante la potestà genitoriale, il quale deve firmare la documentazione di adesione a fedERa per nome e per conto del minorenne e una liberatoria per permettere l'accesso al minore ai servizi federati. Le credenziali saranno consegnate solo all'adulto esercitante la potestà genitoriale.

1.2.1.4 Gestione decessi e revoche

L' utente può chiedere al gestore dell'identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione o revoca della propria identità digitale. Il gestore di identità se riscontra inattività della utenza digitale per un periodo continuativo superiore a ventiquattro mesi o in caso di decesso della persona fisica, revoca l'identità digitale. In entrambi i casi l'identità digitale può essere riemessa ex-novo solo a seguito di una nuova richiesta da parte dell'utente direttamente alla RA, presentando a vista un documento di identità.

1.2.1.5 Gestioni illeciti e frodi di identità digitale

Richiesta dell'interessato di sospensione o revoca della identità digitale: Nel caso in cui l'utente ritenga che la propria identità digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo, invia, a mezzo posta elettronica, una richiesta di sospensione dell'identità digitale al gestore della stessa (ente o LepidaSpA) e al fornitore di servizi presso il quale essa risulta essere stata utilizzata. Alla richiesta di sospensione è allegata copia di un

documento di riconoscimento in corso di validità. Salvo il caso in cui la richiesta sia inviata tramite posta elettronica certificata, il gestore dell'identità digitale e il fornitore di servizi verificano, attraverso l'attributo secondario, la provenienza della richiesta di sospensione dal soggetto titolare dell'identità digitale e forniscono la conferma della ricezione della medesima richiesta. La richiesta può essere invitata anche per posta raccomandata AIR. Se la richiesta è sottoscritta con firma digitale o firma elettronica qualificata, alla stessa non va allegata copia del documento di riconoscimento. L'utente può chiedere al gestore dell'identità digitale, in qualsiasi momento e a titolo gratuito, la sospensione o revoca della propria identità digitale ovvero la modifica dei propri attributi secondari e delle proprie credenziali di accesso. A tali richieste il gestore dell'identità digitale provvede tempestivamente.

Comportamento del gestore d' identità digitale e del service provider: Nel caso di abuso o illecito, il gestore dell'identità digitale sospende tempestivamente l'identità digitale per un periodo massimo di trenta giorni informandone il richiedente. Scaduto tale periodo, l'identità digitale è ripristinata o revocata. Il gestore revoca l'identità digitale se riceve dall'interessato copia della denuncia penale presentata all' Autorità Giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione.

1.2.2 Metodi di autenticazione

La federazione prevede l'utilizzo di tre metodi di autenticazione coerentemente con SPID.
Ogni SP integrato deve scegliere, tra le seguenti tipologie di autenticazione, quale prevedere per i propri servizi:

- **Password:** In fase di autenticazione, all'utente viene chiesto l'inserimento di una password che viene verificata con quella rilasciata dall'Idp. Per segnalare il supporto, da parte dell'SP, o l'uso da parte dell'Idp, di questo metodo si usa la classe *urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport*.
- **One-time password:** Affinchè l'IdP possa usare questo metodo di autenticazione, l'utente deve aver fornito un numero di cellulare all'IdP. Oltre all'inserimento della password rilasciata dall'IdP all'utente, all'utente viene chiesto di inserire una codice che viene inviato dall'IdP al cellulare. Per segnalare il supporto, da parte dell'SP, o l'uso da parte dell'IdP, di questo metodo si usa la classe *urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword*.
- **Smarcart:** L'utente viene autenticato usando il certificato X.509 contenuto in una carta elettronica di autenticazione. Per segnalare il supporto, da parte dell'SP, o l'uso da parte dell'IdP, di questo metodo si usa la classe *urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard*. Tale modalità corrisponde al terzo livello di autenticazione di SPID.

1.2.3 Attributi

Nell'ambito di fedERa sono definiti gli attributi elencati e aggiornati sul sito di LepidaSpA. La scelta del nome degli attributi non è a discrezione dell'SP. Quest'ultimo infatti può sceglierli tra quelli censiti nella federazione. La naming convention relativa agli attributi qualificati è definita dal gestore della federazione.
Il SP deve definire un profilo utente definendo come obbligatori solo quegli attributi necessari alla fruizione del servizio, i quali devono risultare pertinenti e non eccedenti in relazione alla tipologia e alle funzioni offerte del servizio.
Tutti gli aspetti relativi agli attributi dovranno essere evoluti per adeguarsi all'evoluzione di SPID sia per gli IdP che per gli SP.