Allegato 1

Servizio

Governance e linee guida tecnico-organizzative della Federazione

INDICE

1. **Introduzione** 3
   - 1.1 **Definizione e Acronimi** 3
   - 1.2 **Scopo del documento** 4
   - 1.3 **Destinatari** 4

2. **Il Sistema FedERa** 5

3. **Il governo della Federazione** 5
   - 3.1 **Definizione criteri e modalità di adesione a FedERa** 5
   - 3.2 **Revisione del Protocollo di Adesione** 6

4. **Linee guida organizzative della Federazione: soggetti, ruoli e responsabilità** 7
   - 4.1 **Identity Provider** 7
   - 4.2 **Gestore della Federazione** 8
   - 4.3 **Service Provider** 8

5. **Linee guida tecniche della Federazione: modalità d'identificazione, livelli e attribiti** 10
   - 5.1 **Identificazione utenti** 10
   - 5.2 **Sicurezza della password** 10
   - 5.3 **Metodi di autenticazione** 11
   - 5.4 **Attributi** 11
   - 5.5 **Certificati** 12

6. **Privacy e trattamento dei dati: ruoli e reponsabilità** 13

1. Introduzione

1.1 Definizione e Acronimi

1) Community Network dell'Emilia-Romagna (*CN-ER*): la Community Network dell'Emilia-Romagna (*CN-ER*), istituita con la delibera regionale 1045/07 per creare le condizioni organizzative per dare attuazione alle finalità e ai progetti contenuti nel pitER (2007-2009), 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 CN-ER 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 Lepida S.p.A. Con la Convenzione che dà vita alla CN-ER si è realizzato l'Accordo Quadro fra gli Enti aderenti, da cui sono derivati e deriveranno, durante il periodo di validità, gli specifici accordi attuativi per l'adesione alle singole iniziative del PiTER, fra cui anche il progetto FedERa;

2) 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;

3) 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;

4) Utente: soggetto al quale viene rilasciata una identità digitale con la quale potrà richiedere l'accesso ai servizi erogati dal Service Provider; l'utente in tale contesto opera per il tramite del proprio browser;

5) Identity Provider (IdP): soggetto che nell'ambito di FedERa è abilitato a rilasciare un'identità digitale all'utente e a verificarla; l'identità digitale consentirà all'utente di autenticarsi al Service Provider 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;

6) Service Provider (SP): soggetto che eroga un servizio all'utente che si sia autenticato per il tramite dell'identità digitale rilasciata dall'IdP. 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;

7) Gateway (GW): il sistema che collega l'utente all'IdP il quale ne verifica l'identità; riceve dall'utente l'dentità rilasciata dall'IdP e i relativi Dati personali; indirizza l'utente verso un Service Provider per consentirgli l'accesso ad un servizio; in sintesi fornisce all'utente, su richiesta dello stesso, informazioni che consistono in asserzioni circa l'identità dell'utente e circa la verifica effettuata; mantiene un log degli eventi;

8) Gestore del Gateway: soggetto che gestisce il Gateway; 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;

9) 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;

10) Soggetto Aderente ovvero Aderente: il Soggetto Aderente – di natura pubblica e privata - può essere un IdP o un SP sottoscrittore del protocollo di adesione alla Federazione;

11) Referente Organizzativo (RO): è la persona fisica nominata dal Soggetto Aderente quale punto di contatto per qualsiasi questione di tipo organizzativo attinente la Federazione;

12) Referente Tecnico (RT): è la persona fisica nominata dal Soggetto Aderente quale punto di contatto per qualsiasi questione di tipo tecnica attinente la Federazione;

13) Ente Proponente: Ente che nell'ambito di FedERa può proporre l'adesione di un Soggetto diverso dagli ENTI aderenti alla CN-ER e dagli Enti Soci di Lepida S.p.A.. L'ENTE proponente deve aver già aderito alla Federazione e deve essere socio di Lepida S.p.A.

1.2 Scopo del documento

Il presente documento ha lo scopo di definire il sistema di governo, organizzativo e gestionale della Federazione, andando a definire i soggetti coinvolti, stabilendone ruoli, responsabilità e modalità di interazione tra gli stessi.

1.3 Destinatari

I destinatari di tale documento sono tutti i soggetti coinvolti nella Federazione e pertanto: Regione Emilia-Romagna, la CN-ER e i suoi organismi di rappresentanza (CPI e CT), Lepida S.p.A.; i Soggetti Aderenti che possono rivestire il ruolo di Identity Provider e/o di Service Provider; la CN-ER; il CPI; il CT.

2. Il Sistema FedERa

FedERa è il sistema realizzato da Lepida S.p.A. nell'ambito degli interventi del PiTER, che permette agli utenti di acquisire le identità digitali federate (credenziali) con le quali poter richiedere l'accesso ai servizi online erogati dai diversi soggetti aderenti al sistema (Regione, Enti Locali, altre PP.AA. e soggetti di natura pubblica o privata), mediante un sistema di autenticazione federata.

Per essere riconosciuti nei servizi on-line messi a disposizione dalla Federazione, l'utente fa uso di un'unica credenziale di autenticazione FedERa.

3. Il governo della Federazione

Il governo della Federazione è demandato: alla Regione Emilia-Romagna, alla CN-ER, la quale opera anche per il tramite del proprio rappresentante; al CPI; al CT e a Lepida S.p.A..

Alla CN-ER è riconosciuto il ruolo di promotore e coordinatore delle attività finalizzate a garantire coesione tra i diversi enti aderenti, incoraggiando e promuovendo la stipula di accordi attuativi e protocolli per realizzare gli scopi sottesi a progetti e sistemi d'interesse generale e comune.

Quanto previsto nel presente documento è l'unica modalità di governo, organizzazione e gestione prevista per la Federazione, salvo le modifiche che potranno essere apportate secondo la forma e le modalità definite nel seguito.

3.1 Definizione criteri e modalità di adesione a FedERa

L'adesione al Sistema FedERa avviene attraverso la stipula del Protocollo di cui il presente documento costituisce allegato e si perfeziona con la sottoscrizione di apposito contratto tra Soggetti Aderenti e Lepida S.p.A..

Per gli aderenti che fanno parte dell'agggregazione CN-ER il protocollo si sostanzia in un Accordo Attuativo della CN-ER.

In particolare, su delega del Comitato Permanente di Indirizzo e Coordinamento, il Comitato Tecnico definisce i criteri per autorizzare la sottoscrizione del Protocollo di Adesione a FedERa da parte di soggetti diversi dagli ENTI aderenti alla CN-ER e dagli Enti Soci di Lepida S.p.A..

I suddetti criteri sono approvati nell'ambito del Comitato Permanente di Indirizzo e Coordinamento con gli Enti locali.

Unitamente ai suddetti criteri, il CPI definisce congiuntamente con Regione Emilia-Romagna, le eventuali condizioni economiche da applicare ai Soggetti Aderenti e le modalità di pagamento delle stesse.

La proposta di adesione di un soggetto diverso dagli ENTI aderenti alla CN-ER e dagli Enti Soci di Lepida S.p.A., deve essere segnalata a Lepida S.p.A., che ha il compito di avviare l'iter autorizzativo da parte di un ENTE Proponente.

Il CT verifica che il nuovo Soggetto Aderente abbia i requisiti definiti per potersi federare e in caso positivo approva l'adesione a FedERa, che dovrà perfezionarsi con la sottoscrizione del Protocollo di Adesione. Nel caso contrario rifiuta l'adesione del nuovo Soggetto alla Federazione.

Regione Emilia-Romagna, preso atto della deliberazione del CT, procede alla sottoscrizione del Protocollo di Adesione con il nuovo Soggetto Aderente.

Il Comitato Tecnico comunica periodicamente le nuove adesioni autorizzate al CPI che provvede a ratificarle.

Lepida S.p.A. prende in carico tutto il processo collegato all'attivazione dei servizi per la federazione e gestisce i rapporti con il Soggetto Aderente, con il quale stipula apposito contratto di servizio.

Lepida S.p.A. comunica al CPI periodicamente i nuovi contratti sottoscritti con i soggetti autorizzati dal Comitato Tecnico.

3.2 Revisione del Protocollo di Adesione

La proposta di variazione e/o aggiornamento del protocollo o di suoi allegati potrà essere avanzata singolarmente dalla CN-ER; da Lepida S.p.A., dal CPI o congiuntamente da parte di 10 Enti Soci di Lepida S.p.A., già aderenti a FedERa.

A seguito di una proposta di variazione del Protocollo di Adesione e/o suoi Allegati, il CT verifica l'opportunità di apportare le modifiche richieste.

Il CT incarica Lepida S.p.A. di apportare, tra le modifiche richieste, quelle ritenute necessarie e di produrre la nuova versione del Protocollo di Adesione e/o dei suoi Allegati.

Il nuovo testo del Protocollo di Adesione e/o degli Allegati, condiviso con il rappresentante della CN-ER, sarà oggetto di deliberazione del CPI.

A seguito dell'approvazione da parte del CPI, la Regione Emilia-Romagna e Lepida S.p.A. procederanno a darne comunicazione a tutti i membri della Federazione.

Le variazioni al Protocollo o suoi allegati decorreranno dal sessantesimo giorno successivo alla comunicazione.

Il Soggetto Aderente potrà, a seguito delle eventuali modifiche apportate, esercitare il diritto di recesso dal Protocollo nei tempi e modi definiti nello stesso.

4. Linee guida organizzative della Federazione: soggetti, ruoli e responsabilità

Ogni Aderente nomina un Referente Organizzativo (RO), che costituisce il punto di contatto dell'Aderente con il Gestore della Federazione. L'Aderente si impegna a comunicare tempestivamente al Gestore della Federazione l'eventuale variazione del RO.

L'Aderente fornirà alcune informazioni che potranno essere usate dal Gestore della Federazione per scopi di promozione della Federazione stessa, ed in particolare una descrizione dell'Aderente. L'Aderente riconosce alla Federazione il diritto di pubblicare il nome dell'Aderente ai fini della promozione della Federazione stessa.

4.1 Identity Provider

Gli Identity Provider (IdP) sono i soggetti che rilasciano credenziali di autenticazione agli utenti, eventualmente previa la verifica di un documento di identità.

Gli IdP provvedono a rendere i loro sistemi conformi alle regole tecniche della Federazione, ed in particolare:

- provvedono al riconoscimento della persona a cui rilasciano le credenziali in conformità ad uno dei livelli di identificazione definiti successivamente;
- implementano politiche di gestione delle password in conformità ad uno dei livelli definiti successivamente;
- autenticano gli utenti usando uno o più dei metodi di autenticazione previsti nella Federazione, definiti successivamente.

A seguito del rilascio delle credenziali e in fase di richiesta dell'utente di accesso ad un qualsiasi servizio integrato in FedERa, l'IdP di competenza, al quale l'utente viene reindirizzato da parte del gateway, procede a verificare le credenziali rilasciate e a reindirizzare l'utente per il tramite del browser al gateway per completare l'accesso al servizio richiesto.

4.1.1 Registrazione di IdP

L'Aderente prende visione di tutta la documentazione tecnica messa a disposizione dalla Federazione e chiede al gestore della Federazione la registrazione di un servizio di IdP.

L'Aderente nomina un Referente Tecnico (RT) per il servizio che mantiene i contatti con il Gestore della Federazione riguardo la corretta configurazione del servizio. L'Aderente si impegna a comunicare tempestivamente al Gestore della Federazione l'eventuale variazione del RT.

L'Aderente deve fornire, ai fini della registrazione, le informazioni definite dalle regole tecniche, riguardo l'accreditamento degli utenti:

- quale livello di identificazione, tra quelli definiti dalle regole tecniche della Federazione, implementa;
- quale password policy, tra quelle definiti dalle regole tecniche della Federazione, implementa.

L'Aderente deve fornire la lista degli attributi utente che rilascia nelle sessioni di autenticazione.

L'Aderente deve anche fornire alcune informazioni che potranno essere usate dal Gestore della Federazione per scopi di promozione della Federazione stessa, ed in particolare:

- l'URL a cui sono disponibili le modalità di registrazione;
- una descrizione del servizio.

4.2 Gestore della Federazione

Lepida S.p.A. assumendosi il ruolo di Gestore della Federazione provvederà a garantire:

- il funzionamento del gateway 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 Aderenti, consultabile sul sito di FedERa, per ciascuno dei quali viene indicato con quali funzioni il Soggetto Aderente si integra al sistema (IdP e/o SP);
- il necessario supporto per la definizione degli strumenti necessari a garantire l'uniformità e standardizzazione degli atti successivi e conseguenti quali a mero titolo esemplificativo e non esaustivo, Informative, designazione dei responsabili ovvero degli incaricati al trattamento dei dati.

Lepida S.p.A. in qualità di gestore del gateway provvederà in fase di richiesta di accesso ai servizi da parte dell'utente a:

- recepire il re-indirizzamento dell'utente sul gateway da parte del SP;
- re-indirizzare l'utente, che per il tramite del proprio browser ha fatto richiesta di accesso ad un servizio, verso l'IdP per la necessaria verifica delle credenziali;
- re-indirizzare l'utente, che ha superato la verifica delle credenziali da parte dell'IdP, verso il SP per consentire all'utente di completare l'accesso al servizio richiesto.

Nel caso in cui il Soggetto Aderente ne faccia richiesta, Lepida S.p.A. metterà a disposizione dello stesso l'applicazione telematica, gestita dalla stessa Lepida S.p.A., funzionale all'esercizio del ruolo di Identity Provider.

4.3 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 regole tecniche della Federazione. Il SP, a seguito di una richiesta di accesso ad un servizio gestito, provvederà a re-indirizzare l'utente al gateway il quale a sua volta provvederà a re-indirizzarlo all'IdP per la verifica delle credenziali.

Il SP al quale il gateway 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 allo stesso.

Con la federazione di un proprio SP, il Soggetto Aderente, riconosce l'identità digitale rilasciata da un qualsiasi IdP federato, purchè l'utenza possieda livello di identificazione e password policy minimi richiesti dal servizio.

4.3.1 Registrazione di SP

L'Aderente prende visione di tutta la documentazione tecnica messa a disposizione dalla Federazione e chiede al gestore della Federazione la registrazione di un servizio di SP.

L'Aderente nomina un Referente Tecnico (RT) per il servizio che mantiene i contatti con il Gestore della Federazione riguardo la corretta configurazione del servizio. L'Aderente si impegna a comunicare tempestivamente al Gestore della Federazione l'eventuale variazione del RT.

L’Aderente deve fornire, ai fini della registrazione, tutte le informazioni definite successivamente ed in particolare:

- quale livello minimo di identificazione accetta, tra quelli definiti successivamente, per gli utenti che si autenticano al servizio;
- quale password policy minima accetta, tra quelle definiti successivamente, per gli utenti che si autenticano al servizio.

L’Aderente deve fornire la lista degli attributi utente che si aspetta nelle sessioni di autenticazione.

L’Aderente deve anche fornire alcune informazioni che potranno essere usate dal Gestore della Federazione per scopi di promozione della Federazione stessa, ed in particolare:

- l’URL a cui è disponibile il servizio;
- una descrizione del servizio.

5. Linee guida tecniche della Federazione: modalità d'identificazione, livelli e attributi

5.1 Identificazione utenti

L'identificazione è la procedura con cui un IdP associa una identità fisica ad una utenza. Nella Federazione sono definiti tre livelli di identificazione.

Nessuna identificazione

Non c'è nessun controllo sulla veridicità dei dati associati all'utenza. L'IdP non ha alcun dato per risalire all'identità dell'utente.

Tipicamente l'utente si registra compilando un form web.

Identificazione debole

L' utente dimostra che ha accesso ad una SIM/USIM. Non c'è nessun controllo diretto sulla veridicità dei dati associati all'utenza, mentre questo è demandato al soggetto terzo che ha rilasciato la SIM/USIM.

L'IdP conserva il numero di SIM/USIM che è stata usata nella procedura di identificazione.

Identificazione forte

I dati degli utenti sono verificati da un operatore dell'IdP che ne controlla la corrispondenza con quelli contenuti in un documento di identità valido presentato dall'utente. L'IdP può accettare documenti consegnati di persona, spediti via fax o spediti per posta.

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. Equivalentemente l'utente si registra al servizio usando una carta di autenticazione elettronica tipo carta nazionale dei servizi o carta di identità elettronica. I dati dell'utente sono verificati dall'utente a fronte di un documento valido. L'IdP conserva gli estremi di un documento.

5.2 Sicurezza della password

Sono definiti tre livelli di sicurezza delle password.

Password minima

L'IdP richiede che le password siano lunghe almeno sei caratteri.

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 e che siano cambiate ogni sei mesi.

Password per dati sensibili

L'IdP implementa regole di sicurezza delle password che consentono operare su dati sensibili ai sensi del D.Lgs n.196. In particolare L'IdP implementa controlli che assicurano che le password siano lunghe almeno otto caratteri e che siano cambiate ogni tre mesi.

5.3 Metodi di autenticazione

La Federazione prevede l'utilizzo dei seguenti metodi di autenticazione.

Password

All'utente viene chiesto l'inserimento di una password che viene verificato 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

Perché 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*.

Smartcard

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*.

5.4 Attributi

Nell'ambito della federazione sono definiti almeno gli attributi elencati di seguito, che ciascun IdP può decidere di rilasciare nelle sessioni di autenticazione.

Nell'utilizzo dei seguenti attributi, gli IdP si impegnano ad usare la semantica definita di seguito.

nome

Attributo a singolo valore contenente il nome dell'utente.

cognome

Attributo a singolo valore contenente il cognome dell'utente.

dataNascita

Attributo a singolo valore contenente la data di nascita dell'utente nel formato GG/MM/AAAA.

luogoNascita

Attributo a singolo valore contenente, per i nati in Italia il comune di nascita, per i nati all'estero la nazione di nascita.

sesso

Attributo a singolo valore contenente il sesso dell'utente. Il valore deve contenere la stringa 'M' per utenti di sesso maschile, 'F' per utenti di sesso femminile.

CodiceFiscale o codiceFiscale

Attributo a singolo valore contente il codice fiscale dell'utente. In caso di IdP e SP SAML V1.1 si usa la sintassi codice Fiscale per compatibilità con SP ed IdP del progetto PEOPLE.

emailAddress

Attributo a singolo valore contenente un recapito di posta elettronica dell'utente. Dovrebbe essere valorizzato con un indirizzo di tipo PEC, ma può essere valorizzato con un indirizzo normale.

emailAddressPersonale

Attributo a singolo valore contenente l'indirizzo di posta elettronica dell'utente.

trustLevel

Attributo a singolo valore contenente quale dei livelli di identificazione definiti alla sezione 1.1 è stato applicato all'utente.

policyLevel

Attributo a singolo valore contenente quale delle policy di sicurezza password definite alla sezione 1.2 è implementato per l'utente.

5.5 Certificati

I metadata esposti da IdP e SP devono essere protetti da connessione HTTPS. Gli endpoint di single sign one degli IdP e di consumo delle asserzioni dovrebbero essere protetti da connessione https.

Gli IdP dovrebbero firmare sia l'asserzione di autenticazione che il response e devono firmare almeno una fra asserzione e response. I SP dovrebbero firmare le richieste di autenticazione. I certificati di firma possono essere self-signed nel caso di SP o IdP che espongono i metadata tramite HTTPS .

6. Privacy e trattamento dei dati: ruoli e reponsabilità

Il modello tecnico e organizzativo presentato nella pagine precedenti non prevede alcuna comunicazione diretta di dati personali fra i Soggetti Aderenti.

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.