



Progetto fedERa

**Architettura e Scenari di integrazione di
Service Provider e Identity Provider
sul territorio regionale**

SOMMARIO

1. La federazione fedERa	4
1.1. Contesto: le Infrastrutture SiRAC-People e ICAR INF-3	4
1.1.1. PEOPLE	4
1.1.2. ICAR.....	7
1.1.3. Considerazioni.....	11
1.2. Architettura e caratteristiche generali dell'infrastruttura federa.....	11
1.3. Soggetti interagenti.....	12
1.4. Domini interagenti.....	14
1.5. Circle-of-Trust.....	16
1.6. Affidabilità dell'identità e dell'autenticazione	17
1.7. Considerazioni aggiuntive.....	20
2. Casi d'uso di integrazione di servizi	22
2.1. Scenari d'interazione con gateway multiprotocollo FedERa e senza gateway locale	23
2.1.1. Accesso a servizi ICAR/FedERa per utenti ICAR/FedERa nell'ambito del dominio regionale 24	
2.1.2. Accesso a servizi ICAR/FedERa per utenti PEOPLE sul territorio di RER	27
2.1.3. Accesso a servizi ICAR di un ente locale di RER per utenti ICAR/FedERa.....	29
2.1.4. Accesso a servizi PEOPLE di un ente locale di RER per utenti ICAR/FedERa	29
2.1.5. Accesso a servizi PEOPLE di un ente locale di RER per utenti PEOPLE di RER ..	30
2.1.6. Accesso a servizi ICAR di un ente locale di RER per utenti FedERa	31
2.1.7. Accesso a servizi ICAR di RER per utenti PEOPLE di RER.....	32
2.1.8. Accesso a servizi PEOPLE di un ente locale di RER per utenti ICAR/fedERa	34
2.1.9. Accesso a servizi PEOPLE di RER per utenti PEOPLE di RER.....	35
2.2. Scenari d'interazione senza gateway multiprotocollo centrale o locale	36
2.2.1. Accesso ai servizi PEOPLE per utenti ICAR/FedERa	37

3. Riferimenti38

1. LA FEDERAZIONE FEDERA

Di seguito vengono elencati tutti i soggetti che fanno parte dello scenario complessivo d'interazione del sistema FedERa e i domini di cui possono far parte. Inoltre vengono fornite alcune definizioni e considerazioni generali in merito all'affidabilità dei processi di registrazione e autenticazione, ai Circle of Trust e ai servizi ad essi afferenti.

1.1. CONTESTO: LE INFRASTRUTTURE SIRAC-PEOPLE E ICAR INF-3

A fondamento dell'infrastruttura fedERa vi è l'interoperabilità con i due principali punti di riferimento a livello nazionale in materia di autenticazione federata e gestione delle identità digitali, costituiti dalla comunità dei portali PEOPLE e dalla federazione definita nell'ambito del progetto ICAR. La prima delle due trova già una certa diffusione sul territorio nazionale mentre la seconda sarà gradualmente adottata a livello dei singoli enti locali e centrali, con il consolidamento ed il rilascio dei componenti architetturali costitutivi.

Nel seguito vengono presentati i tratti salienti delle architetture definite per tali due comunità, limitatamente alla tematica della gestione delle identità digitali e all'autenticazione degli utenti nello specifico.

1.1.1. PEOPLE

Nell'ambito del progetto PEOPLE è attualmente in esercizio una comunità di portali erogatori di servizi di e-government rivolti ad utenti finali (cittadini). Ciascuno dei portali della comunità può richiedere o no, sulla base del singolo servizio erogato, che l'utente si autentichi presso uno dei soggetti (Identity Provider) abilitati alla fornitura del servizio di autenticazione, prima di vedersi riconosciuto l'accesso. L'autenticazione avviene mediante l'immissione di opportune credenziali rilasciate dallo stesso Identity Provider, sotto forma di coppie username e password, piuttosto che mediante l'utilizzo di strumenti quali smart-card di vario tipo.

A sovrintendere l'intercomunicazione tra il portale PEOPLE erogatore dei servizi da un lato e i vari Identity Provider dall'altro è posta l'infrastruttura chiamata SIRAC. Quest'ultima, in particolare, ha il compito di ricevere le richieste di autenticazione per un determinato servizio scelto dall'utente e di propagarle verso uno degli Identity Provider disponibili e abilitati, dopo aver coinvolto l'utente stesso che può scegliere con quale di essi intende interagire. La piattaforma SIRAC dispone altresì

di funzionalità di Single-Sign-On (SSO) grazie alle quali è definito da essa un insieme di portali presso i quali viene condiviso il contesto di autenticazione. Questo equivale a fare in modo che un utente, autenticatosi in seguito all'accesso ad uno dei portali di tale insieme, si trova automaticamente autenticato anche per l'accesso agli altri, indipendentemente da quale è stato l'Identity Provider presso cui l'autenticazione effettiva è stata condotta.

Nella figura seguente è descritto, mediante diagramma di sequenza UML, uno scenario tipico di accesso ad un servizio erogato da un generico portale PEOPLE da parte di un utente che non ha ancora effettuato l'autenticazione presso alcuno dei portali gestiti dall'infrastruttura SIRAC. Nel diagramma sono evidenziati i principali attori-componenti presenti nel sistema, a partire dall'utente e dal servizio richiesto, evidenziando allo stesso tempo le due funzionalità principali svolte dall'infrastruttura SIRAC, rappresentate dalla componente di Single-Sign-On (SSO) e da quella di discovery degli Identity Provider (WAYF). Più in dettaglio i passi dello scenario illustrato sono i seguenti:

- l'utente accede ad uno dei servizi e-government erogati da un portale appartenente alla comunità PEOPLE.
- la richiesta dell'utente viene gestita dai componenti di integrazione con l'infrastruttura SIRAC dispiegati presso il portale PEOPLE, a protezione degli accessi.
- i componenti di integrazione con l'infrastruttura SIRAC verificano l'esistenza di una sessione di lavoro già autenticata (contesto di autenticazione locale) e, dal momento che l'utente si è appena presentato al portale, producono una richiesta di autenticazione diretta a SIRAC con l'indicazione del servizio scelto dall'utente.
- la richiesta di autenticazione viene inviata al componente SIRAC-SSO per l'attivazione della relativa procedura.
- alla ricezione della richiesta di autenticazione, il componente SIRAC-SSO verifica l'esistenza di una sessione di lavoro già autenticata relativa al portale PEOPLE presso cui il servizio è stato richiesto. Analogamente, anche in questo caso tale sessione non viene trovata e la richiesta deve procedere fino ad un Identity Provider.
- a questo scopo, SIRAC-SSO attiva il componente di discovery degli Identity Provider, SIRAC-WAYF.
- il componente SIRAC-WAYF presenta all'utente un'interfaccia con l'elenco degli Identity Provider noti all'infrastruttura SIRAC e disponibili per effettuare l'autenticazione

- l'utente sceglie su quale Identity Provider intende effettuare l'autenticazione
- SIRAC-WAYF restituisce la scelta dell'utente a SIRAC-SSO che può inviare la richiesta di autenticazione all'Identity Provider selezionato
- La richiesta di autenticazione raggiunge l'Identity Provider selezionato
- L'Identity Provider presenta all'utente un'interfaccia mediante cui immettere le credenziali per l'autenticazione.
- L'utente immette le credenziali.
- L'Identity Provider verifica che le credenziali immesse siano adeguate.
- L'Identity Provider prepara un messaggio di risposta in standard SAML 1.1 contenente i dettagli relativi all'avvenuta autenticazione e lo invia a SIRAC-SSO.
- SIRAC-SSO crea un contesto di autenticazione SSO.
- SIRAC-SSO estrae dal messaggio ricevuto dall'Identity Provider i dettagli relativi all'utente autenticatosi e li invia ai componenti di integrazione presso il portale PEOPLE originario.
- I componenti di integrazione presso il portale PEOPLE creano un contesto di autenticazione locale che potrà essere riutilizzato per un certo tempo durante gli accessi futuri allo stesso portale/servizio.
- Si procede all'attivazione del servizio richiesto dall'utente autenticatosi.
- Il servizio richiesto è erogato all'utente autenticatosi.

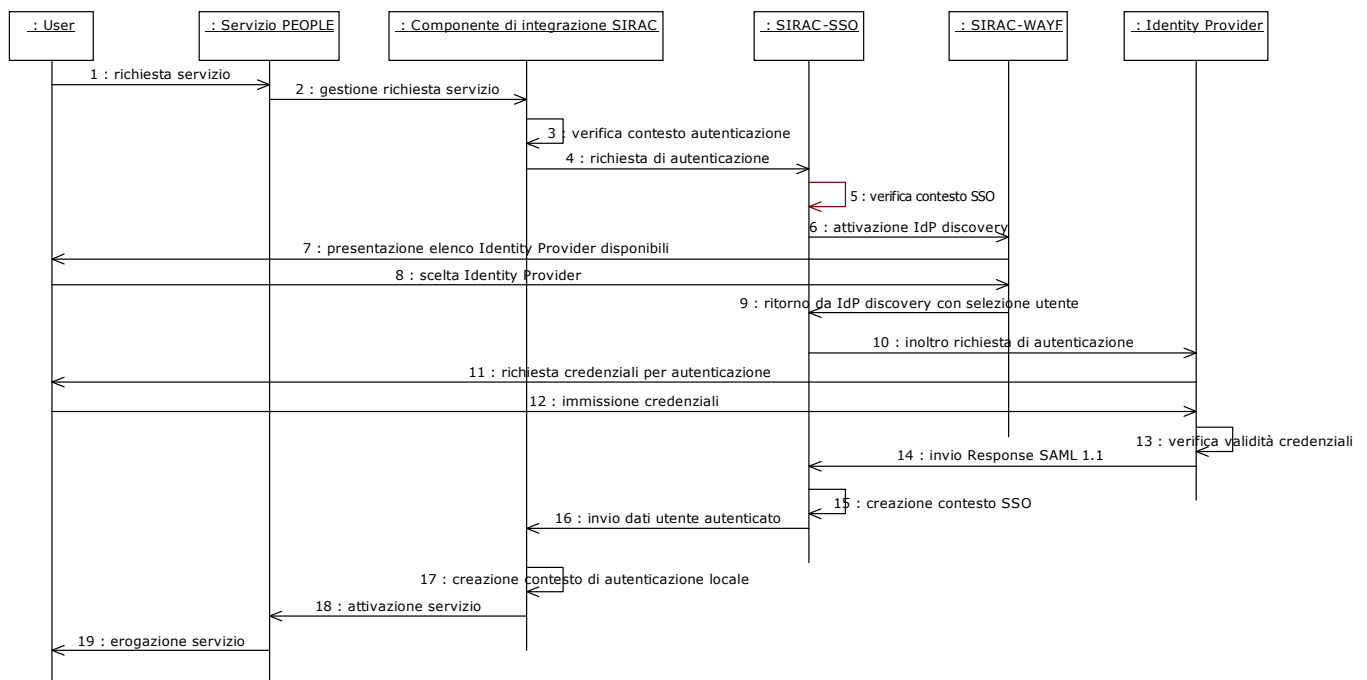


Figura 1 – L'accesso ad un servizio PEOPLE mediato da SIRAC-SSO

1.1.2. ICAR

Il progetto ICAR, attualmente in fase di attuazione e dispiegamento presso le Regioni, prevede tra i suoi interventi infrastrutturali la realizzazione di un sistema di gestione delle identità digitali federato nel quale si trovano ad interoperare diversi domini amministrativi. Ciascuno di tali domini dispone in generale di un insieme di erogatori di servizi applicativi (Service Provider) che possono avvalersi di una piattaforma per il controllo degli accessi e per la profilazione degli utenti; essa appare come un'entità distribuita e composta da svariati soggetti che a vario titolo sono abilitati a svolgere un ruolo di certificazione durante la fase di autenticazione (Identity Provider) o di gestione delle informazioni relative agli utenti (Attribute Authority). La complessità dell'intero sistema vengono mascherati ai singoli Service Provider mediante l'introduzione di un elemento di disaccoppiamento (Local Proxy) locale al proprio dominio amministrativo, che si fa carico di gestire tutte le richieste di autenticazione provenienti dal dominio, instradandole verso gli Identity Provider opportuni, coinvolgendo l'utente nella fase di discovery. Un elemento aggiuntivo dell'architettura, chiamato Profile Authority, si configura come il responsabile del mantenimento delle informazioni dei profili di un insieme di utenti, consentendo loro di scegliere in modo granulare quali tra esse utilizzare durante l'accesso ai servizi. Tale componente, previsto dallo scenario generale del progetto ICAR, può essere presente nel generico dominio amministrativo per gestire le

informazioni relative agli utenti che a tale dominio afferiscono; esso interagisce inoltre con le varie Attribute Authority presenti nella federazione allo scopo di ottenere le certificazioni delle varie parti dei profili che si trova a gestire. Grazie a questa infrastruttura, ogni utente, indipendentemente dal dominio di appartenenza, può fruire dei servizi di qualunque Service Provider federato, con la possibilità di autenticarsi presso uno qualunque degli Identity Provider federati e facendo circolare soltanto il set di informazioni strettamente necessarie per ciascun accesso. Anche nel progetto ICAR si fa ricorso alla notazione SAML per lo scambio dei messaggi e delle informazioni relative all'autenticazione degli utenti, ma a differenza del progetto PEOPLE, in ICAR la versione della specifica SAML impiegata è la più recente 2.0 invece che la 1.1 utilizzata in PEOPLE. Gli aspetti di fiducia e sicurezza vigenti nella federazione sono regolati da una terza parte fidata, nota come Responsabile del Dominio di Cooperazione o Garante, a cui è affidato il compito di abilitare i vari soggetti a svolgere i rispettivi ruoli (di certificazione, di intermediazione, di erogazione) mediante convalida a mezzo di firma digitale apposta sui appositi documenti in standard SAML 2.0 (metadati) esposti da ciascuno di tali soggetti e messo a disposizione della comunità.

Nella seguente Figura.1 è descritto, mediante diagramma di sequenza UML, uno scenario tipico di accesso ad un servizio erogato da un generico Service Provider facente parte della federazione ICAR da parte di un utente che non ha ancora effettuato l'autenticazione. Nel diagramma sono evidenziati i principali attori-componenti presenti nel sistema, a partire dall'utente e dal servizio richiesto, evidenziando l'attraversamento dei componenti Local Proxy e Profile Authority. Quest'ultimo può essere omesso, qualora non si renda necessario avvalersi delle relative funzionalità di gestione dei profili utente (o qualora esse vengano intraprese in altro modo, ad esempio direttamente ad opera di un Identity Provider). Si noti che nel diagramma per semplicità sono state omesse tutte le interazioni con l'entità nota con il nome di Authority Registry, responsabile della gestione delle informazioni relative a tutti i soggetti della federazione: per conoscere i vari indirizzi di destinazione dei messaggi da utilizzare nello scenario, infatti, i soggetti interagenti interrogano il registry che fornisce le coordinate opportune. Nella prima parte (passi da 1 a 4) di Figura.1 sono illustrate anche le interazioni essenziali generate quando un utente accede ai servizi di una delle Profile Authority allo scopo di creare o mantenere uno dei propri profili. In dettaglio i passi dello scenario sono i seguenti:

Fase di gestione profili

- l'utente accede ad una delle Profile Authority esistenti (tipicamente quella presso il proprio dominio amministrativo, ad esempio quella presso la propria Regione o Comune) per effettuare delle operazioni di creazione o gestione di uno o più profili;

- durante tali operazioni, la Profile Authority contatta una o più Attribute Authority che hanno titolo a certificare le informazioni dichiarate dall'utente (attributi);
- la Profile Authority riceve le varie certificazioni di attributo da parte delle Attribute Authority interrogate;
- la Profile Authority utilizza le certificazioni ricevute per aggiornare i profili mantenuti presso di sé.

Fase di accesso ai servizi

- l'utente richiede l'accesso ad un servizio erogato da uno dei Service Provider di uno dei domini della federazione
- il Service Provider, dopo aver verificato che la sessione di lavoro corrente non è autenticata, invia una richiesta di autenticazione in standard SAML 2.0 al Local Proxy del proprio dominio
- il Local Proxy accede all'Authority Registry per ottenere un elenco delle Profile Authority disponibili e presenta all'utente un'interfaccia con il relativo elenco da cui viene richiesta una scelta
- l'utente sceglie dall'elenco la Profile Authority presso cui sono memorizzati i propri profili
- il Local Proxy modifica opportunamente la richiesta di autenticazione e la inoltra alla Profile Authority scelta
- la Profile Authority destinataria contatta l'Authority Registry per ottenere l'elenco degli Identity Provider disponibili per la fase di autenticazione e presenta un'interfaccia all'utente con tale elenco da cui viene richiesta una scelta
- l'utente sceglie dall'elenco su quale Identity Provider intende effettuare l'autenticazione
- la Profile Authority modifica opportunamente la richiesta di autenticazione e la inoltra all'Identity Provider scelto
- l'Identity Provider presenta richiedi all'utente di immettere le credenziali per l'autenticazione
- l'utente inserisce le credenziali
- l'Identity Provider verifica che le credenziali inserite siano corrette

- l'Identity Provider prepara un messaggio di risposta in standard SAML 2.0 contenente i dettagli relativi all'avvenuta autenticazione e lo invia alla Profile Authority
- la Profile Authority utilizza la risposta ricevuta per ricercare tra i propri profili quelli dell'utente che si è autenticato e li presenta tra le scelte possibili all'utente
- l'utente sceglie il profilo che intende trasferire al Service Provider per l'accesso al servizio richiesto
- la Profile Authority assembla le informazioni del profilo selezionato in un nuovo messaggio di risposta SAML 2.0 che invia al Local Proxy del dominio mittente
- il Local Proxy del dominio mittente riceve il messaggio di risposta e lo gira internamente al dominio verso il Service Provider originariamente contattato dall'utente
- al termine, dopo che il Service Provider ha memorizzato il fatto che questa sessione di lavoro è ora autenticata, il servizio viene erogato all'utente

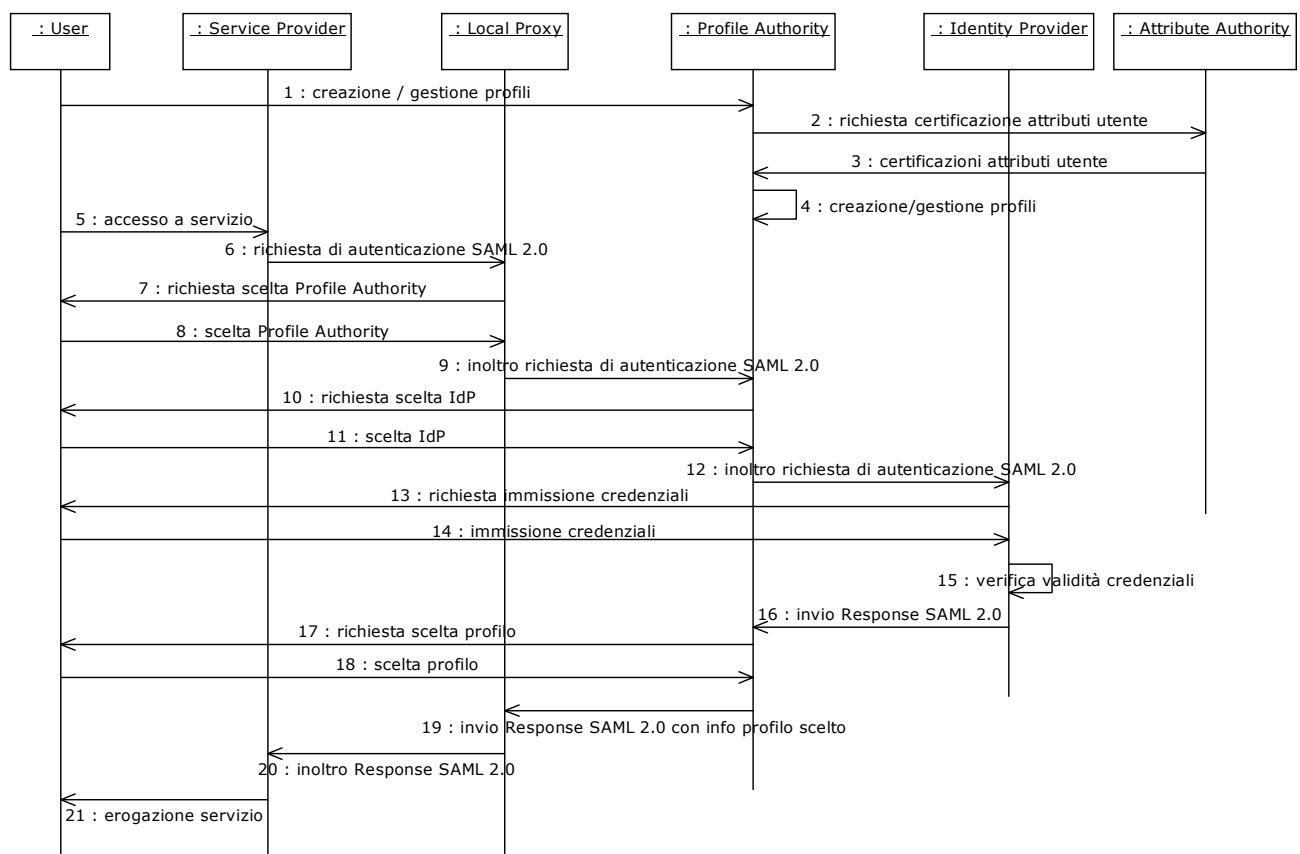


Figura.1 - Scenario di gestione profilo utente e accesso ad un servizio ICAR

1.1.3. Considerazioni

L'infrastruttura fedERa si propone di mantenere la compatibilità e l'interoperabilità con entrambi i modelli PEOPLE/SIRAC e ICAR sopra delineati nei loro tratti essenziali. In particolare fedERa valorizza i risultati di entrambi i progetti e consente pertanto agli erogatori di servizi PEOPLE già attivi sul territorio della Regione di continuare ad avvalersi delle funzionalità di Single-Sign-On e accesso agli Identity Provider preesistenti sul territorio; allo stesso tempo consente a tali erogatori di interagire, in modo trasparente rispetto all'attuale funzionamento, con l'intera federazione dei soggetti illustrati in precedenza nell'ambito del progetto ICAR. La soluzione offre pertanto pieno supporto ad entrambe le versioni della specifica e dei protocolli SAML (1.1 e 2.0) così come recepite ed implementate nelle infrastrutture SiRAC e ICAR, mantenendo invariate le attuali interfacce verso gli estremi della catena di interazione (Service Provider ed Identity Provider) e consentendo allo stesso tempo una più efficiente e sicura gestione dei dati dei profili dei vari utenti finali che richiedono l'accesso ai servizi online.

1.2. ARCHITETTURA E CARATTERISTICHE GENERALI DELL'INFRASTRUTTURA FEDERA

L'architettura del sistema fedERa è costituita da tre macro-componenti principali:

- Sistema di autenticazione (Identity Provider): erogano il servizio di autenticazione per gli utenti fedERa verificando le credenziali utente e preparando le asserzioni SAML (1.1 o 2.0) che dovranno essere trasmesse agli erogatori dei servizi finali;
- Gateway multiprotocollo di autenticazione: Componente con funzione di gateway di dominio e di mediatore fra i servizi di front-end erogati dagli enti sul territorio che richiedono l'autenticazione e gli Identity Provider della federazione (quindi non solo l'Identity Provider Federa). Il Gateway Multiprotocollo è responsabile di supportare le interazioni con i Service Provider ed Identity Provider della federazione utilizzando entrambi i protocolli SAML 1.1 e SAML 2.0.
- Sistema di gestione di identità digitali IdM: applicazione complessiva di gestione utenti con funzionalità per utenti di varie tipologie:
 - utenti fruitori del sistema di autenticazione, con funzionalità di registrazione, cambio password, cambio profilo e tutto quanto è richiesto in merito;

- o utenti della Registration Authority (RA), con funzionalità di provisioning utenti, reporting e altre funzionalità di gestione;
- o utenti amministratori, con funzionalità di gestione del sistema, di monitoraggio e di reporting.

Ognuno di tali elementi prevede un'interazione con l'utente, sia esso utente finale, utente di una Registration Authority o utente amministratore del sistema.

Uno schema logico complessivo di tali elementi può essere riassunto in Figura 2.

In tale figura gli elementi introdotti dal progetto FedERa sono evidenziati in colore giallo.

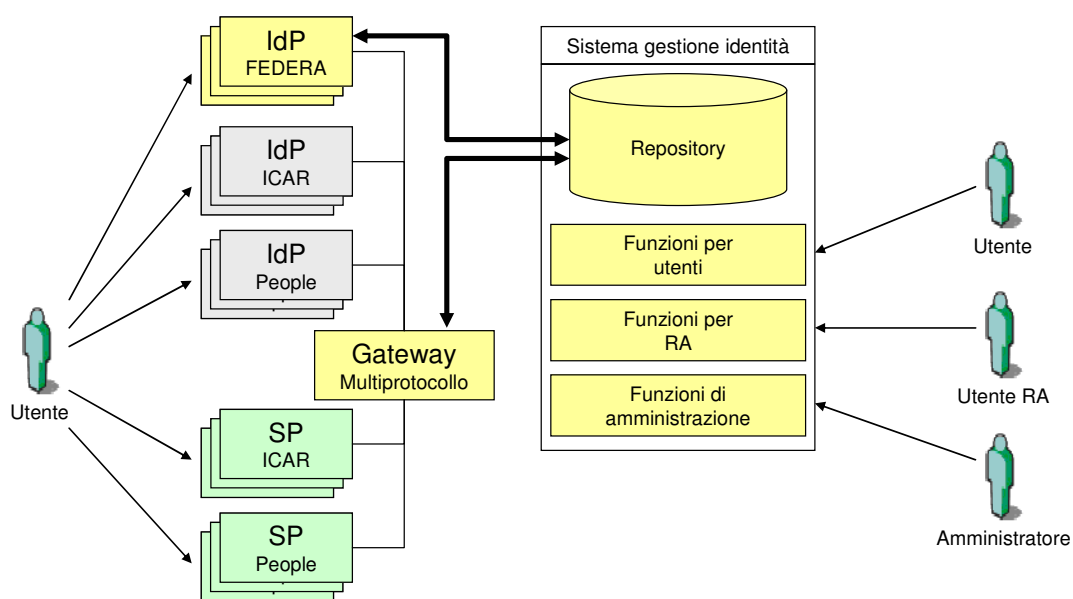


Figura 2 – Schema logico complessivo dell'architettura

Tutte le componenti realizzate saranno rilasciate in open source, senza necessità quindi da parte del committente di pagare costi di licenza per l'utilizzo delle componenti stesse.

1.3. SOGGETTI INTERAGENTI

Nello scenario operativo complessivo saranno presenti in generale i seguenti soggetti:

- IdP ICAR: sono tutti gli Identity Provider disponibili nella federazione ICAR al di fuori della Regione Emilia Romagna ed esterni al sistema FedERa.
- IdP PEOPLE: sono tutti gli Identity Provider PEOPLE qualificati a livello nazionale (es. Postecom, Infocamere). Tutti questi IdP sono omogenei tra loro per quanto riguarda il

processo di registrazione utenti.

- IdP FedERa: è il sistema di autenticazione di Lepida SpA.
- IdP locale: sono tutti gli eventuali Identity Provider locali a un dominio amministrativo che non devono essere resi noti al di fuori di esso (es. un repository di utenti locali ad uno specifico ente di RER).
- SP ICAR: sono tutti i Service Provider abilitati alla comunicazione con l'infrastruttura ICAR, presenti in domini amministrativi interni o esterni a RER. Tali SP si integrano con l'infrastruttura ICAR secondo quanto definito nel relativo documento di specifica architettureale.
- SP PEOPLE: sono tutti i Portali PEOPLE esistenti nei domini amministrativi di RER.
- SP ICAR/FedERa: sono tutti i Service Provider del dominio centrale di RER integrati con il sistema FedERa.
- AR ICAR: è l'Authority Registry centrale della federazione ICAR, gestito dal Garante della federazione ICAR. Censisce tutti gli IdP, tutte le PA e tutti i Local Proxy ICAR e in aggiunta anche il Gateway Multiprotocollo di FedERa (FedGW).
- LP ICAR: sono tutti i Local Proxy della federazione ICAR così come censiti in AR ICAR.
- PA ICAR: sono tutte le Profile Authority della federazione ICAR, così come censite in AR ICAR.
- FedGW: è il gateway multiprotocollo del dominio FedERa regionale, che sarà censito in ICAR AR al pari dei vari LP già presenti.
- FedAR: è una copia dell'AR ICAR, locale al dominio di FedERa. Oltre a tutti i soggetti censiti da AR ICAR, censisce anche tutti gli IdP PEOPLE associati agli enti sul territorio di RER.
- FedLGW (opzionale): è una versione del gateway multiprotocollo da dispiegarsi localmente a un dominio amministrativo di RER (es. un Comune) per gestire le autenticazioni verso i servizi erogati presso tale dominio. Svolge il ruolo di gateway di secondo livello tra in singolo ente locale e il gateway FedERa (FedGW).
- FedLAR (opzionale): è una copia di FedAR, presso il dominio di un ente locale di RER (es. un Comune) ed esterno al dominio centrale di RER e a qualunque altro dominio ICAR. Oltre a tutti i soggetti censiti da FedAR, censisce anche gli eventuali IdP locali a

tale dominio amministrativo.

1.4. DOMINI INTERAGENTI

Il sistema FedERa si troverà a operare in un ambiente nel quale sono presenti tutte le tipologie di soggetti presentate nel paragrafo precedente. Nel caso più generale tutti tali soggetti saranno dispiegati presso vari domini amministrativi, interni ed esterni a RER. Si farà di seguito riferimento alle seguenti tipologie di domini:

- Domini ICAR esterni a RER: comprendono SP, LP, PA e IdP ICAR di un generico ente che partecipa alla federazione ICAR;
- Dominio FedERa: comprende i SP ICAR del dominio FedERa regionale, il sistema di autenticazione e il gateway multiprotocollo (entrambi di Lepida SpA) e FedAR;
- Dominio di un ente locale di RER (es. un Comune): comprende in generale sia SP ICAR che SP PEOPLE, eventualmente alcuni IdP locali per autenticare tipologie particolari di utenti del dominio. Può, opzionalmente, includere anche un FedLGW e un FedLAR. Non comprende invece IdP ICAR poiché il sistema di autenticazione che sarà dispiegato nel dominio FedERa sarà dotato di funzionalità multi-dominio e, come tale, farà virtualmente parte di tale ente locale, in quanto in grado di erogare il servizio di autenticazione per gli utenti di tale ente, internamente a RER.

I soggetti e i domini interagenti introdotti sopra sono rappresentati nella seguente figura, dove sono visualizzate anche le relazioni che legano i vari Authority Registry presenti e descritti in precedenza con i soggetti da essi censiti. In questo modo risultano chiare le responsabilità del mantenimento di tali informazioni presso ciascun registro.

Si evidenzia che l'insieme degli IdP PEOPLE non fanno logicamente parte di alcuno dei domini amministrativi (Regione, Comuni ecc.), in quanto in tale progetto essi si configurano come entità indipendenti che possono erogare il servizio di autenticazione e registrazione a utenti di più domini. Esempi di tali IdP sono quelli messi a disposizione da Postecom e Infocamere. Si evidenzia anche che nemmeno l'Authority Registry ICAR entra a far parte di alcun dominio amministrativo, in quanto entità sotto la gestione e la responsabilità dell'autorità centrale a livello nazionale. Tale registro infatti esiste come copia master per l'intera federazione ICAR del quale è già oggi prevista l'esistenza di repliche locali, presso i vari LP delle regioni partecipanti.

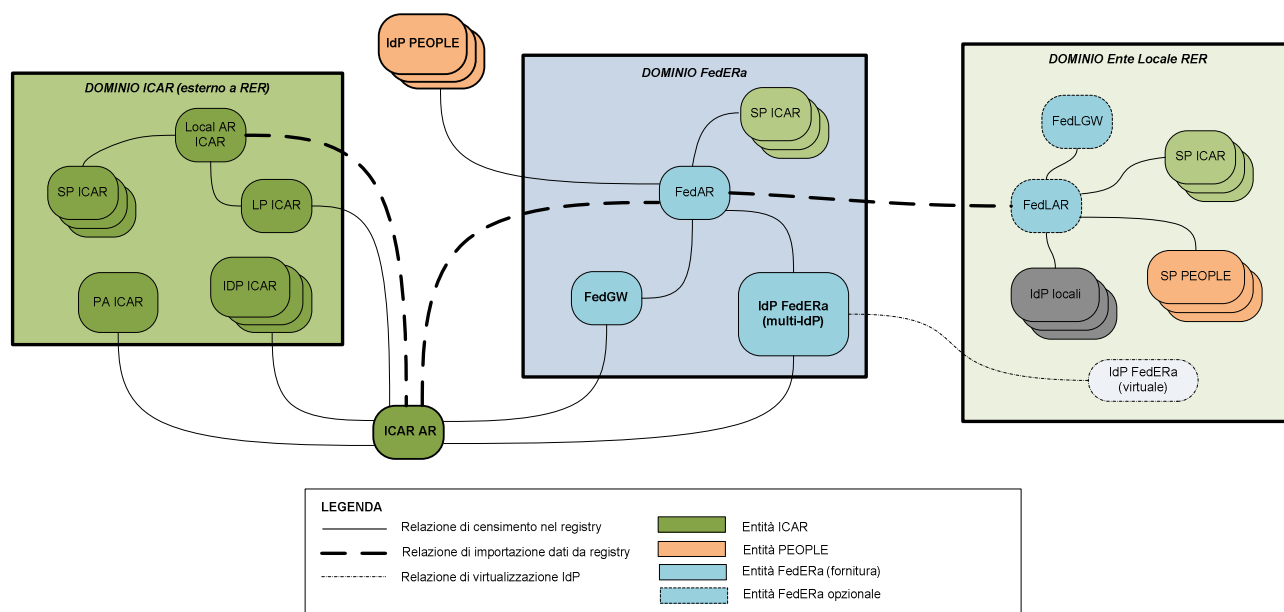


Figura4 – Quadro d'insieme FedERa

In colore azzurro sono stati indicati i componenti/entità del sistema fedERa. In particolare è evidenziato il gateway multiprotocollo (FedGW) ed il sistema di autenticazione (IdP FedERa) con i vari IdP “virtuali” che esso rappresenta localmente ai vari domini di RER. Per una migliore definizione di “IdP virtuale” si rimanda alla sezione successiva. Quest’ultimo diventa logicamente parte anche di tutti i domini degli enti locali presenti in RER che fruiscono del servizio di IdP erogato da IdP FedERa, il quale è, come detto, in grado di gestire una configurazione multi-dominio. Per questo IdP FedERa locale al generico ente RER è classificato come “virtuale”.

Gli “IdP locali” al generico dominio di RER sono da intendersi come IdP che gestiscono utenze particolari (es. CA-PEOPLE locali) e che non sono noti all’esterno di tale dominio. Tali IdP “legacy” si assume abbiano interfacce SiRAC/PEOPLE o ICAR e non sono oggetto del progetto FedERa.

Come oggetto del progetto FedERa sono stati considerati anche i registry locali di FedERa (FedAR e FedLAR), necessari per abilitare qualunque scenario d’interazione in conformità a quanto definito nel progetto ICAR: essi si configurano come copie locali dell’Authority Registry ICAR, al pari di quanto accade per i Local Authority Registry presenti nel generico dominio ICAR, con la differenza che essi sono in grado di gestire informazioni aggiuntive per quanto riguarda gli IdP censiti; in particolare vengono memorizzati il livello minimo di affidabilità dell’identità digitale e della policy per la password (cfr. 1.6) associato a tale IdP e la policy di default per la gestione della password. Da un punto di vista logico esiste una relazione di contenimento tra i vari Authority Registry, per cui FedLAR contiene tutti i dati presenti in FedAR, il quale a sua volta contiene tutti i dati presenti in ICAR AR.

Da ultimo si vuole sottolineare il fatto che la presenza di FedLGW e FedLAR presso il generico dominio di un ente locale di RER deve essere considerata opzionale (da cui il tratteggio in figura). Tuttavia, al gateway multiprotocollo è affidata la gestione dei CoT e dell'associazione ai vari servizi erogati nel proprio dominio (si veda la sezione successiva per dettagli). Questo comporta che dispiegare in ciascun dominio un gateway e un corrispondente AR locale consente di sgravare l'amministrazione regionale di gran parte dei compiti di gestione dei servizi erogati presso tale dominio contribuendo a garantire l'interoperabilità nei vari scenari d'interazione. L'assenza di tali elementi in uno dei domini locali non consentirebbe, inoltre, di gestire eventuali IdP locali al dominio a meno di non censirli anche in FedAR, rendendoli però così accessibili anche ad altri domini privi di registro locale e al dominio FedERa nel suo complesso, cosa che non si ritiene consigliabile. Per tali motivi e per mantenere un certo livello di autonomia agli enti locali e ridurre il carico su RER, è preferibile mantenere una copia locale del gateway e del registry presso i vari domini locali. Si noti comunque che dal punto di vista tecnico è possibile operare l'una o l'altra scelta, in modo indifferente.

1.5. CIRCLE-OF-TRUST

Uno degli obiettivi dell'infrastruttura fedERa è di supportare la definizione di Circle-of-trust (CoT) fra le entità della federazione. Più precisamente per Circle-of-Trust (CoT) si intende un insieme di IdP omogenei rispetto a:

- livello minimo di affidabilità dell'identità digitale ad essi associato (si veda la sezione successiva per ulteriori dettagli)
- livello minimo di password policy ad essi associato
- elenco degli attributi dei profili utente restituiti a valle dell'autenticazione

I CoT possono essere strutturati in modo gerarchico cioè un CoT può far riferimento ad altri CoT, oltre poter includere puntualmente alcuni IdP specifici. In questo modo è possibile rendere più agevole il processo di definizione dei CoT e mutuare alcune informazioni/requisiti già specificati per altri CoT nella definizione di uno nuovo.

Un SP può essere associato a uno e un solo CoT (eventualmente visto come aggregazione di CoT): mediante tale associazione, un SP indica quali sono gli attributi dei profili utente, il livello di affidabilità dell'identità e il livello di password policy richiesti. I requisiti relativi al metodo di autenticazione richiesto per l'accesso (es. smart-card, password ecc.) fanno parte del profilo di ciascun SP e verranno invece inseriti dal SP nei messaggi di richiesta di autenticazione. Per

quanto riguarda i SP PEOPLE, essi potranno essere inclusi solo in CoT nei quali sono presenti IdP che dichiarano di trasferire almeno tutte le informazioni presenti nel profilo PEOPLE, dei quali si accetta che non tutti vengano valorizzati. Tuttavia, nel caso in cui l'IdP non disponga di un valore per l'attributo relativo al domicilio elettronico dovrà utilizzare per esso lo stesso valore dell'attributo e-mail, che dovrà essere reso obbligatorio.

Ad un CoT possono essere associati più SP, cioè tutti quelli che presentano i medesimi requisiti (vedi punto precedente).

1.6. AFFIDABILITÀ DELL'IDENTITÀ E DELL'AUTENTICAZIONE

L'infrastruttura FedERa pone come requisito la possibilità di discriminare l'accesso ad un servizio da parte di un Service Provider basandosi su tre fattori complementari: in particolare richiede che sia possibile selezionare, a priori e nel modo più trasparente possibile, il *livello di affidabilità dell'identità digitale* e il *livello minimo di password policy* dell'utente (oltre ovviamente all'insieme di meccanismi di autenticazione considerati accettabili dallo specifico servizio), in modo da accettare risposte di autenticazione che garantiscono un certo livello di *affidabilità complessiva dell'autenticazione* dell'utente. In altre parole deve essere possibile, ad esempio, selezionare a priori soltanto gli utenti per i quali è garantita un'alta affidabilità nell'accertamento dell'identità e un livello di password policy uguale o superiore a quello di interesse per lo specifico servizio o insieme di servizi erogati da un Service Provider.

Per soddisfare tale requisito è necessario che:

- nella richiesta di autenticazione preparata dal Service Provider e ricevuta dall'IdP attraverso l'infrastruttura fedERa sia possibile indicare i requisiti minimi desiderati di affidabilità complessiva dell'autenticazione dell'utente; in alternativa, è necessario inviare tale richiesta ad un soggetto per il quale si sa a priori che l'autenticazione effettuata risulta compatibile con i requisiti;
- la risposta di autenticazione preparata dall'IdP e restituita all'infrastruttura FedERa consenta la verifica a posteriori del rispetto del livello minimo di affidabilità complessiva dell'autenticazione precedentemente richiesto.

Inoltre tali requisiti devono essere soddisfatti, ove possibile, senza introdurre estensioni particolari nel protocollo SAML utilizzato per l'interazione tra i diversi componenti dell'infrastruttura FedERa.

Relativamente al requisito sopraindicato, con la dicitura **“livello di affidabilità dell'identità**

digitale” viene inteso nel seguito il livello di affidabilità dell’identità dell’utente, definito dal sistema sulla base della procedura di accertamento dell’identità in fase di registrazione.

Vi sono poi altri elementi tra loro complementari, alcuni che fanno parte del profilo dell’utente e altri specifici dell’interazione con l’IdP, che insieme al primo concorrono a formare il **livello di affidabilità complessivo dell’autenticazione**.

Più in dettaglio, nell’infrastruttura FedERa, gli elementi che concorrono alla definizione dell’affidabilità complessiva dell’autenticazione per un utente sono i seguenti:

Il livello di affidabilità dell’identità digitale. Si tratta di una proprietà del profilo utente non dipendente dalla specifica interazione con l’IdP. I valori possibili per tale proprietà sono i seguenti:

- non identificato;
- identificazione indiretta;
- identificazione certa.

La password policy attiva per lo specifico utente. Anche questa è una proprietà del profilo dell’utente e non dipende dalla specifica interazione con l’IdP, inoltre il valore di questa proprietà è rilevante soltanto nel caso in cui venga utilizzata la password come meccanismo di autenticazione nella specifica interazione con l’IdP. I valori possibili per questa proprietà sono:

- nessuna password policy applicata;
- password policy conforme ai requisiti per l’accesso a dati personali;
- password policy conforme ai requisiti per l’accesso a dati sensibili.

Il meccanismo di autenticazione utilizzato. Questa proprietà, a differenza delle precedenti, non è una proprietà del profilo dell’utente, ma dipende dal meccanismo di autenticazione effettivamente utilizzato dall’utente in ciascuna specifica interazione con l’IdP:

- userid/password;
- OTP;
- SmartCard;

Nel sistema fedERa gli IdP sono quindi classificati in base ai descritti elementi che determinano l’affidabilità dell’identità:

- IdP di tipo ‘C’. Attestano l’autenticazione di utenti caratterizzati da una bassa affidabilità dell’identità digitale (es. utenti che hanno effettuato la registrazione online)

- IdP di tipo 'B'. Attestano l'autenticazione di utenti caratterizzati da una affidabilità media dell'identità digitale (es. utenti che hanno effettuato la registrazione indiretta con invio di raccomandata)
- IdP di tipo 'A'. Attestano l'autenticazione di utenti caratterizzati da una alta affidabilità dell'identità digitale (es. utenti che hanno effettuato la registrazione con riconoscimento de-visu). Tra questi IdP si effettua l'ulteriore distinzione fra:
 - o IdP di tipo A 'base'. Attestano l'autenticazione di tutti gli utenti ad alta affidabilità dell'identità digitale e attribuzione delle credenziali.
 - o IdP di tipo A+. Attestano l'autenticazione degli utenti ad alta affidabilità dell'identità digitale per i quali è definita almeno una password policy conforme a quella richiesta per l'accesso a dati personali.
 - o IdP di tipo A++. Attestano l'autenticazione degli utenti ad alta affidabilità dell'identità digitale per i quali è definita almeno una password policy conforme a quella richiesta per l'accesso a dati sensibili.

I singoli IdP devono essere singolarmente indirizzabili sia dall'interno dell'infrastruttura FedERa sia dall'esterno, in modo da poter stabilire univocamente (e a priori) le proprietà minime di affidabilità degli utenti per i quali il singolo IdP emette risposte di autenticazione.

In Tabella 1 si riportano i casi possibili con le relative combinazioni: non sono presenti i casi considerati incongruenti, vale a dire l'applicazione di password policy per utenti senza identificazione certa.

TIPO IDP	IDENTIFICAZIONE	PWD POLICY	METODO DI AUTENTICAZIONE	RISPOSTA ALL'UTENTE	RISPOSTA AL SERVIZIO
ANY	Non registrato	N/A	SmartCard	Autenticazione ok	Utente autenticato
C	Non identificato	No policy	Password	Autenticazione ok	Utente autenticato
			OTP	Autenticazione non possibile	nessuna risposta
			SmartCard	Autenticazione ok (*)	Utente autenticato
B	Identificazione	No policy	Password	Autenticazione ok	Utente autenticato

	e Indiretta		OTP	Autenticazione ok	Utente autenticato		
			SmartCard	Autenticazione ok (*)	Utente autenticato		
A	Identificazione Certa	No policy	Password	Autenticazione ok	Utente autenticato		
			OTP	Autenticazione ok	Utente autenticato		
			SmartCard	Autenticazione ok	Utente autenticato		
A+		Dati personali		Password	Autenticazione ok (**)	Utente autenticato	
				OTP	Autenticazione ok	Utente autenticato	
				SmartCard	Autenticazione ok	Utente autenticato	
A++			Dati Sensibili		Password	Autenticazione ok (**)	Utente autenticato
					OTP	Autenticazione ok	Utente autenticato
					SmartCard	Autenticazione ok	Utente autenticato

Tabella 1 - Risposte all'utente e al servizio che l'IDP deve fornire per livello di identificazione utente, policy sulla password e tipo di autenticazione effettuata dall'utente

() In questo caso il sistema dovrebbe proporre all'utente, ad autenticazione avvenuta, di effettuare un upgrade del livello di affidabilità della propria **identità**, analogamente a quanto previsto dal caso d'uso "Identificazione tramite CIE/CNS".*

*(**) Solo se il livello effettivo di password policy associata all'utente autenticato corrisponde con il livello minimo associato alla tipologia dell'IdP.*

Ogni IdP virtuale restituirà la risposta di autenticazione ad esso relativo se l'utente soddisfa il livello di affidabilità minimo che egli certifica.

1.7. CONSIDERAZIONI AGGIUNTIVE

Un IdP è associato ad un dominio di utenti che possono utilizzarlo per autenticarsi dopo aver svolto fase di registrazione online secondo le varie modalità supportate. Da un punto di vista puramente concettuale, uno stesso IdP può essere in grado di supportare livelli dinamici di affidabilità dell'identità, cioè in grado di autenticare utenti che hanno seguito processi di registrazione differenti.

Il sistema di autenticazione che sarà realizzato, noto come "IdP FedERa", pur essendo realizzato come un singolo IdP e dispiegato nel dominio centrale di RER, potrà supportare i vari domini di

utenti degli enti locali di RER (es. Comuni, Province), presentandosi così come tanti IdP, ciascuno assegnato ad uno di tali enti. In conformità a quanto affermato sopra relativamente alla gestione dei vari livelli di affidabilità dell'identità e dell'autenticazione, ciascuno di tali IdP potrà essere ulteriormente specializzato in modo da gestire i vari insiemi di utenti sopra definiti, nell'ambito di ciascuno dei domini di RER. Si avrà così ad esempio, nell'ambito dell'IdP FedERa, l'IdP del Comune di Modena di tipo A+, l'IdP dello stesso comune di tipo B e un terzo di tipo C. Lo stesso, potenzialmente, per tutti gli altri domini di RER. Ciascuno degli IdP virtuali così ottenuti disporrà di un proprio end-point al quale essere contattato per ricevere i messaggi di richiesta di autenticazione.

Per garantire l'interoperabilità con la federazione ICAR, nella quale si assume che tutti gli IdP che ne fanno parte supportino unicamente credenziali ad alto livello di affidabilità, per quanto riguarda FedERa dovranno essere registrati presso l'Authority Registry ICAR centrale i soli IdP FedERa di tipo A++. Ciò sarà possibile in quanto ciascuno degli IdP virtuali sarà dotato del proprio identificativo univoco (come da specifica SAML 2.0), uno per ciascun livello di affidabilità corrispondente. In questo modo, solo gli utenti FedERa di un generico dominio di RER che hanno seguito un processo di registrazione ad alta affidabilità e sono dotati del corretto livello di policy per la password potranno accedere a servizi esposti da un SP della federazione ICAR.

Per quanto riguarda i domini ICAR a livello nazionale con i quali è richiesto che il sistema FedERa sia interoperabile, gli utenti afferenti a tali domini dovranno poter far uso del componente Profile Authority, allo scopo di utilizzare un certo numero di profili personali per integrare le informazioni fornite ai servizi cui intendono accedere. Questo deve valere in particolare per l'accesso ai servizi all'interno di FedERa, che non prevede il dispiegamento di una propria Profile Authority.

2. CASI D'USO DI INTEGRAZIONE DI SERVIZI

La funzionalità principale del gateway multiprotocollo consiste nell'abilitare il processo di fruizione dei servizi per i quali è richiesta autenticazione degli utenti. In particolare, durante tale processo di fruizione il gateway è contattato da parte dei Service Provider erogatori dei servizi dei quali si richiede l'accesso. A sua volta, nell'ambito di tale funzionalità il gateway dovrà contattare gli utenti finali a cui sottoporre una richiesta di scelta degli Identity Provider da utilizzare per l'autenticazione ed infine tali Identity Provider scelti per attivare la fase di autenticazione vera e propria, ricevendo da essi il relativo responso. Ove possibile, durante la propria attività di intermediazione dell'autenticazione degli utenti, il gateway multiprotocollo realizzerà anche la funzionalità di Single-Sign-On (SSO), mediante la quale il gateway risponderà ad un Service Provider abilitando l'accesso, senza coinvolgere un Identity Provider, se l'utente richiedente aveva già completato con successo un'autenticazione per l'accesso ad un Service Provider afferente allo stesso Circle-of-Trust. I casi d'uso di dettaglio relativi a questa funzionalità sono illustrati in Figura .

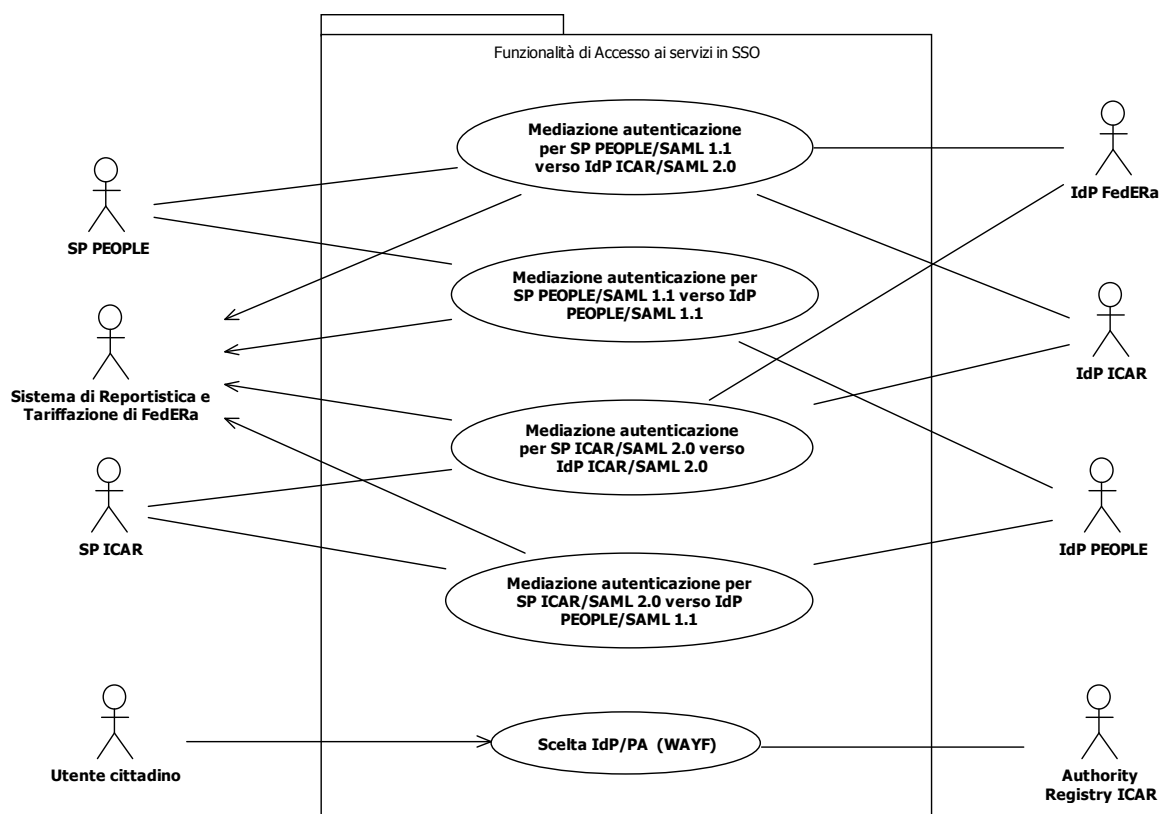


Figura 5- Casi d'uso per la Funzionalità di accesso ai servizi e SSO

Per garantire la massima interoperabilità rispetto alle tipologie di servizi coinvolti e di Identity

Provider disponibili, la funzionalità di accesso ai servizi si specializzerà in altrettante funzionalità più specifiche per supportare SP PEOPLE e ICAR, così come IdP PEOPLE e ICAR, in tutte le relative combinazioni. Dovendo interfacciarsi con un'entità PEOPLE (SP o IdP) verrà adottato il protocollo di comunicazione SAML 1.1, laddove per interagire con entità ICAR o FedERa sarà utilizzato il protocollo SAML 2.0. Come sarà chiaro dal dettaglio degli scenari d'interazione descritto successivamente, la funzionalità di accesso ai servizi vedrà coinvolto anche un Authority Registry FedERa (o quello del dominio FedERa o quello del dominio locale all'ente) per poter ottenere informazioni relative agli altri soggetti con i quali occorre interagire. Nell'ambito della funzionalità di accesso ai servizi il gateway multiprotocollo effettuerà anche la gestione del single-sign-on delle sessioni autenticate, limitatamente ai servizi che afferiscono ad uno stesso CoT: un utente autenticatosi per l'accesso ad uno di essi non dovrà autenticarsi nuovamente per accedere agli altri di tale gruppo. L'appartenenza di due servizi allo stesso CoT garantisce l'omogeneità degli insiemi di attributi richiesti da essi, rendendo quindi possibile il single-sign-on (cfr. primo scenario d'interoperabilità per maggiori dettagli).

Nel seguito si illustreranno i dettaglio gli scenari di interazione per la funzionalità di accesso ai servizi e SSO che risultano essere i più articolati e che richiedono il coinvolgimento del maggior numero di attori all'interno dell'infrastruttura.

2.1. SCENARI D'INTERAZIONE CON GATEWAY MULTIPROTOCOLLO FEDERA E SENZA GATEWAY LOCALE

In questa sezione sono illustrati alcuni scenari nei quali varie tipologie di utenti accedono a varie tipologie di servizi, seguendo un processo mediato e controllato dall'infrastruttura FedERa. Al centro degli scenari vi è il componente di gateway multiprotocollo ma le interazioni avvengono tra tutte le entità presentate in precedenza. Negli scenari analizzati saranno considerate le varie combinazioni possibili di servizi e utenti che vogliono accedervi, illustrando puntualmente lo scambio di messaggi che intercorre in ciascuno dei casi e mettendo in evidenza gli eventuali punti di criticità. Verranno dapprima presentati alcuni scenari nei quali viene dispiegato soltanto il gateway multiprotocollo centrale, nel dominio FedERa e successivamente, nella sezione 2.2 delle varianti dove invece presso i vari domini degli enti locali di RER viene dispiegato una copia locale del gateway (FedLGW), unitamente ad una copia locale dell'Authority Registry FedERa (FedLAR). Entrambe le tipologie di scenari presentano vantaggi e svantaggi, derivanti dall'adozione o meno del gateway locale in aggiunta a quello, sempre presente, a livello centrale. Per ragioni di spazio, nei diagrammi di sequenza che saranno presentati non sono stati dettagliati tutti i componenti

interni a FedGW coinvolti nelle interazioni. Dove ritenuto opportuno verranno mostrati i diagrammi di sequenza UML dei vari scenari, con funzione di service flow ma dotati di un livello di formalità e completezza rappresentativa maggiore.

2.1.1. Accesso a servizi ICAR/FedERa per utenti ICAR/FedERa nell'ambito del dominio regionale

Questo scenario è relativo ad un utente che si autentica presso il sistema di autenticazione (IdP FedERa) di RER e appartiene al dominio regionale centrale (cioè non afferisce ad alcuno dei domini degli enti locali di RER). Tale utente intende accedere ad un servizio ICAR erogato nello stesso dominio FedERa centrale. Il diagramma della sequenza delle interazioni che intercorrono in questo caso è illustrato nella figura seguente.

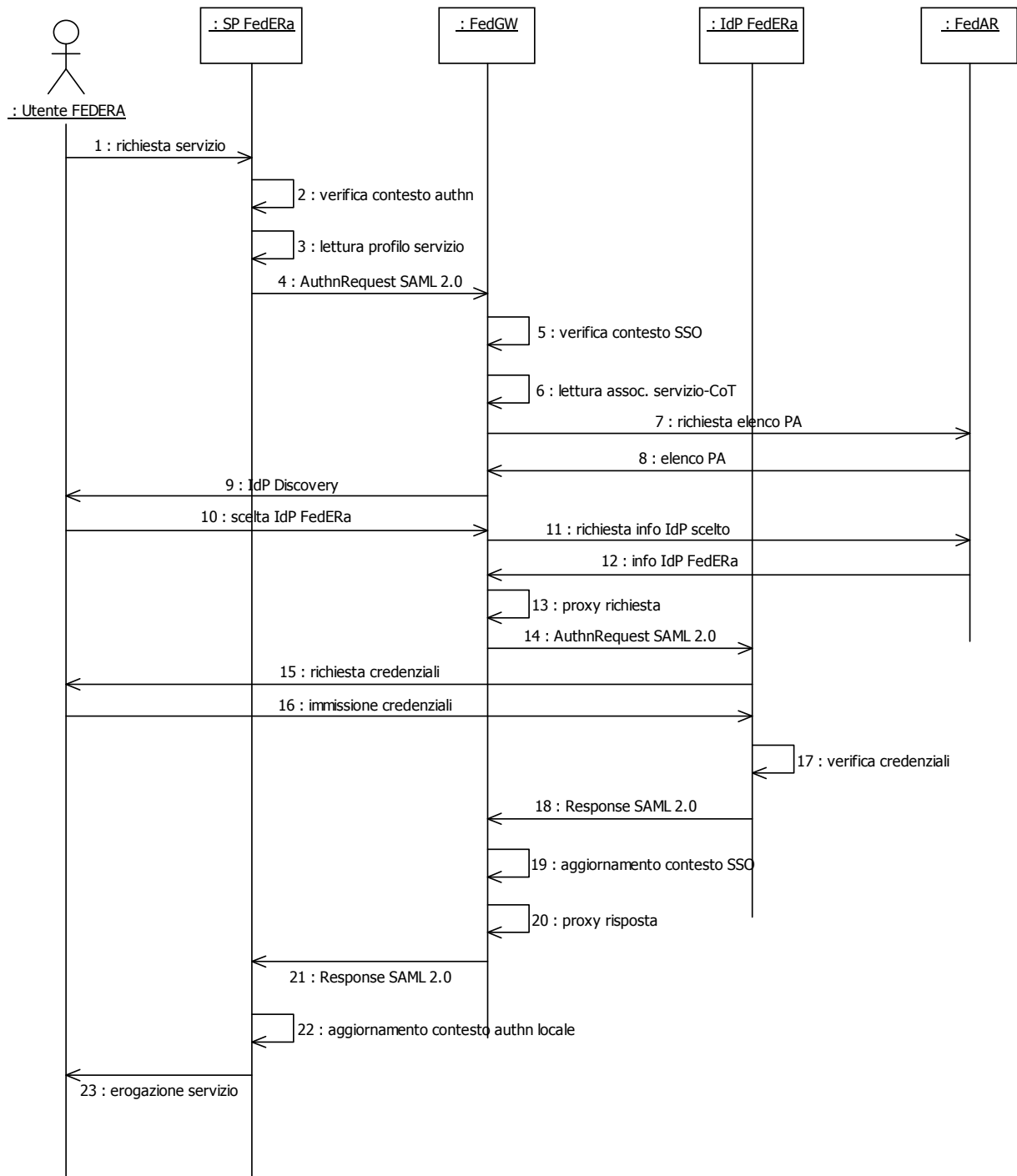


Figura 6 - Accesso ad un servizio ICAR/FedERa da parte di un utente del dominio regionale di FedERa

In questo caso l'utente appartiene al dominio FedERa, e dispone quindi di un account valido presso l'IdP FedERa, cioè un account per cui le credenziali immesse riconducono ad una registrazione effettuata con una delle modalità supportate dal sistema di gestione dell'identità

digitale e conforme a quella associata al CoT associato al servizio richiesto. Lo scenario si articola quindi nei seguenti passi: dopo che l'utente ha richiesto l'accesso ad un servizio erogato nel dominio FedERa, il SP verifica che la sessione di lavoro non sia già stata autenticata (in tale caso risponderebbe immediatamente all'utente erogando il servizio). Legge quindi le informazioni del proprio profilo di servizio che stabilisce le modalità di autenticazione che devono essere richieste (es. autenticazione con password, con smart-card ecc.) e le usa per comporre un messaggio AuthnRequest SAML 2.0 che invia a FedGW. Ricevuto il messaggio, FedGW controlla anzitutto se non esiste già una sessione SSO attiva per il CoT cui è associato il servizio richiesto: in caso affermativo risponde generando un nuovo messaggio Response SAML 2.0 con i dati dell'utente che si era già autenticato, riproducendo la modalità di autenticazione utilizzata in origine e gli stessi attributi prodotti dall'IdP che era stato utilizzato. In aggiunta, viene inserito nel messaggio di Response SAML 2.0 anche l'asserzione di autenticazione prodotta dall'IdP, come attestazione dell'effettiva autenticazione avvenuta. Nel caso in cui invece la sessione SSO non venga trovata, il gateway risolve il CoT relativo al servizio richiesto e attiva la fase di IdP Discovery, chiedendo all'utente di scegliere uno degli IdP afferenti a tale CoT. Nella pagina di scelta il gateway inserisce anche la possibilità per l'utente di indicare l'eventuale Profile Authority che intende utilizzare per integrare le informazioni sul proprio profilo. L'elenco delle PA da presentare è ottenuto mediante apposita richiesta a FedAR. In questo caso si assume che l'utente FedERa non disponga di profili gestiti da alcuna PA della federazione ICAR; la sua scelta riguarda pertanto unicamente uno degli IdP tra quelli proposti, in particolare l'utente sceglie l'IdP FedERa relativo al dominio centrale. FedGW riceve la scelta, modifica il messaggio di AuthnRequest (proxy) e lo invia all'IdP selezionato, ove avviene l'autenticazione mediante scambio di credenziali con l'utente. Se le credenziali immesse sono corrette l'IdP crea un messaggio Response SAML 2.0 che invia a FedGW il quale aggiorna il proprio contesto SSO per tale sessione, modifica il messaggio (proxy) e lo invia al SP originario (che era stato mascherato a IdP FedERa nell'interazione con esso). Il SP a sua volta aggiorna il proprio contesto di autenticazione locale ed eroga il servizio all'utente.

Variante per utenti che dispongono di un profilo presso una Profile Authority

Nel caso di utenti che dispongono di un profilo mantenuto ad opera di una delle Profile Authority della federazione ICAR, è possibile, in fase di IdP Discovery, selezionare anche una Profile Authority presso cui è presente il profilo integrativo che si intende utilizzare per l'accesso al servizio. In questo caso l'interazione n.14 nel diagramma di Figura viene destinata alla Profile Authority scelta, nel dominio dell'utente. Tale PA non ha bisogno di richiedere nuovamente all'utente la scelta dell'IdP per l'autenticazione, dato che FedGW inserisce nel messaggio di

richiesta¹ tale informazione. In tale caso, il resto delle interazioni si svolgono in modo identico a qualunque scenario ICAR, che porta alla selezione di un profilo utente e al ritorno su FedGW in modo analogo a quanto avviene nello scenario base. Si rimanda alla documentazione ICAR INF-3 per maggiori dettagli su tali interazioni.

2.1.2. Accesso a servizi ICAR/FedERa per utenti PEOPLE sul territorio di RER

Questo scenario è simile al precedente in quanto il servizio acceduto è un servizio erogato nel dominio FedERa di RER, con la differenza che l'utente richiedente afferisce ad un IdP PEOPLE che eroga il servizio di autenticazione ad un dominio (es. un Comune PEOPLE di RER). La sequenza di interazioni è illustrata nella figura seguente.

¹ L'indicazione alla PA di quale IdP utilizzare per l'autenticazione viene inserita nell'elemento "IDPList" della struttura "Scoping" dei messaggi AuthnRequest SAML 2.0

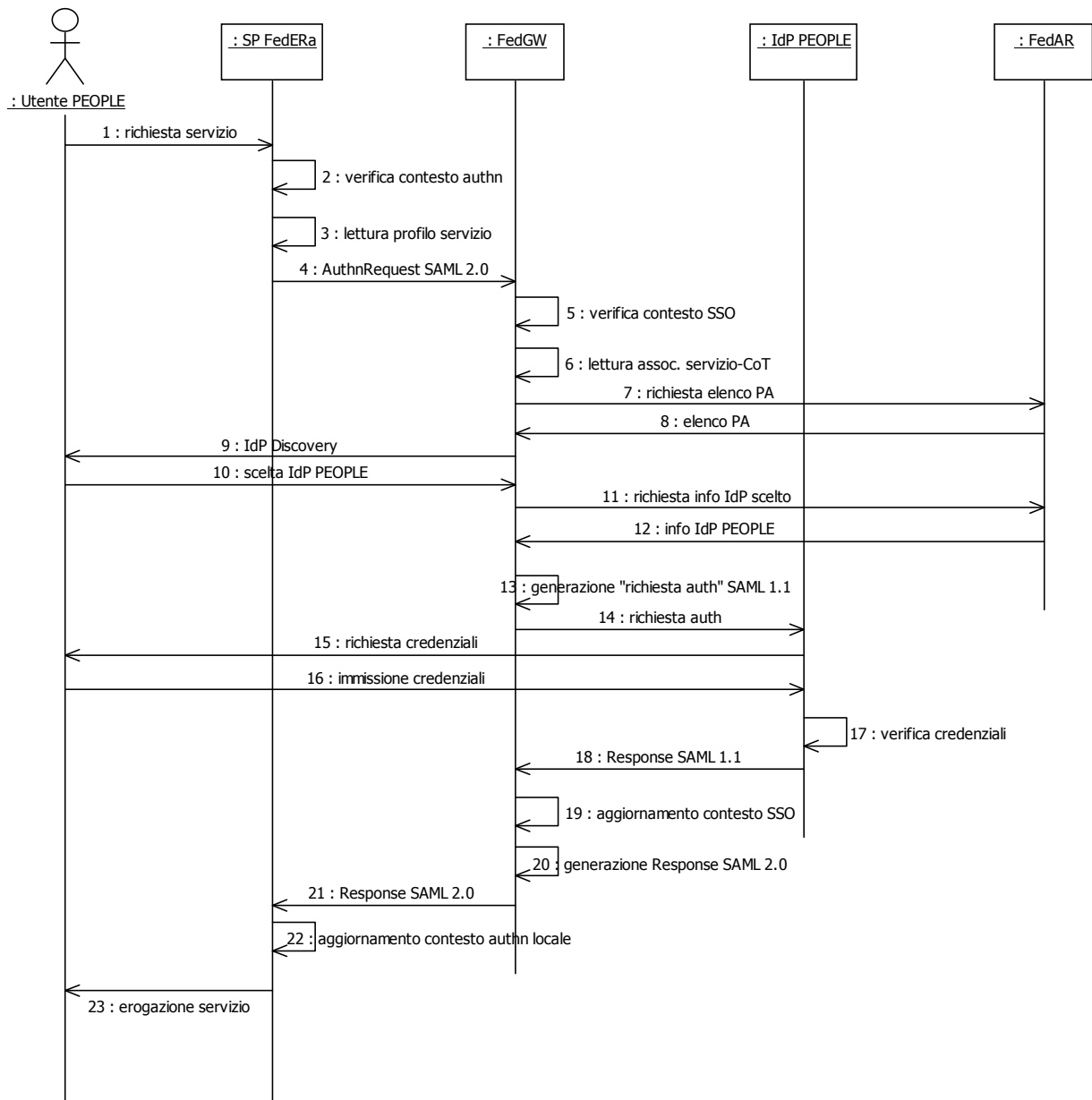


Figura 7 - Accesso ad un servizio ICAR/FedERa da parte di un utente PEOPLE sul territorio di RER

Si noti tuttavia che in questo scenario vi sono due importanti differenze nel comportamento del gateway multiprotocollo nella sequenza di andata e in quella di ritorno (interazioni 13 e 20): il gateway infatti ha il compito di conciliare il protocollo utilizzato per le richieste in ingresso (SAML 2.0) con quello da utilizzare per le richieste in uscita verso l'IdP PEOPLE (SAML 1.1). In particolare, dal momento che nel caso del protocollo SAML 1.1 non esiste un vero messaggio di richiesta di autenticazione, introdotto nella versione 2.0 del protocollo, la richiesta consisterà in un messaggio HTTP-GET o HTTP-POST come descritto nella relativa interfaccia di uscita, in

conformità alle specifiche SiRAC/PEOPLE. La richiesta generata dovrà essere indirizzata al servizio, presso l'IdP PEOPLE, in grado di richiedere all'utente delle credenziali in modo conforme al contesto di autenticazione richiesto, come presente nel messaggio AuthnRequest inviato dal SP FedERa. Dal momento che FedAR, come definito dalla specifica ICAR INF-3, non mantiene informazioni relative a diversi indirizzi presso un IdP che possono attivare modalità di autenticazione diverse e poiché per le entità PEOPLE non è prevista la presenza di file di metadati (che peraltro non sono definiti nella versione 1.1 della specifica SAML), ne consegue che l'Authority Registry di FedERa (FedAR) dovrà gestire questo tipo di informazioni aggiuntive, valide unicamente per IdP PEOPLE e non applicabili ad alcun altro IdP SAML 2.0. Anche durante la sequenza di risposta, il gateway multiprotocollo dovrà svolgere una funzione di adattamento, opposto, dal protocollo SAML 1.1 utilizzato dal messaggio ricevuto da IdP PEOPLE, a SAML 2.0 da utilizzare per rispondere a SP FedERa. La struttura dei messaggi di Response nei due protocolli è piuttosto simile, pertanto per questo adattamento non vengono evidenziate particolari criticità.

Da ultimo, si sottolinea che nel caso di scelta di un IdP PEOPLE, l'interfaccia di IdP Discovery non consentirà all'utente scegliere anche una Profile Authority per aggiungere un eventuale profilo personale che integri i dati restituiti dall'IdP (cfr. variante allo scenario precedente). La necessità di adattare il protocollo in uscita verso l'IdP PEOPLE non consentirebbe infatti di inviare un messaggio di AuthnRequest ad una generica Profile Authority della federazione ICAR, poiché questa non dispone di capacità di interagire con l'IdP PEOPLE scelto. Nel caso di accesso da parte di utenti PEOPLE, pertanto, al servizio richiesto potrà pervenire soltanto l'insieme di attributi standard, così come definito dalla specifica SiRAC/PEOPLE.

2.1.3. Accesso a servizi ICAR di un ente locale di RER per utenti ICAR/FedERa

Questo scenario è una variante dei precedenti, con la differenza che ad essere acceduto è un servizio ICAR di uno dei domini degli enti locali di RER (es. un Comune). In questo caso nulla cambia nella sequenza di interazioni se non il SP contattato. Si sottolinea che in questo caso il gateway centrale di FedERa dovrà riconoscere (mappare) tutti gli SP ICAR presenti presso i vari enti locali di RER, mantenendo le informazioni relative ai CoT di afferenza e non potranno essere gestiti IdP locali al dominio dell'ente.

2.1.4. Accesso a servizi PEOPLE di un ente locale di RER per utenti ICAR/FedERa

In questo scenario, a differenza dei precedenti, il servizio richiesto è erogato da un SP PEOPLE

che interagisce con l'esterno in modo conforme alle specifiche SiRAC/PEOPLE e al protocollo SAML 1.1. La sequenza di interazioni non è sostanzialmente diversa da quella del primo scenario presentato, salvo per il fatto che al gateway multiprotocollo pervengono delle richieste di autenticazione che specificano unicamente il servizio scelto dall'utente e la modalità di autenticazione (debole o forte), così come nota al SP PEOPLE tramite accesso al proprio profilo. Il gateway multiprotocollo, infatti, in questa situazione si comporta al pari del sottosistema SiRAC SSO così come dispiegato presso i portali PEOPLE. Alla ricezione di tale richiesta lo scenario prosegue come già indicato, con la richiesta all'utente di scelta dell'IdP che in questo caso è un IdP FedERa. Dato si intende accedere ad un servizio PEOPLE, tale IdP deve necessariamente essere in grado di trasferire tutte le informazioni del profilo PEOPLE richiesto dal servizio². A valle della scelta dell'IdP, il gateway dovrà adattare il protocollo in uscita al fatto che l'IdP da contattare è conforme allo standard SAML 2.0. Il resto delle interazioni resta identico salvo la penultima in cui il gateway deve produrre un messaggio di risposta al SP conforme alle specifiche SiRAC/PEOPLE, contenente cioè tutti i dati del profilo PEOPLE.

2.1.5. Accesso a servizi PEOPLE di un ente locale di RER per utenti PEOPLE di RER

L'ultimo scenario presentato nel caso di presenza di un unico gateway centrale coinvolge sia servizi che utenti PEOPLE. L'infrastruttura FedERa svolge in questo caso il ruolo svolto dalla piattaforma SiRAC SSO. Da un punto di vista logico le interazioni rimangono ancora una volta le stesse dei casi precedenti, salvo per il fatto che i vari messaggi di richiesta e risposta ricevuti e prodotti dovranno essere tutti conformi sia alla specifica SiRAC/PEOPLE che allo standard SAML 1.1. Proprio come nel primo degli scenari presentati, in questo caso non vi è necessità di adattamento di protocollo. A differenza della piattaforma SiRAC SSO, il gateway attiverà le fasi di IdP Discovery in standard SAML 2.0 e interrogazione dell'Authority Registry locale (FedAR) al pari degli altri scenari. Scenari d'interazione con gateway multiprotocollo FedEra e con gateway locale

In questa sezione vengono ripresi alcuni degli scenari già presentati in precedenza, nei quali è stata introdotta la presenza di un gateway multiprotocollo locale ai vari domini degli enti locali di RER. Verranno evidenziate le differenze rispetto agli scenari già illustrati, unitamente alle

² Può essere creato un CoT apposito per tutti i servizi PEOPLE di RER, al quale associare gli IdP PEOPLE standard e anche alcuni altri IdP (ICAR, FedERa) che rispettino i requisiti sul profilo.

considerazioni rispetto ai vantaggi e agli svantaggi che tale approccio presenta rispetto alla situazione con un unico gateway centrale, a livello di dominio FedERa.

2.1.6. Accesso a servizi ICAR di un ente locale di RER per utenti FedERa

In questo scenario viene illustrato in dettaglio l'accesso ad un servizio erogato in uno dei domini amministrativi di RER (es. un Comune) presso il quale è stato dispiegato un gateway multiprotocollo locale (FedLGW), unitamente al relativo Authority Registry locale (FedLAR).

La sequenza di interazioni per questo scenario è rappresentata in Figura 8.

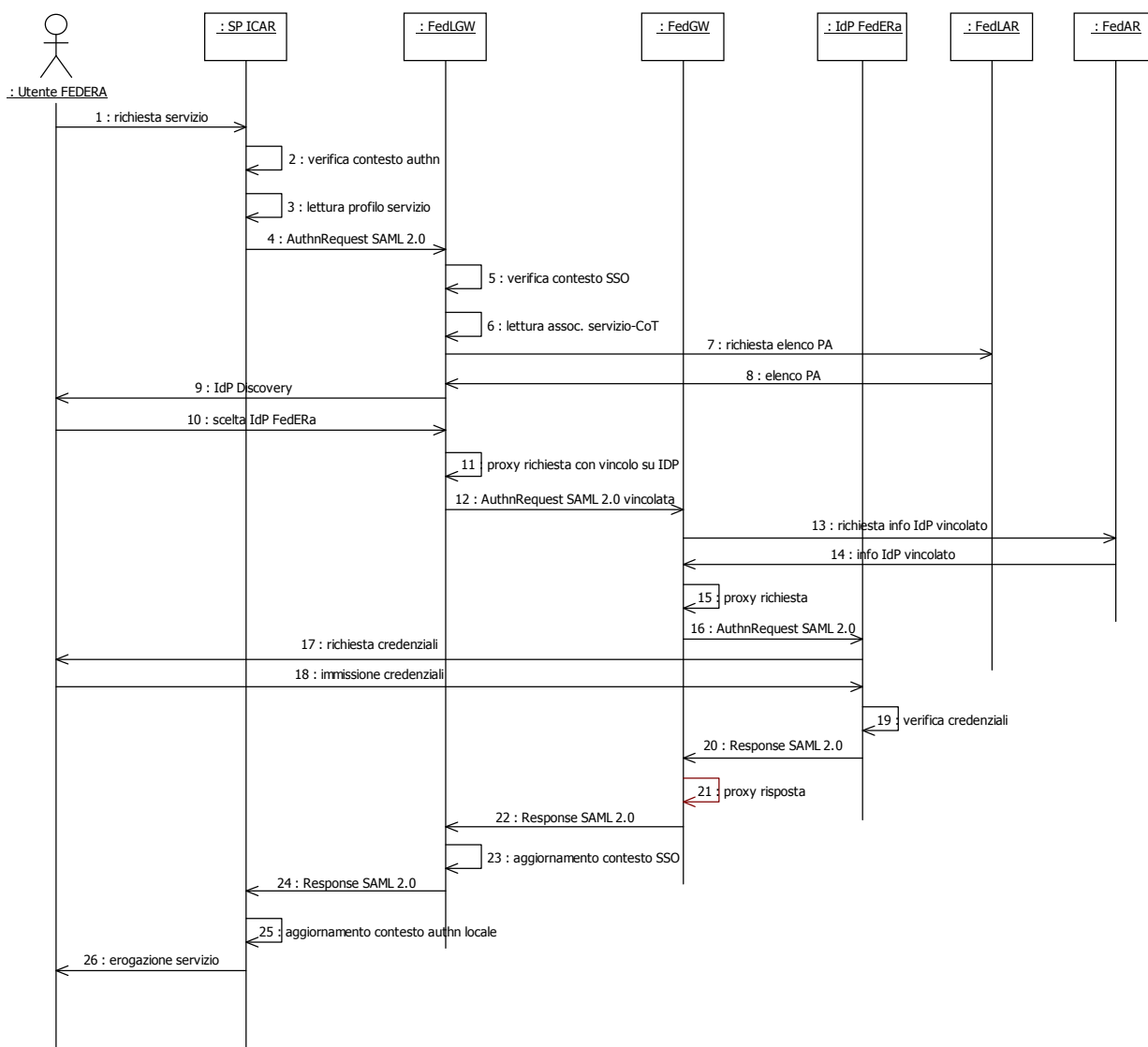


Figura 8 - Accesso a servizi ICAR di RER per utenti FedERa

In questo caso le funzioni di controllo e gestione della sessione di single-sign-on così come della risoluzione delle associazioni tra servizi e CoT è demandata al gateway locale che svolge, per le interazioni iniziali (da 1 a 10) gli stessi compiti che svolge il gateway centrale nello scenario senza gateway locale. La presenza del gateway locale consente di introdurre un elemento di indirizzazione e disaccoppiamento ulteriore, rispetto a quanto possibile con il solo gateway centrale, riducendo così il carico di lavoro imposto al dominio FedERa. Ciascuno dei gateway locali infatti è responsabile di censire e riconoscere i SP del proprio dominio e di associarli ai CoT definiti localmente. Un gateway locale inoltre, unitamente al proprio registry locale, è in grado di gestire anche la presenza di IdP (e relative comunità di utenti) noti soltanto al dominio e non visibili all'esterno.

Dopo le prime interazioni che si concludono con la scelta, da parte dell'utente dell'IdP da utilizzare per l'autenticazione, il gateway locale (FedLGW) interroga FedLAR nel proprio dominio per ottenere informazioni su tale IdP. A questo punto rigenera il messaggio AuthnRequest SAML 2.0 (proxy) producendone uno nuovo che invia al gateway centrale (FedGW). In questo e negli scenari che seguiranno, che rappresentano le varianti di quelli già indicati alla sezione precedente ma con gateway locale, ogni comunicazione interna che intercorre tra i due gateway avviene sempre utilizzando il protocollo SAML 2.0. In particolare, dato il livello di indirizzazione ulteriore che si genera, è opportuno che il messaggio di richiesta inviato dal primo al secondo gateway contenga le informazioni necessarie a far sì che il secondo non inneschi un nuovo processo di IdP Discovery, già effettuato dal primo. A tale scopo nel messaggio AuthnRequest SAML 2.0 inviato a FedGW, FedLGW indica nella struttura IDPList la restrizione sull'IdP scelto dall'utente (IdP FedERa nel dominio RER di appartenenza dell'utente). Tale restrizione rappresenta un vincolo utilizzabile dal destinatario del messaggio per guidare la fase di proxying verso l'IdP scelto. FedGW consulta pertanto FedAR per ottenere le informazioni necessarie a contattare l'IdP FedERa e quindi invia un nuovo messaggio AuthnRequest verso di esso, attivando l'autenticazione vera e propria. I messaggi di Response SAML 2.0 prodotti nella catena di risposta si propagano dall'IdP fino a FedGW che si limita a rimandarlo a FedLGW il quale svolge, di nuovo, gli stessi compiti che FedGW aveva nello scenario privo di gateway locale: aggiornamento della sessione SSO e risoluzione del SP da cui era partita la richiesta originaria. Al termine il SP riceve la Response finale ed eroga il servizio.

2.1.7. Accesso a servizi ICAR di RER per utenti PEOPLE di RER

Questo scenario è simile al precedente con la differenza che l'IdP che viene contattato è un IdP PEOPLE, che dialoga su protocollo SAML 1.1. La sequenza di messaggi scambiati è illustrata nella figura seguente.

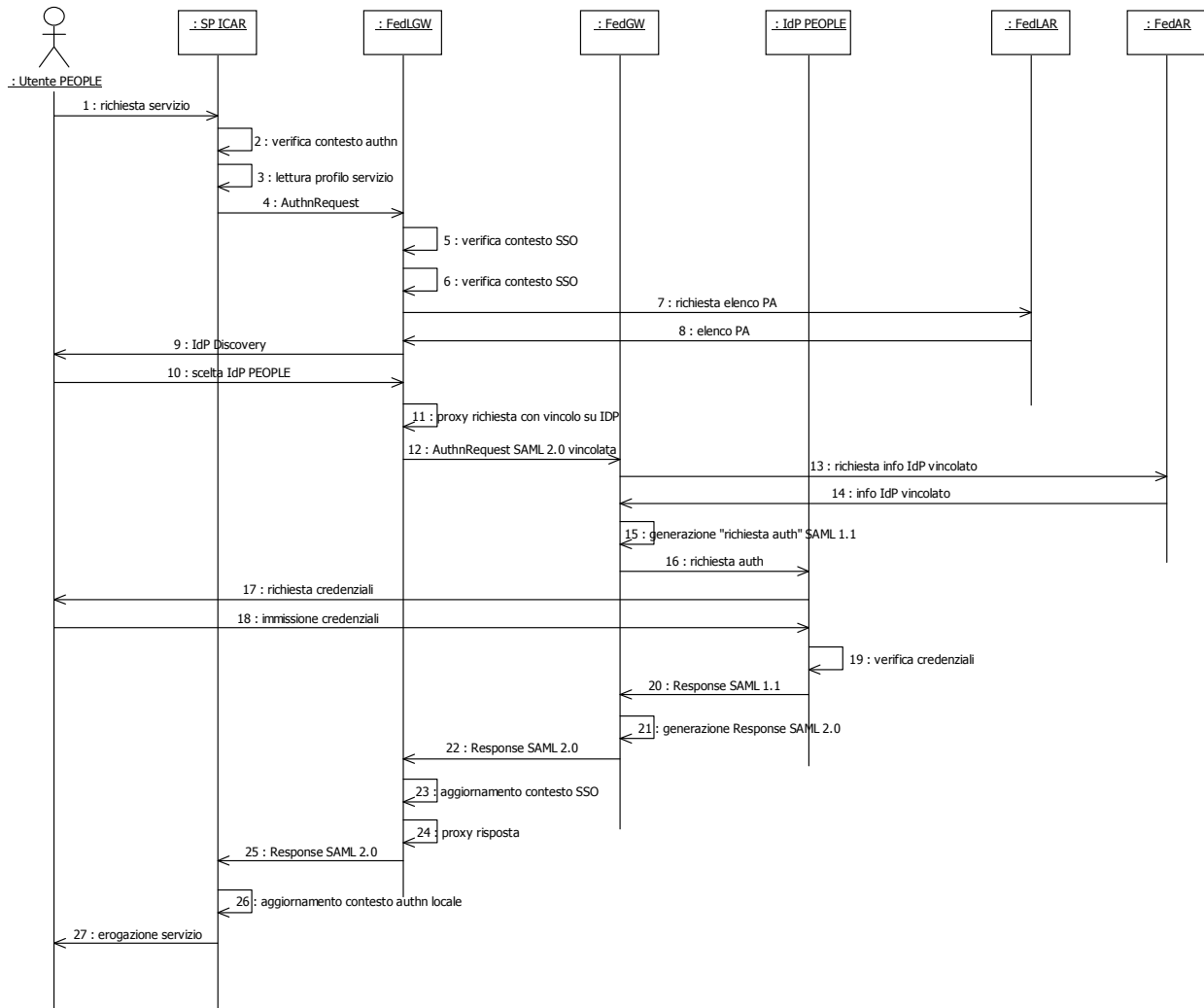


Figura 9 – Accesso a servizi ICAR di RER per utenti PEOPLE di RER

Come è possibile vedere, le interazioni sono identiche fino al passo 15 al quale il gateway centrale, dopo che quello locale ha svolto gli usuali compiti di risoluzione CoT e gestione SSO, si trova a dover rispettare il vincolo-restrizione sull'IdP che deve essere contattato. Dopo aver consultato FedAR per ottenere informazioni relative a tale IdP, deve adattare il protocollo in ingresso, SAML 2.0, a quello da utilizzare per invocare il servizio di autenticazione sull'IdP (SAML 1.1). A questo scopo nelle informazioni restituite da FedAR ricerca l'indirizzo specifico corrispondente alla modalità di autenticazione richiesta (forte o debole) e procede ad invocarlo. Simmetricamente, ricevuta la risposta SAML 1.1 dall'IdP procederà ad adattarla creandone una nuova su protocollo

SAML 2.0, diretta al gateway locale. Da qui in poi lo scenario è identico al precedente.

2.1.8. Accesso a servizi PEOPLE di un ente locale di RER per utenti ICAR/fedERa

Questo scenario è analogo ai precedenti, con l'aggiunta di un gateway locale all'ente presso il quale sono erogati i servizi richiesti. La sequenza di messaggi scambiati è illustrata nella figura seguente.

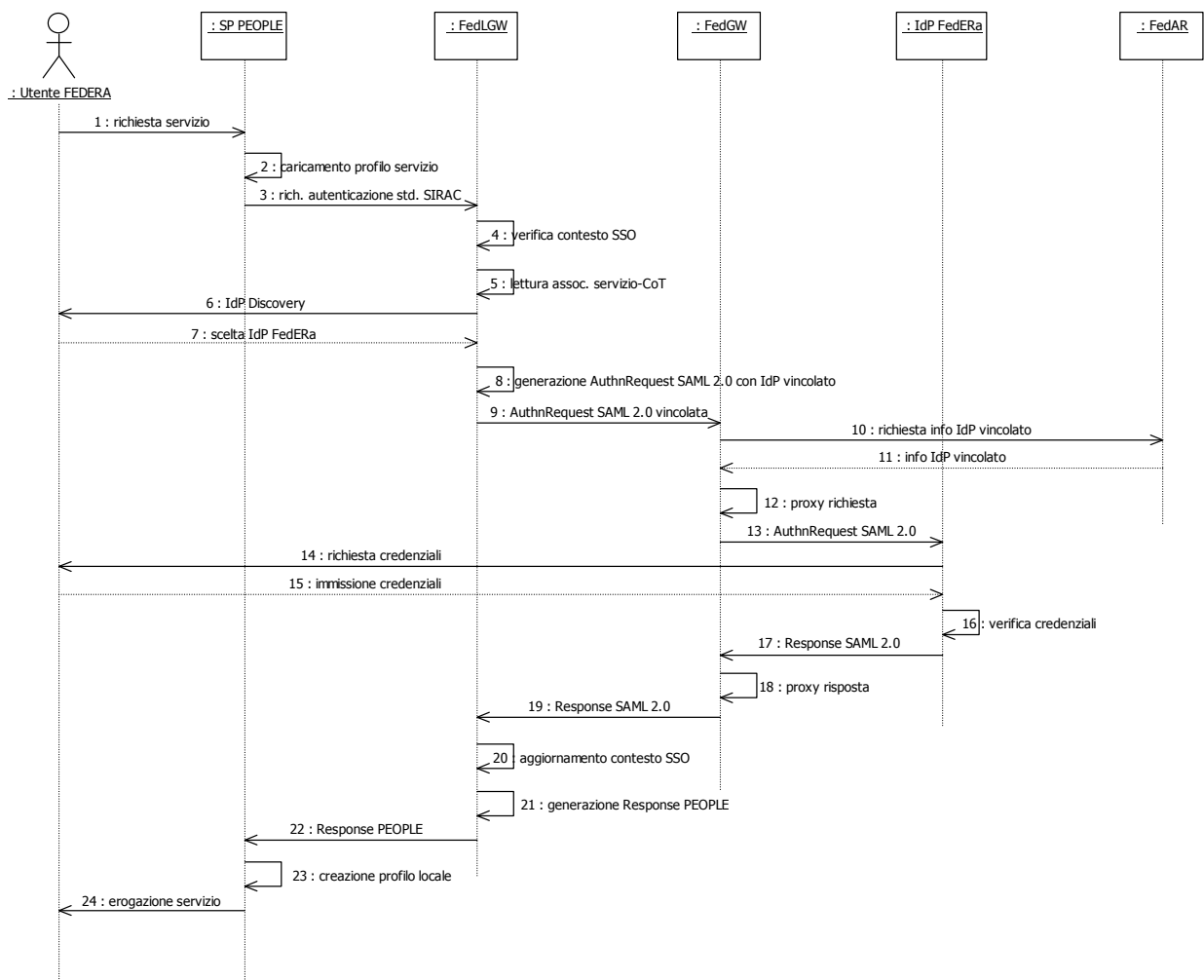


Figura 10 - Accesso a servizi PEOPLE di un ente locale di RER per utenti ICAR/fedERa

Analogamente a quanto detto per le varianti dotate di gateway locale, le interazioni iniziali coincidono a quelle dello scenario con solo gateway centrale. Al pari di FedGW nello scenario menzionato, FedLGW in questo caso deve essere in grado di comportarsi, verso il SP PEOPLE contattato, come il sottosistema SIRAC di un portale PEOPLE, potendo cioè ricevere richieste di autenticazione che specificano il servizio e la modalità di autenticazione richiesta. A valle della

fase di gestione SSO e IdP Discovery che FedLGW svolge al pari di quanto FedGW fa nello scenario menzionato, FedLGW guida il comportamento di FedGW a cui passa il controllo generando un messaggio AuthnRequest SAML 2.0 indicando l'IdP che deve essere utilizzato, così come scelto dall'utente. Lo scenario prosegue come di consueto, contattando l'IdP ICAR o FedERa scelto. Al termine, per poter rispondere al SP PEOPLE, il gateway locale che riconosce tale SP genera un messaggio di risposta comportandosi al pari dell'infrastruttura SiRAC, inserendo le informazioni del profilo dell'utente PEOPLE ricevute e la modalità di autenticazione utilizzata. Il messaggio così strutturato viene inviato al SP PEOPLE che aggiorna il proprio contesto di autenticazione locale e procede all'erogazione del servizio richiesto.

2.1.9. Accesso a servizi PEOPLE di RER per utenti PEOPLE di RER

Da ultimo viene ripresentato lo scenario in cui sia il servizio sia l'IdP contattati sono PEOPLE. In questo caso sia il gateway locale che quello centrale devono interagire con l'esterno mediante protocollo SAML 1.1: il primo nei confronti del SP PEOPLE da cui proviene la richiesta di autenticazione e il secondo verso l'IdP PEOPLE che deve essere contattato. Vengono mantenute, al solito, le responsabilità mutue dei due gateway: al primo resta in carico il riconoscimento dei servizi del proprio dominio con la relativa gestione dei CoT e al secondo l'attivazione della fase di autenticazione presso l'IdP in modo guidato dal primo, mediante vincolo contenuto nel messaggio di richiesta inviato dal primo al secondo. Proprio quest'ultima osservazione è alla base della necessità di utilizzare il protocollo SAML 2.0 nelle interazioni tra i due gateway; il gateway locale, infatti, ricevuta la richiesta di SP PEOPLE in modo conforme alla specifica SiRAC/PEOPLE e svolte le fasi di gestione SSO e IdP Discovery, produce un messaggio AuthnRequest SAML 2.0 per il gateway centrale, in cui indica il vincolo sull'IdP da utilizzare. Il resto dello scenario procede come già illustrato nei casi precedenti. La sequenza di messaggi scambiati è illustrata nella figura seguente.

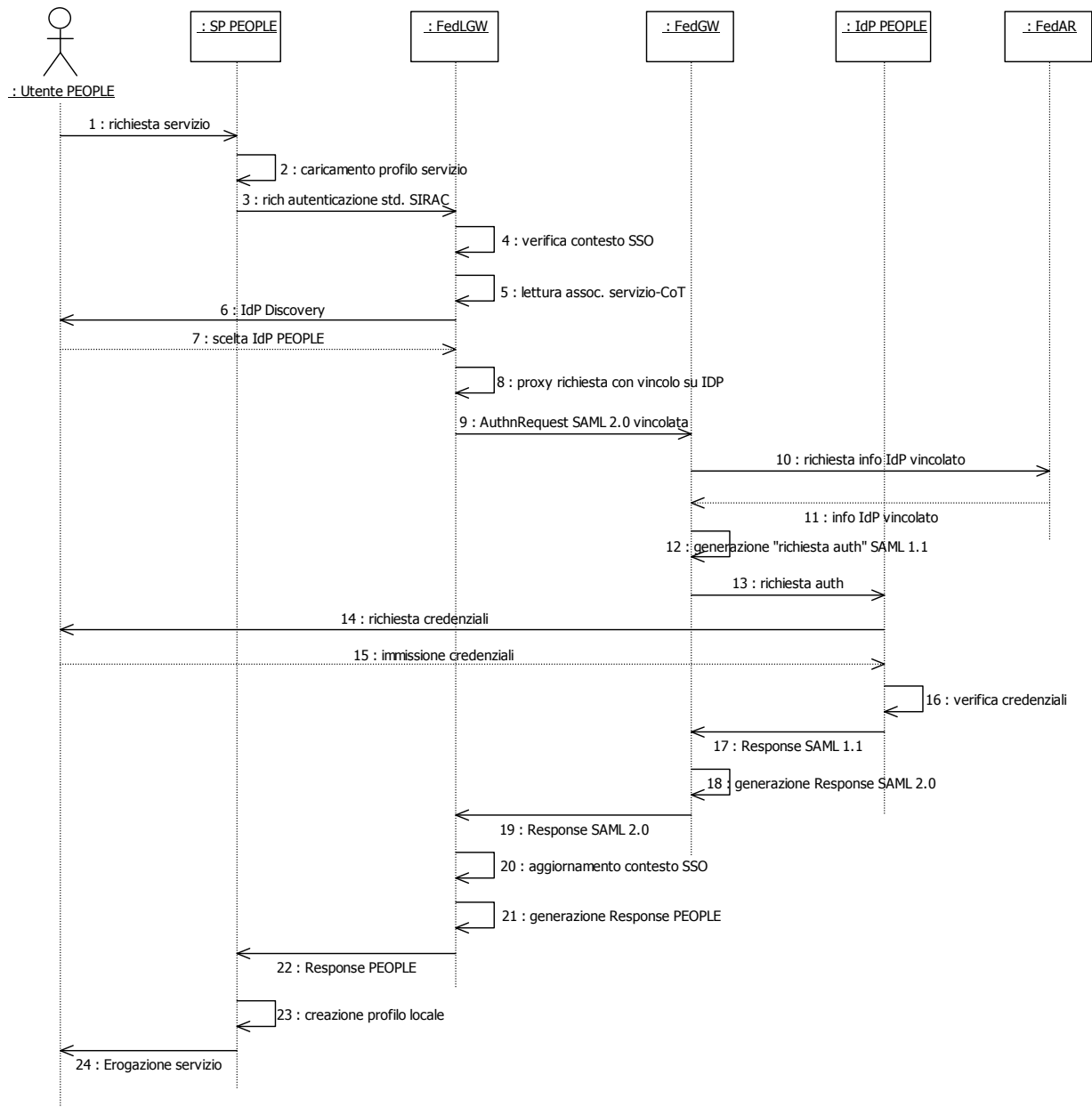


Figura 11 - Accesso a servizi PEOPLE di RER per utenti PEOPLE di RER

2.2. SCENARI D'INTERAZIONE SENZA GATEWAY MULTIPROTOCOLLO CENTRALE O LOCALE

Infine, in questa sezione sarà presentato l'unico scenario d'interazione rilevante tra i vari soggetti presentati che non prevede l'utilizzo di alcun gateway multiprotocollo ma solo del sistema di autenticazione di FedERa.

2.2.1. Accesso ai servizi PEOPLE per utenti ICAR/FedERa

Questo scenario è rivolto agli utenti registrati presso uno dei domini FedERa che vengono messi in grado accedere ai servizi PEOPLE degli enti locali sul territorio di RER presso cui è dispiegato un portale PEOPLE.

In particolare tale portale PEOPLE fa uso dell'infrastruttura SiRAC per la gestione della fase di autenticazione, che viene normalmente affidata ad un IdP PEOPLE. Nel momento in cui il sistema di autenticazione di FedERa sarà reso disponibile, esso esporrà anche le interfacce per il dialogo su protocollo SAML 1.1, al pari di qualunque altro IdP PEOPLE. Pertanto, per tali enti l'infrastruttura SiRAC presente potrà essere riconfigurata per utilizzare il nuovo IdP FedERa per l'autenticazione degli utenti, in luogo di quello precedentemente utilizzato, senza necessità di ulteriori interventi di integrazione. Non viene dettagliata la sequenza delle interazioni per la quale si rimanda alla documentazione PEOPLE.

Si segnala che l'adozione di questo scenario dovrebbe essere intrapresa soltanto come misura transitoria, dal momento che ciò esclude l'accesso alle funzionalità di definizione dei CoT, l'associazione dei vari servizi ai CoT ecc., messi a disposizione dal gateway multiprotocollo.

3. RIFERIMENTI

- [1] ICAR - Sistema Federato Interregionale di Autenticazione: MODELLO ARCHITETTURALE DI RIFERIMENTO, <http://www.progettoicar.it>.
- [2] ICAR - Sistema Federato Interregionale di Autenticazione: SPECIFICA DELLE INTERFACCE APPLICATIVE ESTERNE, <http://www.progettoicar.it>.
- [3] Progetto PEOPLE - Specifica dei servizi infrastrutturali di registrazione, autenticazione e comunicazione (SiRAC). V. 0.9.9 – 27/09/2005
- [4] People SiRAC: Autenticazione integrata e Single-Sign-On
- [5] OASIS Security Services (SAML) TC, Security Assertion Markup Language (SAML) V2.0 Technical Overview, Working Draft 08, 12 settembre 2005. <http://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf>
- [6] OASIS Security Services (SAML) TC, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [7] OASIS – “Technical Overview of the OASIS Security Assertion Markup Language (SAML) v1.1”
- [8] OASIS – “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1” - OASIS Standard, 2 September 2003
- [9] OASIS – “Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1” - OASIS Standard, 2 September 2003