Identità digitale federata: il caso ICAR-INF3

Francesco Meschia
CSI-Piemonte

Il task INF-3 di ICAR

- Identità digitale **federata tra le Regioni**
- Identità digitale **a supporto di SPC**
- Identità digitale **per gli operatori pubblici**
  - Pensando già all'estensione ai **cittadini** e **agli intermediari**
- Identità digitale secondo i modelli **user-centrici**
- Un modello in cui le Regioni potessero **riconoscersi**
  - Anche come tecnologie, implementazioni, prodotti

Il modello di governo e condivisione del task

- Criticità dovute a:
  - **Innovatività** del tema
  - **Complessità** del tema
  - **Maturazione** delle tecnologie necessarie
  - Necessità di operare scelte su **standard** e **tecnologie**
  - Necessità di preservare gli **investimenti**
- Condivisione tra le Regioni e Province coinvolte
  - **Indispensabile**
  - **Virtuosa**

Il modello di governo e condivisione del task

- **Recupero** delle competenze dei partecipanti
  - Da esperienze regionali e da progetti visti come good practice (PEOPLE, IRIDE, InterOp, ecc.)
- Copiosa produzione iniziale di **deliverable documentali**
  - Condivisi, studiati, approvati dai partecipanti
- Copertura **completa** del tema
  - Modello concettuale
  - Modello organizzativo
  - Modello architetturale

Il modello di governo e condivisione del task

- La condivisione dei modelli concettuali e organizzativi ha richiesto tempo
  - Tempo **investito** e non semplicemente **usato**
  - Stretta collaborazione tra Regione Piemonte, Regione Lombardia, Regione Veneto e Regione Friuli-Venezia-Giulia
  - Condivisione e concertazione con tutti i partecipanti
- La condivisione ha prodotto **consapevolezza**
  - Delle **direzioni** intraprese
  - Delle **scelte**
  - Del **ruolo** delle parti coinvolte del progetto

Il modello concettuale

- Ha individuato le **parti coinvolte**
- Ha fissato i **requisiti del sistema**
- Ha esaminato diverse **strade** per conseguirli
- Ha proposto una soluzione innovativa e **user-centrica**
- Ha proposto un meccanismo a supporto della **fiducia** tra le parti federate
- Ha tracciato la strada per l'**evoluzione** del sistema e le linee guida del dispiegamento

Il modello organizzativo

- Ha descritto i **rapporti** tra i domini coinvolti
- Ha proposto e descritto un sistema di **relazioni** a supporto della fiducia
- Ha fissato i **compiti** in carico alle Regioni
- Ha fissato i **benefici** attesi dalle Regioni
- Ha proposto un insieme di **procedure** per il governo del sistema

Il modello architetturale

- Ha fissato in **formalismo tecnico** le decisioni prese nel corso delle modellazioni concettuali ed organizzative
- Rappresenta una **vista d'insieme**, benché a livello tecnico, sull'intero sistema di identità digitale federato
- Ha delineato **casi d'uso, formalismi, protocolli, relazioni con SPC, evoluzioni previste**
- Un "**reference manual**" di ICAR-INF3

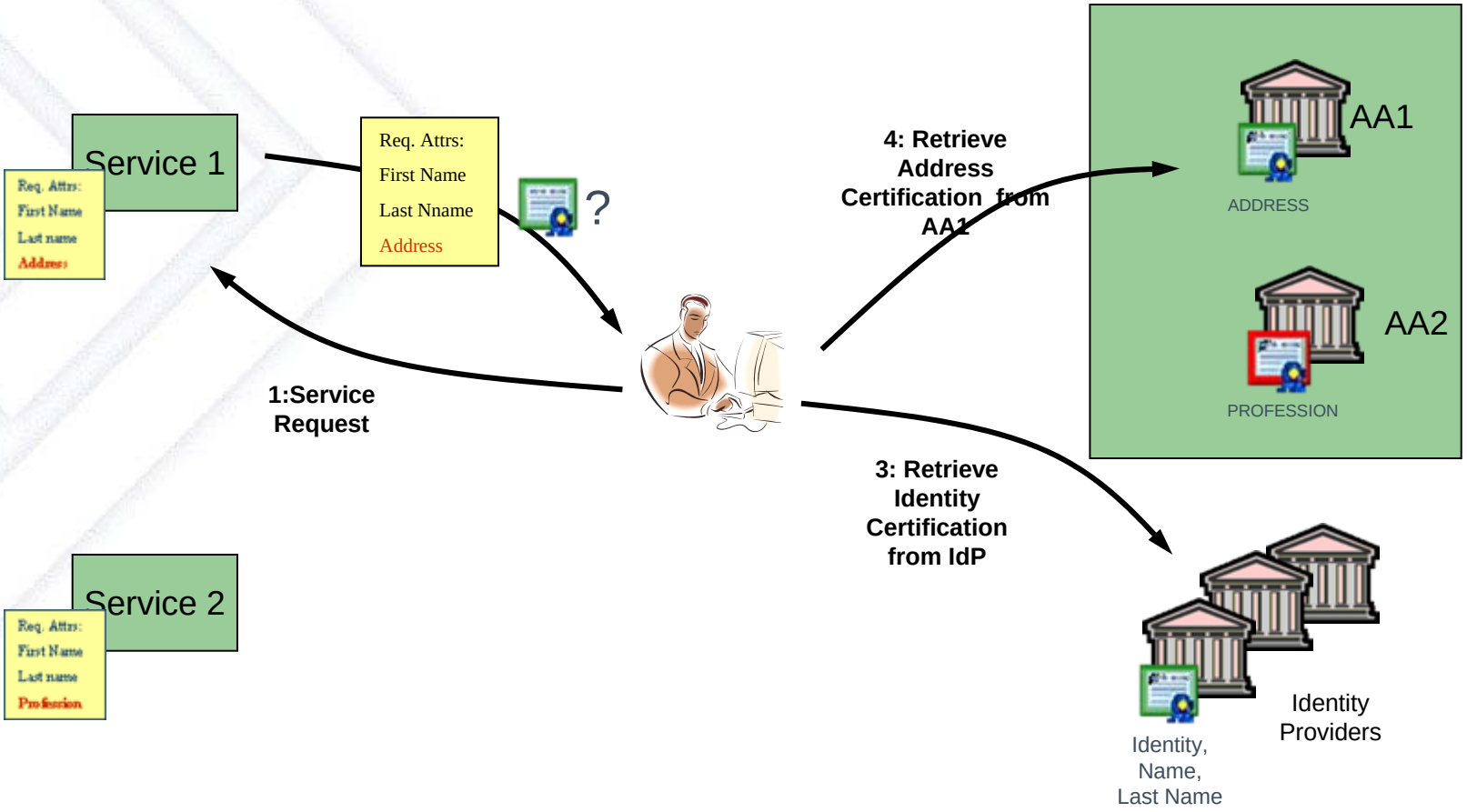
Il modello architetturale

- Nel modello ICAR, diversi soggetti certificano **“pezzi” diversi** dell’identità delle persone
  - “Identity Provider” e “Attribute Authority” possono essere distinti
- I “Service Provider” hanno però bisogno **dell’identità “completa”**, non “a pezzi”
- Il modello ICAR ha perciò introdotto il concetto di **“profilo utente”**

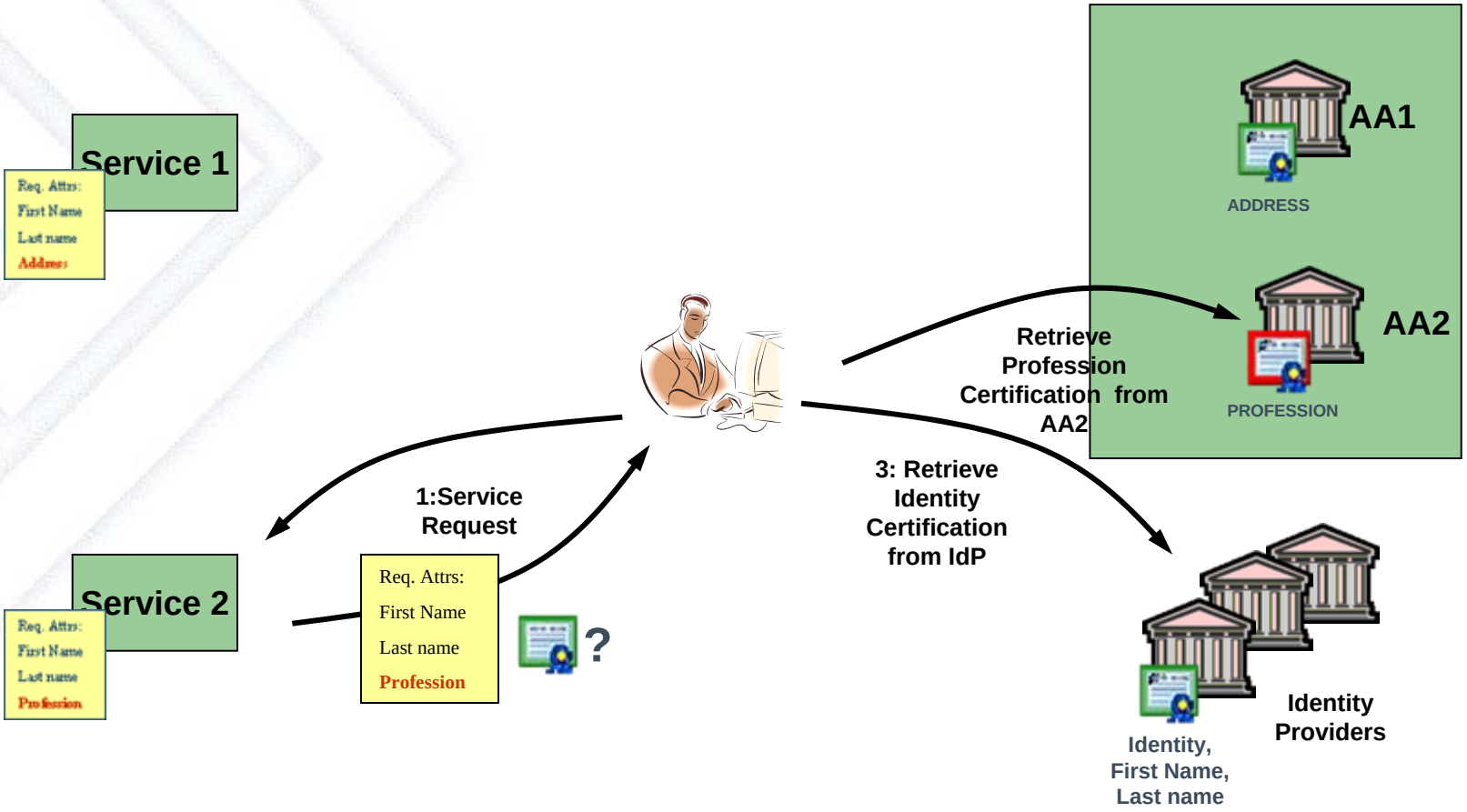
Il profilo INF-3

- Il profillo è come un **portafogli**
  - Tiene traccia **dell'identità** del soggetto, e dei suoi **attributi** e ruoli
- Un utente può avere **diversi profili**
  - Ciascuno dei quali è una diversa **"sezione"** della sua **"persona digitale"**
- I service provider non possono conoscere **nessuna informazione** su un utente oltre a quelle incluse nel profilo
  - L'utente **controlla** in questo modo ciò che di lui si vede in rete
  - **User-centric-identity**

Esempio di interazione user-centrica



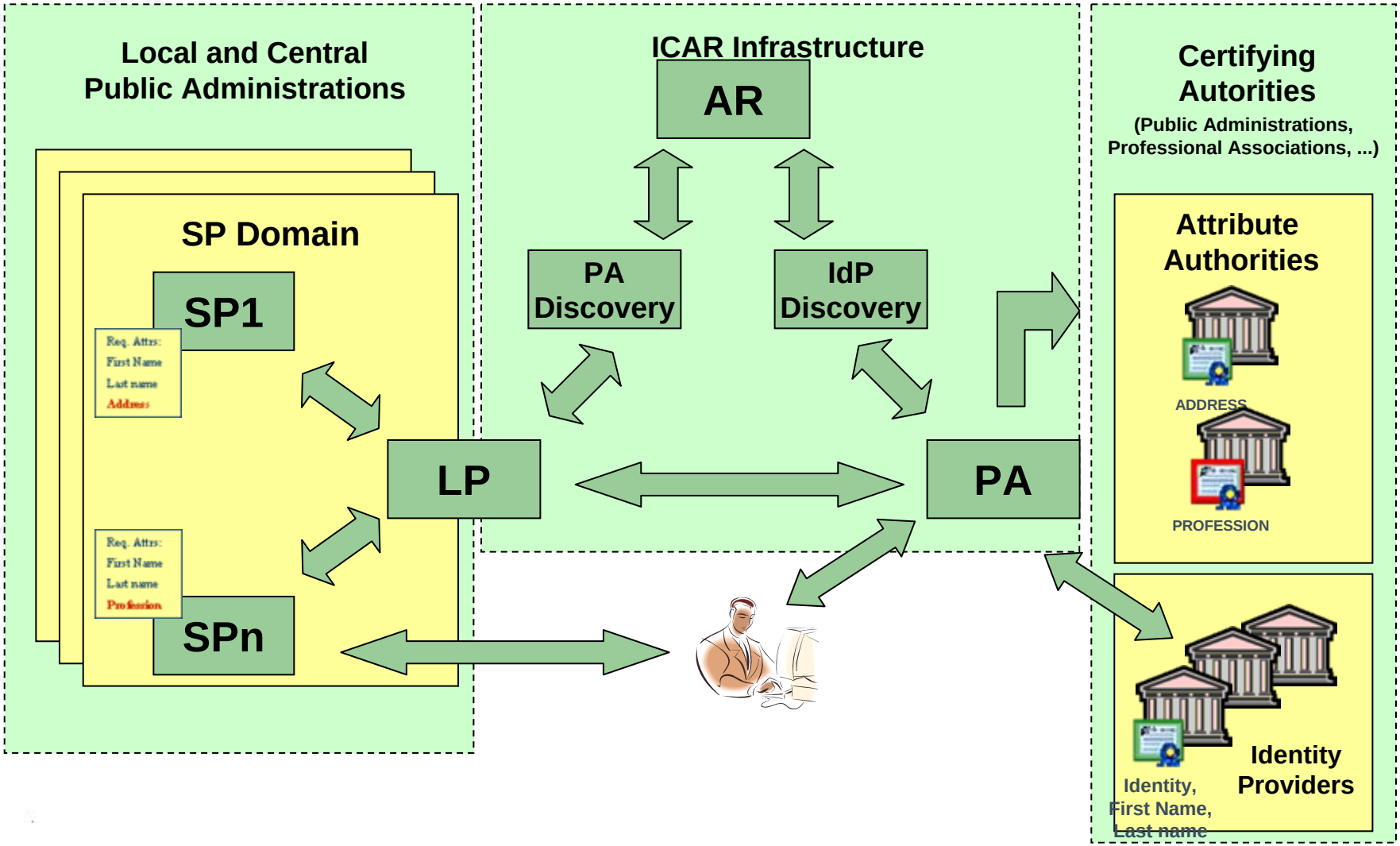
Esempio di interazione user-centrica



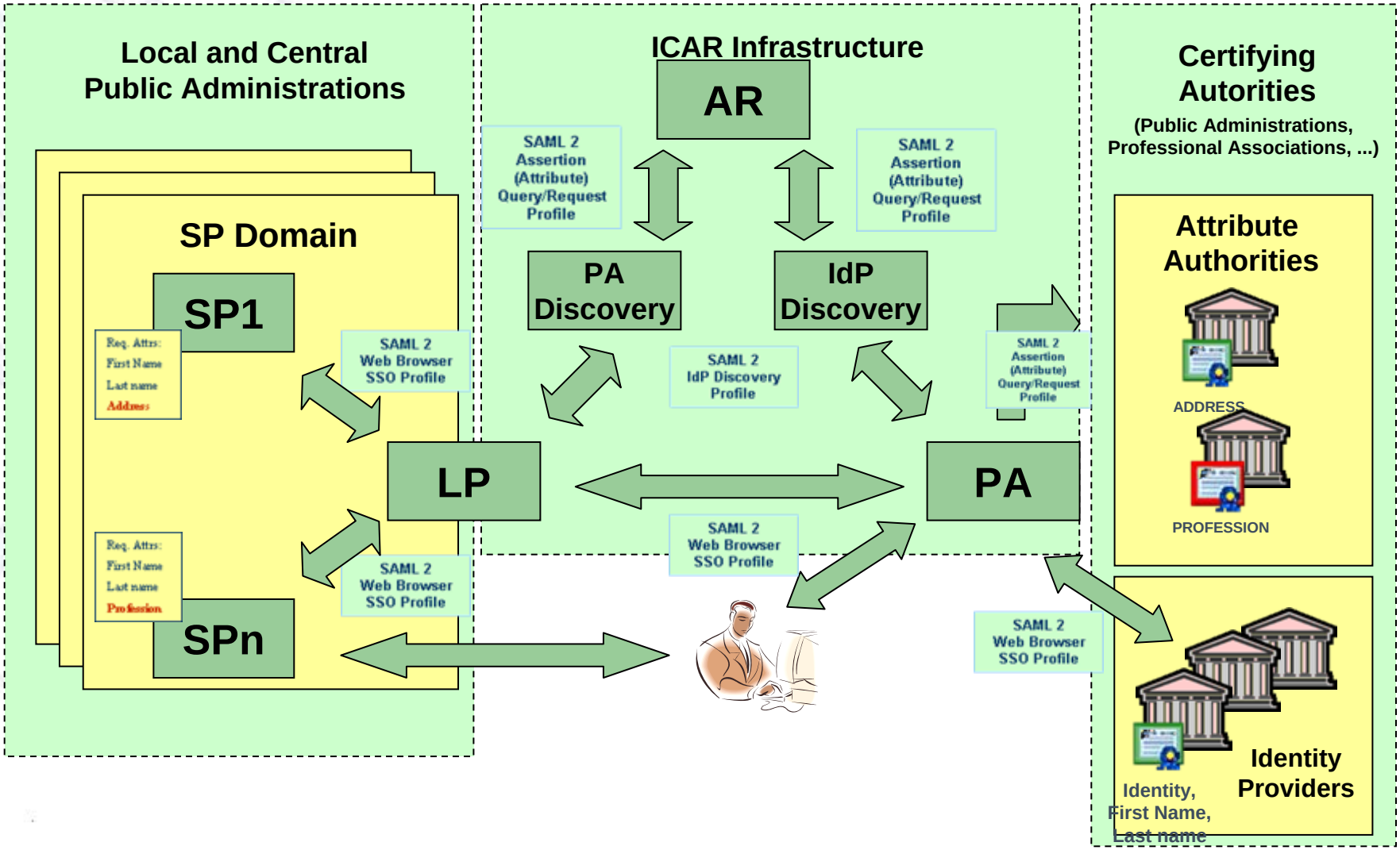
Gli standard e l'architettura INF-3

- ICAR INF-3 è basato sui protocolli, profili e binding **SAML 2.0**
- Uno dei requisiti architetturali di INF-3 è quello di **non introdurre nuovi standard o profili**
  - Allo scopo di facilitare l'integrazione con **prodotti standard** open o commerciali, sia lato IdP sia lato SP
- Si è perciò scelto di rendere esterna a IdP e SP la **"trust fabric"** della federazione
- Introducendo il componente bifronte **"Local Proxy"**
  - Che è un IdP+AA nei confronti dei SP, e un SP nei confronti di IdP e AA
- La struttura della trust fabric è basata su scambio dinamico di **metadati SAML 2.0**
  - E su un componente "root" chiamato **"Authority Registry"**

Architettura ICAR INF-3



Architettura ICAR INF-3



L'implementazione di riferimento

- Segue il concetto di "**reference implementation**" diffuso nel mondo degli standard aperti
  - Basato su tecnologie e componenti **open source** o con licenze libere
  - Mostra come deve funzionare il sistema di identità federata nel suo complesso
  - Fornisce implementazioni **pronte per essere ingegnerizzate** dei i componenti "infrastrutturali" del sistema
  - Fornisce implementazioni di esempio per i componenti che le Regioni reperiranno **sul mercato**
  - Il codice è a sua volta rilasciato con licenze **open source**

I prossimi passi

- Già avviate partecipazioni a convegni internazionali, con manifestazioni di interesse per il carattere innovativo dell'iniziativa
- Dispiegamento dei componenti regionali in corso, a cura delle Regioni
- Collaborazione con **CNIPA**
  - Il modello architetturale è ora parte delle specifiche SPC relative a **GFID (Gestione Federata Identità Digitale)**
- Studio di casi di **interoperabilità**
  - Ad esempio con Shibboleth 2.0