FedERa: sinergie tra federazioni di identità ed enti locali

Gianluca Mazzini - Direttore Generale Lepida SpA

Scenario

- sistema per la federazione delle identità
- sottosistemi interagenti per realizzare le funzionalità di gestione dell'identità digitale degli utenti afferenti a vari domini
- identity provider realizzato in FedERa oppure presso uno qualunque degli Identity Provider esistenti sul territorio nazionale
- service provider facilmente integrabili
- conformità agli standard di interoperabilità definiti nell' ambito dei progetti ICAR INF-3 e SIRAC-PEOPLE
- supporto protocollo SAML 2.0 e SAML 1.1

Architettura

- erogazione servizio di autenticazione verificando le credenziali utente
- scambio mediante asserzioni SAML che vengono trasmesse agli erogatori dei servizi finali
- gateway multiprotocollo con funzione di gateway di dominio
- gateway multiprotocollo come mediatore tra i servizi di front-end
- gestione degli utenti
- gestione del ciclo di vita con registrazione, attivazione, sospensione
- gestione tipologie utenti con amministratori, utenti finali

Funzionamento

- il browser chiama il servizio
- il servizio interroga il gateway multiprotocollo che fa da mediatore tra service provider e identity provider
- il gateway multiprotocollo restituisce all'utente, attraverso il browser, la lista di identity provider presso i quali l'utente può autenticarsi
- l'utente seleziona l'identity provider
- l'identity provider verifica le credenziali tramite asserzione SAML
- l'asserzione SAML viene trasmessa al servizio

Circle of Trust

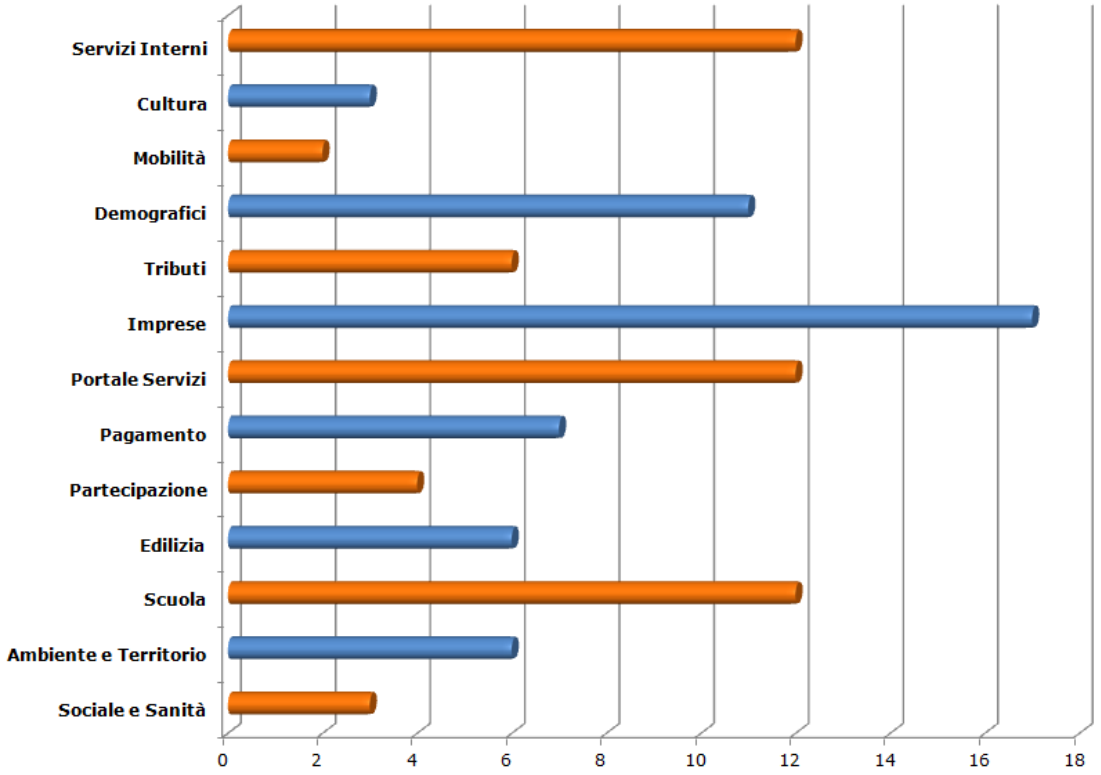
- livello minimo di affidabilità dell'identità digitale ad essi associato
- livello minimo di password policy ad essi associato
- elenco minimo degli attributi utente restituiti a valle dell'autenticazione
- un service provider integrato può essere associato a uno e un solo CoT
- il service provider viene informato sul set minimo degli attributi utente che si aspetta di ricevere, sul livello di affidabilità dell'identità e sul livello di password policy
- ad un CoT possono essere associati più service provider
- tra tutti i service provider associati ad un CoT il Gateway Multiprotocollo FedERa abilita la funzionalità di Single Sign On

Livelli Affidabilità

- basso C, senza password policy, autoregistrazione, form di registrazione online senza riconoscimento de visu
- medio B, senza password policy, riconoscimento indiretto, credenziali rilasciate associando l'identità del richiedente ad un numero telefonico e quindi ad una SIM
- alto A, senza password policy, riconoscimento forte, de visu oppure con smart card oppure con fax oppure con PEC
- alto A+, con password policy che scade ogni 6 mesi, per dati Personali, ogni utente può richiederlo online
- alto A++, con password policy che scade ogni 3 mesi, per dati Personali, ogni utente può richiederlo online
- password policy: con almeno 4 alfabetici 2 numerici 1 extra alfabetico, lunghezza almeno 8, history 3

Diffusione

- identity provider 341
- identity provider esterni 12
- registration authority 324
- utenti registrati su identity provider interni 77K
- service provider 105
- service provider WiFi 11

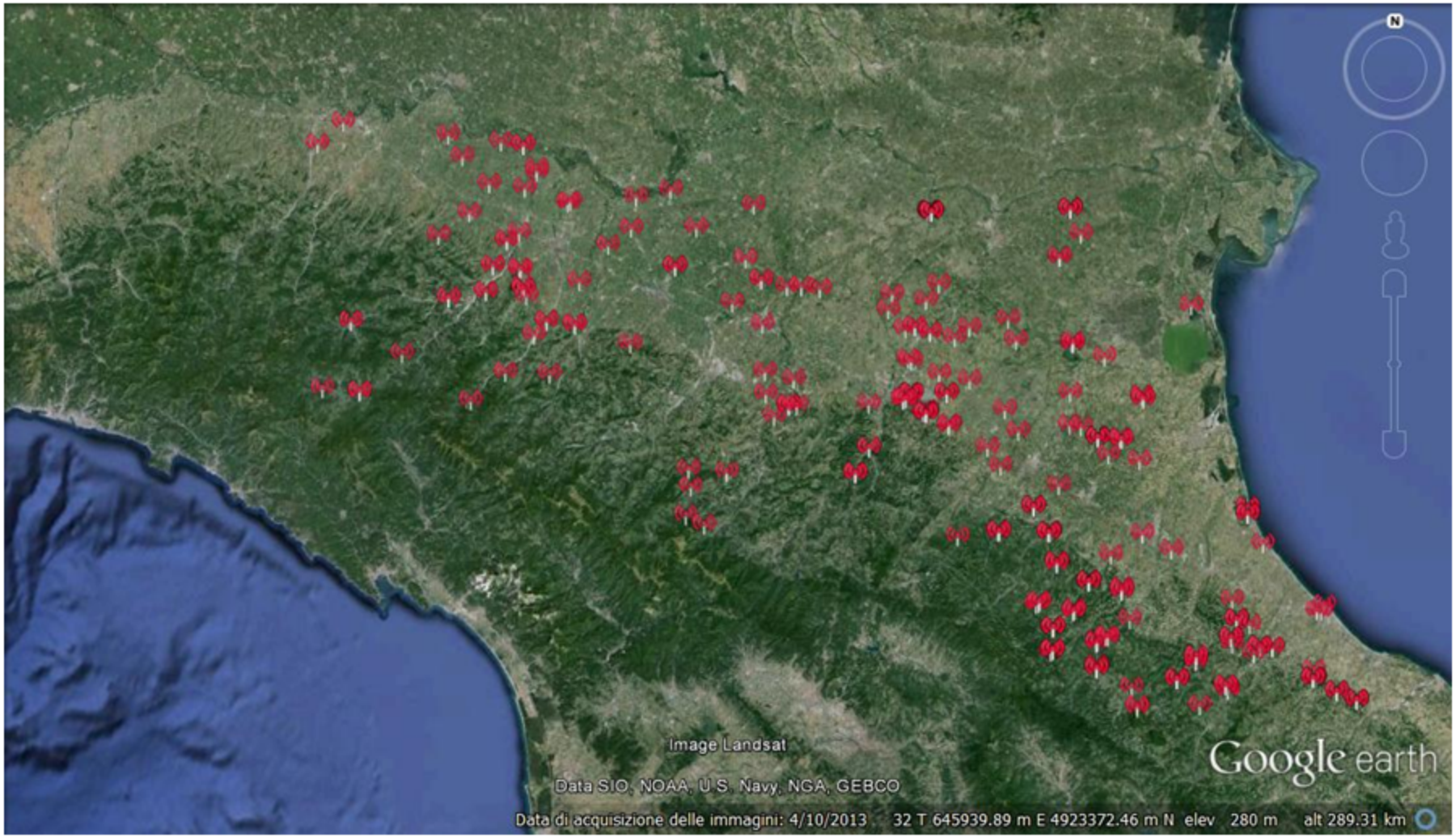


lepidaspa

Identity Provider Esterni

- Comune di Reggio Emilia
- Comune di Modena
- Regione Emilia-Romagna
- Ordine degli Avvocati di Bologna
- Università di Modena e Reggio Emilia
- Università di Ferrara
- AUSL di Reggio Emilia
- Fascicolo Sanitario Elettronico
- AUSL di Modena
- ASMN di Reggio Emilia
- Università di Bologna
- Ordine dei dottori commercialisti e degli esperti contabili di Bologna

Service provider WiFi (>400 punti)



lepidaspa

Prospettive

- modifica livello affidabilità A con invio password mediante due media differenti
- aumento dei cittadini federati mediante WiFi
- integrazione con SPID quando saranno disponibili le specifiche
- aumento della usabilità utente per semplificare l’ ottenimento di credenziali
- integrazione con sistema di federazione degli attributi per service provider “Sono Io”
- meccanismi per l’implementazione su sistemi mobile
- integrazione e federazione con altre piattaforme nazionali