REGISTRAZIONE IDENTITÀ DIGITALI, USER REQUEST, USER OFFICE

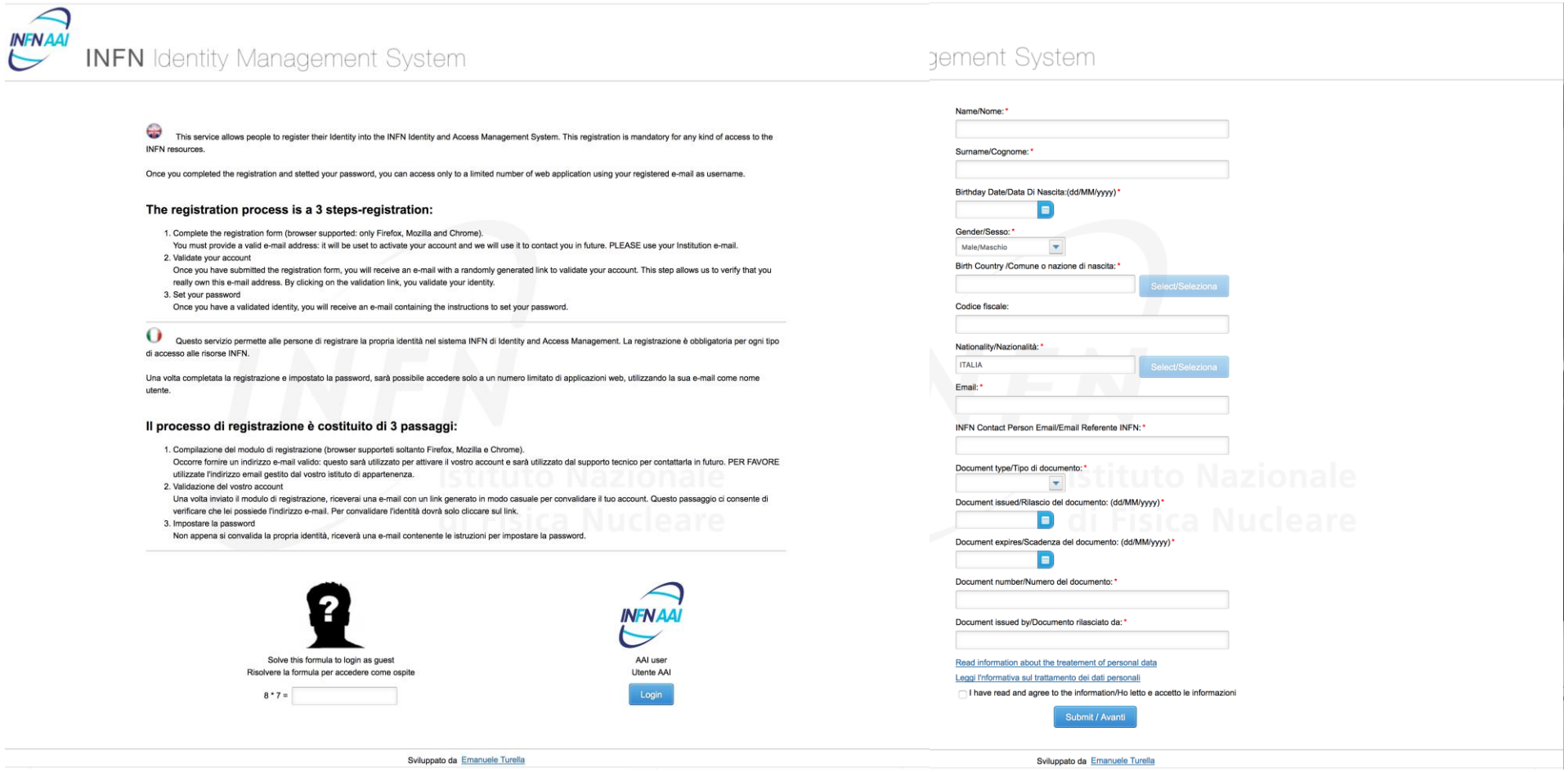
WS CCR - Rimini
11/06/2018

Roberto Lulli, Michele Tota – AAI-WG

Agenda

- Registrazione Identità Digitali
  - Lo stato attuale (perché è necessario un nuovo sistema)
  - Implicazioni e condizioni al contorno
- Implementazione
  - User Request
  - User Office

NuovaAnagrafica oggi



NuovaAnagrafica oggi

- Modulo web sviluppato alcuni anni or sono
  - Auto-registrazione mediante semplice
    - verifica e-mail del registrando (hand-shake via invio e-mail all'indirizzo indicato in fase di registrazione)
    - indicazione di un Referente Interno (e-mail *@*.infn.it in GODiVA)
  - Registrazione **autenticata** via INFN-AAI (nessun livello di autorizzazione)
  - Nessun workflow per la verifica della Identità e dei dati registrati nella Identità Digitale
  - Nessuna definizione del ruolo di Validatore
  - Nessuna definizione del ruolo di Referente Interno
  - Manca la presa visione e l'accettazione di:
    - Disciplinare per l'utilizzo delle Risorse Informatiche
    - Privacy policy
- Alla fine del flusso di auto-registrazione l'utente ha un account temporaneo INFN-AAI

Registrazione Identità Digitali

- Necessaria una revisione del sistema per aderire al Disciplinare e alle misure minime di sicurezza
- Non si può prescindere dalla correttezza e dalla validità dei dati
- Documento di analisi di policy, flussi e ruoli di verifica (dati, identità, richieste) in draft quasi-finale:
  - Introduce anche per le ID dell'INFN il concetto di Level of Assurance (LoA)
    - INFN-AAI LoA1 —> LoA1 dell'ISO-IEC 29115 ("Little or no confidence in the asserted identity") —> non c'è corrispondente livello SPID
    - INFN-AAI LoA2 —> LoA2 dell'ISO-IEC 29115 —> livello 1 SPID
    - INFN-AAI LoA3 —> LoA3 dell'ISO-IEC 29115 —> livello 2 SPID
    - INFN-AAI LoA4 —> LoA4 dell'ISO-IEC 29115 —> livello 3 SPID
  - Definisce i ruoli di Referente interno e Addetto al riconoscimento

Focus su utenti

- Il nuovo sistema prevede che sia sempre l'utente ad effettuare autonomamente sia la registrazione che le richieste relative a risorse
  - di tipo amministrativo/gestionale
    - Associazione, Recruiting, ecc. ecc.
  - di tipo «fisico»
    - Accesso al territorio, a risorse ICT, ecc. ecc.
- In funzione del tipo di risorsa, può essere necessario
  - Opportuno livello di confidenza (LoA) della Identità Digitale
  - Opportune autorizzazioni

Auto-registrazione & LoA

- Nella prima fase del processo di auto-registrazione viene verificata solo la corrispondenza tra l'Identità Digitale e l'indirizzo e-mail del registrando
- Auto-registrazione → Identità Digitale in LoA1
- Accesso a «servizi pubblici»
  - Agenda, Recruiting, Iscrizione a newsletters, ecc. ecc.
  - Portale Utente
    - Gestione profilo personale
    - Gestione richieste

Flussi

- L'accesso a risorse che richiedono una verifica dell'Identità dovrà essere soggetta a
  - Approvazione della richiesta da parte di un «Referente interno» che autorizza l'utilizzo della risorsa
  - Verifica dell' Identità da parte di un «Addetto al riconoscimento» che dovrà
    - Verificare la correttezza dei dati inseriti dall'utente (confrontandoli con i documenti)
    - Verificare «de visu» (anche in video) la corrispondenza tra la persona e i documenti - validità
- Se il referente interno autorizza e l'identità è ancora in LoA1, si attiva il flusso di verifica da parte dell'Addetto al riconoscimento
- L'esito positivo di questa verifica porta l'Identità in LoA2 e «congela» anche i dati certificati

Ruoli

- Per implementare questi flussi è quindi fondamentale definire le figure di:
  - Referente Interno: una lista di «referenti interni» per ogni «risorsa» che possano autorizzare o meno
    - Es. Farm di calcolo locale dell'esperimento X → responsabile locale/nazionale
  - Addetto al Riconoscimento: una lista di «addetti al riconoscimento» per ogni struttura
    - Es. personale delle segreterie che effettuano già tale compito per le associazioni o le ospitalità (del personale o di direzione, …)

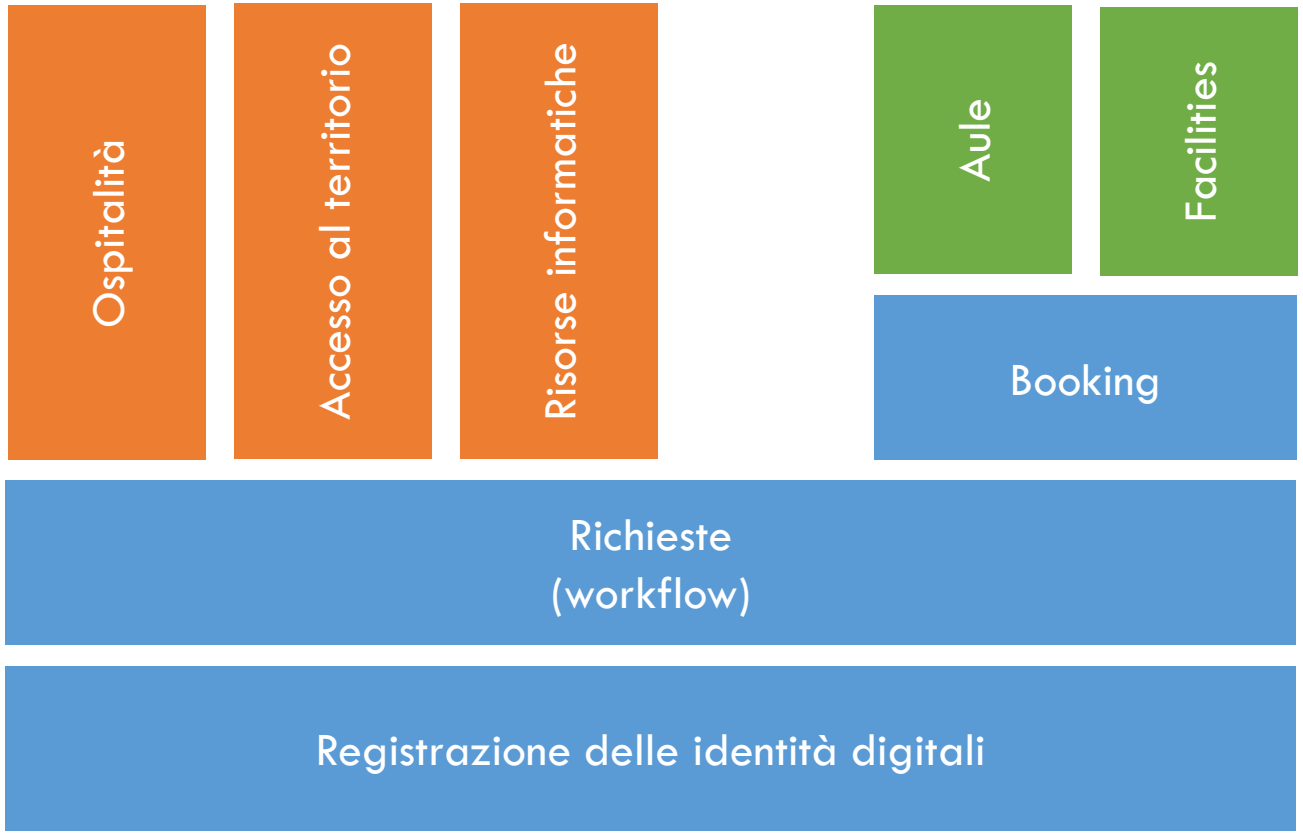
Note

- Tempi brevi per il dispiegamento
  - Il documento è quasi ultimato
  - L'implementazione software è in stato avanzato
- Addio username temporanee
- Benvenuta INFN Identity Card

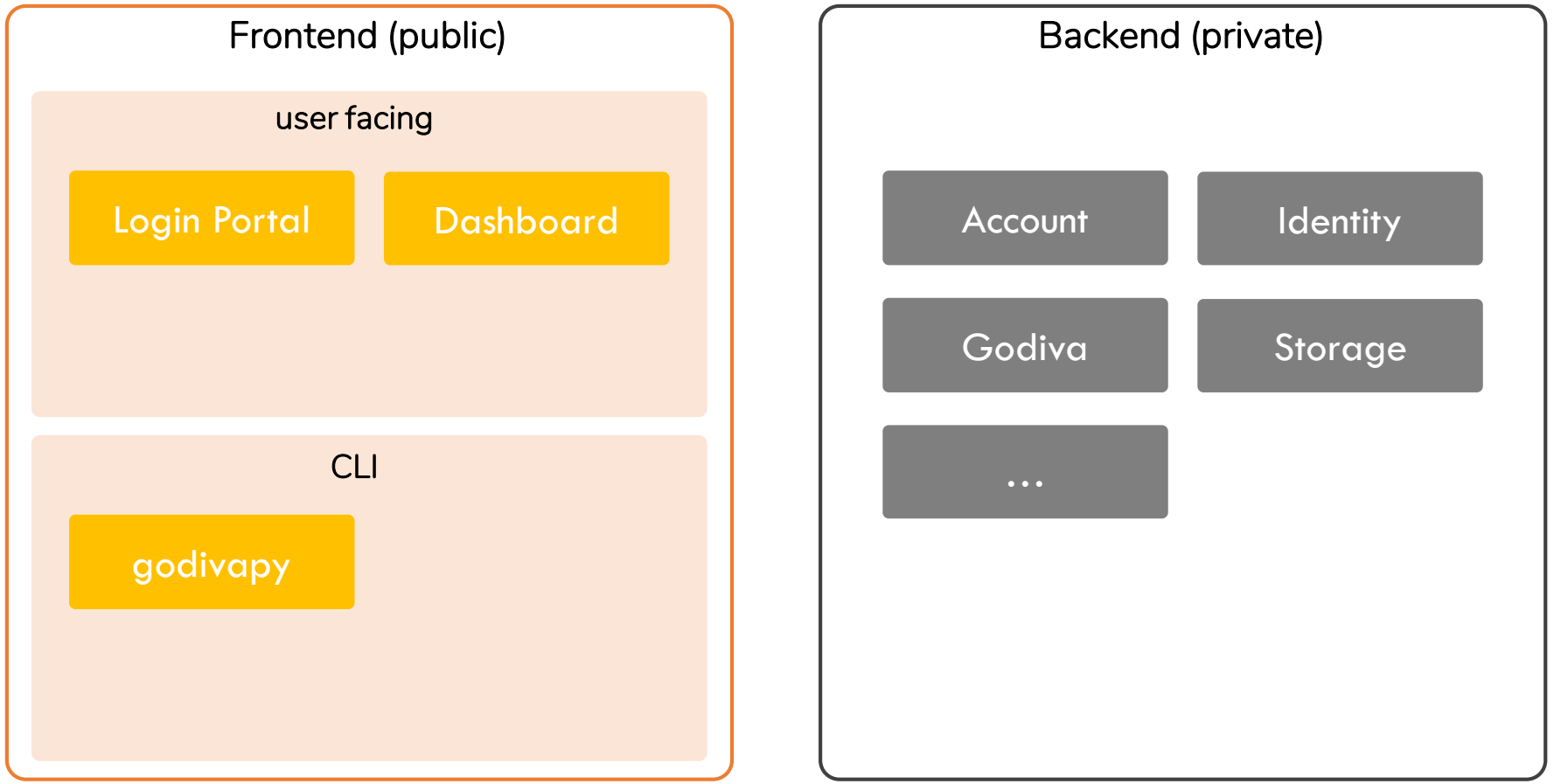
Necessità pervenute

- Registrazione delle identità digitali
- Richiesta di accesso al territorio
- Richiesta di ospitalità
- Richiesta di risorse informatiche
- Booking delle facilities
- Booking delle aule
- Phonebook
- Gestione nodi per valutazione rischio informatico
- …

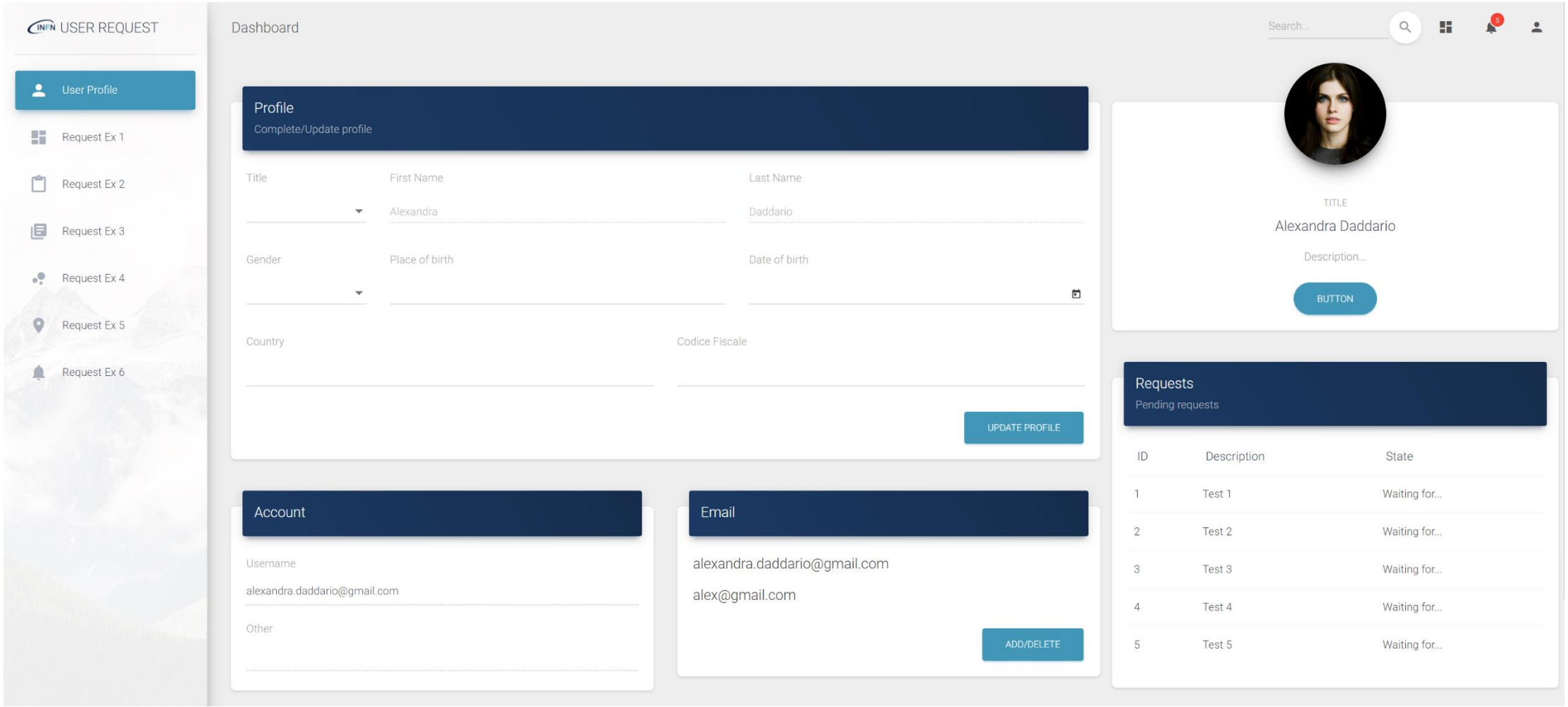
Analisi delle richieste



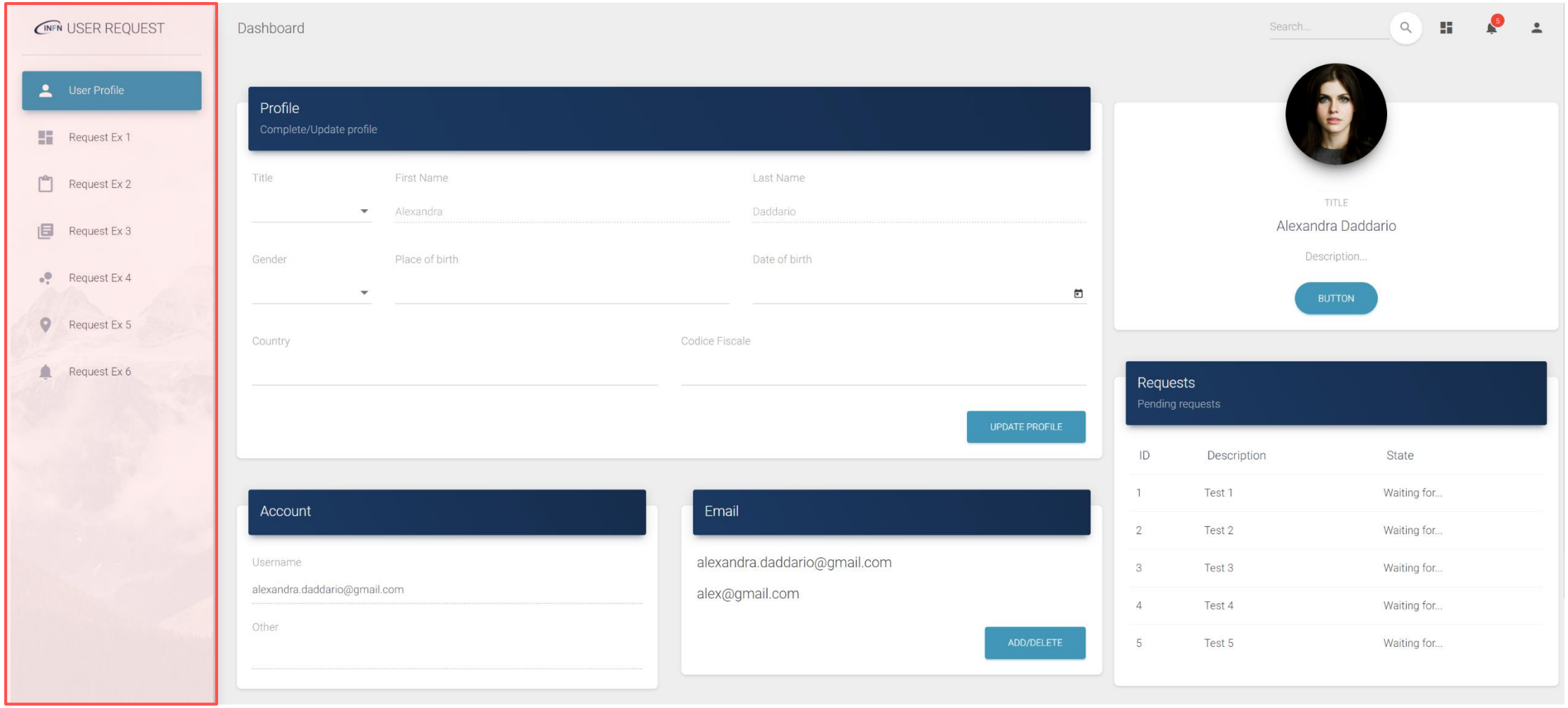
Microservices@INFN



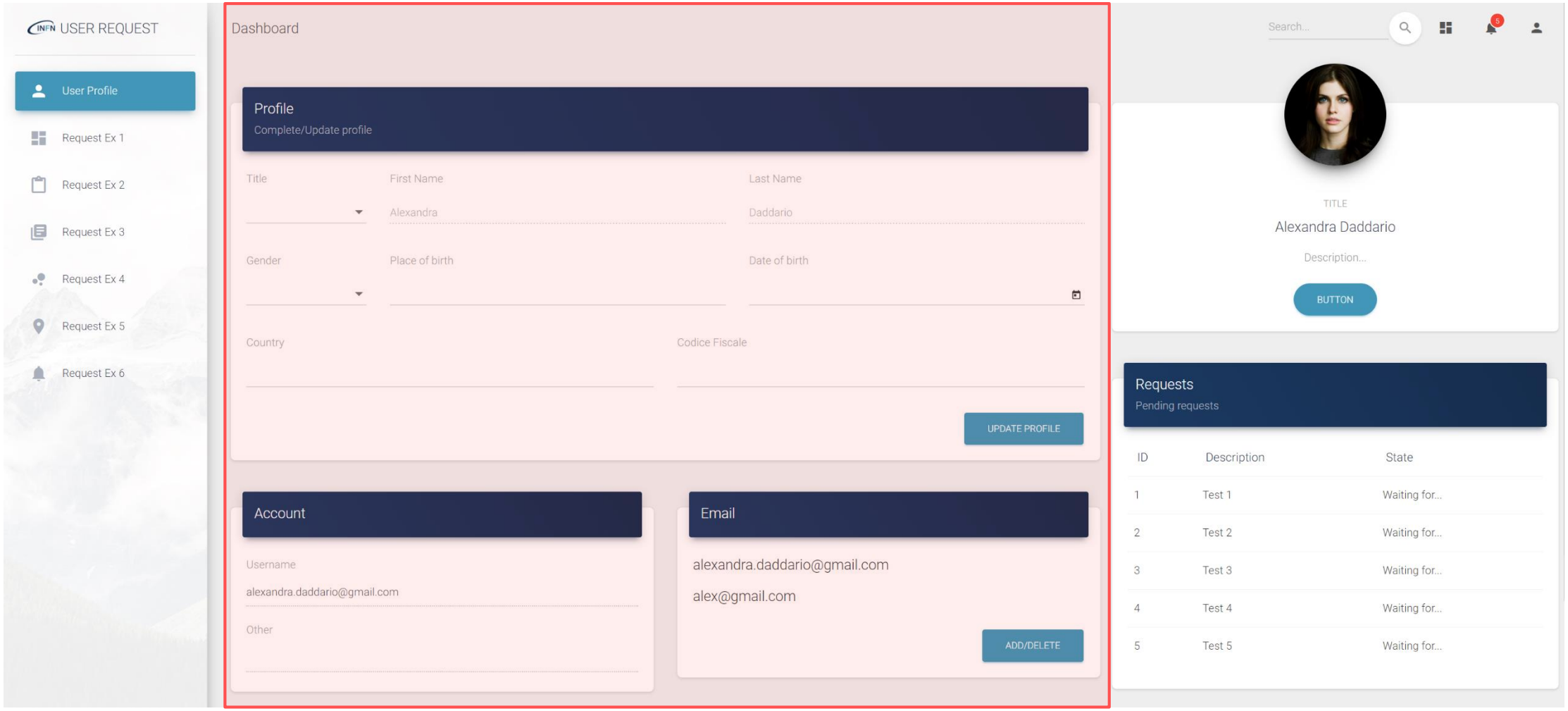
User Request



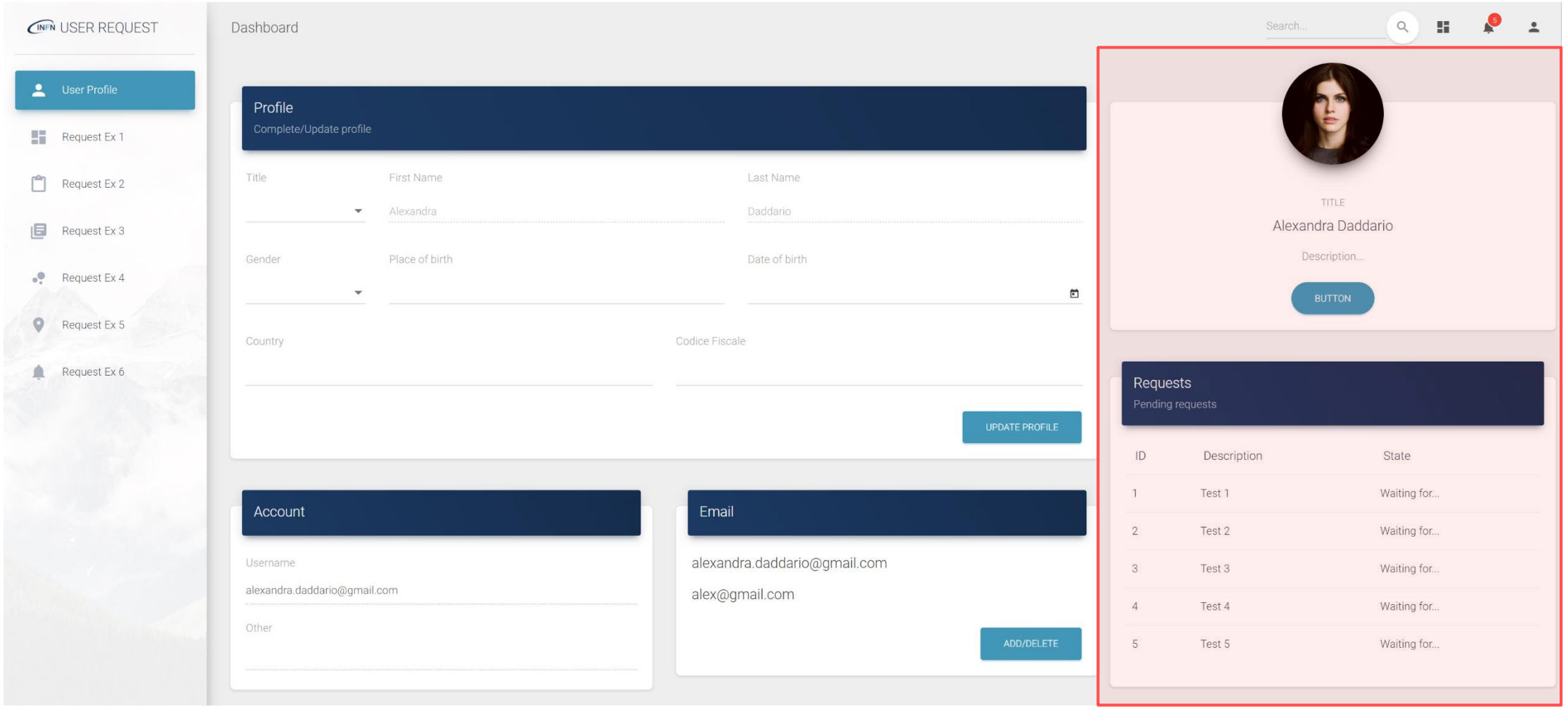
User Request (left panel)



User Request (main panel)



User Request (summary panel)



User Office

- Portale di accesso per l'approvazione delle richieste e gestione workflow
- Analogo al portale User Request

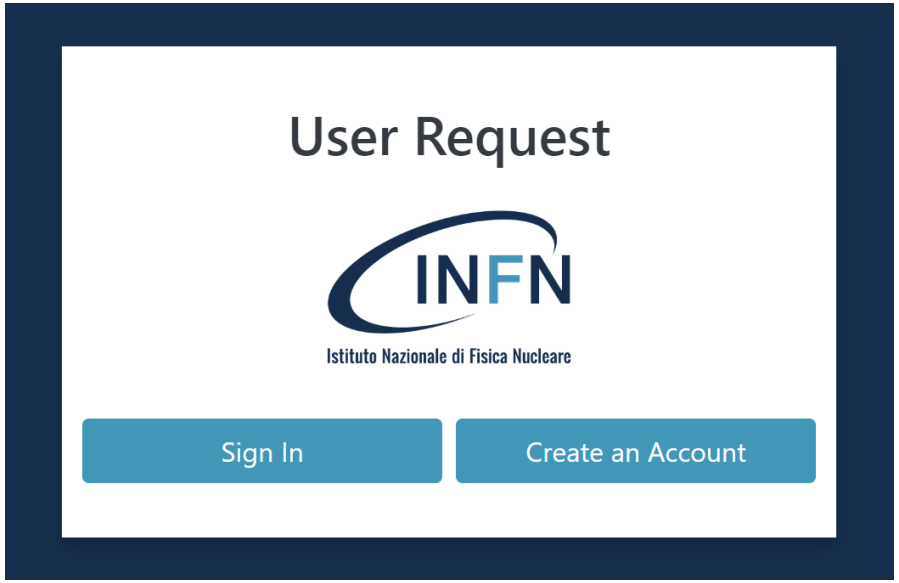
Command line interface

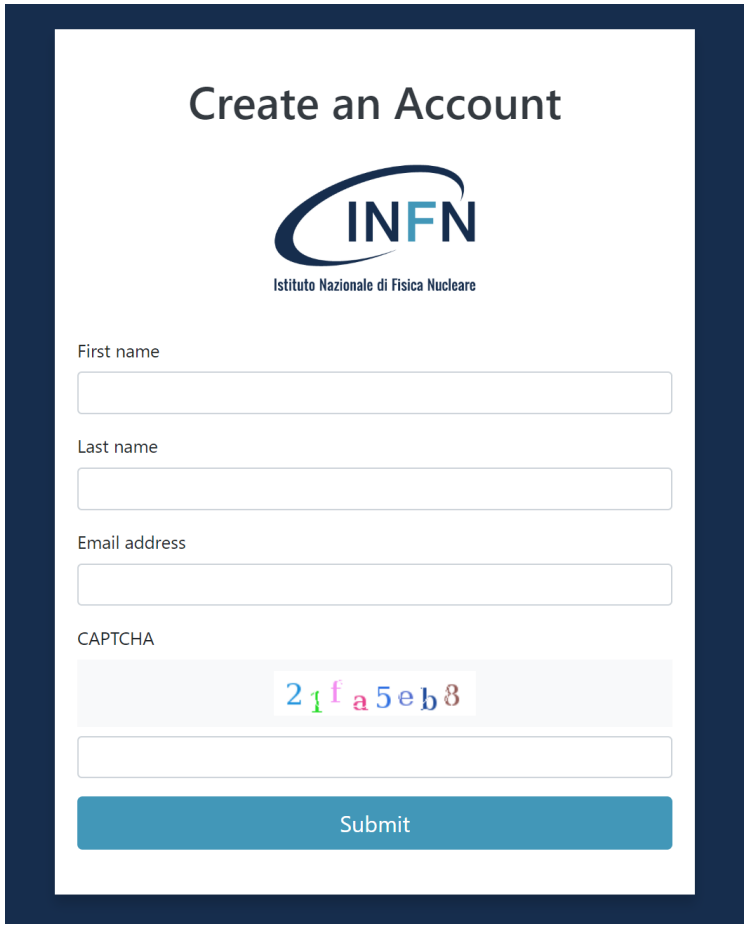
- Chiama API esportate dai microservizi

- Esempio:

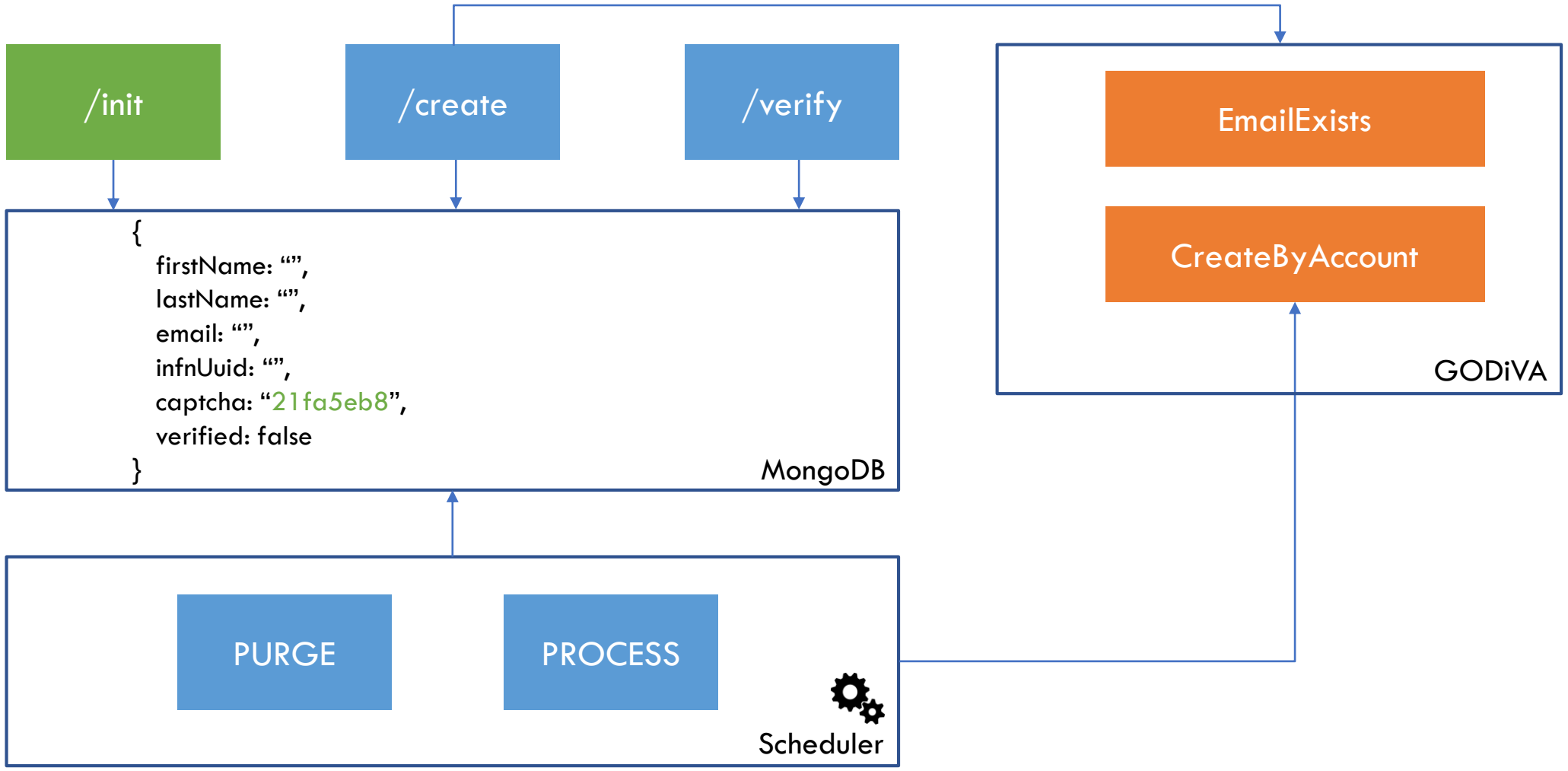
```
godivapy identity –uuid xxxxxxx addrole --title-
id 198 --domain i:infn:roma1:csn1:ua9 --from
2010-01-01 --to 2080-10-10
```

Registrazione Identità Digitale

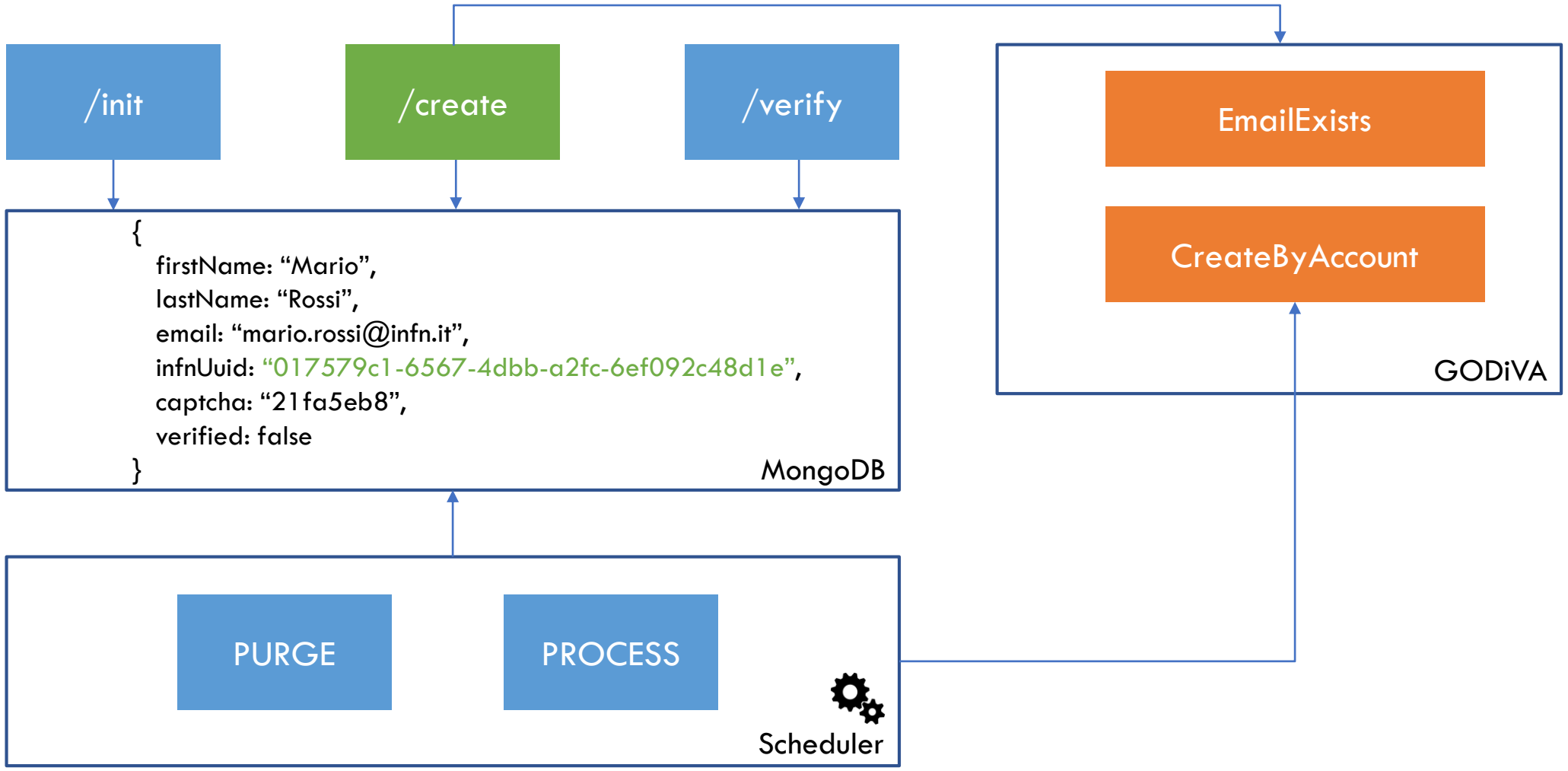




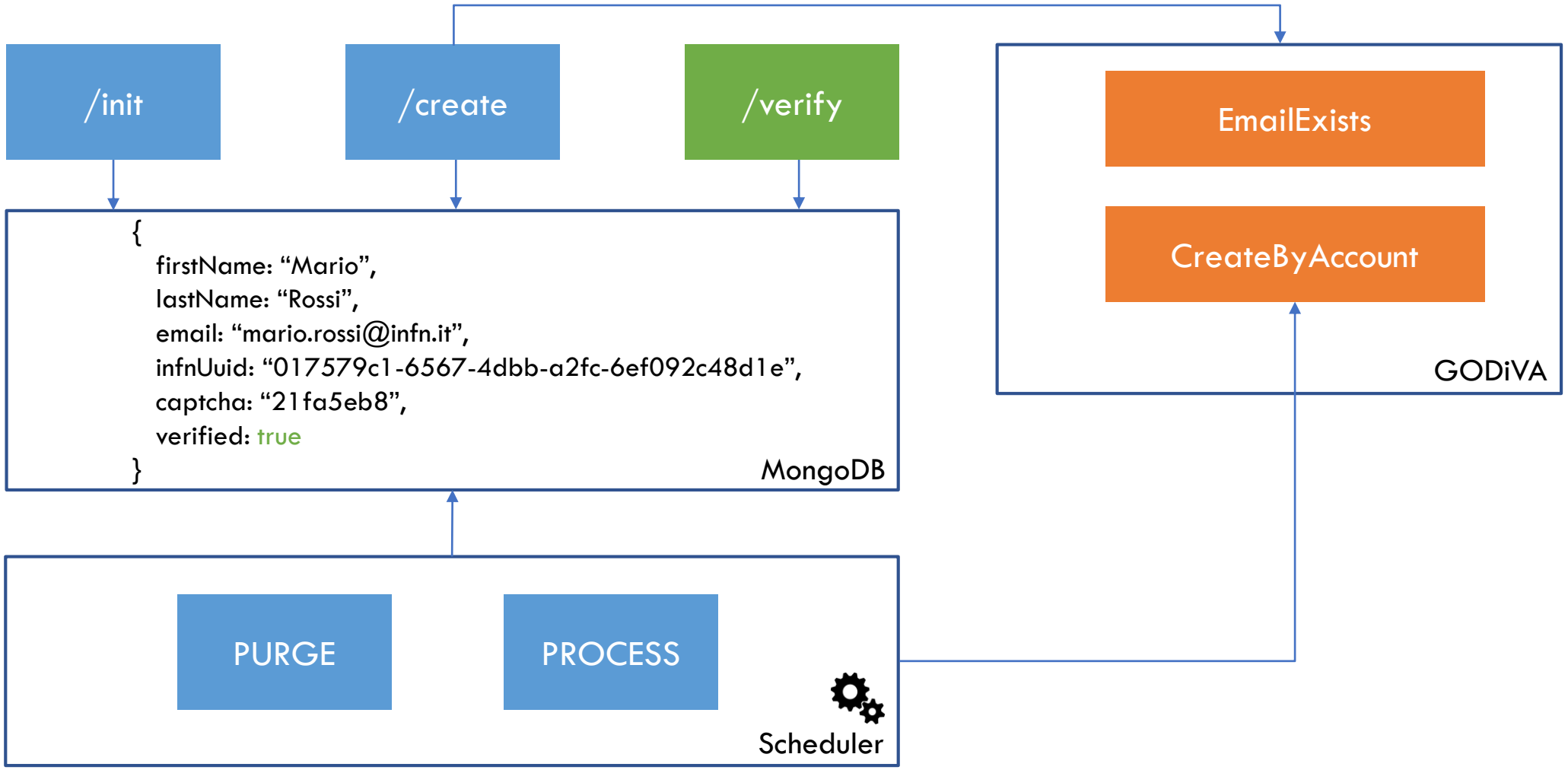
Registrazione Identità Digitale



Registrazione Identità Digitale

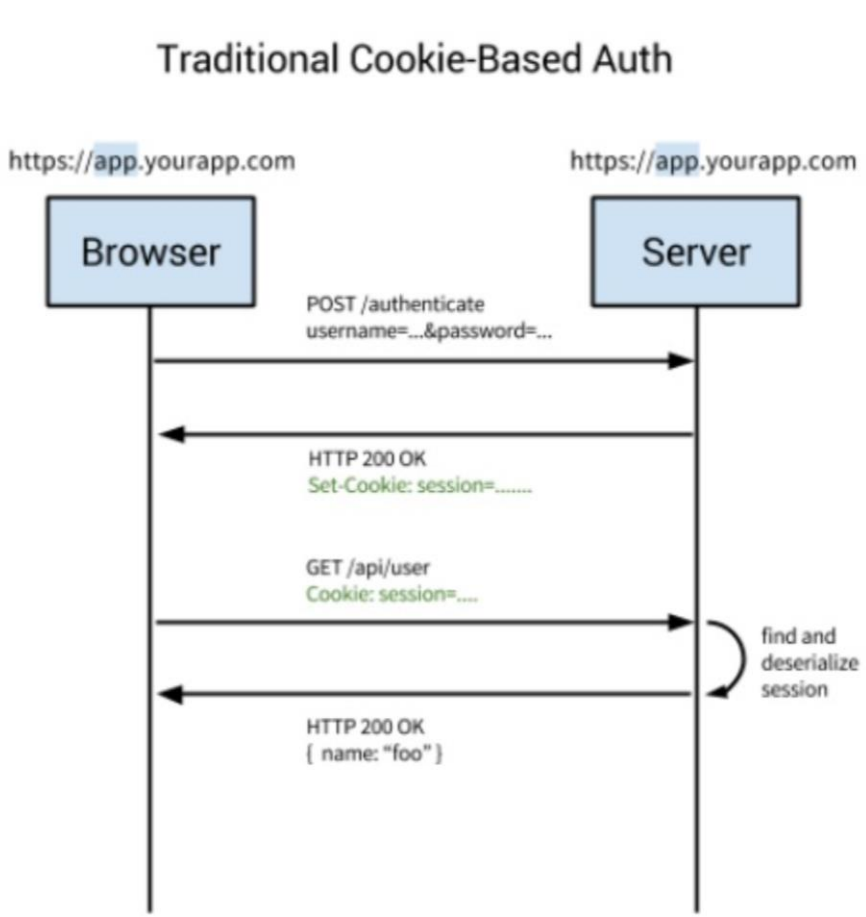


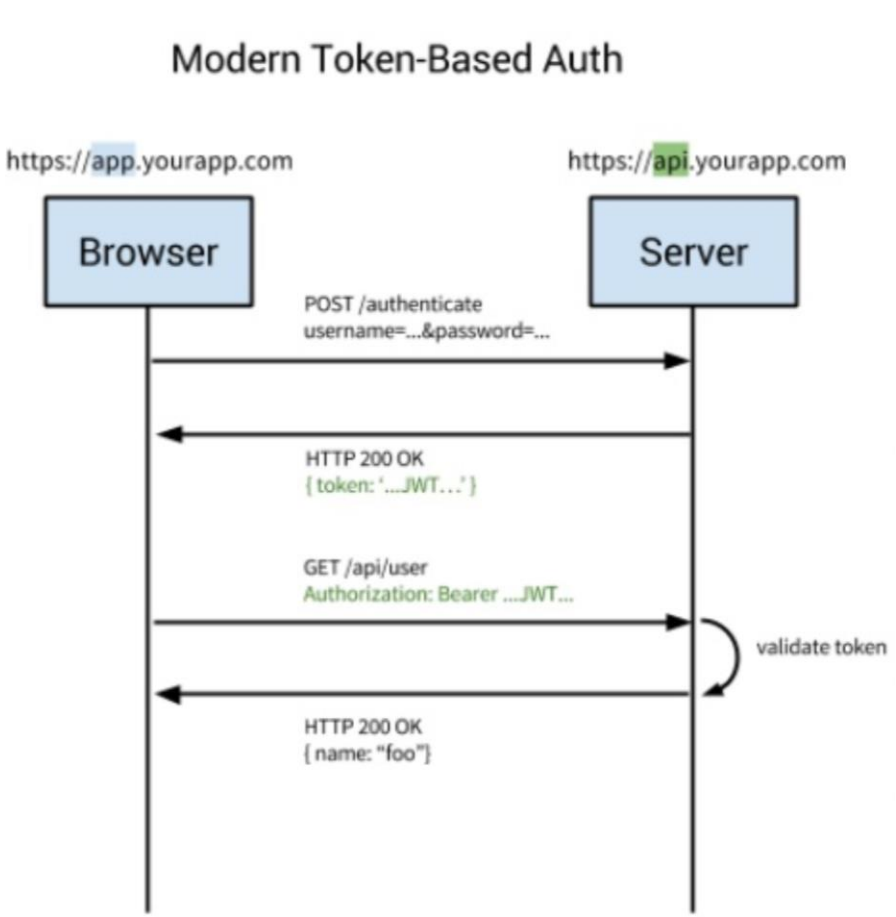
Registrazione Identità Digitale



Interoperabilità tra i servizi: JWT

- Architettura con servizi disaccoppiati
- JSON Web Token è il più utilizzato (Google, Microsoft, Netflix…)
- Trasporta informazioni che possono essere verificate attraverso firma digitale
- Self-contained: i microservizi possono fidarsi delle informazioni contenute nel JWT senza necessità di salvarle in una sessione
- Non avendo necessità di mantenere una sessione (stateless) il sistema può scalare più facilmente


Traditional Cookie-Based Auth
https://app.yourapp.com
https://app.yourapp.com
Browser
Server
POST /authenticate
username=...&password=...
HTTP 200 OK
Set-Cookie: session=.....
GET /api/user
Cookie: session=....
find and
deserialize
session
HTTP 200 OK
{ name: "foo" }


Modern Token-Based Auth
https://app.yourapp.com
https://api.yourapp.com
Browser
Server
POST /authenticate
username=...&password=...
HTTP 200 OK
{ token: '....JWT...' }
GET /api/user
Authorization: Bearer ....JWT...
validate token
HTTP 200 OK
{ name: "foo"}

Come è fatto un JWT

Un JWT è formato da tre parti separate da un . (punto)

Header

L'header contiene 2 campi:

- Il tipo
- L'algoritmo di hashing utilizzato (HMAC SHA256 in questo caso)

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

Plain-text header

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
```

base64encode header

Payload

- Costituito da ”Claims”, i campi dove vengono inserite le informazioni che vogliamo trasportare attraverso il token.
- Ci sono tre tipi di Claims:
  - Registered
  - Public (definite in Internet Assigned Numbers Authority – JSON Web Token Registry)
  - Private

```
{
  "iss": “services.infn.it",
  "exp": 1300819380,
  “infn-uuid": “f8d35e28-2532-43c8-989c-3faa58f5cba4"
}
```

Plain-text payload

```
eyJpc3MiOiJzZXJ2aWNlcy5pbmZuLmlOIiwiZXhwIjoxMzAwO
DE5MzgwLCJpbmZuLXV1aWQiOiJmOGQzNWUyOC0yNTMy
LTQzYzgtOTg5Yy0zZmFhNThmNWNiYTQifQ
```

base64encode payload

Signature

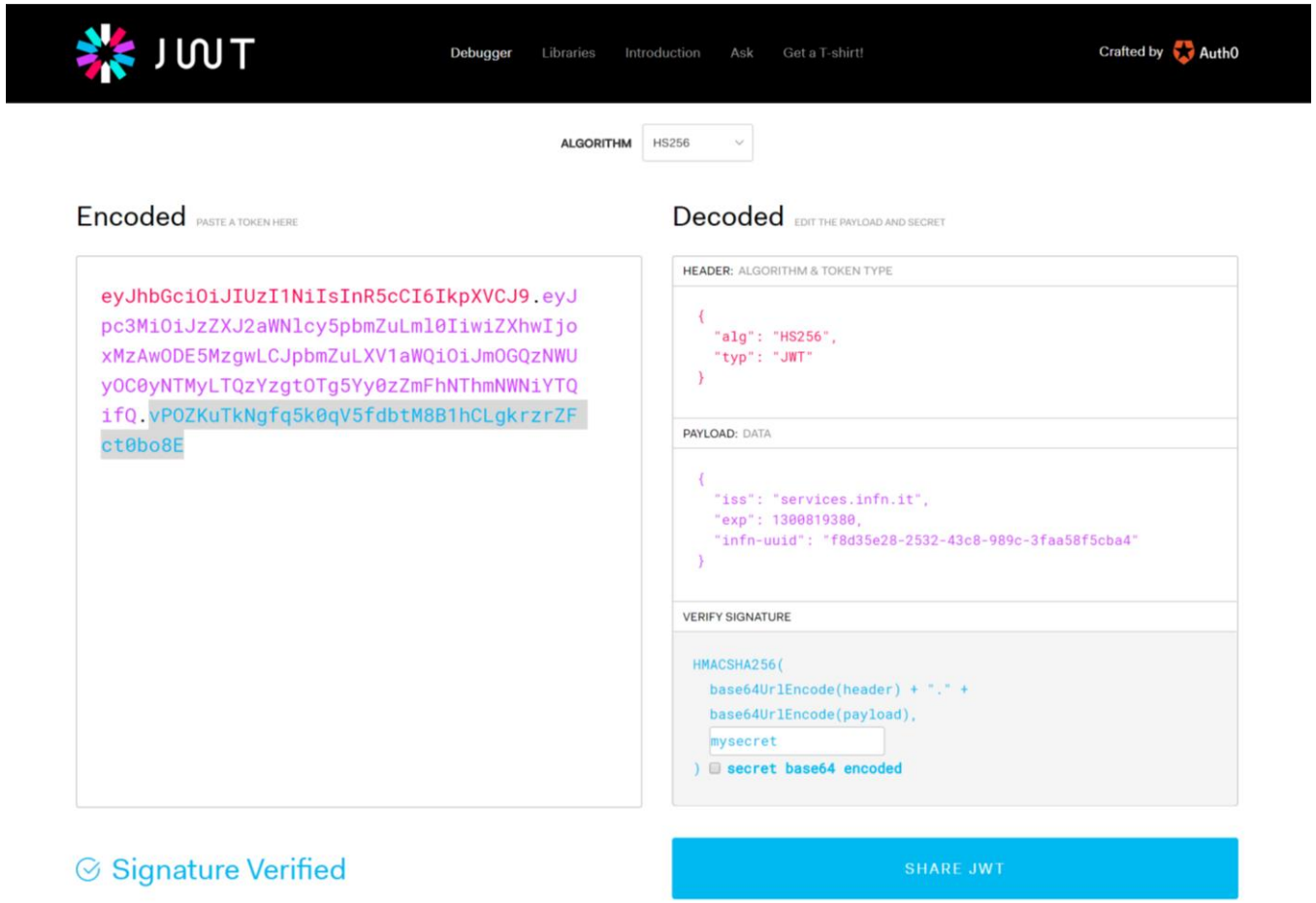
Hashing delle seguenti informazioni:

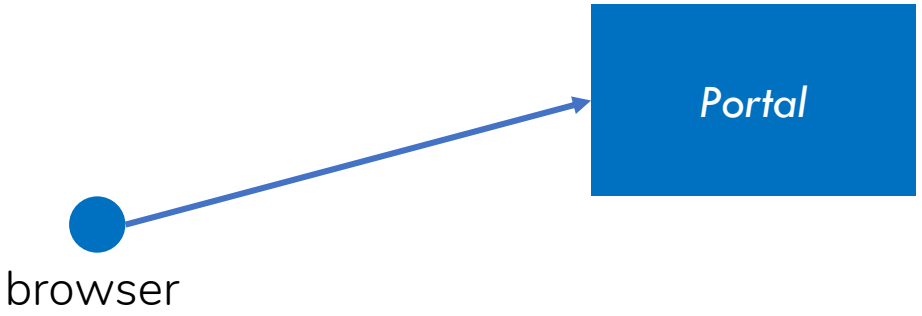
- Header
- Payload
- Secret (tipicamente una chiave privata di un certificate x509)

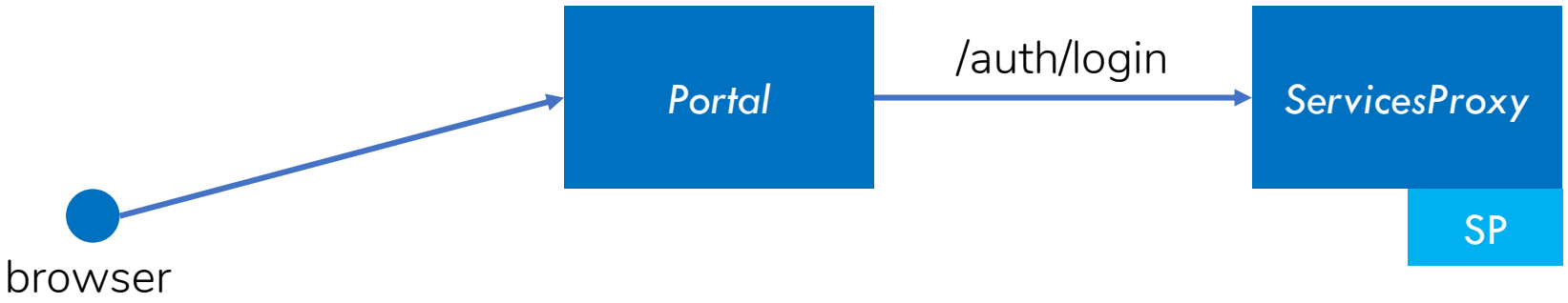
Solo il server conosce il secret e solo lui può creare nuovi token JWT.

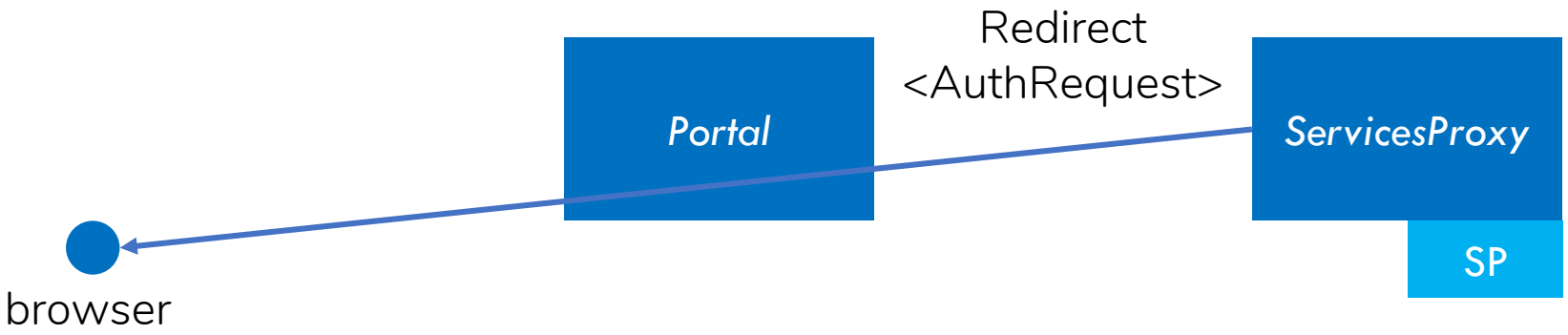
```
var encodedString = base64UrlEncode(header) + "." + base64UrlEncode(payload);

HMACSHA256(encodedString, 'secret');
```

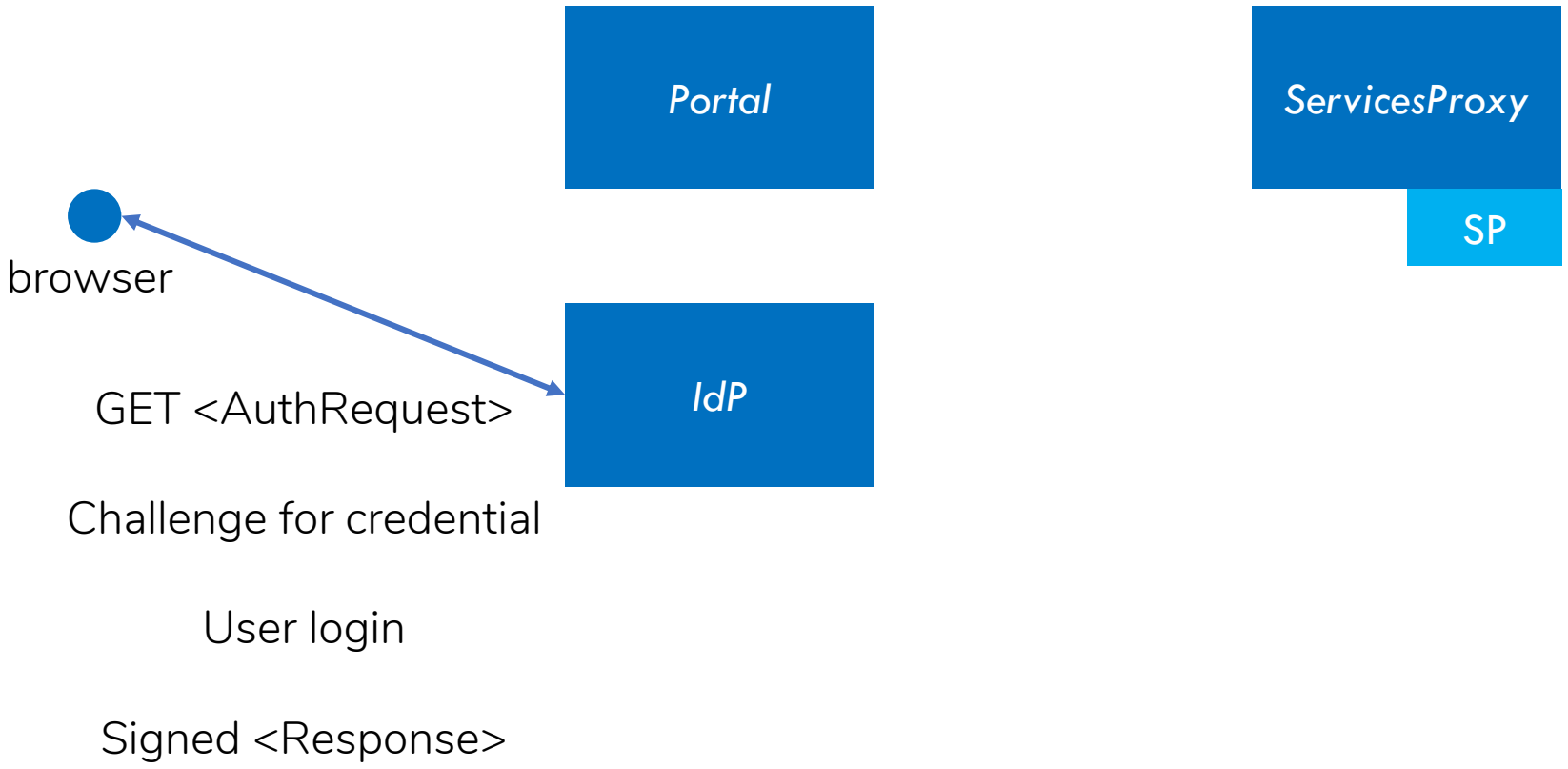
JWT Debugger - https://jwt.io/

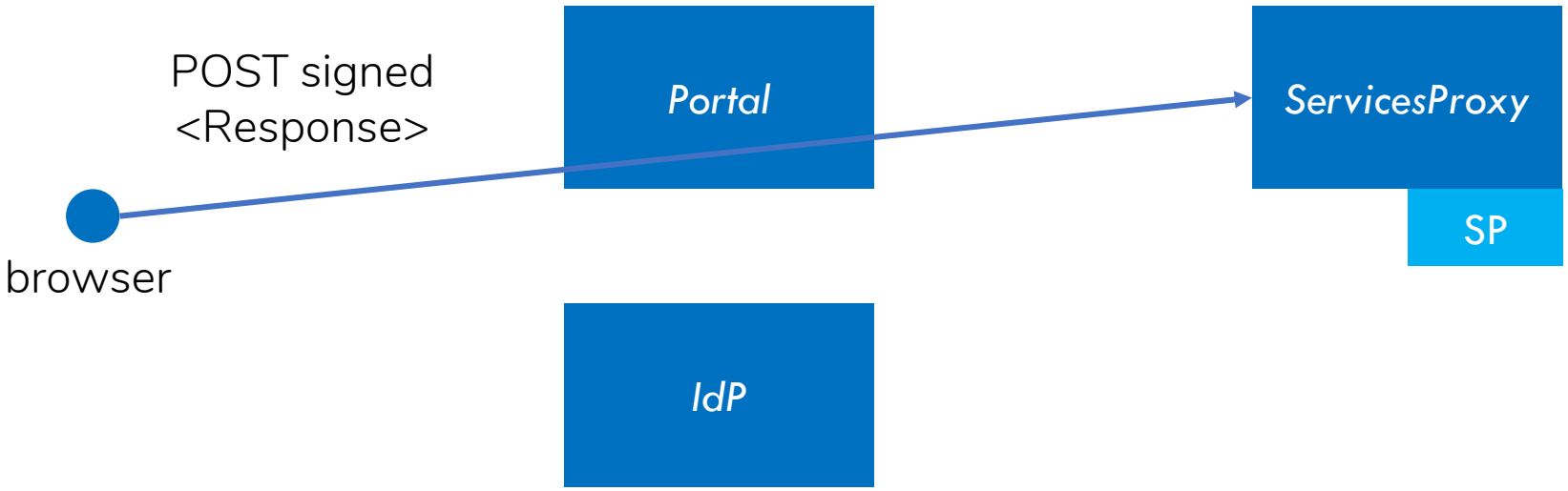


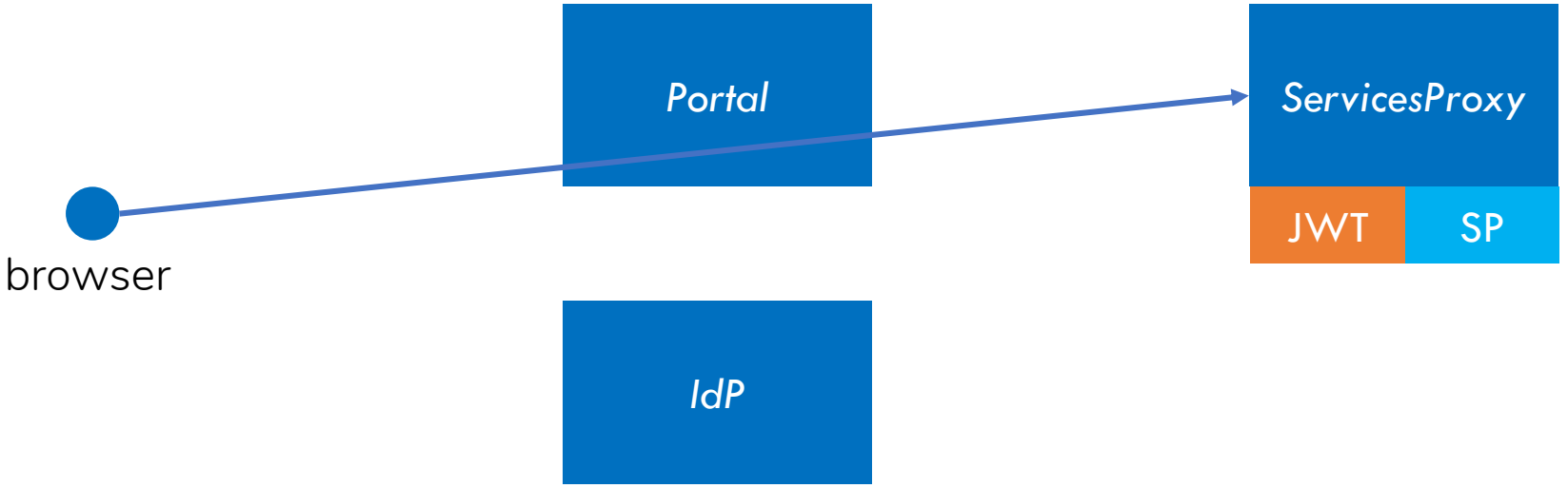

Portal
browser


Portal
/auth/login
ServicesProxy
SP
browser

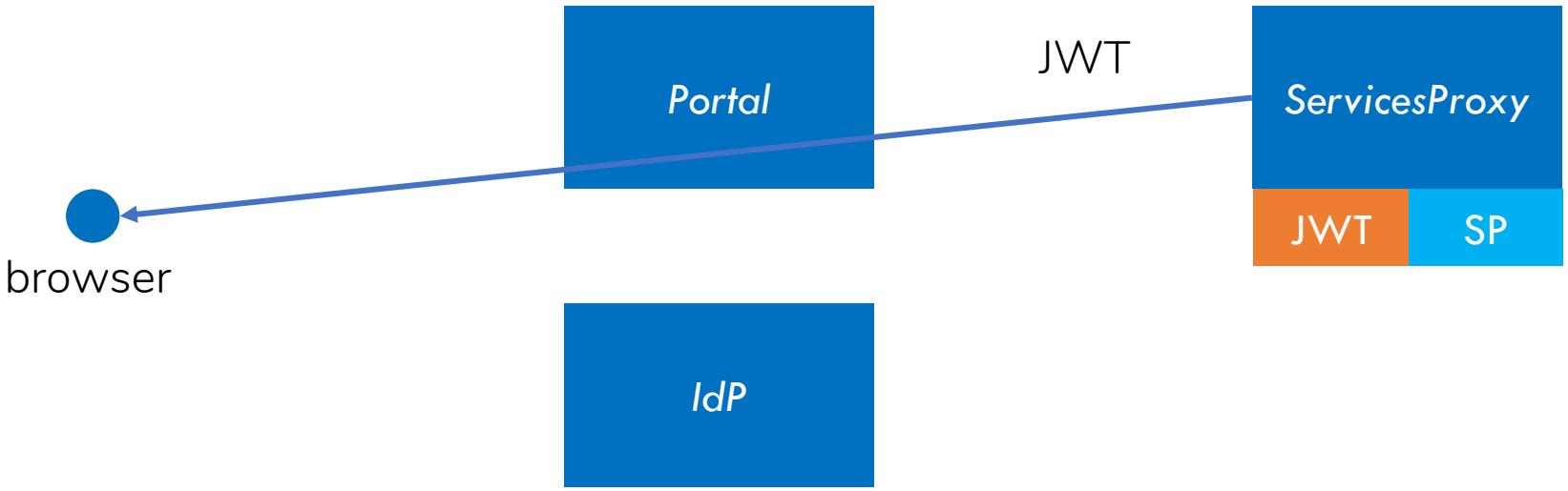

Redirect
<AuthRequest>
Portal
ServicesProxy
SP
browser

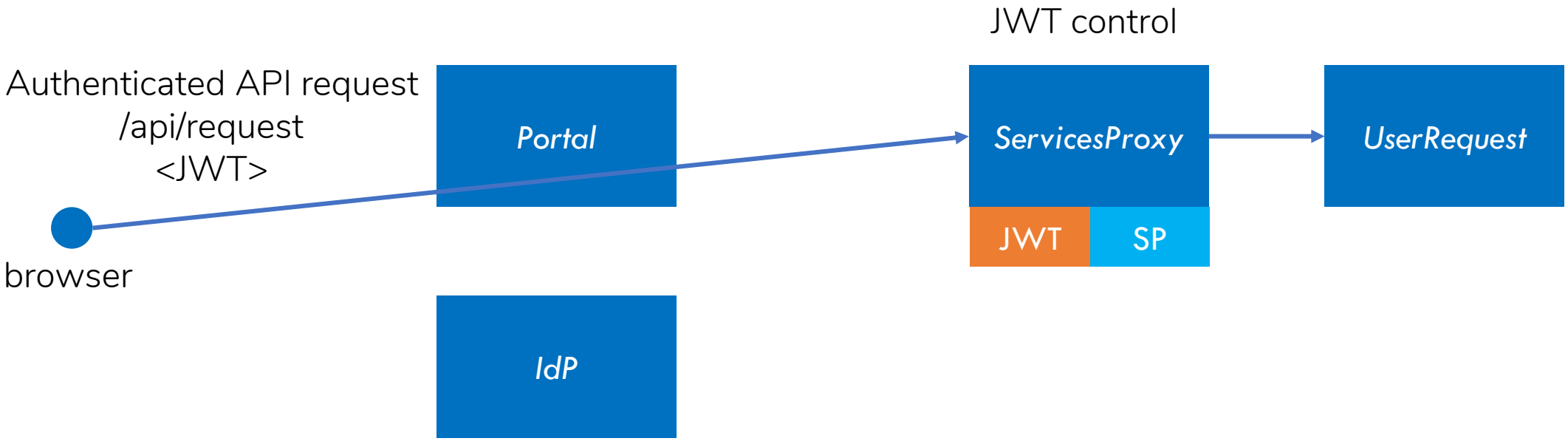

Portal
ServicesProxy
SP
browser
IdP
GET <AuthRequest>
Challenge for credential
User login
Signed <Response>

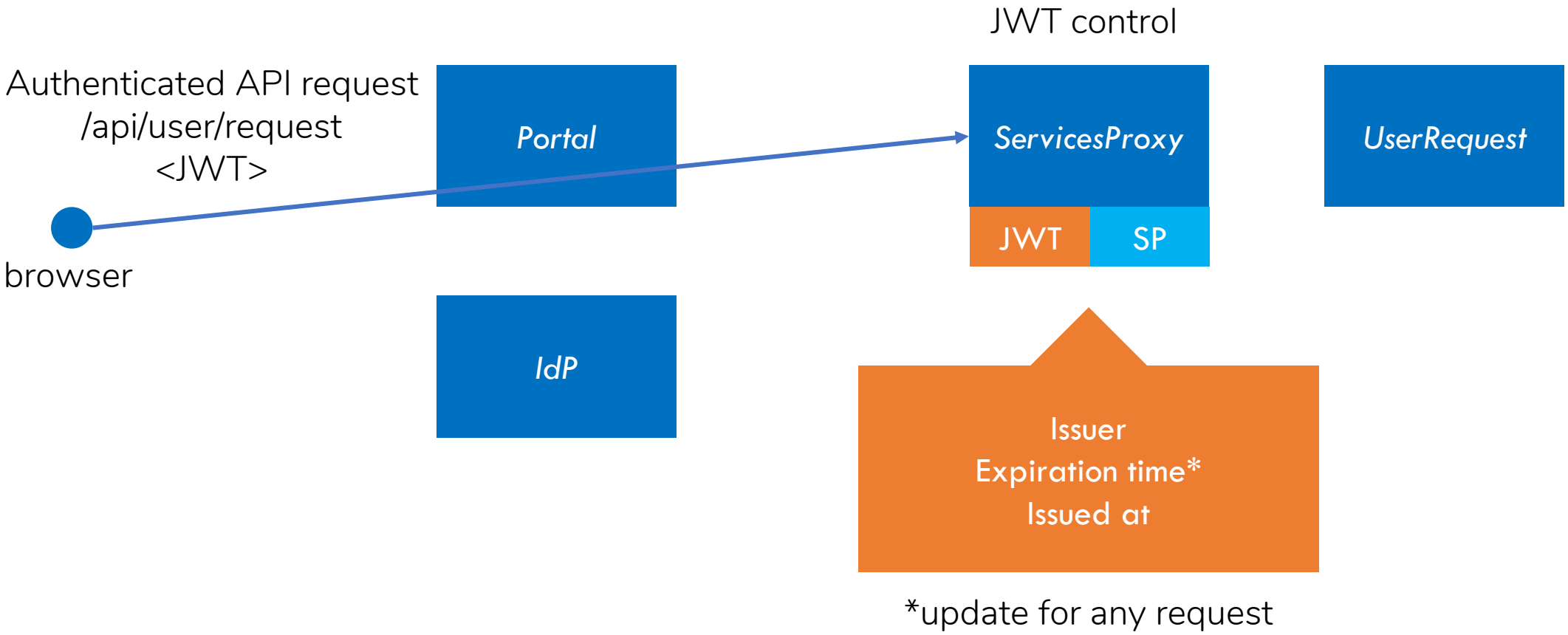

POST signed
<Response>
Portal
ServicesProxy
SP
browser
IdP



Assertion SAML (infn-uuid)
JSON Web Token


Portal
JWT
ServicesProxy
JWT
SP
browser
IdP


JWT control
Authenticated API request
/api/request
<JWT>
Portal
ServicesProxy
UserRequest
JWT
SP
browser
IdP



*update for any request

Continuous Integration

- Baltig
- Continuous integration su creazione di un tag
  - Compilazione
  - Testing
  - Creazione docker
- Deploy manuale su infrastruttura dei microserizi (verrà automatizzato)

Chi siamo

Claudio Bisegni

Calcolo@LNF — Mateusz Gospodarczky

Michele Tota

Calcolo@Roma1 — Marco Esposito

Massimo Pistoni (team coordinator)

Cloud experts @Bari — Marica Antonacci

Giacinto Donvito

Sistema Informativo — Francesco Serafini

Emanuele Turella

Sviluppo software

Infrastruttura

Grazie per l'attenzione