INFRASTRUTTURA DI AUTENTICAZIONE ED AUTORIZZAZIONE

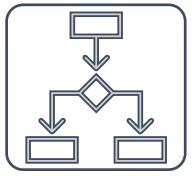
Regione Toscana

Agenda

Autenticazione

Attributi Qualificanti

Autorizzazione

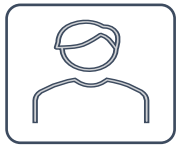


Modalità Integrazione

Autenticazione

CNS (>100 Certificati)

CIE



SPID (Fisici e Giuridici)

EIDAS (Fisici e Giuridici)

SERVER TO SERVER

Autenticazione

- Single Sign-on
- Single Logout
- Livelli di sicurezza
- Memorizzazione a norma
- Controllo Accessi

Attributi Qualificanti

- Recuperati attraverso:
  - RFC 146
  - Attribute Authority SPID
  - IDP Spid
  - IDP Eidas

Attributi Qualificanti

- Evita realizzazione integrazioni custom
- Tracciamento fruizione attributi
- Visibilità limitata
- Gestione Approvazioni utente

Autorizzazione

- Attributi (ABAC)
- Ruoli (RBAC)
- Livello di autenticazione
- Tipo di autenticazione
- Assegnazione manuale (amministrazione delegata)

Applicazioni Integrabili

APPLICAZIONI NATIVE (Mobile e Desktop)

APPLICAZIONI WEB (Server side e SPA)

MICROSERVIZI

IOT (Smart Tv, Wearable, …)

Applicazioni Native / IOT

- Autenticazione semplificata basata su:
  - QRCode
  - Totem
  - OTP
  - CIE
  - SPID
- Durata:
  - Limitata nel tempo
  - Persistente con possibilità di revoca
- Tool a supporto Mobile

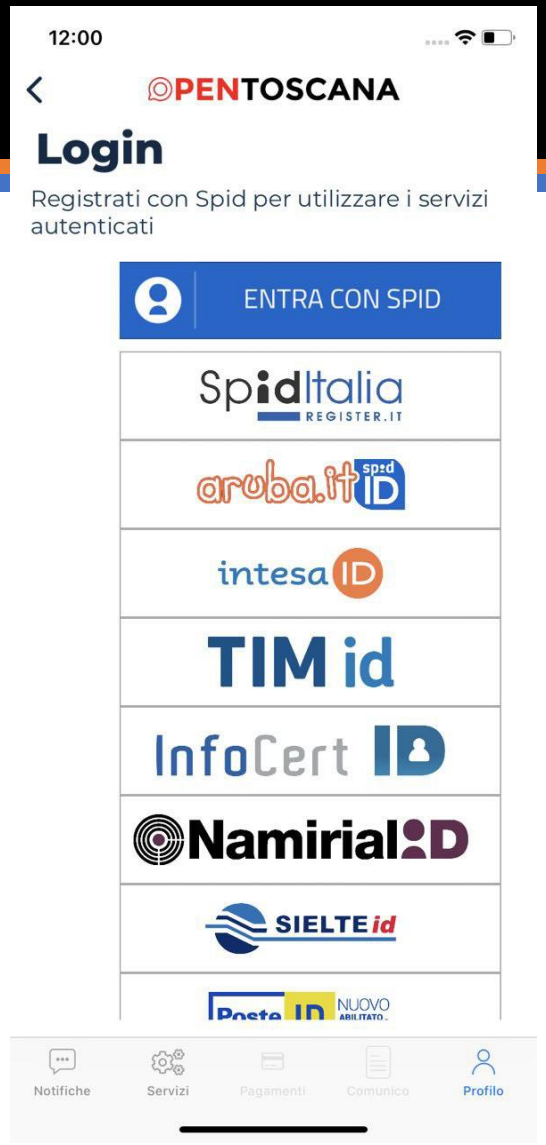
OPENTOSCANA

aperta, innovativa, online

LOGOUT

Ciao, FRANCESCO!

Applicazione	Dispositivo	Sistema operativo	IP Address	Ultimo accesso	Auth Level	Auth Type	
Open Toscana	iPhone	iOS	172.168.1.1	16/09/2019 12:15	2	SPID Poste id	DISCONNETTI



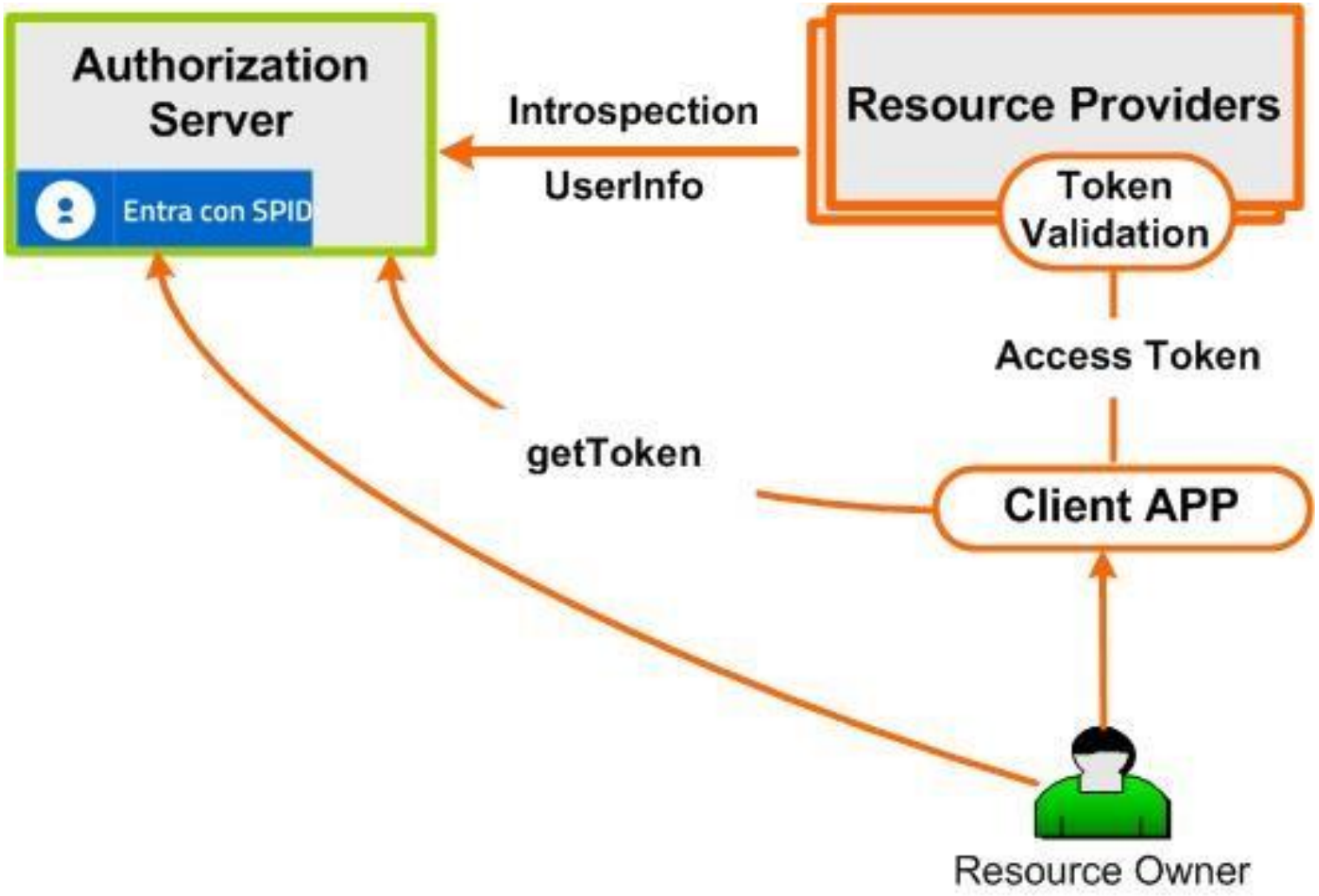
SERVIZIO IDP LIST

- Generazione di un bottone SPID responsive integrabile direttamente nelle applicazioni
- Recupero della lista degli IDP attivi per una costruzione ad-hoc del bottone SPID
- Utilizzabile sia in ambito mobile che in ambito web-application.

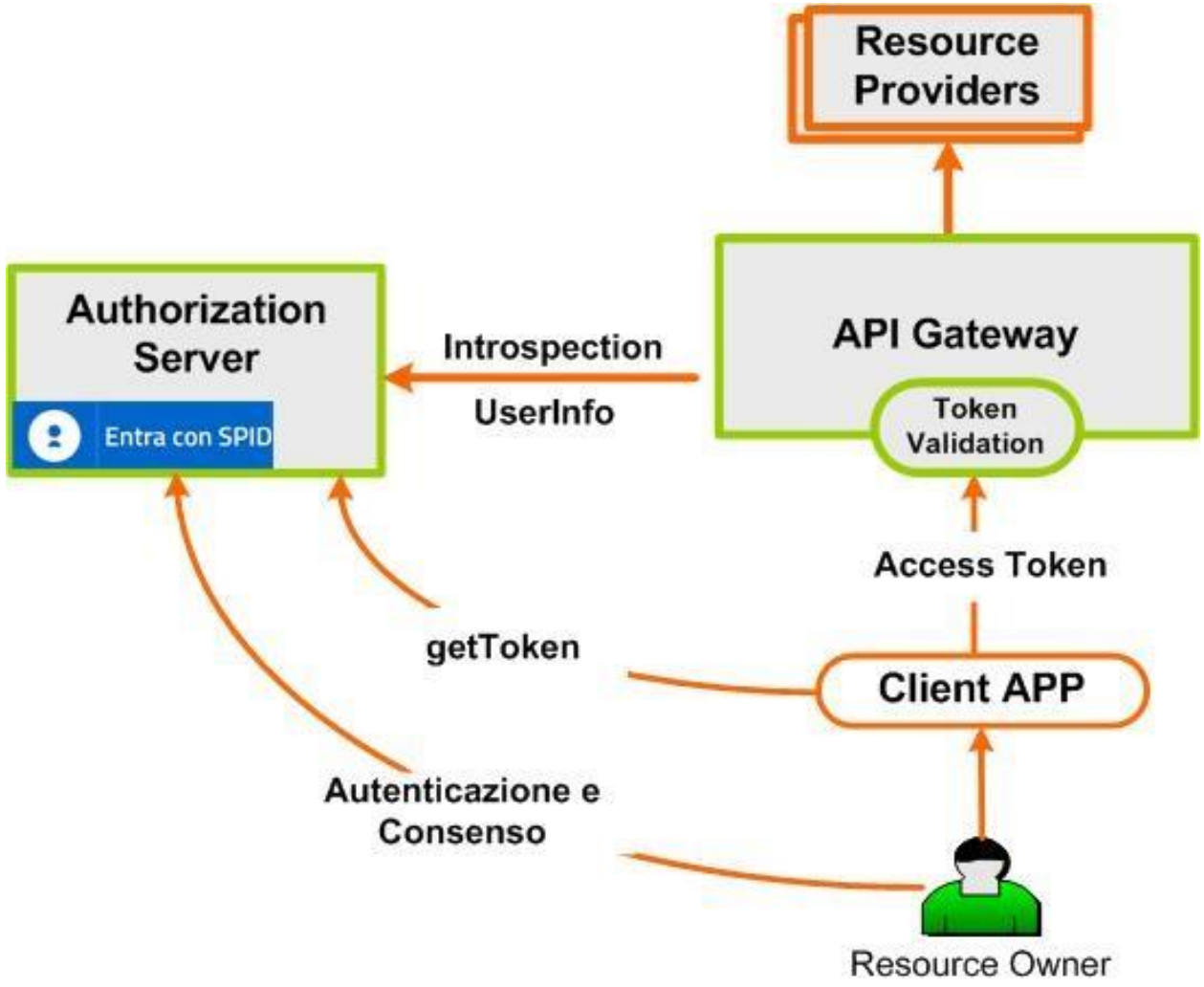
Integrazione

- Attraverso standard:
  - Oauth2
  - OpenId Connect
  - Saml2
- Attraverso Infrastruttura:
  - API Gateway
  - Application Server Template

SCENARIO


Authorization Server
Entra con SPID
Introspection
UserInfo
Resource Providers
Token Validation
Access Token
getToken
Client APP
Resource Owner

SCENARIO GATEWAY



Modalita di Integrazione

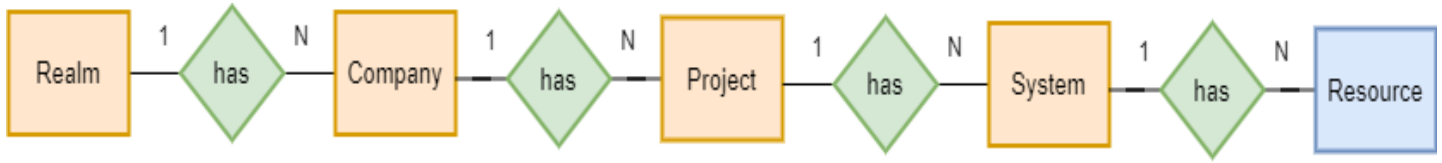
APPLICAZIONI NATIVE (Mobile e Desktop)

APPLICAZIONI WEB (Server side e SPA)

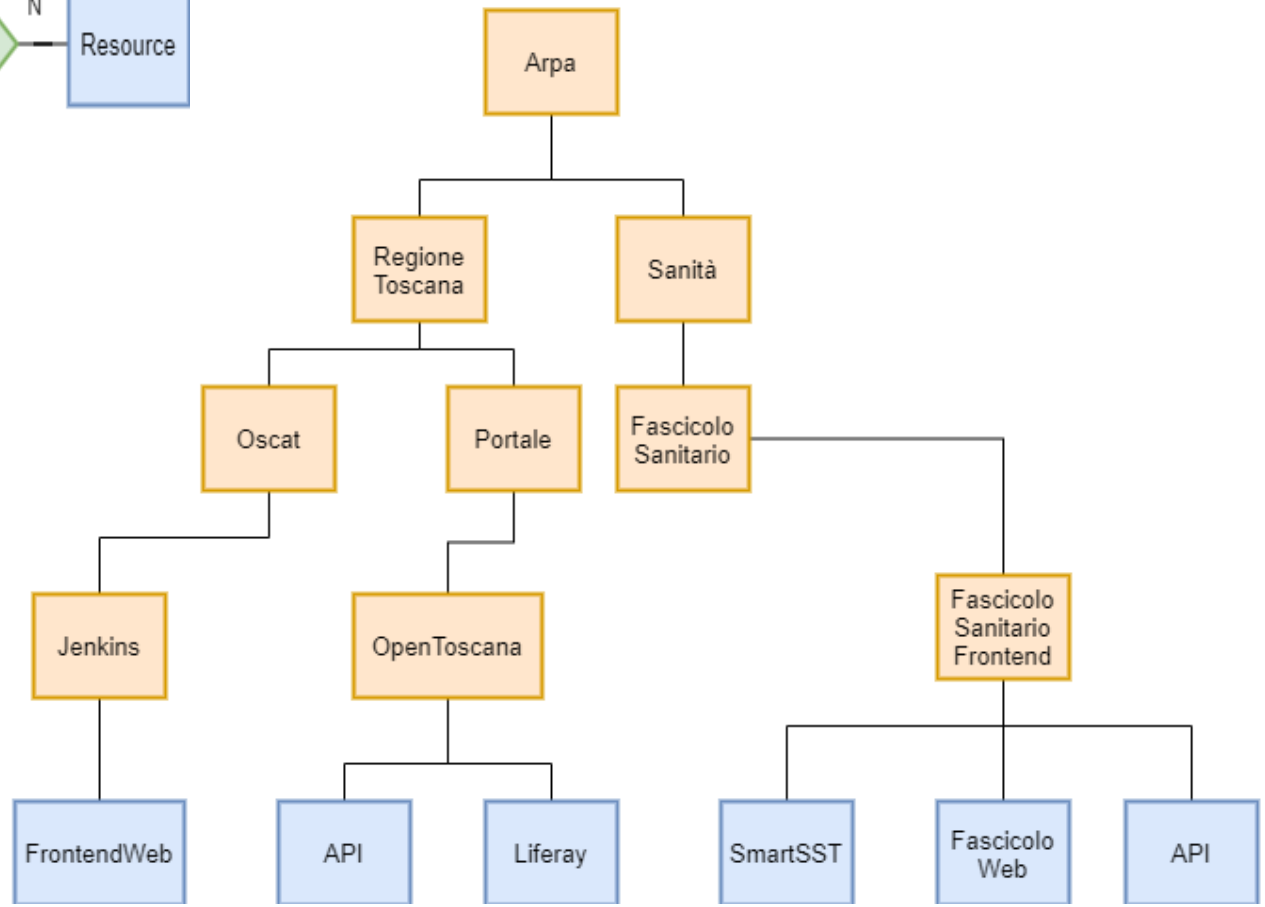
MICROSERVIZI

IOT (Smart Tv, Wearable, …)

Amministrazione delegata



- Amministratori gerarchici
- Approvazione operazioni
- Monitoraggio



Richiesta di integrazione

- Documentazione: http://oscat.rete.toscana.it/docman/?group_id=803
- Indirizzo per effettuare le richieste di integrazione: arpa@regione.toscana.it

Monitoraggio accessi applicazione integrata

- Log strutturati delle interazioni tra le applicazioni e l'authorization server
- Configurazione di un index-alias Elasticsearch (da richiede ai gestori dell'ELK di Regione Toscana) per poter ottenere i log strutturati relativi alla propria applicazione
- Maggiori informazioni nel documento ARPA – Monitoraggio Accessi Applicativi

Monitoraggio accessi applicazione integrata


```
"event": {
        "username": "<CODICE-FISCALE>",
        "tokenID": "AQIC5wM2LY4SfcxkcBXKN2PNGYF3YBKmXZC699nQ9an4QQ8.*MxAAIwMw..*",
        "authType": "Arpa",
        "auth_time": "1604928529",
        "clientId": "<CLIENT-ID>",
         "auth_method": "validate_access_token",
        "authID": "openam02_2969_16049285****_83093",
        "authTS": "1604928523841",
        "identity_provider": "arpa",
        "userId": "c72eb89e-3fa7-4211-9739-f3ad*********",
        "ipAddress": "159.213.***.***",
        "token_id": "8e2cabb3-a128-4d2b-8216-b*********",
        "identity_provider_identity": "<CODICE-FISCALE>",
        "authSpidCode": "arpa-rsalsn65r16d612b",
        "authLevel": "4",
        "type": "USER_INFO_REQUEST"
}
```

DOMANDE?