Experiences Using OAuth 2.0 in Federated and Multichannel Open Service Platform

Raman Kazhamiakin   Giada Sciarretta

FONDAZIONE BRUNO KESSLER

Smart Community

ST SECURITY & TRUST

3rd OAuth Security Workshop (OSW18)
Trento - MARCH 15, 2018

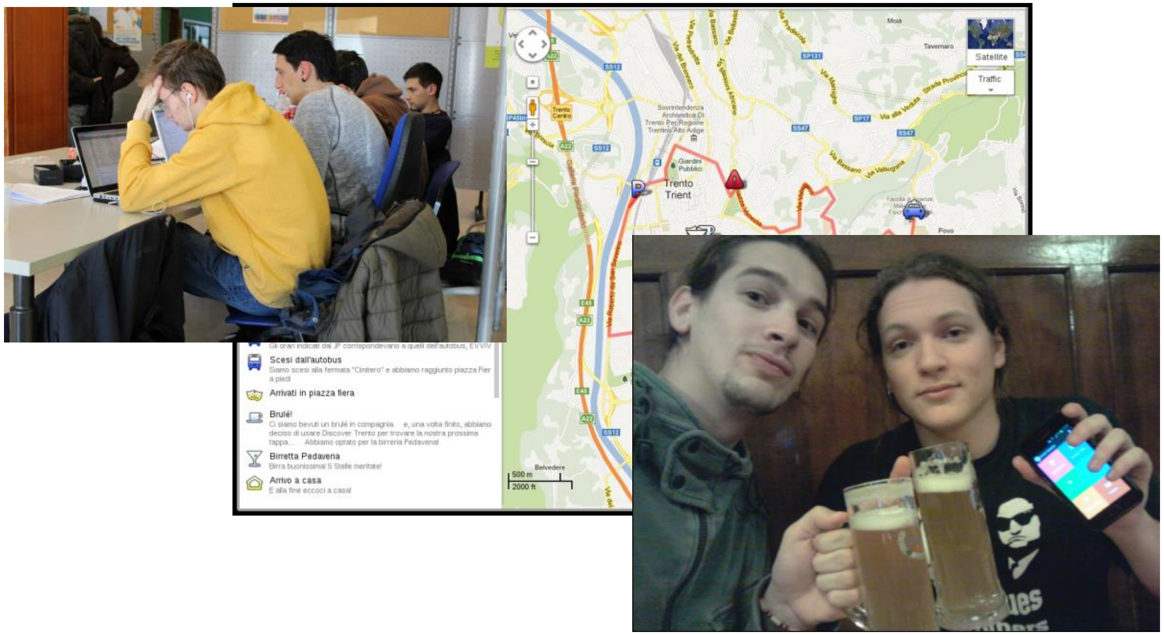
Outline

- Smart Community Platform
  - From Smart Campus …
  - … to Open Services
  - Authentication and Authorization for Open Platform
- Integrating External IdPs in Platform
- Integrating Second Factor Authentication

Smart Campus

- Project with the Univiersity of Trento
  - «Build Services **WITH** and **FOR** Students»

- Driven and developed by the community
  - Students as designers, developers, testers, users…
  - Contests and Hackatons
  - End-to-end student development teams


Gli orari indicati dal JP corrispondevano a quelli dell'autobus, EVVIV

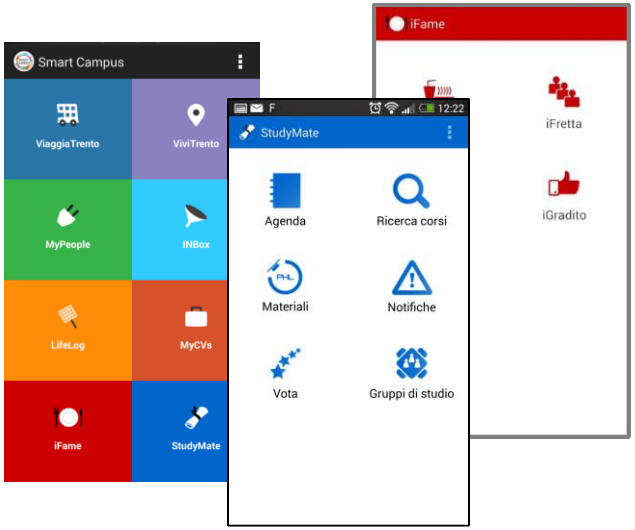
Scesi dall'autobus
Siamo scesi alla fermata "Cimitero" e abbiamo raggiunto piazza Fier a piedi

Arrivati in piazza fiera

Brulé!
Ci siamo bevuti un brulé in compagnia e, una volta finito, abbiamo deciso di usare Discover Trento per trovare la nostra prossima tappa.... Abbiamo optato per la birreria Pedavena!

Birretta Pedavena
Birra buonissima! 5 Stelle meritate!

Arrivo a casa
E alla fine eccoci a casa!



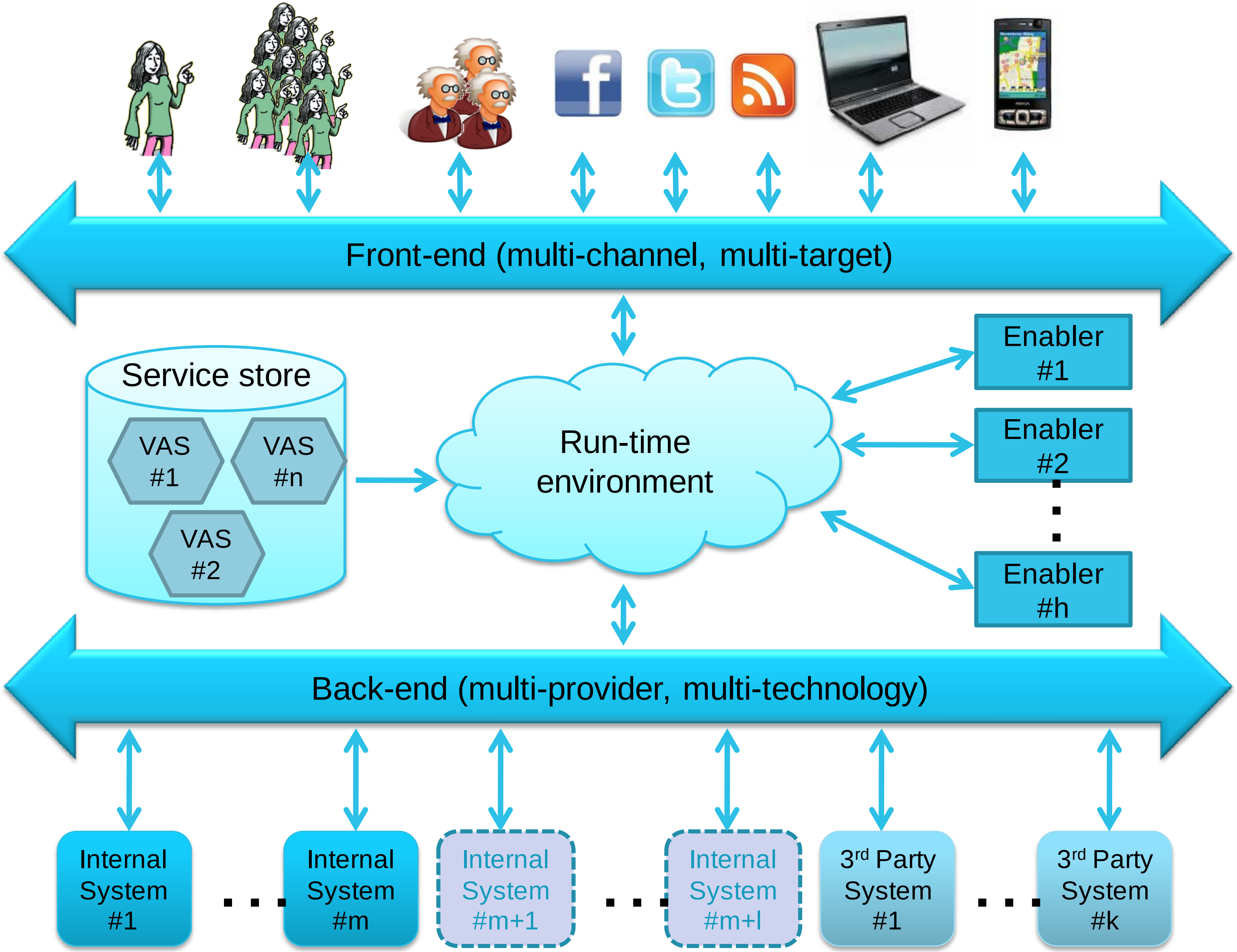
Smart Campus

- Project with the Univiersity of Trento
  - «Build Services **WITH** and **FOR** Students»

- Driven and developed by the community
  - Students as designers, developers, testers, users…
  - Contests and Hackatons
  - End-to-end student development teams

- Open Platform
  - **Multi-channel**: Web and mobiles apps → Open API
  - **Common services**: communication, profiling, storage…
  - **Common security**: OAuth2.0 protocol
  - **Extensible security**: custom and dynamic scopes, role-based access…
  - **Extensible identity management**: from UniTN (Shibboleth) to multiple options (FBK, Google, Facebook, Trento Province authentication)

Smart Campus: Architecture



Front-end (multi-channel, multi-target)

Service store

VAS #1

VAS #n

VAS #2

Run-time environment

Enabler #1

Enabler #2

Enabler #h

Back-end (multi-provider, multi-technology)

Internal System #1

Internal System #m

Internal System #m+1

Internal System #m+l

3rd Party System #1

3rd Party System #k

Smart Community: Open Services

- Bring the vision to Smart City level
  - **Open Services**
    - Standard and Open Documentation (Swagger)
    - Standard protocols (REST/JSON, OAuth2.0)
    - Service **catalogue**, **access** management, **testability** (API management)
  - Heterogeneous, multi-provider sources
    - Public and **private** data
    - PA and local companies

GiPro

FUTURA TRENTO BENE COMUNE

SCUOLA CLIMB

Streetlife

WeLive

Simpatico

Viaggia Trento

100% TRENTO

NORTH LAKE GARDA TRENTINO ITALY TESORI NASCOSTI

VIAGGIA Play&Go

Open Service Platform: Challenges

- Open Platform to 3rd party providers and consumers
  - Publish **own APIs**

  - Access **sensitive** data (e.g., personal data) via existing APIs

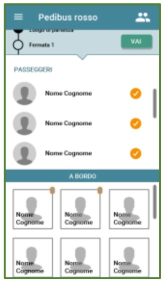
  - Support security «**customization**»
    - Local/national providers and protocols
      - CPS, SPID, Vivo Scuola
      - Shibboleth, LDAP, CAS, «native» login

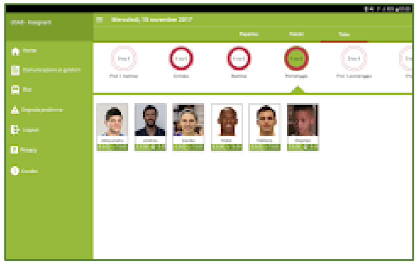
  - **Multi-channel**
    - Web app, mobile, IoT, non-API resources

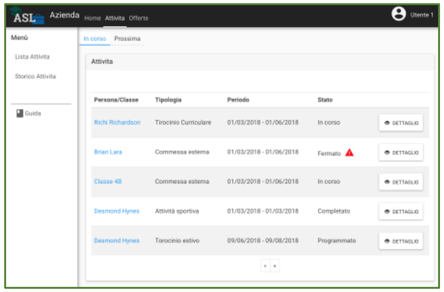
  - **Different** authentication requirements
    - Weak, but flexible for end users (e.g., Facebook, Google)
    - Strong for PA services (SPID, CPS, two-factor authentication)

Use Case: Education Domain

- Family of products at different levels and different areas
  - Pre-school, elementary, high school
  - Communications, management, education, …
- Different channels and technologies
  - Mobile apps, desktop, interactive boards, IoT







Attività

Persona/Classe	Tipologia	Periodo	Stato	
Richi Richardson	Tirocinio Curriculare	01/03/2018 - 01/06/2018	In corso	DETTAGLIO
Brian Lara	Commessa esterna	01/03/2018 - 01/06/2018	Fermato	DETTAGLIO
Classe 4B	Commessa esterna	01/03/2018 - 01/06/2018	In corso	DETTAGLIO
Desmond Hynes	Attività sportiva	01/03/2018 - 01/03/2018	Completato	DETTAGLIO
Desmond Hynes	Torocinio estivo	09/06/2018 - 09/08/2018	Programmato	DETTAGLIO

- Security aspects
  - **Common** framework for identity management and service access across apps
  - Different **authentication** mechanisms (SPID, Google, LDAP)
  - Different **roles** (“normal” users, school staff, students)
  - Different types of **data** and **operations**: **strong** authentication required for certain cases
  - Personalized access **delegation** (e.g., for parents)

Open Services: Why OAuth2.0?

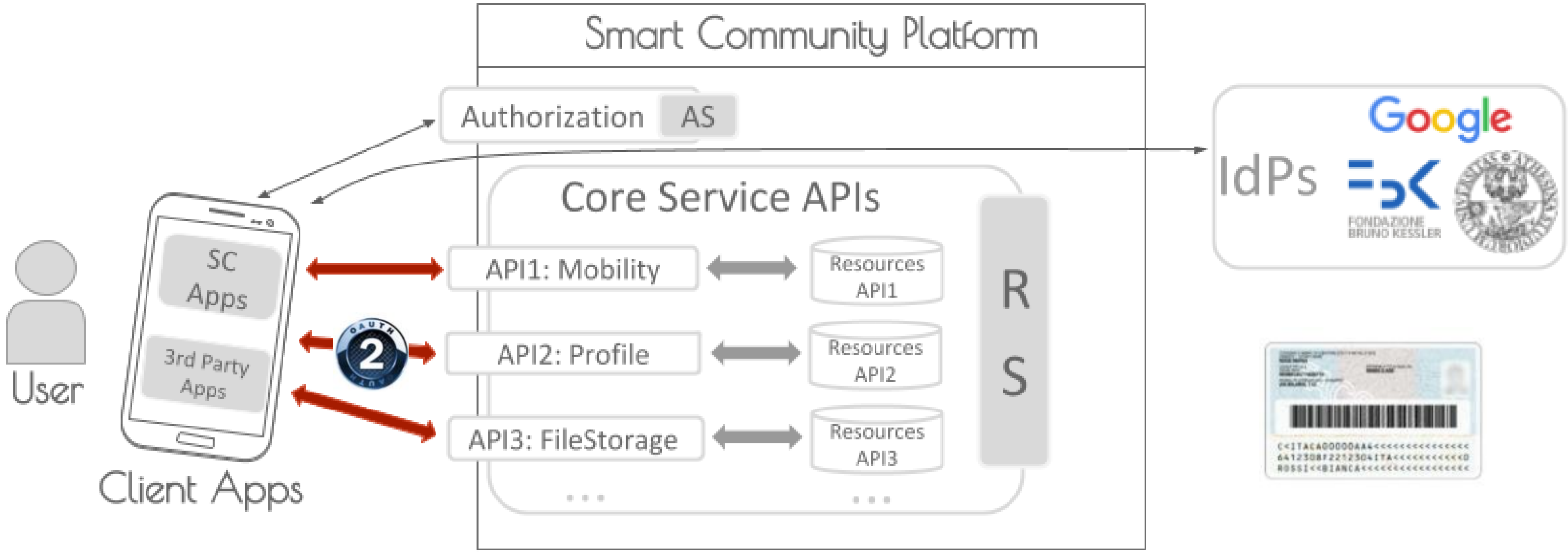
- Reference security protocol for APIs
  - Exploited by most API Management solutions
  - Supported by many API providers and components
- Easy to integrate
  - In the platform components
  - In client applications
- Easy to extend and customize
  - Scopes, flows
  - Authentications

Challenges

- Usage for “non-standard” API settings and integrations
  - Web-sockets, MQTT (IoT domain)
  - Resource access (e.g., images, OGC services)
- Flow customization in open environment

Smart Community: OAuth

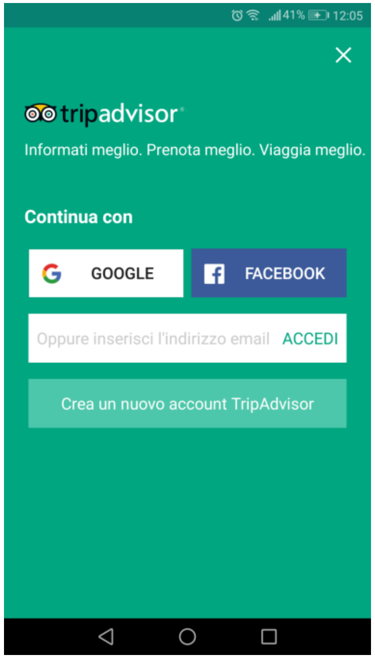
Design a delegation access solution for smart city apps to access data stored by Smart Community platform through APIs



- Smart Community AS does not manage authentication → use of external IdPs
- Some applications (mostly of the PA) require an high level of assurance on the identity proofing and authentication

Integration with Google

- For mobile apps, you may prefer to use Google Sign-in
  https://developers.google.com/identity/protocols/OAuth2InstalledApp

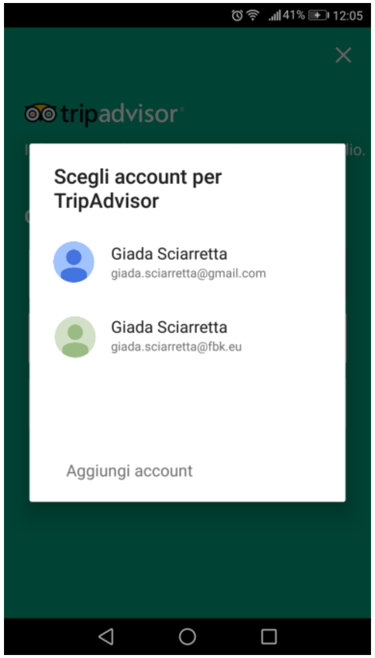


Informati meglio. Prenota meglio. Viaggia meglio.

Continua con

Oppure inserisci l'indirizzo email ACCEDI

Crea un nuovo account TripAdvisor

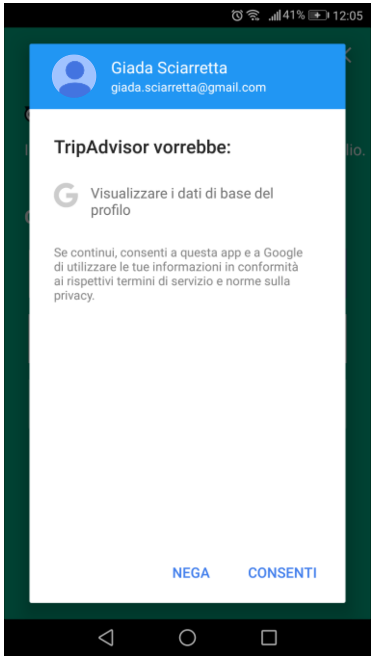


Scegli account per TripAdvisor

Giada Sciarretta
giada.sciarretta@gmail.com

Giada Sciarretta
giada.sciarretta@fbk.eu

Aggiungi account



Giada Sciarretta
giada.sciarretta@gmail.com

TripAdvisor vorrebbe:

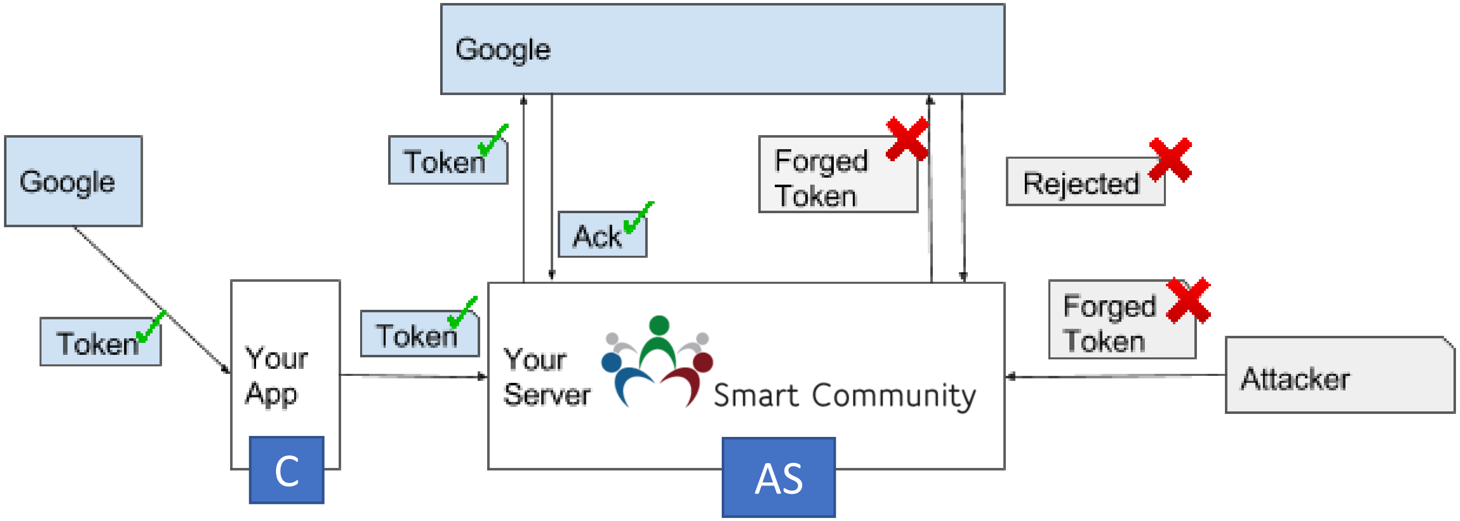
Visualizzare i dati di base del profilo

Se continui, consenti a questa app e a Google di utilizzare le tue informazioni in conformità ai rispettivi termini di servizio e norme sulla privacy.

- Google Sign-in supports OAuth-OpenID Connect

? How do we integrate Google OIDC with SC OAuth?

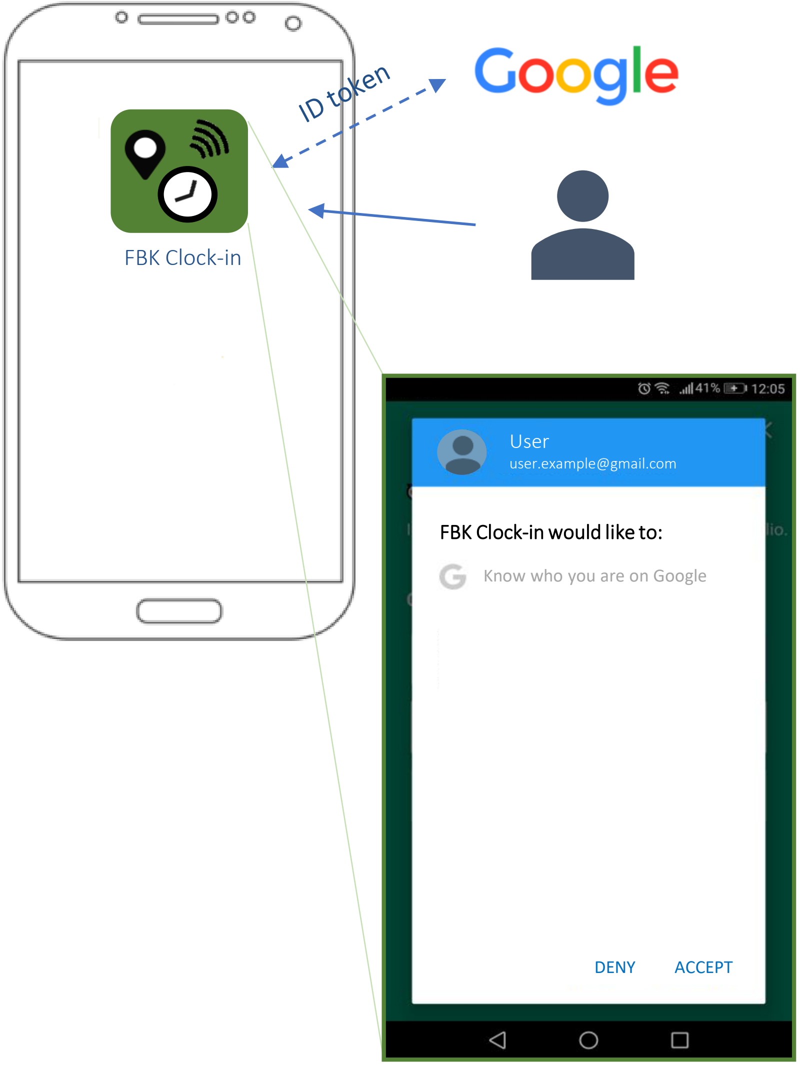
One Solution: Backend Authn



After a user successfully signs in, send the user's **ID token to your server** using HTTPS. Then, on the **server, verify** the integrity of the ID token and use the user information contained in the token to establish a session or create a new account.

https://developers.google.com/identity/sign-in/android/backend-auth

SC OAuth + Google Backend Authn

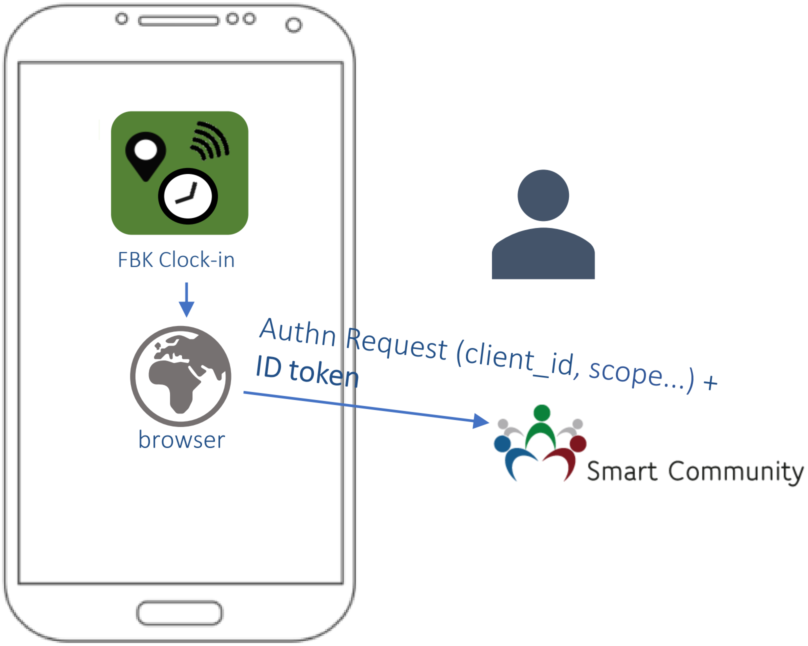


User
user.example@gmail.com

FBK Clock-in would like to:

Know who you are on Google

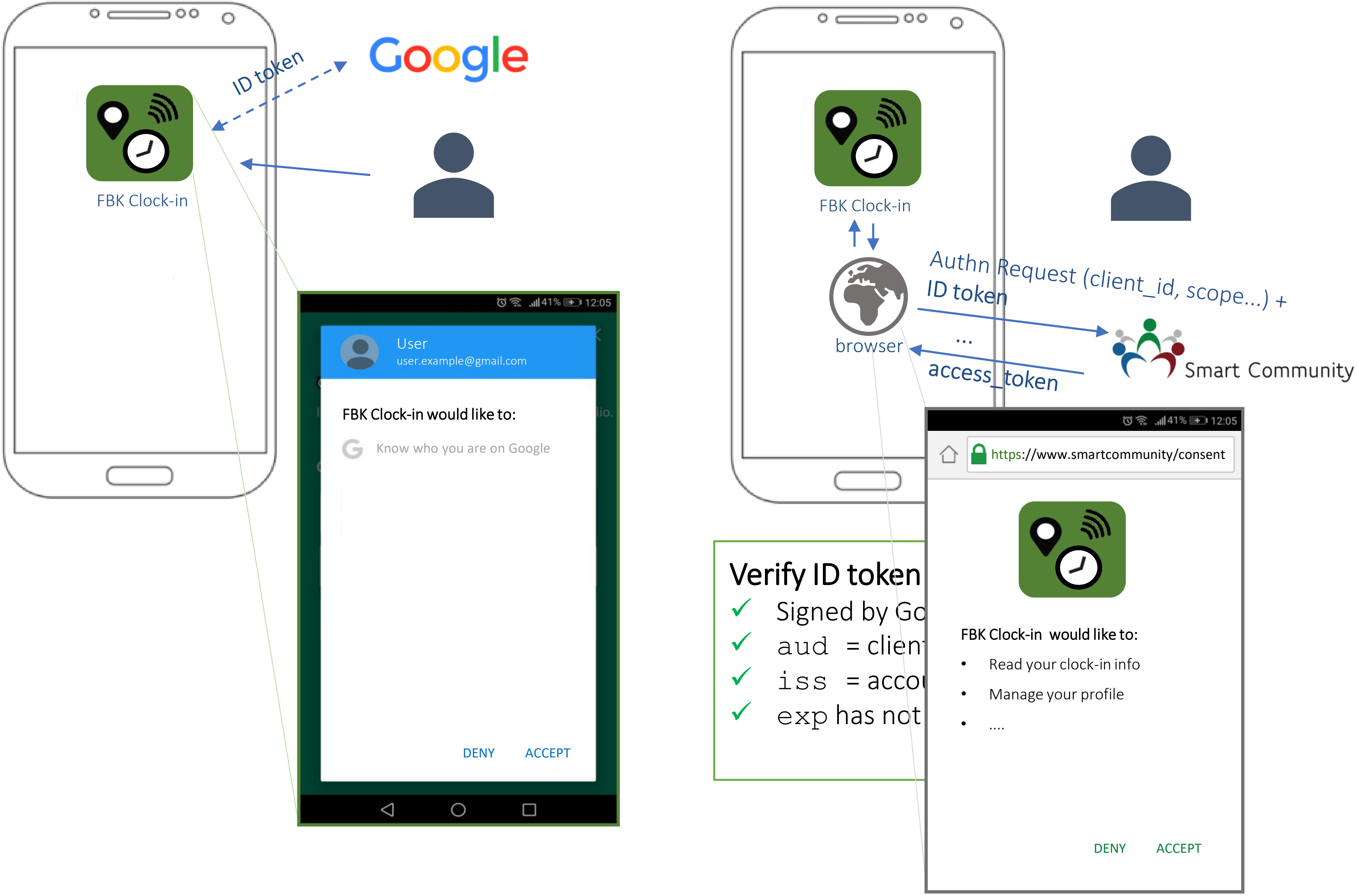
DENY ACCEPT



Verify ID token

- ✓ Signed by Google
- ✓ `aud` = client ID of FBK clock-in
- ✓ `iss` = accounts.google.com
- ✓ `exp` has not passed

SC OAuth + Google Backend Authn



User
user.example@gmail.com

FBK Clock-in would like to:

Know who you are on Google

DENY ACCEPT

https://www.smartcommunity/consent

FBK Clock-in would like to:

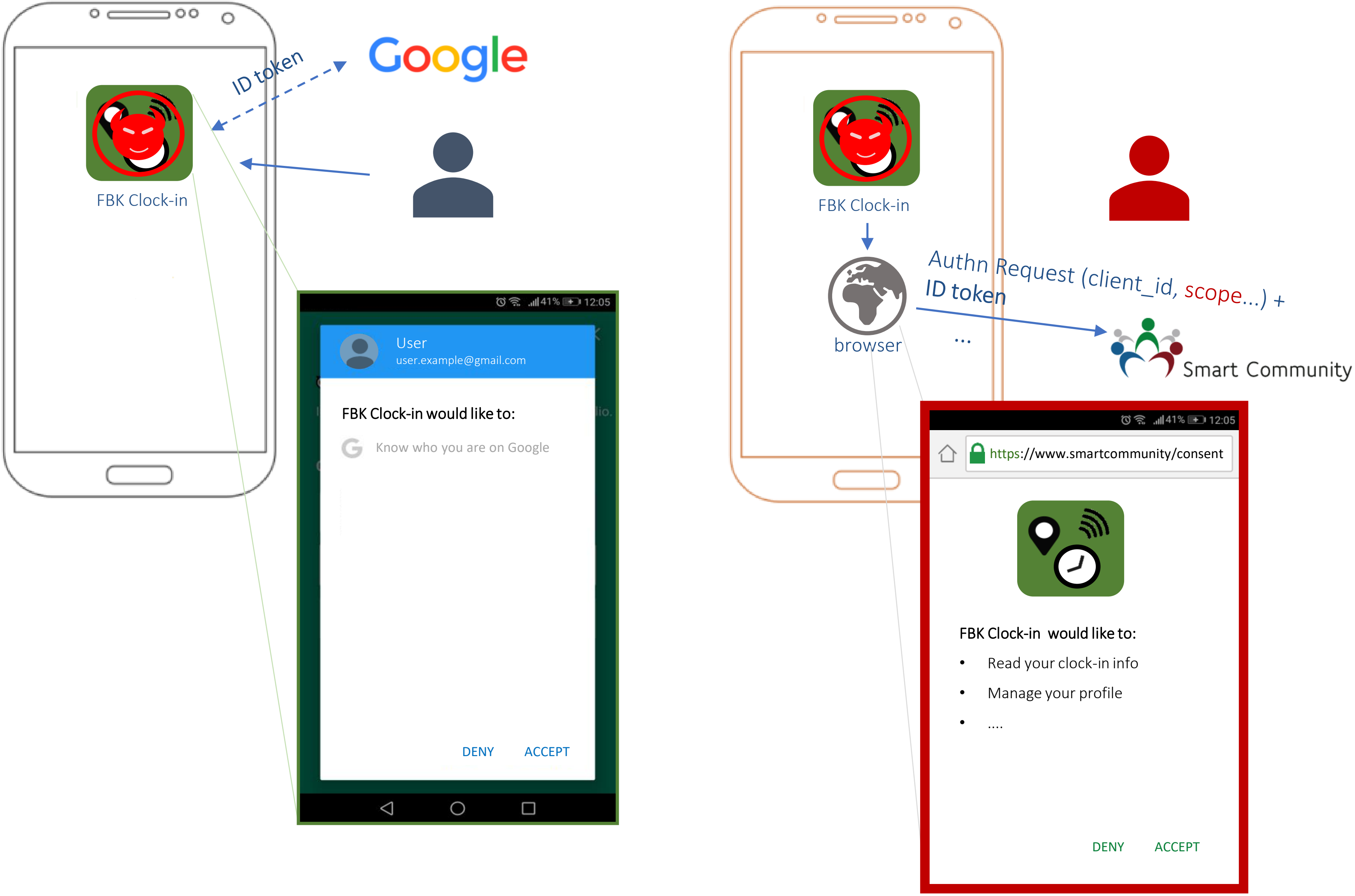
- Read your clock-in info
- Manage your profile
- ....

DENY ACCEPT

Verify ID token

✓ Signed by Go
✓ aud = client
✓ iss = accou
✓ exp has not

User Impersonation Attack



User
user.example@gmail.com

FBK Clock-in would like to:

Know who you are on Google

DENY ACCEPT

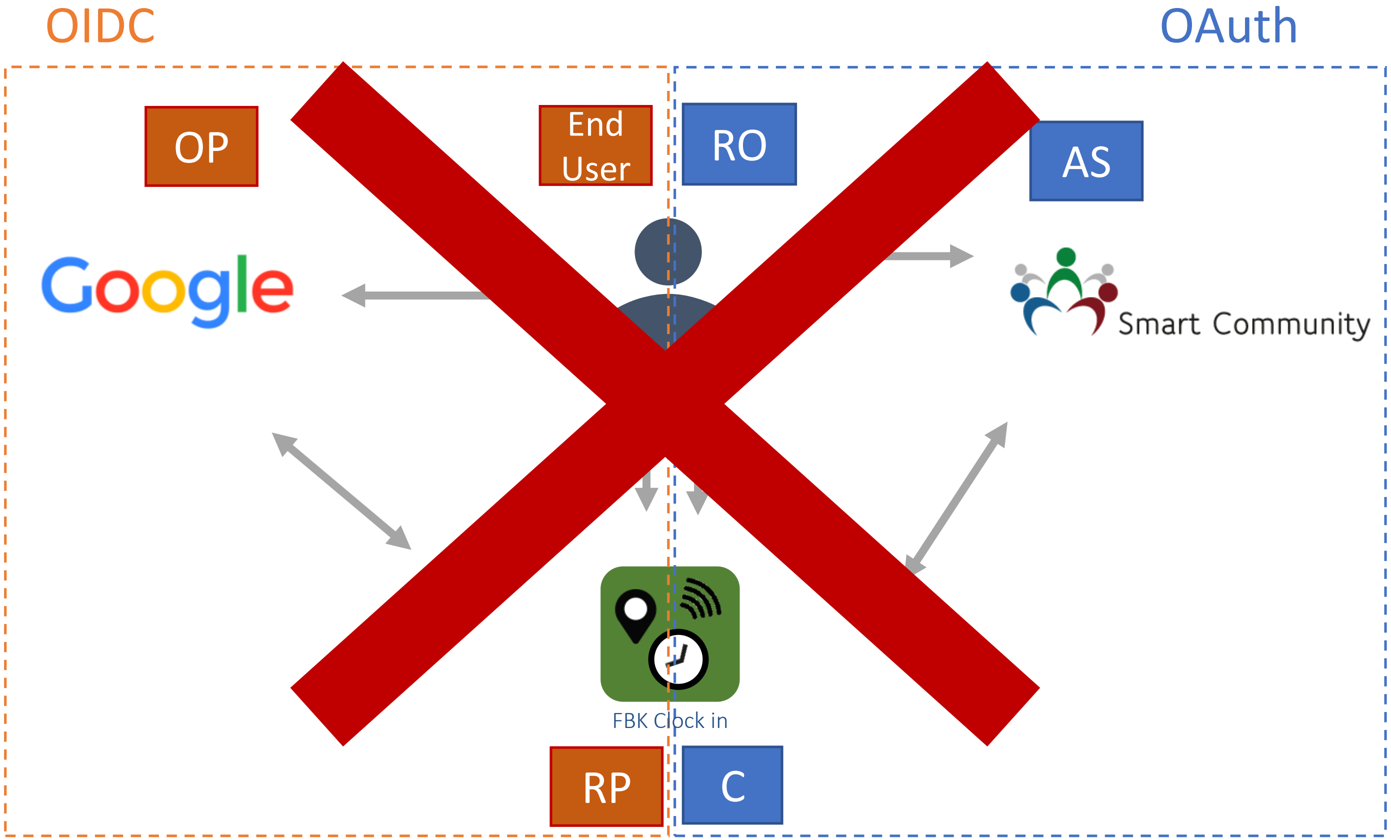
https://www.smartcommunity/consent

FBK Clock-in would like to:

- Read your clock-in info
- Manage your profile
- ....

DENY ACCEPT

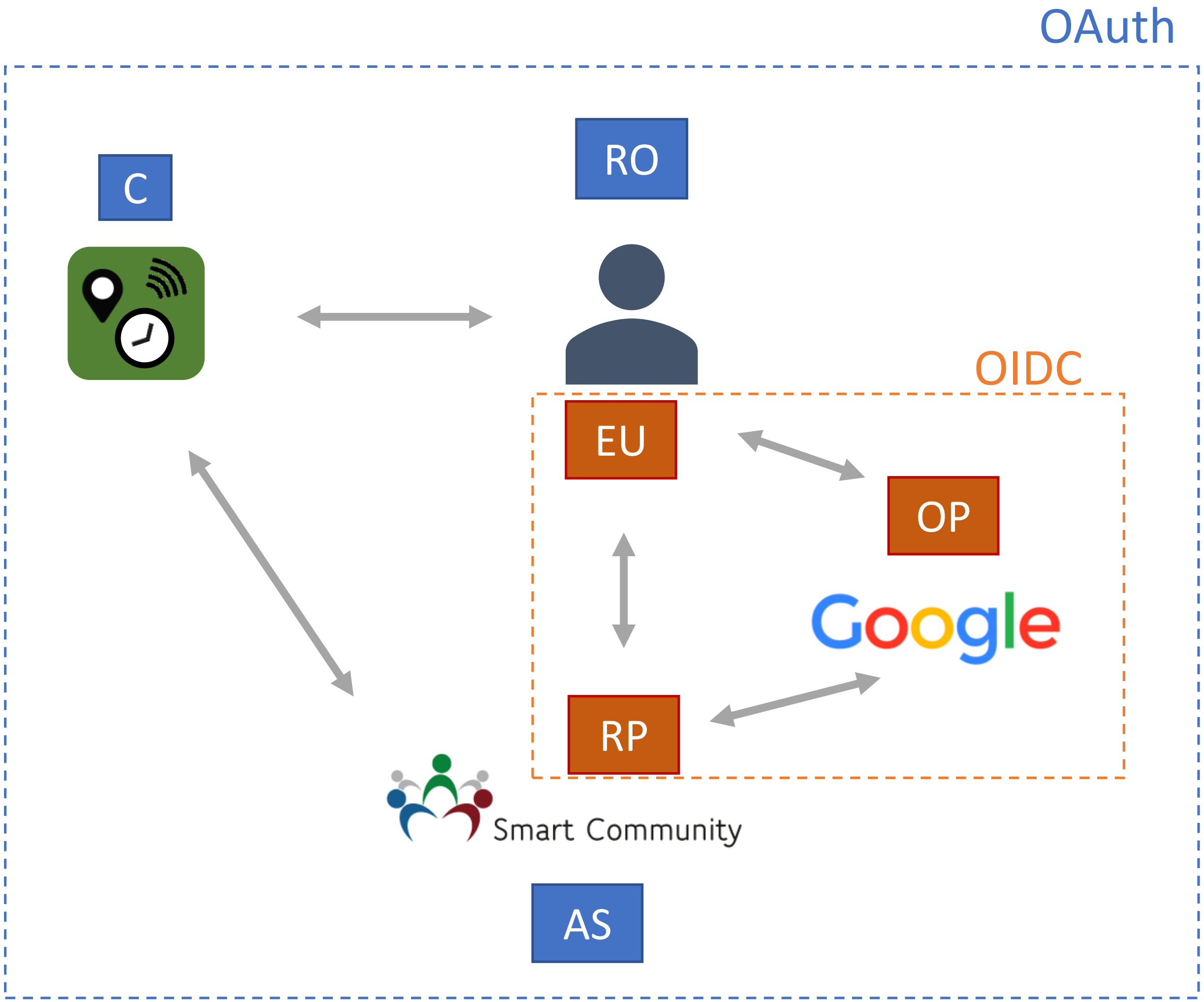
First OIDC and Then OAuth



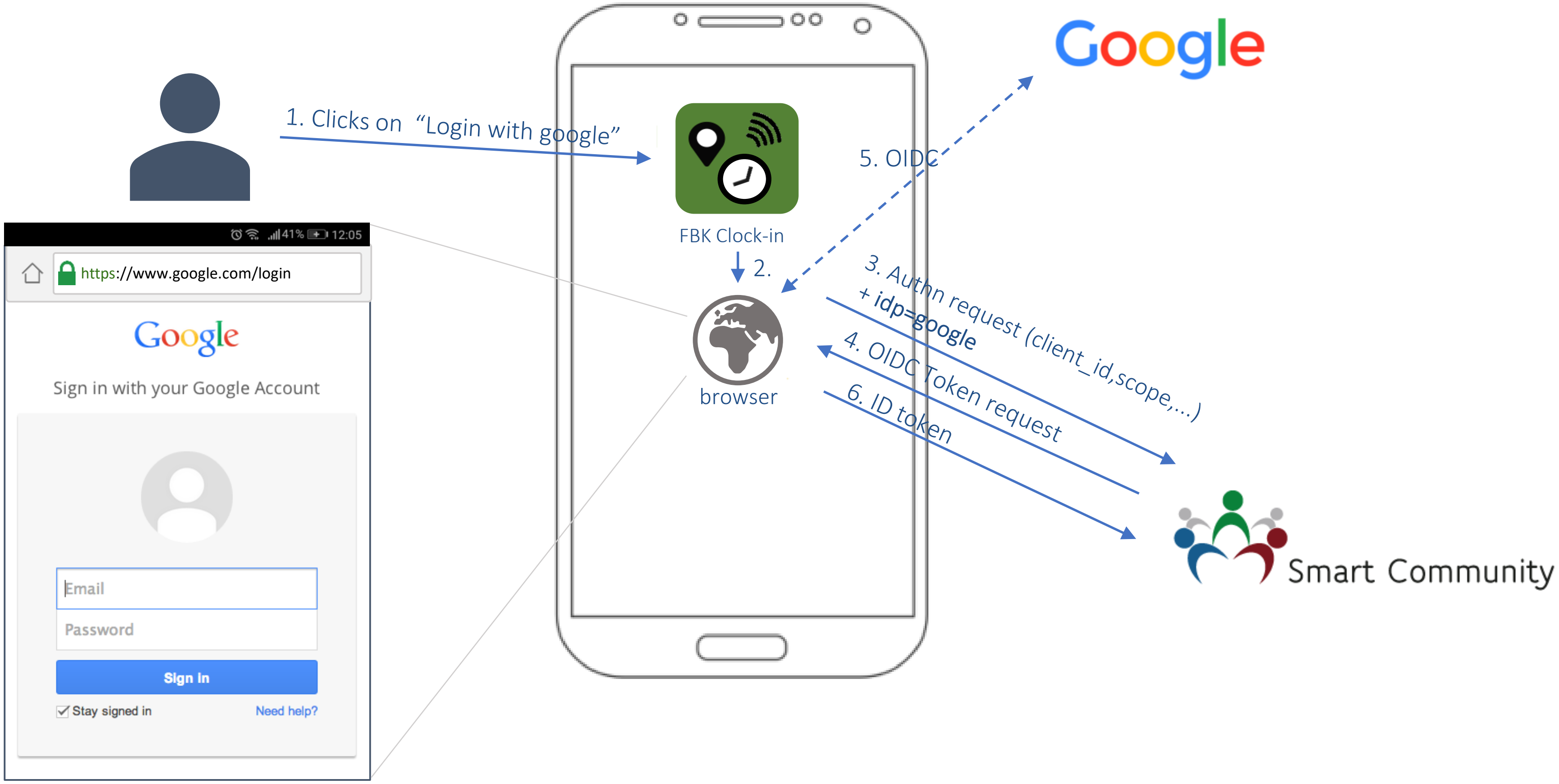
FBK app obtains Google ID token

FBK app obtains an access_token from SC exchanging ID token

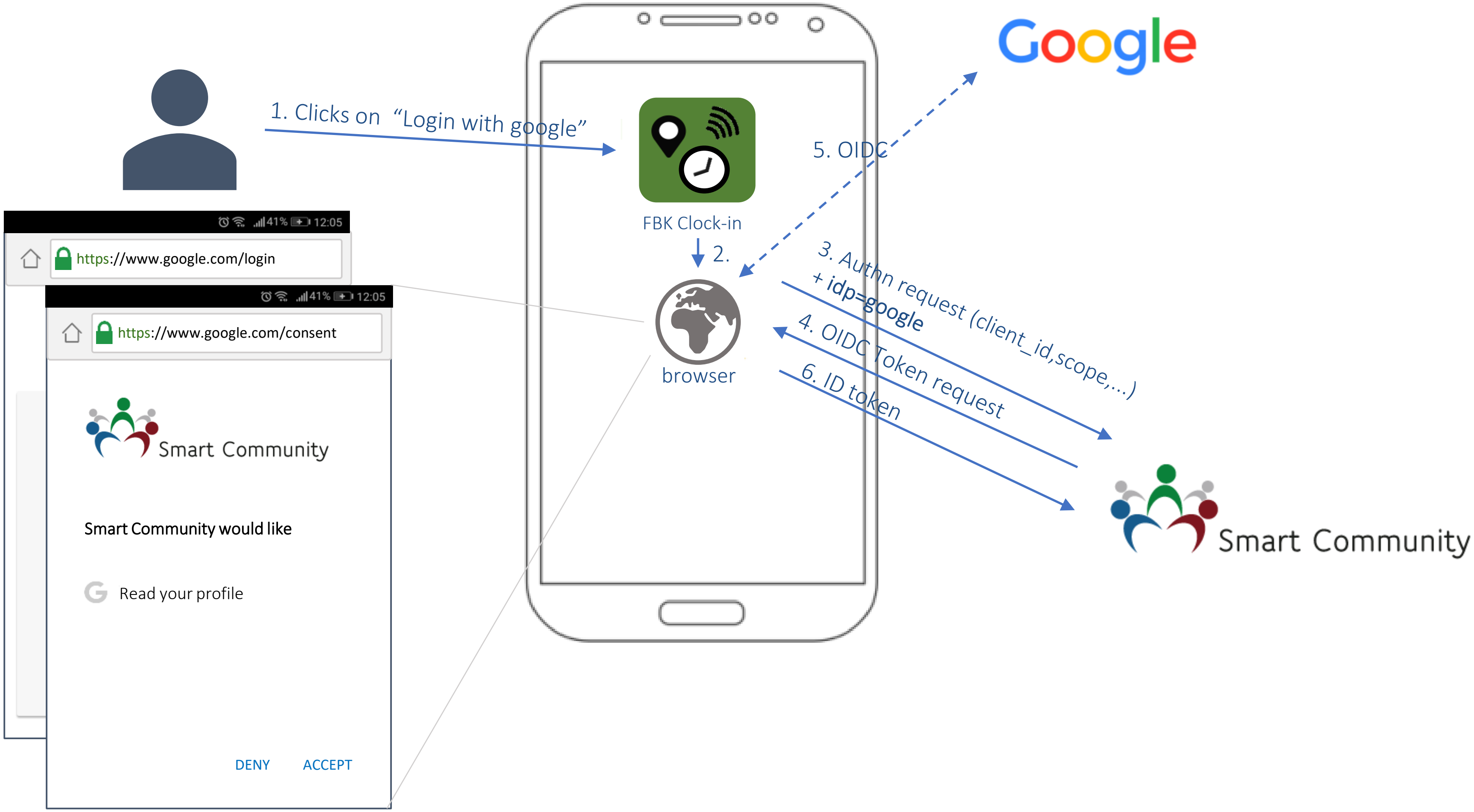
OIDC as Part of OAuth



OIDC as Part of OAuth



OIDC as Part of OAuth



https://www.google.com/login

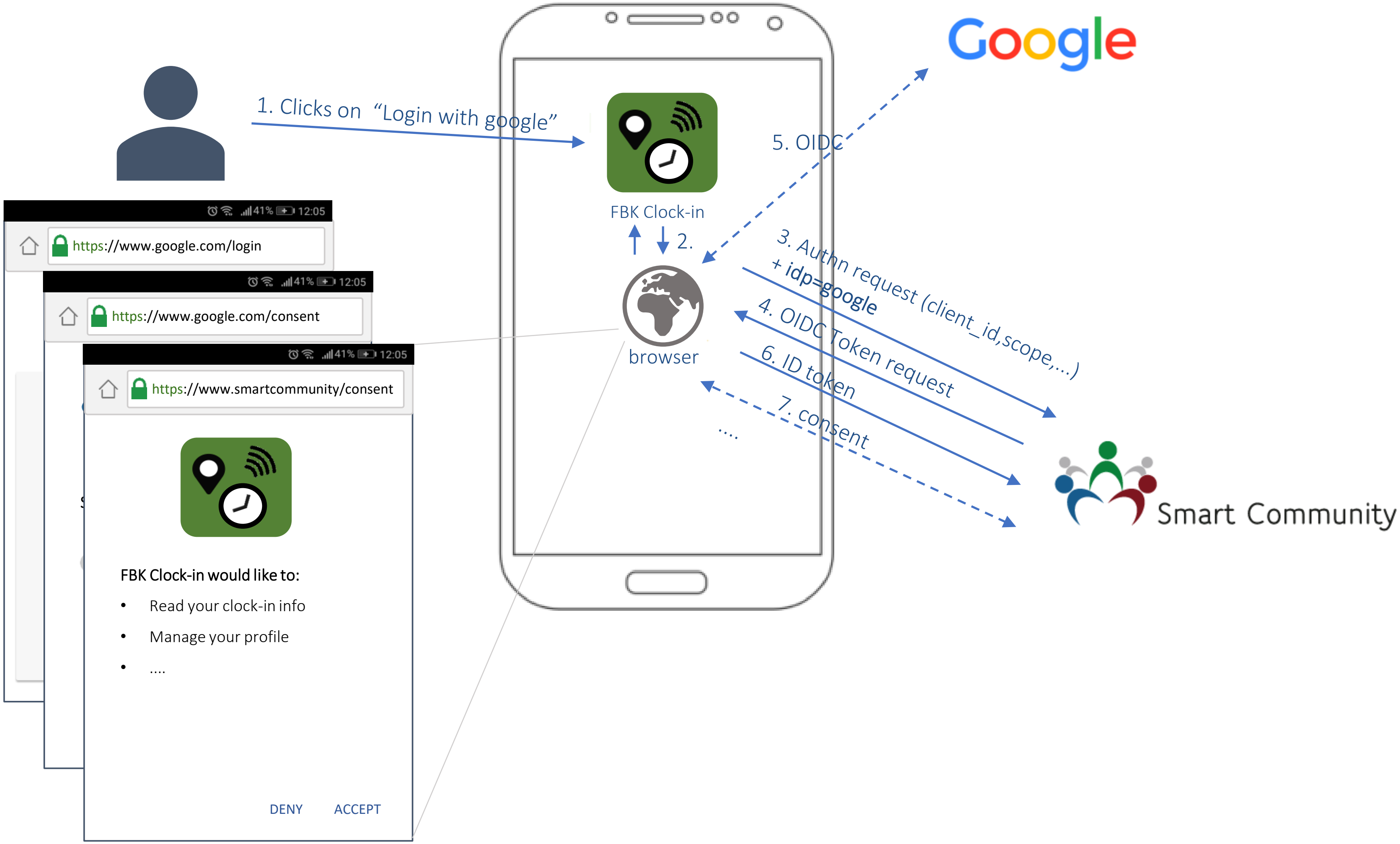
https://www.google.com/consent

Smart Community

Smart Community would like

Read your profile

OIDC as Part of OAuth



https://www.google.com/login

https://www.google.com/consent

https://www.smartcommunity/consent

FBK Clock-in would like to:

- Read your clock-in info
- Manage your profile
- ....

DENY ACCEPT

Lessons Learned and Discussion

- Native authentication (e.g., Google sign-in) is not suitable for open platforms where client apps are developed by third parties

- We need to use standard browser-based authentications

  + security, interoperability

  – usability

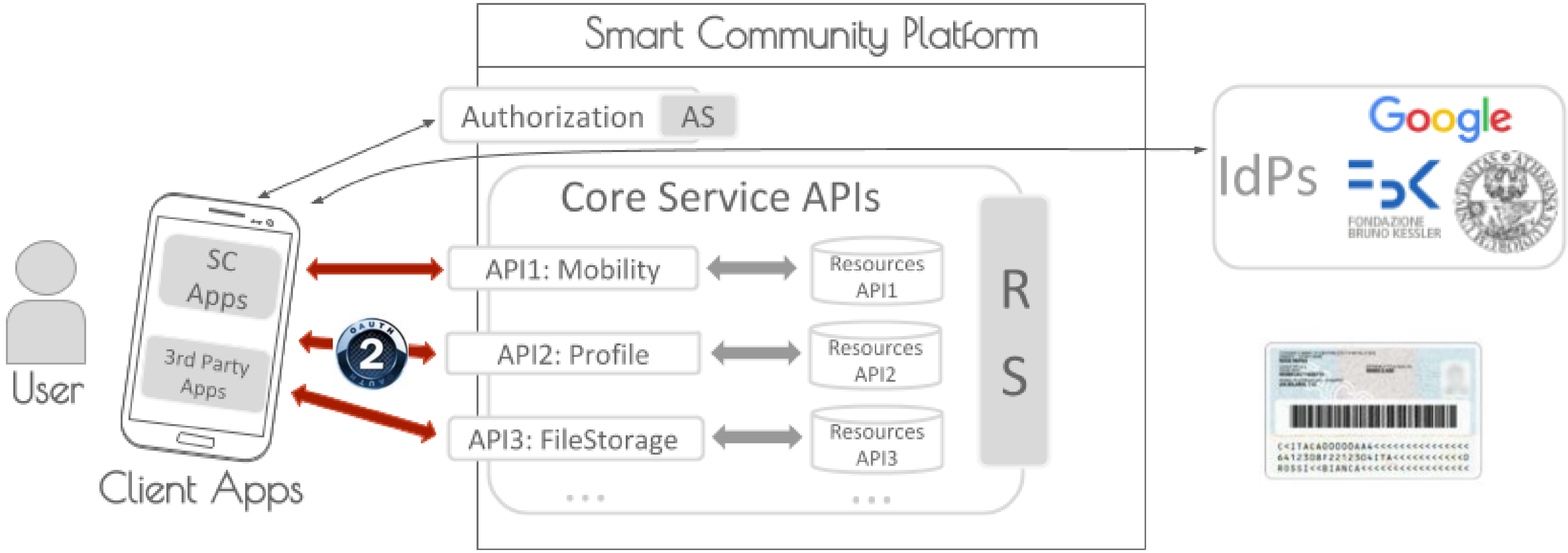
  (session cookie on the browser depends on the IdP and user)

feedback

questions

Smart Community: OAuth

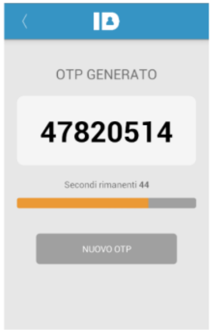
Design a delegation access solution for smart city apps to access data stored by Smart Community platform through APIs



- Smart Community AS does not manage authentication
→ use of external IdPs
- Some applications (mostly of the PA) require an high level of assurance on the identity proofing and authentication

Current Usability Problems

- Current PA solutions (e.g., ADC, SPID, ...) are not designed for mobile applications:
  - Use of desktop smartcard reader
  - Use of OTP generator app
  - Use of short session (requiring the user login at every access)



OTP GENERATO

47820514

Secondi rimanenti 44

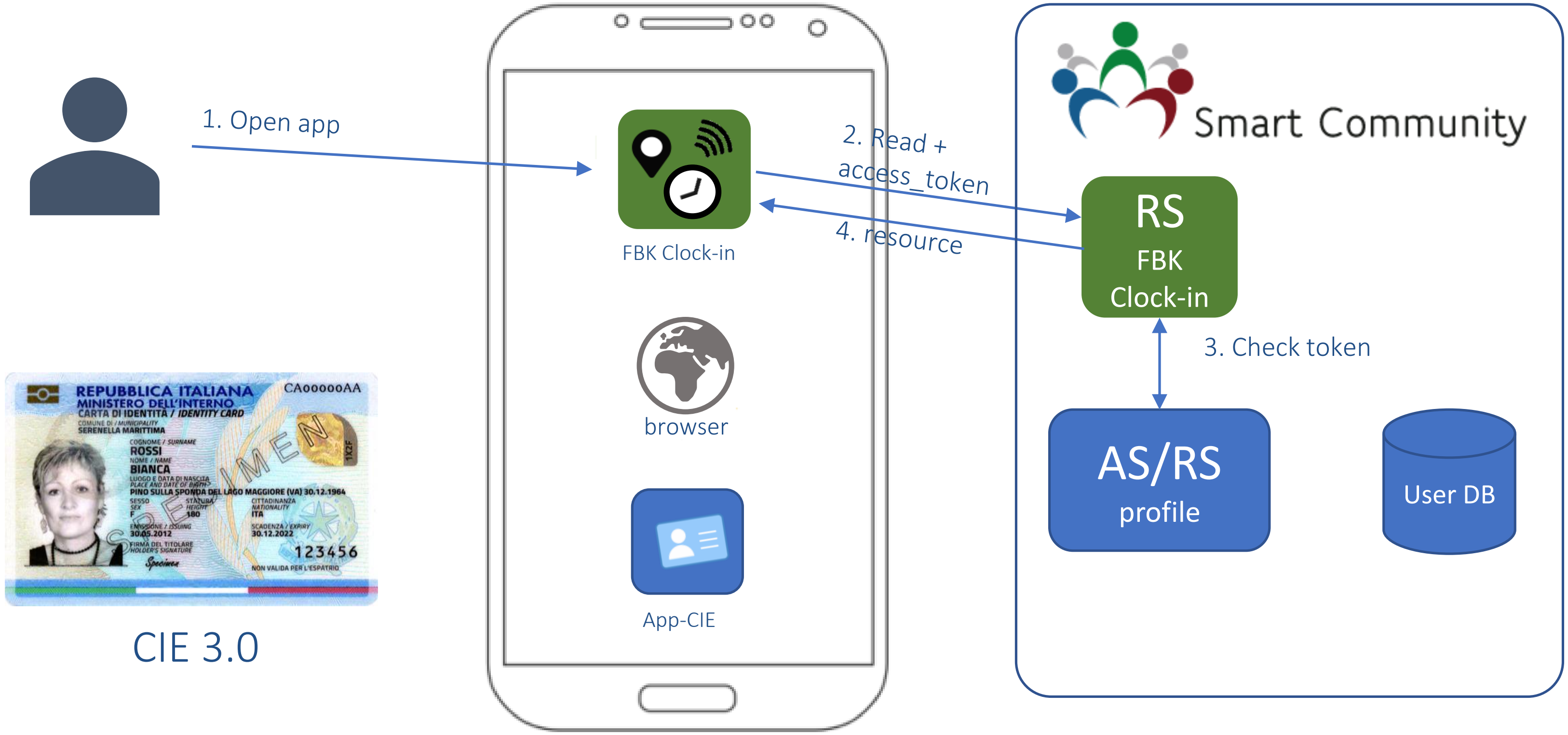
- Smart Community Requirements:
  - daily use → need to establish a longer user session
  - some apps require different authentication levels for different operations

? How do we combine SC OAuth for native apps with a second factor authentication in a usable way?

SC OAuth + 2nd Factor Authn

- To provide a second factor we are using the Italian Electronic Identity Card (CIE 3.0) that supports a contactless interface (NFC) for mobile use
- FBK Clock-in has a valid access_token with scope clock_in.read and sc.profile

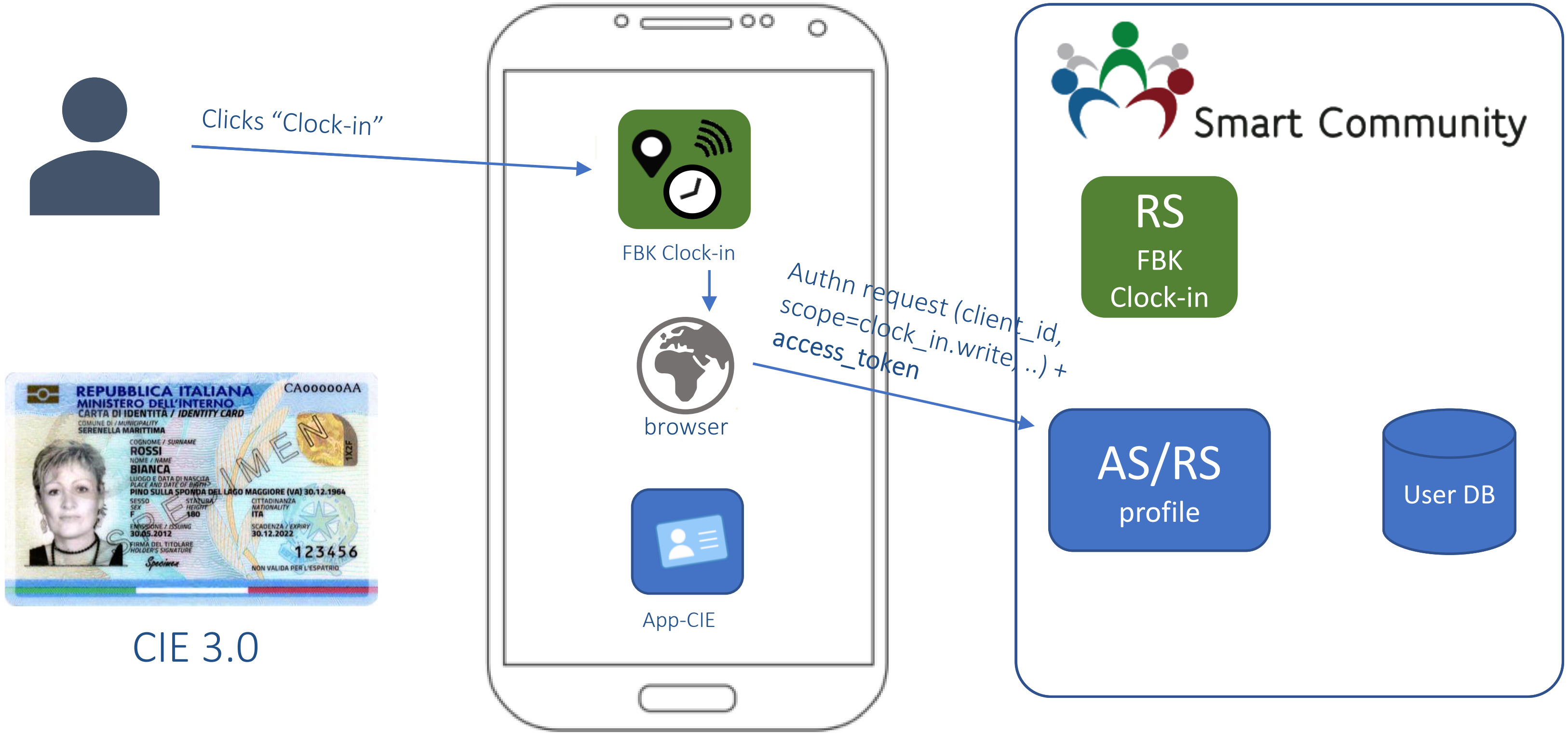
ISTITUTO POLIGRAFICO E ZECCA DELLO STATO



CIE 3.0

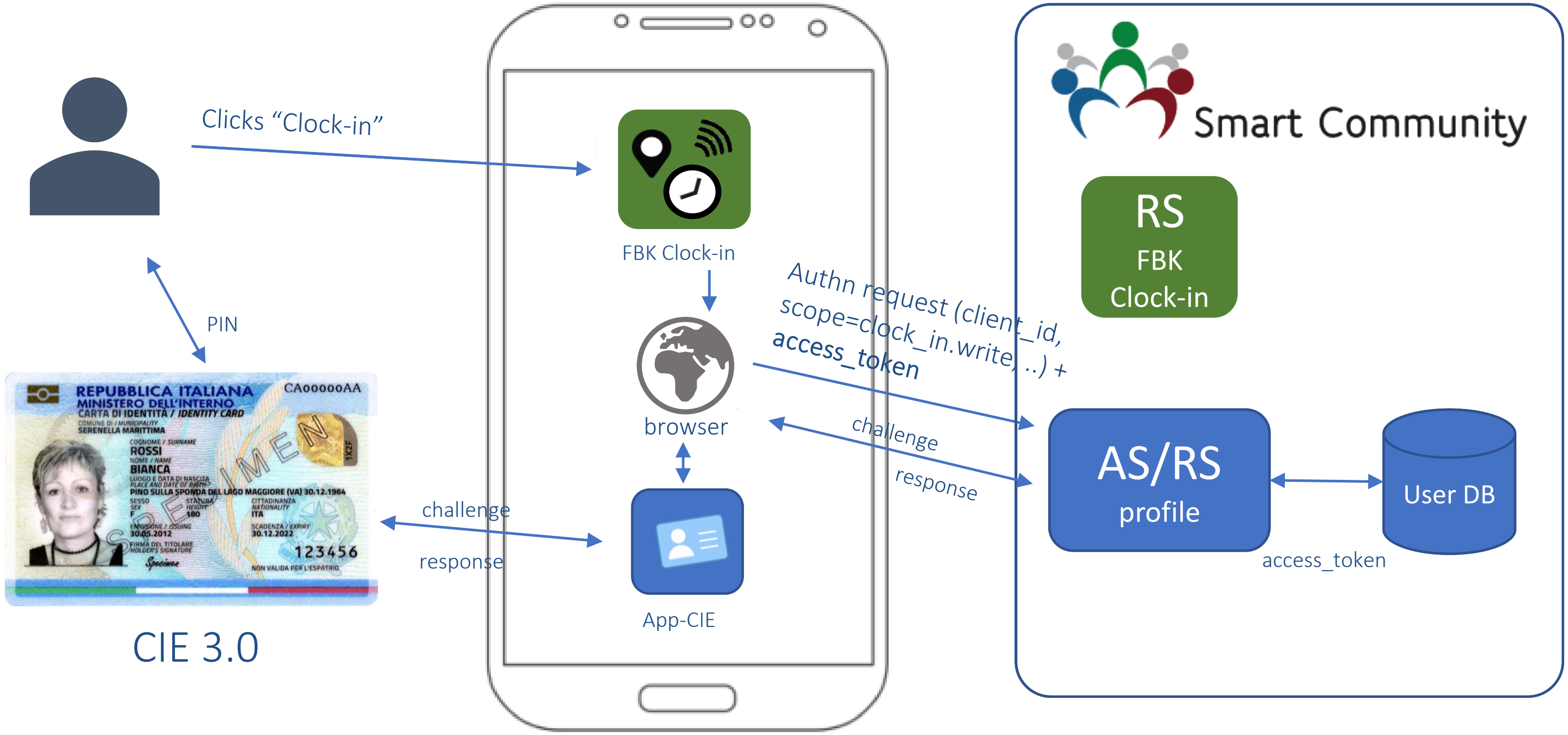
SC OAuth + 2nd Factor Authn

- To provide a second factor we are using the Italian Electronic Identity Card (CIE 3.0) that supports a contactless interface (NFC) for mobile use
- FBK Clock-in has a valid access_token with scope clock_in.read and sc.profile



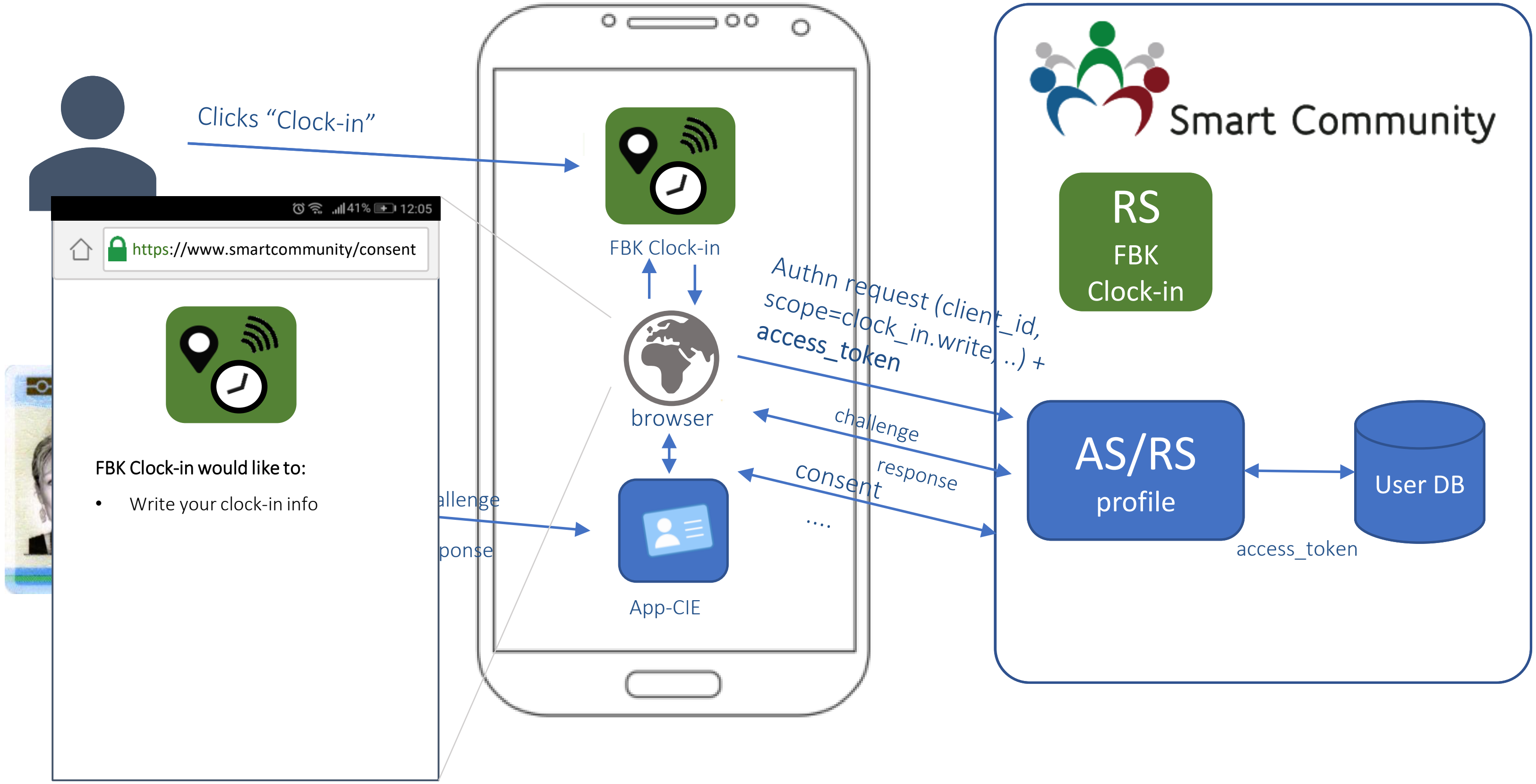
SC OAuth + 2nd Factor Authn

- To provide a second factor we are using the Italian Electronic Identity Card (CIE 3.0) that supports a contactless interface (NFC) for mobile use
- FBK Clock-in has a valid access_token with scope clock_in.read and sc.profile



SC OAuth + 2nd Factor Authn

- To provide a second factor we are using the Italian Electronic Identity Card (CIE 3.0) that supports a contactless interface (NFC) for mobile use
- FBK Clock-in has a valid access_token with scope clock_in.read and sc.profile



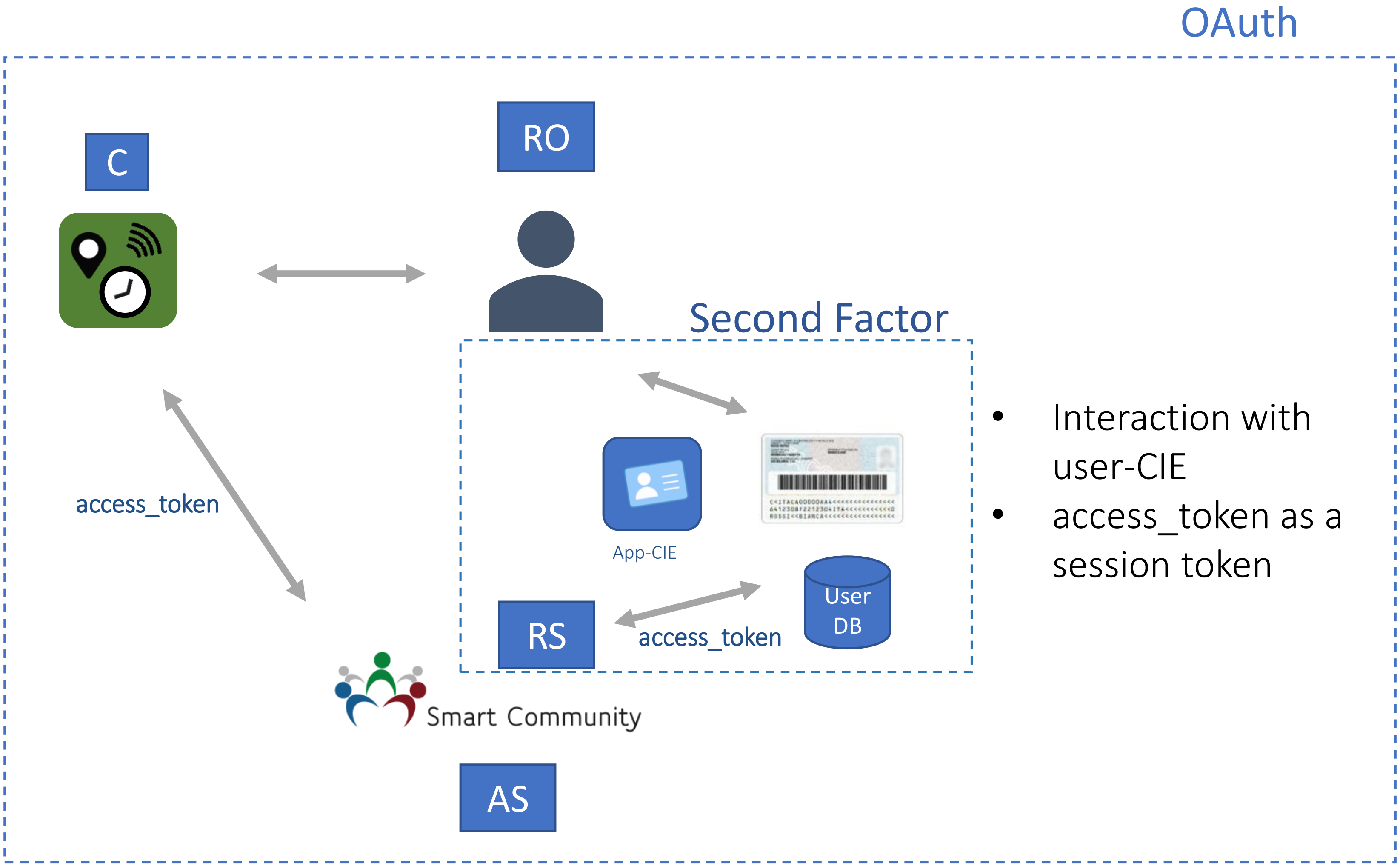
41% 12:05

https://www.smartcommunity/consent

FBK Clock-in would like to:

- Write your clock-in info

SC OAuth + 2nd Factor Authn



- Interaction with user-CIE
- access_token as a session token

Lessons Learned and Discussion

- PA apps require a high level of assurance on authentication and identity proofing
  → use of multi-factor authentication solution
  → use of strong identity (linked to real person)

  Google identity (self-asserted) + CIE identity = strong identity?

- We need to extend OAuth/OIDC for native apps to manage authentication session [especially with external IdPs]
  → Use an OAuth/OIDC token as session token to request another token

  [George Fletcher and Nat Sakimura. *Native SSO for Mobile Apps*]

feedback

questions