

WORK
SHOP
GARR
2024

NET
MAKERS

Security-by-design e Identità Digitale: da Entra con CIE/SPID al Digital Wallet

Giada Sciarretta

Fondazione Bruno Kessler

Per le domande:

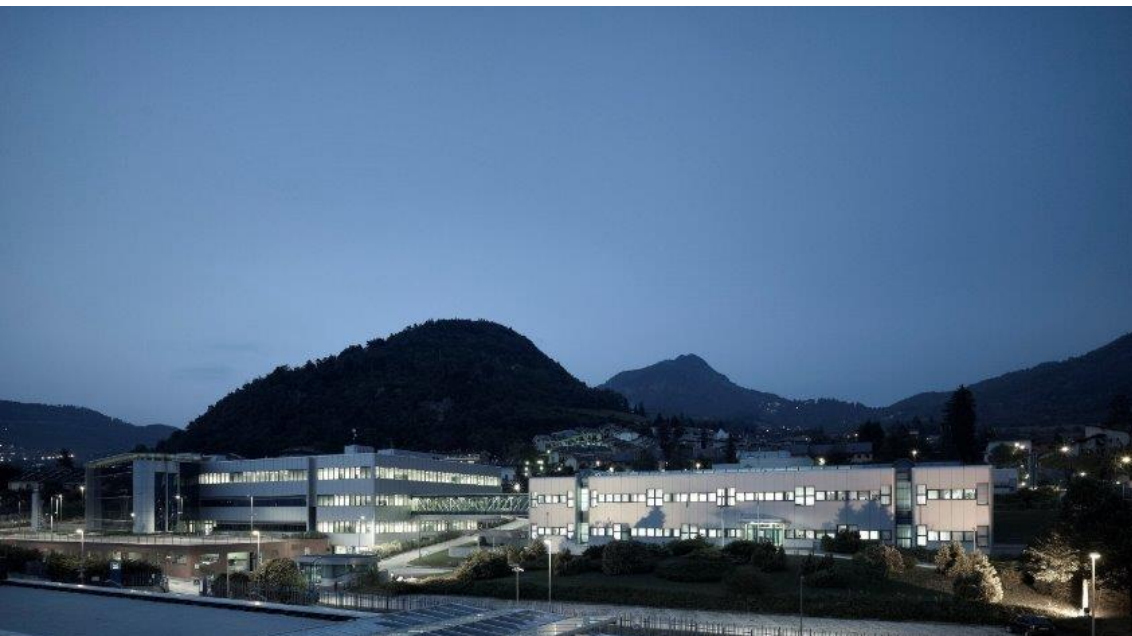


wooclap.com e
codice WSGARR24

Who we are

Fondazione Bruno Kessler (FBK)

- Research and Innovation institute in Trento, Italy
- 12 research centers: from technology to humanities and social sciences



FBK at a glance

450+

researchers

136

PhD students from 25 different
Countries

200+

thesis students, visiting professor,
visitors

700+

students involved in the FBK activities

4.645 sq m

labs for scientific research

230.000

and more titles in a special library

Center for Cybersecurity Fondazione Bruno Kessler (FBK)



Digital Identity



Applied Cryptography



Threat and Anomaly
Detection



Center for Cybersecurity Digital Identity



OpenID Connect Specification

iGOV and OIDC Federation profiles



Activities in the context of EUDIW

PID Issuance, Trust model, Threat Model, Revocation



OpenID Connect Specification

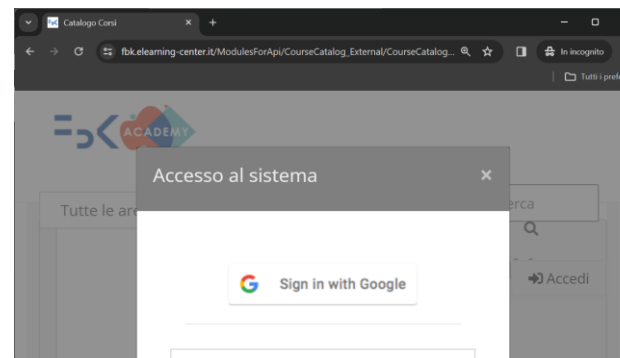
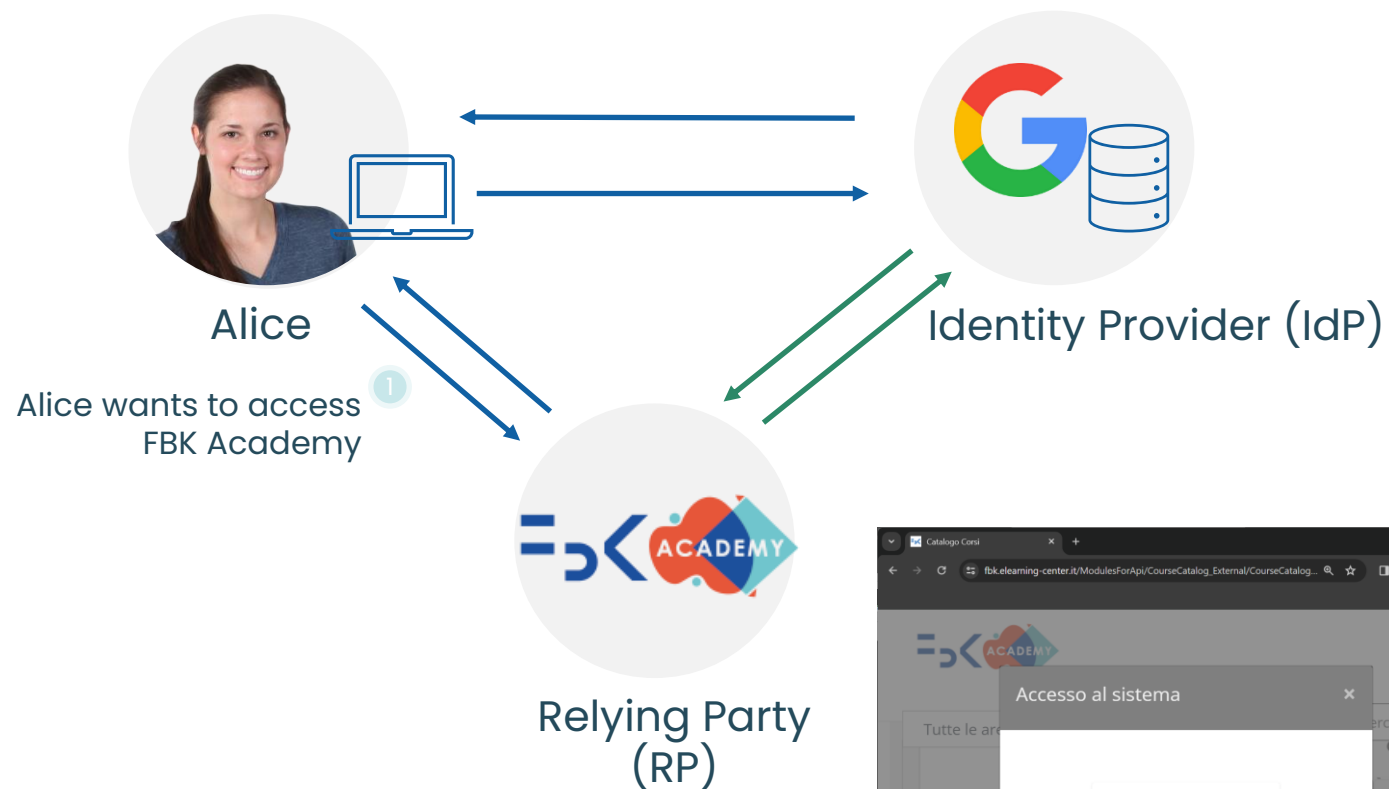
iGOV and OIDC Federation profiles



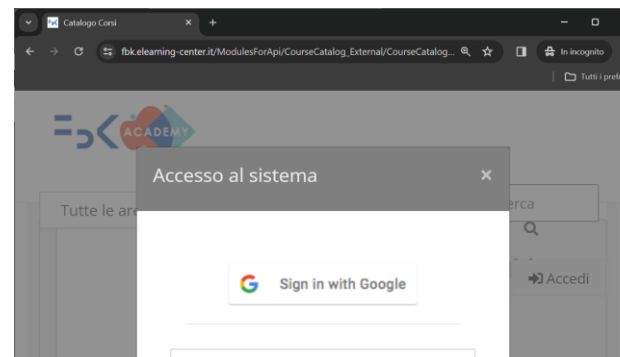
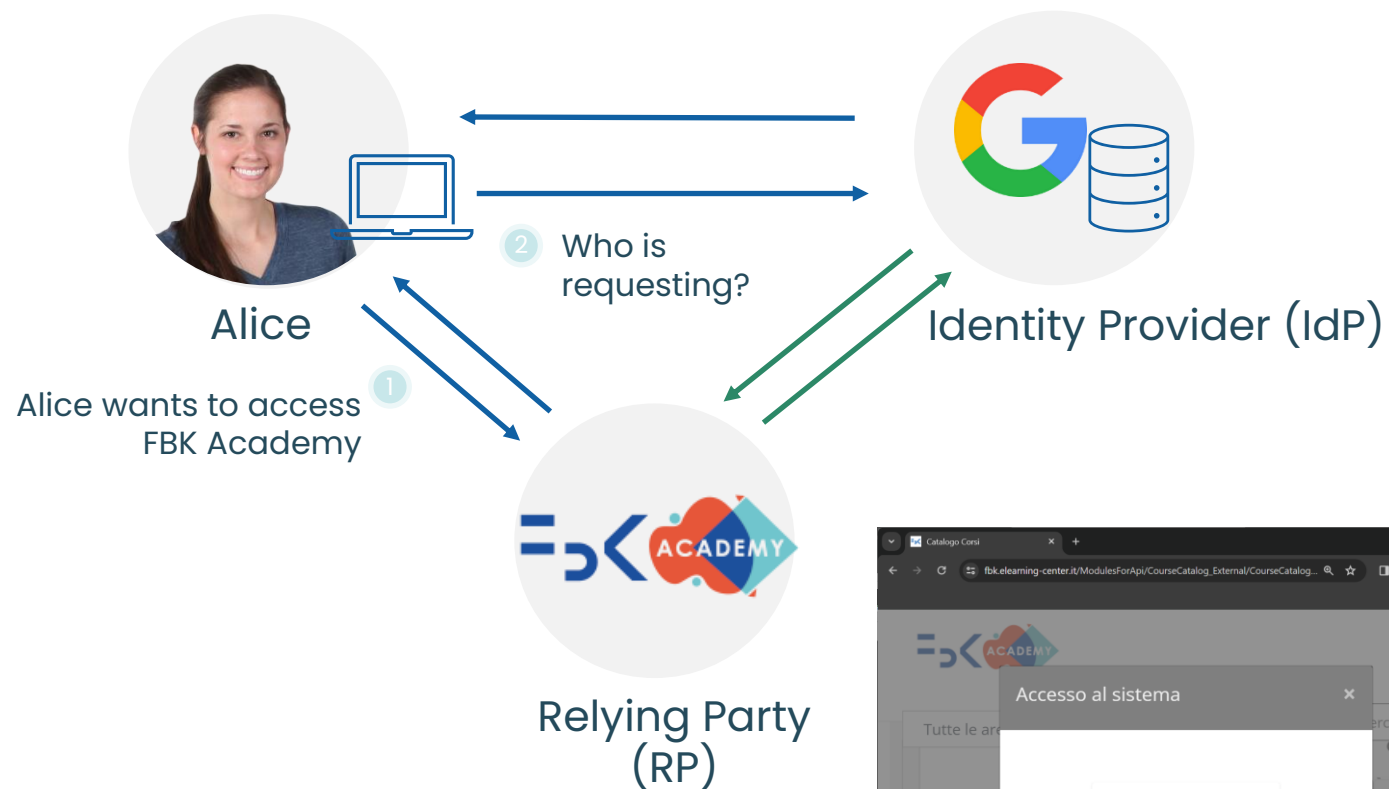
Activities in the context of EUDIW

PID Issuance, Trust model, Threat Model, Revocation

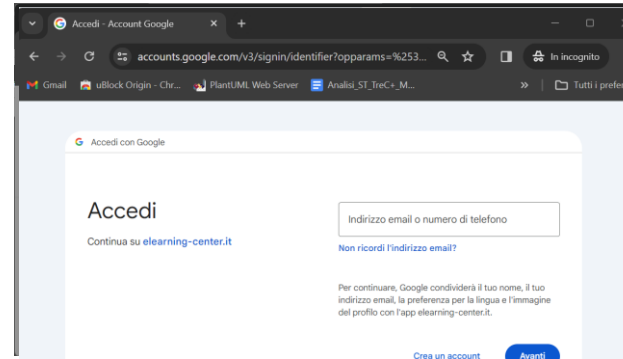
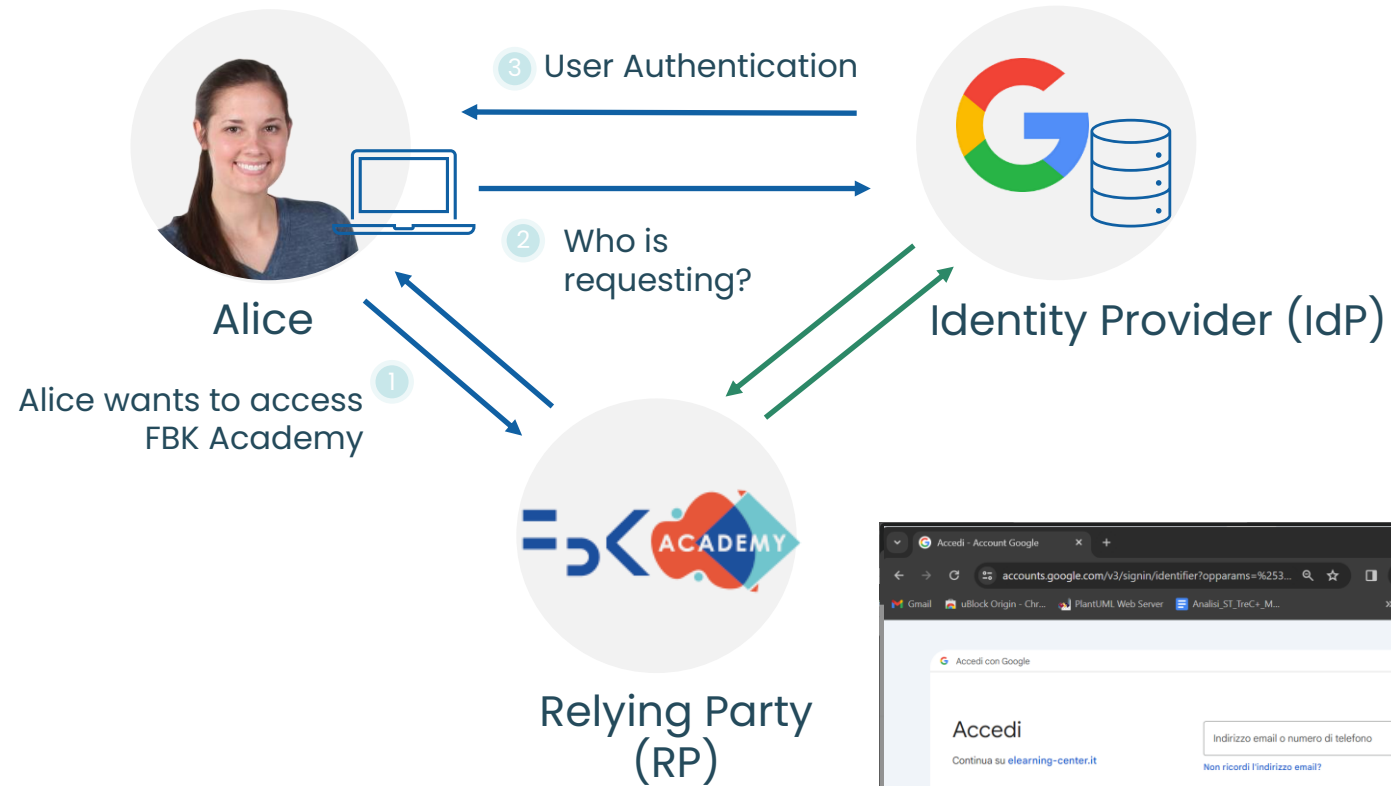
OpenID Connect High Level Flow



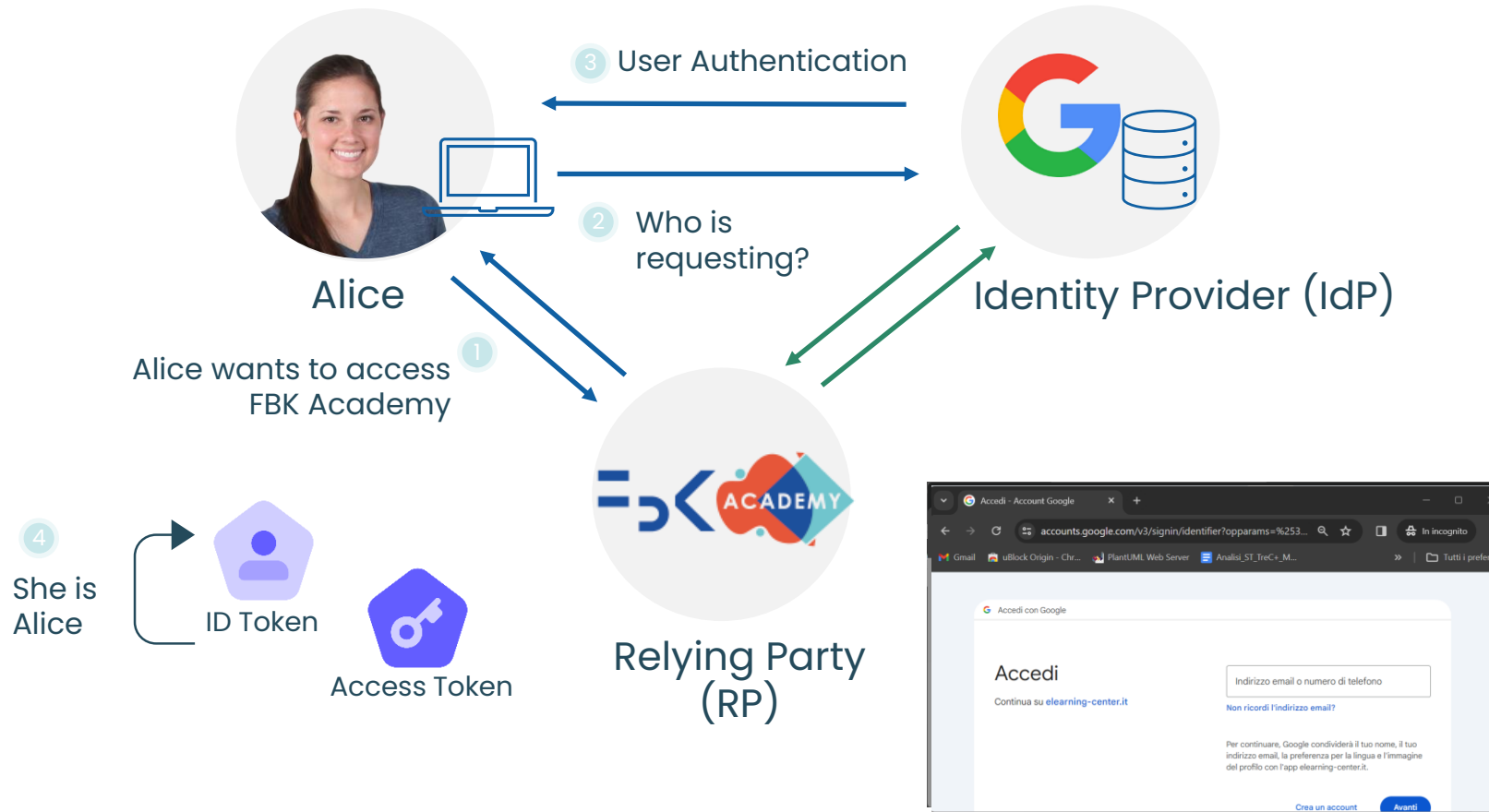
OpenID Connect High Level Flow



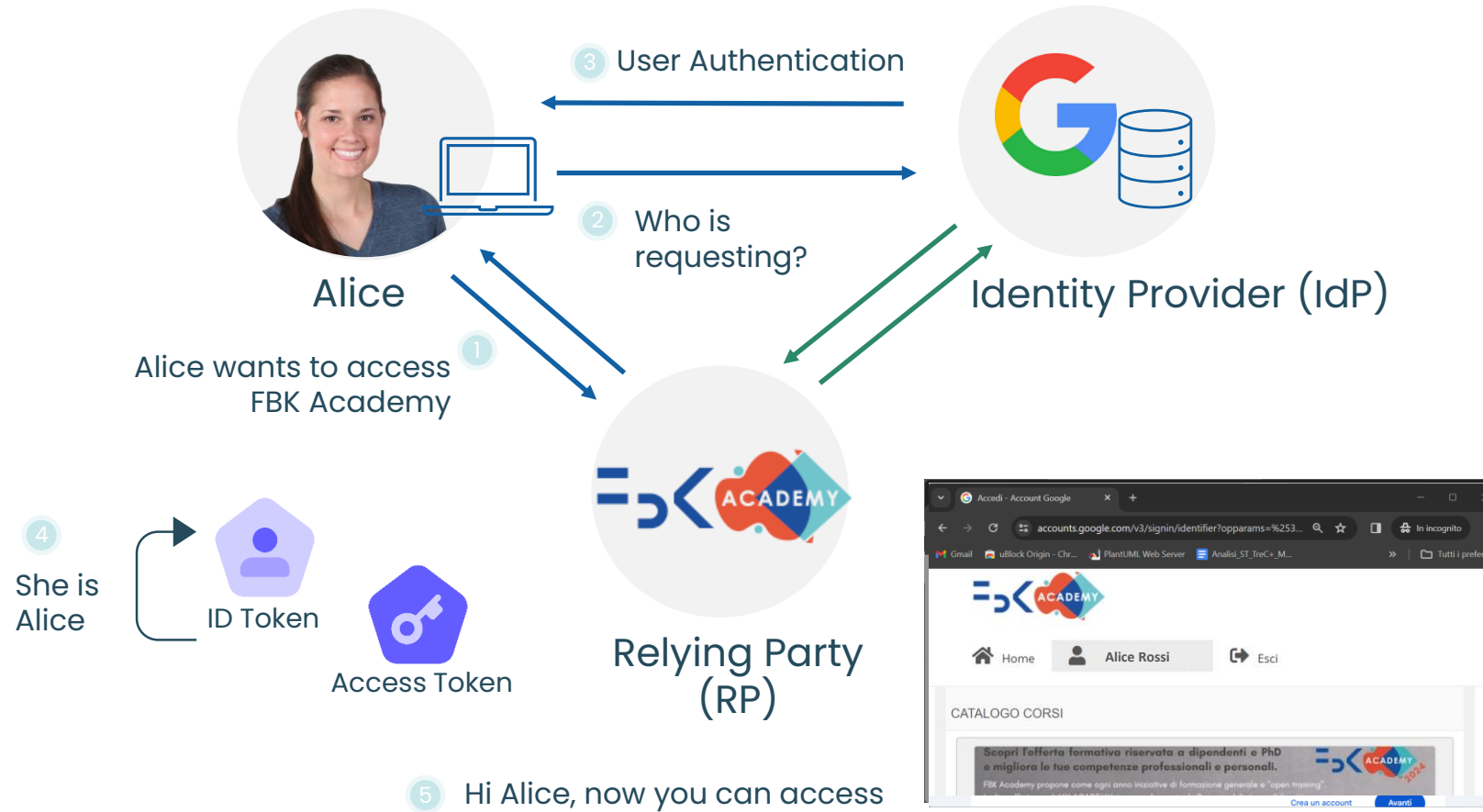
OpenID Connect High Level Flow



OpenID Connect High Level Flow



OpenID Connect High Level Flow



Italian eIDAS notified eID schemes

SPID and CIE

2 eID schemes:



SPID, Public Digital Identity System
(handled by AgID)



CIE id, based on
(owned by Ministry of Interior, handled by IPZS)



Amir Sharif, Matteo Ranzi, Roberto Carbone, Giada Sciarretta, Silvio Ranise. **SoK: A Survey on Technological Trends for (pre)Notified eIDAS Electronic Identity Schemes.** In: 17th International Workshop on Frontiers in Availability, Reliability and Security (FARES2022).

Italian eIDAS notified eID schemes

SPID and CIE

2 eID schemes:



SPID, Public Digital Identity System
(handled by AgID)



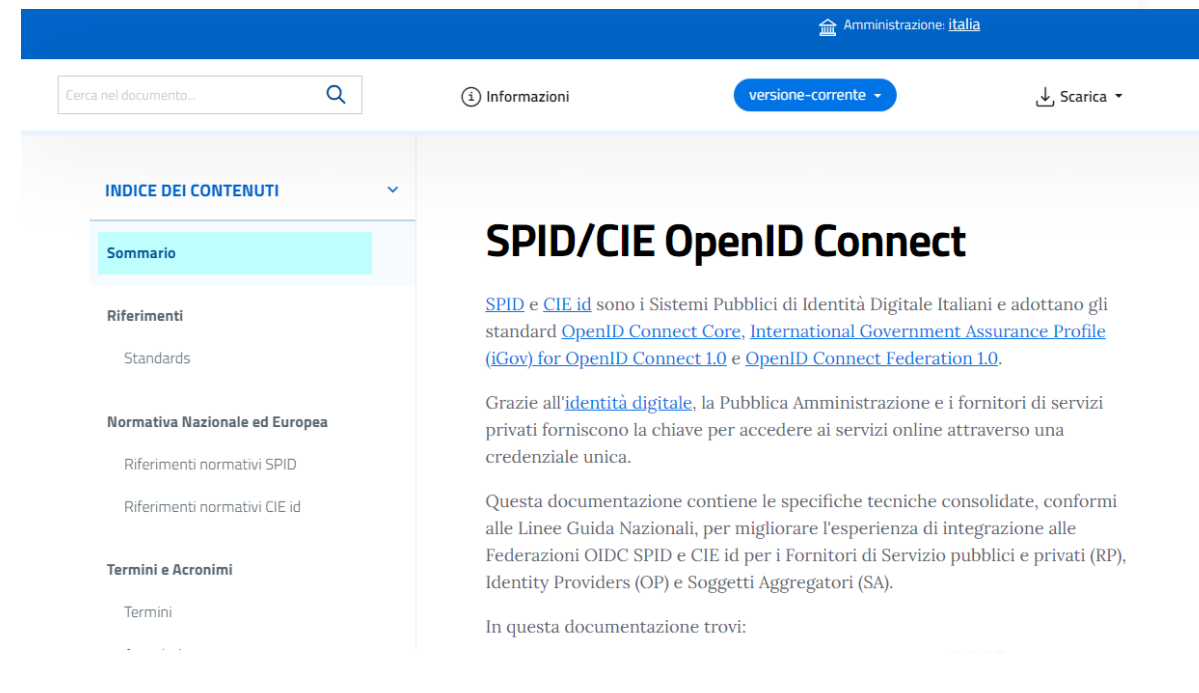
CIE id, based on
(owned by Ministry of Interior, handled by IPZS)



From SAML 2.0 to OpenID Connect



<https://docs.italia.it/italia/spid/spid-cie-oidc-docs>



The screenshot shows the documentation page for SPID/CIE OpenID Connect. The page title is "SPID/CIE OpenID Connect". The main content area contains the following text: "SPID e CIE id sono i Sistemi Pubblici di Identità Digitale Italiani e adottano gli standard OpenID Connect Core, International Government Assurance Profile (iGov) for OpenID Connect 1.0 e OpenID Connect Federation 1.0." Below this, it states: "Grazie all'identità digitale, la Pubblica Amministrazione e i fornitori di servizi privati forniscono la chiave per accedere ai servizi online attraverso una credenziale unica." Further down, it says: "Questa documentazione contiene le specifiche tecniche consolidate, conformi alle Linee Guida Nazionali, per migliorare l'esperienza di integrazione alle Federazioni OIDC SPID e CIE id per i Fornitori di Servizio pubblici e privati (RP), Identity Providers (OP) e Soggetti Aggregatori (SA)." At the bottom, it says: "In questa documentazione trovi:"



Amir Sharif, Matteo Ranzi, Roberto Carbone, Giada Sciarretta, Silvio Ranise. **SoK: A Survey on Technological Trends for (pre)Notified eIDAS Electronic Identity Schemes.** In: 17th International Workshop on Frontiers in Availability, Reliability and Security (FARES2022).

OpenID Connect in Italy

Challenges and motivation



OpenID Connect in Italy

Challenges and motivation



The OAuth 2.0 Authorization Framework
RFC 6749

JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens

[RFC 9068](#)

JSON Web Token Best Current Practices

[RFC 8725](#)

Best Current Practice

Resource Indicators for OAuth 2.0

[RFC 8707](#)

OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

[RFC 8705](#)

OAuth 2.0 Token Exchange

[RFC 8693](#)

OAuth 2.0 Device Authorization Grant

[RFC 8628](#)

OAuth 2.0 Authorization Server Metadata

[RFC 8414](#)

OAuth 2.0 for Native Apps

[RFC 8252](#)

Best Current Practice

Authentication Method Reference Values

[RFC 8176](#)

Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)

[RFC 7800](#)

OAuth 2.0 Token Introspection

[RFC 7662](#)

Proof Key for Code Exchange by OAuth Public Clients

[RFC 7636](#)

OAuth 2.0 Dynamic Client Registration Management Protocol

[RFC 7592](#)

Experimental

OAuth 2.0 Dynamic Client Registration Protocol

[RFC 7591](#)

JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants

[RFC 7523](#)

Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants

[RFC 7522](#)

Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants

[RFC 7521](#)

JSON Web Token (JWT)

[RFC 7519](#)

OAuth 2.0 Token Revocation

[RFC 7009](#)

OAuth 2.0 Threat Model and Security Considerations

[RFC 6819](#)

Informational

An IETF URN Sub-Namespace for OAuth

[RFC 6755](#)

Informational

The OAuth 2.0 Authorization Framework: Bearer Token Usage

[RFC 6750](#)

The OAuth 2.0 Authorization Framework

[RFC 6749](#)

JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens

[RFC 9068](#)

JSON Web Token Best Current Practices

[RFC 8725](#)

Best Current Practice

Resource Indicators for OAuth 2.0

[RFC 8707](#)

OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

[RFC 8705](#)

OAuth 2.0 Token Exchange

[RFC 8693](#)

OAuth 2.0 Device Authorization Grant

[RFC 8628](#)

OAuth 2.0 Authorization Server Metadata

[RFC 8414](#)

OAuth 2.0 for Native Apps

[RFC 8252](#)

Best Current Practice

Authentication Method Reference Values

[RFC 8176](#)

Proof-of-Possession Key Semantics for JSON Web

[RFC 7800](#)

OAuth 2.0 Token Introspection

[RFC 7662](#)

Proof Key for Code Exchange by OAuth Public Cli

[RFC 7636](#)

OAuth 2.0 Dynamic Client Registration Management Protocol

[RFC 7592](#)

Experimental

OAuth 2.0 Dynamic Client Registration Protocol

[RFC 7591](#)

JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants

[RFC 7523](#)

Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and

RFCs

OAuth 2.0 Step Up Authentication Challenge Protocol

[RFC 9470](#)

OAuth 2.0 Demonstrating Proof of Possession (DPoP)

[RFC 9449](#)

OAuth 2.0 Rich Authorization Requests

[RFC 9396](#)

JWK Thumbprint URI

[RFC 9278](#)

OAuth 2.0 Authorization Server Issuer Identification

[RFC 9207](#)

OAuth 2.0 Pushed Authorization Requests

[RFC 9126](#)

The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)

[RFC 9101](#)

Authentication and Authorization Grants

derations

earer Token Usage

JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens

[RFC 9068](#)

JSON Web Token Best Current Practices

[RFC 8725](#)

Best Current Practice

Resource Indicators for OAuth 2.0

[RFC 8707](#)

OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

[RFC 8705](#)

OAuth 2.0 Token Exchange

[RFC 8693](#)

OAuth 2.0 Device Authorization Grant

[RFC 8628](#)

OAuth 2.0 Authorization Server Metadata

[RFC 8414](#)

OAuth 2.0 for Native Apps

[RFC 8252](#)

Best Current Practice

Authentication Method Reference Values

[RFC 8176](#)

Proof-of-Possession Key Semantics for JSON Web

[RFC 7800](#)

OAuth 2.0 Token Introspection

[RFC 7662](#)

Proof Key for Code Exchange by OAuth Public Cli

[RFC 7636](#)

OAuth 2.0 Dynamic Client Registration Management Protocol

[RFC 7592](#)

Experimental

OAuth 2.0 Dynamic Client Registration Protocol

[RFC 7591](#)

RFCs

OAuth 2.0 Step Up Authentication Challenge

[RFC 9470](#)

OAuth 2.0 Demonstrating Proof of Possession

[RFC 9449](#)

OAuth 2.0 Rich Authorization Requests

[RFC 9396](#)

JWK Thumbprint URI

[RFC 9278](#)

OAuth 2.0 Authorization Server Issuer Ident

[RFC 9207](#)

OAuth 2.0 Pushed Authorization Requests

[RFC 9126](#)

The OAuth 2.0 Authorization Framework: JW

[RFC 9101](#)

Active Individual Drafts

Identity Assertion Authorization Grant

[draft-parecki-oauth-identity-assertion-authz-grant](#)

2024-10-20

OAuth Profile for Open Public Clients

[draft-jenkins-oauth-public](#)

2024-10-15

Global Token Revocation

[draft-parecki-oauth-global-token-revocation-01](#)

2024-09-22

OAuth 2.0 for First-Party Applications

[draft-parecki-oauth-first-party-apps-00](#)

2024-07-08

Proof of Issuer Key Authority (PIKA)

[draft-barnes-oauth-pika](#)

2024-07-08

OAuth Client ID Metadata Document

[draft-parecki-oauth-client-id-metadata-document](#)

2024-07-08

AuthZEN Request/Response Profile for OAuth 2.0 Rich Authorization Requests

[draft-brossard-oauth-rar-authzen](#)

2024-07-08

OAuth Status Assertions

[draft-demarco-oauth-status-assertions](#)

2024-06-18

OAuth 2.0 Delegated B2B Authorization

[draft-janicijevic-oauth-b2b-authorization](#)

2024-05-13

Active Drafts

OAuth 2.0 Attestation-Based Client Authentication draft-ietf-oauth-attestation-based-client-auth-01	2024-10-21
Token Status List draft-ietf-oauth-status-list-00	2024-10-21
OAuth 2.0 for Browser-Based Applications draft-ietf-oauth-browser-based-apps-15	2024-10-20
Selective Disclosure for JWTs (SD-JWT) draft-ietf-oauth-selective-disclosure-jwt-07	2024-10-18
OAuth 2.0 Protected Resource Metadata draft-ietf-oauth-resource-metadata-01 RFC Ed Queue	2024-10-15
OAuth 2.0 for First-Party Applications draft-ietf-oauth-first-party-apps	2024-10-08
SD-JWT-based Verifiable Credentials (SD-JWT VC) draft-ietf-oauth-sd-jwt-vc-01	2024-09-18
Cross-Device Flows: Security Best Current Practice draft-ietf-oauth-cross-device-security-04	2024-07-08
OAuth Identity and Authorization Chaining Across Domains draft-ietf-oauth-identity-chaining	2024-07-08
Transaction Tokens draft-ietf-oauth-transaction-tokens-00	2024-07-04
OAuth 2.0 Security Best Current Practice draft-ietf-oauth-security-topics-24 RFC Ed Queue	2024-06-03
The OAuth 2.1 Authorization Framework draft-ietf-oauth-v2-1-09	2024-05-15
JWT Response for OAuth Token Introspection draft-ietf-oauth-jwt-introspection-response RFC Ed Queue	2021-09-04

OAuth 2.0 Dynamic Client Registration Management Protocol

[RFC 7592](#)

Experimental

OAuth 2.0 Dynamic Client Registration Protocol

[RFC 7591](#)

Active Individual Drafts

Identity Assertion Authorization Grant draft-parecki-oauth-identity-assertion-authz-grant	2024-10-20
OAuth Profile for Open Public Clients draft-jenkins-oauth-public	2024-10-15
Global Token Revocation draft-parecki-oauth-global-token-revocation-01	2024-09-22
OAuth 2.0 for First-Party Applications draft-parecki-oauth-first-party-apps-00	2024-07-08
Proof of Issuer Key Authority (PIKA) draft-barnes-oauth-pika	2024-07-08
OAuth Client ID Metadata Document draft-parecki-oauth-client-id-metadata-document	2024-07-08
AuthZEN Request/Response Profile for OAuth 2.0 Rich Authorization Requests draft-brossard-oauth-rar-authzen	2024-07-08
OAuth Status Assertions draft-demarco-oauth-status-assertions	2024-06-18
OAuth 2.0 Delegated B2B Authorization draft-janicijevic-oauth-b2b-authorization	2024-05-13

OpenID Connect in Italy

Challenges and Motivation

Final Specifications

- [OpenID Connect Core](#) – Defines the core OpenID Connect functionality: authentication built on top of OAuth 2.0 and the use of claims to communicate information about the End-User
- [OpenID Connect Discovery](#) – Defines how clients dynamically discover information about OpenID Providers
- [OpenID Connect Dynamic Registration](#) – Defines how clients dynamically register with OpenID Providers
- [OAuth 2.0 Multiple Response Types](#) – Defines several specific new OAuth 2.0 response types
- [OAuth 2.0 Form Post Response Mode](#) – Defines how to return OAuth 2.0 Authorization Response parameters (including OpenID Connect Authentication Response parameters) using HTML form values that are auto-submitted by the User-Agent using HTTP POST
- [OpenID 2.0 to OpenID Connect Migration 1.0](#) – Defines how to migrate from OpenID 2.0 to OpenID Connect
- [OpenID Connect RP-Initiated Logout](#) – Defines how a Relying Party requests that an OpenID Provider log out the End-User
- [Session Management](#) – Defines how to manage OpenID Connect sessions, including postMessage-based logout functionality
- [Front-Channel Logout](#) – Defines a front-channel logout mechanism that does not use an OP iframe on RP pages
- [Back-Channel Logout](#) – Defines a logout mechanism that uses direct back-channel communication between the OP and RPs being logged out
- [OpenID Connect Core Error Code unmet_authentication_requirements](#) – Defines the unmet_authentication_requirements authentication response error code
- [Initiating User Registration via OpenID Connect](#) – Defines the prompt=create authentication request parameter

Implementer's Drafts

- [OpenID Federation 1.0](#) – Defines how parties within a federation can establish trust with one another
- [Self-Issued OpenID Provider V2](#) – Enables End-users to use OpenID Providers (OPs) that they control
- [OpenID Connect Native SSO for Mobile Apps](#) – Enables native applications by the same vendor to share login information
- [OpenID for Verifiable Presentations \(OpenID4VP\)](#) – Defines a mechanism on top of OAuth 2.0 to allow presentation of claims in the form of Verifiable Credentials as part of the protocol flow

Drafts

- [OpenID Connect Claims Aggregation](#) – Enables RPs to request and Claims Providers to return aggregated claims through Ops
- [OpenID Federation Extended Subordinate Listing](#) – Extends OpenID Federation to facilitate listings of large numbers of subordinates
- [OpenID Federation Wallet Architectures](#) – Defines how to perform trust establishment for Wallet ecosystems with OpenID Federation
- [OpenID Connect Relying Party Metadata Choices](#) – Enables RPs to express a set of supported values for RP metadata parameters

OpenID Connect in Italy

Challenges and Motivation

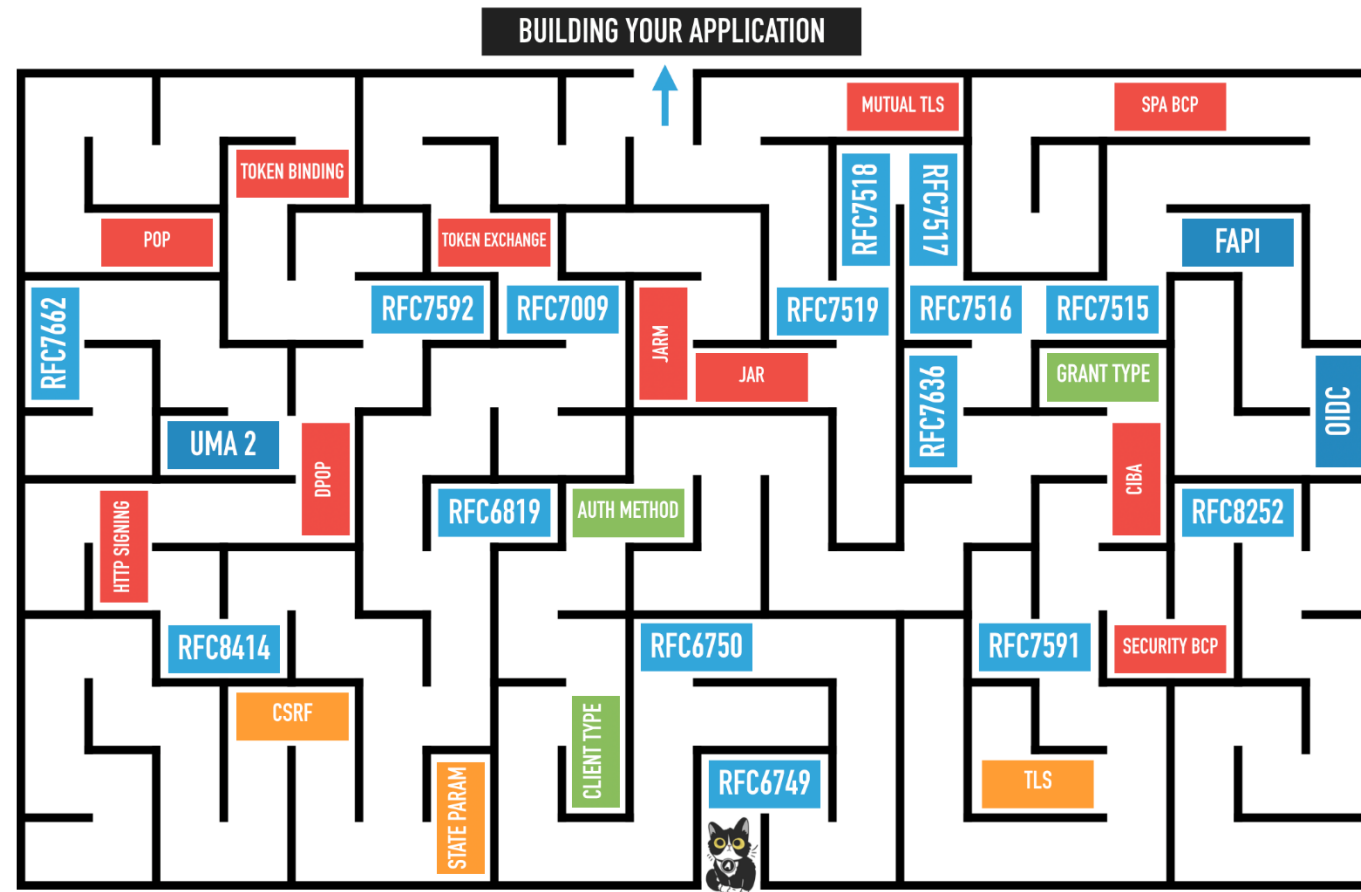
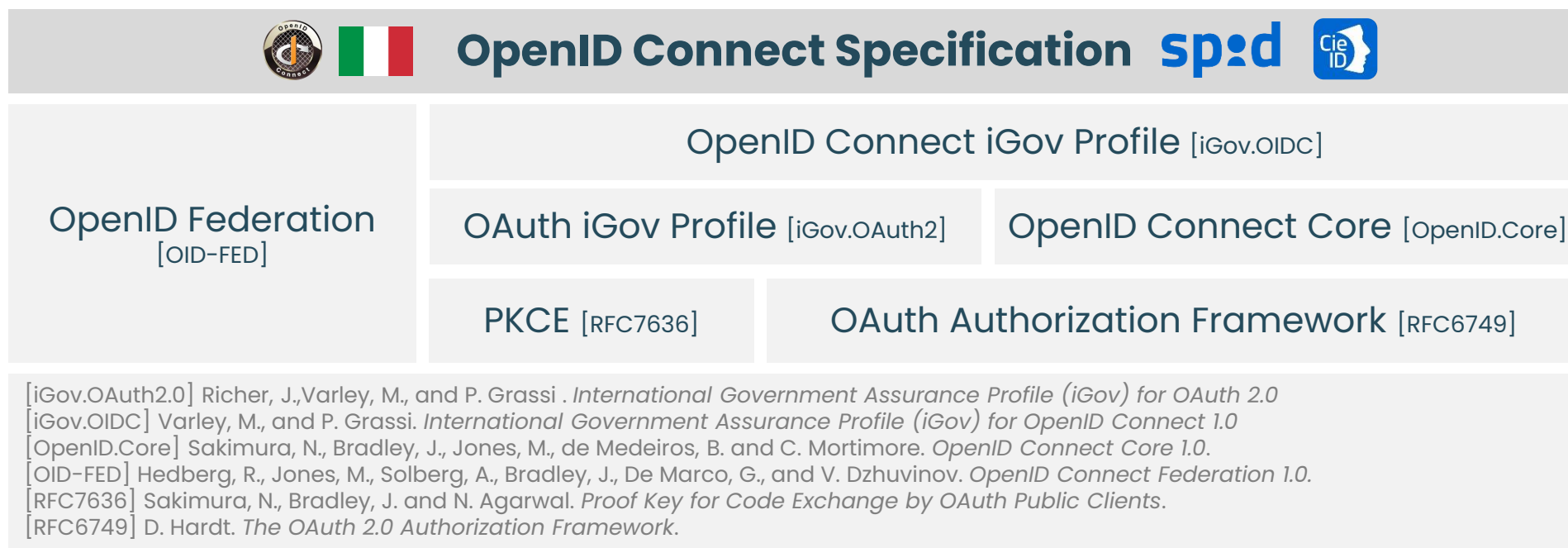


Image source: <https://aaronparecki.com/2019/12/12/21/its-time-for-oauth-2-dot-1>

OpenID Connect in Italy

Challenges and Motivation

- The Italian OIDC specification is based on the *International Government Assurance* profile (iGov) for OpenID Connect 1.0 [iGov.OIDC] that is built on top of the *OpenID Connect Core profile* [OpenID.Core]
- Metadata exchange and trust are managed adopting *OpenID Federation 1.0* [OID-FED]



OpenID Connect in Italy

Security Considerations

Security

Mitigate code injection/replay
(authorization code + PKCE)

Mitigate Mix-Up attack
(iss)

Mitigate Authn request modification
(request)

Enable Strong Authentication
(acr_value)

Mitigate client impersonation
(private_key_jwt)

Mitigate CSRF
(PKCE or State or Nonce)

Mitigate ID Token replay
(nonce)

Privacy

Mitigate User's tracking using sub
(pairwise)

Data minimization
(Claims)

User consent
(prompt=login consent)

OpenID Connect in Italy

Security Considerations

Security



Mitigate code injection/replay
(authorization code + PKCE)

Mitigate Mix-Up attack
(iss)

Mitigate Authn request modification
(request)

Enable Strong Authentication
(acr_value)

Mitigate client impersonation
(private_key_jwt)

Mitigate CSRF
(PKCE or State or Nonce)

Mitigate ID Token replay
(nonce)

Privacy

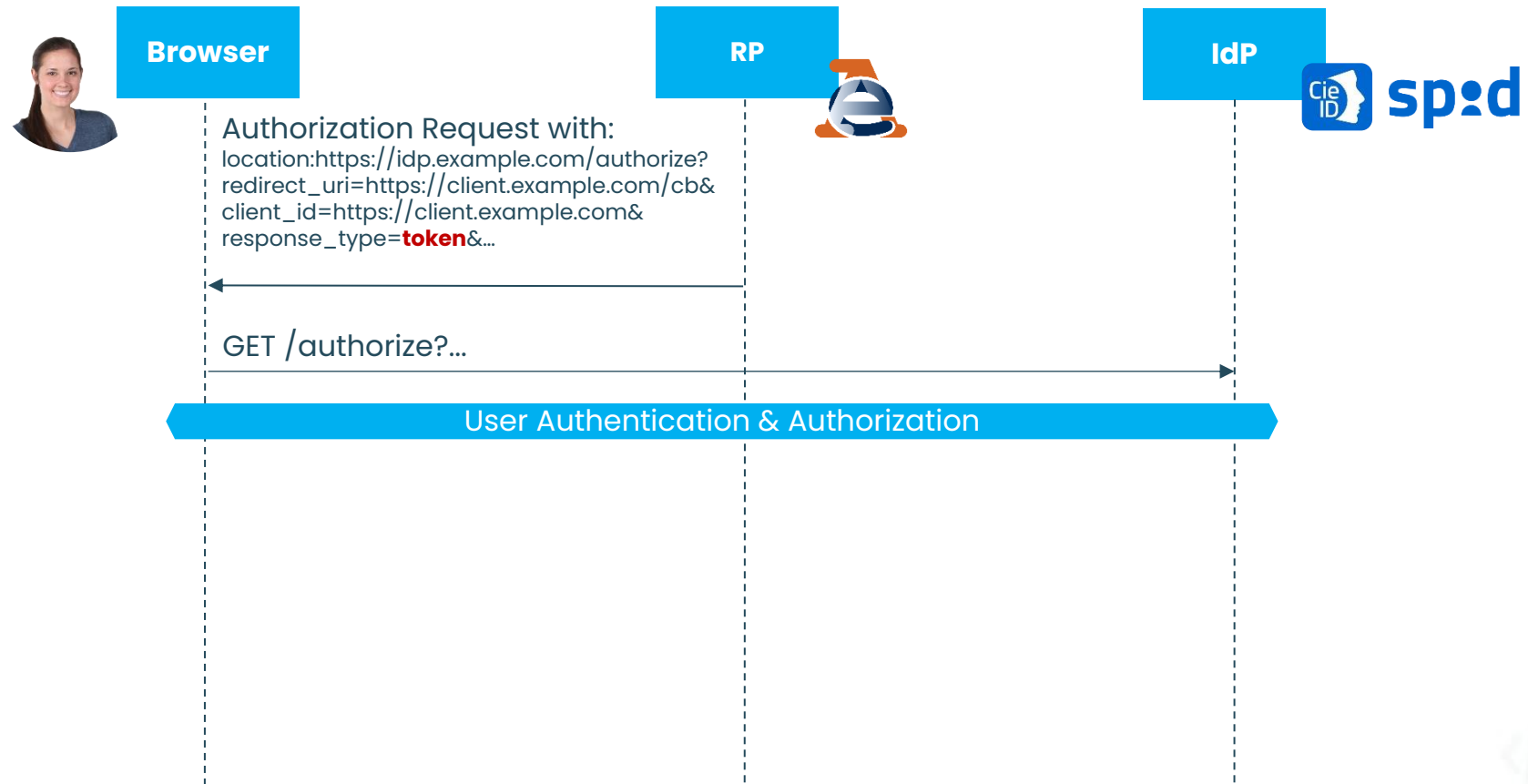
Mitigate User's tracking using sub
(pairwise)

Data minimization
(Claims)

User consent
(prompt=login consent)

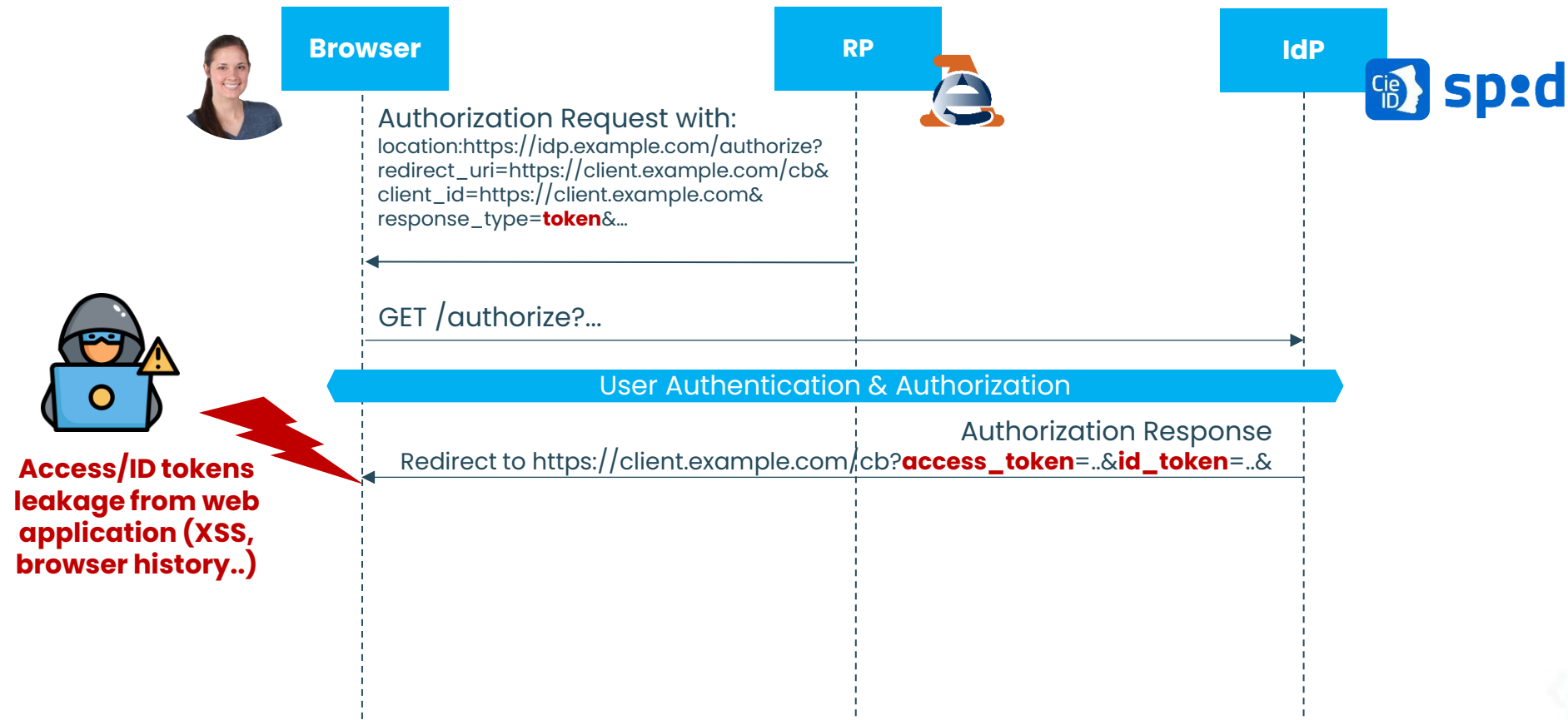
OpenID Connect in Italy

Authorization Request: **DO NOT USE Implicit Flow**



OpenID Connect in Italy

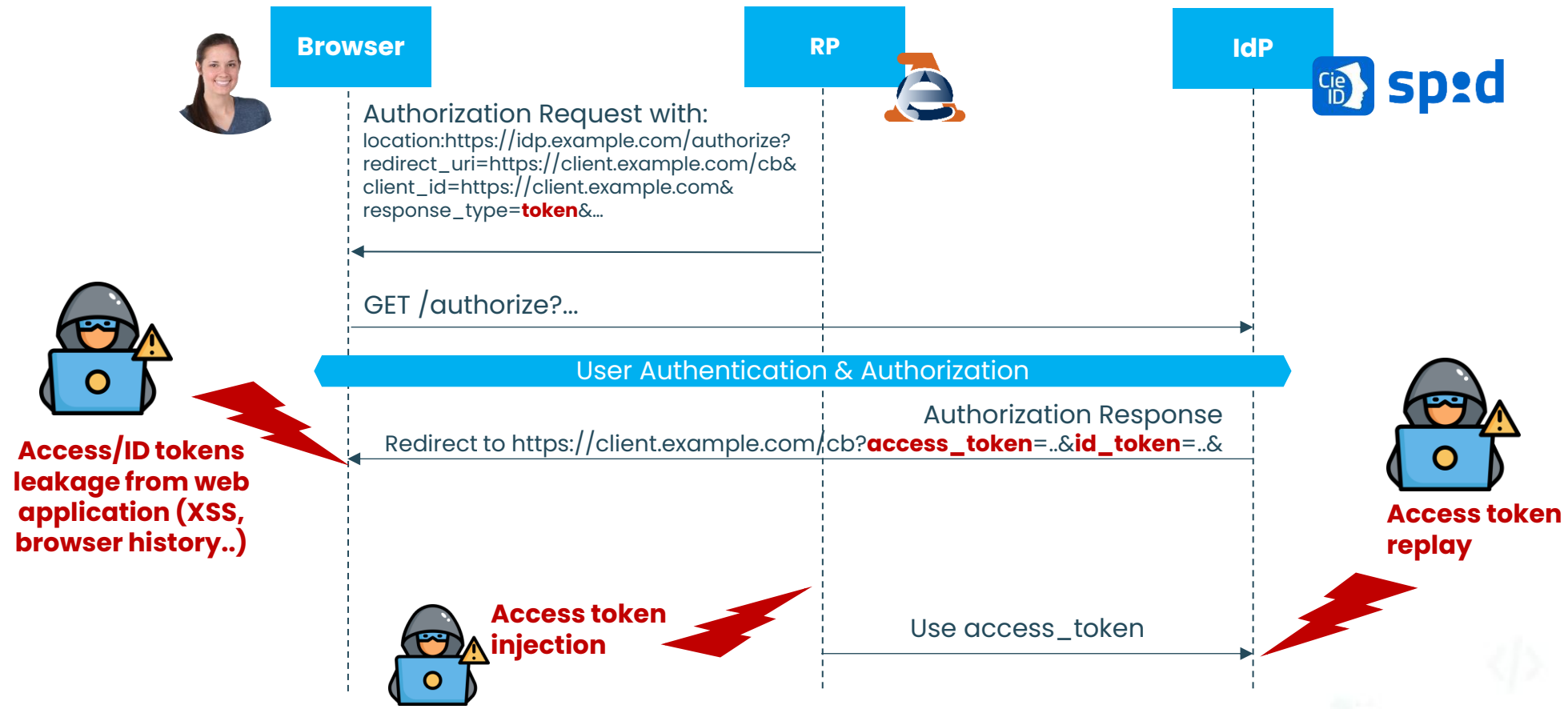
Authorization Request: **DO NOT USE Implicit Flow**



Credits: Daniel Fett

OpenID Connect in Italy

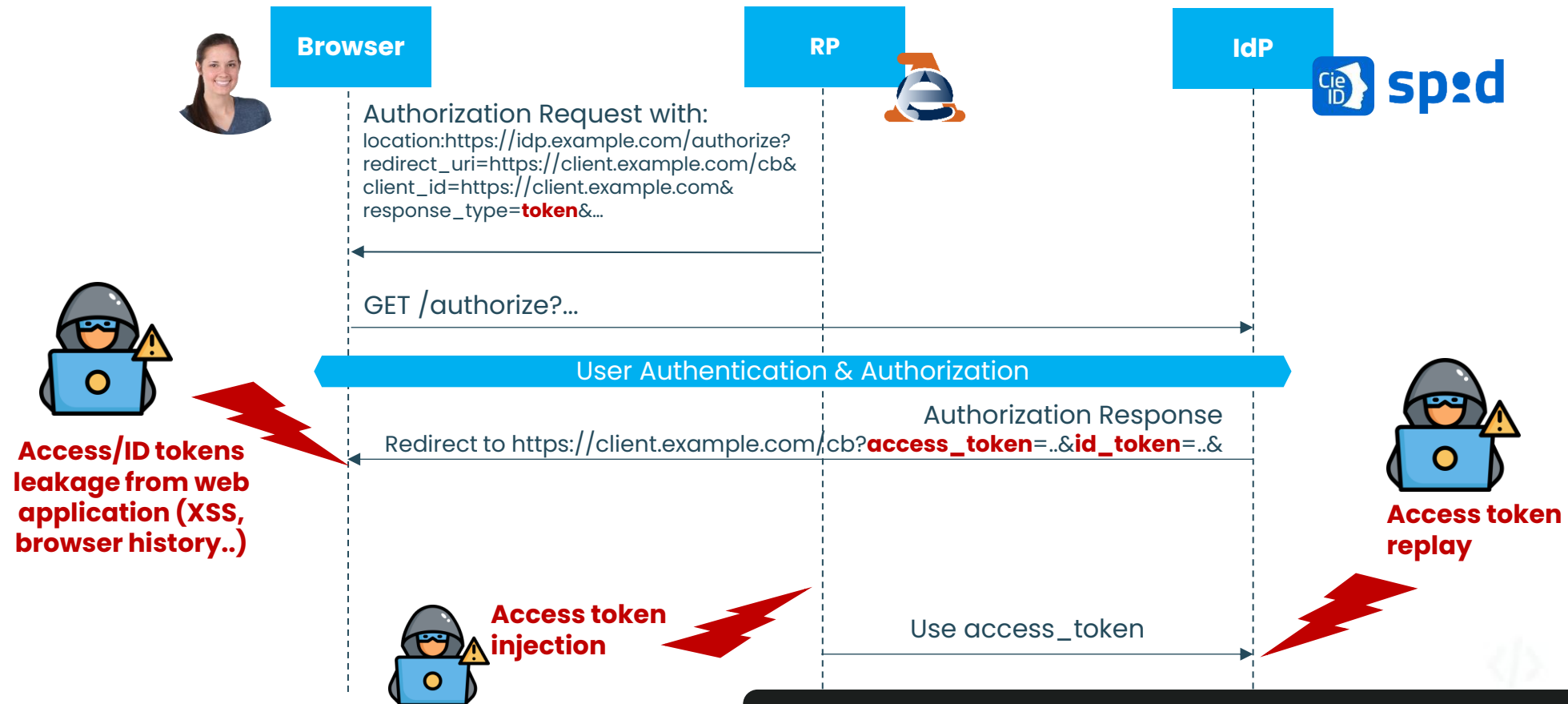
Authorization Request: **DO NOT USE Implicit Flow**



Credits: Daniel Fett

OpenID Connect in Italy

Authorization Request: **DO NOT USE Implicit Flow**

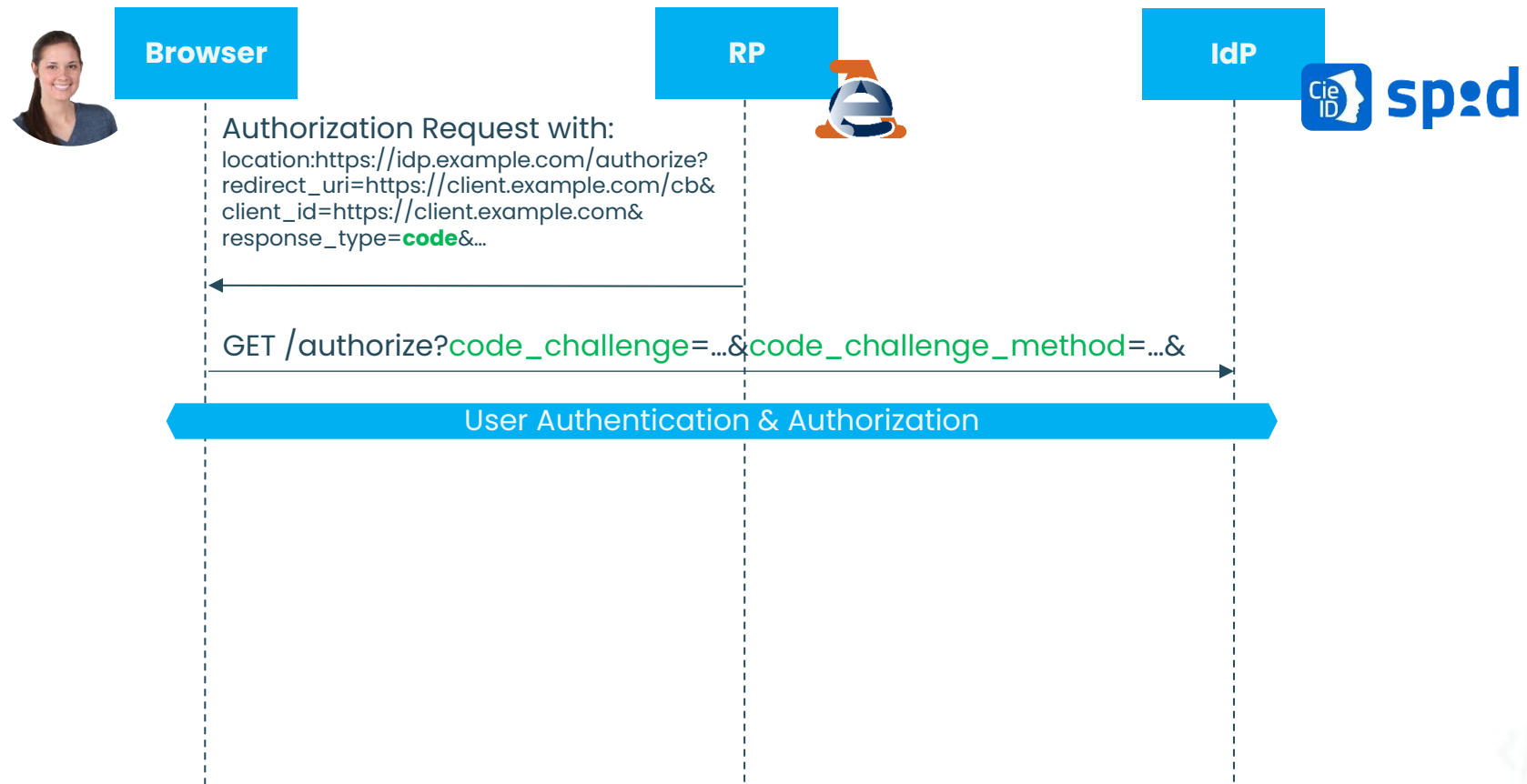


The attacker is able to impersonate Alice

Credits: Daniel Fett

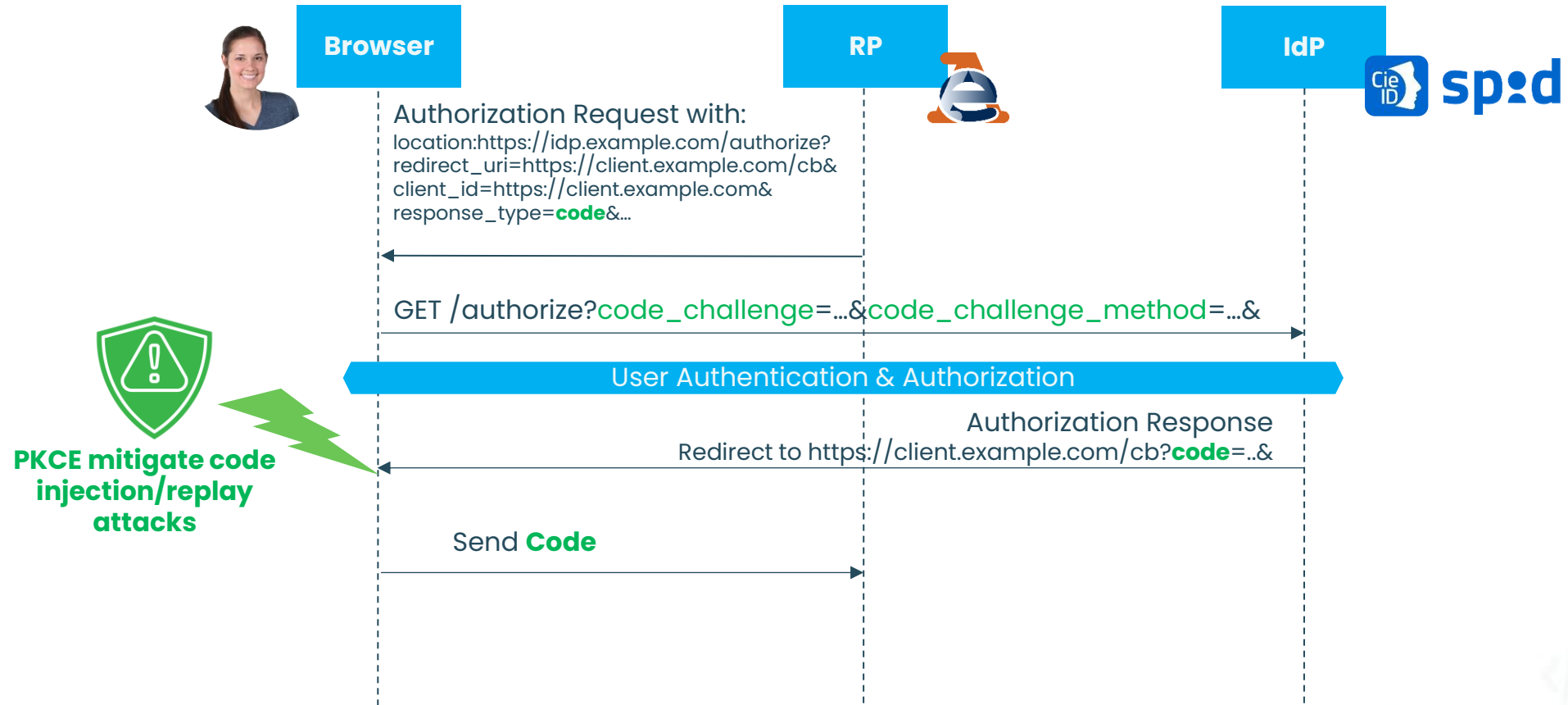
OpenID Connect in Italy

Authorization Request: Authorization Code Flow + PKCE



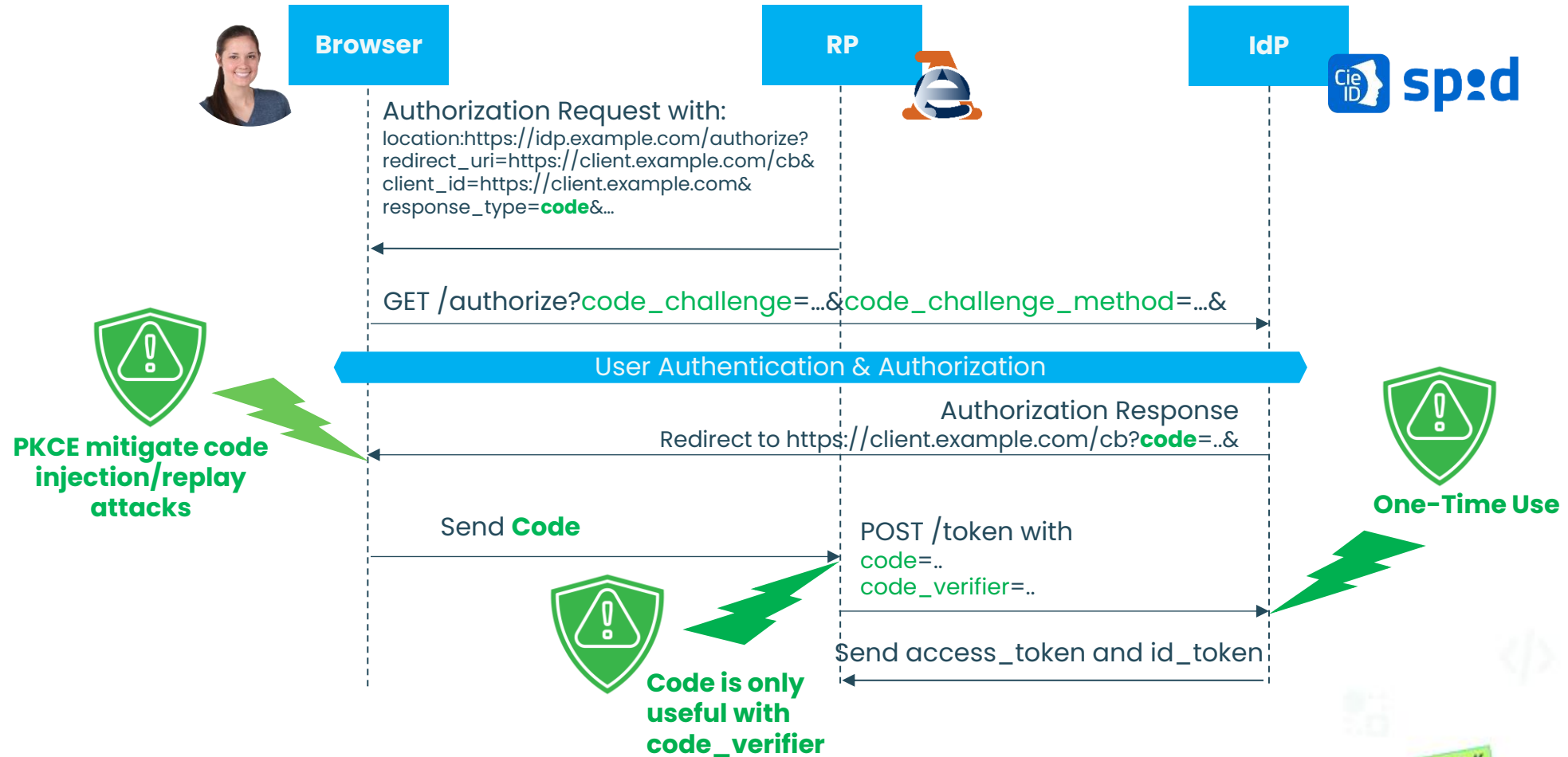
OpenID Connect in Italy

Authorization Request: Authorization Code Flow + PKCE



OpenID Connect in Italy

Authorization Request: Authorization Code Flow + PKCE



Actionable Security

Enforce Security with Automatic Tools

Micro-Id-Gym

MIG is a flexible and extendable tool designed to perform security testing on Identity Management protocol implementations like SAML, OIDC and OAuth.

 <https://github.com/stfbk/mig>

 <https://developers.italia.it/it/software/github.com/stfbk/mig>



Andrea Bisegna, Roberto Carbone, Ivan Martini, Valentina Odorizzi, Giulio Pellizzari, Silvio Ranise. **Micro-Id-Gym: Identity Management Workouts with Container-Based Microservices.** In: *International Journal of Information Security and Cybercrime (IJISP)*, Volume 8, Issue 1.

Actionable Security

Enforce Security with Automatic Tools

Micro-Id-Gym

MIG is a flexible and extendable tool designed to perform security testing on Identity Management protocol implementations like SAML, OIDC and OAuth.

 <https://github.com/stfbk/mig>  <https://developers.italia.it/it/software/github.com/stfbk/mig>

TLSAssistant

TLS analyzer that provides:

- actionable hints that can be used to patch the identified vulnerability
- compliance analyses against five agency-issued technical guidelines: AgID ver.2020-01, ANSSI v1.2, BSI TR-02102-2 and TR-03116-4, Mozilla v5.7, NIST SP 800-52 Rev. 2 (and related)

 <https://github.com/stfbk/tlsassistant>  <https://developers.italia.it/it/software/github.com/stfbk/tlsassistant>



TLSAssistant



Matteo Rizzi, Salvatore Manfredi, Giada Sciarretta, Silvio Ranise. **A Modular and Extensible Framework for Securing TLS.** In: *12th ACM Conference on Data and Application Security and Privacy (CODASPY 2022).*

Riccardo Germania, Salvatore Manfredi, Matteo Rizzi, Giada Sciarretta, Alessandro Tomasi, Silvio Ranise. **Automating Compliance for Improving TLS Security Postures: An Assessment of Public Administration Endpoints.** In: *21th International Conference on Security and Cryptography (SECRYPT 2024).*



OpenID Connect Specification

iGOV and OIDC Federation profiles



Activities in the context of EUDIW

PID Issuance, Trust model, Threat Model, Revocation

eIDAS Timeline

spod | AgID Agenzia per
l'Italia Digitale

NOTIFIED

September
2018

National
eID schemes
<2014

July
2014

eID.AS

September
2019



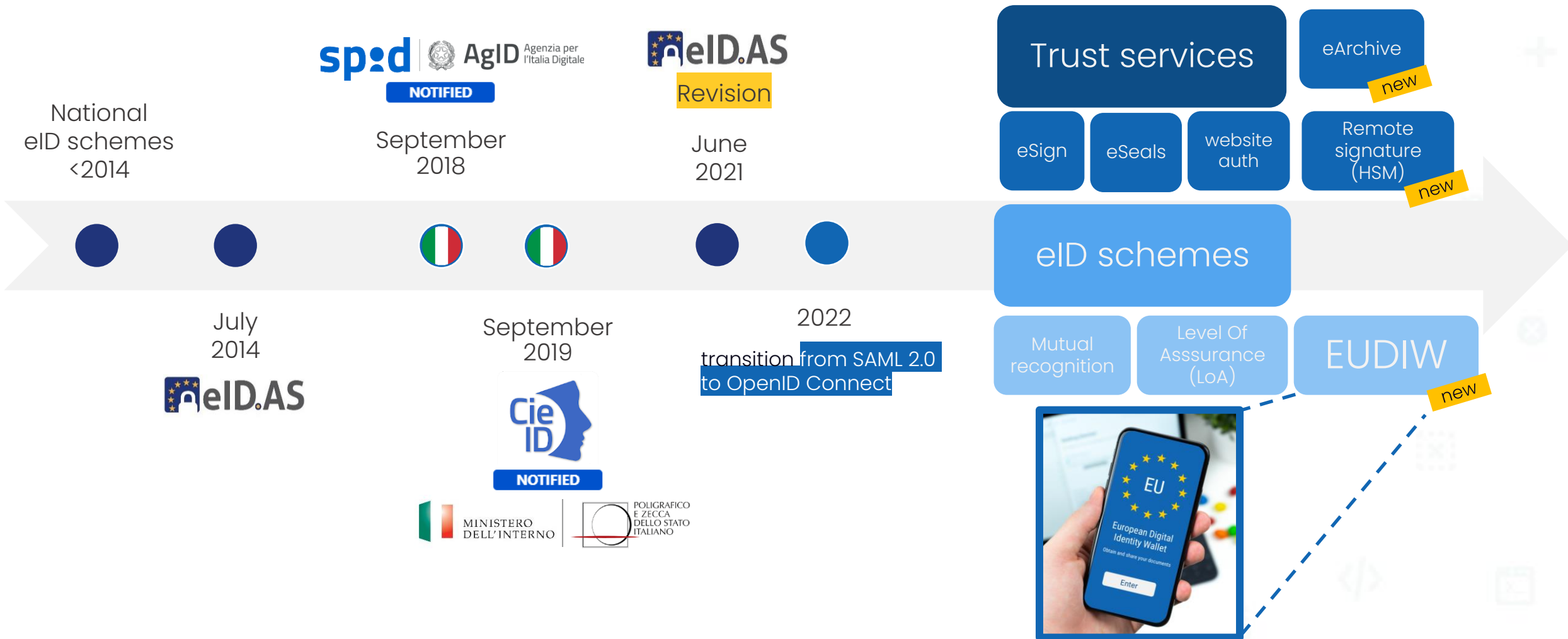
NOTIFIED



2022

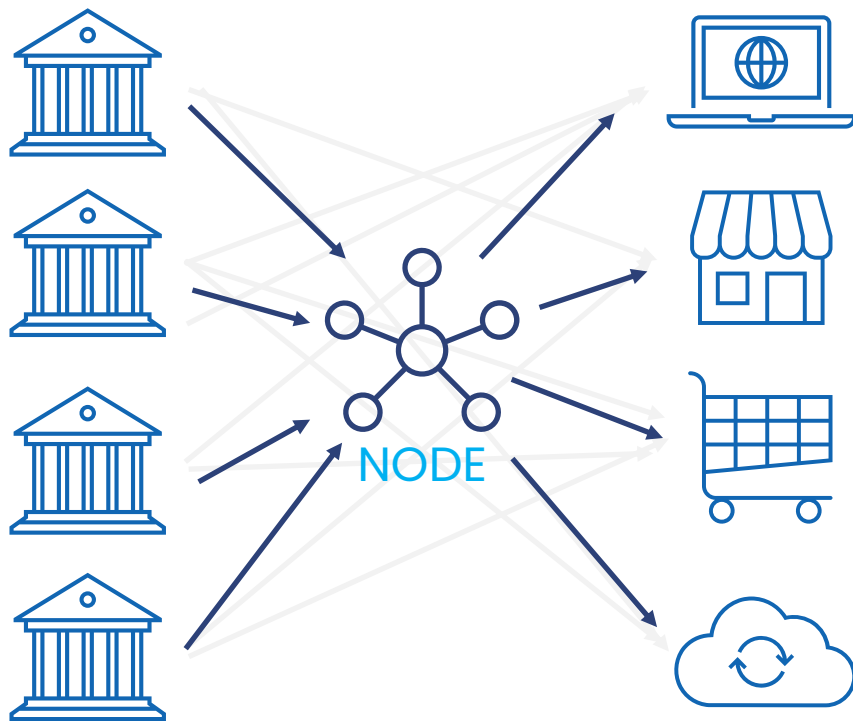
transition from SAML 2.0
to OpenID Connect

eIDAS Timeline



EUDI Wallet

A Different Paradigm



 eID.AS 1.0



 eID.AS 2.0

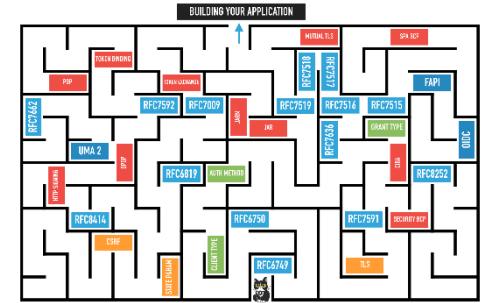
EUDI Wallet

New Set of Standards

- O. Terbu, D. Fett, B. Campbell. **SD-JWT-based Verifiable Credentials (SD-JWT VC) – draft 05.**
- T. Lodderstedt, K. Yasuda, T. Looker. **OpenID for Verifiable Credential Issuance – draft 14.** (OpenID4VCI)
- O. Terbu, T. Lodderstedt, K. Yasuda, T. Looker. **OpenID Connect for Verifiable Presentations – draft 22.** (OpenID4VP)
- **ISO/IEC 18013-5:** Personal identification --- ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application, First edition, 2021-09.
- **ISO/IEC 18013-7:** Personal identification ISO-compliant driving licence - Part 7: Mobile driving licence (mDL) add-on functions
- **ISO/IEC 23220-1:** Cards and security devices for personal identification - Building blocks for identity management via mobile devices, Part 1: Generic system architectures of mobile eID systems
- **ISO/IEC TS 23220-3:** Cards and security devices for personal identification - Building blocks for identity management via mobile devices, Part 3: Protocols and services for issuing phase
- **ISO/IEC TS 23220-4:** Cards and security devices for personal identification - Building blocks for identity management via mobile devices - Part 4: Protocols and services for operational phase.
- G. De Marco, R. Hedberg, M.B. Jones, J. Bradley. **OpenID Federation Wallet Architectures 1.0 – draft 03.**
- T. Looker, P. Bastian, C. Bormann. **Token Status List – draft 05.**
- G. De Marco, O. Steele, F. Marino, M. Adomeit. **OAuth Status Assertions – draft 05.**
- ...

EUDI Wallet

New Set of Standards



- O. Terbu, D. Fett, B. Campbell. **SD-JWT-based Verifiable Credentials (SD-JWT VC) – draft 05.**
- T. Lodderstedt, K. Yasuda, T. Looker. **OpenID for Verifiable Credential Issuance – draft 14.** (OpenID4VCI)
- O. Terbu, T. Lodderstedt, K. Yasuda, T. Looker. **OpenID Connect for Verifiable Presentations – draft 22.** (OpenID4VP)
- **ISO/IEC 18013-5:** Personal identification --- ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application, First edition, 2021-09.
- **ISO/IEC 18013-7:** Personal identification ISO-compliant driving licence - Part 7: Mobile driving licence (mDL) add-on functions
- **ISO/IEC 23220-1:** Cards and security devices for personal identification - Building blocks for identity management via mobile devices, Part 1: Generic system architectures of mobile eID systems
- **ISO/IEC TS 23220-3:** Cards and security devices for personal identification - Building blocks for identity management via mobile devices, Part 3: Protocols and services for issuing phase
- **ISO/IEC TS 23220-4:** Cards and security devices for personal identification - Building blocks for identity management via mobile devices - Part 4: Protocols and services for operational phase.
- G. De Marco, R. Hedberg, M.B. Jones, J. Bradley. **OpenID Federation Wallet Architectures 1.0 – draft 03.**
- T. Looker, P. Bastian, C. Bormann. **Token Status List – draft 05.**
- G. De Marco, O. Steele, F. Marino, M. Adomeit. **OAuth Status Assertions – draft 05.**
- ...



EUDI Wallet

Our contributions

EUDI Wallet

Our contributions

- Study of selective disclosure mechanisms



Hiding-Commitment and selective disclosure signature mechanisms

18/01/1995

Andrea Flamini, Giada Sciarretta, Amir Sharif, Alessandro Tomasi, Silvio Ranise. **A First Appraisal of Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials.** In: *20th International Conference on Security and Cryptography (SECRYPT 2023)*.

A. Flamini, G. Sciarretta, M. Scuro, A. Sharif, A. Tomasi, S. Ranise. **On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials.** In: *Journal of Information Security and Applications (JISA)*.

EUDI Wallet

Our contributions

- Study of selective disclosure mechanisms
- Definition of the PID/(Q)EAA Issuance flow

Security

- PID credential request replay**
(c_nonce)
- EUDIW impersonation**
(client authentication and Wallet Attestation check)
- Tamper Authentication request**
(Push Authorization Request)
- Obtaining access token**
(DPoP)
- Obtaining authorization code**
(PKCE)
- Session misuse**
(PKCE or State or Nonce)
- Malicious Issuer/Wallet**
(OpenID Federation Trust Model)

Privacy

- Selective disclosure**
(SD-JWT)
- User consent**
(prompt=login consent)
- Unlinkability**
(Ephemeral keys)

OpenID Federation 1.0 [OID-FED]	OpenID For Verifiable Credentials [OID4VCI]	
	OAuth Authorization Framework [RFC6749]	
	OAuth 2.0 Attestation-Based Client Authentication [OAUTH-ATTESTATION-CLIENT-AUTH].	
	Pushed Authorization Requests (PAR) [RFC 9126]	Rich Authorization Requests (RAR) [RFC 9396]
	JWT Authorization Requests (JAR) [RFC 9101]	JWT Authorization Response Modes (JARM)
	Proof Key for Code Exchange (PKCE) [RFC7636]	
	OAuth 2.0 Demonstrating Proof-of-Possession (DPoP) [RFC9449]	
	SD-JWT-VC [I-D.ietf-oauth-sd-jwt-vc] and MDOC-CBOR [ISO18013-5]	

 <https://italia.github.io/eudi-wallet-it-docs/versione-corrente/en/pid-eaa-issuance.html>

EUDI Wallet

Our contributions

- Study of selective disclosure mechanisms
- Definition of the PID/(Q)EAA Issuance flow
- Threat model and risk assessment

Our current threat model counts:

72 threats

83 security controls

We are currently working on a risk assessment tool to help stakeholders in the decision-making process to prioritize the security controls to implement.

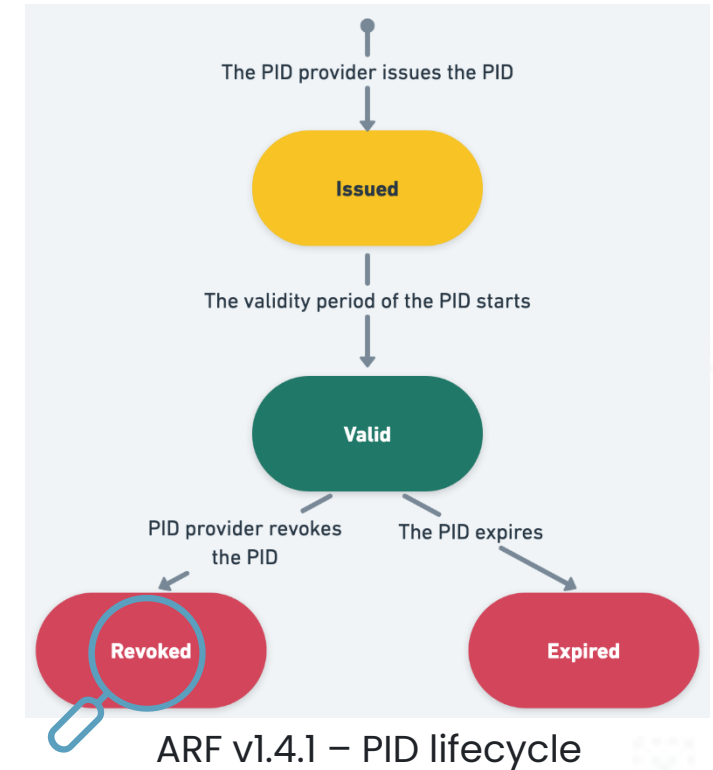


Amir Sharif, Zahra Ebadi Ansaroudi, Giada Sciarretta, Daniela Pöhn, Majid Mollaeefar, Wolfgang Hommel, Silvio Ranise. **Protecting Digital Identity Wallet: A Threat Model in the Age of eIDAS 2.0.** In: *19th International Conference on Risks and Security of Internet and Systems (CRISIS 2024)*.

EUDI Wallet

Our contributions

- Study of selective disclosure mechanisms
- Definition of the PID/(Q)EAA Issuance flow
- Threat model and risk assessment
- Study of credential status mechanisms
 - CRL
 - OCSP (with stapling)
 - Token Status List
 - OAuth Status Assertions
 - Dynamic Status List
 - Accumulators




European Digital Identity Wallet Architecture and Reference Framework (ARF). <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md>

EUDI Wallet

Our contributions

- Study of selective disclosure mechanisms
- Definition of the PID/(Q)EAA Issuance flow
- Threat model and risk assessment
- Study of credential status mechanisms
- Definition of an interoperable Trust Framework

OpenID Federation Wallet Architectures 1.0

 <https://github.com/openid/federation-wallet>

EUDI Wallet Large Scale Pilot

Potential
For European Digital Identity



Co-funded by
the European Union

As FBK, we beneficiary in the **POTENTIAL Large-Scale Pilot**

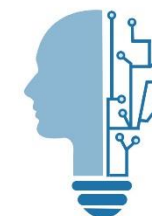
- PilOTs for European digital Identity wALlet
- 140+ organizations, 20 member states
- Aims at fostering innovation, collaboration and growth in 6 digital identity sectors:
 - eGov Services
 - Bank Account Opening
 - SIM Card Registration
 - Mobile Driving Licence
 - Qualified eSignature
 - ePrescription



PROVINCIA AUTONOMA
DI TRENTO



Trentino
Digitale SpA



TRENTINO SALUTE
4.0

3rd International Workshop on Trends in Digital Identity

TDI 2025

February 3, 2025 – Bologna, Italy

ITASEC

Co-located with the Joint National Conference on Cybersecurity
(ITASEC & SERICS 2025)

WORK
SHOP
GARR
2024

NET
MAKERS

Thanks!

g.sciarretta@fbk.eu
<https://st.fbk.eu/>

Per le domande:



wooclap.com e
codice WSGARR24