IPZS ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

Monitoring and Compliance in OpenID Federation: from CIE to EUDI Wallet

Workshop GARR 2025

Marco Basili <*m.basili [at] ipzs.it*>
Pasquale Cerqua <*p.cerqua [at] ipzs.it*>

Direzione Innovazione, Strategia di Ricerca e Prodotto - CLASSIFICAZIONE: PUBBLICO

Roma, 05/11/2025

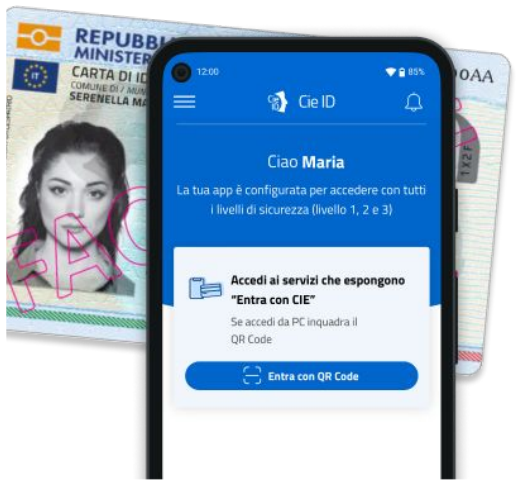
For any question:
wooclap.com with
code **WSGARR25**

Documento di proprietà dell'Istituto Poligrafico e Zecca dello Stato S.p.A. Sono vietate copie e distribuzioni, per intero o in parte, non espressamente autorizzate.

From Physical Documents to Digital Identity

Continuity of **trusted identity** provision across **physical** and **digital** domains

Physical Identity



Digital Identity CIE

Digital Identity Wallet

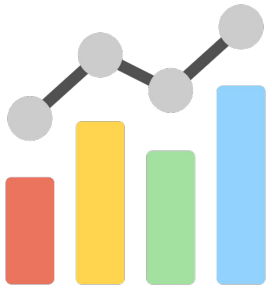
IPZS

CIE eID Scheme

Governance by **Ministry of the Interior**

Go live in **2019** with **SAML2**

Go live in **2023** with **OpenID Connect**



- Over **55 million** of identity provided to citizens
- **+ 100 million** accesses during the 12 months
- Over **10 million** accesses in the last month
- **+18000** Service Providers

IPZS

Evolution: Learning from SAML Experience

SAML2 Federation: Operational Challenges

1. **Metadata Management** Complexity
2. Limited **Policy** Enforcement
3. **Static Trust** Model
4. **Scalability** Constraints

CLASSIFICAZIONE: PUBBLICO

Graphic resources provided by www.freepik.com

Need for dynamic, scalable, policy-driven approach

Graphic resources provided by www.freepik.com

OpenID Federation: Dynamic Trust Framework

What is **OpenID Federation**

A modern **API-based** Trust framework for metadata exchange and **dynamic** trust chain establishment

DYNAMIC

Trust chains verified on-demand

SCALABLE

Native delegation, federation of federations by design

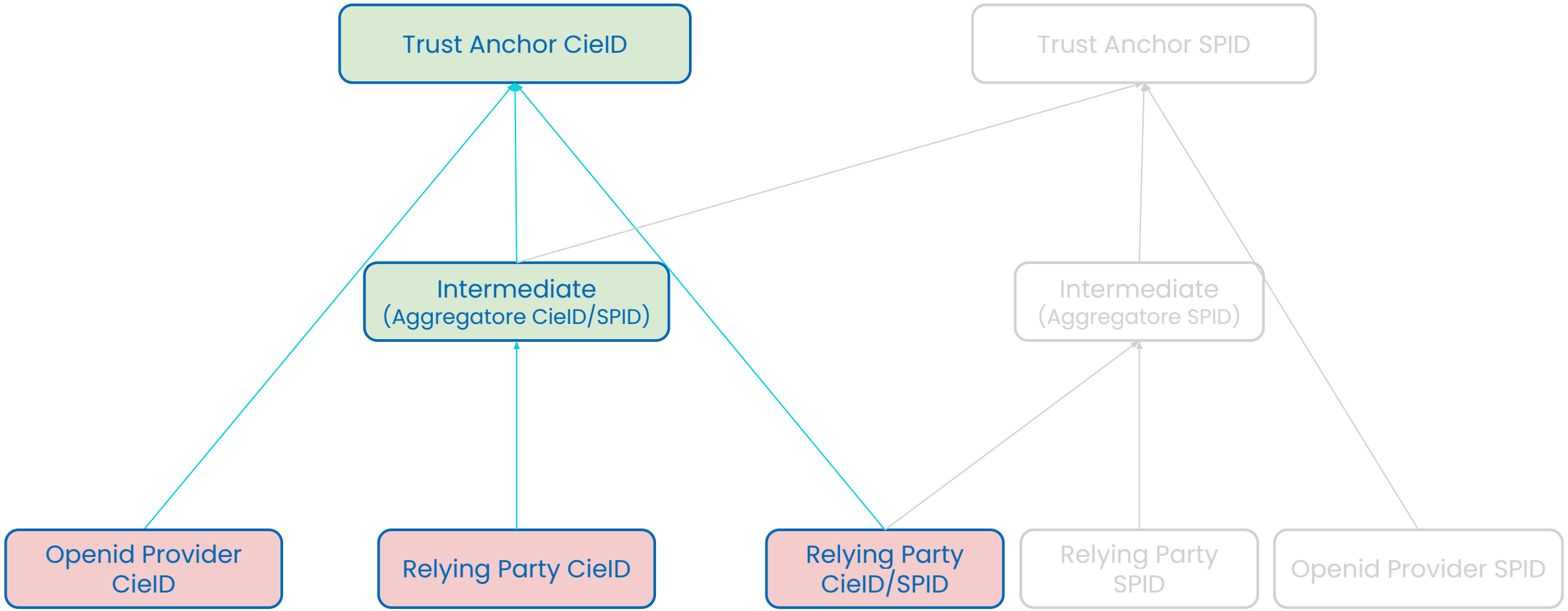
POLICY-DRIVEN

Central enforcement without entity updates

Graphic resources provided by www.freepik.com

IPZS

CieID Federation Ecosystem: Actors and Delegation



IPZS

Core Components

Entity Configuration:

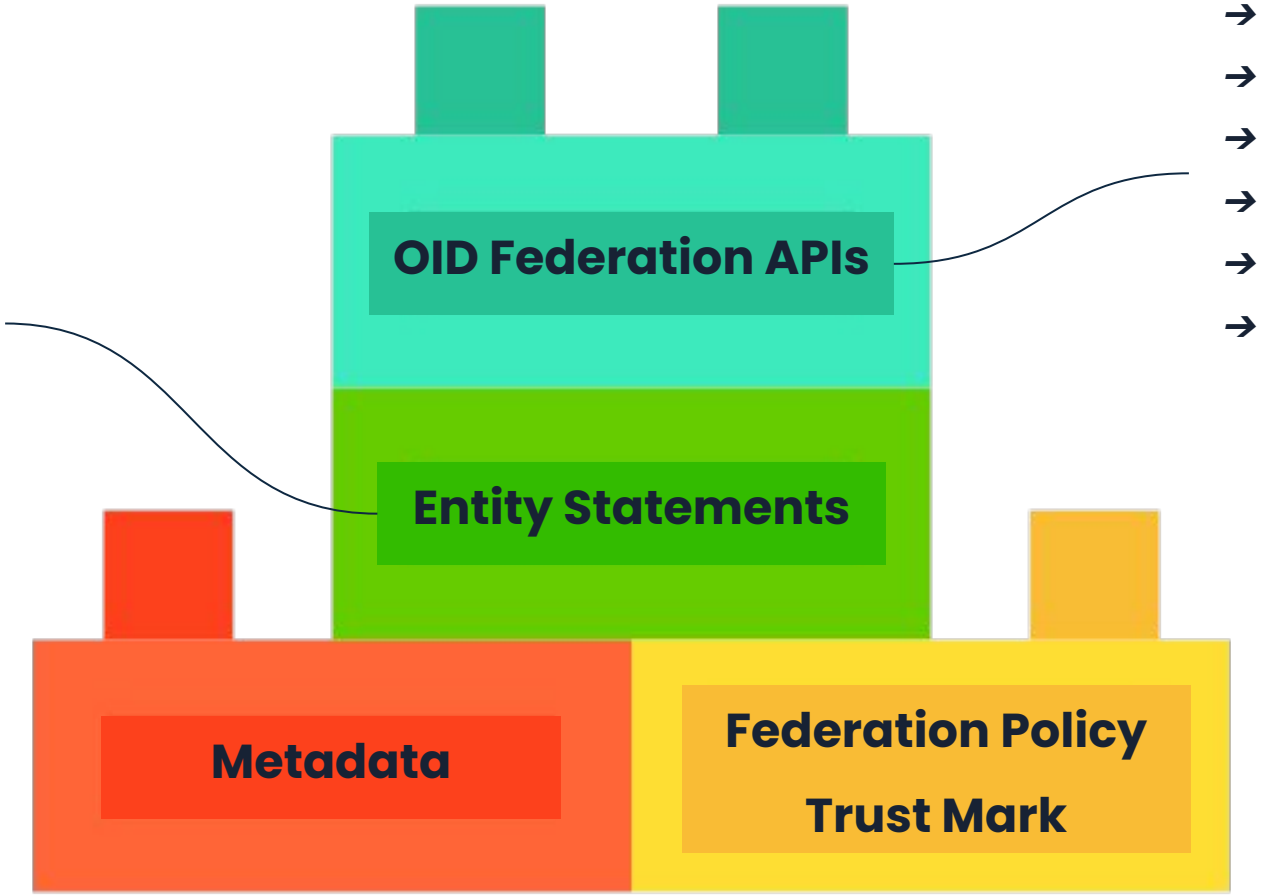
Self-signed JWT

Subordinate Statement:

JWT signed by TA or Intermediate issued to Leaf Entities

Available at:

.well-known/openid-federation

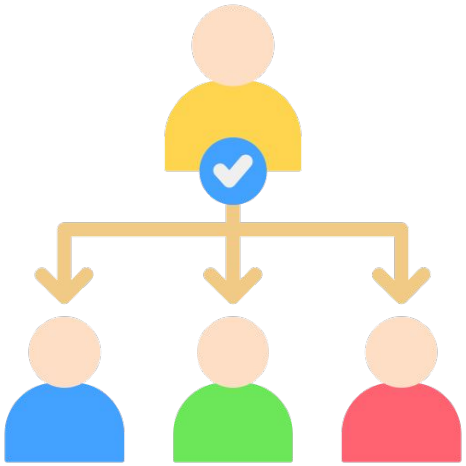


- *Fetch*
- *Listing*
- *Resolve*
- *Trust Mark*
- *Trust Mark Status*
- *Federation Historical Keys*

Graphic resources provided by www.freepik.com

IPZS

CieID Federation Ecosystem: Key Concepts



Onboarding Delegation

TA can delegates entity management to Intermediaries (Soggetti Aggregatori)

Trust Chain

Entities can establish the Trust using a verification path
(i.e. RP → SA → TA or OP → TA)

Graphic resources provided by www.freepik.com

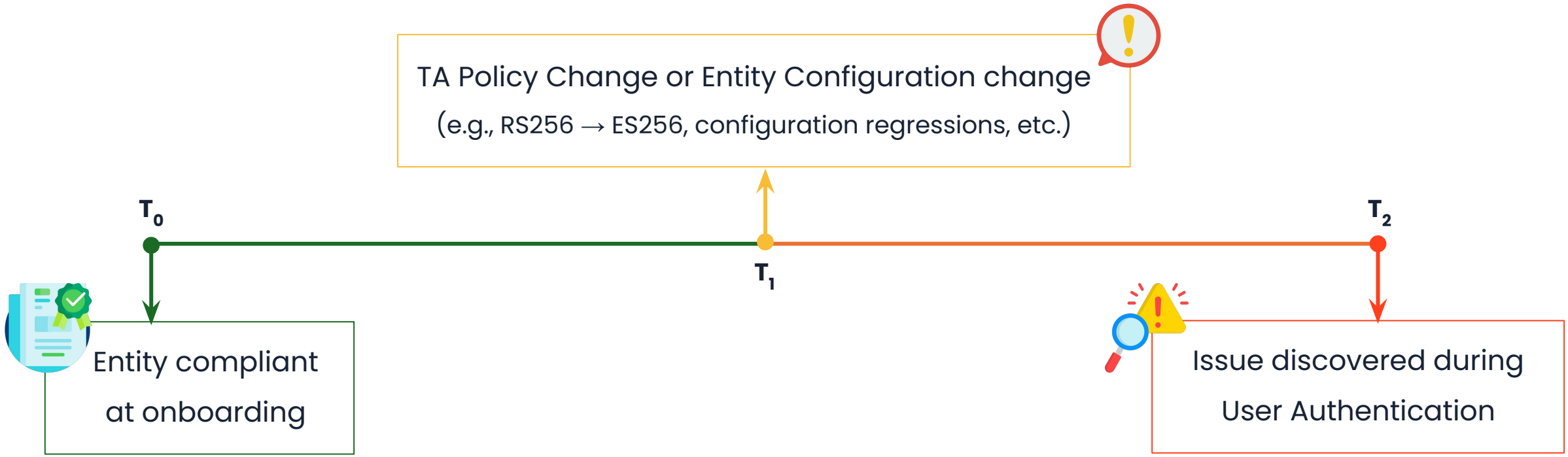
IPZS

Beyond onboarding
Ensuring trust over time

CLASSIFICAZIONE: PUBBLICO

Graphic resources provided by www.freepik.com

The Problem: Compliance Drift Over Time

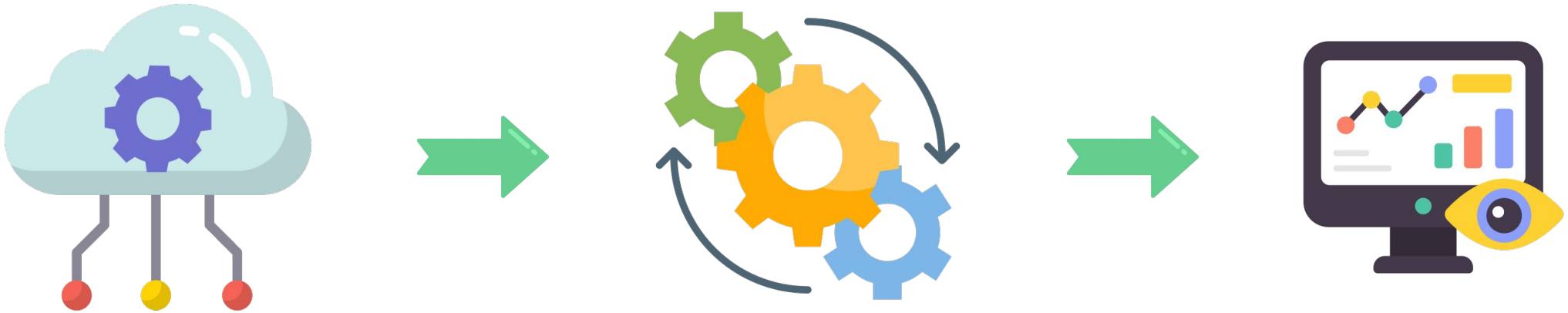


OpenID Federation Framework enables continuous monitoring

Graphic resources provided by www.freepik.com

IPZS

Monitoring Architecture: Layered Design



Layer 1

Federation APIs

API interface collecting all relevant Federation artifacts (Metadata, Entity Statements, Trust Marks, etc.)

Layer 2

Validation & Policy

Validation services handling trust chains, applying policies, verifying trust marks and signatures, and entity lifecycle

Layer 3

Monitoring & Observability

Continuous validation engines (at configuration and protocol level)

Health dashboards

Audit trail systems

Graphic resources provided by www.freepik.com

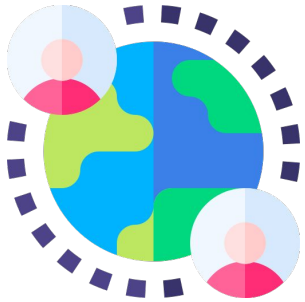
IPZS

European Digital Identity Wallet (EUDIW)

allows users to be in control of their personal data

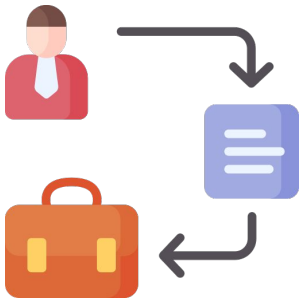
The European Wallet: Monitoring at Unprecedented Scale

Multi-Level Trust Architecture: Hierarchical trust model



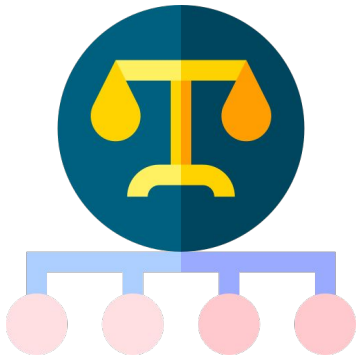
Interoperability

Many actors across borders (Wallet Providers, Credential Issuers, Relying Parties)



Cross Border Services

Diverse use cases (eGov, payments, education, health, travel, etc.)



Regulatory

Different Legal Framework

Graphic resources provided by www.freepik.com

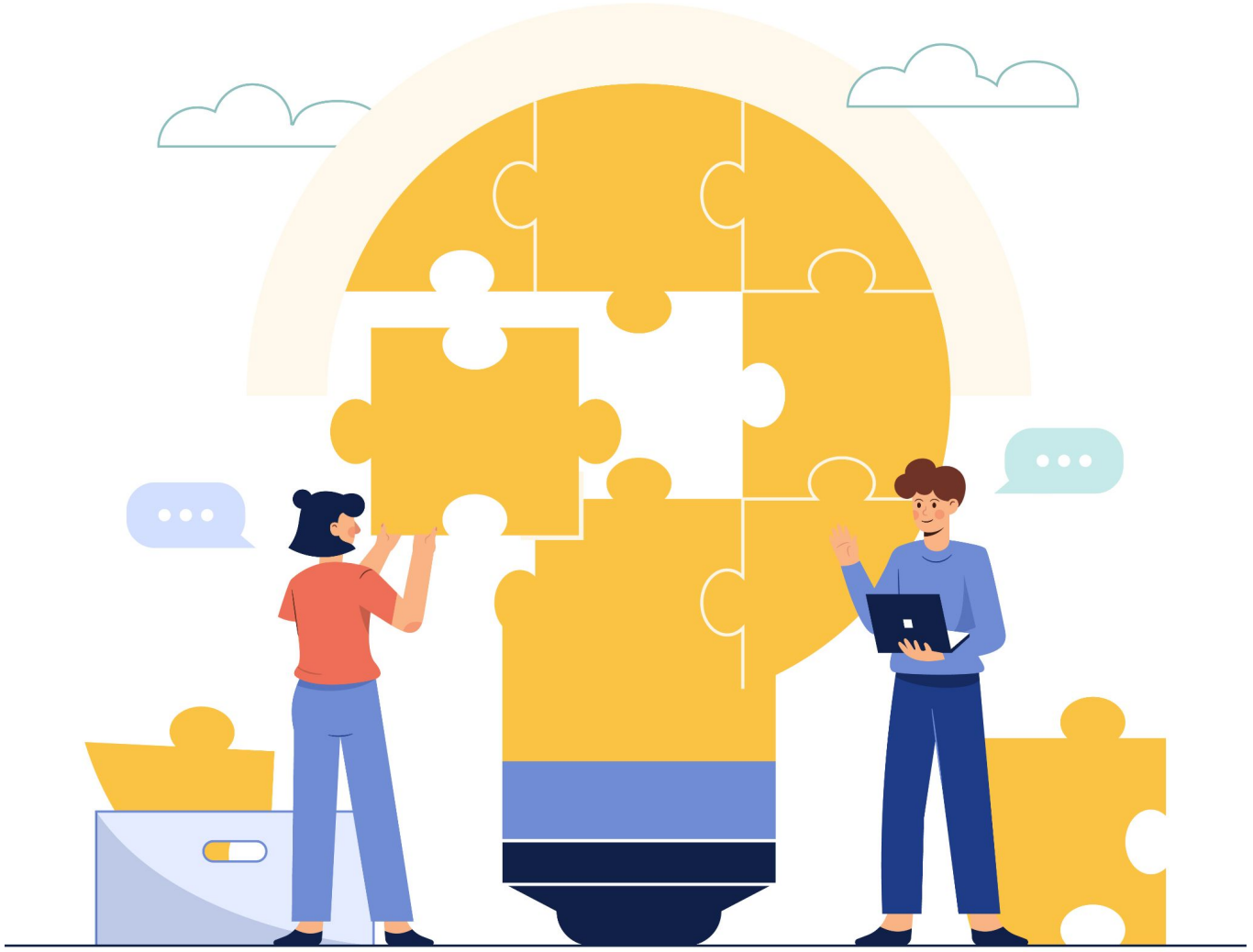
IPZS

How to ensure cross-border compliance?

CLASSIFICAZIONE: PUBBLICO

Graphic resources provided by www.freepik.com

Monitoring based on Federation natively integrated in Trust Framework



CLASSIFICAZIONE: PUBBLICO

Graphic resources provided by www.freepik.com

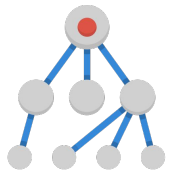
Why Federation Enables Monitoring

API-based

Programmatic access, automation-friendly

Declarative

Machine-readable JSON, parsable at scale



Distributed yet coordinated

Monitoring at each level (TA, SA)

Revocation built-in

Native to protocol, not bolt-on

Monitoring is not added to OpenID Federation

OpenID Federation IS the monitoring infrastructure

Graphic resources provided by www.freepik.com

IPZS

Monitoring Tools Ecosystem: Open Source & Documentation

Tools

- **Micro-Id-Gym (MIG)**: Web authentication protocol compliance testing (https://github.com/stfbk/mig)
- **Federation Browser**: User-friendly interface for navigating Federation based ecosystems (https://github.com/italia/openid-federation-browser)
- **Federation Entity Validator** (COMING SOON)

IPZS ISTITUTO POLIGRAFICO E ZECCA DELLO STATO + FONDAZIONE BRUNO KESSLER CENTER FOR CYBERSECURITY

Documentation

- **OpenID Federation** (https://openid.net/specs/openid-federation-1_0.html)
- **Manuale Tecnico CieID** (https://docs.italia.it/italia/cie/cie-manuale-tecnico-docs/it/master/index.html)
- **Manuale Operativo CieID** (https://federazione.servizicie.interno.gov.it/docs/cie-manuale-operativo-docs)
- **Specifiche Tecniche IT-Wallet** (https://github.com/italia/eid-wallet-it-docs)

Graphic resources provided by www.freepik.com

IPZS

ISTITUTO
POLIGRAFICO E ZECCA
DELLO STATO

For any question:
wooclap.com with
code **WSGARR25**

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO S.p.A.
Società per azioni con socio unico - Capitale sociale € 340.000.000 i.v.
Partita I.V.A. n. 00880711007 - Codice fiscale e R.I. 00399810589 - R.E.A. 86629
Sede legale: via Salaria, 691 - 00138 Roma - tel. 0685081 - protocollo@pec.ipzs.it - fax 0685082517/2626 - N. Verde 800864035
Società con Sistemi di Gestione Certificati UNI EN ISO 9001, UNI EN ISO 45001, UNI EN ISO 14001, UNI CEI EN ISO/IEC 27001, UNI EN ISO 22301, ISO/IEC 20000-1, ISO 14298, UNI ISO 37001
www.ipzs.it