WORKSHOP GARR 2022

NET MAKERS

Novità dal mondo SSO

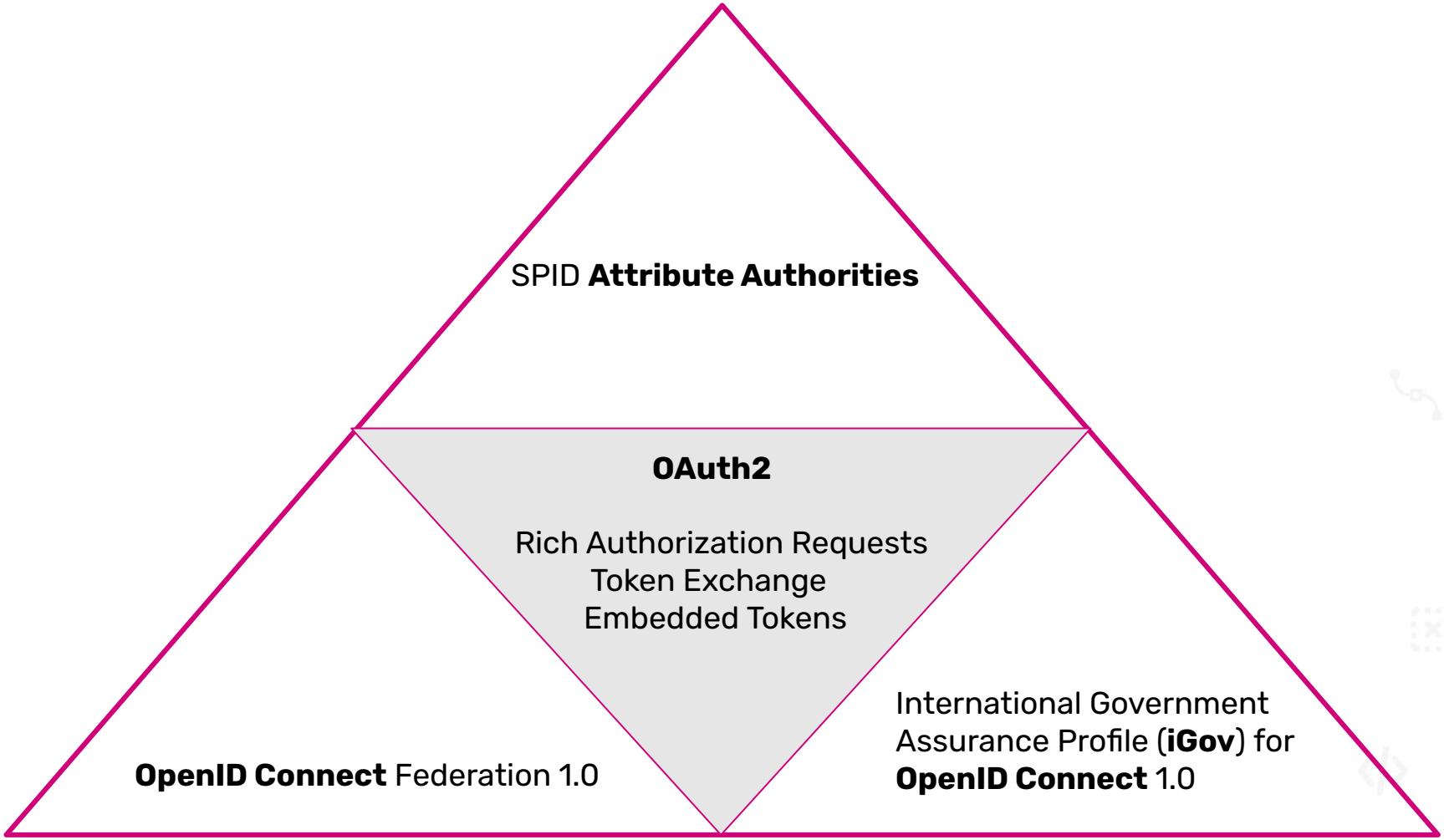
Linee guida sulle Attribute Authority e lo standard OpenID Connect Federation

Antonio Giovanni Colella, AgID
Giuseppe De Marco, DTD

La nuova infrastruttura basata su OpenID Connect

- **Piano Triennale della PA 2022 e 2021 2023:**
  - Piattaforme tecnologiche della Pubblica Amministrazione: offrono funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della PA.
  - SPID: DPCM 24 ottobre 2014 n.285
  - Piattaforma Gestione Deleghe (SDG) consente di delegare una persona fisica per agire presso le pubbliche amministrazioni.
- **PNRR misura 1.4.4 Adozione Identità Digitale**
  - Favorire l'adozione dell'identità digitale (Sistema Pubblico di Identità Digitale, SPID e Carta d'Identità Elettronica, CIE) e dell'Anagrafe nazionale della popolazione residente (ANPR).
- **Pubblicazioni AgID**:
  - Linee Guida SPID OpenID Connect e Avviso 41
  - Linee guida gestori di attributi qualificati (LLGG Attribute Authorities)
  - Regolamento SPID OpenID Connect Federation 1.0

Componenti della nuova Infrastruttura OpenID



Perché OpenID Connect?

- Paradigma **REST,** tecnologia HTTP, formato **JWT**:
  - Facile da implementare.
  - Accessibile alle nuove generazioni di implementatori.
  - Riduce i costi implementativi.
  - Riduce l'onere computazionale della verifica delle firme.
- **Framework** flessibile ed estendibile:
  - Estendibile mediante ecosistema OAuth2 (Standard sottostante).
  - Mobile friendly
  - Usabile in eIDAS 2.0, specifiche in rapida evoluzione:
    - OpenID for Verifiable Presentations
    - SIOPv2
    - OpenID Verifiable Credentials Issuance
    - ISO 18013-{5,7}
    - ISO 23220-{2,3,4}

Prima di iniziare - definizioni e acronimi

- Relying Party (**RP**). Fornitore di servizi digitali, nel gergo quotidiano un sito web con l'accesso *Entra con SPID* o *Entra con CIE*.

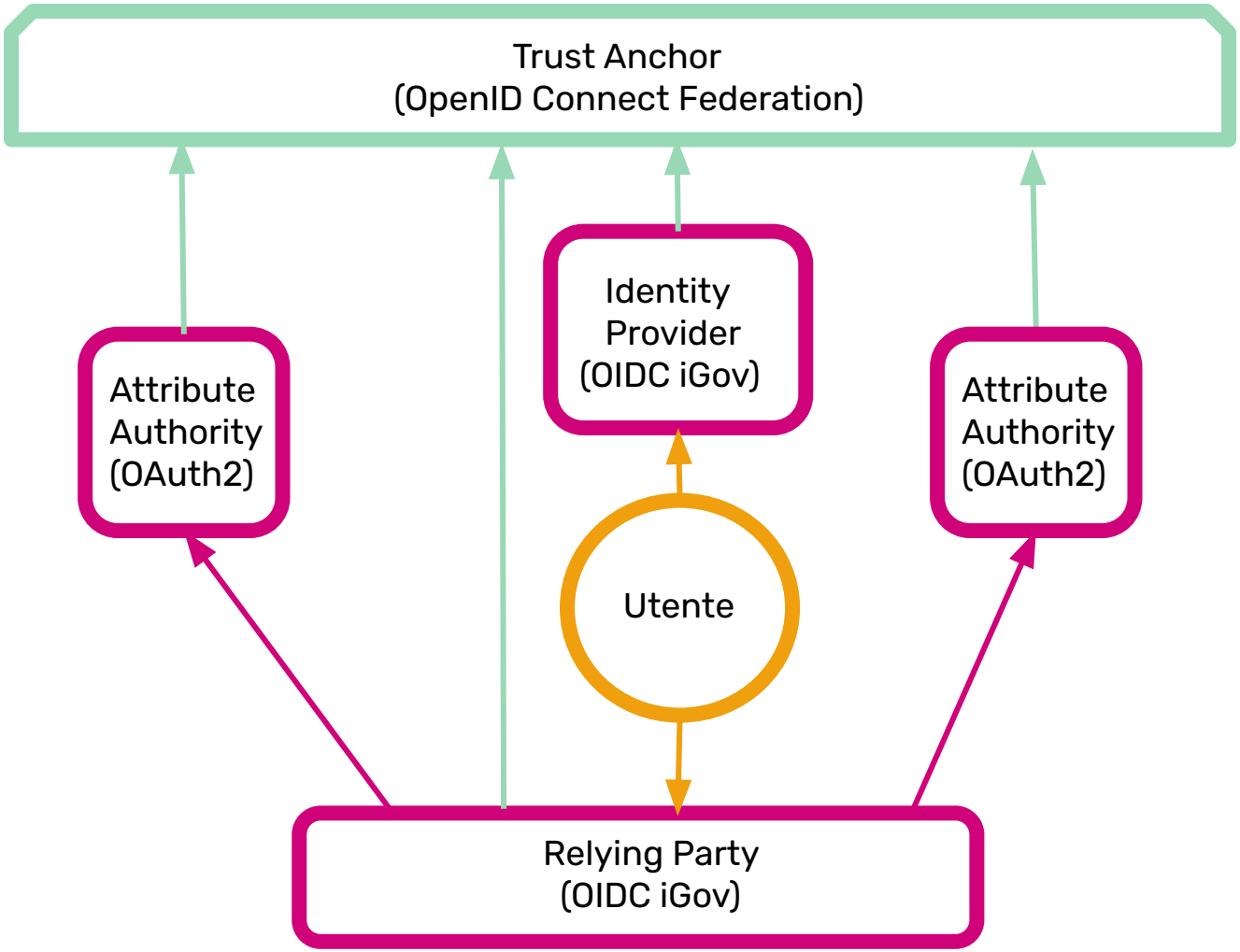
- OpenID Provider (**OP**), anche detto Identity Provider. Gestore della identità digitale dei cittadini.

- Trust Anchor (**TA**), anche detta autorità di federazione. Nel nostro caso AgID per SPID e Ministero dell'Interno per CIE id.

- Intermediario (**SA**), anche detto Soggetto Aggregatore. Organizzazione, riconosciuta dal Trust Anchor, che accredita RP SPID o CIE id mediante un proprio sistema di onboarding.

- Attribute Authority (**AA**) gestore degli attributi degli utenti. Rilascia gli attributi di un utente ad un **RP** di fiducia con il consenso esplicito dell'utente.

Attribute Authorities overview



Flusso di autenticazione e rilascio di attributi

1. L'**utente chiede** ad un RP **di essere autenticato**, selezionando l'OP che gestisce la sua identità digitale.
2. Il RP include nelle richiesta le AA che necessita di interrogare per l'espletamento delle sue funzionalità estese.
3. Il **OP autentica il RP** e le AA mediante Federation 1.0 e valida la richiesta, la pagina di autenticazione viene presentata.
4. **L'utente immette le proprie credenziali**, consente all'invio dei propri attributi dall'OP al RP **e consente al RP di interrogare le AA**.
5. L'OP rilascia il codice di autorizzazione e in seguito i Token (Access, ID e un Grant per ogni AA consentita dall'utente).
6. **Il RP ottiene gli attributi dell'utente e i Grant Token.**
7. Il RP si autentica sulla AA e sottomette il Grant Token.
8. **La AA** valida la richiesta e il Grant Token, e **rilascia il suo Access Token** corrispondente alle proprie policy (Bearer, DPoP, exp …).
9. **Il RP consuma le risorse OpenAPI della AA** con il Token appena rilasciato e per conto dell'utente.

International Government Assurance Profile (iGov) for OpenID Connect 1.0

Che cos'è?

- Profilo implementativo di OpenID Connect Core 1.0 che migliora la sicurezza e le buone pratiche in una specifica consolidata.

Cosa fa?

- Definisce le risorse (endpoint) e i formati delle richieste e delle risposte HTTP affinché due organizzazioni (RP e OP) possano autenticare e condividere gli attributi di un utente in sicurezza e sotto il controllo del soggetto interessato.

Cosa stiamo facendo per OIDC iGOV?

- Partecipiamo attivamente allo sviluppo della specifica per la pubblicazione di DRAFT 4 e suoi successivi.

OpenID Connect 1.0 Federation 1.0

Che cos'è?

- Standard per la costruzione di una federazione OIDC e OAuth2.

Cosa fa?

- Specifica come i partecipanti di una federazione, nei ruoli di Client, RP, OP, AS, RS e Intermediari (Soggetti Aggregatori), ottengono i metadata gli uni degli altri con la garanzia di una terza parte fidata (Trust Anchor) che definisce le regole e le politiche. Definisce una API di federazione, una infrastruttura interattiva della fiducia.

Cosa stiamo facendo per OIDC Federation 1.0?

- Partecipiamo attivamente allo sviluppo della specifica, dal DRAFT 17 ad oggi (DRAFT 24).

Attribute Authorities (OAuth2)

Che cosa sono?

- Profilo implementativo per l'arricchimento degli attributi utente all'interno dei sistemi di identità digitali SPID e CIE, con il requisito della privacy e della consapevolezza dell'utente.

Cosa fa?

- Specifica come un RP chiede l'autorizzazione ad un OP per acquisire gli attributi gestiti da organizzazioni di terze parti e aderenti alla federazione delle identità digitali nazionali. Il consenso dell'utente viene firmato digitalmente in un token ad-hoc denominato Grant Token.

Cosa stiamo facendo per i Grant Token in OAuth2?

- partecipiamo in IETF (Internet Engineering Task Force) per la standardizzazione degli Embedded Token.

Casi d’uso e scenari implementativi

- **Sistema gestione deleghe**
  DECRETO 30 marzo 2022, Disciplina delle modalità di funzionamento del Sistema di Gestione Deleghe («SGD») (22A04328) (GU Serie Generale n.180 del 03-08-2022).

- **Affiliazioni** organizzative.

- Certificazioni, **attestazioni** firmate.

- Non solo attributi: **risorse computazionali**.

Le risorse (RS) delle AA sono rappresentabili mediante OpenAPI. Le AA definiscono l’infrastruttura autorizzativa (AS). I RS possono essere implementati con estrema libertà perché avulsi dai metodi di approvvigionamento delle autorizzazioni e del token di accesso.

Ci sono domande?

Contribuisci insieme a noi alle specifiche tecniche:

Regole Tecniche SPID e CIE id OpenID Connect:
https://github.com/italia/spid-cie-oidc-docs

Specifica iGov
https://bitbucket.org/openid/igov/

Specifica Federation 1.0
https://bitbucket.org/openid/connect/

Specifica Embedded Tokens
https://github.com/rifaat-auth0/ietf

Domande e risposte #1

Q0: Quando sarà possibile accreditarsi all'interno di SPID OIDC?
A0: AgID - Gennaio 2023, attività pilota da Dicembre 2022.

Q1: Le AA sono usabili anche in **SAML2 o esclusivamente in OpenID**?

A1: Le LLGG SPID AA contengono un profilo SAML2 per il rilascio dei Grant Token nella SAML2 response, tuttavia non esistono ad oggi profili implementativi SAML2 delle AA. **Le interazioni con le AA sono esclusivamente OAuth2 sia per OpenID che per un'eventuale implementazione SAML2**.

Q2: **Perché l'OP rilascia i Grant Token** piuttosto che direttamente gli attributi estesi ottenibili dalle AA?

A2: Gli Identity Provider non devono ottenere le informazioni degli utenti oltre a quelle già in loro possesso.

Domande e risposte #2

Q3: **Perché** ottenere un nuovo token da parte delle AA e **non usare direttamente l'Access Token rilasciato dall'OP**?
A3: Perché:

1. **Tante AA** otterrebbero il medesimo Access Token e **potrebbero riutilizzarlo verso altre AA**. I RS devono autenticare il RP ed evitare che una terza AA possa riutilizzare un Access Token. Il token deve essere *sender-constrained* e aderente alle policy interne della AA che lo ha emesso, in termini di prova di possesso, durata …

2. Ogni AA può funzionare con livelli di sicurezza superiori ai requisiti minimi e con policy proprie. **La AA non riconosce access token non emessi da lei**. Il Grant Token trasporta esclusivamente la prova del consenso avvenuto e le informazioni minime necessarie per la AA di destinazione (*audience-constrained*).

Domande e risposte #3

Q4: **Perché non** avete usato **Aggregated o Distributed Claims di OpenID**?
A4: Perché:

1. Ogni AA può funzionare con livelli di sicurezza superiori ai requisiti minimi e con policy proprie. **La AA non riconosce access token non emessi da lei**.
2. **Le AA consentono l'erogazione di risorse complesse e non solo di attributi OpenID o OpenID 4 IDA**.
3. Il modello AA è pensato per risorse distribuite su domini diversi e afferenti ad organizzazioni diverse.

Domande e risposte #4

Q5: Che **differenza** c'è **tra AA e PDND**?

A5: **AA è user-centric**.

1. Le AA hanno il **requisito del consenso dell'utente** e del controllo sulle transazioni che lo riguardano.
2. PDND è una infrastruttura di interoperabilità dove le interazioni avvengono tra organizzazioni diverse e mediante stipule di convenzioni. Il consenso dell'utente non è richiesto.
3. Nelle AA **il rapporto di fiducia con Entità afferenti al settore privato e pubblico si equivalgono**, perché il flusso è sotto il controllo dell'utente e niente può accadere senza il suo consenso e non oltre il tempo limitato alla sessione di autenticazione.