The INDIGO-DataCloud AAI

A. Ceccanti, M. Hardt, B. Wegh, P. Millar, S. Licehammer, M. Caberletti, E. Vianello

The INDIGO **Authentication and Authorization Infrastructure** (AAI) leverages and extends existing standards (OpenID Connect, OAuth2, SCIM) to enable secure composition of resources from multiple providers in support of scientific applications. The central **Identity and Access Management** (IAM) service provides tools to implement brokered user authentication, identity harmonization, account linking as well as Virtual Organization (VO) management. Identity information is provided to relying services via **OpenID Connect,** which allows simpler integration in off-the-shelf software. The **Token Translation Service** (TTS) integrates services that do not directly support OpenID Connect, by creating credentials on-demand from the identity information provided by the IAM. This poster introduces the main INDIGO AAI components and highlights the main architectural decisions that were taken during the first year of the INDIGO project.

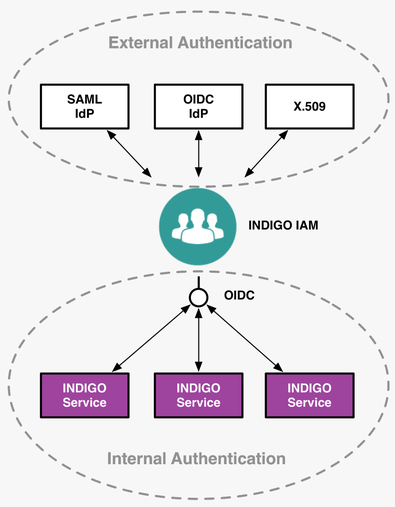
1. Identity = OpenID Connect

The **INDIGO** [1] **AAI** Identity layer leverages the **OpenID Connect** [2] standard to provide user authentication and identity information to INDIGO services. This approach provides several advantages:

- Standardized and widely adopted solution
- Accommodation of several authentication mechanisms (via identity brokering)
- Simplified integration in relying services
- Native support for delegation and offline access
- Native support for dynamic client registration

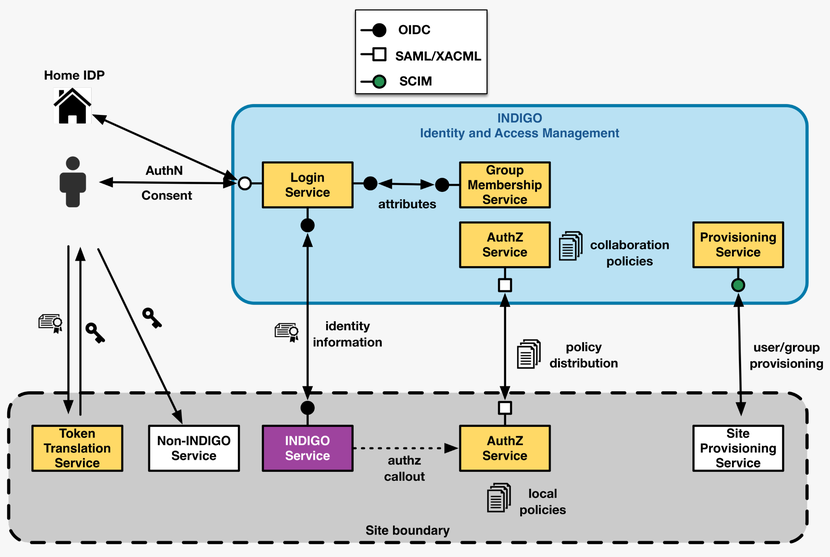
2. Identity harmonization and brokering

The **INDIGO Identity and Access Management (IAM)** [3] service deals with user authentication and identity brokering, allowing users to authenticate with local username and password, SAML, X.509 certificates, or via a remote OpenID Connect provider (e.g., Google). The different identities are linked to a single INDIGO user profile, which provides each user with a **unique, persistent identifier**. This identifier is then used for auditing, accounting and authorization at all relying services. Other attributes, like group membership information, can be linked to the user profile, and then exposed to relying services via standard **OpenID Connect i**nterfaces.



3. Authorization = OAuth 2 + XACML

INDIGO services expose functionality through HTTP APIs protected by **OAuth 2** [4]: only agents presenting a valid and trusted **OAuth access token** are granted access to INDIGO services. This token is obtained by client applications from the **INDIGO IAM service** and provides access to identity information (e.g., group membership and other attributes) and other authorization information (e.g., OAuth scopes). Fine-grained, powerful and distributed attribute-based authorization is implemented by integrating the **Argus authorization service** [5] with the INDIGO AAI identity layer. This provides policy distribution and centralized XACML policy management.



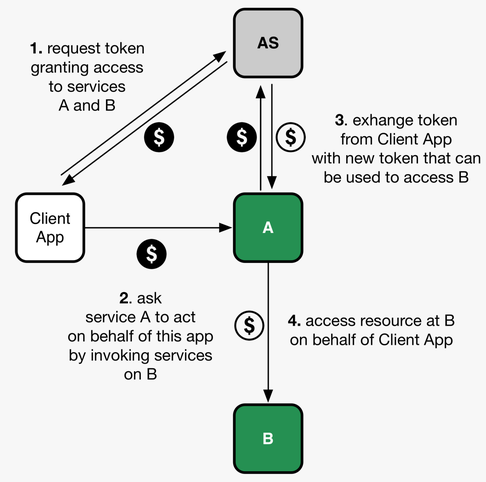
4. Identity provisioning

INDIGO IAM leverages the standard **System for Cross Domain Identity Management (SCIM)** [8] version 2.0 to implement identity provisioning, de-provisioning and management.

The SCIM APIs provides means to **propagate identity and group information to relying services**, to implement, for instance, **dynamic account creation and other resource lifecycle management at various levels of the INDIGO infrastructure** depending on events related to user identity status.

5. Delegation and offline access

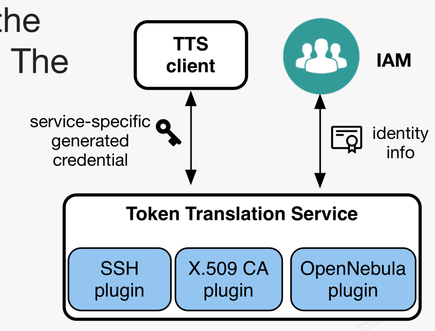
OAuth and OpenID Connect **support delegation and offline access natively**. To support **chained delegation across services**, in which a component can act both as a service and as a client for another downstream service, the INDIGO IAM provides a partial implementation of the **OAuth token exchange draft standard** [6]**.**
The token exchange is used in particular to implement **controlled delegation of offline access rights across applications** (i.e., the ability to execute tasks on behalf of a user while the user is not connected).



6. Token translation and non-HTTP services

INDIGO AAI integrates services that rely on different authentication mechanisms (e.g., X.509 certificates, SSH keys, Amazon S3 keys) via the **INDIGO Token Translation Service (TTS)** [7].
The **TTS** translates an OpenID Connect authentication assertion, like the one issued by the IAM service, into one of the supported downstream service credentials. The TTS currently supports the generation of:

- SSH keys
- X.509 certificates
- OpenNebula username/password credentials



7. References

1. The INDIGO-DataCloud project: https://www.indigo-datacloud.eu/
2. OpenID Connect: http://openid.net/connect/
3. INDIGO Identity and Access Management: https://github.com/indigo-iam/iam
4. OAuth 2: https://tools.ietf.org/html/rfc6749
5. Argus Authorization Service: http://argus-documentation.readthedocs.io/en/latest/
6. OAuth token exchange draft standard: http://bit.ly/oauth-token-exchange
7. The INDIGO Token Translation Service: https://github.com/indigo-dc/tts
8. SCIM: http://www.simplecloud.info/

INDIGO - DataCloud receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement RIA 653549