Identity Federations in Practice – Atlases

M. Procházka, J. Feit, L. Matyska, L. Hejtmánek, et al.

CESNET, a. l. e., Prague; Institute of Compt. Science, Masaryk University, Brno

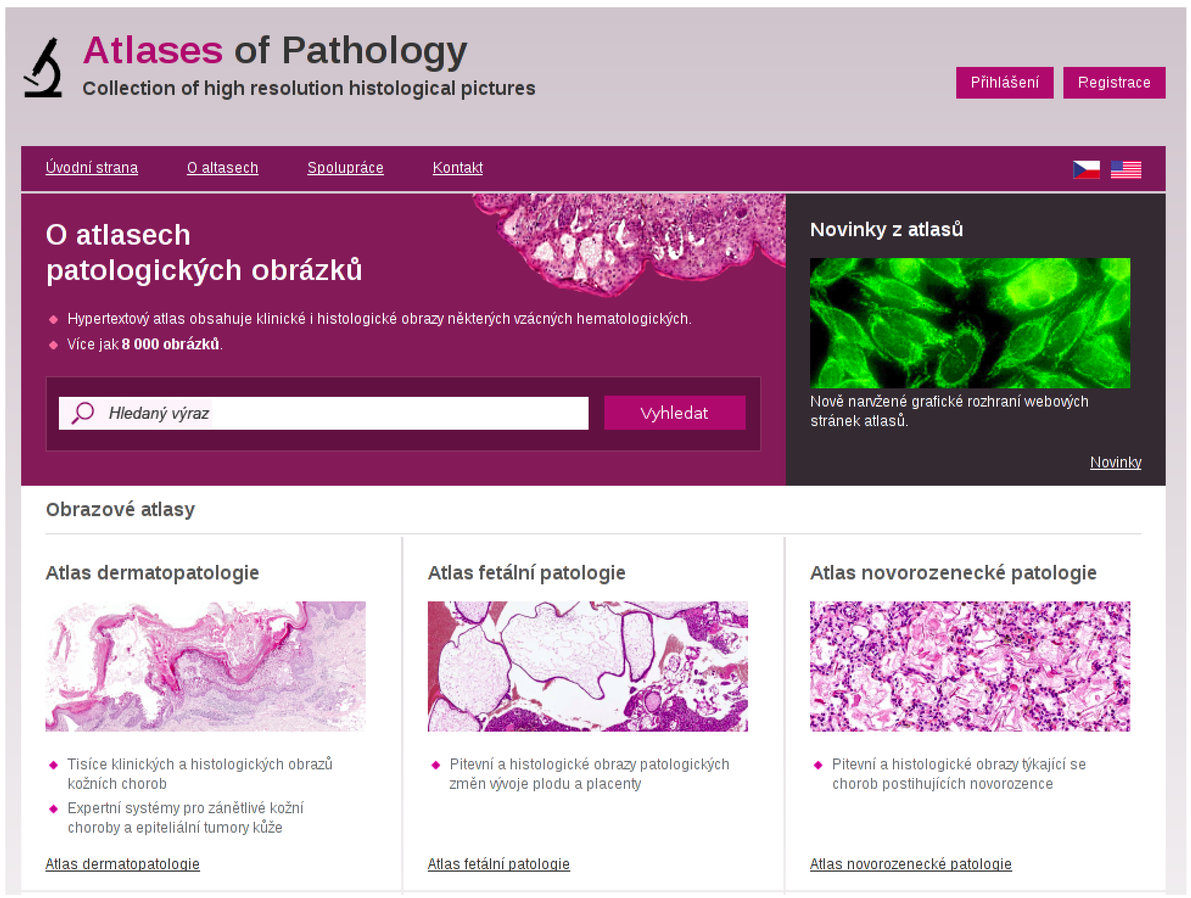
Atlases - Pathology Images

A unique collection of thousands images from various fields of pathology medicine. The set contains microscopic images that are taken in very high resolution, which is extended on regular basis. The images collected are access using a virtual microscope available from common web browsers. The physicians who are working with the pictures also add additional annotations providing more information about the diseases studied.

The use of Atlases is free of charge but user registration is required. In order to not force users to create yet another account, Atlases accept users' federated identities.

List of joined identity federations

- more than **27000** registered users
- connected to **16** identity federations across the globe
- around **2000** users using federated identity
- more than **6300** images and still growing



Atlases new main page

Identity Federations

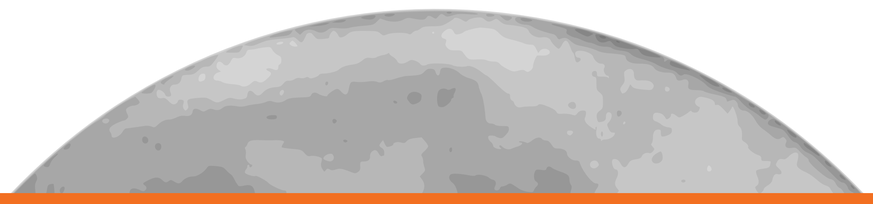
Identity federations are becoming more and more popular and deployed as new means to prove our identity in the digital world. Although current federations target mainly web application, also grids and clouds try to leverage from the federated identities, which is not always easy. As we have learned during several years of operating the Atlases, current identity federations also reveal their drawbacks and limitations.

Drawbacks of Current Identity Federations

- huge administrative overhead associated with setting a trust relationship between end services and national identity federations
- significant effort is needed to maintain service provider subscription in the joined identity federations
- registration of a service provided with an identity federation is a long and difficult process. Potential users of the service have to wait until the whole process has been finished.
- A users' access to the service depends on their identity provider being on-line all the time. If the identity provider is not available, the users' cannot use any service even though they are running smoothly.
- The user's identity provider is legally liable for the information disclosed about the user to service providers.
- Users cannot combine attributes from multiple identity providers.
- Users cannot affect identity provider attribute release policy.

Moonshot

MetaCentrum and CESNET are also involved in project Moonshot that brings advantages of identity federations to a broad range of non-Web services. CESNET participates in the project mainly on integrating the technology with Grid tools (e.g. for on-line CAs) and with distributed file systems.

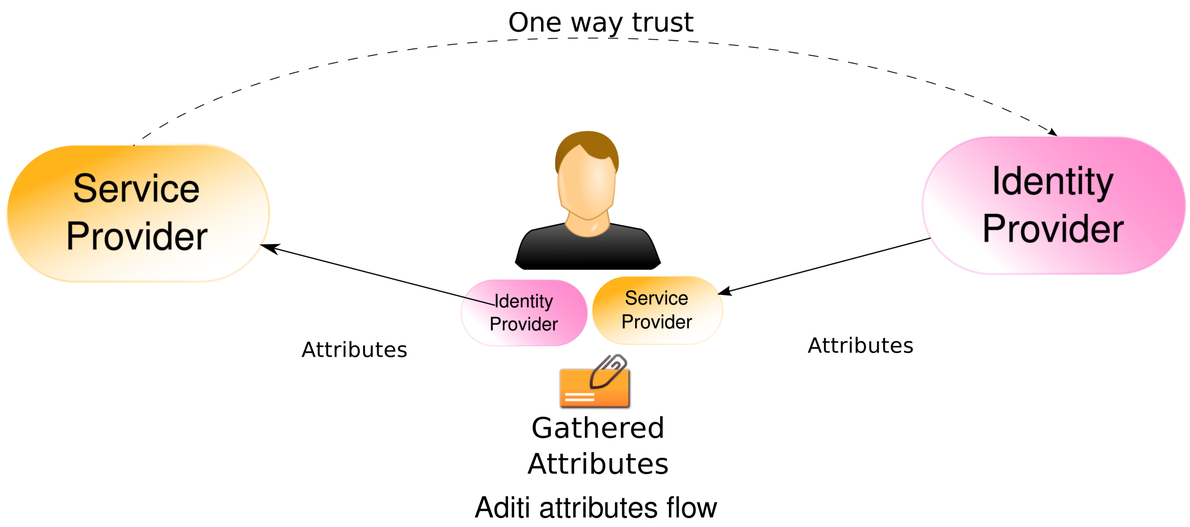


Aditi

In order to overcome the drawbacks of current identity federation we have designed system *Aditi*, which puts the users in the center. Every piece of information from the identity provider flows through the user, so they can manage it on their own.

Simplified data flow in Aditi:

1. The user requests all attributes from their identity provider(s), every single attribute is digitally signed by the identity provider.
2. User can combine attributes into personal *cards* (a set of attributes required by service providers)
3. The appropriate card is sent to the service provider, which checks the trustworthiness of each attribute



Aditi attributes flow

Aditi Advantages

This approach has several advantages compared to the common identity federations:

- Identity providers do not need to maintain any trust with service providers
- Identity provider releases information about the user only to them, without any privacy issues
- The user decides about which attributes from which identity provider will be released to the service provider
- The user can combine attributes from different identity providers
- The user can add their own attributes to cards
- Service providers maintain trust with the identity providers only
- Solution can be integrated with current SAML-based identity federations

http://atlases.muni.cz
http://metacentrum.cz
atlases@ics.muni.cz

MetaCentrum is supported by project CESNET Large Infrastructure, which is part of the programme Projects of Large Infrastructure for Research, Development, and Innovations funded by the Ministry of Education, Youth, and Sports of the Czech Republic.