Report of the collaboration with the SATOSA project

During the deployment phase of a service provider demo of the "SATOSA as IdP of last resource" project, we tested two different backends to see the viability of each of them.

OpenId Connect Backend

This should be the best option, but ORCID does not support email scope right now. ORCID is working on enabling per-client email release during OAuth workflow. This functionality they said should be available at some point in 2020. Until that this is not a valid option.

ORCID Backend

SATOSA has a specific ORCID backend that uses its API to obtain some attributes that are not acquired during the OAuth workflow. Specifically the email address.

During the testing and deployment demo of this backend, we detected some issues:

a) ORCID API has two authentication methods. The first seems like a legacy method that requires two different HTTP headers (*Authorization Type* and *Access Token*). The second is the standard *Bearer token* sent inside the *Authorization* header. The first method does not work in the sandbox API. The second works in all ORCID environments. SATOSA is using the first method, so the backend wasn't working in the sandbox environment.
b) ORCID backend reads from the ORCID API two user attributes: email and address (if available). The way address is read has a bug.
c) ORCID OAuth workflow supports state parameter, but SATOSA backend is not using it.

In order to fix this issues, two Pull Request was sent to the SATOSA repository in Github.

Pull Request 1: Fixed orcid authentication and access to API issues #282 (https://github.com/IdentityPython/SATOSA/pull/282)

This PR resolves issues a and b. An unit tests was sent with the implementation.

Pull Request 2: Add state parameter to ORCID authorization request #284 (https://github.com/IdentityPython/SATOSA/pull/284)

This PR resolves issue c. Other improvements were made:

- Removed start_auth method to use it from base class.
- Added get_request_args method to compose the authorization uri inside base start_auth method.
- Refactorized _authn_response method. Now is very close to base method. The only difference is that auth_info requires two more attributes from the authorization response (orcid and name). But base method only sends access_token. A user_info base method refactorization could resolve this in a way than _authn_response does not need to be overloaded.
- ORCID test was modified too to check state parameter.