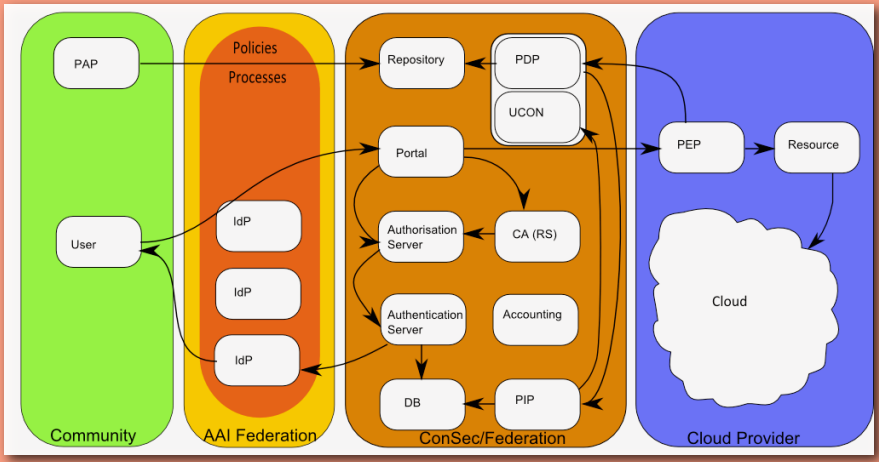
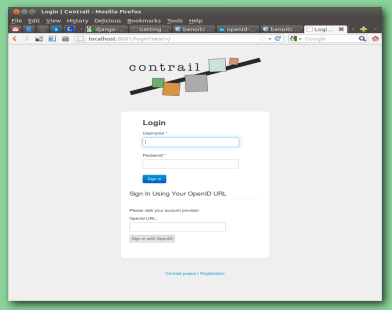


ConSec federated security architecture

ConSec features

The diagram above, at a high level, sketches the advantages of ConSec (the third box in orange.) From left, we have the user's community, either based on a Contrail use case or another collaboration in another project, the role the user adopts when making use of cloud resources. The yellow box denotes the identity management federation, wherein acceptable use policies are defined, and identities are managed. In the simplest case, it could just be a single identity provider, such as a public cloud or social network identity.

In the more complex cases, they could be a full national identity management federation with rules and processes, and the IdP would be provided by the user's employer or university, thus providing a high level of assurance. ConSec is able to simultaneously manage credentials at a different level of assurance, passing the information to the resource. The third box is ConSec itself, which is managing most of the complexity of the authentication and authorisation; and finally, in the fourth box, the resource, with enforcement of access control and access to the resource as well.



contrail
open computing infrastructures for elastic services

Contrail Security

ConSec

Federate Cloud security

Science & Technology Facilities Council

http://contrail-project.eu/consec

ConSec is reusable on complex e-infrastructures

Reusable

One thing is solving problems for Contrail, another thing is to provide reusable and sustainable code which solves problems for others as well. Like many other parts of Contrail, ConSec aims to be modular, so components can be replaced, left out, reused, upgraded, etc. Indeed, ideally ConSec would provide a framework which enables any e-infrastructure provider to make use of federated (i.e., external) identity management. Whenever possible, ConSec itself is built out of standard components using standard protocols.

EUDAT | egi | contrail |

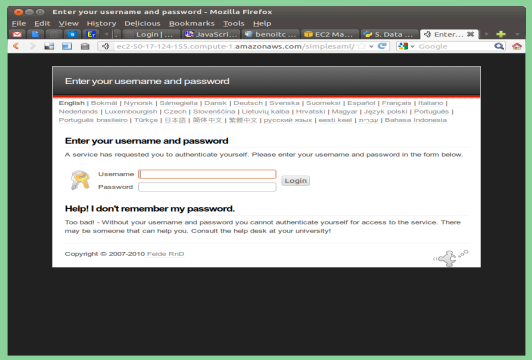
http://contrail-project.eu

ConSec Technical description

In practice, multiple technologies are combined to solve problems. The user's initial interaction with the service is via a portal, and authentication is usually web-based, using either OpenID or SAML SSO (such as Shibboleth).

Within the federation, everything is SOA, and REST web services are used. In order to carry authorisation information with the HTTP headers, we use OAuth2 to delegate the rights to access federation-level services on behalf of users.

The portal will then typically choose to create an X.509 certificate which it manages on behalf of the user: this is because OAuth2 access token carries little information, because services are not in general web services based, because not all services can validate an access token, and because we need more fine grained authorisation data.
The user generally never sees the certificate, but it is used to access



services on their behalf, and the embedded authorisation assertion is used to check the access control via a standard XACML framework. Contrail moreover has implemented an extension to the PDP, called UCON in the diagram (for "usage control") which can re-evaluate an access control decision when the values of attributes change.

If the decision also changes, the PEP is notified of the change, and can suspend or terminate cloud activities. This is useful for "volatile" attributes, such as reputation and the remaining funds in prepaid accounts.

Aims of ConSec

The aim of ConSec is to provide a means for users to use external identities to authenticate to service providers: any acceptable external identity can be used to identify users to any internal service managed by the federation.

The user thus gets single sign-on: that an identity used for other purposes can be used with any federation resource, and, depending on the timing and technology used, will only need to log in once.

And the advantage for the federation operator is that they do not need to worry about allocating (and resetting) user passwords and keeping account records up to date. Finally, the resource provider gets at least an extra level of assurance, that authentication data used by the user for other resources is less likely to be shared with other users, and may even be subject to federation policies.

ConSec is developed in the Contrail project. Contrail is a project managed by the Contrail consortium. It develops a stack of federated Cloud computing tools that can work together.

Contrail is partially funded by the FP7 Programme of the European Commission under Grant Agreement FP7-ICT-257438.

contrail