TCS Portal Project

TCS Portal Project description

Mailinglists

tcs-portal-core

tcs-portal

tcs-portal-reps

Portal software

The portal uses the tailor made Confusa software.

Participants

ACOnet, CSC, CESnet, Forskningsnettet, GARR, RENATER, SUnet, SURFnet, UNINETT

Project organisation

Project coordination: Jan Meijer

Operations: Teun Nijssen, Thijs Kinkhorst

Software development: Henrik Austad, Thomas Zangerl

Portal technical

-uptime (99.8x on 99.9x infra), 17 hours unscheduled downtime

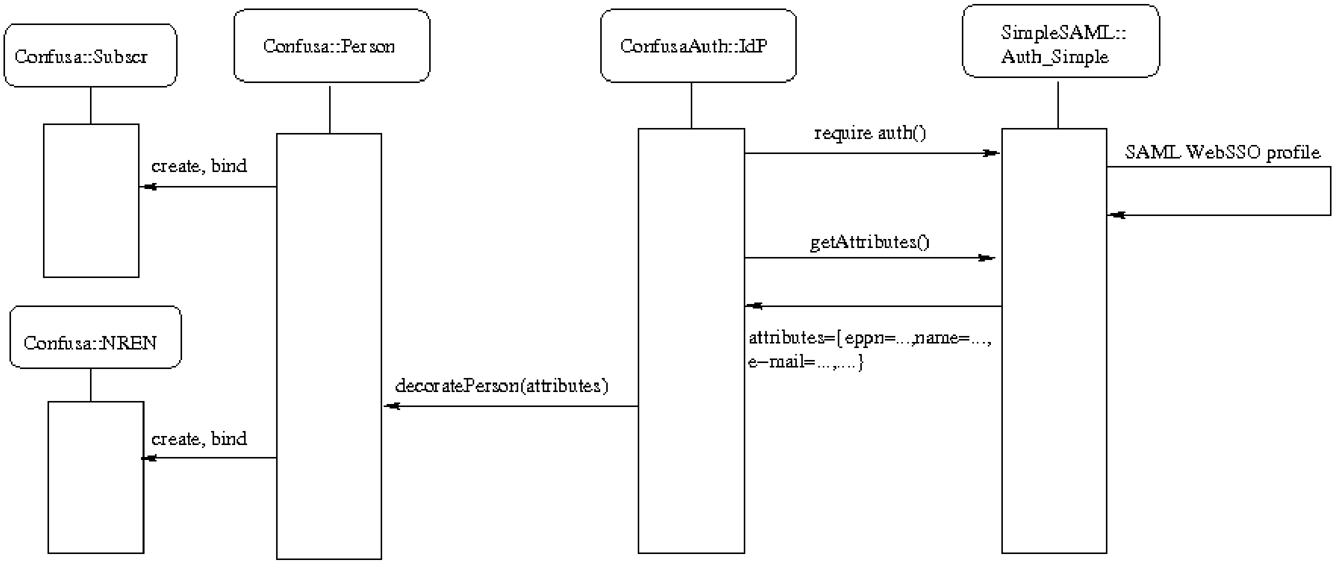
-description

-2x2 virtual machines on separate physical hardware

Workflows

Workflow upon authenticating users

Confusa's authentication mechanisms are largely based upon simpleSAMLphp. simplesamlphp is a server software written in PHP, implementing, among other things, SAML SPs, SAML IdPs, metadata handling and IdP discovery. Confusa's framework hooks into the simpleSAMLphp authentication classes to establish the identity of the user. Once Confusa receives the attributes of the end-user, it "decorates" a specific model class, called Person with the obtained attributes. This process is shown here:



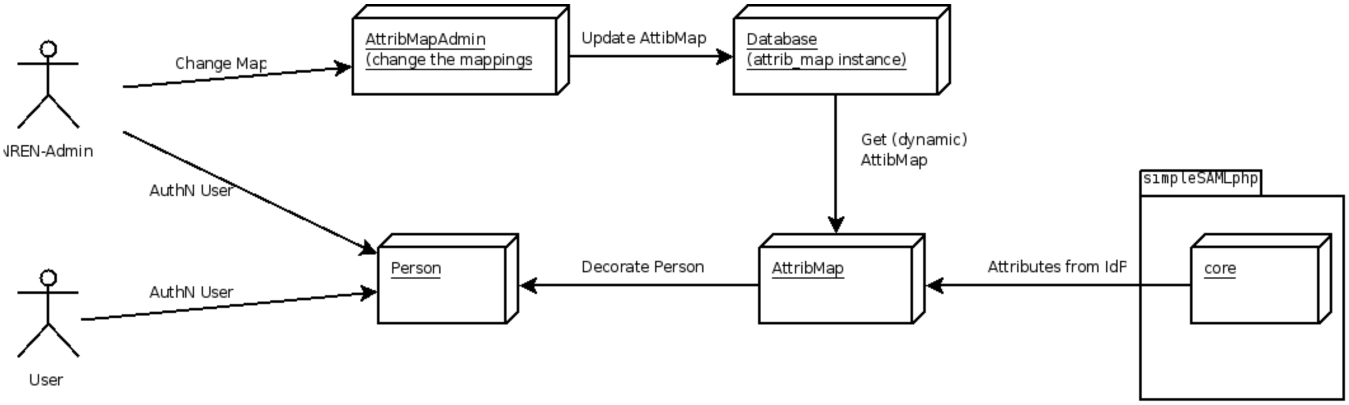
All other classes of Confusa will attempt to retrieve end-user identity information from that shared class. Due to the fact that Confusa is written in PHP and objects do not persist in PHP between two successive site views, the decoration happens on every site-rendering. Thus we can ensure at every access attempt of resources that the user is still freshly authenticated.

Attribute consumption in the cross-federated setup

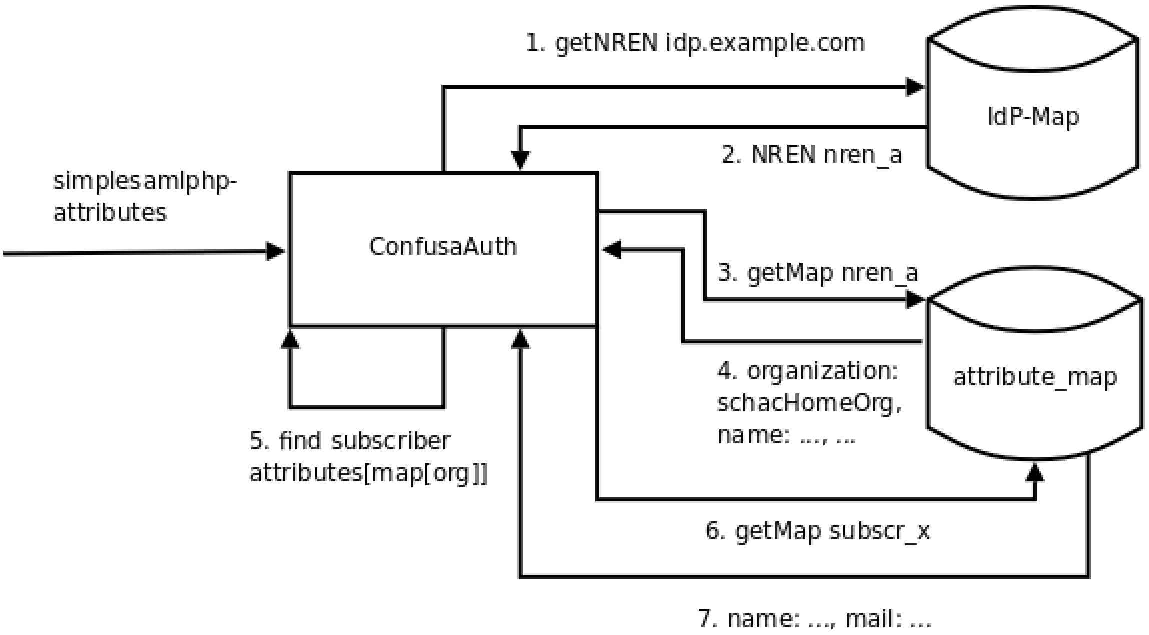
Accepting attribute heterogeneity, Confusa offers subscriber and NREN administrators the possibility to define their own mapping from the required information to federation attributes. The map will be stored in connection with the
NRENs and consulted upon Person decoration (see above). The following algorithm is used to decorate the central Person object with the correct attributes (see also the graphic below):

1. Confusa needs to know the NREN associated with the user at authentication time. For this a static mapping from IdP URLs to NREN names is used.
2. Now the NREN mapping can be retrieved from the database.
3. The attribute mapping of the user's NREN is returned from the database. From this point on, the attribute mapping of the organization name will stay fixed.
4. Using the organization mapping, the organizational affiliation is determinded from the attributes. This organization will be used to query the DB again for a subscriber-mapping which overrides the NREN mapping for all attribute-names except the organization-name and the entitlement.
5. If a subscriber mapping is found, the person will be decorated from the simplesamlphp attributes using the attribute-names defined in the subscriber-mapping. If there is no subscriber mapping in the DB, the NREN-mapping will be used.

Definition of Confusa's attribute map:

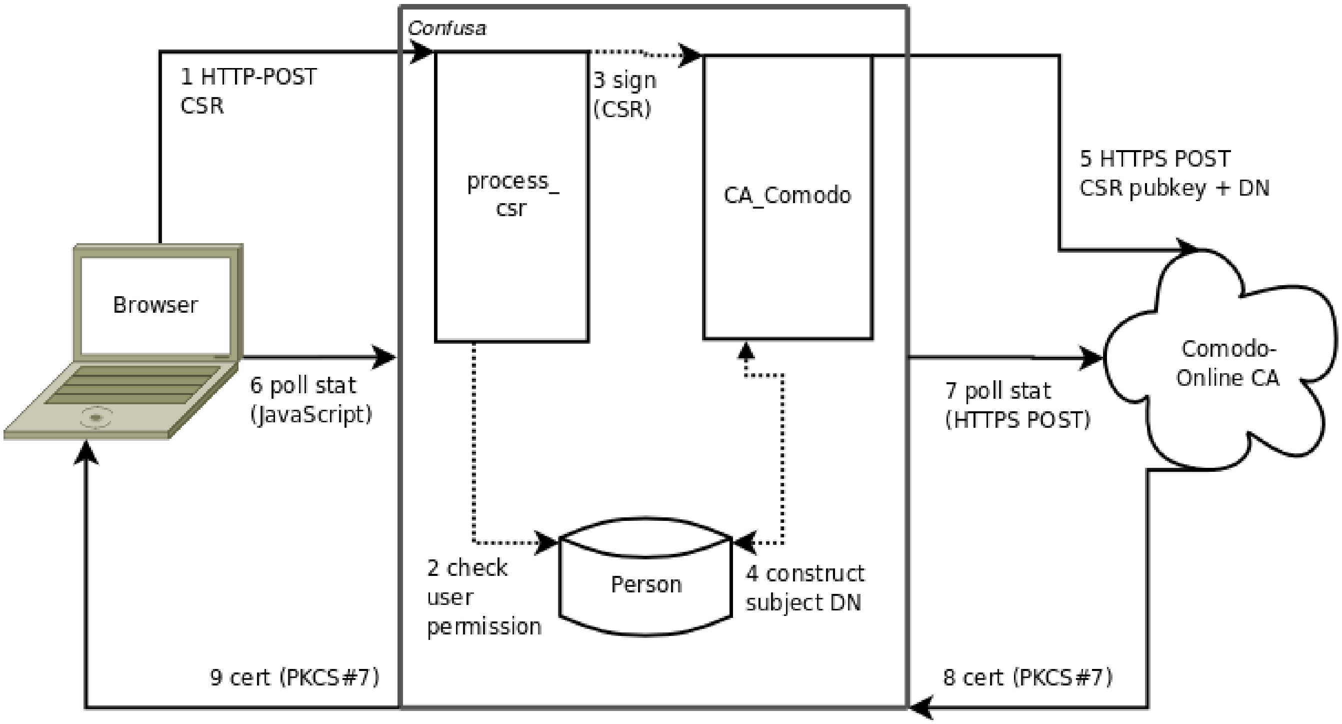


The person decoration process using the attribute map:



Certificate request workflow

The following graphic illustrates the data flow in Confusa upon certificate request:



Especially noteworthy is the fact that the original subject-DN of the certificate signing request is not preserved. Instead the subject-DN is constructed from the decorated Person object, as described in the section "Workflow upon authenticating users".