|  |  |  |
| --- | --- | --- |
| **Title** | Proposal for Identity Provider blacklist |  |
| **Version** | 1 |
| **Author(s)** | Dieter Van Uytvanck |
| **Date** | 2019-08-15 |
| **Status** | Draft |
| **Distribution** | SCCTC, Public |
| **ID** | CE-2019-1487 |

# Introduction

Frequently, CLARIN ERIC receives support request from researchers trying to use federated login to reach resources in CLARIN centres. In many cases, the login problems are caused by Identity Providers not releasing attributes that can uniquely identify a user (ePPN or ePTID).

For services that need to store user-specific settings, like consent to a specific license or account settings, this poses a problem. Also, for the person trying to login this leads to frustration, since the requested resource cannot be reached, and this only becomes clear after providing the username and password. In such cases a CLARIN account needs to be requested.

In case of attribute release problems, the administrators of the respective Identity Provider are contacted by the Service Provider operator and/or CLARIN ERIC, with some background information and the polite request to release the necessary attributes, in line with the recommendations as listed at:

* <https://www.clarin.eu/content/attributes-service-provider-federation>
* [https://doku.tid.dfn.de/de:shibidp3attrfilter#freigabe\_der\_wichtigsten\_attribute\_fuer\_clarin-sps](https://doku.tid.dfn.de/de%3Ashibidp3attrfilter#freigabe_der_wichtigsten_attribute_fuer_clarin-sps)

In many cases, this leads to interaction with the Identity Provider and eventually to a functioning attribute release.

In some cases, this does not lead to a satisfactory outcome, when either:

* no response is given (even when 2 reminders are sent)
* the Identity Provider indicates that personal attributes will not or cannot be released
* the Identity Provider requires additional and unscalable administrative steps, like additional forms that need to be signed by the Service Provider

Since 2016, the outcomes of these interactions are systematically tracked.

#  Suggested next step

In case an Identity Provider is contacted about lacking attribute release, and it turns out to be consciously unwilling to release attributes that enable to uniquely identify a user, CLARIN should blacklist the Identity Provider by:

* Adding it to a machine and human readable online list
* Removing it from its SAML metadata feeds
* Removing it from its central discovery service
* Informing the Identity Provider about this blacklisting and the possibility to be removed (upon change of the attribute release policy).

# Initial candidates for blacklisting

Based on the interactions with Identity Providers during 2018 and 2019 the following Identity Providers could be blacklisted:

|  |  |
| --- | --- |
| **Name** | **Reason** |
| Freie Universität Berlin | Unresponsiveness (5 mails) |
| Technische Universität Dresden | Unscalable administrative requirements (signing forms per service provider) |
| Universität Duisburg-Essen | Unresponsiveness (3 mails) |
| University of Stuttgart | Unresponsiveness (after several emails and contact attempts by the local CLARIN centre) |

To put things into context, this would mean 4 out of 1870 Identity Providers would be blacklisted initially. This list could of course grow over time.