The Hunt For Red IdPs

Lukas Hämmerle
Task Leader "Enabling Users"
GÉANT/SWITCH

eduGAIN Town Hall Meeting, Vienna
1. December 2015
The Mission Scenario

- Nice increase of eduGAIN IdPs
  - Also thanks to move from opt-in to opt-out 😊

- But many eduGAIN IdPs don't "work" 😞
  - Test when users select IdP to authenticate at an eduGAIN service
  - Poor perceived "service quality" of "eduGAIN" for users or SP admins

- That is what triggered ....
The Mission Objectives

1. Locate malconfigured eduGAIN IdPs
2. Provide a public listing of these IdPs
3. Inform federation operator about the issues
The Weapon of Choice

- Public web service similar like the CoCo monitor:

  **eduGAIN Connectivity Check Service (ECCS)**
  [https://technical.edugain.org/eccs/](https://technical.edugain.org/eccs/)

- For each eduGAIN IdP do the following check:
  - Initiate a login process from two eduGAIN SPs (except for disabled IdPs)
  - Check if a reasonable login page is returned
  - Classify error messages (Error = Red, Warning = Yellow)
  - Display results on a public web page

- The check seems easy but there are false positives:
  - The hub of Hub&Spoke federations often don't react like expected
  - HTTP Basic Auth, redirects with JavaScripts, strange TLS configurations, ...
  - There is an option to exclude IdPs or whole federations from checks
The Yellow Submar... ahm... Identity Providers

- Yellow IdPs = IdPs in category "Warning"
  - are probably working but they don't seem to consume eduGAIN metadata, i.e. they issue an error message that the test SPs are unknown

- Probably a configuration problem (e.g. no automatic metadata download)
  - False positive: Hub&Spoke federations where each IdP has to enable eduGAIN SP
# Yellow Identity Providers in Warning Category

## IdP Data

<table>
<thead>
<tr>
<th>Display Name</th>
<th>entityID</th>
<th>Registration Authority</th>
<th>Contacts</th>
<th>Last Test</th>
<th>Current Result</th>
<th>Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Northampton (IDP)</td>
<td><a href="http://idp.northampton.ac.uk">http://idp.northampton.ac.uk</a> /cafe/metadata</td>
<td><a href="http://ukfederation.org.uk">http://ukfederation.org.uk</a></td>
<td>T: <a href="mailto:mike.aynsworth@northampton.ac.uk">mike.aynsworth@northampton.ac.uk</a> S: <a href="mailto:mike.aynsworth@northampton.ac.uk">mike.aynsworth@northampton.ac.uk</a></td>
<td>2015-11-25 20:47:10</td>
<td>No-eduGAIN-Metadata</td>
<td>View</td>
</tr>
<tr>
<td>University of Sunderland</td>
<td><a href="http://sso.sunderland.ac.uk">http://sso.sunderland.ac.uk</a> /outh/metadata</td>
<td><a href="http://ukfederation.org.uk">http://ukfederation.org.uk</a></td>
<td>T: <a href="mailto:scott.sweeting@sunderland.ac.uk">scott.sweeting@sunderland.ac.uk</a> T: <a href="mailto:dean.hale@sunderland.ac.uk">dean.hale@sunderland.ac.uk</a> T: <a href="mailto:adil.khan@sunderland.ac.uk">adil.khan@sunderland.ac.uk</a> T: <a href="mailto:daniel.dixon@sunderland.ac.uk">daniel.dixon@sunderland.ac.uk</a> T: <a href="mailto:ian.frost@sunderland.ac.uk">ian.frost@sunderland.ac.uk</a> T: <a href="mailto:jan.lundell@sunderland.ac.uk">jan.lundell@sunderland.ac.uk</a> T: <a href="mailto:ian.frost@sunderland.ac.uk">ian.frost@sunderland.ac.uk</a> S: <a href="mailto:rachel.webb@sunderland.ac.uk">rachel.webb@sunderland.ac.uk</a> S: <a href="mailto:laura.wilkinson@sunderland.ac.uk">laura.wilkinson@sunderland.ac.uk</a> S: <a href="mailto:ian.frost@sunderland.ac.uk">ian.frost@sunderland.ac.uk</a></td>
<td>2015-11-25 20:47:11</td>
<td>No-eduGAIN-Metadata</td>
<td>View</td>
</tr>
<tr>
<td>FAMERP - Faculdade de Medicina de Rio Preto</td>
<td><a href="https://1010SE17FAM-V03.famerp.br/idp/shibboleth">https://1010SE17FAM-V03.famerp.br/idp/shibboleth</a></td>
<td><a href="http://cafe.mrp.br">http://cafe.mrp.br</a></td>
<td>T: <a href="mailto:joaomarcelo@famerp.br">joaomarcelo@famerp.br</a></td>
<td>2015-11-25 20:49:32</td>
<td>No-eduGAIN-Metadata</td>
<td>View</td>
</tr>
<tr>
<td>Wigan &amp; Leigh College</td>
<td><a href="https://access.wigan-leigh.ac.uk">https://access.wigan-leigh.ac.uk</a> /cafe/metadata</td>
<td><a href="http://ukfederation.org.uk">http://ukfederation.org.uk</a></td>
<td>T: <a href="mailto:lparr@wigan-leigh.ac.uk">lparr@wigan-leigh.ac.uk</a> T: <a href="mailto:a.unsworth@wigan-leigh.ac.uk">a.unsworth@wigan-leigh.ac.uk</a></td>
<td>2015-11-25 20:47:30</td>
<td>No-eduGAIN-Metadata</td>
<td>View</td>
</tr>
</tbody>
</table>

## Statistics

201 (13.6%) yellow IdPs of 1481 (30.11.2015)
• Have a more serious configuration problem or are not reachable

• False positive: E.g. host temporarily not down or not reachable (behind firewall)
# Red Identity Providers in Error Category

<table>
<thead>
<tr>
<th>Display Name</th>
<th>entityID</th>
<th>Registration Authority</th>
<th>Contacts</th>
<th>Last Test</th>
<th>Current Result</th>
<th>Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hogeschool de Kempen</td>
<td>ADFS01.KEMPEL.NL/ADFS/Services/Trust</td>
<td><a href="http://www.surfconext.nl/">http://www.surfconext.nl/</a></td>
<td>T: <a href="mailto:support@surfconext.nl">support@surfconext.nl</a>, S: <a href="mailto:help@surfconext.nl">help@surfconext.nl</a></td>
<td>2015-11-25 20:49:05</td>
<td>OK</td>
<td>FORM-invalid, No-educGAIN-Metadata, HTTP-Error, CURL-Error</td>
</tr>
<tr>
<td>University College South Denmark</td>
<td>BFJACK-FILES.BU.OCDI.CA/ADFS/Services/Trust</td>
<td><a href="https://www.wayf.dk">https://www.wayf.dk</a></td>
<td>T: <a href="mailto:drift@wayf.dk">drift@wayf.dk</a></td>
<td>2015-11-25 20:49:29</td>
<td>HTTP-Error</td>
<td>View</td>
</tr>
<tr>
<td>Design School Kolding</td>
<td>BFJACK-FILES.BU.OCDI.CA/ADFS/Services/Trust</td>
<td><a href="https://www.wayf.dk">https://www.wayf.dk</a></td>
<td>T: <a href="mailto:drift@wayf.dk">drift@wayf.dk</a></td>
<td>2015-11-25 20:45:11</td>
<td>HTTP-Error</td>
<td>View</td>
</tr>
<tr>
<td>NHTV Brede University of Applied Sciences</td>
<td>BFJACK-FILES.BU.OCDI.CA/ADFS/Services/Trust</td>
<td><a href="https://www.surfconext.nl/">https://www.surfconext.nl/</a></td>
<td>T: <a href="mailto:support@surfconext.nl">support@surfconext.nl</a>, S: <a href="mailto:help@surfconext.nl">help@surfconext.nl</a></td>
<td>2015-11-25 20:48:17</td>
<td>HTTP-Error</td>
<td>View</td>
</tr>
<tr>
<td>Antoni van Leeuwenhoek – Netherlands Cancer Institute</td>
<td>BFJACK-FILES.BU.OCDI.CA/ADFS/Services/Trust</td>
<td><a href="http://www.surfconext.nl/">http://www.surfconext.nl/</a></td>
<td>T: <a href="mailto:support@surfconext.nl">support@surfconext.nl</a>, S: <a href="mailto:help@surfconext.nl">help@surfconext.nl</a></td>
<td>2015-11-25 20:48:34</td>
<td>HTTP-Error</td>
<td>View</td>
</tr>
<tr>
<td>Nuclear Research and Consultancy Group</td>
<td>BFJACK-FILES.BU.OCDI.CA/ADFS/Services/Trust</td>
<td><a href="http://www.surfconext.nl/">http://www.surfconext.nl/</a></td>
<td>T: <a href="mailto:support@surfconext.nl">support@surfconext.nl</a>, S: <a href="mailto:help@surfconext.nl">help@surfconext.nl</a></td>
<td>2015-11-25 20:45:25</td>
<td>HTTP-Error</td>
<td>View</td>
</tr>
<tr>
<td>Nelson and Colne College</td>
<td>BFJACK-FILES.BU.OCDI.CA/ADFS/Services/Trust</td>
<td><a href="https://athenslart.nelson.ac.uk/OA/ADFS/Services/Trust">https://athenslart.nelson.ac.uk/OA/ADFS/Services/Trust</a></td>
<td>T: <a href="mailto:a.mills@nelson.ac.uk">a.mills@nelson.ac.uk</a>, S: <a href="mailto:a.rhodes@nelson.ac.uk">a.rhodes@nelson.ac.uk</a></td>
<td>2015-11-25 20:47:56</td>
<td>CURL-Error</td>
<td>View</td>
</tr>
</tbody>
</table>

### 102 (6.9%) redIdPs of 1481 (30.11.2015)

### 303 (20.5%) Red and Yellow IdPs ☹ (30.11.2015) vs 864 (58.3%) Green IdPs
### Excluded Identity Providers in Disabled Category

<table>
<thead>
<tr>
<th>Display Name</th>
<th>entityID</th>
<th>Registration Authority</th>
<th>Contacts</th>
<th>Last Test</th>
<th>Current Result</th>
<th>Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMOLF</td>
<td></td>
<td></td>
<td></td>
<td>Federation excluded from check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArtEZ Institute of the Arts</td>
<td></td>
<td></td>
<td></td>
<td>Federation excluded from check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Driestar Educatief</td>
<td></td>
<td></td>
<td></td>
<td>Federation excluded from check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOM-bureau</td>
<td></td>
<td></td>
<td></td>
<td>Federation excluded from check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grafisch Lyceum Utrecht</td>
<td></td>
<td></td>
<td></td>
<td>Federation excluded from check</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- IdPs can be disabled by sending an email to edugain@geant.org
- No checks will be done anymore

- **316 (21.3%) Gray IdPs that are excluded from checks** (30.11.2015)
• Way too many IdPs that are not configured properly
  • Or ECCS's checks are wrong/too strict

• Check is not perfect! There are still false positives!
  • We went through the hole list at one point to identify and exclude IdPs that generate false positives but new IdPs were added in the mean time

• Have a look at the results on https://technical.edugain.org/eccs/

• In particular check the IdPs of your federation

• eduGAIN Steering Group Delegates/Deputies will be notified soon
  • In case there are red and yellow IdPs
• **Inspiration:**
  CLARIN, eduGAIN CoCo Monitor

• **Concept:**
  Many people from eduGAIN Steering Committee

• **Development:**
  Marco Malavolti and Andrea Biancini from GARR

• **Operation:**
  eduGAIN Operations Team (Maja Wolniewicz, Tomasz Wolniewicz)
Thank you

lukas.haemmerle@switch.ch

This work is part of a project that has applied for funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).