An Introduction to Federation Policy
(Using the words of wiser people than me)

Nicole Harris

EuroCAMP Meeting,
15 October 2012
(Happy Birthday Mum)
• UK Access Management Focus;
• Advisor to UK federation;
• REFEDS Coordinator;
• PEER Project Manager;
• Shibboleth Consortium Manager;
• Generally opinionated about access and identity.
AND WHEREAS

The terms and conditions set out in this Agreement shall apply to all services available on the platform, and services to allow access federation to specific Identity Provider’s (as hereinafter defined). The services offered shall be provided through an access federation program, and the terms set forth above:

PARTICIPANT: Sobre a الموجودة: As instituições participantes, a Federação (leia-se “Identity Provider’s”) é aqui refeita no nome e representa as instituições participantes.

O presente Termos e Condições, o termo “Provedor de Serviços” referem-se a todas as instituições participantes, incluindo a Federação e suas parceiras.

Para todos os efeitos, aパーティスンテは以下のようなアセスメントを受けるものであり、アセスメントの内容が関係するものである。

1. OBJETIVO

1.1 O presente Termos e Condições são objeto de implementação em todas as instituições participantes, e serão realizadas com os acordos entre a Federação e os Provedores de Serviços.
What are the current problems?

• We don’t know what to call them;
• We don’t know what they are;
• We don’t agree on how to structure them;
• We don’t agree on the content;
• We all start from scratch when writing them;
• We ask the wrong questions...
• ...to the wrong people.

Apart from that it is ALLLL fine.
Federation Policy Best Practise Approach

• Analysis of 15 federation policies;
• Content ‘blocks’ for policy areas defined;
• Preferred structure / ORDER proposed;
• Example wording given;
• Chose your areas, leave out others.

https://refeds.terena.org/index.php/
Federation_Policy_Best_Practise_Approach
SECTION A: Structure

A: STRUCTURE.
GENERAL INFORMATION ABOUT HOW YOUR FEDERATION WORKS

• RFC2119.
• Definitions.
• Background and Purpose.
• Governance.
• Eligibility.
• How to Join.
• How to Withdraw.

STATUS: COMPLETE
SECTION B: Terms of Use

B: TERMS OF USE.
WHAT EVERYONE IS ALLOWED AND NOT ALLOWED TO DO

• Terms of Use (IdP).
• Terms of Use (SP).
• Termination / Dispute Resolution.
• Logging.
• Data Protection.
• Audit.
• Use of Attributes.
• Operator Rights / Role.
• Interfederation / Publish rights.

STATUS: IN PROGRESS
C: LEGAL.
ALL THE LEGAL STUFF

• Liability.
• Jurisdiction and Legal.
• Fee schedule.
• Copyright.

STATUS: IN PROGRESS
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>MEMB</td>
<td>Membership</td>
<td>IdP and SP members</td>
<td>IdP and SP members</td>
<td>IdP and SP members</td>
<td>SP contracts with federation</td>
<td>IdP and SP members</td>
<td>Separate SP (partner) and IdP (member) agreements</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>DESC</td>
<td>Document description</td>
<td>Policy</td>
<td>Federation Rules</td>
<td>Participant Agreement</td>
<td>Federation Policy</td>
<td>Service Provider Contract</td>
<td>IdP Conditions of Use, SP Conditions of Use</td>
<td>Service Agreement, Fed</td>
</tr>
<tr>
<td>12</td>
<td>Z119</td>
<td>RFC2119</td>
<td>1a</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NON</td>
</tr>
<tr>
<td>13</td>
<td>DEPI</td>
<td>Definitions</td>
<td>N/A</td>
<td>5</td>
<td>5.1</td>
<td>5.1.1-1.15</td>
<td>5</td>
<td>NONE</td>
<td>5</td>
</tr>
<tr>
<td>14</td>
<td>BACK</td>
<td>Background</td>
<td>2a,b,c,d,e, f,3a</td>
<td>1.1.1,1.2,1.3,1.4,1.5</td>
<td>0.1,0.6</td>
<td>1.1,1,2.8,1</td>
<td>1,2</td>
<td>NONE</td>
<td>Intro, section 1, appendix 2</td>
</tr>
<tr>
<td>15</td>
<td>ELIG</td>
<td>Eligibility</td>
<td>3b,4,4a</td>
<td>4.1,4.2,4,3</td>
<td>0.3</td>
<td>3.1,5,5,2</td>
<td>NONE</td>
<td>NONE</td>
<td>Intro (parts of), appendix 2</td>
</tr>
<tr>
<td>16</td>
<td>GOVE</td>
<td>Governance</td>
<td>4.2a,b,c, 6.3a</td>
<td>4.3</td>
<td>NONE</td>
<td>8.4</td>
<td>NONE</td>
<td>1.1.1</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>JOIN</td>
<td>How to Join</td>
<td>51.a,b,c</td>
<td>??</td>
<td>0.5</td>
<td>5.3,5.4,5.7</td>
<td>NONE</td>
<td>NONE</td>
<td>appendix 2 (3)</td>
</tr>
<tr>
<td>18</td>
<td>WITH</td>
<td>How to Withdraw</td>
<td>6.2a</td>
<td>13,1,14,14,2</td>
<td>NONE</td>
<td>6.1,8,3</td>
<td>14</td>
<td>NONE</td>
<td>appendix 4</td>
</tr>
<tr>
<td>19</td>
<td>SECTION B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>TERM</td>
<td>Termination / Dispute Resolution</td>
<td>4.3a,b,c,10a</td>
<td>12.2,13,3,3,13,1,16,2,16</td>
<td>3</td>
<td>2.1,5,1,5.2,5.3,10.1,</td>
<td>8.1,11,14</td>
<td>2,8,12</td>
<td>1.7</td>
</tr>
<tr>
<td>21</td>
<td>LOGS</td>
<td>Logging</td>
<td>NONE</td>
<td>8.8</td>
<td>NONE</td>
<td>NONE</td>
<td>4.2,3</td>
<td>NONE</td>
<td>NON</td>
</tr>
<tr>
<td>22</td>
<td>TOU</td>
<td>Terms of Use (IdP)</td>
<td>4.3c, 4.4b,4.4c,1,4-4.02.5a.5b</td>
<td>6.1.6,2,6.5,8,1,18,2,8,3,3,8,6,8,9,8,10</td>
<td>6.3,6,2,7,3,11,3,</td>
<td>3.2,3,3,3,5,5,6,7</td>
<td>4.5,1,5.2,5.3,5.4</td>
<td>NONE</td>
<td>NON</td>
</tr>
<tr>
<td></td>
<td>HOW TO WITHDRAW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Austria ACOnet</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(6.2A) The ACOnet Identity Federation member MAY cancel an ACOnet Identity Federation membership at any time by sending a written request to the ACOnet Identity Federation Operations Team. A cancellation of the ACOnet Identity Federation membership implies the automatic and immediate cancellation of the use of all Technology Profiles for the organization.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13.1 A Subscriber may voluntarily withdraw from the Australian Access Federation upon 20 Working Days’ notice to AAF Inc. Following cessation of the Subscriber’s participation (under any circumstances), AAF Inc. will cease to publish the Subscriber’s Metadata and will inform the remaining Subscribers that the Subscriber is no longer a Subscriber; 14.2 the Subscriber will, at its own cost: 14.2.1 cease to hold itself out as being a Subscriber and, if it is an Identity Provider will inform its End Users that its subscription has ceased; and 14.2.2 remove the Federation logo from all of its materials.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><strong>Australia AAF</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.1 Should a member organization decide to leave the federation on its own volition, the intention needs to be communicated to the Federation Operations writing, at least one month in advance. The Federation Operator will make preparations for technical disconnection of the member within the time frame and publish the information at the <a href="http://www.eduID.au">www.eduID.au</a> information portal. 8.3 All modifications to this Policy need to be announced three months in advance and discussed with all federation members as possible. In case of a new rule being deemed unacceptable by a member, that member is obliged to leave the federation by the date the new rule becomes effective (following Section 6 of this Document). Parties that fail to do so agree with the new wording of the Federation Policy without reservation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>Czech Republic eduID</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>Denmark WAYF</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14 Notice and termination  Either party may terminate the contract by serving one month’s written notice of the end of a month. This deadline does not apply in the event of breach of contract, cf. clause 8.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. Validity period, amendment and termination of the Agreement  The Agreement shall be valid until further notice. The notice period for termination of the Agreement shall be six months.  The Operator shall be entitled to change the Appendices to this Agreement upon hearing to the Federation’s Advisory Group. The amendment shall be notified to the Federation Partners in writing at least three (3) months prior to the effective date of the amendment. The notification shall be delivered to the administrative contact person designated by the Federation Partner, as set forth in section 9. In addition, the amendment shall be informed on the Operator’s website accessible to the Federation Partners. The information shall then</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
“NOW THEREFORE in consideration of the mutual covenants set out in this Agreement and for other good and valuable consideration (the receipt and sufficiency of which is hereby acknowledged by each of the parties), the parties agree as follows:”

CANADIAN ACCESS FEDERATION ‘POLICY’

Nothing on:

• Governance
• How to Withdraw
• Attributes
• Publication

(In this document)
RedIRIS Identity Service
Conditions of Use for Identity Providers
Version 1.0 – 20080220

1. Knows and accepts the rules, procedures and technical requirements for the connection of their identity management system with the RedIRIS Identity Service, as specified at http://www.rediris.es/PeRI. Applicants accept the appropriate changes that may take place, and that shall be communicated with sufficient time through the service website, and directly to the RedIRIS Official Loción ("Personas de Enlace con RedIRIS", referred to as "PeRI" in the rest of this document) of the corresponding affiliated institution.

2. Knows that breaking these conditions can imply the discontinuation of the service.

3. Declares that data included in this document are accurate, apart error or omission in good faith.

4. Commits to permanently update the information included in this document, informing the PeRIs of any change that takes place.

5. Assumes that RedIRIS, in all procedures related to service provision, will act according to the data provided in this document.

6. Knows and accepts that any falsity or error in the data included in this document can be cause of the discontinuation of the service.

7. Knows and accepts that once the service is active it can be revoked in case of violation of the requirements.

8. Knows and assumes that the service can be revoked in case of serious technical negligence.

9. Declares that, according to their best knowledge, the connection of the identity provider identified below with the RedIRIS Identity Service does not harm the rights of any third party.

10. Knows and accepts that the service is provided by RedIRIS in non-commercial terms for its users in the research and academic community, and that RedIRIS shall not be held liable for any damage caused, directly or indirectly, by the usage of the service.

11. Knows and assumes that RedIRIS will perform personal data processing according to the Ordo Lógicas 15/1999 on Personal Data Protection and the regulations developing it.

12. Knows and assumes that the rights to access and rectification can be exercised according to the above mentioned regulations. The right to cancellation and opposition can only be exercised after the discontinuation of the service, since personal data processing by RedIRIS is required for the use of the RedIRIS Identity Service.
WHERE DOES IT GO?

• EVERYTHING I’ve mentioned needs to be defined somewhere;
• There is nothing you can ‘leave out’ of your thinking;
• There are things you can leave out of your policy;

• Does it go in the policy?
• Does it go in appendices?
• Does it just go on the website?
REFEDS work is on existing federations;
Standardising existing problems;
Full-scale, not lightweight;
Both processes compatible in:
  • Wording;
  • Sections;
  • Approach.
“The software knows NOTHING about federations.”
Scott Cantor, Shibboleth Developer.

“Federations are SOCIAL constructs.”
Ian Young, Technical Architect  UK federation.

“Let the metadata FLOW.”
Leif Johansson, Man of Many Titles.

AND

“That’s not what we MEANT to do...”
Everyone who has written a federation policy
Common Mistakes

• What am I signing?
• Eligibility mistakes;
• Publication (interfederation);
• Enabling exchange......or protection your XXXX?
• Writing policy without all the information;
• Ignoring interoperability issues.
• Do I sign the policy?
  
  • Makes it difficult to introduce even minor changes;
  • Different people on different versions;
  • Sets it up clearly as a contractual arrangement.

• Do I agree to abide by ‘terms’ or ‘rules’?
  
  • More flexible in terms of core document;
  • Template letter or attached form;
  • Lightweight approach.
• Be clear early on who is eligible.
• Be clear early on who DECIDES who is eligible.
• Include a catch-all.
• IdP membership normally most difficult:
  • Restrict to members of the NREN?
  • Restrict to research and education?

“Subscription to the Federation is available to organisations and institutions which undertake or support education, research or research and development in Australia.”

“In order to become an Identity Provider in the ACOnet Identity Federation an organization MUST be eligible for ACOnet participation and MUST become a participant of ACOnet.”

“Eligibility for membership and the enrolment process is set out in the Federation Operator Procedures.”
• Don’t forget to assert the right to publish.
• Don’t restrict the right to publish.

“The Member grants the Federation Operator the right: to publish and otherwise use and hold the Metadata for the purpose of administering the operation of the Federation; to publish the Member’s name for the purpose of promoting the Federation.”

“In order to facilitate collaboration across national and organisational borders SWAMID MAY participate in interfederation agreements.”

“This Agreement governs the Edugate Federation’s national access management federation only. For the avoidance of doubt this Agreement does not apply to interfederation access, confederation access or metadata exchange.”
- The federation policy is a social construct;
- The federation policy is about socialising the metadata;
- Federation definitions:

  “The ACOnet Identity Federation is introduced to facilitate and simplify the offering of shared services across the (identity) federation.”

  “The purpose of the Federation is to create a framework within which Members can exchange access management information in a way that is responsible and respects End User privacy.”

- Federation policies do NOT to protect members from each other.
- More enabling, less protecting (liability).
DON’T let your policy define your structure;
DO inform your policy with well made decisions;
Before you write policy be clear on:
  • Scope / eligibility;
  • Governance;
  • Funding models now and future;
  • Rights and roles of Operator;
  • Rights and roles of IdPs and SPs.
  • Future plans.
• DON’T back yourself in to a corner:

  “Any metadata file which makes use of parts of metadata published by eduGAIN MUST include either a reference with a URL to the eduGAIN Metadata Terms of Use [ToU] or the entire ToU text. It MUST be placed at the top of the metadata file formatted as an XML comment.”

"Publications under clause 1 above will be at the request of the Member who controls each Entity."