Trust & Identity WG Meeting & SWITCH edu-ID Update Event

andres.aeschlimann@switch.ch
Virtual meeting, 20.5.2020
Picture taken from https://identityblog.switch.ch
Invited speakers

Stéphane Recrosio Uni FR
Head of IT Infrastructure & Operations

Maarten Kremers SURFnet
Technical Product Manager
Trust, Identity & Security
Agenda

- Success of the SWITCH edu-ID: Adoptions (UniFR)
- News flash
- P5 program
- SWITCH edu-ID and other initiatives (eduID @ SURFnet)
- Break
- Roadmaps (IdP Hosting, Documentation on IdP deployment)
- SWITCHaai News
- SWITCHpki News
- Farewell, then Q&A (open ended)
To ask your questions, use the chat window anytime
Logistics

• You can start a private chat with anyone:

![Private chat interface]

• You can also use Jitsi from SWITCH: [https://www.switch.ch/meet/](https://www.switch.ch/meet/) (but not now 😊)

• No recordings, but slides
Logistics

For best results, use the app: https://help.switch.ch/interact/downloads/
Logistics

Express your mood
«The only mistake in life is the lesson not learned»
A. Einstein

edu-ID @ UniFR
agenda

• Project summary / planning – do’s and don’ts
• Communication – do’s and don’ts
• (Extended) Support – do’s and don’ts / metrics
• Tips’n tricks
Project summary

1. Adoption planning & concept
2. Technical implementation
3. User transition
Project summary

June – December ‘18

Adoption planning & concept

Scenario selection
Technical design

May – October ‘19

Technical implementation

Linking scenario
Synchro mechanism
Testing SP
Testing linking & synchro
Migration to production

November – February ‘20

User transition

Communication
User support
AAI switch-off

Monthly conference calls with SWITCH
Planning – Do’s and Don’ts

Start early

Go-live outside of academic semester

Deployment of SWITCHhub in December helped

Start early

Underestimate testing

Exam period
Lassen Sie sich nicht aussperren!
Erstellen Sie noch vor Ende Januar Ihre SWITCH edu-ID!
Infos und Anleitung unter: unifr.ch/go/eduid

Ne restez pas bloqué·e dehors!
Créez votre SWITCH edu-ID avant la fin janvier!
Infos et mode d’emploi: unifr.ch/go/eduid
## Communication plan

<table>
<thead>
<tr>
<th>Tâche</th>
<th>Resp.</th>
<th>% terminé</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Présentation à la DIT</td>
<td>JT</td>
<td>100</td>
</tr>
<tr>
<td>Page explicative edu-ID</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Présentation MyTools</td>
<td>NTE</td>
<td>100</td>
</tr>
<tr>
<td>Ecrans d'annonce</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Email de la DIT aux collaborateurs</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Email de la DIT aux étudiants</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Article sur forum des CI</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Affichage &quot;news&quot; dans my.unifr.ch</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Affiches edu-ID</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Article Newsletter de la Rectrice</td>
<td>Unicom</td>
<td>100</td>
</tr>
<tr>
<td>Présentation aux CI (séance CI)</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>Info sur canaux AGEF (facebook, fachschaft, page web agef)</td>
<td>SR</td>
<td></td>
</tr>
<tr>
<td>Info aux Service Providers</td>
<td>JT</td>
<td>100</td>
</tr>
<tr>
<td>2ème email invitant à la création de compte (ciblé)</td>
<td>SR</td>
<td>100</td>
</tr>
<tr>
<td>3ème email invitant à la création de compte (ciblé)</td>
<td>SR</td>
<td></td>
</tr>
<tr>
<td>4ème email invitant à la création de compte (ciblé)</td>
<td>SR</td>
<td></td>
</tr>
<tr>
<td>Bloc Moodle informant de la création du compte edu-ID</td>
<td>NTE</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>septembre</th>
<th>octobre</th>
<th>novembre</th>
<th>décembre</th>
<th>janvier</th>
<th>février</th>
</tr>
</thead>
<tbody>
<tr>
<td>Présentation à la DIT</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
<td>40</td>
</tr>
<tr>
<td>Page explicative edu-ID</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
</tr>
<tr>
<td>Présentation MyTools</td>
<td>47</td>
<td>48</td>
<td>49</td>
<td>50</td>
<td>51</td>
<td>52</td>
</tr>
<tr>
<td>Ecrans d'annonce</td>
<td>53</td>
<td>54</td>
<td>55</td>
<td>56</td>
<td>57</td>
<td>58</td>
</tr>
<tr>
<td>Email de la DIT aux collaborateurs</td>
<td>59</td>
<td>60</td>
<td>61</td>
<td>62</td>
<td>63</td>
<td>64</td>
</tr>
<tr>
<td>Email de la DIT aux étudiants</td>
<td>65</td>
<td>66</td>
<td>67</td>
<td>68</td>
<td>69</td>
<td>70</td>
</tr>
<tr>
<td>Article sur forum des CI</td>
<td>71</td>
<td>72</td>
<td>73</td>
<td>74</td>
<td>75</td>
<td>76</td>
</tr>
<tr>
<td>Affichage &quot;news&quot; dans my.unifr.ch</td>
<td>77</td>
<td>78</td>
<td>79</td>
<td>80</td>
<td>81</td>
<td>82</td>
</tr>
<tr>
<td>Affiches edu-ID</td>
<td>83</td>
<td>84</td>
<td>85</td>
<td>86</td>
<td>87</td>
<td>88</td>
</tr>
<tr>
<td>Article Newsletter de la Rectrice</td>
<td>89</td>
<td>90</td>
<td>91</td>
<td>92</td>
<td>93</td>
<td>94</td>
</tr>
<tr>
<td>Présentation aux CI (séance CI)</td>
<td>95</td>
<td>96</td>
<td>97</td>
<td>98</td>
<td>99</td>
<td>100</td>
</tr>
<tr>
<td>Info sur canaux AGEF (facebook, fachschaft, page web agef)</td>
<td>101</td>
<td>102</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info aux Service Providers</td>
<td>103</td>
<td>104</td>
<td>105</td>
<td>106</td>
<td>107</td>
<td>108</td>
</tr>
<tr>
<td>2ème email invitant à la création de compte (ciblé)</td>
<td>109</td>
<td>110</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info aux Service Providers</td>
<td>111</td>
<td>112</td>
<td>113</td>
<td>114</td>
<td>115</td>
<td>116</td>
</tr>
<tr>
<td>Bloc Moodle informant de la création du compte edu-ID</td>
<td>117</td>
<td>118</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2020 SWITCH | 15
Communication vs nb of affiliations

Comptes edu-ID affiliés à l'unifr

- Activation bloc info Moodle
- Email aux étudiants
- Email au staff
- Email systématique
- Newsletter du Rectorat
- Arrêt AAI
- Début SP

© 2020 SWITCH | 16
Communication – Do’s and Don’ts

Call to action

Target your communication

Be (more and more) directive

Multi-channel

Start (too) early

Ready-to-use edu-ID consists of 2 parts (account + affiliation)

Attribute pull is tricky to explain…
(extended) support

• Adobe licence model change on December 1st

• Staff had to go to SWITCHhub (login via edu-ID) to get new licence

• Too many changes at once

• Painful experience, however *a blessing in disguise* for edu-ID
(extended) support – student support

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lieux</td>
<td>Mis 4130</td>
<td>Per21-A040</td>
<td>Mis 4130</td>
<td>Per21-A040</td>
<td>Mis 4130</td>
</tr>
<tr>
<td>Horaires</td>
<td>08h-10h</td>
<td>10h-12h</td>
<td>12h-14h</td>
<td>14h-18h</td>
<td>08h-10h</td>
</tr>
<tr>
<td>Eric</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loïc</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>AYA Yann</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dylan</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Laura</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leah</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lara</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fabian</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Céline</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Quentin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

10 personnes

© 2020 SWITCH | 19
(extended) support – metrics

• Go-live week (January 28th)
  • Very few requests

• Semester start (February 17th)
  • Visits < 10 /day
  • Emails ~15 / day

• Staff
  – Peak at ~ 10 / day

• Support requests raised to SWITCH not included
(extended) support – do’s and don’ts

- Increase according to the communication plan
- Prepare workaround (unblock users)
- Split staff and students (if possible)
- Videos were appreciated

- Overestimate visits (like we did)
Tips’n tricks

• Multiple stakeholders
  ➢ Appoint a Project Manager
  ➢ Setup a recurring conference/visio call

• Identify your user populations early (use cases)

• Establish working relationship with SWITCH
  ➢ Excellent collaboration / support / coaching / listening from SWITCH
Thank you
Backup slides
## Detailed planning

<table>
<thead>
<tr>
<th>Tâche</th>
<th>Resp.</th>
<th>% terminé</th>
<th>20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1 2 3 4 5 6 7 8 9 10 11 12 13</th>
<th>Commentaire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Développement interface de synchronisation + création compte depuis my.unifr.ch</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Développement opérateur page Moodle</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tests</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Définition des scénarios de test</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT/SWITCH</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mise en place de l'environnement de test</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affiliation</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Géraldация</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Moodle</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login SP (avec vérification du type d'affiliation (staff, stud., affiliate))</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JT</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login CAMPUS</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Micromus</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Synchro Campus Mgmt - SWITCH edu-ID</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activation de l'affiliation/creation de compte dans my.unifr.ch</td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mise en prod &quot;splash screen&quot; Moodle</td>
<td>JM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Présentation à la DIT</td>
<td>IT</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Présentation MyTools</td>
<td>NTE</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Informations à l'auteur</td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail de la DIT aux collaborateurs</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail de la DIT aux étudiants</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail de la DIT aux étudiants</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affichages &quot;nouveau&quot; dans my.unifr.ch</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affichages &quot;nouveau&quot; dans my.unifr.ch</td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Affichages edu-ID</td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Newsletter de la DIT</td>
<td>Université</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Présentation aux CI (durant le CI)</td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info sur campus ADIF (facebook, fachshaf, page web agef)</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info aux service fonctionnels</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail invitant à la création de compte (cibô)</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail invitant à la création de compte (cibô)</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email invitant à la création de compte (cibô)</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email invitant à la création de compte (cibô)</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SR</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Création Moodie informant de la création du compte edu-ID</td>
<td>IM</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support Center</td>
<td>IM/HC</td>
<td>100</td>
<td></td>
<td>13/01/20, HC confirme que le support est prêt</td>
</tr>
<tr>
<td>Micromus</td>
<td>IM/HC</td>
<td>100</td>
<td></td>
<td>13/01/20, HC confirme que le support est prêt</td>
</tr>
<tr>
<td>Support pro/pas-go-live</td>
<td>IM/HC</td>
<td>100</td>
<td></td>
<td>13/01/20, HC confirme que le support est prêt</td>
</tr>
<tr>
<td></td>
<td>IM/HC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arrêt AAI - Mt 28 janvier</td>
<td>IM/HC</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Début de semestre</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2020 SWITCH | 25
Compte SWITCH edu-ID

Nous avons constaté que vous ne possédez pas encore de compte SWITCH edu-ID, ou que votre compte SWITCH edu-ID n’est pas lié à votre compte Unifr.
Dès le 29 janvier 2020, vous devrez vous connecter à Moodle avec votre compte SWITCH edu-ID.

Créer/lier le compte SWITCH edu-ID →
Step 2: trigger edu-ID account creation – **WITHOUT** edu-ID

Afin d'accéder à certains services, vous devez lier votre compte SWITCH edu-ID à votre compte Unifr. En cliquant sur 'Continuer' vous serez invité à vous connecter à votre compte SWITCH edu-ID, ce qui vous permettra de valider votre affiliation à l'université de Fribourg. Si vous ne possédez pas de compte SWITCH edu-ID, vous aurez la possibilité d'en créer directement un.
Votre compte SWITCH edu-ID est déjà lié à votre compte Unifr. Aucune action n'est nécessaire.
Things that worked - communication
• Affiche en page de garde
• Comm / canaux avec impact pour chacun d’eux +/-/+++/
• Plan de comm
• Identification des populations: tiers, mobilité
• Workarounds (AAI linking / link for mobility)
• Extended student support
• Go-live outside semester +++
Status SLSP

Lukas Hämmerle
SLSP

• **SLSP launches December 2020**
  – Offers service to users of more 30 research library networks
  – ExLibris-hosted Alma/Primo system

• **End-users register and authenticate with edu-ID**
  – Pre-registration starts in summer
  – Data (attributes) flow only in one direction from edu-ID to SLSP
  – If edu-ID data changes, SLSP data is updated automatically (within seconds if the user applied change)
Overview

Test/Preview (only temporarily available): [https://registration-test.slsp.ch/](https://registration-test.slsp.ch/)
Involvement of SWITCH

• SWITCH has actively helped integrate edu-ID since September 2019
  – Many of the features added for SLSP also benefit other services/organisations (e.g. more options for custom views, better service notification in case of data changes, )

• edu-ID also benefits from SLSP
  – Several hundred thousand new edu-ID user accounts will be created
  – SLSP n ca(in the future) report back to edu-ID if postal or e-mail addresses or phone numbers are no longer correct

Do universities need to prepare for SLSP launch?

• Short answer: **No**

• Longer answer: To facilitate registration for your users ensure your IdP releases to SLPS Registration service these attributes:
  – Date of birth
  – Home/Business postal address (at least one)
  – Home/Business/Mobile phone number (at least one)
  – Library card number (new CardUID value)

• More information on [https://switch.ch/edu-id/organisations/idm/slsp-integration/](https://switch.ch/edu-id/organisations/idm/slsp-integration/)
Kerberos/SPNEGO for edu-ID IdP

Daniel Lutz
Kerberos/SPNEGO for edu-ID IdP

Seamless login experience on edu-ID IdP

• Will be available as an option per organisation, mainly for staff members.
• Users don’t need to enter username/password on the IdP if they are authenticated in the local Windows domain.
• Supported on domain-joined Windows clients only. (Other clients supporting Kerberos could be enabled, too.)
• Cross-Realm Trust allows to support multiple organisations in parallel.
• Clients to be supported are configured on the edu-ID IdP per organisation (limiting to clients supporting it, e.g. based on the client’s network or user agent identifier string). Other clients (e.g. road warriors) can still log in with username/password.
Kerberos/SPNEGO for edu-ID IdP

How it works:

Active Directory edu-ID

Service

Username

Password

Seamless Access

Trust

Domain Joined Clients

@UNI-A.CH

@EDUID.CH

@UNI-B.CH

@UNI-C.CH

KDC

edu-ID

KDC

edu-ID IdP
Azure AD – O365 Integration

Thomas Bärecke
Microsoft Azure AD with Pass-Through-Authentication (PTA)

0. User provisioning with scripts to AAD

1. Access attempt (unauthenticated)

2. Home realm discovery (WAYF)

3. Authentication

4. Service access (authenticated)

Office 365

SWITCH edu-ID (production federation)

Microsoft Cloud

SWITCH edu-ID (edu-ID adopted)

Admin
Limitations and workarounds

• Limitation: Bilateral non-standard configuration
• Current solution: Special configuration on SWITCH edu-ID IdP

• Long-term solution: Proxy

• Limitation: One Microsoft Custom Domain per SAML-IdP only
• Shortly available solution: One proxy per domain
Proxy architecture

Bundled together in Shibboleth IdP V4.0

Multiple instances for multiple domains

Azure AD / O365

Shib IdP
Shib SP

SWITCH edu-ID IdP

Microsoft

SWITCHhaai federation

Azure AD – O365 Integration
Read-only Mode for Technical Accounts

Lukas Hämmerle
Characteristics

• Account can be **used for login but cannot be changed**

• Account is assigned eduPersonEntitlement value: [https://eduid.ch/spec/read-only-account/](https://eduid.ch/spec/read-only-account/)

• Only organisation admins can set/remove read-only status

• Created primarily for technical accounts

• More information: [https://www.switch.ch/edu-id/organisations/idm/read-only-account/](https://www.switch.ch/edu-id/organisations/idm/read-only-account/)
Characteristics

• To try it out yourself as organisation admin: https://eduid.ch/web/organisation-administrator/

• On "Create a new Technical Account" page
  Create account in the read-only state. This will prevent account modification until the account is made writeable by an administrator.

• In list of technical accounts:
Handling of Duplicate Accounts and Prevention Mechanisms

Lukas Hämmerle
Causes for Duplicate Accounts

• User is **not aware** that he already has an account

• User creates duplicate accounts **on purpose**
  • E.g. for testing or debugging purposes
  • This can hardly be prevented

• User **cannot be linked** to existing account
  • Mostly because a shared unique identifier is missing
  • E.g. during a migration
Account Creation Recapitulation

Minimum data to create edu-ID account:
- First name - Not unique
- Last name - Not unique
- Verified E-mail address - Unique, but user often has many

How to prevent duplicate accounts?
Preventing Duplicates

• It’s **impossible** to prevent all duplicates 😞

• **Names cannot be used** reliably and in a data privacy-respecting way
  • Name and birthday are much better but not sufficient

• **Strategy:**
  • **Prevent** as many duplicates as possible
  • Provide **merge process** (for admins and users)
  • Actively asks users to merge their (potential) duplicate accounts
  • Merge accounts for which we have hard/verified facts
Preventing Duplicates with Cookie

- **Longterm cookie** stores info that user has account
- Create Login button is disabled on login page
- Warning is shown when user tries to register again

![SWITCH.edu-ID](image)

- Only works for current browser/device
Identifying Duplicates

• Adding/linking already associated unique values (mail, mobile number, AAI identifiers, ORCID ID) triggers warning and sometimes email to user if duplicates exist already

• Sometimes too late to prevent duplicate at this point
  • But user is informed about duplicate merge
Account Deduplication Goals

- **Self-deduplication**
  - Information provided should be as clear as possible
  - Keep it as simple as possible: As few decisions for user as needed

- **Secure and safe deduplication without misuse**
  - User must proof that he owns the credentials for both accounts

- **Accountability**
  - We keep track of which accounts were merged by whom

- **Notify SP Admins automatically**
  - Technical contacts of affected SPs are sent an e-mail
  - User also gets receipt to proof that he owned the two accounts

- **Voluntary Deduplication**
  - Motivate/remind users to merge but generally no forced merge
Deduplication = Account Merge

- Accounts merged by administrator on request of user
  - SWITCH could also proactively merge accounts according to Terms of Use (Article 7.e): “SWITCH reserves the right to merge and/or delete any accounts identified as duplicates, which may lead to loss of data or restricted access to services.”
  - But currently no active enforcement of 7.e

- Accounts merged by users themselves (since May 2018)
  - Users are shown link to account merge page or they are reminded via email (previous slide)

- Account merge always has side effects!
  - Account that is archived often was used to access services
  - User’s identifier attributes on these services change with merge
Account (Self-) Merges By End-Users

- Peak around time organisation adopts edu-ID
- Around 15 merges per week in the past months
- Till May 15th 2020 of 1’672 merges performed, 846 (50.5%) were initiated by end-users
Summary

• We try our best to prevent duplicates
  • But not all duplicates can be prevented…

• Merge process to ensure that number of duplicates is low
  • User can merge accounts and is encouraged to do so
  • Side effects of merge should be kept low, therefore user and all affected SP admins are informed via e-mail about changes
Re-use of E-mail Adresses: How to Prevent Impact on edu-ID Accounts

Lukas Hämmerle
E-Mail address in edu-ID

- Used as login name (like for many cloud services today)
- Any e-mail address associated to account can be used to login or for password reset!

**Risk:**
User looses e-mail address, another user inherits it and takes over original owner’s edu-ID account
E-Mail Address Recycling

• Every e-mail provider has own policy regarding address recycling:
  – Gmail never recycles
  – Most e-mail providers recycle addresses after some grace period (e.g. 1 year for Hotmail, 6 months for Yahoo, GMX deletes account after 6 months inactivity and may recycle after 12 months)

• What about universities? Schools? Companies?
  – Example: Staff member with same name inherited address of student after just a few days of grace period
Counter-Measures by edu-ID

- If user loses university affiliation, **edu-ID automatically removes e-mail addresses**
  - If no other address is available, “.inactive” is appended to address.
  - User can regain account on his own if password still known
  - Reserved domain .inactive prevents password reset

- **Remind inactive users** of their account
- Remind users to **add long-term non-organisation address**
Counter-Measures by edu-ID II

• Starting in May/June 2020: **Bounce Mail Processing**
  – Bounce mail processing will recognize inactive addresses and remove them automatically.

```
(Permanent) Bounce mail received after N days

Send e-mail to bounced address

Received another bounce?

yes

Remove/replace e-mail and possibly inform user

no

e-Mail address probably still works
```
Limitations of Bounce-Mail Processing

• Only works if we ever receive a bounce-mail or trigger one
  – edu-ID users don’t receive regular e-mails to their contact address
  – Additional/linked identities e-mail address are currently not checked regularly

• Does not work if e-mail address is recycled in less than N

• Future extension:
  Check e-mail addresses actively (by sending an e-mail) or via commercial service. But how often?
Counter Measures for End-User

- Keep e-mail addresses of edu-ID account **up-to-date**
- Enable Two-Step login (**multi-factor authentication**)
- Ideally add your **(privately) owned long-term e-mail address** as contact address
Edu-ID for small organizations

Rolf Brugger
## Small Organizations vs. Universities

<table>
<thead>
<tr>
<th></th>
<th>Small Organizations</th>
<th>Universities</th>
</tr>
</thead>
<tbody>
<tr>
<td># members</td>
<td>&lt; ~100</td>
<td>&gt; ~100</td>
</tr>
<tr>
<td>member fluctuation</td>
<td>low</td>
<td>High for students; average for teaching and researching staff</td>
</tr>
<tr>
<td>IdM</td>
<td>Simple IdM, low degree of integration, many manual IdM processes</td>
<td>Well organized IdM with high degree of automation</td>
</tr>
</tbody>
</table>
How to give small organizations access to SPs?

• Access management in our community: often based on organization membership

• Examples:
  – Learning management systems for members of selected universities
  – Subscription to services on a per-organization basis (SWITCHdrive, SWITCHportfolio, …)
# Solution approaches

## Fully compatible “homeOrg”

<table>
<thead>
<tr>
<th>Solution</th>
<th>Integration Cost</th>
<th>Federation Partner Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full edu-ID Integration</strong></td>
<td>Relatively high</td>
<td>Org needs to be federation</td>
</tr>
<tr>
<td></td>
<td>integration cost</td>
<td>partner (paperwork, cost, know-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>how)</td>
</tr>
<tr>
<td><strong>Edu-ID Integration with manual on-offboarding</strong></td>
<td>Manual process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is tedious and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>error prone</td>
<td></td>
</tr>
<tr>
<td><strong>IdM service for small organizations</strong></td>
<td><em>Not a service yet</em></td>
<td></td>
</tr>
</tbody>
</table>

## Easy to implement / low-cost

<table>
<thead>
<tr>
<th>Solution</th>
<th>Scalability</th>
<th>SP Entitlement Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entitlements via shared attribute API</strong></td>
<td>API only, Doesn’t</td>
<td>Not all SP are capable to</td>
</tr>
<tr>
<td></td>
<td>scale well</td>
<td>interpret entitlement</td>
</tr>
<tr>
<td><strong>Entitlements via virtual home org (VHO)</strong></td>
<td>VHO Service likely</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to be discontinued</td>
<td></td>
</tr>
<tr>
<td><strong>Entitlements or group attribute via group management</strong></td>
<td><em>Not a service yet</em></td>
<td></td>
</tr>
</tbody>
</table>
Update of Service Description

https://www.switch.ch/edu-id/about/terms/

Petra Kauer-Ott
Updates for services & organisations

Added descriptions:
- Classic and extended attribute model (& usage)
- Updates/completion of data in background
- (Organisation) Administration Interface
- Intended use of technical accounts
- Duration of data processing at SWITCH (incl. backup)

Emphasis on duties for SPs:
- Restricted use of SWITCH edu-ID identifier
- Inform user before loss of affiliation
Updates for end users (1)

Emphasis:

• **Email**: keep contact up to date
• **End of affiliation**: loss of organisational email address
Updates for end users (1)

Emphasis:

• **Email**: keep contact up to date
• **End of affiliation**: loss of organisational email address

• **Duplicates**: duty to merge them
Updates for end users (1)

Emphasis:

• **Email**: keep contact up to date
• **End of affiliation**: loss of organisational email address

• **Duplicates**: duty to merge them
Updates for end users (2)

Emphasis:

• **User consent:**
  updates and completion of user data in background

Added description:

• **Deprovisioning process:**
  reminders, deactivation after 5 years, deletion after 10 years

• **Right to information**
Updates for end users (3)

Change:
- User consent: technical identifiers not displayed

<table>
<thead>
<tr>
<th>technical identifier</th>
<th>example values</th>
</tr>
</thead>
<tbody>
<tr>
<td>swissEduPersonUniqueID</td>
<td><a href="mailto:845938727494@ethz.ch">845938727494@ethz.ch</a>,</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:288aac23dbf9e1460c86b1a5a04c6af875f724ce@uzh.ch">288aac23dbf9e1460c86b1a5a04c6af875f724ce@uzh.ch</a></td>
</tr>
<tr>
<td></td>
<td>/shibbolethla6c2c4d4-08b9-4ca7-8ff9-43d83e6e1d35</td>
</tr>
<tr>
<td>swissEduID</td>
<td>7b91bdaf-da5c-4851-ae02-26416dfda1c2</td>
</tr>
</tbody>
</table>

https://www.switch.ch/edu-id/services/login/user-consent/
Help – a request for information!
Help – a request for information!

Request for information:
- Postpone / Feign death
- Panic
- Search data ...

Deadline:
- Analyse data
- Prepare procedure
- Send receipt
- Check authorisation
- Precise question & prepare data
- Deliver data
- Document request & improve procedure

© 2020 SWITCH