Virtual Home Organization & Guest Login
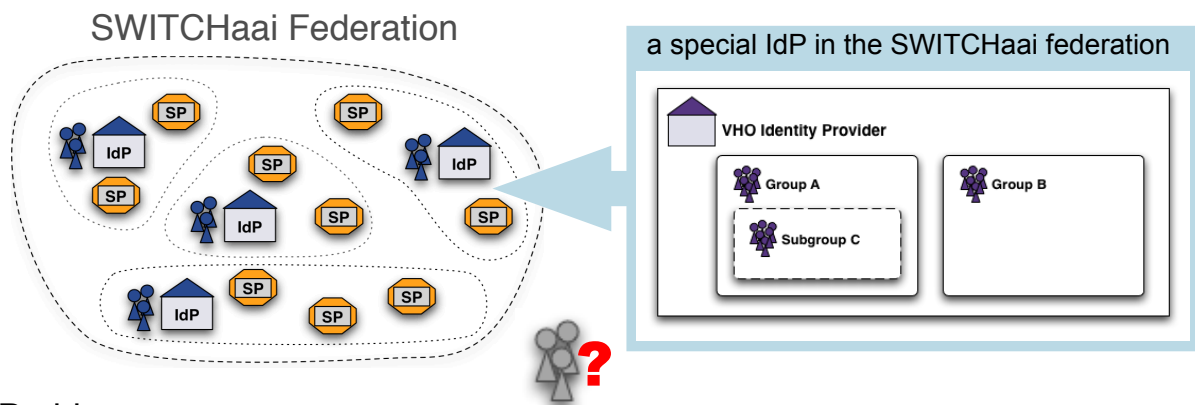
SWITCH

Serving Swiss Universities

SWITCHaai Team
aai@switch.ch

Agenda

1. Motivation & Context

2. SWITCH VHO Service

3. VHO Administration Tool

4. Guest Login

Motivation & Context

SWITCHaai Federation

a special IdP in the SWITCHaai federation

VHO Identity Provider

Group A

Subgroup C

Group B

Problem

- Resource (SP) configured to only accept AAI users
- Users from outside the federation need access to the resource

Solution

- Resource owner manages these users in the
 Virtual Home Organization (VHO)

© 2012 SWITCH

Agenda

1. Motivation & Context

2. SWITCH VHO Service

3. VHO Administration Tool

4. Guest Login

© 2012 SWITCH

SWITCH VHO Service

- Targeted end user groups
  - Attendees of a further education or other training
  - Collaboration projects from private companies or foreign universities, which are not in the SWITCHaai federation

- Resource owners can manage end user accounts themselves

© 2012 SWITCH
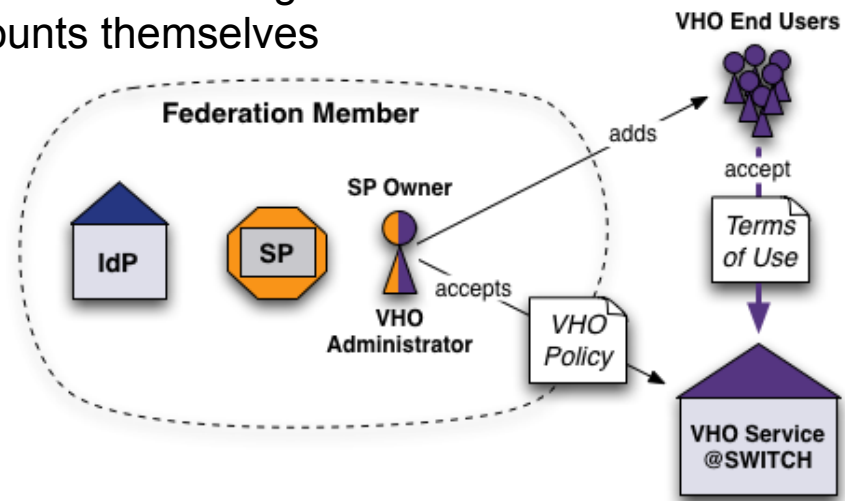
Service Subscription Process
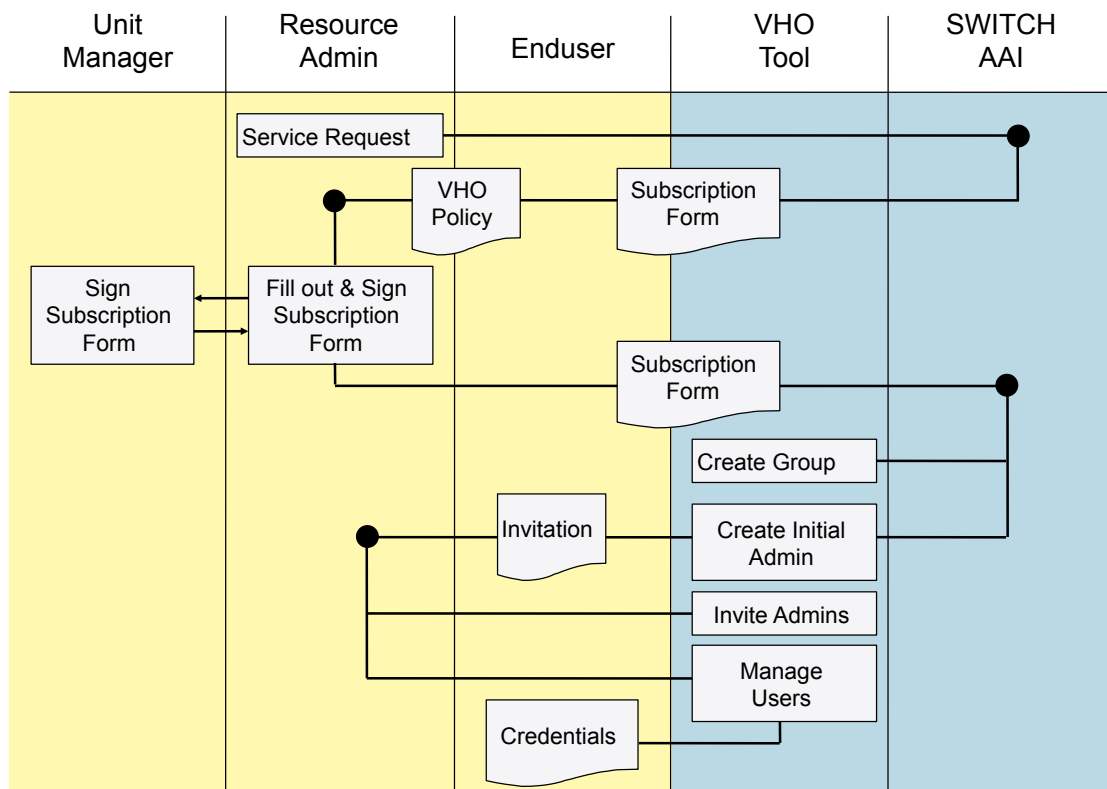
© 2012 SWITCH

Agenda

(1) Motivation & Context

(2) SWITCH VHO Service

(3) VHO Administration Tool

(4) Guest Login

© 2012 SWITCH

VHOtools - Key functionalities

- Administrator services
  - Manage one or more groups, which can be structured hierarchically
  - Define description for each group (support contact, mail templates)
  - Create new user accounts with some AAI attributes (E-Mail, entitlement, …)
  - Modify, delete and expire user accounts (incl. password resets)
  - Import and export of user lists
  - View group statistics
  - Account expiration reminder

- End user services
  - Login
  - User self-service password changes
  - Support information

© 2012 SWITCH

Screenshots administration tool (1)

demogroupa : 81 active - 18 expired - 0 deleted users

Choose action:
- ✓ Choose action:
- Set expiration date = now
- Choose expiration date
- Update field
- Delete
- Purge
- Download HTML

Search: [   ] [Search]
(use * or % for wildcard search. The search is performed on username, first and last name... and custom fields)

search users

...ong **inactive** orphans

3 4 5 6 ... 9 10 Next »

sort by any attribute

shortcuts to: edit, expire, delete & password reset

		Expiration date	**Last modification date**	**Last login date**	**Actions**
☐	dga-user01		09.11.2007	31.07.2012	👥
☐	dga-user02		09.11.2007	26.06.2012	👥
☐	dga-user03	03.07.2011	09.11.2007	13.08.2012	👥
☑	dga-user04	01.05.2013	09.11.2007	25.06.2012	👥
☐	dga-user05	11.05.2014	09.11.2007	12.05.2012	👥
☐	dga-user06	05.06.2014	09.11.2007	07.08.2012	👥
☐	dga-user07	30.08.2012	09.11.2007	10.08.2012	👥
☐	dga...8	9.08.2014	09.11.2007	08.06.2012	👥
☐	dga...	05.2012	09.11.2007	07.07.2012	👥
☐	dg...	2.10.2014	09.11.2007	29.06.2012	👥

predefined actions

user's state indicator

dates: creation, last modification, last login, expiration & custom info

[Choose action: ▾]

Page: « Previous **1** 2 3 4 5 6 ... 9 10 Next »
View: short medium long **inactive** orphans
Legend: active expired deleted

paged users list & custom views

© 2012 SWITCH

Screenshots administration tool (2)

Create or modify user accounts using web forms...

demogroupa : Edit user

Fields marked with an asterisk (*) are mandatory.

Username dga-user06
uniqueID d642431@test.vho-switchaai.ch

Last name * [Walker]
First name * [William]
E-mail * [William.Walker@dga.edu.us]
Entitlement * [http://example.edu.org/dga]

ℹ All entitlements must be prefix...
Use one line per entitlement, if yo...

Business phone number [+1 4444 333 22 06]
ℹ e.g.+41 44 268 15 05

Business postal address [Golden Lane 6
6000 San Francisco]

ℹ Enter the full postal address wi...

Preferred Language [en ▾]
Description [   ]

ℹ The description is intended for...
It will never be released to any re...

Affiliation affiliate
Home organization vho-switchaai.ch
Home organization type vho

Expiration date [▾] or enter date [05.06.2014]
ℹ The date format is dd.mm.YYYY
After the expiration date is reached the user won't be able to login with his VHO account

Custom field 1 [   ]
ℹ This is a field for your own purpose, i.e.: project, training or applicant name
It will never be released to any resource

Custom field 2 [   ]
ℹ Another field for your own purpose
It will never be released to any resource

[Cancel]   [Save]

demogroupa : View active user

[Expire] [Delete] [Reset password] [Edit]

Username: dga-user06
uniqueID: d642431@test.vho-switchaai.ch

Last name: Walker
First name: William
E-mail: William.Walker@dga.edu.us
Entitlement: http://example.edu.org/dga
Business phone number: +1 4444 333 22 06
Business postal address: Golden Lane 6
6000 San Francisco
Preferred Language: en
Affiliation: affiliate
Home organization: test.vho-switchaai.ch
Home organization type: vho

Expiration date: 05.06.2014 14:03:11
Creation date: 09.11.2007 15:48:35
Last modification date: 09.11.2007 15:48:35
Last login date: 07.08.2012 14:03:11

© 2012 SWITCH

Screenshots administration tool (3)

...or easy mass user creation by file upload

demogroupa : Import users from CSV file

You can import a list of users in the VHO using a CSV (Comma Separated Values ⧉) file.
Please use the vho-import.xls ⊞ template to create your users list, then just export the sheet in CSV format in order to create CSV file that allows you to import your users in the VHO. The character encoding of the CSV file should be **ISO-8859-1**.

CSV Data Specifications
At least the fields marked with an asterisk (*) need to be in your CSV header:
- **username***: The prefix **dga-** will be added automatically if missing.
- **password**: If the field has no value, a new password will be generated.
  Please choose a good password if you define one: minimum 6 characters,
  mixed uppercase and lowercase letters and at least one number.
- **surname***: The last name.
- **givenname***: The first name.
- **mail*** The email address of the user.
- **eduPersonEntitlement**: If the field has no value, **http://example.edu.org/dga** will be used as default prefix/value.
  For multiple entitlements please add additional **eduPersonEntitlement** columns.
- **postalAddress**: Use the dollar sign "**$**" for line breaks.
- **telephoneNumber**: e.g. international format +41 44 268 15 05
- **preferredLanguage**: Must be one of de/fr/it/en.
- **description**: For your internal use. i.e. PhD Student.
- **dateExpire**: Expected format is **dd.mm.YYYY**
  If the field has no date, the user will expire in **1 week**.

- An AAI UniqueID will be generated automatically for each user.
- The file encoding should be **ISO-8859-1**. (You can change the encoding in the preferences)
- Additional columns in your CSV file will be ignored.

Choose the CSV file containing your users list to i   :   Delimiter
Choose File | no file selected

auto detect
✓ ;

Process CSV file

© 2012 SWITCH

Screenshots administration tool (4)

Mail templates

New user

Subject: New VHO-Account

($NAME$, $USERNAME$, $PASSWORD$, $GROUPADMIN$, $CUSTO

Dear $NAME$,

We created you a new AAI account in the Virtual Home Organization.

Username: $USERNAME$
Password: $PASSWORD$

Please be aware that the username and password are case sensitive.

For changing your password, please visit https://tools.test.vho-switchaai.ch/passw

If you have any problem using your credential, please contact directly the VHO help
help desks is available online at https://tools.test.vho-switchaai.ch/support/

When using your account and you have to choose a SWITCHaai Home Organization,
please select *Virtual Home Organisation @SWITCHaai*.

Customize e-mail templates for
'new user' or 'reset password'
notifications

Define custom views
for the list of users

Define views for list users function

	Name	Sort attribute	Sort order	Users per page
A:	short	Username	ascending	20
B:	medium	Username	ascending	20
C:	long	Username	ascending	20
D:	inactive	Expiration date	ascending	10
E:	orphans	Last login date	ascending	view all

The expired and deleted users will **only** be shown in view **D**.

A	B	C	D	E	Attributes
✓	✓	✓	✓	✓	Username
☐	☐	☐	☐	☐	uniqueID
✓	☐	✓	☐	✓	Last name
✓	☐	✓	☐	✓	First name
✓	☐	✓	☐	✓	E-mail
☐	☐	✓	☐	☐	Entitlement
☐	☐	☐	☐	☐	Business phone number
☐	☐	☐	☐	☐	Business postal address
☐	☐	☐	☐	☐	Preferred Language
☐	☐	✓	☐	☐	Description
☐	☐	☐	☐	☐	Affiliation
☐	☐	☐	☐	☐	Home organization
☐	☐	☐	☐	☐	Home organization type
☐	✓	✓	✓	☐	Expiration date
☐	✓	✓	☐	✓	Creation date
☐	✓	✓	✓	☐	Last modification date
☐	✓	☐	✓	✓	Last login date
☐	☐	✓	☐	☐	Custom field 1
☐	☐	✓	☐	☐	Custom field 2

Save

Reset configuration

© 2012 SWITCH

Screenshots administration tool (5)

Group statistics

Group	Valid users 100%	Active last week		Active last month		Active last 3 months		Active last 6 months		Active last 12 months		Not active last 12 months		Never active *created < 6 months*		Never active *created > 6 months*		Expired		Orphans		
																						C
demogroupb	99	0	0.0%	21	21.2%	36	36.4%	22	22.2%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	20	20.2%	0	0.0%	☐
demogroupa	99	0	0.0%	27	27.3%	45	45.5%	9	9.1%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	18	18.2%	0	0.0%	☐
demosubgraa	99	3	3.0%	19	19.2%	40	40.4%	11	11.1%	0	0.0%	0	0.0%	0	0.0%	0	0.0%	26	26.3%	0	0.0%	☐

The VHO groups highlighted should be cleaned up
Reason: > 20% orphaned accounts

Orphans are calculated as the sum of:
- accounts with no login in the past 12 months
- accounts never used and created more then 6 months ago

[Export orphaned accounts of selected groups]

Account expiration
reminder notification

```
We want to inform you, that the following accounts
will expire within the next 6 weeks:

expiration date    | user account
------------------------------------
Tue, 03. Jun. 2008 | dga-user10
Wed, 11. Jun. 2008 | dgb-user56
                   | dgb-user82
```

© 2012 SWITCH

VHOtools demo access

SWITCH provides a demo access to the VHOtools
with some dummy group and user entries.

Try it out yourself!

    https://tools.test.vho-switchaai.ch/

choose this organisation

    Test Virtual Home Organisation

use these credentials

    username: switch-demoadmin(AAITest)

    password: demoadmin

For further information

    http://switch.ch/aai/vho/

© 2012 SWITCH

Agenda

▶

① Motivation & Context

② SWITCH VHO Service

③ VHO Administration Tool

④ Guest Login

Why a Guest Login?

- Some AAI Services have users from outside the federation

- Resource owner does not want to manage guest accounts in a VHO-group; or doing so would not scale

- Self-registered user accounts with self-provided user attributes are acceptable for the service
  - no verification at all for given name and surname
  - e-mail address only verified on registration
  ➡ Do not rely on the quality of Guest Login user data!

- SWITCH needed a scalable Guest Login for the SWITCHtoolbox service

Audience for Guest Login?

- Guest Login is only usable for Service Providers in the
  - SWITCHaai Federation
  - AAI Test Federation

- Service Providers have to specifically enable Guest Login
  - Follow these instructions; in fact it's a 'bilateral configuration'

    http://switch.ch/aai/support/serviceproviders/guest-login.html

➡ Guest Login is not part of the SWITCHaai Federation metadata since its self-registered user accounts would not be acceptable

© 2012 SWITCH

Guest Login vs VHO?

Topic	Guest Login	Virtual Home Organization (VHO)
Policy and regulations for managing accounts	No	Yes
Papers to sign	No	Yes
Accounts can be used for more than one service	Yes	Generally not
Responsibility of account management	User himself	VHO Group administrator(s)
In SWITCHaai and AAI Test federation	No	Yes
Data quality of user information	Poor, user can modify his own data	Controllable by VHO administrator(s)

http://switch.ch/aai/support/serviceproviders/guest-login.html

© 2012 SWITCH