PAUL SCHERRER INSTITUT

PSI

WIR SCHAFFEN WISSEN – HEUTE FÜR MORGEN

Dmitry Ozerov :: Software Scientist :: Paul Scherrer Institute

Identity Management

(multiple accounts and tools to deal with them)

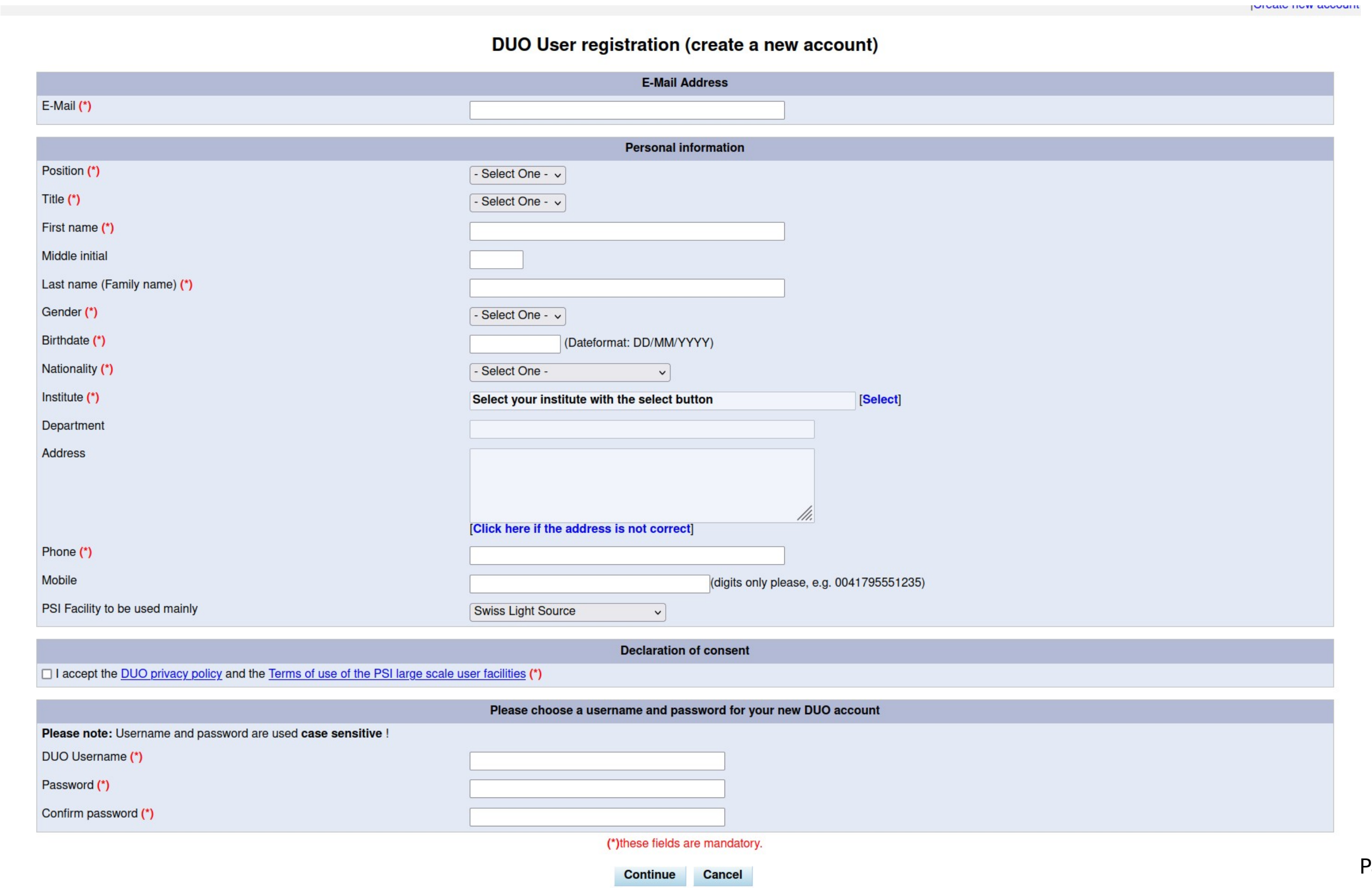
25.7. AWI meeting

Involved groups

PSI Large Facilities (SLS, SwissFEL, SINQ, SuS,CHRISP...) - stackeholders
UserOffice (NUM) – proposal submission, evaluation, tools (DUO)
AIT - AD, Security
AWI – services (storage, computing, nomachine, data transfer..)
GFA – beamline consoles, ssh-gateways

Changes made during last years in identity management by collaboration with Markus Knecht (DUO) and Bjoern Abt (AD, Security) will be covered

DUO Account



|Create new account

DUO User registration (create a new account)

E-Mail Address	
E-Mail (*)	

Personal information	
Position (*)	- Select One -
Title (*)	- Select One -
First name (*)	
Middle initial	
Last name (Family name) (*)	
Gender (*)	- Select One -
Birthdate (*)	(Dateformat: DD/MM/YYYY)
Nationality (*)	- Select One -
Institute (*)	**Select your institute with the select button** [**Select**]
Department	
Address	[**Click here if the address is not correct**]
Phone (*)	
Mobile	(digits only please, e.g. 0041795551235)
PSI Facility to be used mainly	Swiss Light Source

Declaration of consent

☐ I accept the DUO privacy policy and the Terms of use of the PSI large scale user facilities (*)

Please choose a username and password for your new DUO account

Please note: Username and password are used **case sensitive** !

DUO Username (*)	
Password (*)	
Confirm password (*)	

(*)these fields are mandatory.

DUO Account (duo user)

Self registration

For people who had nothing with PSI before (don’t have PSI account) – possibility to submit proposal for experiment

Lives in DUO database

Possibility to reset password by user (using provided mail)

What can be done with DUO account:

- edit/(re)submit proposal
- apply for badge/guesthouse
- after experiment: provide feedback, register publication

-* (if proposal accepted and experiment scheduled) PI can add PSI accounts to pgroup

-* (if associated ext- account) possibility to reset ext- account password

>28.000 DUO users registered

Experiment account (e-account)

For each accepted proposal, beamtime is scheduled and unique e-account is created. This e-account is used to store data (to separate data of different experiments)

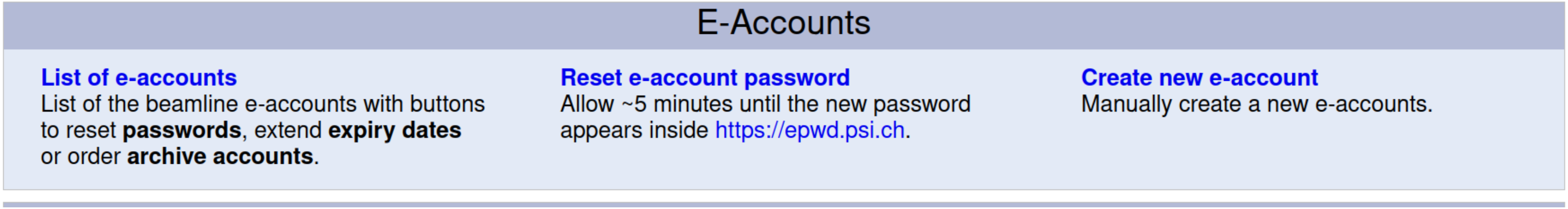
e-accounts were in a separate openldap server (made by Derek Feichtinger) and had simple passwords (based on PI name) and covered (needed by) SLS only

With introduction of Ra cluster(DaaS project, end user analysis service) – need to move e-accounts to AD to have link(pgroup) between PSI accounts and e-accounts

Request from security: accounts in AD should have lifetime and stronger password

>11.000 e-accounts/pgroups currently (SLS, SwissFEL, SINQ, SuS) (used only at SLS)

E-accounts tools



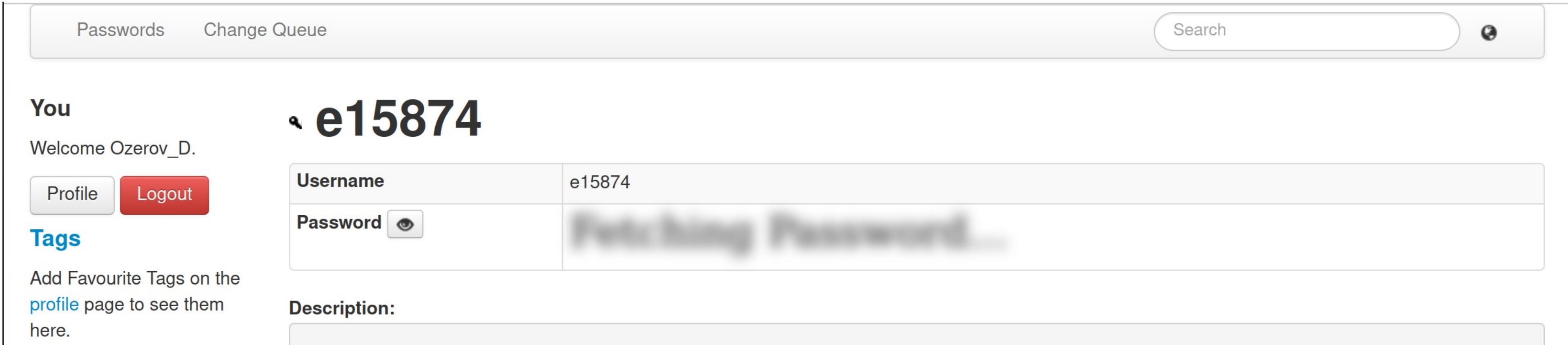
E-Accounts

List of e-accounts
List of the beamline e-accounts with buttons to reset **passwords**, extend **expiry dates** or order **archive accounts**.

Reset e-account password
Allow ~5 minutes until the new password appears inside https://epwd.psi.ch.

Create new e-account
Manually create a new e-accounts.

https://epwd.psi.ch : service to get e-accounts passwords for members of pgroup and beamline people



You

Welcome Ozerov_D.

Tags

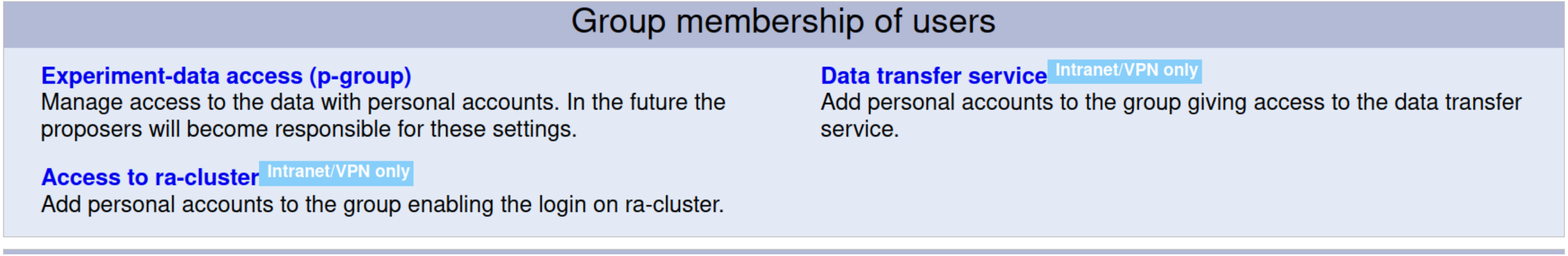
Add Favourite Tags on the profile page to see them here.

e15874

Username	e15874
Password	Fetching Password...

Description:

Group tools (pgroup, Ra, data transfer)



Group membership of users

Experiment-data access (p-group)
Manage access to the data with personal accounts. In the future the proposers will become responsible for these settings.

Access to ra-cluster Intranet/VPN only
Add personal accounts to the group enabling the login on ra-cluster.

Data transfer service Intranet/VPN only
Add personal accounts to the group giving access to the data transfer service.

Possibility for beamline people to give access to:
- experiment data (pgroup)
- Ra cluster (svc-cluster_ra)
- data transfer service (svc-data_ra)

(on request from beamline people, latter was added possibility for PI to add people to pgroup)

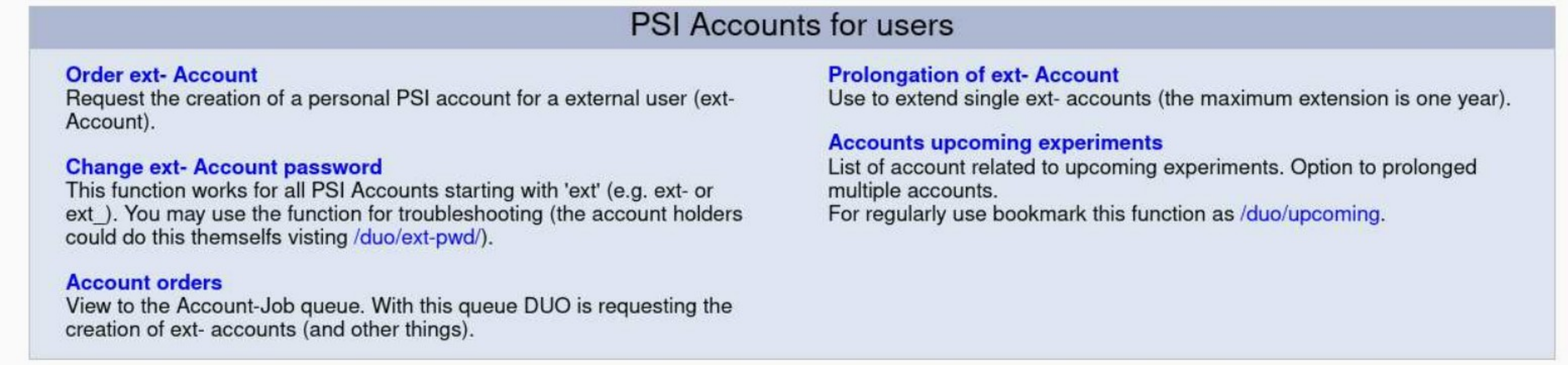
PSI accounts

Internal (PSI people) and external (“ext-”) accounts

Security requirements for PSI accounts:

- Password change every 6 months
- Lifetime (max 1 year) for “ext-” accounts (prolongation can only be done by PSI person)
- Access from outside of PSI – only with the PSI personal accounts (no e-accounts, no shared (gac-) accounts) to Ra cluster for data analysis; to beamline consoles during data taking
- (new) enforced *FA (Authentication) for access from outside

PSI accounts (tools)



PSI Accounts for users

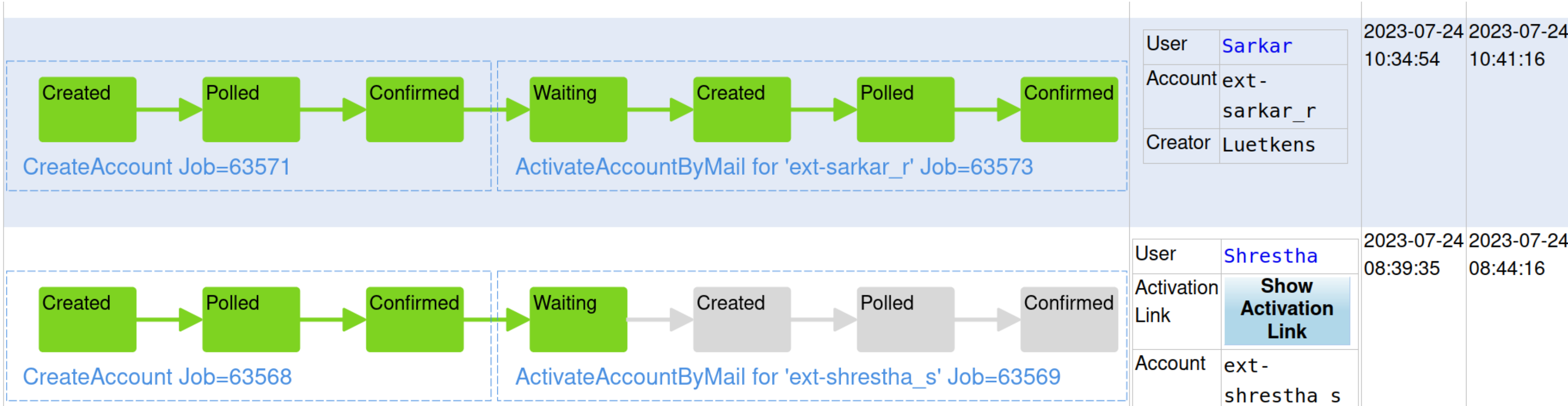
Order ext- Account
Request the creation of a personal PSI account for a external user (ext-Account).

Change ext- Account password
This function works for all PSI Accounts starting with 'ext' (e.g. ext- or ext_). You may use the function for troubleshooting (the account holders could do this themselfs visting /duo/ext-pwd/).

Account orders
View to the Account-Job queue. With this queue DUO is requesting the creation of ext- accounts (and other things).

Prolongation of ext- Account
Use to extend single ext- accounts (the maximum extension is one year).

Accounts upcoming experiments
List of account related to upcoming experiments. Option to prolonged multiple accounts.
For regularly use bookmark this function as /duo/upcoming.



Created → Polled → Confirmed
CreateAccount Job=63571

Waiting → Created → Polled → Confirmed
ActivateAccountByMail for 'ext-sarkar_r' Job=63573

User	Sarkar
Account	ext-sarkar_r
Creator	Luetkens

2023-07-24 10:34:54 | 2023-07-24 10:41:16

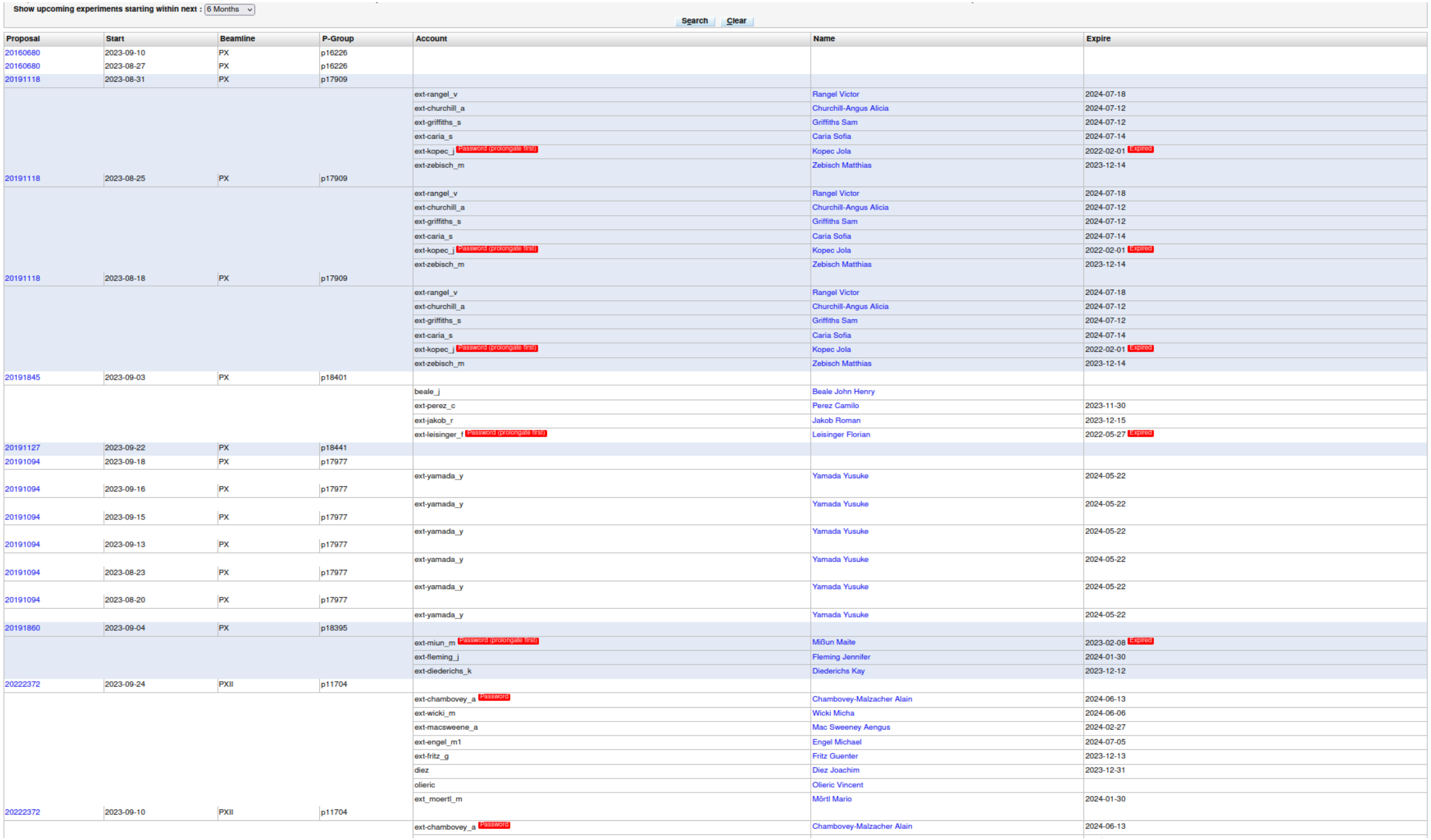
Created → Polled → Confirmed
CreateAccount Job=63568

Waiting → Created → Polled → Confirmed
ActivateAccountByMail for 'ext-shrestha_s' Job=63569

User	Shrestha
Activation Link	Show Activation Link
Account	ext-shrestha_s

2023-07-24 08:39:35 | 2023-07-24 08:44:16

PSI accounts (tools)



Show upcoming experiments starting within next : 6 Months

Proposal	Start	Beamline	P-Group	Account	Name	Expire
20160680	2023-09-10	PX	p16226			
20160680	2023-08-27	PX	p16226			
20191118	2023-08-31	PX	p17909			
				ext-rangel_v	Rangel Victor	2024-07-18
				ext-churchill_a	Churchill-Angus Alicia	2024-07-12
				ext-griffiths_s	Griffiths Sam	2024-07-12
				ext-caria_s	Caria Sofia	2024-07-14
				ext-kopec_j Password (prolongate first)	Kopec Jola	2022-02-01 Expired
				ext-zebisch_m	Zebisch Matthias	2023-12-14
20191118	2023-08-25	PX	p17909			
				ext-rangel_v	Rangel Victor	2024-07-18
				ext-churchill_a	Churchill-Angus Alicia	2024-07-12
				ext-griffiths_s	Griffiths Sam	2024-07-12
				ext-caria_s	Caria Sofia	2024-07-14
				ext-kopec_j Password (prolongate first)	Kopec Jola	2022-02-01 Expired
				ext-zebisch_m	Zebisch Matthias	2023-12-14
20191118	2023-08-18	PX	p17909			
				ext-rangel_v	Rangel Victor	2024-07-18
				ext-churchill_a	Churchill-Angus Alicia	2024-07-12
				ext-griffiths_s	Griffiths Sam	2024-07-12
				ext-caria_s	Caria Sofia	2024-07-14
				ext-kopec_j Password (prolongate first)	Kopec Jola	2022-02-01 Expired
				ext-zebisch_m	Zebisch Matthias	2023-12-14
20191845	2023-09-03	PX	p18401			
				beale_j	Beale John Henry	
				ext-perez_c	Perez Camilo	2023-11-30
				ext-jakob_r	Jakob Roman	2023-12-15
				ext-leisinger_f Password (prolongate first)	Leisinger Florian	2022-05-27 Expired
20191127	2023-09-22	PX	p18441			
20191094	2023-09-18	PX	p17977			
				ext-yamada_y	Yamada Yusuke	2024-05-22
20191094	2023-09-16	PX	p17977			
				ext-yamada_y	Yamada Yusuke	2024-05-22
20191094	2023-09-15	PX	p17977			
				ext-yamada_y	Yamada Yusuke	2024-05-22
20191094	2023-09-13	PX	p17977			
				ext-yamada_y	Yamada Yusuke	2024-05-22
20191094	2023-08-23	PX	p17977			
				ext-yamada_y	Yamada Yusuke	2024-05-22
20191094	2023-08-20	PX	p17977			
				ext-yamada_y	Yamada Yusuke	2024-05-22
20191860	2023-09-04	PX	p18395			
				ext-miun_m Password (prolongate first)	Mißun Maite	2023-02-08 Expired
				ext-fleming_j	Fleming Jennifer	2024-01-30
				ext-diederichs_k	Diederichs Kay	2023-12-12
20222372	2023-09-24	PXII	p11704			
				ext-chambovey_a Password	Chambovey-Malzacher Alain	2024-06-13
				ext-wicki_m	Wicki Micha	2024-06-06
				ext-macsweene_a	Mac Sweeney Aengus	2024-02-27
				ext-engel_m1	Engel Michael	2024-07-05
				ext-fritz_g	Fritz Guenter	2023-12-13
				diez	Diez Joachim	2023-12-31
				olieric	Olieric Vincent	
				ext_moertl_m	Mörtl Mario	2024-01-30
20222372	2023-09-10	PXII	p11704			
				ext-chambovey_a Password	Chambovey-Malzacher Alain	2024-06-13

PSI accounts (tools)

Possibility to create ext- account by simplified procedure (information about user is taken from DUO-account registration; request to make account is made by beamline person (PSI))

Extended this functionality to CHRISP, SINQ and SuS Facilities

>2.000 ext- accounts created this way since 2017

Identity management (summary)

Current identity management has logic and needed tools to function, but as result of evolution – heavy in understanding, not easy for support and use

SLS darktime is a possibility to simplify identity management (Marie @iCaSIT, Feb. 2023)

(replacement of duo account with federated ? DUO already supports Umbrella. Data transfer(globus part) is integrated with SwitchAAI(only internal psi accounts), which is planned to be replaced(AIT) with Switch EDU-ID))

DUO

DUO is highly overloaded with the additional tools/features, compared to initial idea as proposal submission/evaluation system

(not covered in this talk: allowance to mount sls storage via duo; steering of ssh-gateway for beamline/machine network)

As service accessible to external users (for proposal submission) – a potential threat (creation of personal accounts, steer allowance to use services; access to data, reset of PSI accounts password..)

SLS darktime may help to make DUO/Identity management better

Thanks for you attention