SIRTFI face to face meeting at SWITCH - July 12-13 2017

Participants:
Thomas, Ann, Pal, Mario, Rhys (remote), Hannah NIcole , Jule

Ann: We know SIRTFI it is viable via national pilots, now: what eduGAIN should be doing about SIRTFI ? Policy, Support, Human infrastructure,..Central components
What do federation expect from us ?

Nicole: What is hiding behind the proxy (SNCTFI).

Hannah: would be interesting in terms of endorsement - to be made

What types of services is mostly important

Ann: Question to Thomas - How persuasive was for campuses to know that some SPs require SIRTFI ?
Thomas : first was not motivating - but when users went to IdPs admins, then it was effective.

Rhys: few came to us, the only way for us is services indicating that at some point they are going to require it.
CERN have many local users

Nicole: Another impacting thing, and motivating, was when we went through the document at Internet2 and people realized : well, we do this anyhow ! it is easy.

Use the Moodle Course from AARC
Federations have to be involved, UK, D, F, DK

UK federation: every now and then,we have dissemination events. We are also planning at a bigger scale such events.
Horizon 2020 funding : D, UK F, NL, E, I - these 6 countries are the mostly budgeted one - it an indicator on Research going on.

Hannah: how easy would people change their policies ? Monitoring could play a role, showing who is doing SIRTFI and who is not.
Ann; 2 main issues: How to specify the policy and how to implement the policy in the system

Pal: set a SIRTFI stamp in every entity - It should be a stamp. Like eccs - technical.edugain.org - you can check how federations stand with EC adoptions…
Federations should be warned -
BCP for eduGAIN to be published could take care of SIRTFI too

We are reducing the policy (declaration and a SAML profile (or OIDC profile at some point) - then the rest will be referred through the BCP, like R&S and CoCo.
Once this is out, that should be the place to use.

Process of the community committing to something : this is what is mostly about.

Nicole: Is it worth to have some sort of Award program for IdPs ?
For Campus the issues is who make the decisions, people understanding, legal fear, how to make that decision making
GDRP could be use to leverage this - A GEANT white paper is in work about this.
Since you need to do something in this space already - White paper out during summer
Pal is re-writing it completely, after having spoken to lawyers and others.

Nicole: making interviews with Campuses who did it to show how easy it was ? FANW is a Campus in Switzerland (Applied Science)
EPFL and ETH have done SIRTFI .
University of Thessaloniki

EPFL IdP is cloud based.
Rhys: Univ. of Glasgow is one of our SIRTFI IdPs - Glasgow was a pushy one, could be a good one.
Make a couple of questions to show how easy was to adopt it

Mario: if we really ensure everyone has the elements to do SIRTFI and the tools./means, why don't' we ask Federation to “almost request it” ?
Ann: With the BCP we are sort of doing this. It is really the closest thing there is to required.

Hannah: some people asked to be shown why this is useful .
Ann: We could script some workshops….recording of the TNC session - what would help.

Other option: track email flows among people.

Ann: key is providing the right people with the right information .

Centralized eduGAIN support for SIRTFI
We want to manage the incident - not the content
Triage person has to delete sensitive / personal information if she sees it coming
Pal: No secret information has to come in
eduGAIN eScience support -have you a mandate for the security part ? not really.
It is via email ? Where the national one needs some help
Thomas: Few tickets - e.g.: 5 tickets in June. We did not advertised it widely yet.
Option to have CERN supporting on the security part -

Hannah: have you find a security officer for GEANT ? Yes, Paul Drake -
Operational security experts
Evangelos could be someone acting as an operational security expert

Ann: We scoped some central staff - move along the lines of the e-Science support

Ann (blackboard) :Potential Work items:

1. WP: eduGAIN BCP [owner: Nicole]
2. WP: Outreach Material + WS training
3. WP: Central Support [owner: Thomas]
4. WP tooling including tools and processes / Monitoring and warning for BCPs

This could be added to Gn4.3 proposal from 2019 onward

Federation not being enough supportive : could eduGAIN bypass this issue ?
Would eduGAIN be allowed to add a bit to the feeds metadata - technically you could do it
Politically an issue

Ann: We should really focus on the Federations as main target - at least for the next 6 months

Tooling: a query service could make use of eduGAIN DB. The eduGAIN DB is already there.
It still depends on the Federation metadata . Is Federated -
Do we need an independent SIRTFI registry?

Hannah : A reputation portal for SIRTFI ? - they flag particularly bad behavior, we could want to flag also good behaviors (if you downrate somebody) - Ann : might be risky and tricky.

Rhys: we are responsible for the enforcing of it - we should just remove the SIRTFI Assurance profile assertion from them .

Nicole: probably more useful a set of procedure you will have to prove once you as an IdP you want to recover your SIRTFI tag - Rhys: but let's keep it consistent across federation, for example using BCP. BCP should not allow people to shop from another federation for any reason.

About 3) - Central Support: Incident workflows / Workflows for monitoring / Advisory / Info Blog / [Reactive/Proactive]

==========

Back to the original agenda:
What role eduGAIN can play ? we identified 4 work items

BCP : Nicole - we still need to figure out what it will look like, for example a simple web page stating " we expect mature entities to do the following things.."

Consultation about it ? Not really recommended [Next eduGAIN consultation will be on the SAML profile]

Question Ann to Nicole: What is missing to build the strawman BCP document ?
Nicole: I need to put material together focusing on federation operators
End of August - Initial timeline will be August

There is some material for CoCo - mostly linking to documentation
A staged release of the BCP is on option : the 4 areas are CoCo, SIRTFI, R&S , MFA/Assurance
BCP approach: to be a good eduGAIN citizen you should comply with BCP

How to bundle the self-assessment tool in a workflow ? The tools helps to identifying possible issues, not really to solve .
It is on a cloud survey platform ? The self assessment tool : how to evolve, sustain it ?
The self assessment tool needs to be bundled to the federation.

A stand alone tool people could refer to and then redirect to the federations - rather than directly inject information inside the MD (the finnish approach).

We should clarify what it really means for federation to support SIRTFI:

- Should be able to produce documentation and training material
- WIlling to introduce flags and remove them based on failure to comply
- Need to manage the operational requirements

==========coffee break ==========

Outreach and Materials

Question to the fedops : What kind of material could be of use to support federation in supporting SIRTFI ?

Interviews ?

Pal: I need to know which services are asking for SIRTFI.
Rhys: Case studies: these are the services that use it and will require it

SIRTFI uptake very related to CoCo.Indicative but not enough CoCo will succeed depending on GDPR compliance
With SIRTFI you get only something of GDPR : Article 33 - 34 from GDPR, section 2.
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
Pal: In CoCo version2 we ask for SIRTFI

So: 7 SPs asserting SIRTFI : one of it is CERN, CILogon (for eduGAIN), EGI (for AARC pilots), NIKHEF server proxy… mostly pilots

We really need to push it on the SP side now. CERN has done his bit.
Hannah: ORCID is willing to do it -

Best practices for SPs: It is time AARC works on this !
How to convince SPs ? With the same arguments we use for IdPs .
We need SPs ? which ones ?
ELIXIR / GEANT proxy / CORBEL
REMS of ELIXIR " Resource Management System
DARIAH
UMBRELLA (got funding from H2020 to do non-web stuff - moonshot)- they are in eduGAIN
EUDAT
OpenAccessRepository
ORCID

We need to add to this WIKI section
https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home

AARC should help on the SP part

For Dissemination and Outreach material - let's ask
Rosanna Norman / NA2 Geant
https://www.linkedin.com/in/rosannanorman/?ppe=1

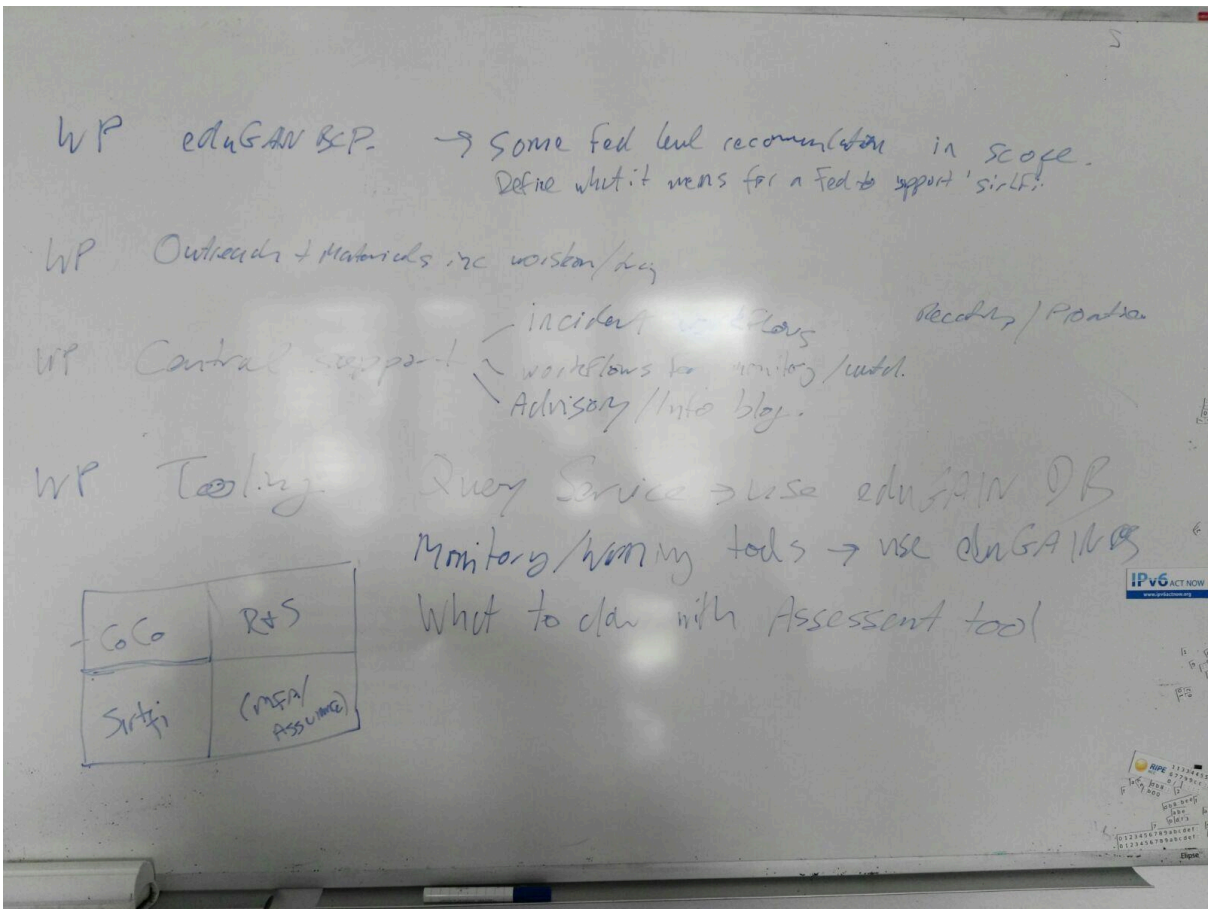
NREN PR Team - Federica Tanolongo GARR / AARC an option to ask ?

Workshops : we need to draft an IdP side and an SP side

Ann: I want to discuss how to direct users demand on SIRTFI to Federations systematically - rather than word of mouth tomorrow in the tooling part

Mario: a point is to leverage "special eduGAIN support" for SPs through SIRTFI compliance.

Tomorrow



========== END OF DAY 1==========

Tools

Ann: We should use SIRTFI as an example of policy filtering in discovering service. We would need to be in contact with RA21.

Tooling should therefore be compatible with future DS

Another tool we really want with top priority - the inline user support:
User AuthN, comes to SP, SP rejects them - Reason could be IdP non SIRTFI compliant - then provides user inline with enough info to contact campus and support (some notes from a meeting that Jule, Pål and Hannah held https://docs.google.com/document/d/1VbmFM2j-SxREg-rGGY3RLbbYVw2tUOajeoosGUpSgz8/edit#)

SimpleSAMLphp

Error messaging as a standalone service ? Rhys: didn't InCommon do something like that ? You need some additional info on the MD.

https://spaces.internet2.edu/display/InCFederation/Error+Handling+Service

Discovery and Error handling are 2 bits of the issue

Ann: Long term: Policy Based proxy is the most elegant solution.

EduGAIN Attribute Release Check : https://release-check.edugain.org/ (EARC)
A good move would be to extend it to add all the BCP of eduGAIN - (H: would be useful if we could launch the tool with details of the checks it needs to pass, e.g. link with parameters of attributes, entity categories etc)

Need to talk to Lukas - Need to check if Jule could be involved in this

One concrete action is to include/extend to be an overall “good citizen’policy checker/maturity checker.

We can start by saying “here is what we believe is the correct error handling for SIRTFI”

Rhys: Simple but effective error messages for the user - as a re-direct

Pal & Nicole: We need to handle the error messages to be more human readable.

Error handling made by 3 bits:

- Defining what error handling at SP side
- Adapt the I2 error handling services to be more human
- Technical redirect happening at the SP

Pal: we need to write down how we want this to function: Ann: we need to document some workflows - Involved some Software Development of course.
We need the modelling - Scott could take a look at this.

Mario: how does this relate to Hannah’s tool http://sirtfi.cern.ch/ ?

Hannah: We do Policy based filtering on SIRTFI for the discovery service. For user support we pull data from the eduGAIN feed and find support contacts.
We filter based on release of SIRTFI - We ask for minimal attributes
We only list the organizations with a Display Name in english (the tool is for users, not people who know entity IDs)
In DS starting from the eduGAIN MD feed - and find the contacts

Operational steps for us:

Step 1 model the workflows from a user perspective - discovery and error handling. Hand over discovery workflows to RA21/geant project

Step 2 analyse existing available components on how they could meet it
Step 3 re-architect to eliminate duplication/make modular
Step 4 concrete implementation with SimpleSAMLphp and extending attribute release check
Step 5 include SP to try out

Ann: as Federations, do you see it credible to SP to tell them how error handling should be done
Rhys :It is reasonable to try

After we modelled the Workflow, We can handle then the Discovery Service Model to the GEANT RA21 involved persons (CESNET and SUNET - Leif …)

Pal: Who should work on this ? Pal, Jule, Mario, Hannah

Specs for support:

We need and easy way to grab security contacts, including in bulk and link them to the relevant fedop security contact
(also of use for other contacts e.g. helpdesk etc. Expand eduGAIN DB)

Bulk Notification tool
Group management for policies to access bulk notification tool

Ticketing system
We should use the same ticketing system as edugain support. In the beginning a new ticket goes to the edugain support for manual triage.

Avoid panic issue / Defacing / Reputation

Contacts / Trust : we should try to have a list of trusted contacts @ federations
Security Desktop staff do not change / roll over so much since it is a very technically skilled profile

Monitoring

What do we need to monitor around SIRTFI ? What centrally should we be monitoring so that when a SIRTFI case comes in, people do a quick triage.

A SIRTFI case: somebody thinks there has been an incident:

IS the entity SIRTFI contact ---> contact the SIRTFI contact and federations contacts - Both entities and federations should be notified

We need to check (Tomasz) that contacts are in the Metadata -
Tomasz tools flags missing contacts but does not do anything specific
(https://technical.edugain.org/entities)

Tooling for future audit/fire drills
E.g. being able to scan patch levels legally etc.?
Poss Gn4-3

Monitor : At the moment : Compliance with SIRTFI and Good Citizenship (of the IdP) check - In future: access error logs

We have to model the workflow from the user perspective and then match to an architecture

========== break ==========

F-thicks monitoring could be combined with separate error handling services (reporting unsuccessful login) - we could use it as a cross-check

F-Thicks is configuration in Shibboleth
[Pal: we Shib 3 needed to change error handler

What already exist in current support

After Coffee: What do we do when non-Sirtfi-compliant entities are affected by a security incident? (Central Support - WHat to do for entities not SIRTFI supporting)

For non SIRTFI compliant entities - if there is an incident - you direct users to fedops contacts of the given federation - or get in contact with us at the Best Effort

Central Support

Thomas describes what exist currently in central support:

We have a ticketing system and a couple of email addresses
We have a team of 5 - including me and Lukas - 2 people always on duty for the whole week
There is a public slack channel - edugain support pilot channel edugain_support_channel

It is opened for others - we already have some fedops - in edugain.slack.com channel edugain_support_pilot

The 5 people on shift are the operating the local federation

Current Workflow:

First one who sees the tickets checks it - asking federations for actions - review if actions are done.
Summary of the facts available to the community - anonymized - this is still missing - a sort of newsletter for the interested security contacts

Ann: we are moving eduGAIN website to wordpress - so there could be place for blogs to report - for example
We need to do reporting on KPIs for the project in any case. We could extrapolate advisories

The channel is to expedite communication - or add edugain-support.slack.com

Handling personal/sensitive information - if accidentally received, 1 business day to delete from system and reopen in new anonymous form. Need a trash queue to manage in the system to achieve this. Cleaning trash can be automated.
Document what is a business day.

Use dedicated security queue.
Addresses to be pointed at OTRS are:
security@edugain
abuse@edugain
edugain-security@geant.org <- this as the ticket reply

Write a privacy policy for eduGAIN support, inc. security.
Link to privacy policy in footer.

Staffing: escalation rota for security (check with Paul D if Evangelos might be a 'volunteer'). Check if Romain also interested.

SIRTFI is handing over its support part to task2 Jra3 eScience support

Password dump alerting. Important not to store sensitive data (even if it may be public). Can direct users to https://haveibeenpwned.com (latest password dumps may not be available)
---------- Sent out 2017-07-13 12:11 ----------
Draft email for edugain-sg list:

Dear eduGAIN SG members,

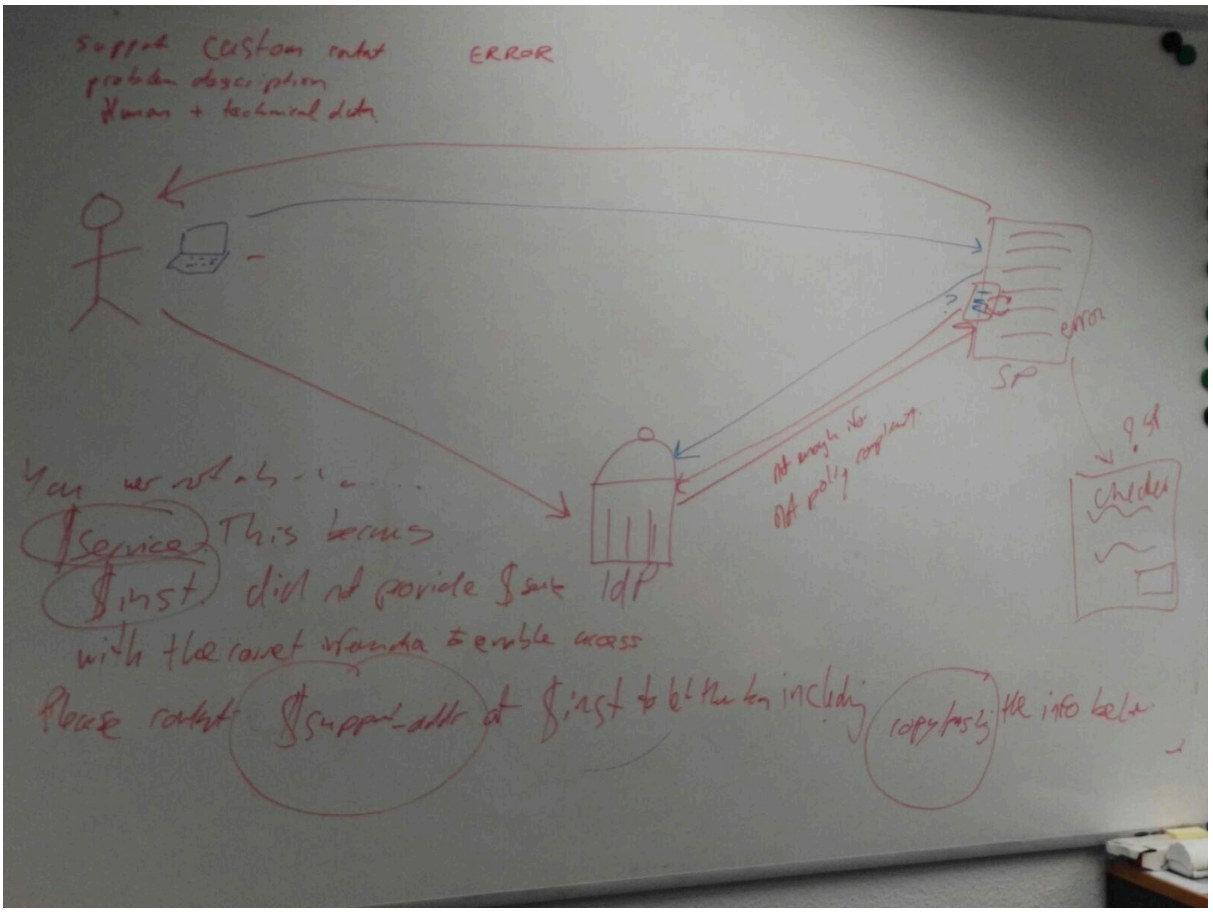
As you know, eduGAIN has been piloting enhanced support for complex interfederation troubleshooting. Following an analysis of the requirements for implementing Sirtfi, a central coordination element is foreseen. The workflows and systems for this are very similar, so after the summer holidays we will be looking at extending the eduGAIN support pilot to also cover Sirtfi. If you have any comments or feedback, please let us know.

Contact for this work is Thomas Baerecke (thomas.baerecke@switch.ch).

Pål Axelsson
On behalf of the GÉANT project Sirtfi Working group

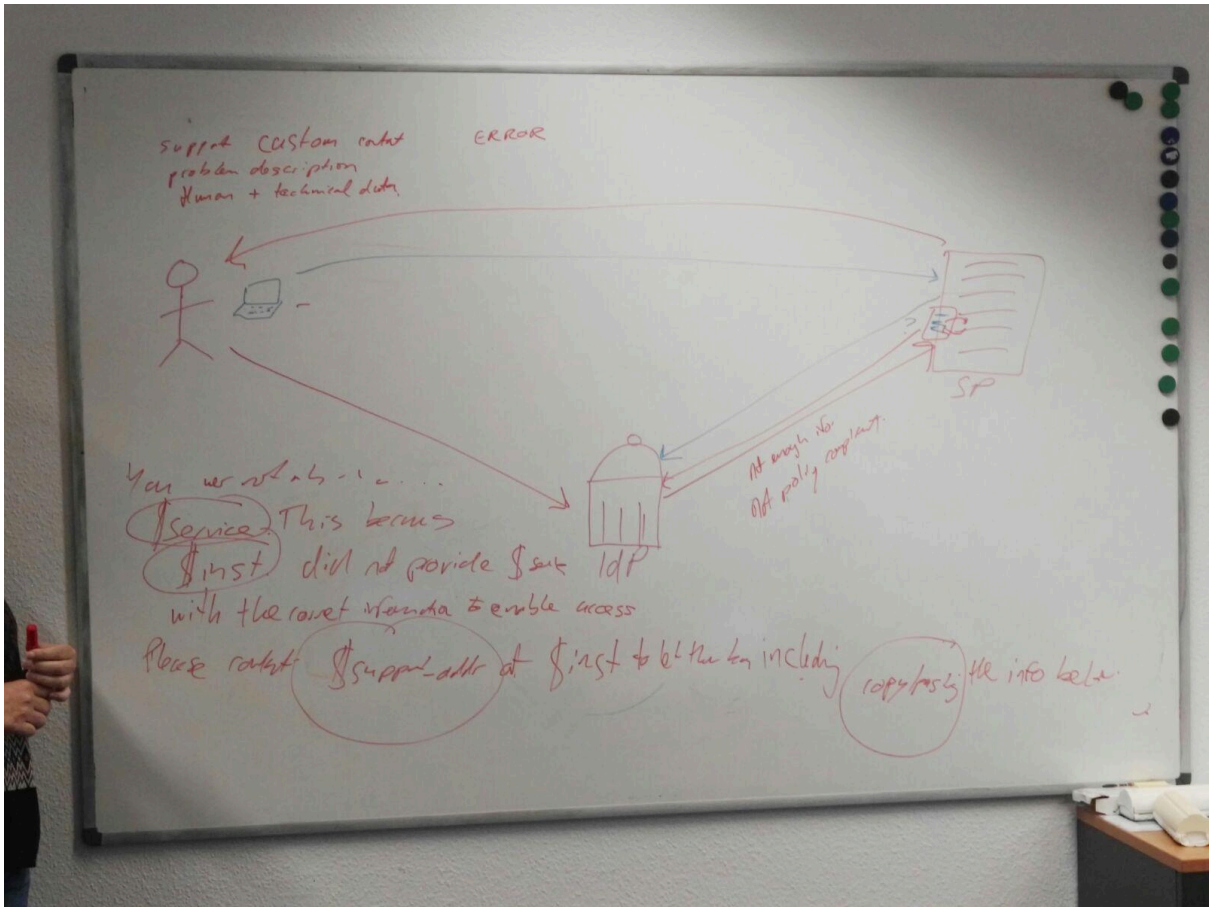
==========

WORKFLOW MODELLING FOR SIRTFI - USER EXPERIENCE / ERROR HANDLING



==========

Wrap up: VC in early September


support custom content
problem description
Human + technical data
ERROR
SP
IdP
$service
$inst
with the correct information to enable access
$support_url
copy/paste