TAS^3: Use Cases, User Interfaces Screens and Designs

Sampo Kellomäki (sampo@zxidp.org)

October 4, 2010

N.B. This document is heavily derived from `tas3-user-interface.pd` by the same author.

Contents

1 Intro

This document specifies some of the user interfaces that need to be developed for TAS^3. It attempts to consider the CC[1] view point and feasibility for implementing the user interfaces.

The inventory is as follows

1. SSO flow including

   a. IdP selection at SP

   b. Login at IdP

   c. Optional: selection of attributes to send from IdP to SP

   d. Optional: user consent to federation and/or sending attributes

   e. Visualization of the successful login at SP

   f. Local and Single Logout flows

   Most of the SSO flow is in-built to IdP and SP products. Only case of CC relevance would be if CC is used to build the SP. In essence CC provides a "fat client" approach to building a Web GUI and in that case CC would have to supply the IdP selection screen as well as visualization of successful login and the buttons for logout.

   The IdP selection problem is nontrivial as in Least Common Denominator browser assumption there is very little that can be taken for granted. Some designs assume Cookies will persist and use Common Domain Cookie approach (redirect browser to common domain where it can read a cookie indicating which IdP to use), but often users clear the cookies so more often than not this does not really work.

   If there was some persistent setting in the browser to indicate which IdP to use, this problem could be solved. Perhaps CC could somehow have such feature?

   When users choice of IdP can not be remembered (or choice has not been made yet), we are faced with presenting user with list of IdPs to choose from. In some early and trivial deployments there might only be one so the choice is easy. Or it may be possible to use some context, such as users source IP matching corporate or university network to suggest most probable IdP. But in general case, all IdPs that the SP is willing to work with may need to be presented. This can be quite a long list.

[1] Capitain Casa, a Java software toolkit and framework for building user interfaces.

Sometimes the IdP selection is factored out of SP into a special Where Are You From (WAYF) service. Such service may use CDC or other approaches already discussed, but ultimately it is not a magic bullet - same restrictions as in SP case apply.

Another attempt at solving this is the Card Space approach, where the browser is significantly enhanced to help user in choosing the IdP - the notion being that each IdP is repsented by a "card" and only the IdPs that user has relation ship with are shown, significantly reducing the number of choices that need to be presented to the user.

2. New SP intake. This is a business process implemented by either IdP or more generally the Trust Network operator (aka Trust Convener).

   There may be substantial CC scope in providing partner self registration and management GUIs as well as Trust Operator's back office for managing the partners. While certain technical fields must be collected (see screenshots), ultimately this is a business function where aspects like customer care (customer being the partner) and supporting workflows of call center staff are relevant.

3. New User intake. This is a business process typically implemented by IdP.

   There is substantial CC scope in providing the user self registration and management GUIs as well as IdP's back office for managing the users. While certain technical fields must be collected (see screenshots), ultimately this is a business function where aspects like customer care (customer being the user) and supporting workflows of call center staff are relevant.

   A particlar flow not currently depicted in this document is the password recover or reset flow.

   New user intake may also take the form of enterprise bulk provisioning of their entire employee base. There should be CC GUI for this, the audience being the HR department of the enterprise.

4. Privacy Manager. Privacy manager should be full fledged (Web) GUI allowing user to control every aspect of this public image.

   Designing the Privacy Manager Web GUI needs to take in account the multiple dimensions of the access control, such as

   i. Data group or data set

   ii. Data model or schema

   iii. Who asks. Which SP, which user, role

   iv. Time

v. Purpose, business process, business process model

vi. (Illegible)

Lex Pohlman of Kenteq has additional material on UI aspects of multidimensional policies.

5. Interaction for consent and simple permission. This is very limited Web GUI, typically realized as iFrame or Div tag.
6. Interaction for policy editing. More fully reatured cousin of the consent gathering. CC can provide significant improvement in interactivity of the policy editing. This may be part of the Privacy Manager (4).
7. Interaction for credentials and privacy negotiation
8. Interaction for Right of Access, Rectification, and Deletion

1.1 Issues to Consider

Sometopics I consider worthy of usability or user interface research.

1.1.1 Identification of Actors and User's Understanding of the Process

1. When accessing an application, will user understand that there are multiple actors at play?
2. When redirected from SP to IdP will user properly recognize that the IdP is an independent trusted party?
3. What can be done to improve user's understanding of party responsible for each step? We feel it is important from legal, responsibility, and good governance perspective that the users realistically understand who they are dealing with. Are standardized / regulated approaches needed? Or should this just be up to brand of the actor?
4. When we embed a link or user interface element (iFrame), will users correctly understand the provenance of such element? What can be done to improve this understanding? Will the measures be acceptable from convenience, commercial, and branding perspective?
5. What can be done to reduce phishing attacks?

6. Do we need business process overview or progress bar so the user realizes how many steps are still ahead? Should it be possible to go backwards in the process?

7. How to convey atomicity or final commitment to transaction? For example, after you already supplied credit card number (which gives SP the technical capability charge you), will an additional confirmation screen just confuse users? E.g. user supplies credit card and thinks that completed the transaction, but when he arrives to airport there is no ticket because he did not understand that a separate confirmation was needed.

8. Multistep wizards vs. single big screen that asks everything and gets the job done in ne step?

1.1.2 Service Discovery and Credentials and Privacy Negotiation

1. How to insert service selection into the user interface of the service requesting site?

2. How to repesent the ranking criteria? Do we allow user to sort or is this too complex?

> N.B. The default ranking is of great commercial interest (c.f. Google) and should be left for market or business model to determine. However, we are interested whether users really need to have ability to navigate other rankings if they so choose?

3. How complex should remembering choice of default service provider be for given type of service? Is it sufficient to have only one unambiguous default? Or should the default depend on who asks? Or persona? Should choice of default be automatic? If automatic, how to handle exceptional situations where the user does not want it to be automatic?

1.1.3 Policy Editing and User Consent

1. In contextualized incremental policy editing (i.e. asking the consent for specific data as the need arises), what ramifications need to be supported?

   a. Ability to see or edit the global policy?

   b. Ability to see or edit the actual data rather than just the policy?

   c. Ability to see past usage patterns and policy decisions?

2. How can all this be crammed in one user interface without making it cumbersome?

3. How to represent in the user interface the extreme multidimensionality of the general / global policy editing?

   Dimensions (each dimension can have hierarchy to represent scale):

   a. Resource, resource group (data item, data group)
   b. Who (human) asks, group the requester belongs to
   c. Who (server) asks, group the requester belongs to
   d. What is the role of requester? Groups of roles?
   e. What for? Categories of purpose? Specific business processes, business process models?
   f. Tempral dimension? Will the policy expire? Will it be valid only on work days?

   Some of the dimensions can morph into being just permission within some node definedon the grid. For example if the dimensions are Resource and Who, the Purpose dimension could simply be a bunch of itemized permissions that happen to be keyed on specific purposes, without the purpose being visualized as a dimension on its own right.

1.1.4 User data management

1. Dimensionality problem: How to enable user to visualize and edit personas and partial identities?

2. Are personas defined apriori or as the need arises? Are they keyed on "who asks"?

3. Ad-hoc persona formulation at the point of data request. What is right granularity? How to move from one-off persona to a reusable persona?

4. Will personas just confuse users? Do we need fixed categories like Work, Friends, and Family?

1.1.5 Audit Trail

1. How scared are users really about system showing them the internal reference IDs?

   For legal rigour, the reference IDs are essential. There has to be a details screen where they are available. However the theory I want to test is whether users would find a service more credible if it presented this detal up front, or whether the users would be scared away by the technical detail?

2. What is the appropriate "human readable" explanation of the audit trail records? Would such "human readable" interpretation detract from legal accuracy? Could this cause liability?

3. How will users react to the fact that the dasboard only shows summary records and not the actual data? N.B. We will not collect in Dashboard the actual data, because that would make the Dashboard an avenue of attack to get the data. We want the data authorities and data users to keep the data as long as they emit to the audit bus / dashboard comprehensive summary records.

4. What constitutes a relevant overview? Recent events? High value events? Events keyed on particularly sensitive information? How much filtering and discreation should user have?

5. Can user be considered notified by availability of audit trail? Or by having consulted the audit trail, even if the user has not actually read the record that was available to him?

2 Generalized Use Cases

> **Non-normative**. The simulated user interface screenshots in this section are NOT normative. They serve merely to illustrate one feasible way of designing the user interface. The user interface flows are also non-normative, for example the IdP detection or already-logged-in detection may follow different paths. Every step of the way, confirmation questions, wizards, and other user interface devices may be inserted. Depending on business model and branding choises of the Trust Network, there may be some graphical guidelines and restrictions, see [TAS3BIZ] and Governing Agreement of the Trust Network.

This section addresses *Req. D1.2-2.13-Easy*, among others.

These Use Cases deal with User Interaction, therefore they do not illustrate the rather large Web Services proportion that TAS^3 architecture mainly aims to address. Never-the-less, in a User Centric system, we must start with the user - without his impulse (direct or indirect) the back-end Web Services should never happen.

A general assumption has been that Single Sign-On (SSO) will be used, though some other approaches are foreseen as well. Long tail services should especially use SSO as it is unreasonable to ask for user registration for one-off service request.

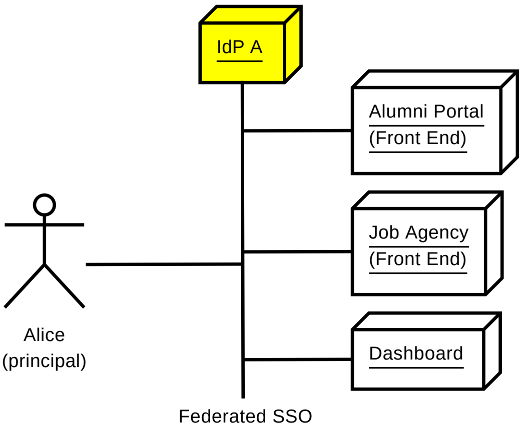


Figure 1: User accesses Front Ends using Single Sign-On.

> **Methodology**. In the Story Boards that follow, the sequence describes user's preception. It does NOT describe protocol flow, which can at times be quite different from User's preception. For example, many SSO protocols call for HTTP redirects, so technically speaking any transfer between screens should pass via User Agent. A big circle in diagram means a protocol step that usually is optimized so that no page is shown to the user (but astute users may notice some flicker). When the optimization for some reason does not work out, the regular user interface screen will be shown. We apply Cognitive Walkthrough method [Wharton94] to elaborate the story boards.

Further technical use cases are presented in the next chapter. While use cases in this section aim at illustrating a possible user experience, the use cases in the next chapter mainly aim at scenarios that allow all TAS^3 functionality to be exercised and tested systematically.

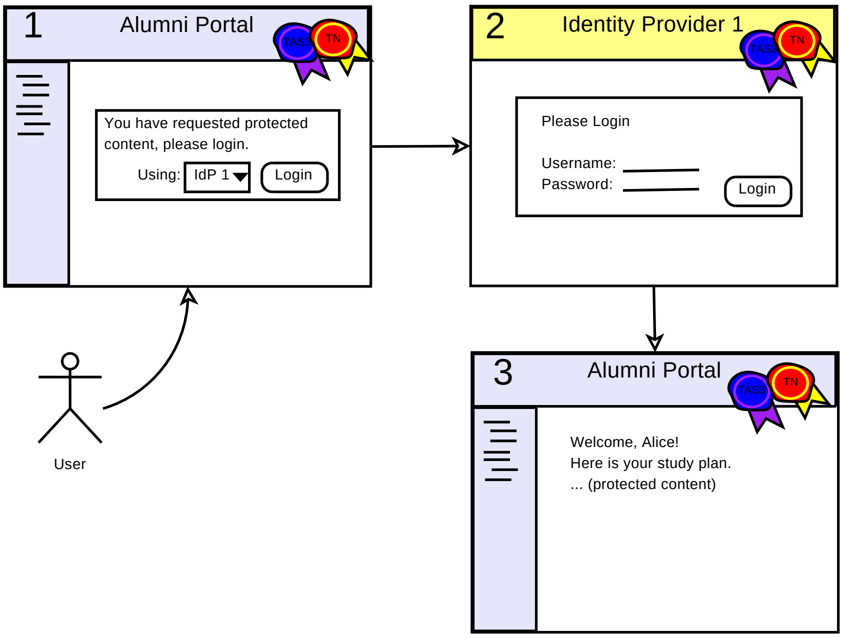
2.1 User Uses Service (First Time in the Session)

The first time use of a service in a session consists of

- First the User interacts with the Front End (FE)
- The User is redirected to IdP (cf. Req 3.1 Existing Accounts)
- The User logs in at IdP
- The User is redirected back to the protected content

This means minimum three steps, but there could be more if there are confirmation questions.

Trust Seals. As can be seen, the user interface is expected to display trust seal of the Trust Network and may display TAS^3 seal as well. These are intended as visible indicators that public associates with trust. Their exact design and realization, including the possibility of not displaying them at all, will depend on the particular Trust Network.



You have requested protected content, please login.

Welcome, Alice!
Here is your study plan.
... (protected content)

Figure 2: Story board: Using service for 1st time in a session.

Cognitive Walkthrough

1. **Choice of IdP**

   Motivation User has taken initiative to perform a task he thinks can be accomplished using a web site. He realizes that some form of authentication or authorization will be required. When the User navigates to the task, a dialog is presented asking for authentication so that authorization can be granted. User will consider engaging in this dialog because he feels the sytem is trustworthy, based on the Trust Seals and based on past successful experiences.

   Available and understandable User will be guided by modality of the interaction to a situation where he will either have to proceed with selection of an IdP or will have to abandon the task. Choosing another task that does not require authentication is also an option. The interaction should be structured such that the requirement for authentication will become evident early on, so that User avoids performing work only to find out that he is unable to proceed.

   Feedback The available IdP choices that are presented should be as narrow and relevant as possible. Federated SSO research recognizes the IdP selection as a major problem. A profileration of case specific solutions have been proposed, but no generic and universally accepted approach has emerged as of 2010. Once IdP is chosen and button is pressed, clear feedback is provided that User has landed on the IdP web site. The IdP screen should provide contextual information about the task which motivated the authentication (such feedback is lacking in step 2 of Fig-2).

2. **Login**

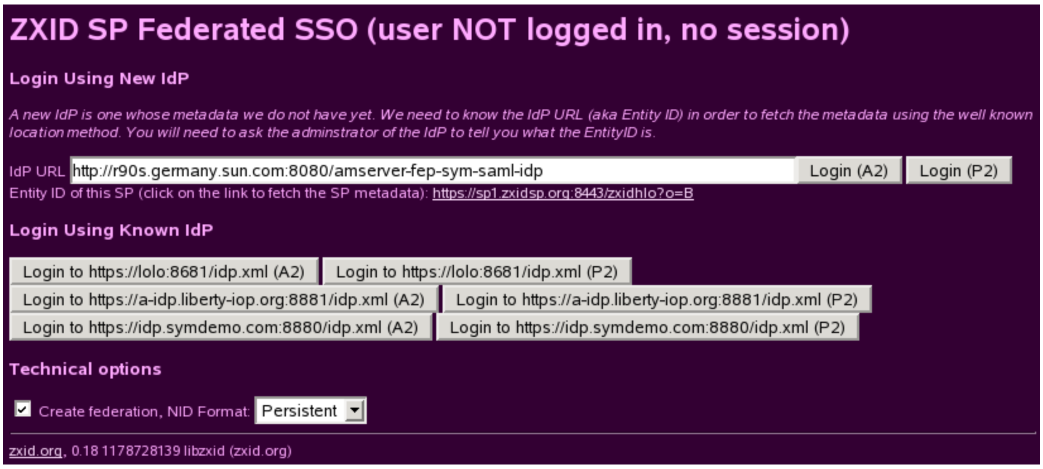
   Motivation User is in the mind set of completing a task and will perform this step if he reasonably can. This mind set is reinforced by IdP providing feedback as to what task requires the authentication.

   Biggest challenge and incovenience for the User will be the necessity to present authentication credentials. This inconvenience can be mitigated by use of Single Sign-On.

   Available and understandable Availability of the logon and the acceptable forms of credentials should be self-evident from the first screen of the IdP. First screen should lay visible all options and avoid any hierarchical navigation to arrive to the desired option.

   Feedback Successful authentication will lead to User being returned to the Front End web site. This in itself is a form of feedback, but it should be reinforced by the web site providing a clear welcome greeting, stating that the User has been authenticated (and possibly authorized as well).

3. **Login complete**. This use case ends here, but an application specific use case will start here.



ZXID SP Federated SSO (user NOT logged in, no session)

Login Using New IdP

A new IdP is one whose metadata we do not have yet. We need to know the IdP URL (aka Entity ID) in order to fetch the metadata using the well known location method. You will need to ask the adminstrator of the IdP to tell you what the EntityID is.

IdP URL http://r90s.germany.sun.com:8080/amserver-fep-sym-saml-idp

Entity ID of this SP (click on the link to fetch the SP metadata): https://sp1.zxidsp.org:8443/zxidhlo?o=B

Login Using Known IdP

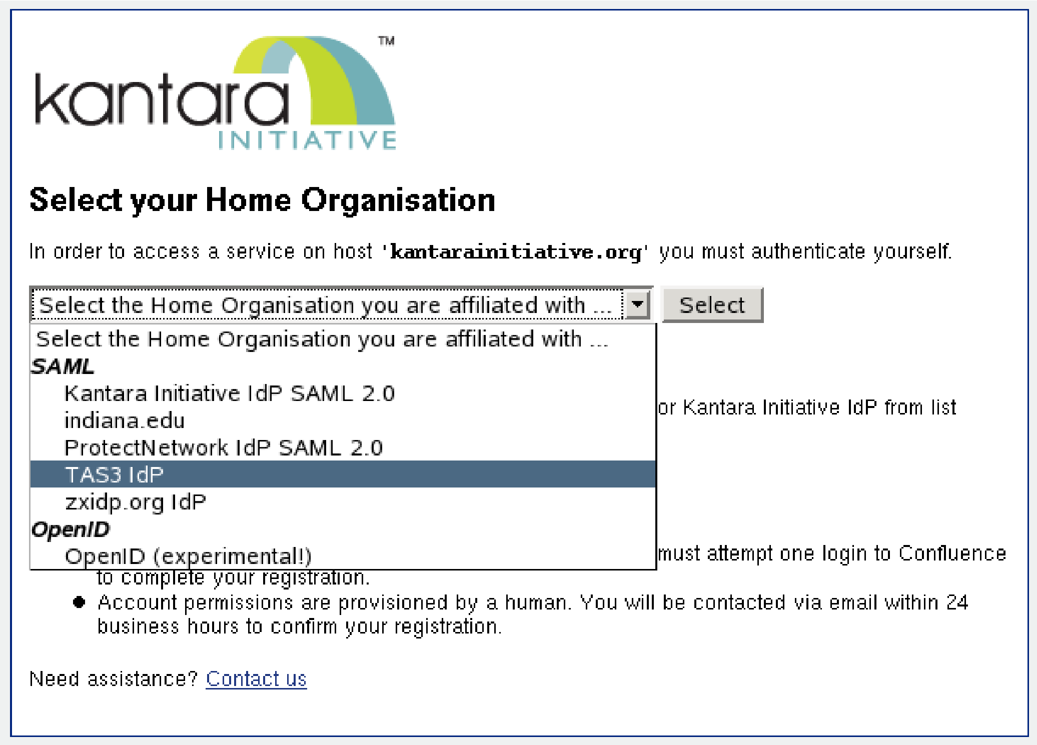
Technical options

☑ Create federation, NID Format: Persistent

zxid.org, 0.18 1178728139 libzxid (zxid.org)

Login (A2)
Login (P2)
Login to https://lolo:8681/idp.xml (A2)
Login to https://lolo:8681/idp.xml (P2)
Login to https://a-idp.liberty-iop.org:8881/idp.xml (A2)
Login to https://a-idp.liberty-iop.org:8881/idp.xml (P2)
Login to https://idp.symdemo.com:8880/idp.xml (A2)
Login to https://idp.symdemo.com:8880/idp.xml (P2)

Figure 3: An early version of ZXID SP's IdP selection, illustrating IdP URL entry by user (allowing any IdP to be used) and presentation of preconfigured choices as buttons (they could also be IdP logo images to provide branding). The button approach has the advantage of showing all options at once and only requiring single click to move on from the screen. It has difficulty in presenting large number of IdPs (more than about 10).



Select your Home Organisation

In order to access a service on host '**kantarainitiative.org**' you must authenticate yourself.

Select the Home Organisation you are affiliated with ...
Select
Select the Home Organisation you are affiliated with ...
SAML
Kantara Initiative IdP SAML 2.0
indiana.edu
ProtectNetwork IdP SAML 2.0
TAS3 IdP
zxidp.org IdP
OpenID
OpenID (experimental!)

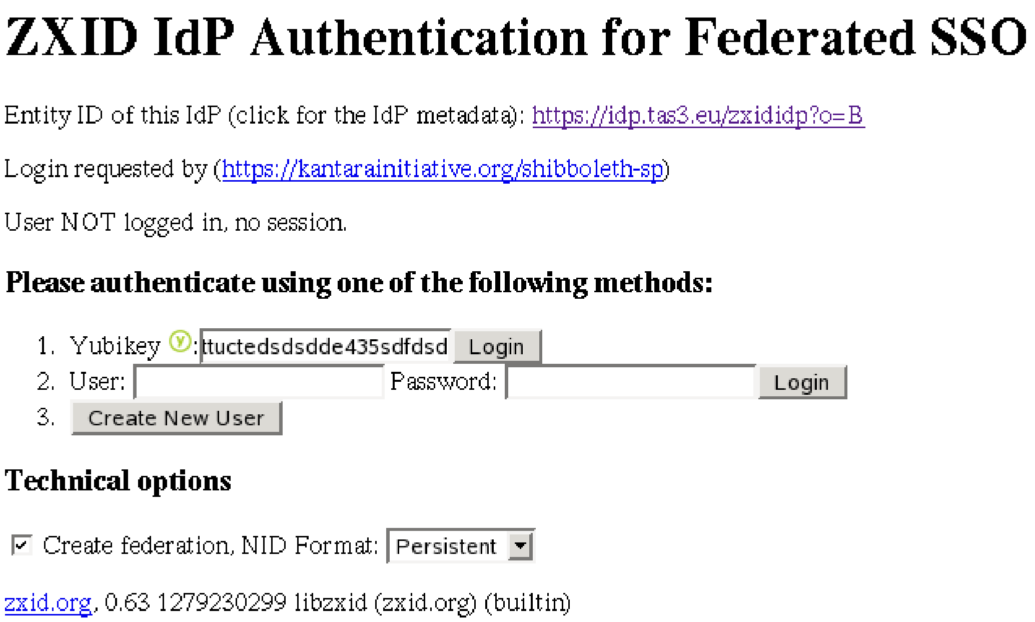
or Kantara Initiative IdP from list

must attempt one login to Confluence to complete your registration.

- Account permissions are provisioned by a human. You will be contacted via email within 24 business hours to confirm your registration.

Need assistance? Contact us

Figure 4: IdP Selection screen of Kantara Initiative WAYF service. This illustrates the popup menu approach with some styling and hierarchical structure in the menu to help user quickly locate the IdP. The popup approach can comforably handle about 30-40 IdPs and starts to be untractable after about 200 IdPs.



ZXID IdP Authentication for Federated SSO

Entity ID of this IdP (click for the IdP metadata): https://idp.tas3.eu/zxididp?o=B

Login requested by (https://kantarainitiative.org/shibboleth-sp)

User NOT logged in, no session.

Please authenticate using one of the following methods:

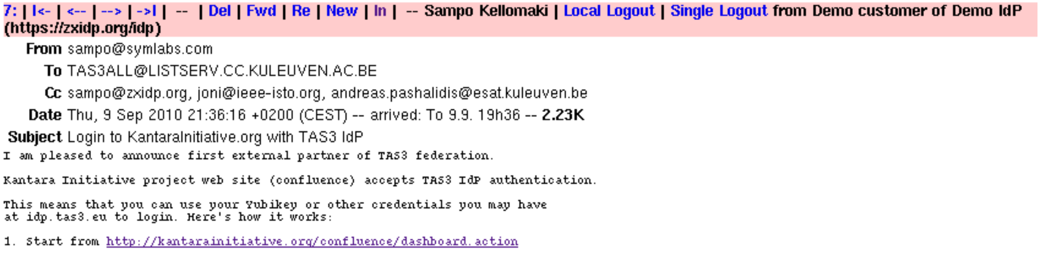
1. Yubikey: ttuctedsdsdde435sdfdsd Login
2. User: Password: Login
3. Create New User

Technical options

☑ Create federation, NID Format: Persistent

zxid.org, 0.63 1279230299 libzxid (zxid.org) (builtin)

Figure 5: Login screen of TAS3 IdP. Note identification of the IdP itself and the SP requesting the SSO (the SP identification could be more user friendly, e.g. showing SP's common name or logo). Users (lack of) session status is made very clear. The two supported authentication methods are offered. A link to new user intake process is offered. The "Technical options" can have fixed values and need not appear in production user interface.



7: | |<- | <-- | --> | ->| | -- | Del | Fwd | Re | New | In | -- Sampo Kellomaki | Local Logout | Single Logout from Demo customer of Demo IdP (https://zxidp.org/idp)

From sampo@symlabs.com
To TAS3ALL@LISTSERV.CC.KULEUVEN.AC.BE
Cc sampo@zxidp.org, joni@ieee-isto.org, andreas.pashalidis@esat.kuleuven.be
Date Thu, 9 Sep 2010 21:36:16 +0200 (CEST) -- arrived: To 9.9. 19h36 -- **2.23K**
Subject Login to KantaraInitiative.org with TAS3 IdP

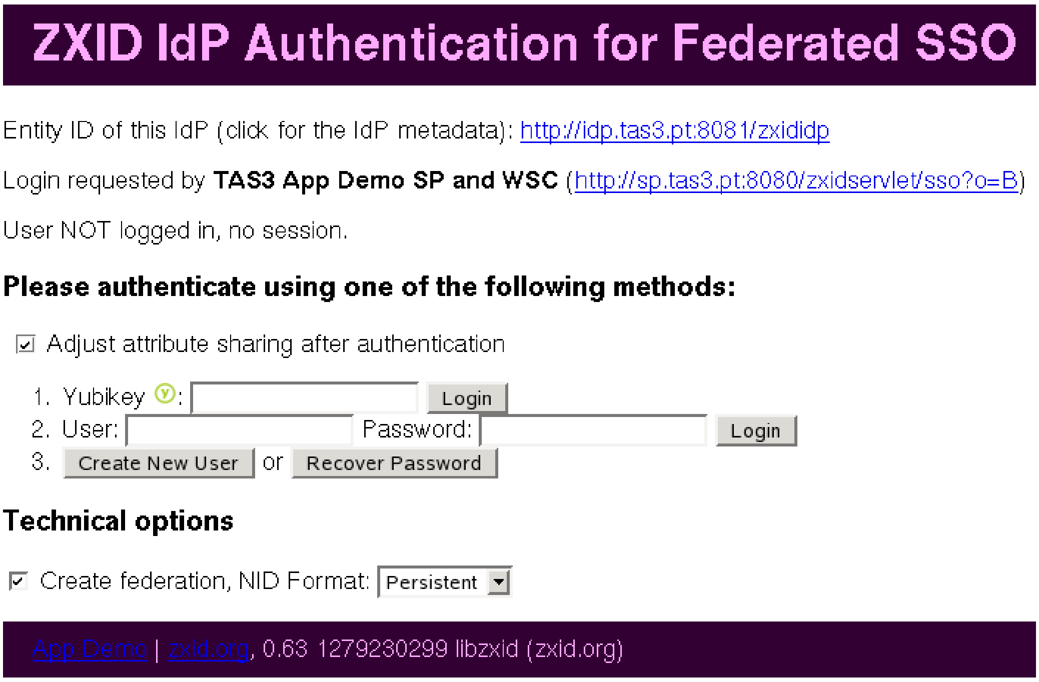
```
I am pleased to announce first external partner of TAS3 federation.

Kantara Initiative project web site (confluence) accepts TAS3 IdP authentication.

This means that you can use your Yubikey or other credentials you may have
at idp.tas3.eu to login. Here's how it works:

1. Start from http://kantarainitiative.org/confluence/dashboard.action
```

Figure 6: A Web Mail application (`pdmail.pl`, using Net::SAML perl module) showing user logged in on the status line. As can be seen, user's Common Name (or nickname) is displayed to greet the user in a friendly way. Appearance of this attribute from SSO reassures the user that SSO was successful and meaningful. Also displayed is the common name or nickname of the IdP that authenticated the user. Finally, we see the Local Logout and Single Logout options. It is important to offer the user at all points an easy way to logout from all places (think leaving internet cafe).



ZXID IdP Authentication for Federated SSO

Entity ID of this IdP (click for the IdP metadata): http://idp.tas3.pt:8081/zxididp

Login requested by **TAS3 App Demo SP and WSC** (http://sp.tas3.pt:8080/zxidservlet/sso?o=B)

User NOT logged in, no session.

Please authenticate using one of the following methods:

☑ Adjust attribute sharing after authentication

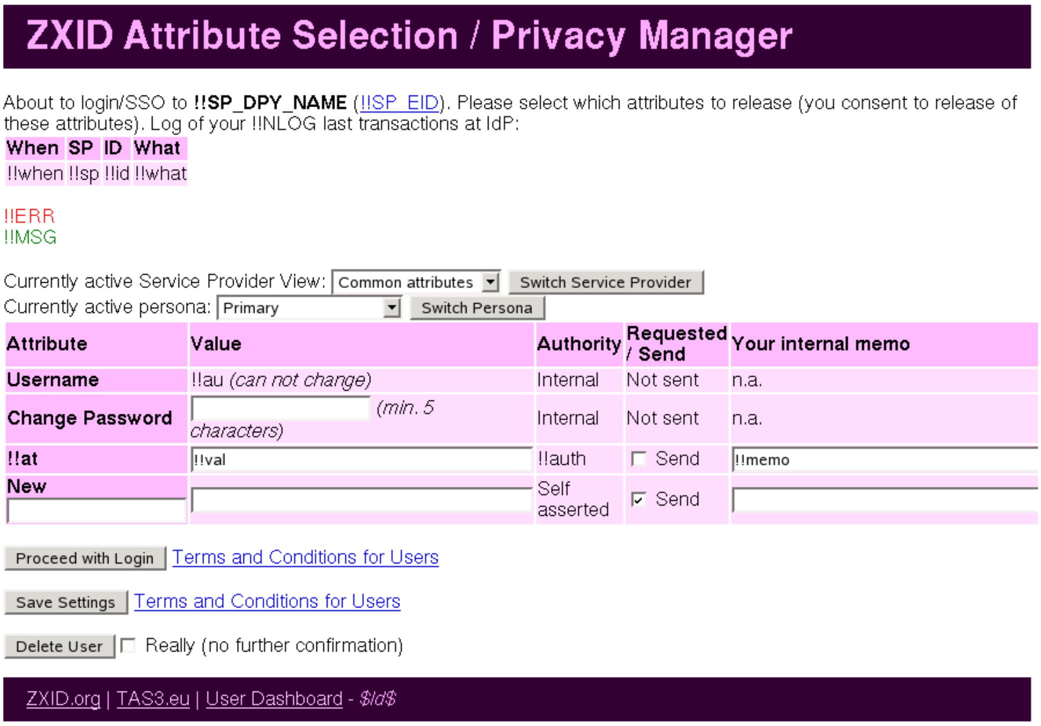
1. Yubikey: ____ Login
2. User: ____ Password: ____ Login
3. Create New User or Recover Password

Technical options

☑ Create federation, NID Format: Persistent

App Demo | zxid.org, 0.63 1279230299 libzxid (zxid.org)

Figure 7: Login screen can offer user to select attributes that are passed (pushed) upon login. If user checks "Adjust attribute sharing", he will pass through a screen allowing fine grained tweaking of what attributes should pass.



ZXID Attribute Selection / Privacy Manager

About to login/SSO to **!!SP_DPY_NAME** (!!SP_EID). Please select which attributes to release (you consent to release of these attributes). Log of your !!NLOG last transactions at IdP:

When	SP	ID	What
!!when	!!sp	!!id	!!what

!!ERR
!!MSG

Currently active Service Provider View: Common attributes
Currently active persona: Primary

Attribute	Value	Authority	Requested / Send	Your internal memo
Username	!!au *(can not change)*	Internal	Not sent	n.a.
Change Password	*(min. 5 characters)*	Internal	Not sent	n.a.
!!at	!!val	!!auth	☐ Send	!!memo
New		Self asserted	☑ Send	

Terms and Conditions for Users

Terms and Conditions for Users

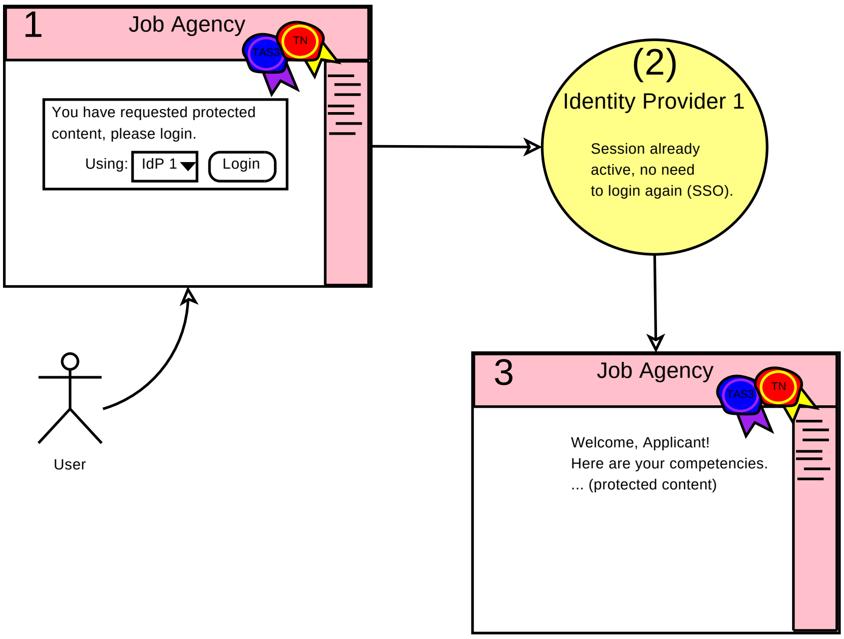
☐ Really (no further confirmation)

ZXID.org | TAS3.eu | User Dashboard - *Id*

Figure 8: After login screen, user gets to choose which attributes to pass. The choice can be saved as permanent policy or setting. Note the visualization of the recent transactions involving user's attributes. This serves to raise user awareness so that he may detect any inapproriate use sooner. N.B. This screen shot is from GUI template and not from actually functional GUI. In general the login time attribute selection is similar to the original user intake process where default sharing status of the attributes was set. Editing the attribute valuse in this screen does not change them globally, but rather takes effect only for this transaction (should these be remembered per SP?).

2.2 Already-Logged-in Optimization (SSO)

Same as above, but without IdP authenticating the user again. The flow does not need to stop at IdP at all. Optimized SSO use case, showing the full convenience of SSO, leading to 2 step process.



You have requested protected content, please login.

Session already active, no need to login again (SSO).

Welcome, Applicant!
Here are your competencies.
... (protected content)

Figure 9: Story board: Using further services after logging in at IdP - Single Sign-On (SSO).

Cognitive Walkthrough

1. **Choice of IdP**: Same cognitive walkthrough as in previous section.
2. **Login**: No cognitive walkthrough needed as no user interface will be presented.
3. **Login complete**. This use case ends here, but an application specific use case will start here.

2.3 User Uses Dashboard

This use case addresses Reqs. *D1.2-2.11-Transp* and *D1.2-3.3-Dash*.

In this use case the user interacts with the TAS3 Dashboard in order to determine the status of a business process he is engaged in. It consists of the following steps:

- The user logs into the Dashboard (possibly using SSO)
- The user sees a page with an overview of the transactions
- The user drills down to visualise a particular business process.
- The user views a particular audit trail and discovers a suspect item.
- The user requests a legally binding audit statement about the transaction.
- Competent authority requests further information about the transaction from the Service Provider that holds the detailed audit trail.

Cognitive Walkthrough

1. **Engaging Dashboard and Choice of IdP**

   Motivation User has taken initiative to find out about the state of some business process or the handing of his PII. User understands, due to training or awareness campaigns, or because a noice was given in the beginning of the business process, that this is possible. User may have found out about the possibility by surfing the web or through a search engine. The mere possibility may spark the User's interest and get him to try the Dashboard out. User may also have noticed an irregularity or complained to some instance and been told to consult his Dashboard.

   Available and understandable Since User is assumed to take initiative, a major hurdle will be how the user finds out about the Dashboard and how to contact it. Some possibilities

   a. A link to the Dashboard is provided as part of the user interface of each business process.
   b. A link to Dashboard is provided in every web site that participates in the Trust Network.
   c. Trust Network operates some sort of a portal and the link can be found there.
   d. Dashboard engages in Search Engine Optimization (SEO) so that User is sure to find the Dashboard through a popular search engine.

   Once the user has found out about the Dashboard, the problem shifts to the IdP selection and authentication. In Fig-10 we have assumed that IdP can be detected and User is already logged in, as the case typically would be immediately after engaging some Front End (e.g. the Job Agency).

However, if time has passed, user may need to choose explicitly an IdP and explicitly authenticate, as in Section "User Uses Service (First Time in the Session)". A confusing situation can arise where user has tried to access the Dashboard, but the first screen he sees is the IdP authentication screen (because IdP detection worked, but user was not logged in yet). This situation should be mitigated either by IdP providing enough context about the operation that is motivating the authentication, or by the Dashboard imposing a splash screen even when IdP choice is already known.

Feedback If IdP was detected and user was already logged in, the first feedback will be Dashboard logged in welcome screen. If authentication is needed, then the IdP context message or the splash screen solutions should be adopted, as described in the previous paragraph.

2. **Login**: no specific cognitive walkthrough requirements. See discussion in in the First Time use case.

3. **Choose Business Process to Audit**

   Motivation User set out on his quest to perform this task.

   Available and understandable The list of the business process instances should be structured so that all business process instances are reachable while at the same time the processes user is most likely to be interested in are presented first or more prominently. Due to potentially large number of processes, we may need to resort to hierarchy or search functions. An ontology of business processes will help in setting up the hierachy and search.

   The business processes should be titled and described in language that the User can relate to. In particular, while codes can be provided for accuracy and reference, every business process should have a human readable name. The resultant translation issues will have to be recognized and addressed.

   Feedback Choice of a business process instance will lead to its visualization where User can clearly identify What, Who, When, and similar information so that user can confirm he has made the right choice. If choice was wrong, User should easily be able to choose another instance.

4. **Choose Detail of Business Process Instance to Audit**

   Motivation Once user sees visualization of the business process instance, he will need to drill down to relevant detail. This may be driven by User's curiosity or perceived notion of culpable part.

Available and understandable The visualization has to be structured so that it honestly depicts the essence of the business process without cluttering the view with details that can be reached later. Every step that User is expected to perform (or has already performed) should be visible as well as major processing steps that are not in User's control, especially those that involve transfer or manipulation of PII.

All descriptions of the steps should be succinct and in human language, with translation issues addressed. Codes and references for the instance and steps can be provided for accuracy, but these should never supplant the human description.

To assist User in drilling into detail, the user interface should make it patently evident where this possibility exists, e.g. by using high-lighting techniques.

Feedback User is assisted in contemplating the choice of drill-in by high-lighting of available options. Once a step is chosen for scrutiny, user will see visualization of that step in great detail. The visualization will be titled in such a way that it is evident to the User that it pertains to the step he chose in the business process instance overview.

5. **View detailed description** This screen shows on human understandable terms what the substance of the transaction is. However, the detailed evidence only appears in the next screen. The idea is that this screen is approachable to an avarage user, without scaring them with the reference IDs.

6. **View evidence and request audit item from Front End**

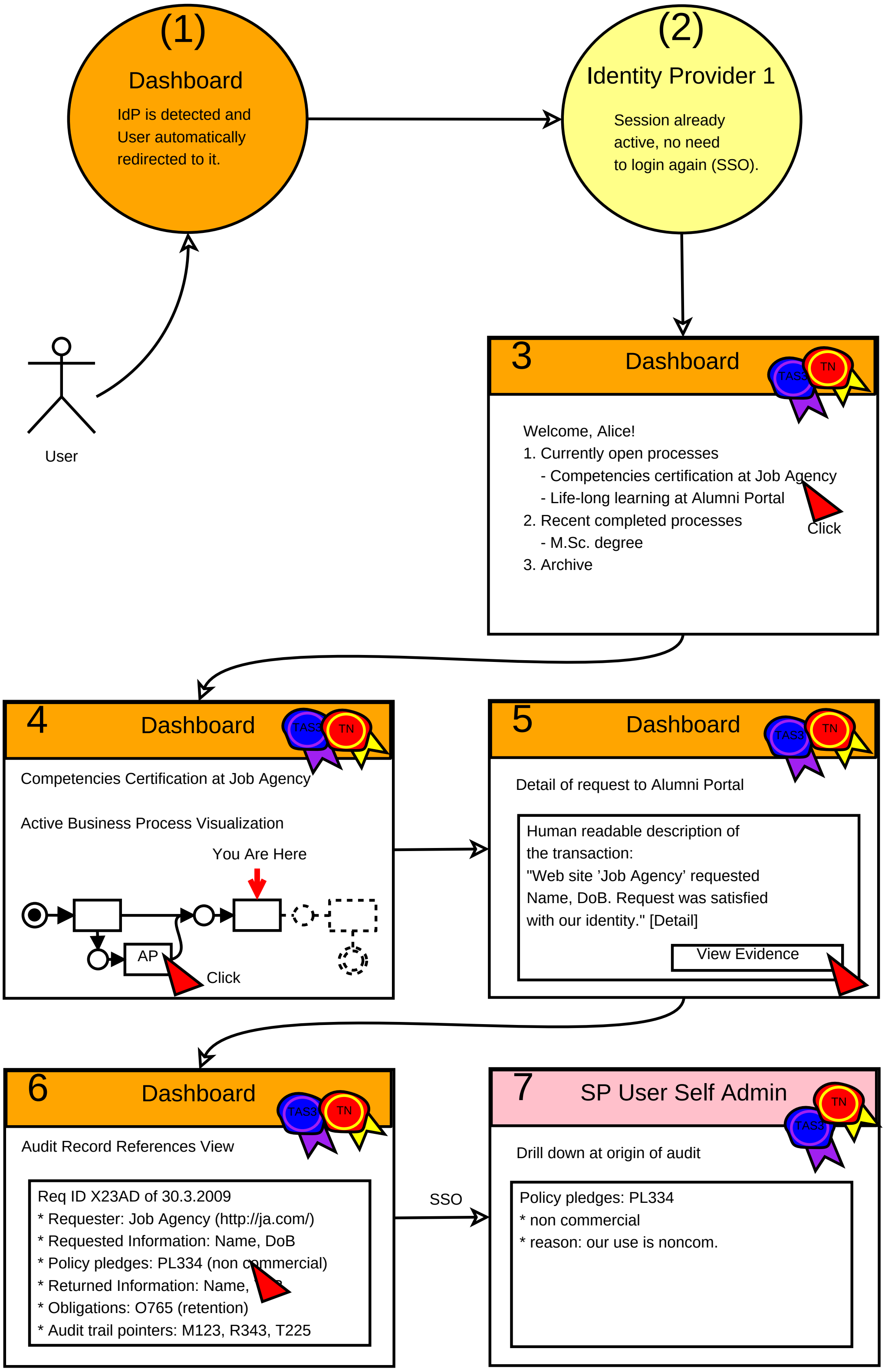
Motivation To request corrective action, user needs to get evidence and reference pointers. Knowing a transaction id is often a requirement for making a request for disclosure of specific items of audit trail. It is also easier to get a court order compelling a release of an audit record when request is specific and well itemized.

7. **View audit item** By clicking on a piece of evidence, user is transferred to Self Administration system of the site where the transaction originally happened (the transfer will require user to perform SSO to the SP, but this is transparent as the user is already logged in the IdP).

8. **Escalate** (not depicted in the figure) (Req. *D1.2-6.9-Complaint*)

If the SP refuses to collaborate with the user in self audit, the user can always pursue the matter in courts, using the evidence he holds in the dashboard.

2.3 User Uses Dashboard


(1)

Dashboard

IdP is detected and User automatically redirected to it.

(2)

Identity Provider 1

Session already active, no need to login again (SSO).

3 Dashboard

Welcome, Alice!

1. Currently open processes
   - Competencies certification at Job Agency
   - Life-long learning at Alumni Portal
2. Recent completed processes
   - M.Sc. degree
3. Archive

4 Dashboard

Competencies Certification at Job Agency

Active Business Process Visualization

You Are Here

5 Dashboard

Detail of request to Alumni Portal

Human readable description of the transaction: "Web site 'Job Agency' requested Name, DoB. Request was satisfied with our identity." [Detail]

View Evidence

6 Dashboard

Audit Record References View

Req ID X23AD of 30.3.2009
* Requester: Job Agency (http://ja.com/)
* Requested Information: Name, DoB
* Policy pledges: PL334 (non commercial)
* Returned Information: Name, ?
* Obligations: O765 (retention)
* Audit trail pointers: M123, R343, T225

7 SP User Self Admin

Drill down at origin of audit

Policy pledges: PL334
* non commercial
* reason: our use is noncom.

Figure 10: Story board: Using Dashboard to audit a business process.

2.3.1 Analysis of Google Dashboard (not apples-to-apples)

Dashboard is becoming an overused and loaded word. Different authors mean different things by it. Dashboards are common in business intelligence world where a dasboard usually represents some configured combination of interesting queries against data warehouse.

TAS^3 dashboard has special focus on data usage visibility and user's independent ability to audit what happens to their data. TAS^3 dashboard tries to provide a legal basis for corrective action by the user in case a SP does not collaborate. Other dashboards usually start from the perspective of user not questioning the validity of use of data and instead try to add value by making useful business intelligence available to the user. Google dashboard is a typical example. It is not independent in that it is the holder of the data, Google, that also provides the dashboard. Thus it can be seen that the aims of Google dashboard are dissimilar to TAS^3 dashboard. Never-the-less, it is educative to analyze the Google Dashboard.

GRAPHIC (../google/google-dash-top)

Figure 11: Some of the top level options of Google dashboard.

Fig-**??**, we see some of the items shown on the top level of Google dashboard. The main problem with this information is that user is not provided with prioritized summary, cf. screen 3 of Fig-10 where most recent is taken to be most relevant. Instead Google chooses to fragment the data across many services, making it difficult to have a quick summary glance.

The Google Dashboard figures presented here have some personal information blanked out with black boxes. It is instructive to observe the amount of PII (Personally Identifiable Information) that had to be blanked out.

Lets now examine some of the drill-ins available on Google Dashboard.

GRAPHIC (../google/google-dash-docs)

Figure 12: Google dashboard: information about shared documents.

Fig-**??** illustrates how shared documents are visualized to the user. The fact that sharing has happened is mostly visible, but specifics are rather scarce. In particular, there are no audit record or policy references that would allow a user to intitiate a due diligence process to understand why the sharing was authorized.

Another interesting feature is the use of email address to identify the collaborators in sharing. Basically this constitutes a golbally unique identifier. It may seem natural in the context of sharing via email, but that does not make it any less perilous. A pairwise pseudonymous identifier architecture would protect the privacy of the collaborators better (but potentially make the listing more cumbersome for the user, unless some nicknames were displayed). On the positive side, the collaborators are not directly shown - instead just the aggregate count is shown.

GRAPHIC (../google/google-dash-webhist)

Figure 13: Google dashboard: Information about web history.

Fig-**??** shows how the history of user initiated searches is visualized. Again we can see total lack of references to any audit records.

What is more, Google Dashboard does not appear to offer any functionality to determine who searched me! All accesses to my data, that are not in form of narrow category of document access, are simply omitted from the Dashboard. It is possible that Google would like to sell this interesting information to its users in form of "analytics" service. As we were unwilling to become Google's customers on this level, we were not able to explore what was avalaible (or not) on that level.

Conclusion is that Google Dashboard is a good example of customer self administration interface that every responsible data holder should provide, but it fails to address legitimate custmer needs for accountability of a service. Thus TAS^3 dashboard can complement the Google Dashboard.

2.4 IdP Detected-Optimization (SSO)

This flow, see Fig-14, can further optimize the already logged in case by allowing the Job Agency to detect that the user has already chosen IdP and therefore use the IdP to log the User in automatically. Essentially the ceremony becomes a one step process.

2.5 User Uses Service, Identity Selector Case (e.g. CardSpace, InfoCard)

In the Identity Selector flow, see Fig-15, the User never interacts with the IdP directly. Instead, the Identity Selector provides a user interface (step 3) for the IdP to query authentication credentials. User experience is entirely managed by the "ceremony" that the Identity Selector presents.

> N.B. As of Sept 2010, our thinking has shifted and we now see the selection of *personas* as a viable alternative to the Identity Selector paradigm.

2.5 User Uses Service, Identity Selector Case (e.g. CardSpace, InfoCard)

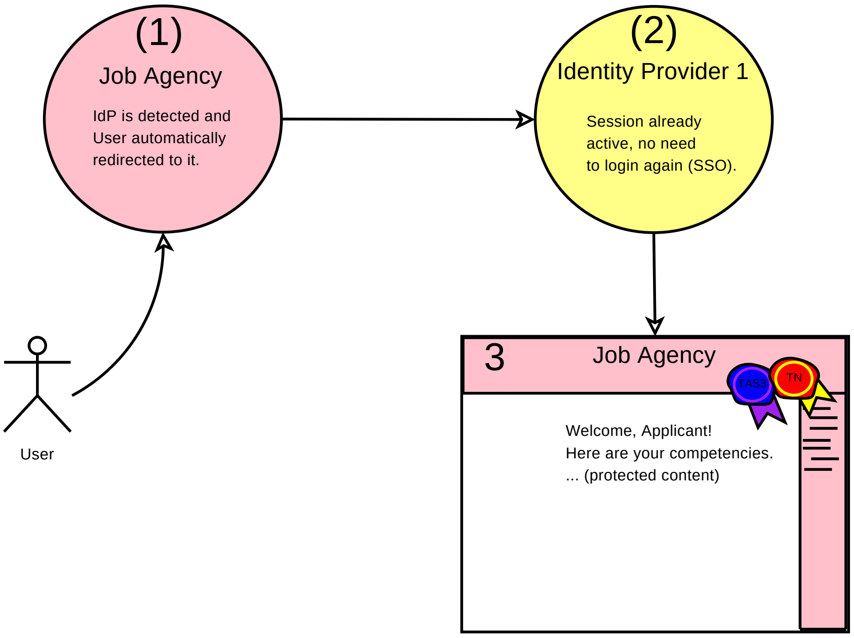

(1)
Job Agency
IdP is detected and User automatically redirected to it.
(2)
Identity Provider 1
Session already active, no need to login again (SSO).
User
3
Job Agency
TAS3
TN
Welcome, Applicant!
Here are your competencies.
... (protected content)

Figure 14: Story board: Fully automatic login - Single Sign-On (SSO) - when IdP can be detected.

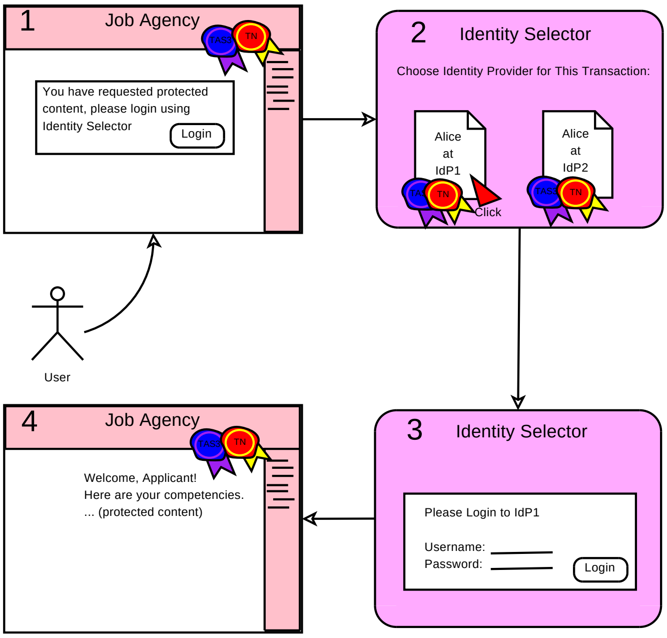


Figure 15: Story board: Identity Selector provides IdP User Interface.

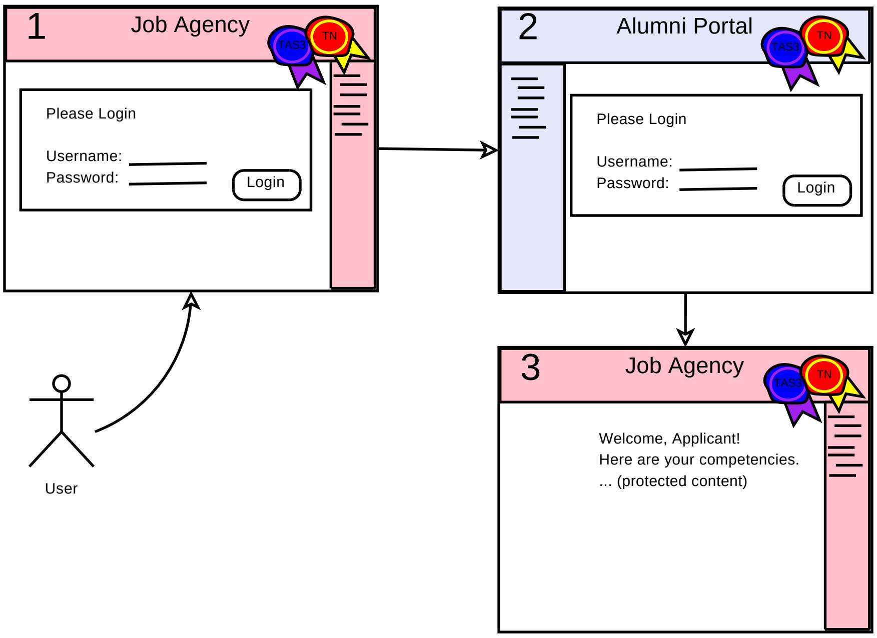


Figure 16: Story board: Using services with local login (not recommended).

2.6 User Uses Service, Local Login Case (not recommended)

> N.B. This use case is **not recommended**. You should use SSO based approaches instead. We document it here only to illustrate the problems associated with multiple logins.

The assumption is that the user will use more than one service. This highlights the inconvenience of user having to authenticate separately to each service. There are further complications under the hood, not least of which are privacy threats. This scenario could be called explicit account linking. While we consider supporting this scenario to be in scope, we do not recommend it unless there is no alternative, or as temporary solution.

Cons Avoid local logins because

- User management overhead due to lost passwords
- Users will use same password on many web sites. This means the web sites can impersonate the user towards each other. Not secure. Not accountable: user can repudiate by claiming that someone impersonated him.

- If you do not let user's pick the password, then they will just write it down. Not secure. Even the very registration mail where you tell what the user's password is, is a security threat.
- Managing strong auth locally is more costly than managing it centrally via IdP.

2.7 User Uses Service, Proxy IdP Case

This sequence, see Fig-17, illustrates the experience of a user logging in to SP that does not directly trust his IdP. The trust is mediated by the "middle" IdP that SP trusts.

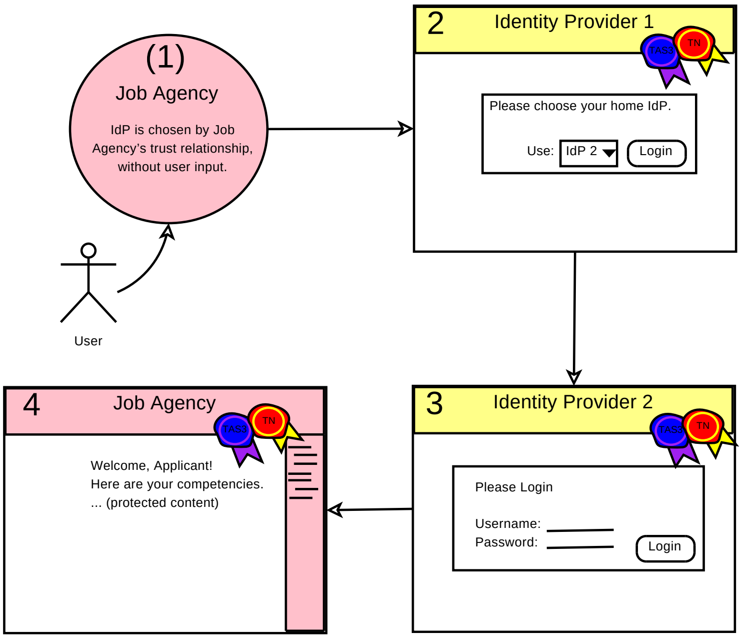


Figure 17: Story board: Login using IdP not trusted by Job Agency.

This sequence can be further optimized if the middle IdP can somehow automatically detect which IdP is the home IdP (similar to Section IdP Detected Optimization SSO) and, of course, if the User is already logged in the SSO optimization of Section Already Logged-in Optimization SSO.

2.8 Consenting to PII Release or Manipulation

This section addresses Reqs. *D1.2-6.3-WhatHowWhyWho*, *D1.2-6.6-Consent*, *D1.2-6.7-Reconsent*, *D1.2-4.1-EnfUCPol*.

2.8.1 Interaction on Front Channel

The obvious choice of having the requesting SP collect User's consent has an obvious conflict of interest issue. In some legal contexts this may be acceptable, but in general we need a way for either the releasing party or some Trusted Third Party to collect the consent.

Alternatively, not shown here, the user may explicitly provide his consent by authenticating to the releasing party and authorising it to release the PII to the SP. Further user cases for accessing releasing parties who are repositories and authorising third party access to repository contents are provided in [TAS3D42Repo].

Cognitive Walkthrough

1. **IdP choice as usual**
2. **Authentication as usual**
3. **User triggers action, as usual**
4. **Consent to release of PII**

   Motivation User will be motivated to take action because it is imposed to him by the modal flow of the interaction. User will be pleased to take action because asking consent is in his protection, but Users do get annoyed if you ask too often - to solve this we would need Privacy Agent, whose Use Cases are to be elaborated later (M30 D2.1?).

   Available and understandable Presentation of the consent question is a major challenge. It needs to be succinct, yet comprehensive and legally binding. Some Users will want high degree of detail and control, while others will be confused by too many options. Fig-18 depicts a dummied-down interface. This may not be appropriate for some users.

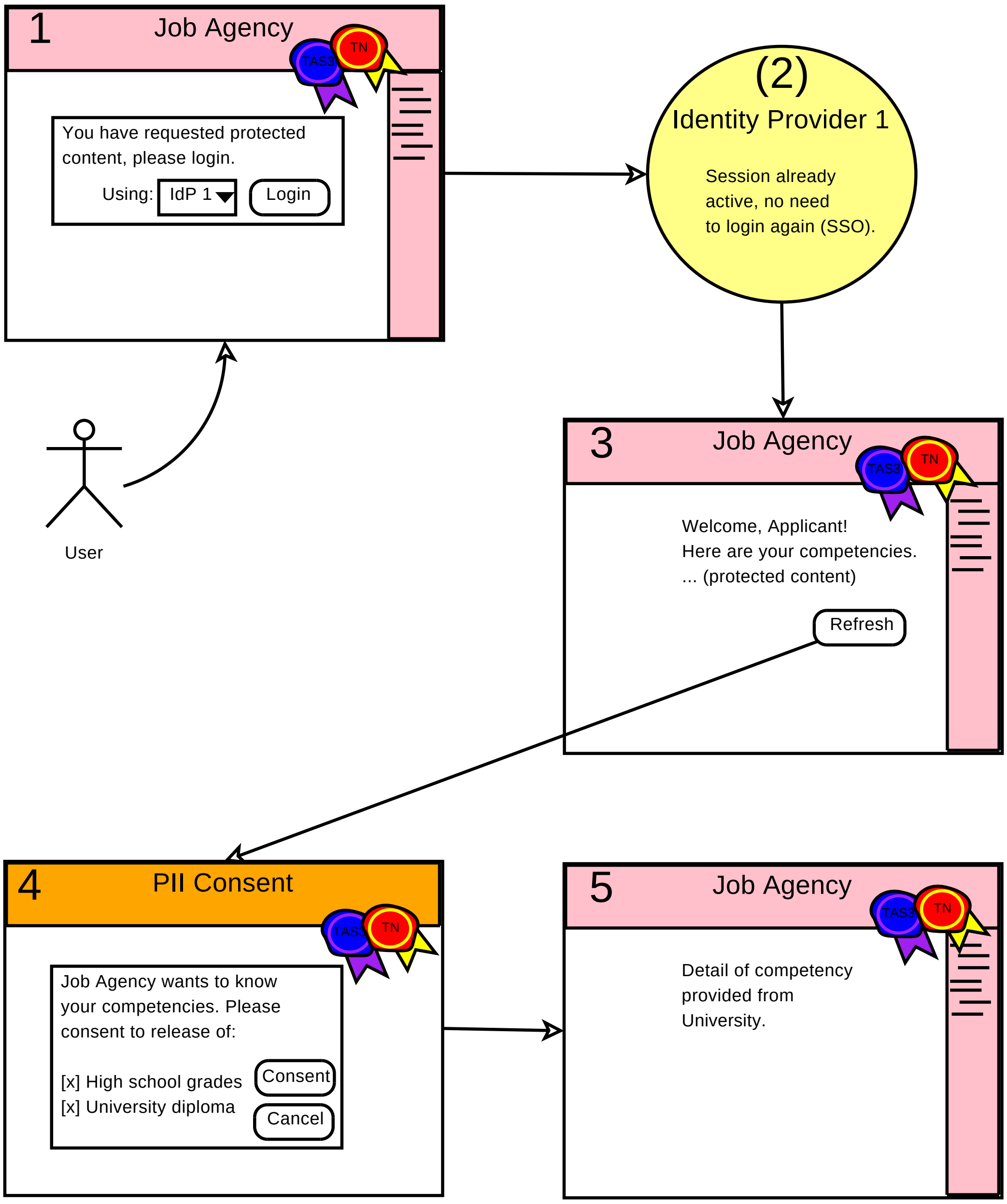
   Feedback Once consent is given, User lands on page that uses the consented information. This may be sufficient in its own right, but could be enhanced by high-lighting the information on the page the user just consented to.

5. **Business process continues with the PII as usual**

2.8.2 Interaction on side channel

This Use Case is similar to the previous one. Only difference is that the consent is asked using a Side Channel, such as mobile phone or instant messaging. The

2.8 Consenting to PII Release or Manipulation



You have requested protected content, please login.

Using: IdP 1 ▼ Login

Session already active, no need to login again (SSO).

Welcome, Applicant!
Here are your competencies.
... (protected content)

Job Agency wants to know your competencies. Please consent to release of:

[x] High school grades
[x] University diploma

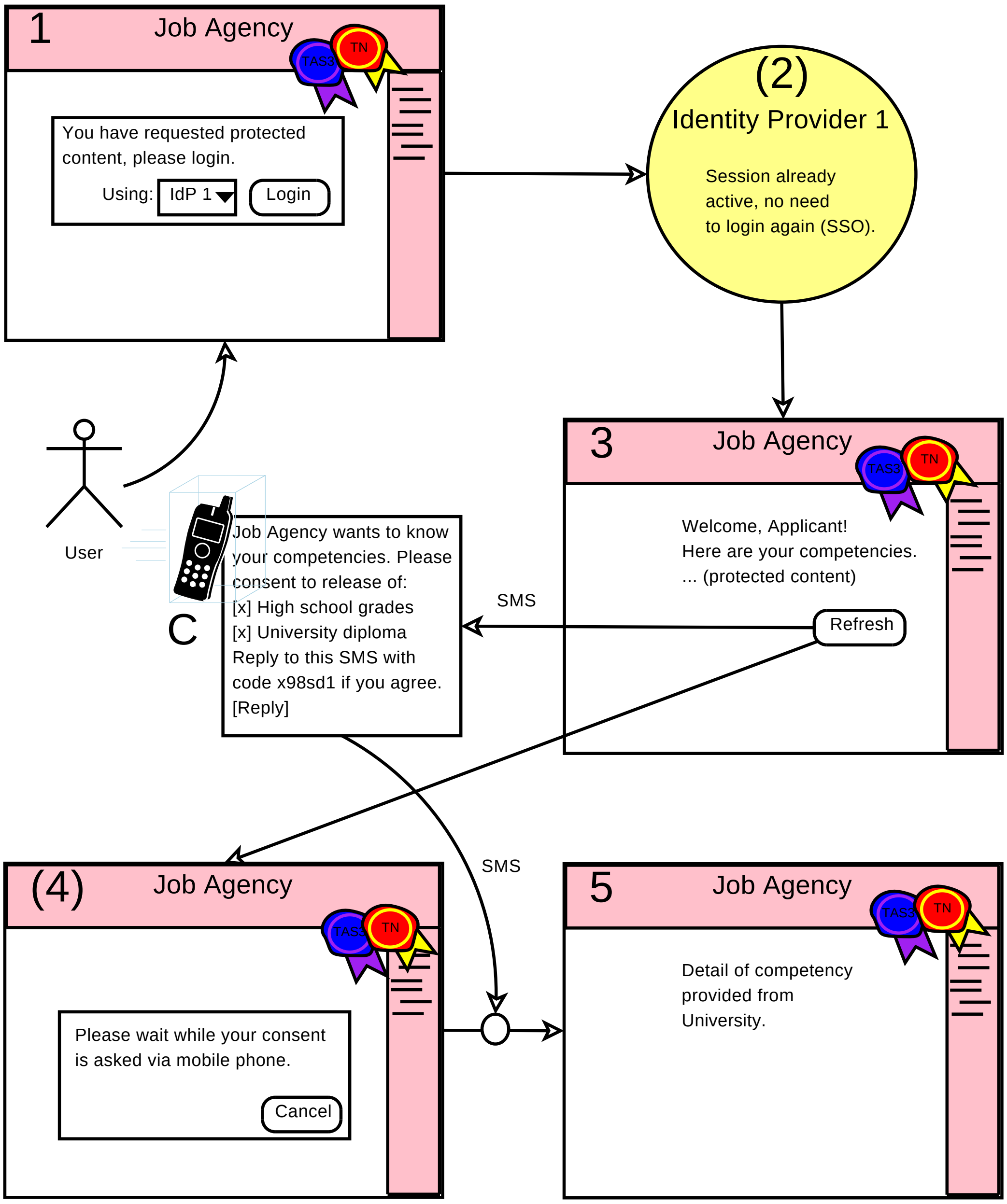
Detail of competency provided from University.

Figure 18: Story board: Presenting a PII consent question in Front Channel interaction.

side channel provides an independent means of communication, a type of second factor to the consent.

The Side Channel approach can also be convenient when consent needs to be asked deep in SOA Web Services calls where Front Channel is not available.

In User-not-present transaction the Side Channel may be the only option for



You have requested protected content, please login.

Session already active, no need to login again (SSO).

Job Agency wants to know your competencies. Please consent to release of:
[x] High school grades
[x] University diploma
Reply to this SMS with code x98sd1 if you agree.
[Reply]

Welcome, Applicant!
Here are your competencies.
... (protected content)

Please wait while your consent is asked via mobile phone.

Detail of competency provided from University.

Figure 19: Story board: Presenting a PII consent question using Side Channel interaction.

asking user's consent, or else the business process needs to be stopped until user provides consent via Dashboard.

2.8.3 Interaction via Dashboard

In User-not-present transaction the business process may stop until user provides input or consent via Dashboard. This alternative will be covered in a future version of this document.

2.8.4 Interaction, such as Consent or Supply of Additional Data, Inserted into FE User Experience

In a deep web services call chain, it is difficult to contact the user for asking consent or soliciting additional data. This can solved with Interaction Service. Ideally such service should appear on the application web page as a user interface element pulled from the user's interaction service (which can be colocated with the Dashboard).

Other viable alternative could be to use an alternate communications channel, such as instant messaging or SMS message, to contact the user. Even in these cases the SP would contact the user's Interaction Service and the service would make the specific choice of communications channel.

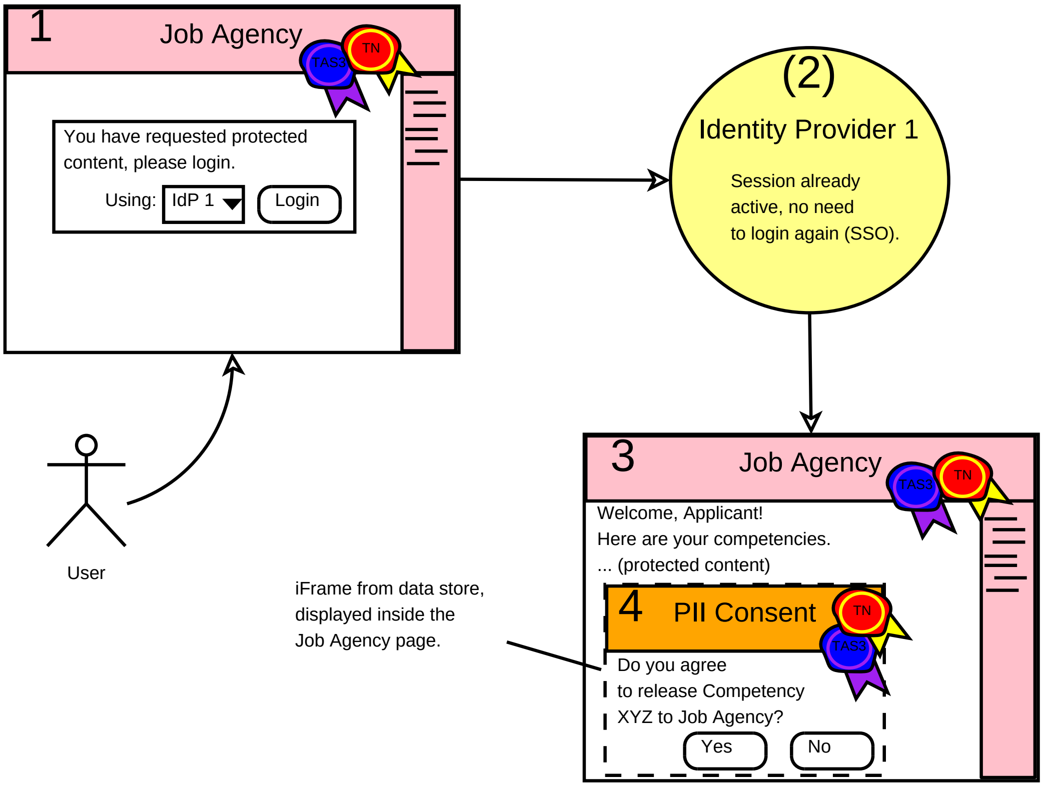

1
Job Agency
TAS3
TN
You have requested protected content, please login.
Using: IdP 1
Login
(2)
Identity Provider 1
Session already active, no need to login again (SSO).
User
iFrame from data store, displayed inside the Job Agency page.
3
Job Agency
TAS3
TN
Welcome, Applicant!
Here are your competencies.
... (protected content)
4
PII Consent
TN
TAS3
Do you agree to release Competency XYZ to Job Agency?
Yes
No

Figure 20: Story board: Presenting a PII consent question using embedded user interface.

2.9 Using Linking Service

1. The Linking Service should be user friendly. It may be the only interface that users see for linking their attributes together (other approaches are possible, see "pull model").

2. A welcome screen explains the purpose of the Linking Service and guides the user through the process of attribute linking. It has

   a. Picking list for choosing IdP

   b. "Connect" button

   c. "View linked accounts" button

   d. "Make linked accounts available to services" button

   e. Notice or pledge about respecting User's privacy

3. When the user selects the "Connect" button, the linking service will redirect the user to the selected IdP, allowing the user to login. After login, the user will be redirected back to the linking service welcome screen.

4. When the user selects "View my linked accounts" he will be presented with the screen with

   a. A table containing two columns, labelled "Organisation" and "Temporary Account Identifier" and at the left hand side by each table entry will be a tick box that the user can tick to remove the linked account. Above the column of tick boxes will be the word Delete.

   b. "Delete" button, which will remove the chosen accounts from the table and return the user to this page

   c. "Home Page" button, which will take the user to Welcome screen

   d. "Make my linked accounts available to services" button, which will take the user to the next screen.

   e. Notice or pledge about respecting User's privacy

5. When the user selects the "Make my linked accounts available to services" button he will be presented with a screen containing

   a. An explanation about opt-in in the linking (if you do not make accounts available, the default will be no linking).

b. A table with 3 columns and a delete tick box beside each row of the table. The table columns are "Service", "Organisation" and "Temporary Account Identifier". The table will always be empty for new users when they first approach this screen.

c. A picking list of all the services in the federation, obtained from the metadata of the federation. The first entry in the list will be "All Other Services".

d. Once the user selects a service provider or "All Other Services" from the picking list, a picking list of all the IdPs that are currently linked together and that appear in the table of the My Linked Accounts Screen, minus the IdPs that have already been paired with the selected service provider is displayed.

   The first row of this picking list will be "All My Linked Accounts". The user will then pick one of his linked accounts or "All My Linked Accounts". If the user picks "All My Linked Accounts" a wild card will be inserted into the third column. If the user picks one of his accounts then the third column will be automatically completed with the account Persistent ID unless the user has two or more accounts at the same IdP, in which case the third column will contain a picking list of Persistent IDs sent from that IdP, minus any already selected for this service provider.

   It is important that the table always lists the service providers in alphabetical order so that the user can easily see which links he has set up for which SPs, and for every SP, the linked IdPs are in alphabetical order.

e. "Delete" button, which will remove the chosen accounts from the table and return the user to this page

f. "Home Page" button, which will take the user to Welcome screen

g. "View my linked accounts" button, which will take the user to the screen referred to in step (4), above.

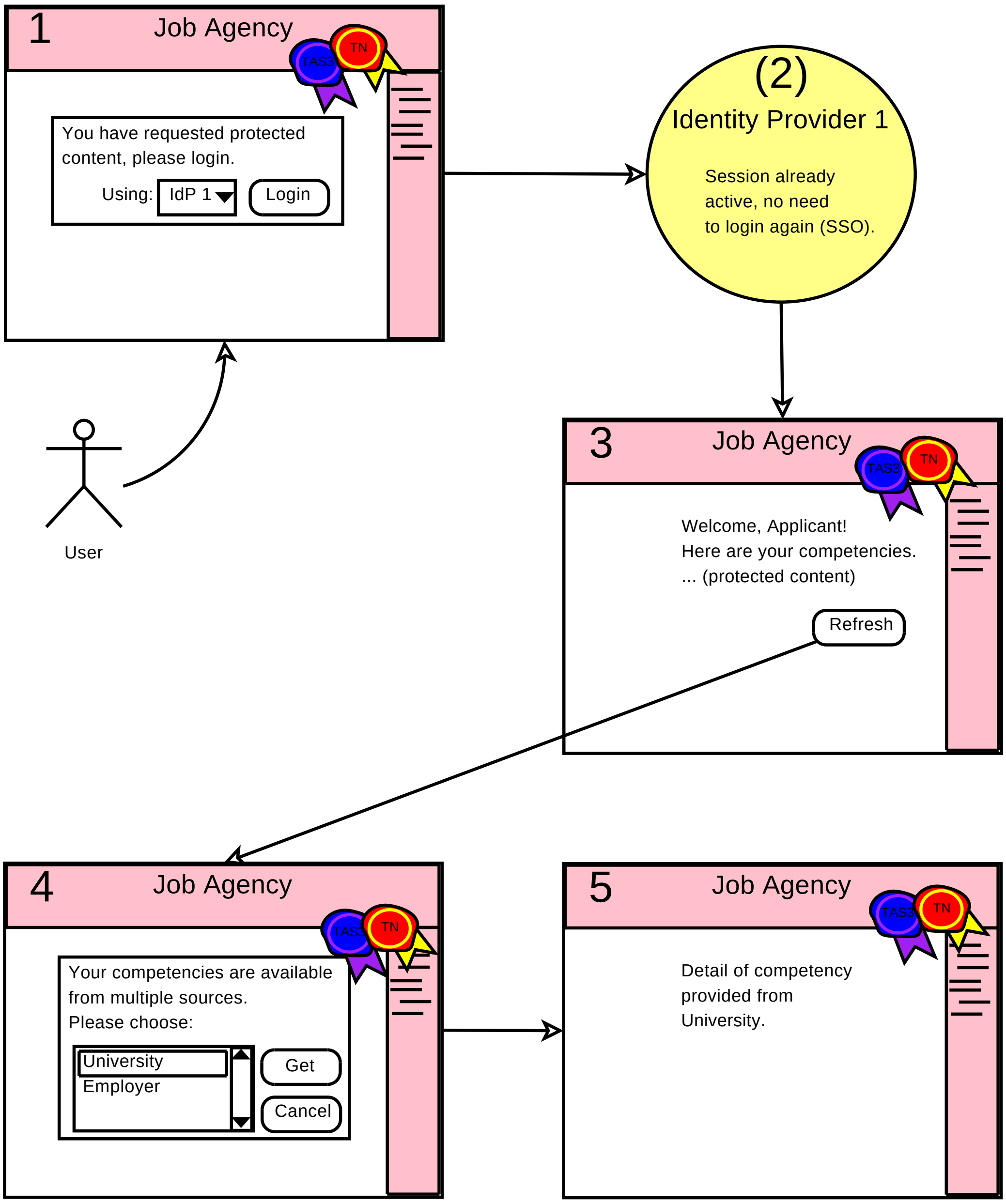
2.10 Choosing amongst Multiple Service Providers

Sometimes user will have choice of multiple possible providers for a given service. In this situation Trust and Privacy Negotiation function can be used to narrow down the list. If after narrowing down more than one choice still remains, it may be reasonable to ask the user to make the choice.

2.10.1 Simple Choice of Provider

Cognitive Walkthrough

1. **IdP choice as usual**



You have requested protected content, please login.

Session already active, no need to login again (SSO).

Welcome, Applicant!
Here are your competencies.
... (protected content)

Your competencies are available from multiple sources.
Please choose:

Detail of competency provided from University.

Figure 21: Story board: Choice of Service Provider.

2. **Authentication as usual**

3. **User triggers action, as usual**

4. **Choose Service Provider**

Motivation The decision point will be imposed to the user through modal user interaction. User will be motivated to make the choice as he may guard different information, e.g. different personae, at different Attribute Authorities.

Available and understandable User's choice should only be solicited if there is genuine choice. System should implement automatic discovery and detection as much as possible.

The choices should be formulated in human language, with translations as appropriate.

Feedback Once User makes his choice, he will land on the requestor's page. This in itself may be sufficient feedback, but indicating on the page where the information came from is recommended.

2.10.2 Credentials and Privacy Negotiation Assisted by User Interaction

Cognitive Walkthrough

1. **IdP choice as usual**

2. **Authentication as usual**

3. **User triggers action, as usual**

4. **Negotiate appropriate supplier for service or information**

Motivation User will be forced to the decision point by modal user interface flow. User will be motivated to make a choice either because he has no prior relationship with proposed SPs and he needs to rely on trust preceptions, or because user wants to be in control and avoid machine deciding for him.

Available and understandable Presenting complex trust based decision is not easy. This topic will be further researched during TAS^3 project.

Feedback Once User makes his choice, he will land on the requestor's page. This in itself may be sufficient feedback, but indicating on the page where the information came from is recommended.

Further Use Cases depicting complex Trust and Privacy Negotiations will be elaborated in other project deliverables.

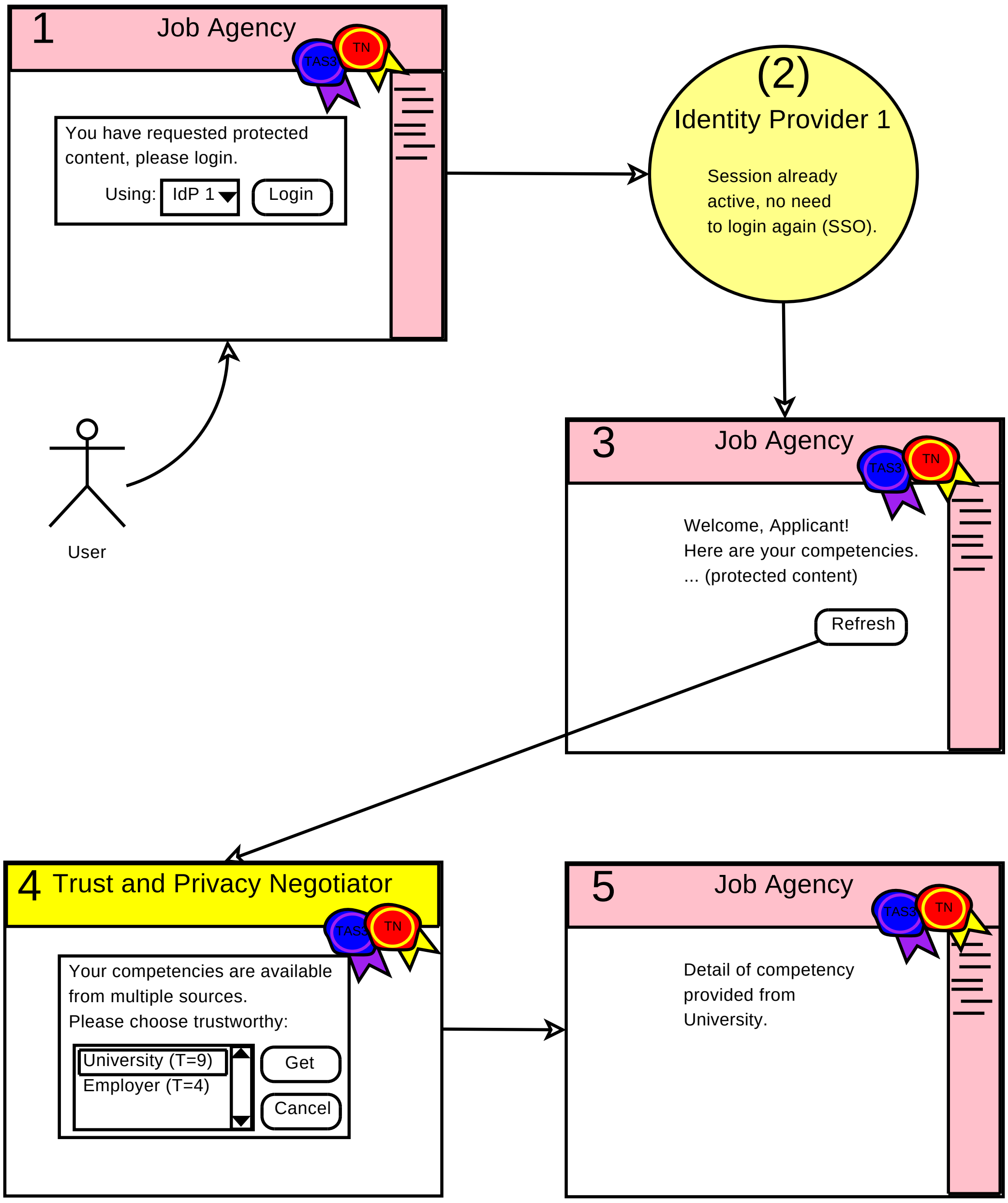

1
Job Agency
TAS3
TN
You have requested protected content, please login.
Using: IdP 1
Login
(2)
Identity Provider 1
Session already active, no need to login again (SSO).
User
3
Job Agency
TAS3
TN
Welcome, Applicant!
Here are your competencies.
... (protected content)
Refresh
4 Trust and Privacy Negotiator
TAS3
TN
Your competencies are available from multiple sources.
Please choose trustworthy:
University (T=9)
Employer (T=4)
Get
Cancel
5
Job Agency
TAS3
TN
Detail of competency provided from University.

Figure 22: Story board: Credentials and Privacy Negotiation with User Interaction.

2.11 User-Not-Present Transaction

User-not-present scenario can be driven in three ways:

1. User has been present in some earlier time and has authorized, indirectly, the transaction. Audit trail MUST show this authorization.

2. There is an over-arching legal or legitimate business requirement. Existence of such requirement MUST be demonstratable from the audit trail.

3. "Break the glass" scenarios. Again audit trail MUST capture legitimate reason why the scenario was invoked and the audit trail should be especially detailed about the actions performed under the break the glass authority.

Actual triggering of the event will depend on a business process. To gain acute authorization to execute the operation, the business process will have to declare its intent and show evidence why it should be authorized (see (1) and (2), above). Then, the operation MUST be thoroughly recorded in the audit trail.

User's only contact point with User-Not-Present transaction is to audit it after the fact using the Dashboard.

2.12 User Present Delegation

See Fig-23.

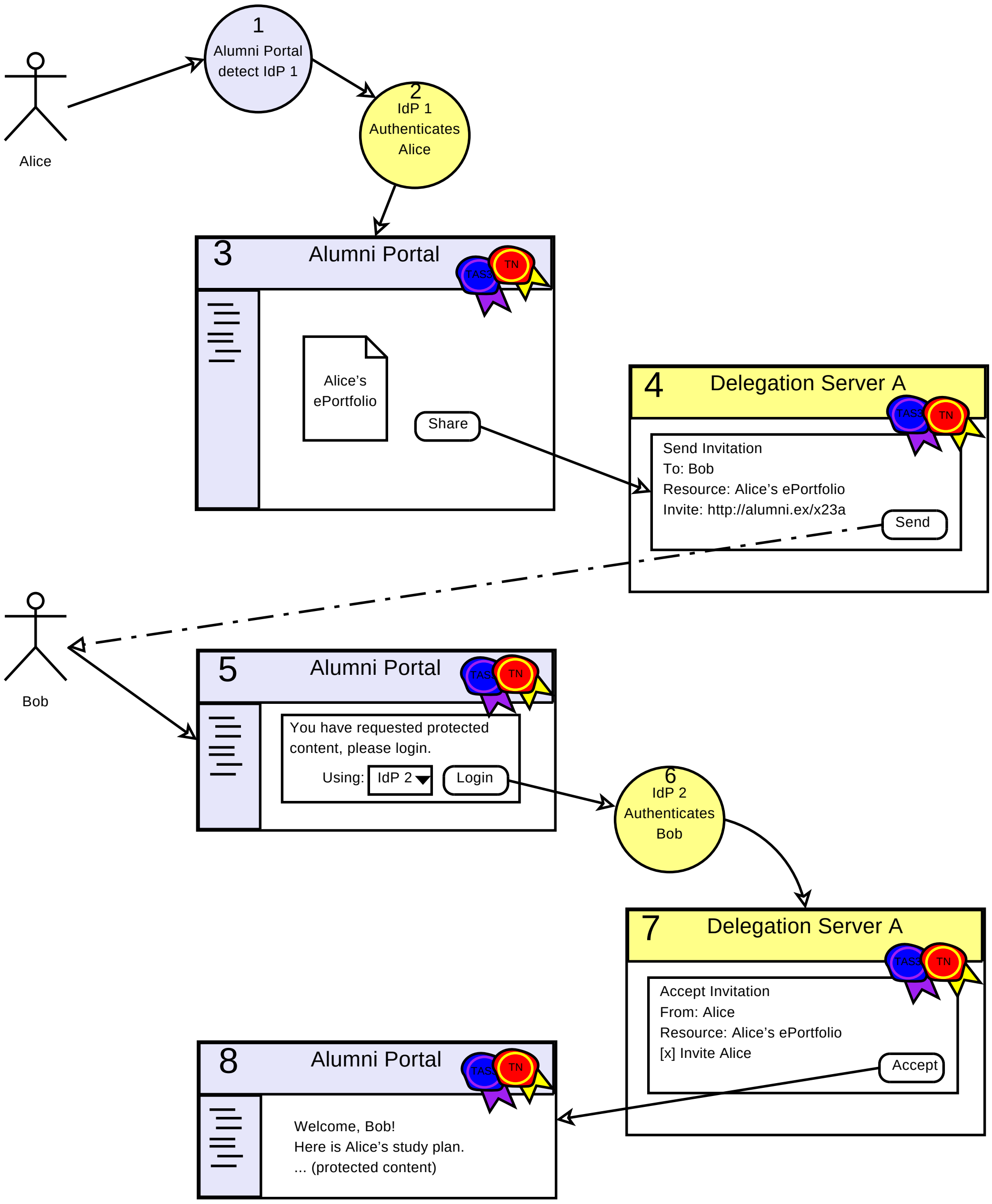
- Problem of choosing to whom to delegate, buddy list visualization
    - How to obtain human readable names without violating privacy of the buddies?

Delegation of permissions to access repositories is addressed more fully in [TAS3D42Repo].

2.13 User-Not-Present Delegation

This will cover situations such as administrative or judicial decisions that result in delegation without the User necessarily wanting the delegation to happen.

We will explore these use cases in more detail in a future deliverable (M30 D2.1).



Send Invitation
To: Bob
Resource: Alice's ePortfolio
Invite: http://alumni.ex/x23a

You have requested protected content, please login.
Using: IdP 2

Accept Invitation
From: Alice
Resource: Alice's ePortfolio
[x] Invite Alice

Welcome, Bob!
Here is Alice's study plan.
... (protected content)

Figure 23: Story board: Alice invites Bob to view her ePortfolio.

2.14 Right of Access, Rectification, and Deletion in FE GUI

Right of Access, Rectification, and Deletion are guaranteed by European regualtion. To support these goals, TAS^3 Dashboard can provide a unified interface to send such requests to various data authorities and stores.

However, in the interest of immediacy and contextual interaction, it is desireable that when user, in the flow of using a web application, detects an errornous data item, he should be able to immediately correct it.

To satisfy this requirement we envision the data authority to provide a user self-management page. The URL of this page is sent whenever the data is released, and the data consuming web site must display the URL so that the user can click it to accomplish correction or deletion.

A more sophisticated variant of this approach is that the data consuming web site inserts a user interface device originating from the data authority. Technically this could be implemented as an iFrame or portlet.

2.15 Policy Editing Inserted into FE User Experience

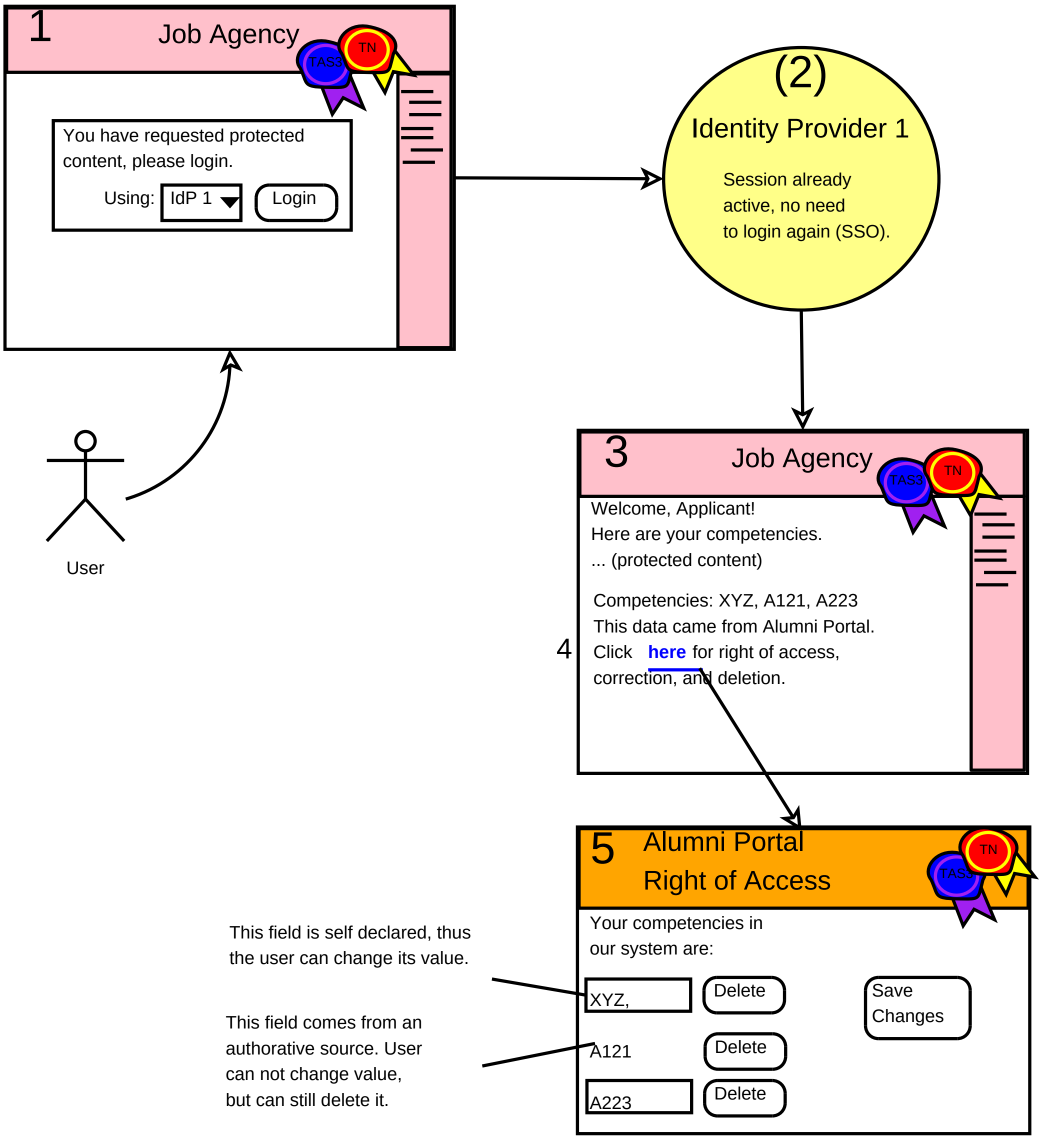
TAS^3 Dashboard can provide a unified central interface for policy editing. This could be implemented by each data holder providing a link to its policy editing interface. The links are centrally available on the dashboard, but the editing itself happens at the data holder.

A more sophisticated variant of this approach is that the dashboard pulls in a user interface device originating from the data authority. Technically this could be implemented as an iFrame or portlet.

However, in the interest of immediacy and contextual interaction, it is desireable that when user, in the flow of using a web application, can directly edit the relevant policies. This can be realized by same means as the dashboard integration: either provide a link to policy editing interface of the data authority, or provide a user interface element pulled from the data authority.

2.16 Credentials and Privacy Negotiation Inserted into FE User Experience

The credentials and privacy negotiation is conceptually between the WSC and the WSP, neither of which necessarily has a user interface. If the already configured policies are enough to conclude the negotiation, this is not a problem. However, it is likely that additional policies would be needed. In this case the CPN Agent acting for the user, should be able to solicit user input. A way to arrange for this is to have a user interface element, such as iFrame, appear directly on the WSP selection page of the application.



You have requested protected content, please login.

Session already active, no need to login again (SSO).

Welcome, Applicant!
Here are your competencies.
... (protected content)

Competencies: XYZ, A121, A223
This data came from Alumni Portal.
Click here for right of access, correction, and deletion.

Your competencies in our system are:

This field is self declared, thus the user can change its value.

This field comes from an authorative source. User can not change value, but can still delete it.

Figure 24: Right of Access using link embedded on page.

2.17 Unified TAS^3 User Interaction Widget

Many of the user interaction aspects could be unified in a TAS^3 interaction widget that is inserted into SP pages (e.g. as iFrame). The widget would then poll or refresh itself periodically from the dashboard server and if there are events of note to report, show a one line notice to the user, with a link for user to click for further interaction.

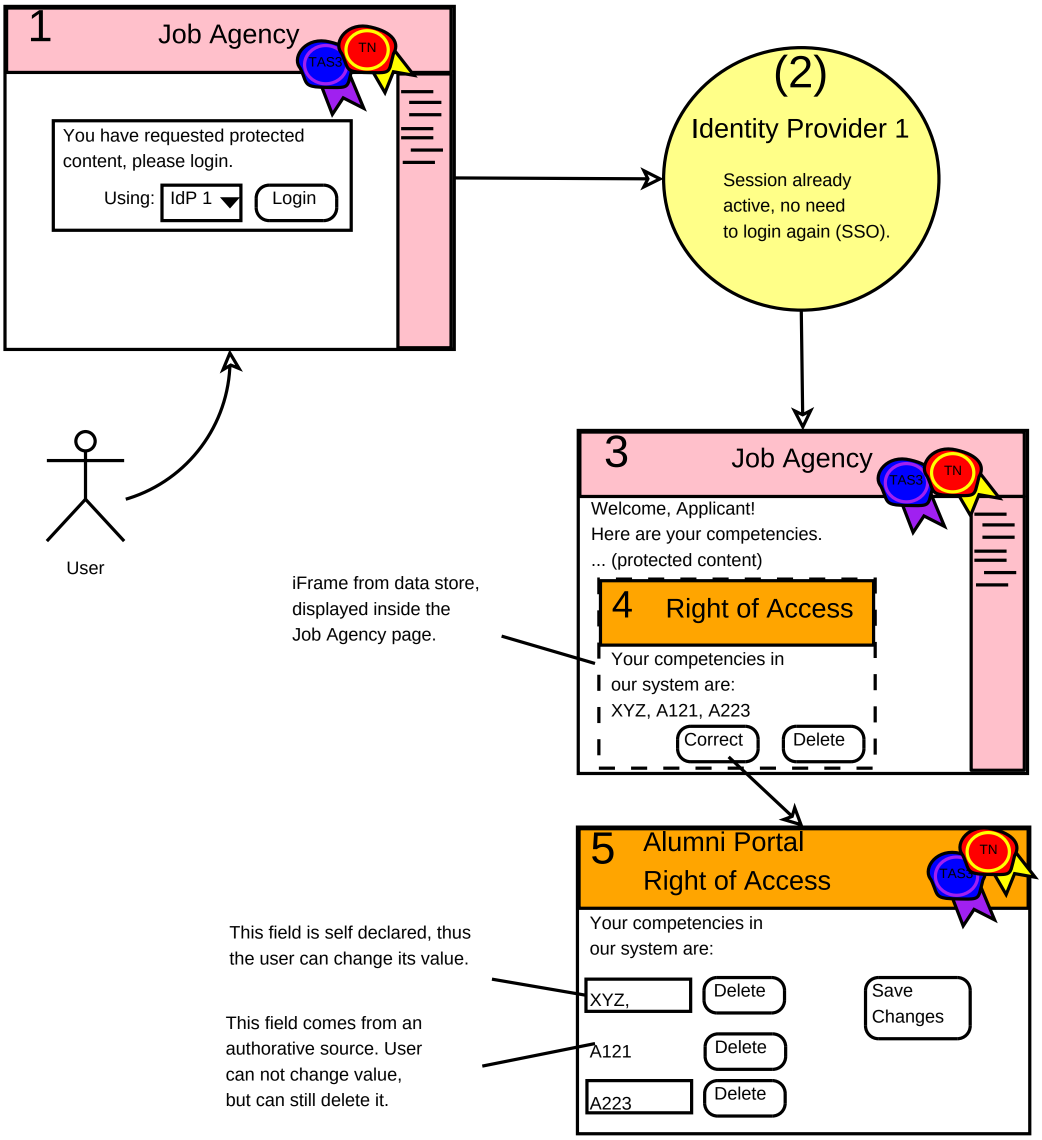

1
Job Agency
TAS3
TN
You have requested protected content, please login.
Using: IdP 1
Login
(2)
Identity Provider 1
Session already active, no need to login again (SSO).
User
3
Job Agency
Welcome, Applicant!
Here are your competencies.
... (protected content)
iFrame from data store, displayed inside the Job Agency page.
4 Right of Access
Your competencies in our system are:
XYZ, A121, A223
Correct
Delete
5 Alumni Portal
Right of Access
Your competencies in our system are:
This field is self declared, thus the user can change its value.
This field comes from an authorative source. User can not change value, but can still delete it.
XYZ,
A121
A223
Delete
Delete
Delete
Save Changes

Figure 25: Story board: Right of access using embedded user interface.

2.18 New SP Intake

The Business Process Model for SP intake can be accessed at `https://portal.tas3.eu/trac/wiki/UseCase/SelfAuditAndSPIntake`

2.18.1 `idp.tas3.eu` (Jeroen's design)

This partner intake process concentrates exclusively on technical aspects such as metadata and service registration. It does not provide any administrative or busi-

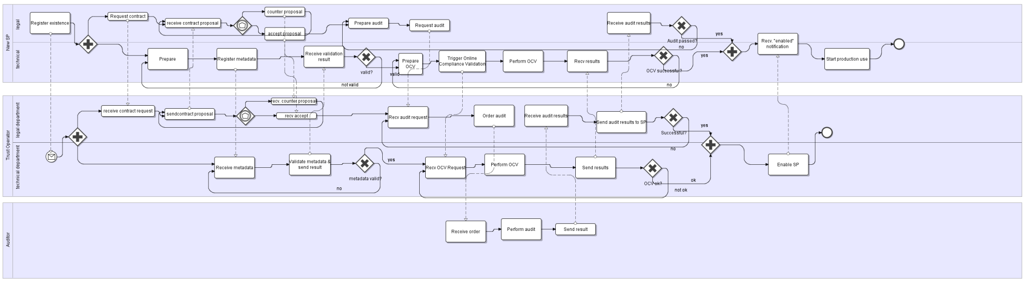
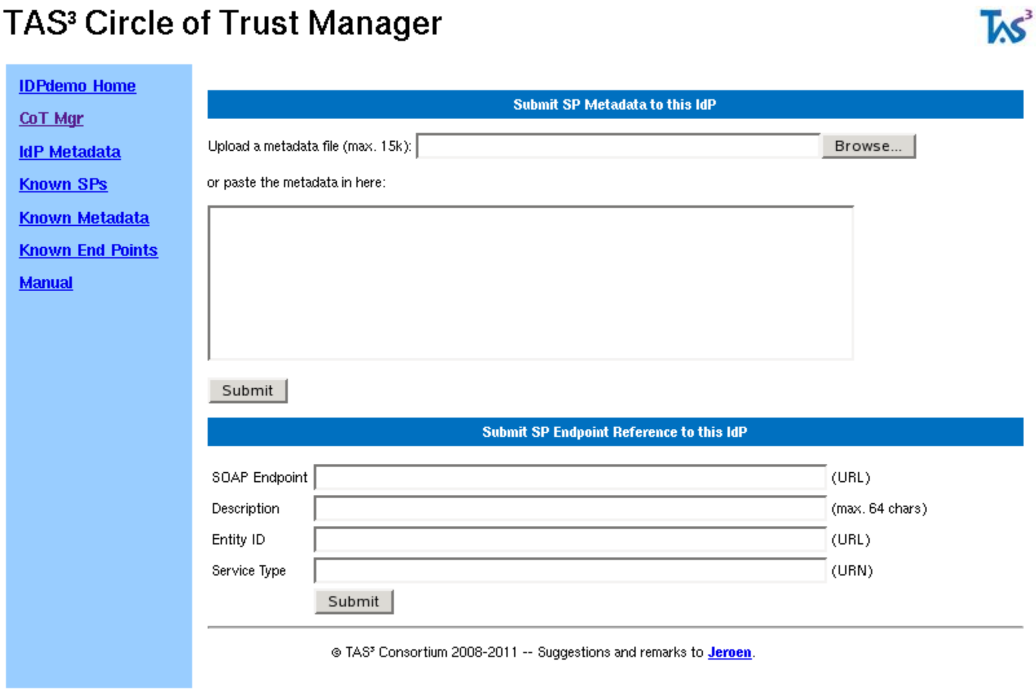


Figure 26: Business Process Model for SP intake (too small, we know, access the version on the web!)

ness data gathering.

These screens can be accessed live over the internet at `https://idp.tas3.eu/cot/`



TAS³ Circle of Trust Manager

[IDPdemo Home](#)
[CoT Mgr](#)
[IdP Metadata](#)
[Known SPs](#)
[Known Metadata](#)
[Known End Points](#)
[Manual](#)

Submit SP Metadata to this IdP

Upload a metadata file (max. 15k): [ ] Browse...

or paste the metadata in here:

Submit

Submit SP Endpoint Reference to this IdP

SOAP Endpoint		(URL)
Description		(max. 64 chars)
Entity ID		(URL)
Service Type		(URN)

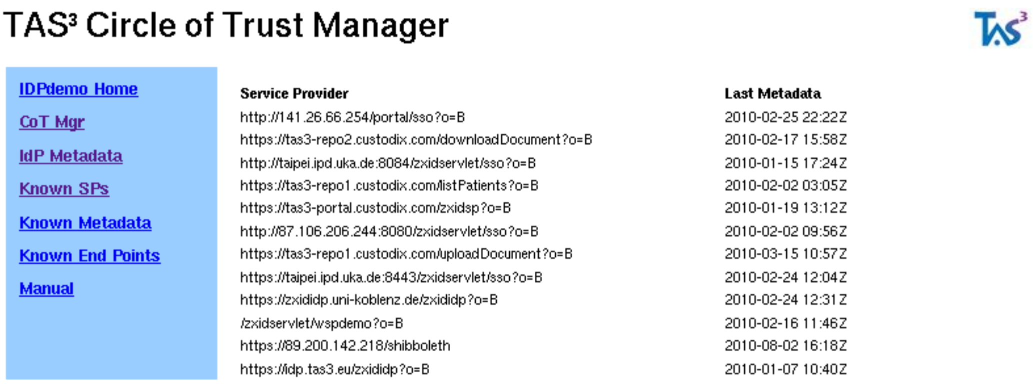
Submit

© TAS³ Consortium 2008-2011 -- Suggestions and remarks to [Jeroen](#).

Figure 27: Main registration ot TAS3 IdP's Circle of Trust (CoT) registration page, illustrating metadata entry and registration of web service end point.

2.18.2 `zxidp.org`

This illustrates the partner intake process of `zxidp.org` free IdP.

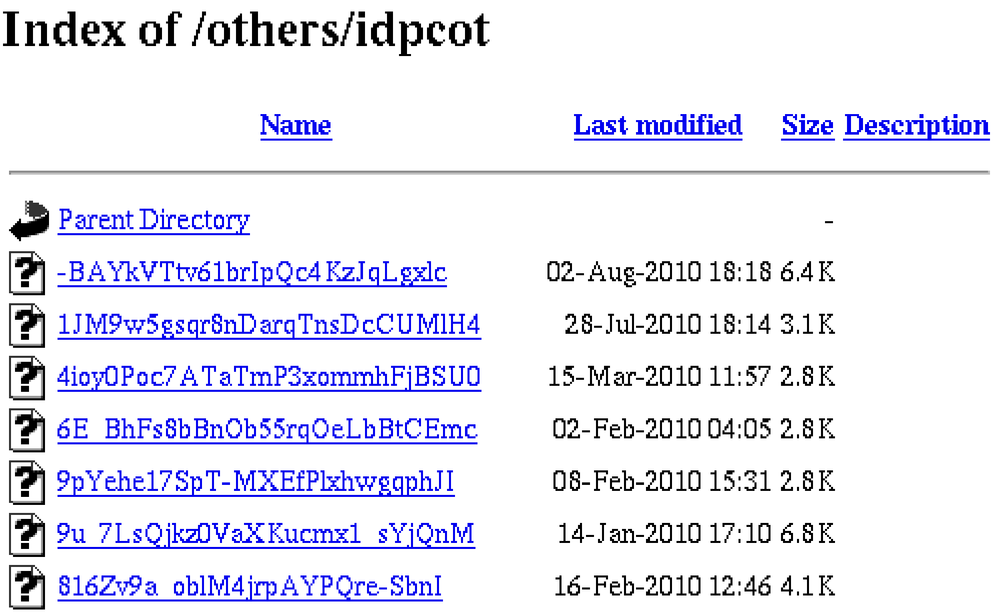


TAS³ Circle of Trust Manager

- IDPdemo Home
- CoT Mgr
- IdP Metadata
- Known SPs
- Known Metadata
- Known End Points
- Manual

Service Provider	Last Metadata
http://141.26.66.254/portal/sso?o=B	2010-02-25 22:22Z
https://tas3-repo2.custodix.com/downloadDocument?o=B	2010-02-17 15:58Z
http://taipei.ipd.uka.de:8084/zxidservlet/sso?o=B	2010-01-15 17:24Z
https://tas3-repo1.custodix.com/listPatients?o=B	2010-02-02 03:05Z
https://tas3-portal.custodix.com/zxidsp?o=B	2010-01-19 13:12Z
http://87.106.206.244:8080/zxidservlet/sso?o=B	2010-02-02 09:56Z
https://tas3-repo1.custodix.com/uploadDocument?o=B	2010-03-15 10:57Z
https://taipei.ipd.uka.de:8443/zxidservlet/sso?o=B	2010-02-24 12:04Z
https://zxididp.uni-koblenz.de/zxididp?o=B	2010-02-24 12:31Z
/zxidservlet/wspdemo?o=B	2010-02-16 11:46Z
https://89.200.142.218/shibboleth	2010-08-02 16:18Z
https://idp.tas3.eu/zxididp?o=B	2010-01-07 10:40Z

Figure 28: SP listing screen that allows determination of whether an SP has been registered.



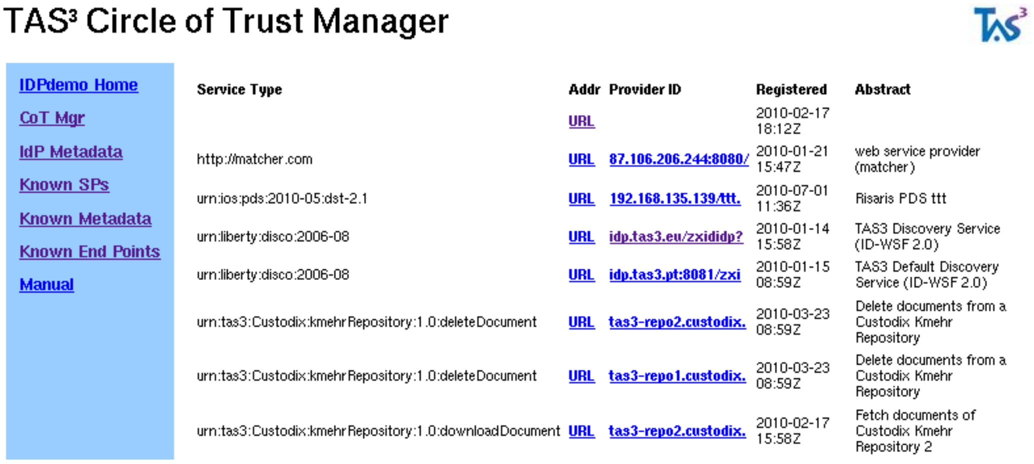
Index of /others/idpcot

Name	Last modified	Size	Description
Parent Directory		-	
-BAYkVTtv61brIpQc4KzJqLgxlc	02-Aug-2010 18:18	6.4K	
1JM9w5gsqr8nDarqTnsDcCUMlH4	28-Jul-2010 18:14	3.1K	
4ioy0Poc7ATaTmP3xommhFjBSU0	15-Mar-2010 11:57	2.8K	
6E_BhFs8bBnOb55rqOeLbBtCEmc	02-Feb-2010 04:05	2.8K	
9pYehe17SpT-MXEfPlxhwgqphJI	08-Feb-2010 15:31	2.8K	
9u_7LsQjkz0VaXKucmx1_sYjQnM	14-Jan-2010 17:10	6.8K	
816Zv9a_oblM4jrpAYPQre-SbnI	16-Feb-2010 12:46	4.1K	

Figure 29: An alternate way of listing SPs, this time with emphasis on accessing the metadata stored at IdP and visualization of the internal "succinct id".

These screens can be accessed live over the internet at `http://zxidp.org/index-idp.html`

2.18 New SP Intake

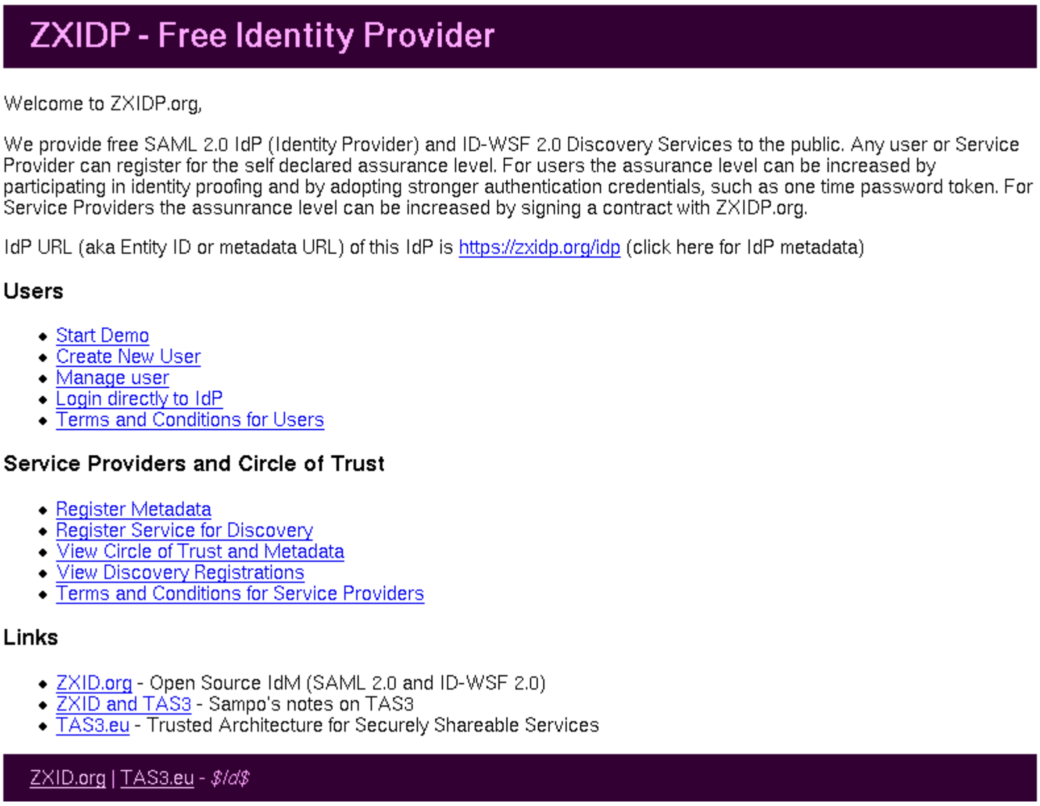


TAS³ Circle of Trust Manager

- IDPdemo Home
- CoT Mgr
- IdP Metadata
- Known SPs
- Known Metadata
- Known End Points
- Manual

Service Type	Addr	Provider ID	Registered	Abstract
	URL		2010-02-17 18:12Z	
http://matcher.com	URL	87.106.206.244:8080/	2010-01-21 15:47Z	web service provider (matcher)
urn:ios:pds:2010-05:dst-2.1	URL	192.168.135.139/ttt.	2010-07-01 11:36Z	Risaris PDS ttt
urn:liberty:disco:2006-08	URL	idp.tas3.eu/zxididp?	2010-01-14 15:58Z	TAS3 Discovery Service (ID-WSF 2.0)
urn:liberty:disco:2006-08	URL	idp.tas3.pt:8081/zxi	2010-01-15 08:59Z	TAS3 Default Discovery Service (ID-WSF 2.0)
urn:tas3:Custodix:kmehrRepository:1.0:deleteDocument	URL	tas3-repo2.custodix.	2010-03-23 08:59Z	Delete documents from a Custodix Kmehr Repository
urn:tas3:Custodix:kmehrRepository:1.0:deleteDocument	URL	tas3-repo1.custodix.	2010-03-23 08:59Z	Delete documents from a Custodix Kmehr Repository
urn:tas3:Custodix:kmehrRepository:1.0:downloadDocument	URL	tas3-repo2.custodix.	2010-02-17 15:58Z	Fetch documents of Custodix Kmehr Repository 2

Figure 30: Endpoint Listing, allowing determination of whether endpoint has been registered and what the details are. Hovering over the "URL" link shows the actual endpoint URL (not illustrated in figure). This is to save horizontal real estate on the screen.



ZXIDP - Free Identity Provider

Welcome to ZXIDP.org,

We provide free SAML 2.0 IdP (Identity Provider) and ID-WSF 2.0 Discovery Services to the public. Any user or Service Provider can register for the self declared assurance level. For users the assurance level can be increased by participating in identity proofing and by adopting stronger authentication credentials, such as one time password token. For Service Providers the assunrance level can be increased by signing a contract with ZXIDP.org.

IdP URL (aka Entity ID or metadata URL) of this IdP is https://zxidp.org/idp (click here for IdP metadata)

Users

- Start Demo
- Create New User
- Manage user
- Login directly to IdP
- Terms and Conditions for Users

Service Providers and Circle of Trust

- Register Metadata
- Register Service for Discovery
- View Circle of Trust and Metadata
- View Discovery Registrations
- Terms and Conditions for Service Providers

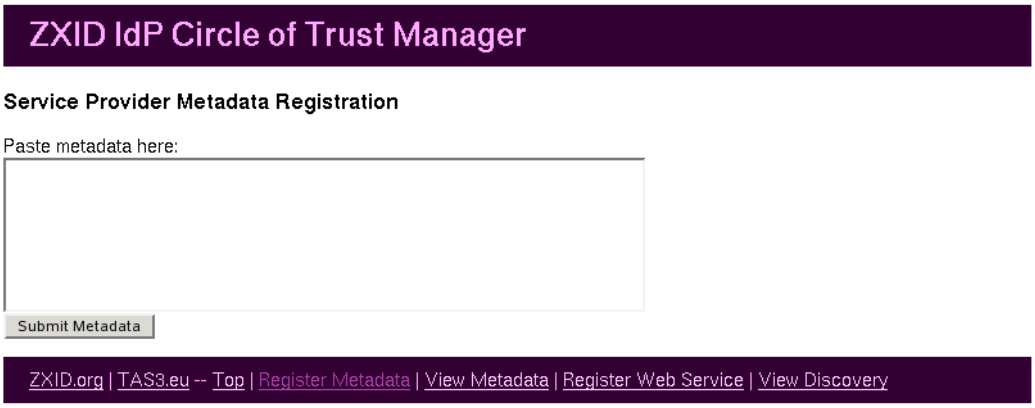
Links

- ZXID.org - Open Source IdM (SAML 2.0 and ID-WSF 2.0)
- ZXID and TAS3 - Sampo's notes on TAS3
- TAS3.eu - Trusted Architecture for Securely Shareable Services

ZXID.org | TAS3.eu - *Id*

Figure 31: Top level menu of `zxidp.org`, providing access to both User and `SP/CoT` management functions

2.18 New SP Intake



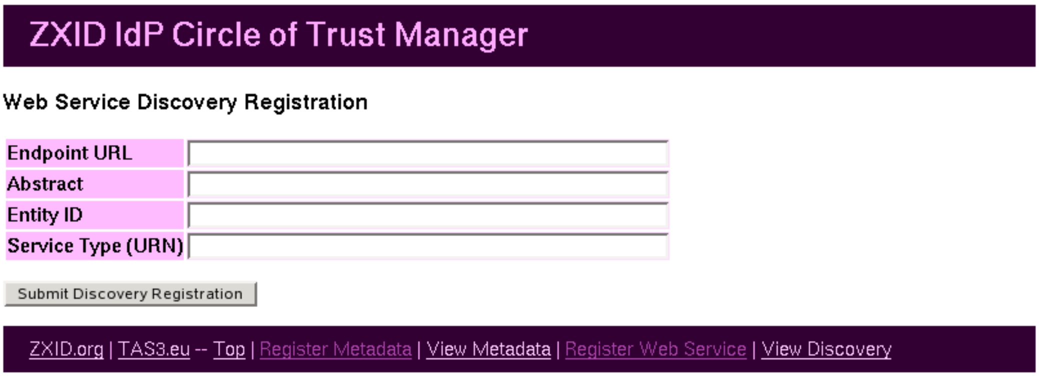
ZXID IdP Circle of Trust Manager

Service Provider Metadata Registration

Paste metadata here:

Submit Metadata
ZXID.org | TAS3.eu -- Top | Register Metadata | View Metadata | Register Web Service | View Discovery

Figure 32: Metadata upload screen



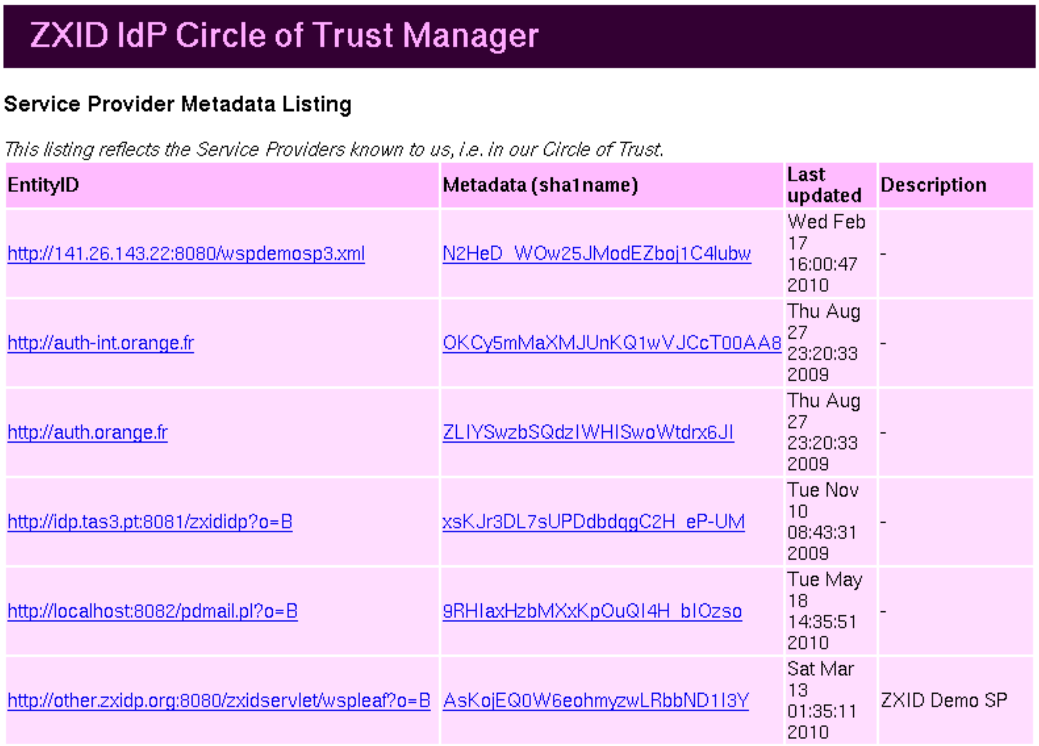
ZXID IdP Circle of Trust Manager

Web Service Discovery Registration

Endpoint URL	
Abstract	
Entity ID	
Service Type (URN)	

Submit Discovery Registration
ZXID.org | TAS3.eu -- Top | Register Metadata | View Metadata | Register Web Service | View Discovery

Figure 33: Service endpoint registration screen



ZXID IdP Circle of Trust Manager

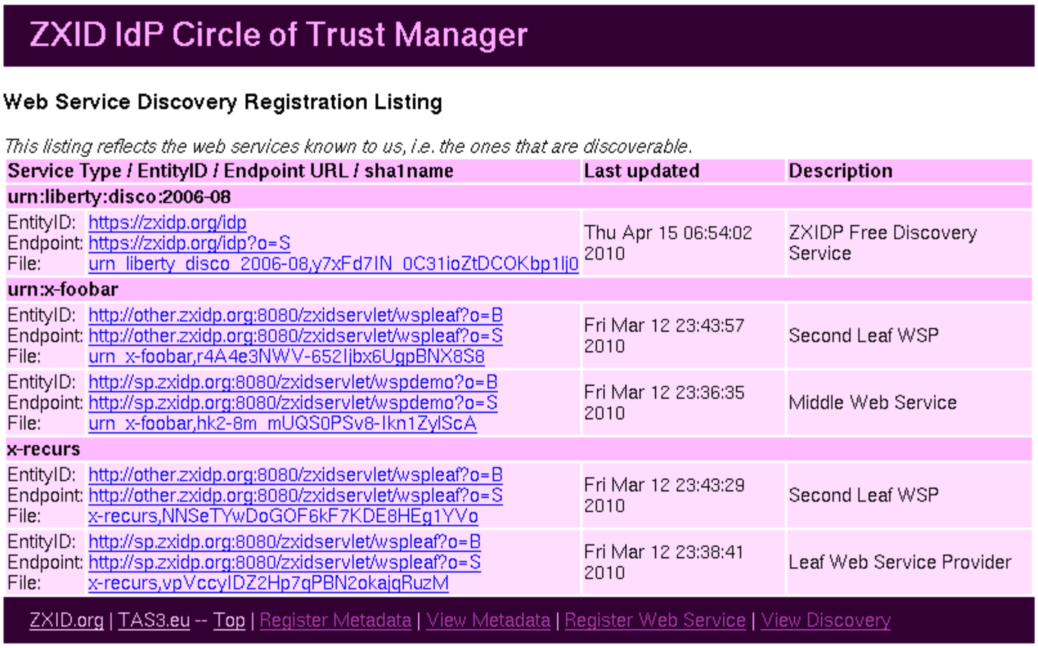
Service Provider Metadata Listing

This listing reflects the Service Providers known to us, i.e. in our Circle of Trust.

EntityID	Metadata (sha1name)	Last updated	Description
http://141.26.143.22:8080/wspdemosp3.xml	N2HeD_WOw25JModEZboj1C4lubw	Wed Feb 17 16:00:47 2010	-
http://auth-int.orange.fr	OKCy5mMaXMJUnKQ1wVJCcT00AA8	Thu Aug 27 23:20:33 2009	-
http://auth.orange.fr	ZLIYSwzbSQdzIWHISwoWtdrx6JI	Thu Aug 27 23:20:33 2009	-
http://idp.tas3.pt:8081/zxididp?o=B	xsKJr3DL7sUPDdbdqgC2H_eP-UM	Tue Nov 10 08:43:31 2009	-
http://localhost:8082/pdmail.pl?o=B	9RHIaxHzbMXxKpOuQI4H_bIOzso	Tue May 18 14:35:51 2010	-
http://other.zxidp.org:8080/zxidservlet/wspleaf?o=B	AsKojEQ0W6eohmyzwLRbbND1I3Y	Sat Mar 13 01:35:11 2010	ZXID Demo SP

Figure 34: Listing of registered SPs. Link to locally stored metadata is provided. Note how many SPs regrettably lack Description field.

2.18 New SP Intake



ZXID IdP Circle of Trust Manager

Web Service Discovery Registration Listing

This listing reflects the web services known to us, i.e. the ones that are discoverable.

Service Type / EntityID / Endpoint URL / sha1name	Last updated	Description
urn:liberty:disco:2006-08		
EntityID: https://zxidp.org/idp Endpoint: https://zxidp.org/idp?o=S File: urn liberty disco 2006-08,y7xFd7IN 0C31ioZtDCOKbp1lj0	Thu Apr 15 06:54:02 2010	ZXIDP Free Discovery Service
urn:x-foobar		
EntityID: http://other.zxidp.org:8080/zxidservlet/wspleaf?o=B Endpoint: http://other.zxidp.org:8080/zxidservlet/wspleaf?o=S File: urn x-foobar,r4A4e3NWV-652Ijbx6UgpBNX8S8	Fri Mar 12 23:43:57 2010	Second Leaf WSP
EntityID: http://sp.zxidp.org:8080/zxidservlet/wspdemo?o=B Endpoint: http://sp.zxidp.org:8080/zxidservlet/wspdemo?o=S File: urn x-foobar,hk2-8m mUQS0PSv8-Ikn1ZylScA	Fri Mar 12 23:36:35 2010	Middle Web Service
x-recurs		
EntityID: http://other.zxidp.org:8080/zxidservlet/wspleaf?o=B Endpoint: http://other.zxidp.org:8080/zxidservlet/wspleaf?o=S File: x-recurs,NNSeTYwDoGOF6kF7KDE8HEg1YVo	Fri Mar 12 23:43:29 2010	Second Leaf WSP
EntityID: http://sp.zxidp.org:8080/zxidservlet/wspleaf?o=B Endpoint: http://sp.zxidp.org:8080/zxidservlet/wspleaf?o=S File: x-recurs,vpVccyIDZ2Hp7qPBN2okajqRuzM	Fri Mar 12 23:38:41 2010	Leaf Web Service Provider

ZXID.org | TAS3.eu -- Top | Register Metadata | View Metadata | Register Web Service | View Discovery

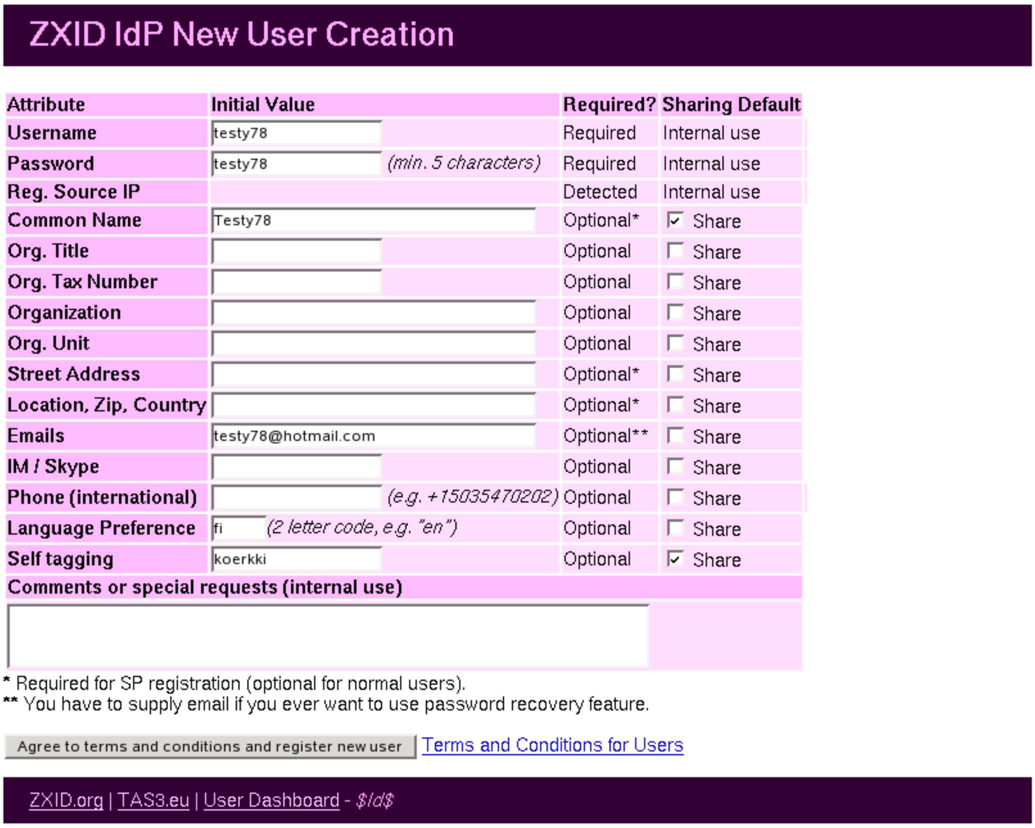
Figure 35: Listing of registered end points, sorted by the type of service they provide.

2.19 New User Intake

2.19.1 `zxidp.org`

This illustrates the user intake process of `zxidp.org` free IdP. Some business aspects are included as well.

These screens can be accessed live over the internet at `http://zxidp.org/index-idp.html`



ZXID IdP New User Creation

Attribute	Initial Value	Required?	Sharing Default
Username	testy78	Required	Internal use
Password	testy78 *(min. 5 characters)*	Required	Internal use
Reg. Source IP		Detected	Internal use
Common Name	Testy78	Optional*	☑ Share
Org. Title		Optional	☐ Share
Org. Tax Number		Optional	☐ Share
Organization		Optional	☐ Share
Org. Unit		Optional	☐ Share
Street Address		Optional*	☐ Share
Location, Zip, Country		Optional*	☐ Share
Emails	testy78@hotmail.com	Optional**	☐ Share
IM / Skype		Optional	☐ Share
Phone (international)	*(e.g. +15035470202)*	Optional	☐ Share
Language Preference	fi *(2 letter code, e.g. "en")*	Optional	☐ Share
Self tagging	koerkki	Optional	☑ Share
Comments or special requests (internal use)			

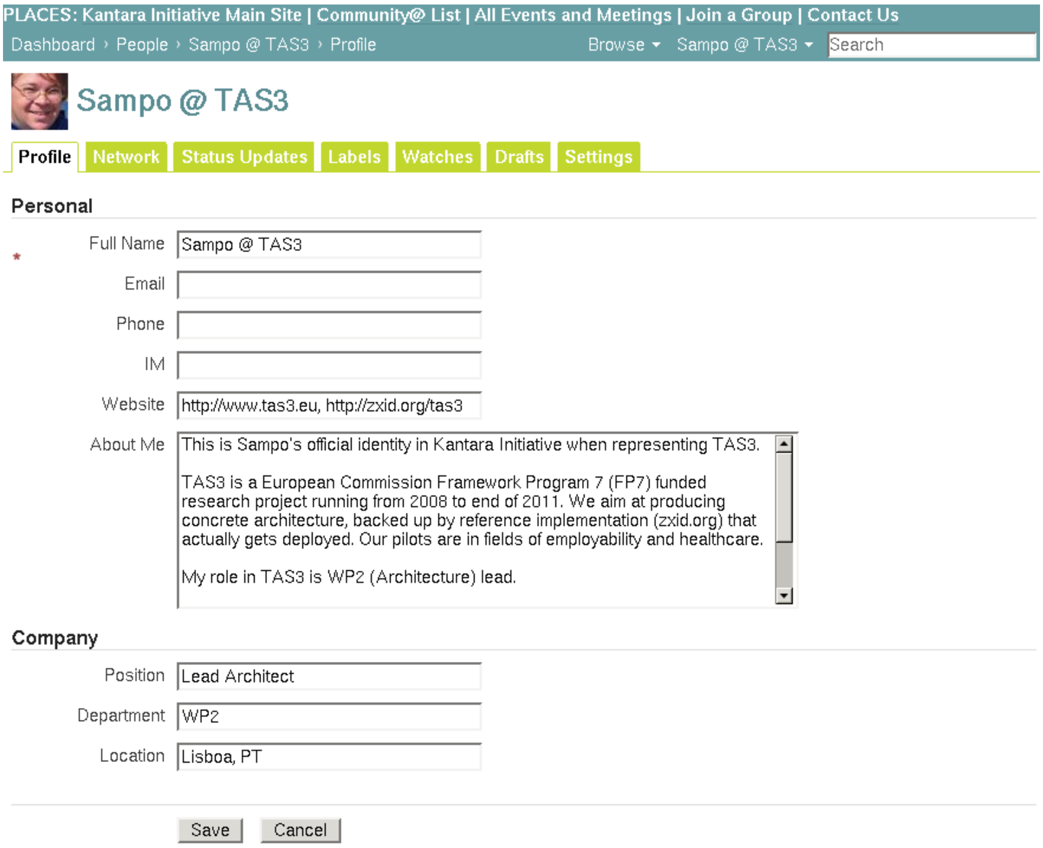
* Required for SP registration (optional for normal users).
** You have to supply email if you ever want to use password recovery feature.

Agree to terms and conditions and register new user
Terms and Conditions for Users
ZXID.org | TAS3.eu | User Dashboard - Id

Figure 36: New user registration screen. Note how almost all fields are optional, but user is on common sense terms encouraged to provide input if they want functionality such as password recovery. The share checkboxes set default sharing policy for the user. It is also important that the user agrees to click-wrap T&Cs.

2.19.2 Kantara Initiative

2.19 New User Intake


PLACES: Kantara Initiative Main Site | Community@ List | All Events and Meetings | Join a Group | Contact Us
Dashboard › People › Sampo @ TAS3 › Profile
Browse ▾
Sampo @ TAS3 ▾
Search
Sampo @ TAS3
Profile
Network
Status Updates
Labels
Watches
Drafts
Settings
Save
Cancel

Personal

Full Name: Sampo @ TAS3 *

Email:

Phone:

IM:

Website: http://www.tas3.eu, http://zxid.org/tas3

About Me: This is Sampo's official identity in Kantara Initiative when representing TAS3.

TAS3 is a European Commission Framework Program 7 (FP7) funded research project running from 2008 to end of 2011. We aim at producing concrete architecture, backed up by reference implementation (zxid.org) that actually gets deployed. Our pilots are in fields of employability and healthcare.

My role in TAS3 is WP2 (Architecture) lead.

Company

Position: Lead Architect

Department: WP2

Location: Lisboa, PT

Figure 37: Kantara Initiative new user profile editing screen. All Altassian Confluence based web sites have similar screen. This screen concentrates mainly on gathering business information.

2.20 Self Audit Business Process

The Business Process Model for Self Audit can be accessed at `https://portal.tas3.eu/trac/wiki/UseCase/SelfAuditAndSPIntake`

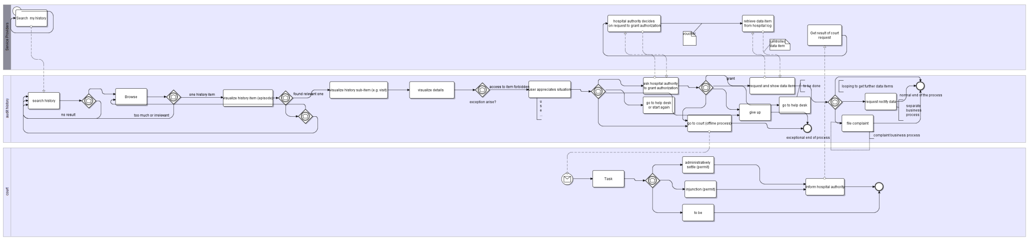

Service Providers
Search my history
hospital authority decides on request to grant authorization
voucher
retrieve data item from hospital log
controlled data item
Get result of court request
audit history
search history
no result
Browse
one history item
too much or irrelevant
visualize history item (episode)
found relevant one
visualize history sub-item (e.g. visit)
visualize details
access to item forbidden
exception arise?
user appreciates situation
u s e ...
ask hospital authority to grant authorization
go to help desk or start again
grant
request and show data item
to be done
go to help desk
give up
go to court (offline process)
exceptional end of process
looping to get further data items
normal end of the process
request rectify data
separate business process
file complaint
complaint business process
court
Task
administratively settle (permit)
injunction (permit)
to be
inform hospital authority

Figure 38: Business Process Model for Self Audit (too small, we know, access the version on the web!).

2.21 Other Use Case Work

[TAS3D42Repo] has an extensive section on use cases, which should be viewed as a complement or extension of what is presented here.

[**?**] has some usage scenarios, especially relating to the pilots, although they are not refined into use cases.

2.22 Future Use Case Work

Some other User Cases we may elaborate on, or that will be elaborated in other TAS^3 deliverables, include:

- Full elaboration of the Trust and Privacy Negotiation Use Case(s)
- SP BPel4People UI
- Trust Guarantor UI
- Bulletin board UI's
- Statistical services from anonymised data UI
- Situation where additional data request deep in the recursive Web Services or business process requires Step-Up authentication
- Processes that may take long time and have start stop states taking longer than a web service call can be reasonably expected to take.

  BPEL engine can monitor this: any timeout is service failure and recorded as such. All service providers must agree to terms SLA on sign up to TAS^3 network and a key element of this will be service reliability and performance.

  - Human steps in process flow can be slow (e.g. process can be waiting sometimes for days / weeks)
- Use case: User wants to audit and complain
  - like on ebay give negative feedback and influence reputation of Service Provider
  - Complaining to wrong entity
  - Misidentifying probable cause
  - Ability trace all the way to the legal evidence

- 3rd party wants to audit or demonstrate that something happened,
  - nonrepudiation
  - articulation to proof in law suits
- Registering a new service to the trust network

References

[FMC03] Frank Keller, Siegfried Wendt: "FMC: An Approach Towards Architecture-Centric System Development", Hasso Plattner Institute for Software Systems Engineering, 2003.

[FMCWeb] "Fundamental Modeling Concepts" http://fmc-modeling.org/

[UML2] http://www.sparxsystems.com.au/resources/uml2_tutorial/

[Wharton94] C. Wharton et al. "The cognitive walkthrough method: a practitioner's guide" in J. Nielsen & R. Mack "Usability Inspection Methods" pp. 105-140, Wiley, 1994.

[CogWalkthruWeb] http://www.cc.gatech.edu/classes/cs3302/documents/cog.walk.html

[IDWSF2IOP] Eric Tiffany, ed.:"Liberty ID-WSF 2.0 Interoperability Testing Procedures", Version Draft 1.0-01, 16. Aug. 2006. File: ID-WSF-2-0-TestProcedures-v1-01.pdf, from http://projectliberty.org/

[IDWSF2MRD] "Liberty ID-WSF 2.0 Marketing Requirements Document", Liberty Alliance, 2006. File: liberty-idwsf-2.0-mrd-v1.0.pdf (from http://projectliberty.org/liberty/strategic_initiatives/requirements/)

[TAS3BIZ] Sampo Kellomäki (EIfEL), ed.: "TAS3 Business Model", TAS3 Consortium, 2009. Document: tas3-biz-model-2009-v05.pdf

[RFC2119] S. Bradner, ed.: "Key words for use in RFCs to Indicate Requirement Levels", Harvard University, 1997.

[TAS3D42Repo] David Chadwick, ed.: "Specification of information containers and authentic repositories", TAS3 Deliverable 4.2, 2009.

[TAS3D14Req] TAS3 Deliverable 1.4, 2009.

Revision History

10 9.9.2010 Sampo

- Added real world screen shots

09 28.4.2010 Sampo

- NOT PUB
- Reviewed existing user interface flows
- Added Az fail scenario and flows, as a new chapter

08 4.4.2009 Sampo

- NOT PUB
- Incorporated comments from David and Luk

07 3.4.2009 Sampo

- First draft out of blue

Document ID `tas3-user-inteface-v10.pdf`

Repository path `repo.tas3.eu:/var/lib/tas3repo/arch/tas3-user-interface.pd` (1.4)

```
export CVSROOT=:ext:repo.tas3.eu:/var/lib/tas3repo
cvs co arch
cd arch
# modify tas3-*.pd
cvs ci -m 'What changed...'
```

URL path `https://portal.tas3.eu/arch/review/tas3-user-interface-v10.pdf`

Commenting

- Please comment on the `TAS3WP02@LISTSERV.CC.KULEUVEN.AC.BE` mailing list, or that failing, send your comments to the editor.
- Any footnotes in this document will not appear in final version. They are editorial comments that may help reviewers to put material in context.