



1 **TAS³: Use Cases, User Interfaces Screens and**
2 **Designs**

3 Sampo Kellomäki (sampo@zxidp.org)

4 October 4, 2010

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

7 **Contents**

8	1 Intro	3
9	1.1 Issues to Consider	5
10	1.1.1 Identification of Actors and User’s Understanding of the	
11	Process	5
12	1.1.2 Service Discovery and Credentials and Privacy Negotiation	6
13	1.1.3 Policy Editing and User Consent	6
14	1.1.4 User data management	7
15	1.1.5 Audit Trail	8
16	2 Generalized Use Cases	8
17	2.1 User Uses Service (First Time in the Session)	10
18	2.2 Already-Logged-in Optimization (SSO)	17
19	2.3 User Uses Dashboard	17
20	2.3.1 Analysis of Google Dashboard (not apples-to-apples) . . .	22
21	2.4 IdP Detected-Optimization (SSO)	23
22	2.5 User Uses Service, Identity Selector Case (e.g. CardSpace, Info-	
23	Card)	23
24	2.6 User Uses Service, Local Login Case (not recommended)	25
25	2.7 User Uses Service, Proxy IdP Case	26
26	2.8 Consenting to PII Release or Manipulation	26
27	2.8.1 Interaction on Front Channel	27
28	2.8.2 Interaction on side channel	27
29	2.8.3 Interaction via Dashboard	30
30	2.8.4 Interaction, such as Consent or Supply of Additional	
31	Data, Inserted into FE User Experience	30
32	2.9 Using Linking Service	31
33	2.10 Choosing amongst Multiple Service Providers	32
34	2.10.1 Simple Choice of Provider	32
35	2.10.2 Credentials and Privacy Negotiation Assisted by User In-	
36	teraction	34
37	2.11 User-Not-Present Transaction	35
38	2.12 User Present Delegation	36
39	2.13 User-Not-Present Delegation	36
40	2.14 Right of Access, Rectification, and Deletion in FE GUI	38
41	2.15 Policy Editing Inserted into FE User Experience	38
42	2.16 Credentials and Privacy Negotiation Inserted into FE User Expe-	
43	rience	38
44	2.17 Unified TAS ³ User Interaction Widget	39
45	2.18 New SP Intake	40

CONTENTS

46	2.18.1 idp.tas3.eu (Jeroen's design)	40
47	2.18.2 zxidp.org	41
48	2.19 New User Intake	47
49	2.19.1 zxidp.org	47
50	2.19.2 Kantara Initiative	47
51	2.20 Self Audit Business Process	49
52	2.21 Other Use Case Work	50
53	2.22 Future Use Case Work	50

54 1 Intro

55 This document specifies some of the user interfaces that need to be developed for
56 TAS³. It attempts to consider the CC¹ view point and feasibility for implementing
57 the user interfaces.

58 The inventory is as follows

59 1. SSO flow including

60 a. IdP selection at SP

61 b. Login at IdP

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

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

64 e. Visualization of the successful login at SP

65 f. Local and Single Logout flows

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

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

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

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

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

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

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

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

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

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

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

108 A particular flow not currently depicted in this document is the password recover
109 or reset flow.

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

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

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

- 117 i. Data group or data set
- 118 ii. Data model or schema
- 119 iii. Who asks. Which SP, which user, role
- 120 iv. Time

1.1 Issues to Consider

121 v. Purpose, business process, business process model

122 vi. (Illegible)

123 Lex Pohlman of Kenteq has additional material on UI aspects of multidimen-
124 sional policies.

125 5. Interaction for consent and simple permission. This is very limited Web GUI,
126 typically realized as iFrame or Div tag.

127 6. Interaction for policy editing. More fully reatured cousin of the consent gath-
128 ering. CC can provide significant improvement in interactivity of the policy
129 editing. This may be part of the Privacy Manager (4).

130 7. Interaction for credentials and privacy negotiation

131 8. Interaction for Right of Access, Rectification, and Deletion

132 **1.1 Issues to Consider**

133 Sometopics I consider worthy of usability or user interface research.

134 **1.1.1 Identification of Actors and User's Understanding of the Process**

135 1. When accessing an application, will user understand that there are multiple
136 actors at play?

137 2. When redirected from SP to IdP will user properly recognize that the IdP is an
138 independent trusted party?

139 3. What can be done to improve user's understanding of party responsible for each
140 step? We feel it is important from legal, responsibility, and good governance
141 perspective that the users realistically understand who they are dealing with.
142 Are standardized / regulated approaches needed? Or should this just be up to
143 brand of the actor?

144 4. When we embed a link or user interface element (iFrame), will users correctly
145 understand the provenance of such element? What can be done to improve this
146 understanding? Will the measures be acceptable from convenience, commer-
147 cial, and branding perspective?

148 5. What can be done to reduce phishing attacks?

1.1 Issues to Consider

- 149 6. Do we need business process overview or progress bar so the user realizes
150 how many steps are still ahead? Should it be possible to go backwards in the
151 process?
- 152 7. How to convey atomicity or final commitment to transaction? For example,
153 after you already supplied credit card number (which gives SP the technical ca-
154 pability charge you), will an additional confirmation screen just confuse users?
155 E.g. user supplies credit card and thinks that completed the transaction, but
156 when he arrives to airport there is no ticket because he did not understand that
157 a separate confirmation was needed.
- 158 8. Multistep wizards vs. single big screen that asks everything and gets the job
159 done in ne step?

160 1.1.2 Service Discovery and Credentials and Privacy Negotiation

- 161 1. How to insert service selection into the user interface of the service requesting
162 site?
- 163 2. How to represent the ranking criteria? Do we allow user to sort or is this too
164 complex?
- 165 N.B. The default ranking is of great commercial interest (c.f.
166 Google) and should be left for market or business model to deter-
167 mine. However, we are interested whether users really need to have
168 ability to navigate other rankings if they so choose?
- 169 3. How complex should remembering choice of default service provider be for
170 given type of service? Is it sufficient to have only one unambiguous default?
171 Or should the default depend on who asks? Or persona? Should choice of
172 default be automatic? If automatic, how to handle exceptional situations where
173 the user does not want it to be automatic?

174 1.1.3 Policy Editing and User Consent

- 175 1. In contextualized incremental policy editing (i.e. asking the consent for spe-
176 cific data as the need arises), what ramifications need to be supported?
- 177 a. Ability to see or edit the global policy?
- 178 b. Ability to see or edit the actual data rather than just the policy?
- 179 c. Ability to see past usage patterns and policy decisions?

1.1 Issues to Consider

- 180 2. How can all this be crammed in one user interface without making it cumber-
181 some?
- 182 3. How to represent in the user interface the extreme multidimensionality of the
183 general / global policy editing?
- 184 Dimensions (each dimension can have hierarchy to represent scale):
- 185 a. Resource, resource group (data item, data group)
 - 186 b. Who (human) asks, group the requester belongs to
 - 187 c. Who (server) asks, group the requester belongs to
 - 188 d. What is the role of requester? Groups of roles?
 - 189 e. What for? Categories of purpose? Specific business processes, business
190 process models?
 - 191 f. Temporal dimension? Will the policy expire? Will it be valid only on work
192 days?

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

198 **1.1.4 User data management**

- 199 1. Dimensionality problem: How to enable user to visualize and edit personas
200 and partial identities?
- 201 2. Are personas defined apriori or as the need arises? Are they keyed on "who
202 asks"?
- 203 3. Ad-hoc persona formulation at the point of data request. What is right granu-
204 larity? How to move from one-off persona to a reusable persona?
- 205 4. Will personas just confuse users? Do we need fixed categories like Work,
206 Friends, and Family?

207 1.1.5 Audit Trail

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

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

- 214 2. What is the appropriate "human readable" explanation of the audit trail
215 records? Would such "human readable" interpretation detract from legal ac-
216 curacy? Could this cause liability?

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

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

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

228 2 Generalized Use Cases

229 **Non-normative.** The simulated user interface screenshots in this sec-
230 tion are NOT normative. They serve merely to illustrate one feasible
231 way of designing the user interface. The user interface flows are also
232 non-normative, for example the IdP detection or already-logged-in
233 detection may follow different paths. Every step of the way, confir-
234 mation questions, wizards, and other user interface devices may be
235 inserted. Depending on business model and branding choices of the
236 Trust Network, there may be some graphical guidelines and restric-
237 tions, see [TAS3BIZ] and Governing Agreement of the Trust Net-
238 work.

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

240 These Use Cases deal with User Interaction, therefore they do not illustrate
241 the rather large Web Services proportion that TAS³ architecture mainly aims to
242 address. Never-the-less, in a User Centric system, we must start with the user -
243 without his impulse (direct or indirect) the back-end Web Services should never
244 happen.

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

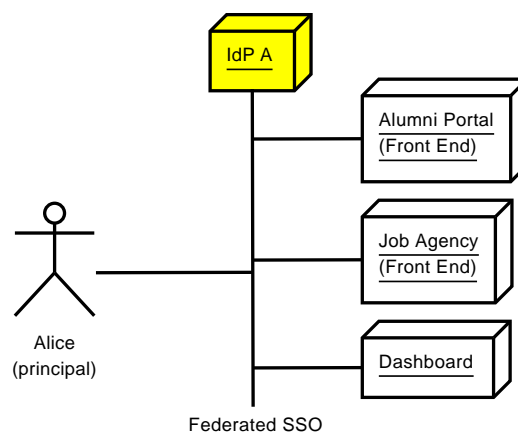


Figure 1: User accesses Front Ends using Single Sign-On.

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

259 Further technical use cases are presented in the next chapter. While use cases
260 in this section aim at illustrating a possible user experience, the use cases in the
261 next chapter mainly aim at scenarios that allow all TAS³ functionality to be exer-
262 cised and tested systematically.

2.1 User Uses Service (First Time in the Session)

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 TAS³ 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.

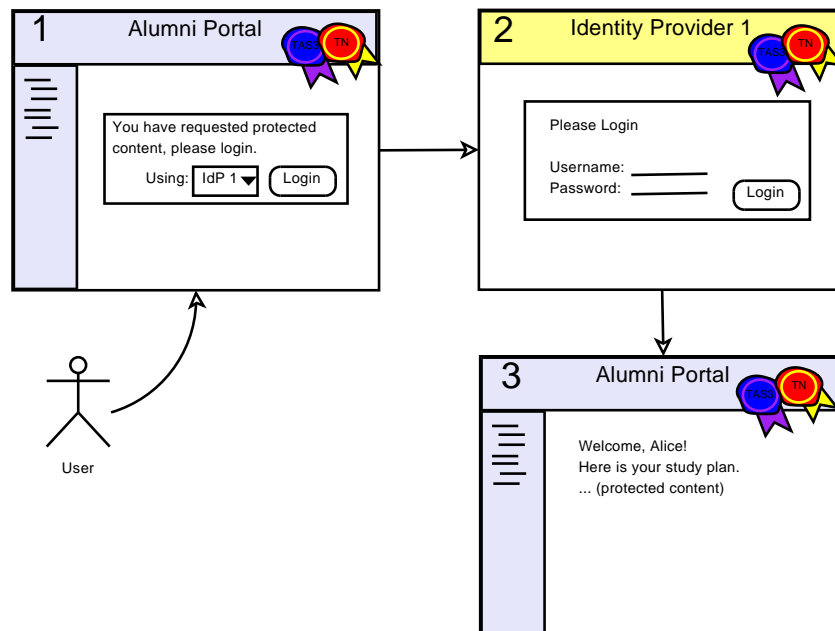


Figure 2: Story board: Using service for 1st time in a session.

Cognitive Walkthrough

2.1 User Uses Service (First Time in the Session)

278 1. Choice of IdP

279 **Motivation** User has taken initiative to perform a task he thinks can be accom-
280 plished using a web site. He realizes that some form of authentication or
281 authorization will be required. When the User navigates to the task, a
282 dialog is presented asking for authentication so that authorization can be
283 granted. User will consider engaging in this dialog because he feels the
284 system is trustworthy, based on the Trust Seals and based on past success-
285 ful experiences.

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

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

301 2. Login

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

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

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

312 **Feedback** Successful authentication will lead to User being returned to the
313 Front End web site. This in itself is a form of feedback, but it should

2.1 User Uses Service (First Time in the Session)

314 be reinforced by the web site providing a clear welcome greeting, stating
315 that the User has been authenticated (and possibly authorized as well).

316 3. **Login complete.** This use case ends here, but an application specific use case
317 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 administrator of the IdP to tell you what the EntityID is.

IdP URL:

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

<input type="button" value="Login to https://lolo:8681/idp.xml (A2)"/>	<input type="button" value="Login to https://lolo:8681/idp.xml (P2)"/>
<input type="button" value="Login to https://a-idp.liberty-iop.org:8881/idp.xml (A2)"/>	<input type="button" value="Login to https://a-idp.liberty-iop.org:8881/idp.xml (P2)"/>
<input type="button" value="Login to https://idp.symdemo.com:8880/idp.xml (A2)"/>	<input type="button" value="Login to https://idp.symdemo.com:8880/idp.xml (P2)"/>

Technical options

Create federation, NID Format:

zxid.org, 0.18.1178728139 libzxid (zxid.org)

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).

2.1 User Uses Service (First Time in the Session)

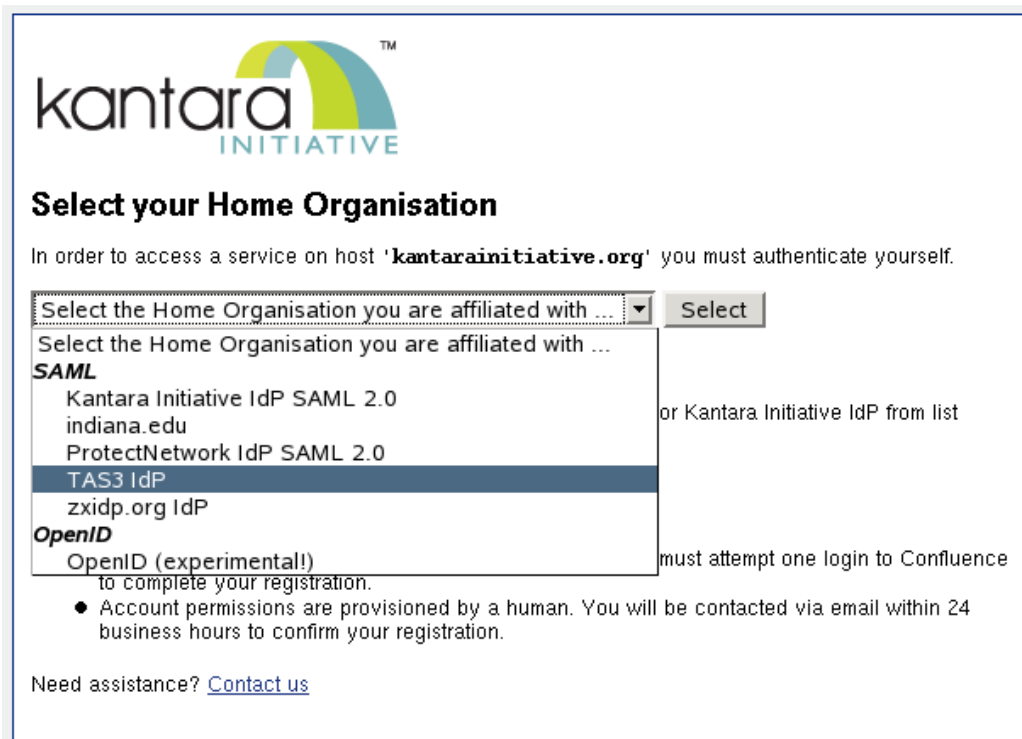


Figure 4: IdP Selection screen of Kantara Initiative WAYF service. This illustrates the popup menu approach with some styling and hierarchical structure in the menu to help user quickly locate the IdP. The popup approach can comfortably handle about 30-40 IdPs and starts to be untractable after about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

2.1 User Uses Service (First Time in the Session)


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 :
2. User: Password:
3.

Technical options

Create federation, NID Format:

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 (pmail.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).

2.1 User Uses Service (First Time in the Session)

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 :
2. User: Password:
3. or

Technical options

Create federation, NID Format:

[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.

2.1 User Uses Service (First Time in the Session)

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 Switch Service Provider

Currently active persona: Primary Switch Persona

Attribute	Value	Authority	Requested / Send	Your internal memo
Username	!!au (<i>can not change</i>)	Internal	Not sent	n.a.
Change Password	<input type="text"/> (min. 5 characters)	Internal	Not sent	n.a.
!!at	!!val	!!auth	<input type="checkbox"/> Send	!!memo
New	<input type="text"/>	Self asserted	<input checked="" type="checkbox"/> Send	<input type="text"/>

Proceed with Login [Terms and Conditions for Users](#)

Save Settings [Terms and Conditions for Users](#)

Delete User Really (no further confirmation)

[ZXID.org](#) | [TAS3.eu](#) | [User Dashboard](#) - *!!d!*

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 inappropriate 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 value in this screen does not change them globally, but rather takes effect only for this transaction (should these be remembered per SP?).

318 **2.2 Already-Logged-in Optimization (SSO)**

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

322

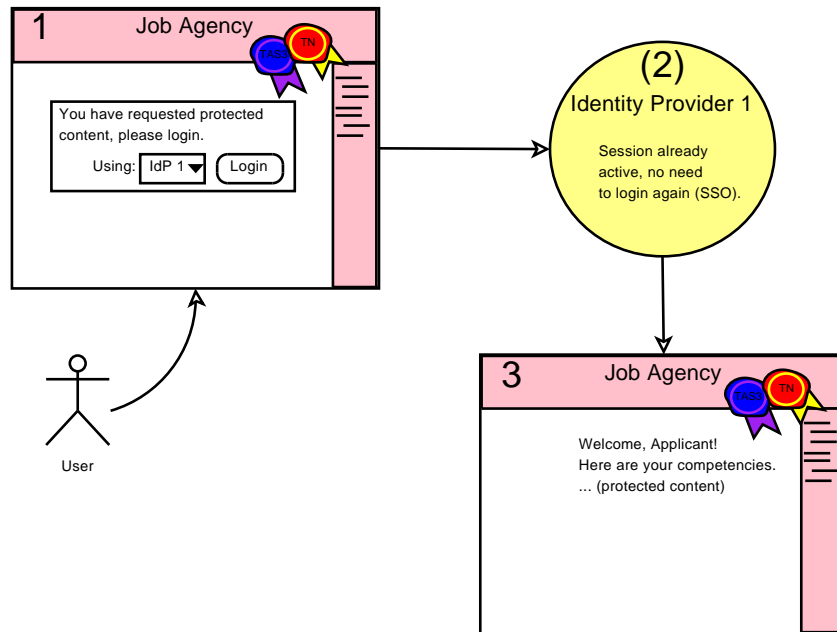


Figure 9: Story board: Using further services after logging in at IdP - Single Sign-On (SSO).

323 **Cognitive Walkthrough**

- 324 1. **Choice of IdP:** Same cognitive walkthrough as in previous section.
- 325 2. **Login:** No cognitive walkthrough needed as no user interface will be presented.
- 326
- 327 3. **Login complete.** This use case ends here, but an application specific use case will start here.
- 328

329 **2.3 User Uses Dashboard**

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

331 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:

332

333

2.3 User Uses Dashboard

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

341 **Cognitive Walkthrough**

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

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

351 **Available and understandable** Since User is assumed to take initiative, a ma-
352 jor hurdle will be how the user finds out about the Dashboard and how to
353 contact it. Some possibilities

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

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

2.3 User Uses Dashboard

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

375 **Feedback** If IdP was detected and user was already logged in, the first feed-
376 back will be Dashboard logged in welcome screen. If authentication
377 is needed, then the IdP context message or the splash screen solutions
378 should be adopted, as described in the previous paragraph.

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

381 3. **Choose Business Process to Audit**

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

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

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

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

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

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

2.3 User Uses Dashboard

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

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

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

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

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

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

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

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

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

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

2.3 User Uses Dashboard

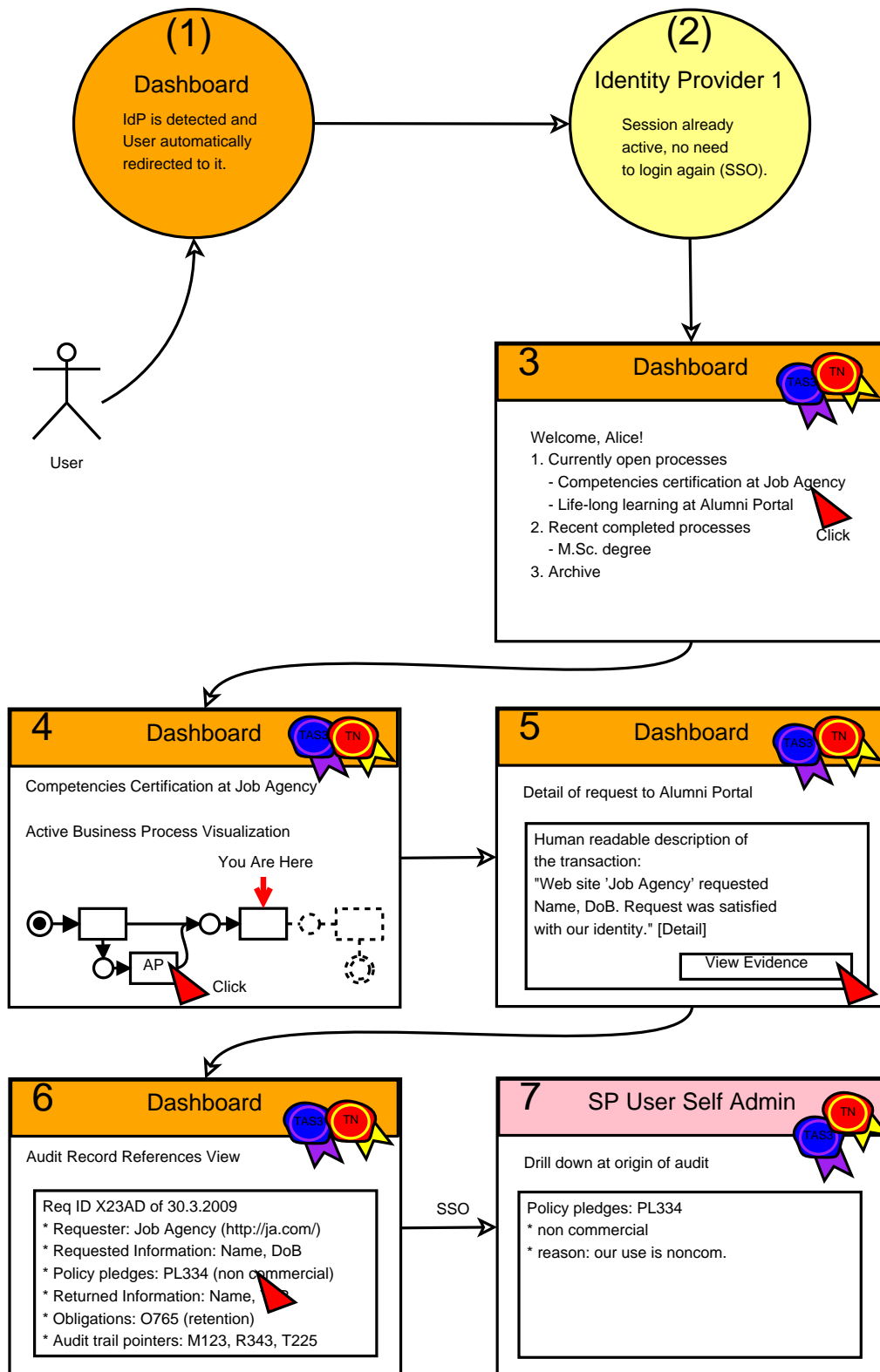


Figure 10: Story board: Using Dashboard to audit a business process

438 2.3.1 Analysis of Google Dashboard (not apples-to-apples)

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

443 TAS³ dashboard has special focus on data usage visibility and user's indepen-
444 dent ability to audit what happens to their data. TAS³ dashboard tries to provide
445 a legal basis for corrective action by the user in case a SP does not collaborate.
446 Other dashboards usually start from the perspective of user not questioning the
447 validity of use of data and instead try to add value by making useful business
448 intelligence available to the user. Google dashboard is a typical example. It is
449 not independent in that it is the holder of the data, Google, that also provides the
450 dashboard. Thus it can be seen that the aims of Google dashboard are dissimilar to
451 TAS³ 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.

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

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

460 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.

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

465 Another interesting feature is the use of email address to identify the collab-
466 orators in sharing. Basically this constitutes a globally unique identifier. It may
467 seem natural in the context of sharing via email, but that does not make it any
468 less perilous. A pairwise pseudonymous identifier architecture would protect the

2.4 IdP Detected-Optimization (SSO)

469 privacy of the collaborators better (but potentially make the listing more cum-
470 bersome for the user, unless some nicknames were displayed). On the positive
471 side, the collaborators are not directly shown - instead just the aggregate count is
472 shown.

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

Figure 13: Google dashboard: Information about web history.

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

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

481 Conclusion is that Google Dashboard is a good example of customer self ad-
482 ministration interface that every responsible data holder should provide, but it
483 fails to address legitimate customer needs for accountability of a service. Thus
484 TAS³ dashboard can complement the Google Dashboard.

485 2.4 IdP Detected-Optimization (SSO)

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

490 2.5 User Uses Service, Identity Selector Case (e.g. CardSpace, 491 InfoCard)

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

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

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

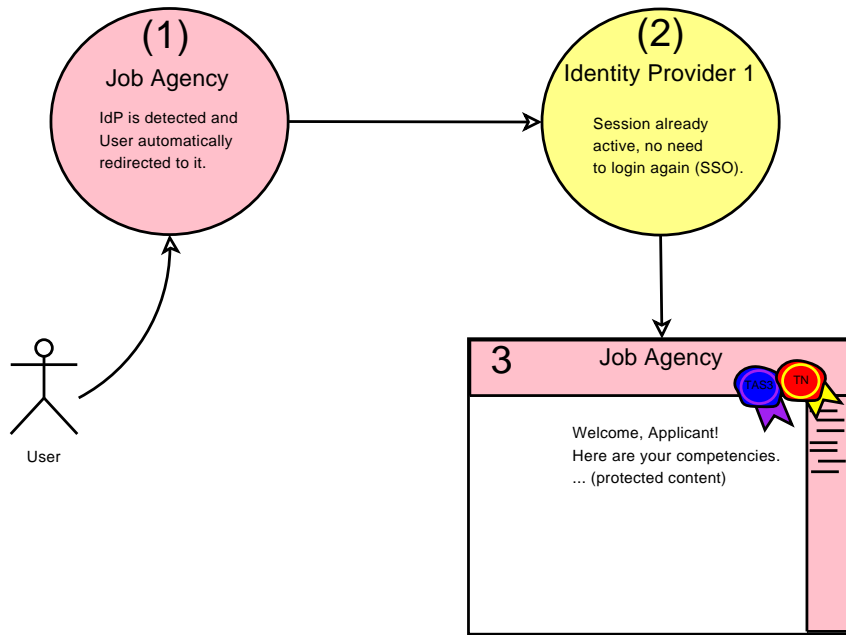


Figure 14: Story board: Fully automatic login - Single Sign-On (SSO) - when IdP can be detected.

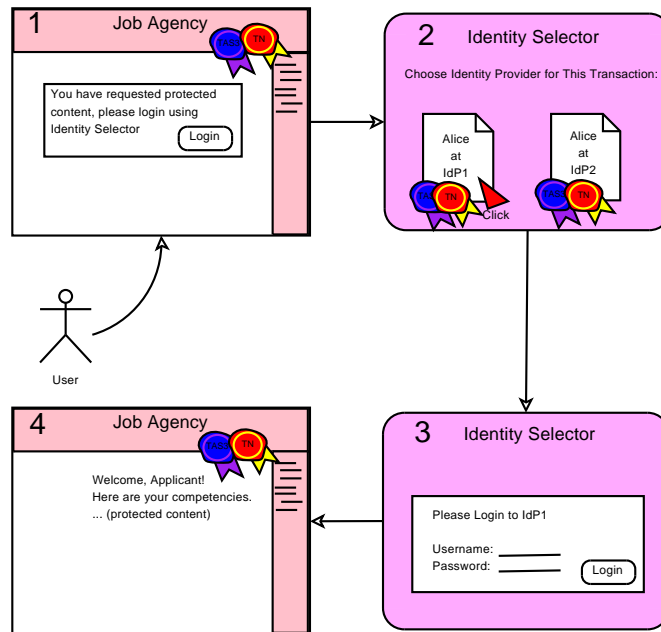


Figure 15: Story board: Identity Selector provides IdP User Interface.

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

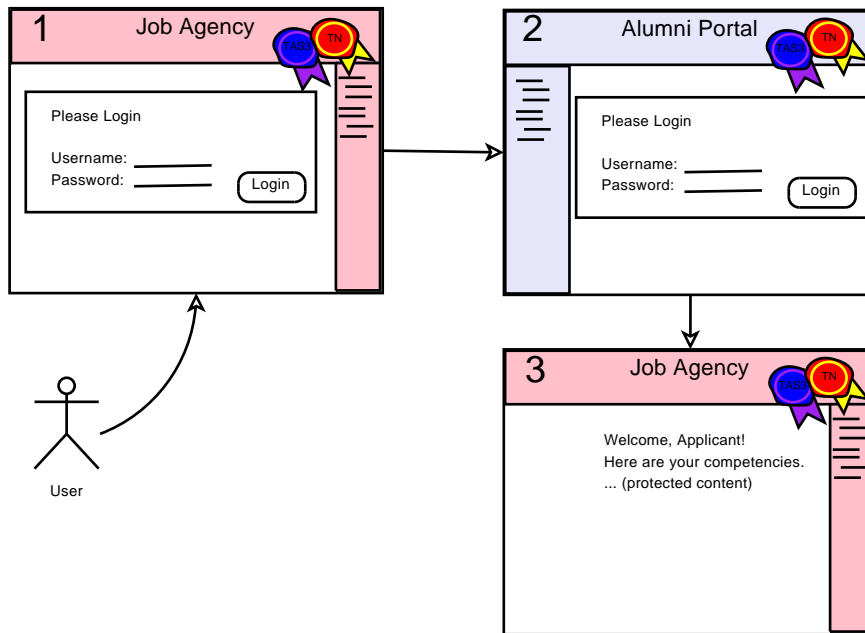


Figure 16: Story board: Using services with local login (not recommended).

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.

2.7 User Uses Service, Proxy IdP Case

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

520 2.7 User Uses Service, Proxy IdP Case

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

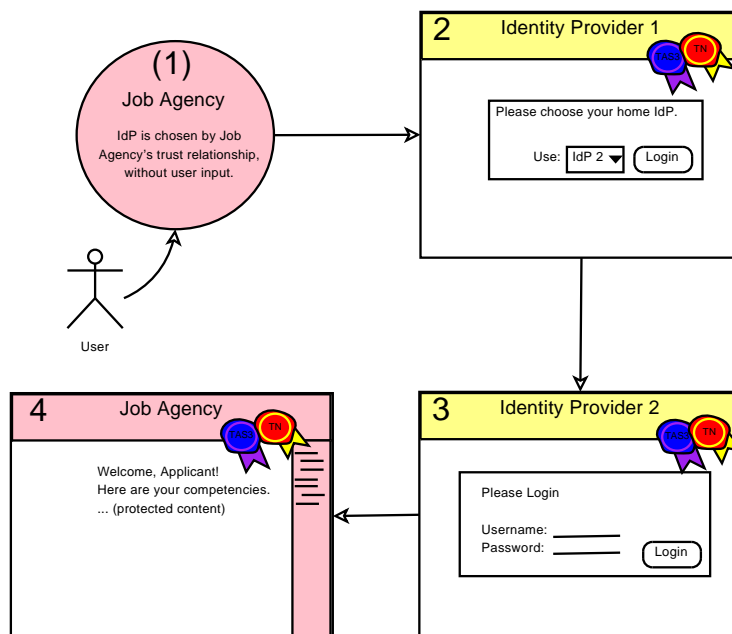


Figure 17: Story board: Login using IdP not trusted by Job Agency.

524 This sequence can be further optimized if the middle IdP can somehow au-
525 tomatically detect which IdP is the home IdP (similar to Section IdP Detected
526 Optimization SSO) and, of course, if the User is already logged in the SSO opti-
527 mization of Section Already Logged-in Optimization SSO.

528 2.8 Consenting to PII Release or Manipulation

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

2.8 Consenting to PII Release or Manipulation

531 **2.8.1 Interaction on Front Channel**

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

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

540 **Cognitive Walkthrough**

541 **1. IdP choice as usual**

542 **2. Authentication as usual**

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

544 **4. Consent to release of PII**

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

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

555 **Feedback** Once consent is given, User lands on page that uses the consented
556 information. This may be sufficient in its own right, but could be en-
557 hanced by high-lighting the information on the page the user just con-
558 sented to.

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

560 **2.8.2 Interaction on side channel**

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

2.8 Consenting to PII Release or Manipulation

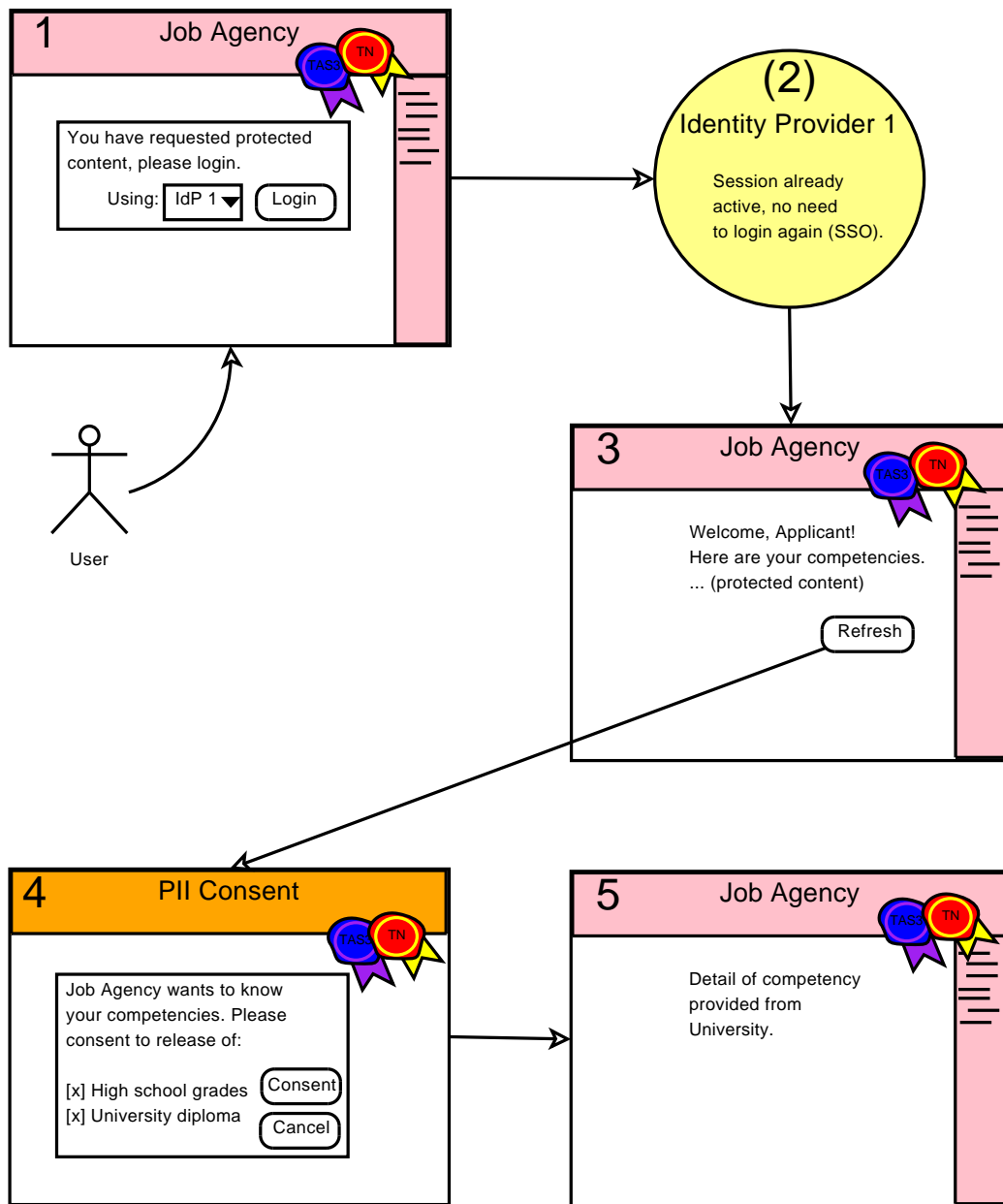


Figure 18: Story board: Presenting a PII consent question in Front Channel interaction.

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

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

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

2.8 Consenting to PII Release or Manipulation

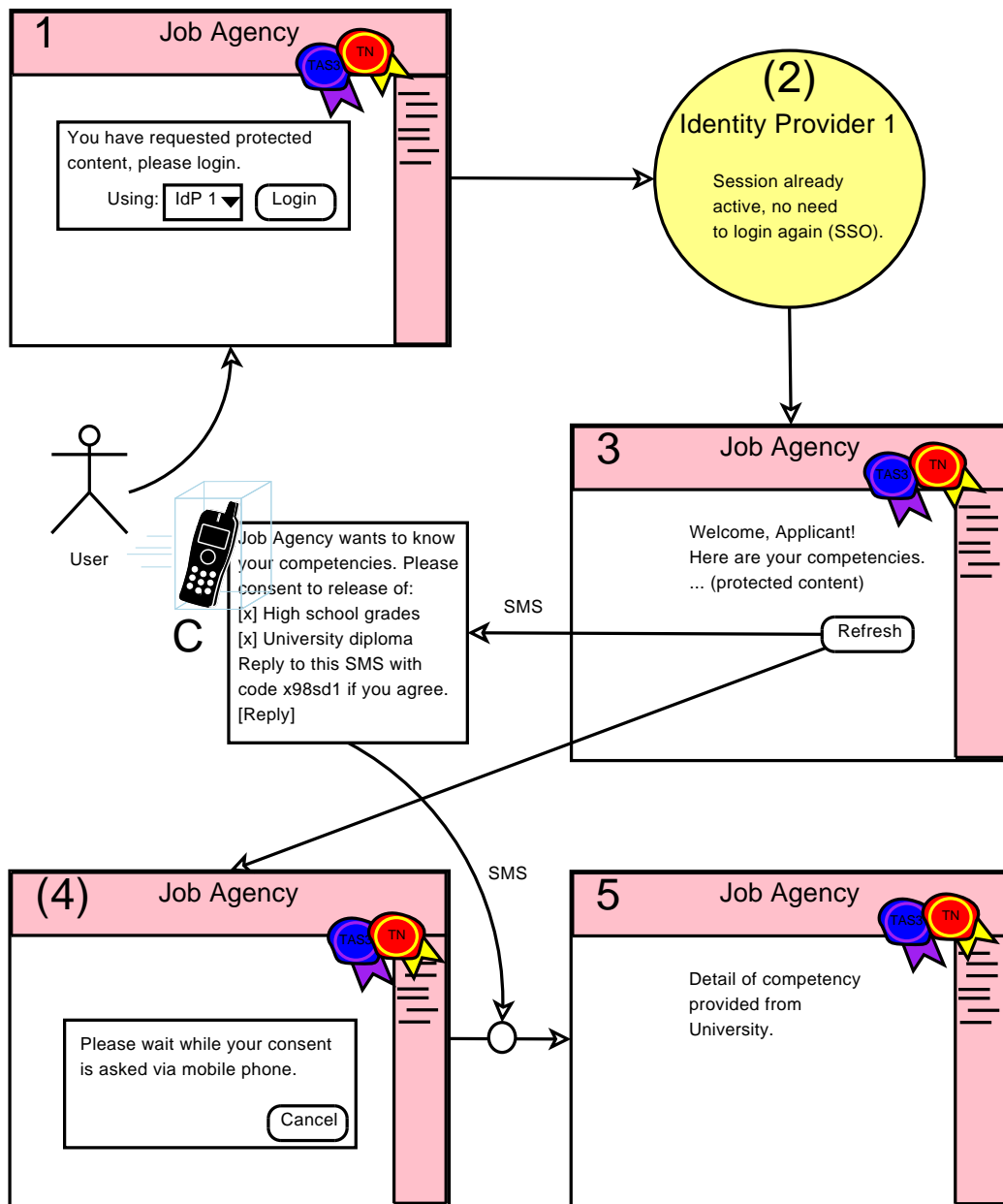


Figure 19: Story board: Presenting a PII consent question using Side Channel interaction.

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

2.8 Consenting to PII Release or Manipulation

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 be 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.

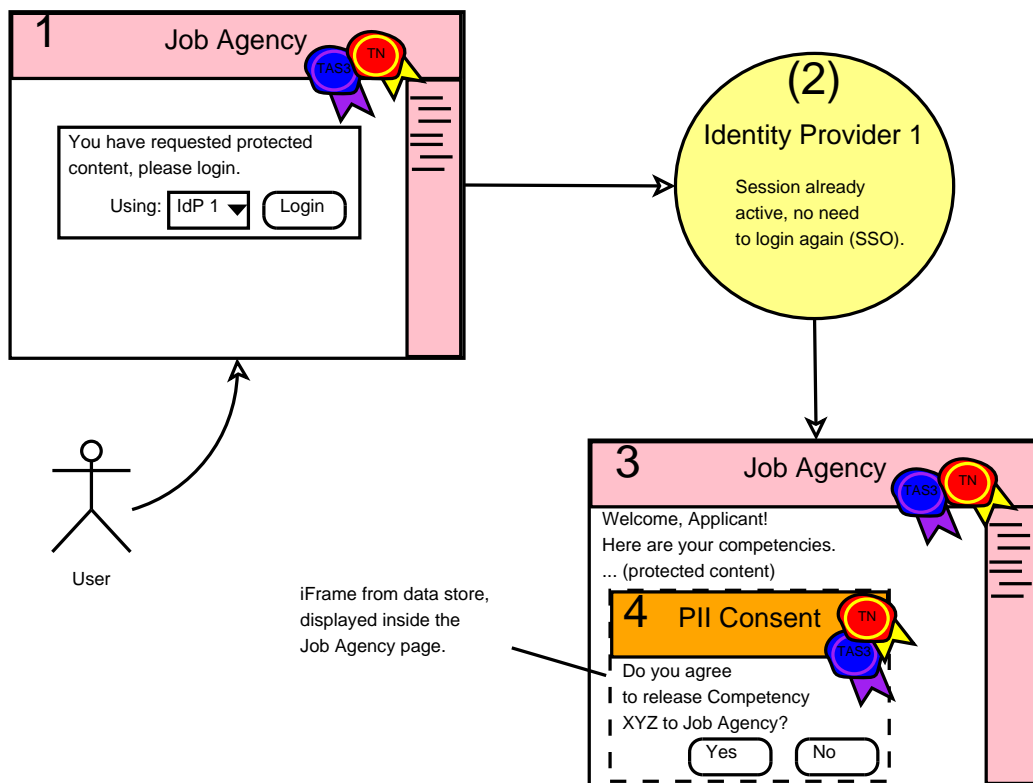


Figure 20: Story board: Presenting a PII consent question using embedded user interface.

585 **2.9 Using Linking Service**

- 586 1. The Linking Service should be user friendly. It may be the only interface that
587 users see for linking their attributes together (other approaches are possible,
588 see "pull model").
- 589 2. A welcome screen explains the purpose of the Linking Service and guides the
590 user through the process of attribute linking. It has
- 591 a. Picking list for choosing IdP
 - 592 b. "Connect" button
 - 593 c. "View linked accounts" button
 - 594 d. "Make linked accounts available to services" button
 - 595 e. Notice or pledge about respecting User's privacy
- 596 3. When the user selects the "Connect" button, the linking service will redirect
597 the user to the selected IdP, allowing the user to login. After login, the user
598 will be redirected back to the linking service welcome screen.
- 599 4. When the user selects "View my linked accounts" he will be presented with the
600 screen with
- 601 a. A table containing two columns, labelled "Organisation" and "Temporary
602 Account Identifier" and at the left hand side by each table entry will be a
603 tick box that the user can tick to remove the linked account. Above the
604 column of tick boxes will be the word Delete.
 - 605 b. "Delete" button, which will remove the chosen accounts from the table and
606 return the user to this page
 - 607 c. "Home Page" button, which will take the user to Welcome screen
 - 608 d. "Make my linked accounts available to services" button, which will take the
609 user to the next screen.
 - 610 e. Notice or pledge about respecting User's privacy
- 611 5. When the user selects the "Make my linked accounts available to services"
612 button he will be presented with a screen containing
- 613 a. An explanation about opt-in in the linking (if you do not make accounts
614 available, the default will be no linking).

2.10 Choosing amongst Multiple Service Providers

- 615 b. A table with 3 columns and a delete tick box beside each row of the table.
616 The table columns are "Service", "Organisation" and "Temporary Account
617 Identifier". The table will always be empty for new users when they first
618 approach this screen.
- 619 c. A picking list of all the services in the federation, obtained from the meta-
620 data of the federation. The first entry in the list will be "All Other Services".
- 621 d. Once the user selects a service provider or "All Other Services" from the
622 picking list, a picking list of all the IdPs that are currently linked together
623 and that appear in the table of the My Linked Accounts Screen, minus the
624 IdPs that have already been paired with the selected service provider is dis-
625 played.
626 The first row of this picking list will be "All My Linked Accounts". The user
627 will then pick one of his linked accounts or "All My Linked Accounts". If
628 the user picks "All My Linked Accounts" a wild card will be inserted into
629 the third column. If the user picks one of his accounts then the third column
630 will be automatically completed with the account Persistent ID unless the
631 user has two or more accounts at the same IdP, in which case the third
632 column will contain a picking list of Persistent IDs sent from that IdP, minus
633 any already selected for this service provider.
634 It is important that the table always lists the service providers in alphabetical
635 order so that the user can easily see which links he has set up for which SPs,
636 and for every SP, the linked IdPs are in alphabetical order.
- 637 e. "Delete" button, which will remove the chosen accounts from the table and
638 return the user to this page
- 639 f. "Home Page" button, which will take the user to Welcome screen
- 640 g. "View my linked accounts" button, which will take the user to the screen
641 referred to in step (4), above.

642 **2.10 Choosing amongst Multiple Service Providers**

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

647 **2.10.1 Simple Choice of Provider**

648 **Cognitive Walkthrough**

649 **1. IdP choice as usual**



2.10 Choosing amongst Multiple Service Providers

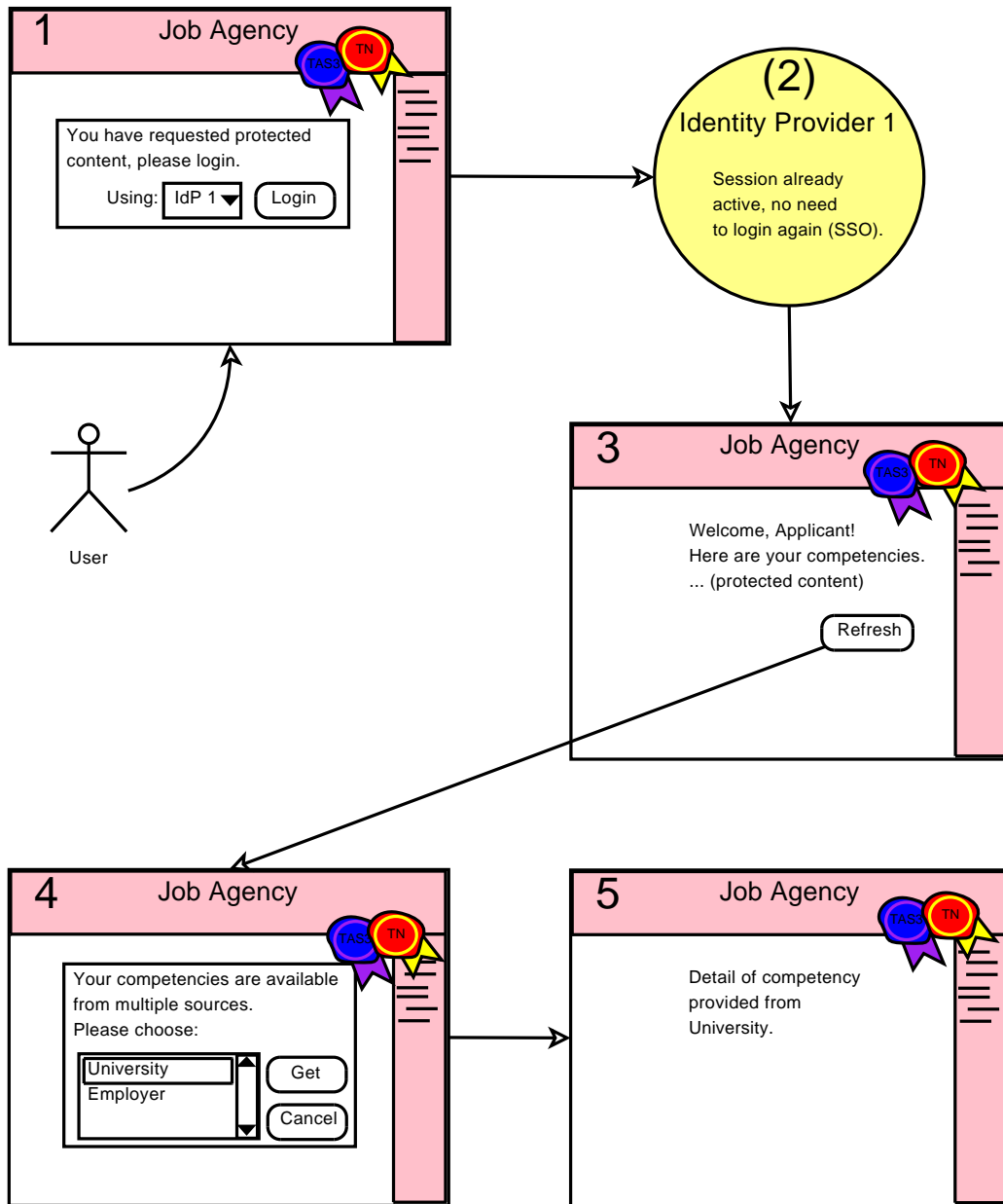


Figure 21: Story board: Choice of Service Provider.

650 2. Authentication as usual

651 3. User triggers action, as usual

652 4. Choose Service Provider

653 **Motivation** The decision point will be imposed to the user through modal

2.11 User-Not-Present Transaction

654 user interaction. User will be motivated to make the choice as he may
655 guard different information, e.g. different personae, at different Attribute
656 Authorities.

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

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

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

665 2.10.2 Credentials and Privacy Negotiation Assisted by User Interaction

666 Cognitive Walkthrough

667 1. IdP choice as usual

668 2. Authentication as usual

669 3. User triggers action, as usual

670 4. Negotiate appropriate supplier for service or information

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

676 **Available and understandable** Presenting complex trust based decision is
677 not easy. This topic will be further researched during TAS³ project.

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

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

2.11 User-Not-Present Transaction

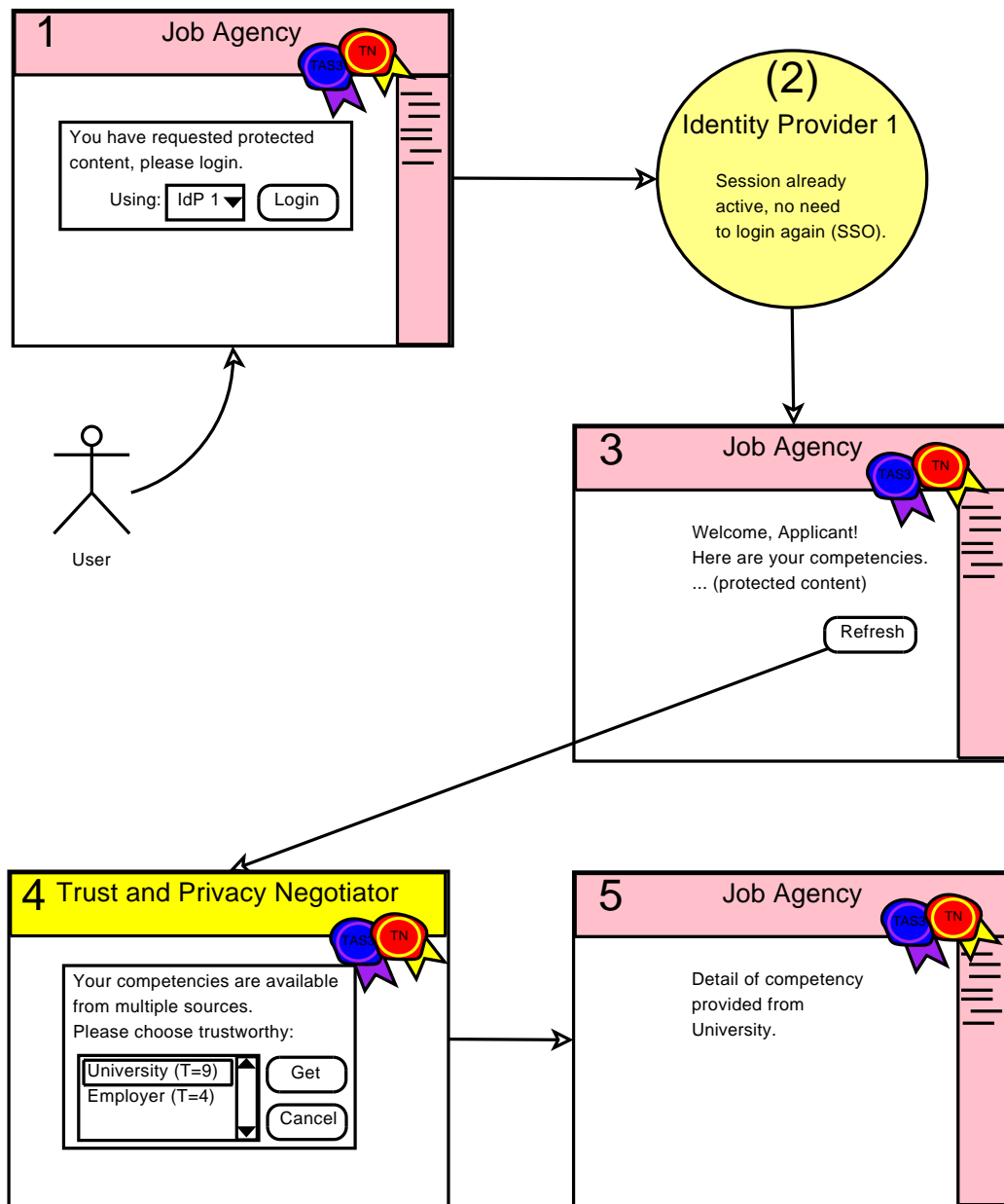


Figure 22: Story board: Credentials and Privacy Negotiation with User Interaction.

683 2.11 User-Not-Present Transaction

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

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

2.12 User Present Delegation

- 687 2. There is an over-arching legal or legitimate business requirement. Existence of
688 such requirement MUST be demonstratable from the audit trail.
- 689 3. "Break the glass" scenarios. Again audit trail MUST capture legitimate reason
690 why the scenario was invoked and the audit trail should be especially detailed
691 about the actions performed under the break the glass authority.

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

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

698 **2.12 User Present Delegation**

699 See Fig-23.

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

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

705 **2.13 User-Not-Present Delegation**

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

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

2.13 User-Not-Present Delegation

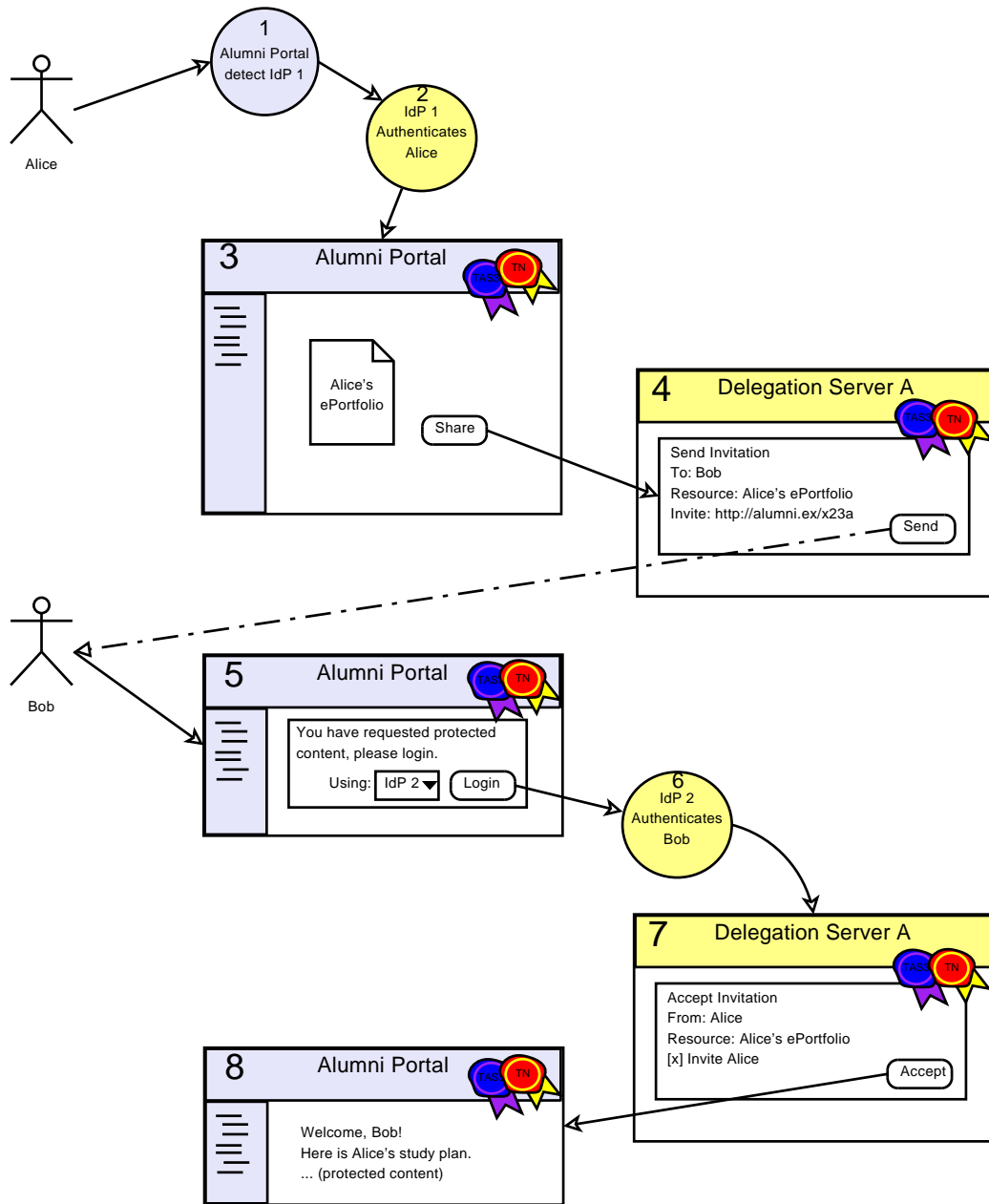


Figure 23: Story board: Alice invites Bob to view her ePortfolio.

710 **2.14 Right of Access, Rectification, and Deletion in FE GUI**

711 Right of Access, Rectification, and Deletion are guaranteed by European regulation.
712 To support these goals, TAS³ Dashboard can provide a unified interface to
713 send such requests to various data authorities and stores.

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

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

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

724 **2.15 Policy Editing Inserted into FE User Experience**

725 TAS³ Dashboard can provide a unified central interface for policy editing. This
726 could be implemented by each data holder providing a link to its policy editing
727 interface. The links are centrally available on the dashboard, but the editing itself
728 happens at the data holder.

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

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

737 **2.16 Credentials and Privacy Negotiation Inserted into FE**
738 **User Experience**

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

2.17 Unified TAS³ User Interaction Widget

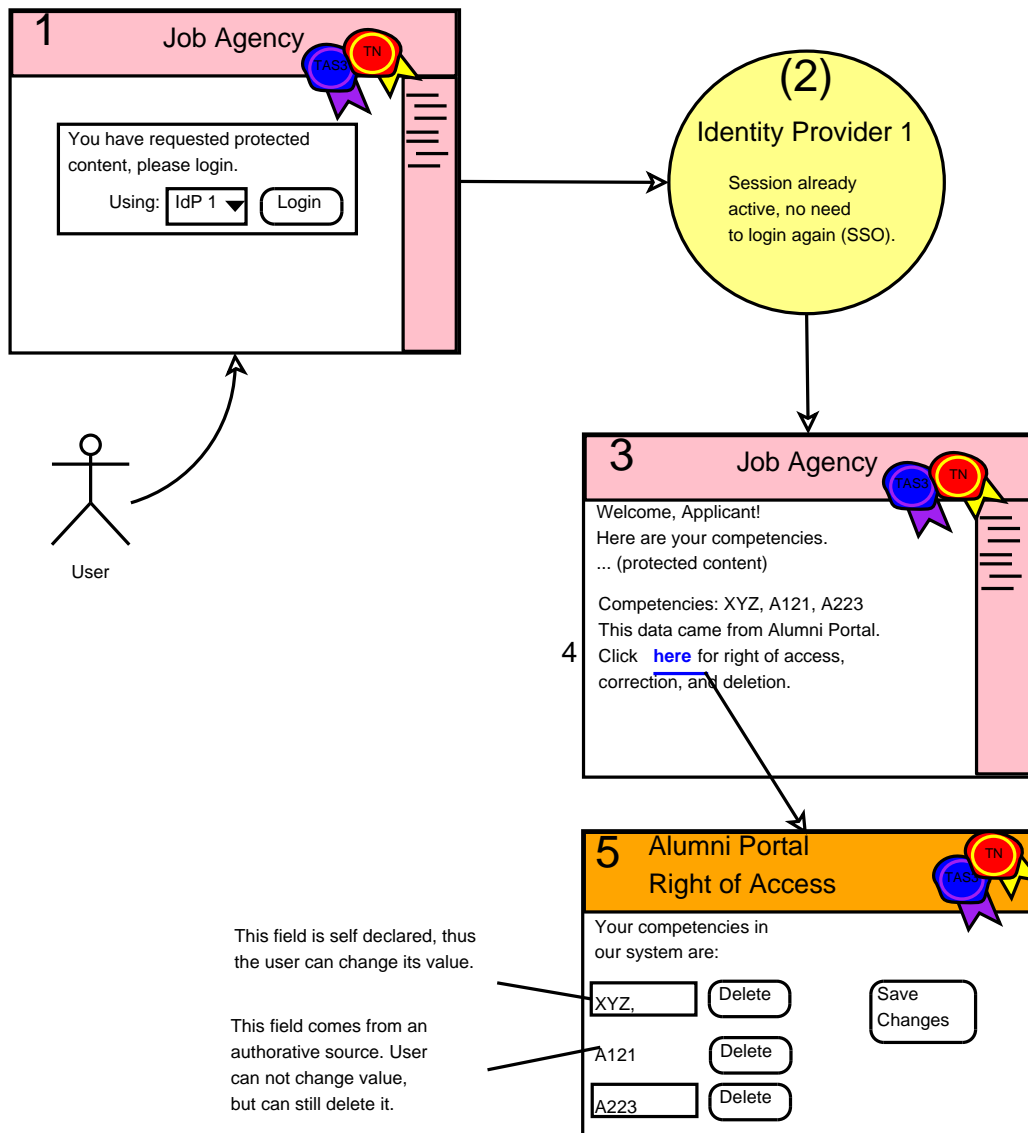


Figure 24: Right of Access using link embedded on page.

746 2.17 Unified TAS³ User Interaction Widget

747 Many of the user interaction aspects could be unified in a TAS³ interaction widget
 748 that is inserted into SP pages (e.g. as iFrame). The widget would then poll or
 749 refresh itself periodically from the dashboard server and if there are events of note
 750 to report, show a one line notice to the user, with a link for user to click for further
 751 interaction.

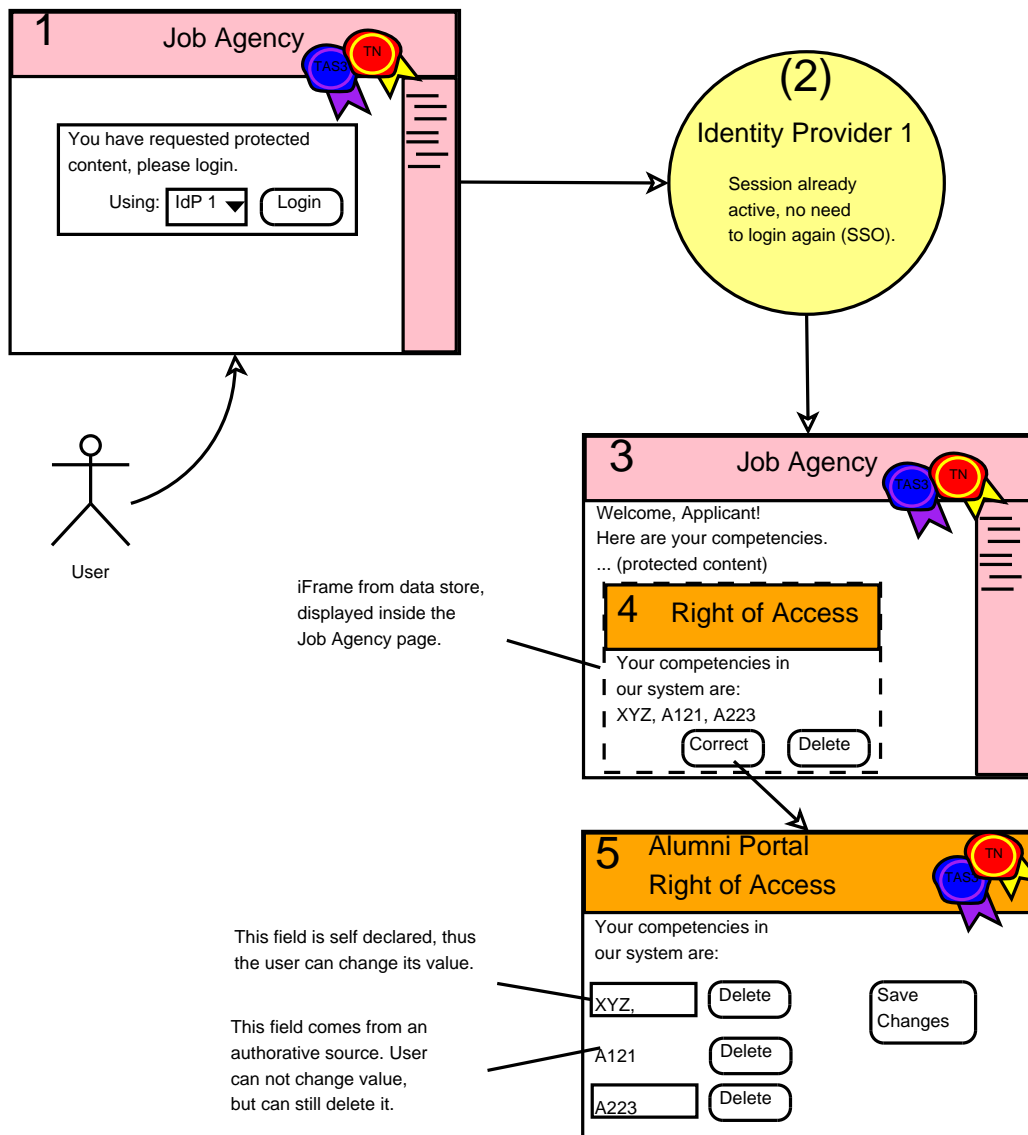


Figure 25: Story board: Right of access using embedded user interface.

752 **2.18 New SP Intake**

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

755 **2.18.1 idp.tas3.eu (Jeroen's design)**

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

2.18 New SP Intake

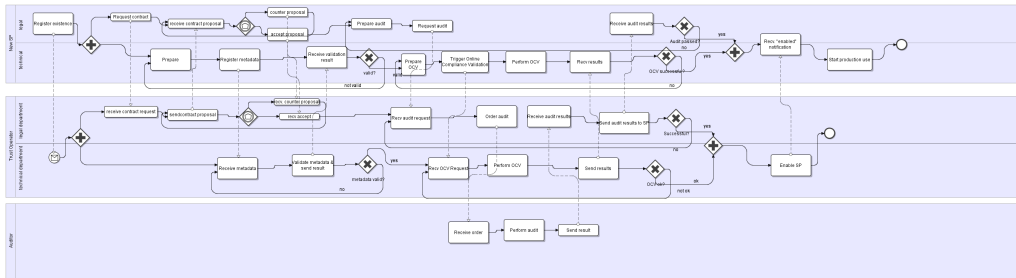


Figure 26: Business Process Model for SP intake (too small, we know, access the version on the web!)

758 ness data gathering.

759 These screens can be accessed live over the internet at
760 <https://idp.tas3.eu/cot/>

TAS³ Circle of Trust Manager



[IDPdmo 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):

or paste the metadata in here:

Submit SP Endpoint Reference to this IdP

SOAP Endpoint (URL)

Description (max. 64 chars)

Entity ID (URL)

Service Type (URN)

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

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

761 2.18.2 zxidp.org

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



TAS³ Circle of Trust Manager



IDPdemo Home	Service Provider	Last Metadata
CoT Mgr	http://141.26.66.254/portal/sso?o=B	2010-02-25 22:22Z
IdP Metadata	http://tas3-repo2.custodix.com/downloadDocument?o=B	2010-02-17 15:58Z
Known SPs	http://taipei.ipd.uka.de:8084/zxidervlet/sso?o=B	2010-01-15 17:24Z
Known Metadata	https://tas3-repo1.custodix.com/listPatients?o=B	2010-02-02 03:05Z
Known End Points	https://tas3-portal.custodix.com/zxidsp?o=B	2010-01-19 13:12Z
Manual	http://87.106.206.244:8080/zxidervlet/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/zxidervlet/sso?o=B	2010-02-24 12:04Z
	https://zxidip.uni-koblenz.de/zxidip?o=B	2010-02-24 12:31Z
	/zxidervlet/wspdemo?o=B	2010-02-16 11:46Z
	https://89.200.142.218/shibboleth	2010-08-02 16:18Z
	https://idp.tas3.eu/zxidip?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

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory			-
-BAYkVTtv61brIpQc4KzJqLgxlC	02-Aug-2010 18:18	6.4 K	
1JM9w5gsqr8nDargTnsDcCUMIH4	28-Jul-2010 18:14	3.1 K	
4loyOPoc7ATaTmP3xommhFjBSUO	15-Mar-2010 11:57	2.8 K	
6E_BhFs8bBnOb55rqOeLbBtCEmc	02-Feb-2010 04:05	2.8 K	
9pYehe17SpT-MXEfPlxhwgqphJI	08-Feb-2010 15:31	2.8 K	
9u7LsQjkz0VaXKucmx1sYjQnM	14-Jan-2010 17:10	6.8 K	
816Zv9aoblM4jrpAYPQre-Sbni	16-Feb-2010 12:46	4.1 K	

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".

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

TAS³ Circle of Trust Manager



IDPdmo Home	Service Type	Addr	Provider ID	Registered	Abstract
CoT Mgr			URL	2010-02-17 18:12Z	
IdP Metadata	http://matcher.com	URL	87.106.206.244:8080/	2010-01-21 15:47Z	web service provider (matcher)
Known SPs	urn:ios:pds:2010-05:dst-2.1	URL	192.168.135.139:ttt	2010-07-01 11:36Z	Fisaris PDS ttt
Known Metadata	urn:liberty:disco:2006-08	URL	idp.tas3.eu:zxidp?	2010-01-14 15:58Z	TAS3 Discovery Service (ID-WSF 2.0)
Known End Points	urn:liberty:disco:2006-08	URL	idp.tas3.pt:8081/zxi	2010-01-15 08:59Z	TAS3 Default Discovery Service (ID-WSF 2.0)
Manual	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 assurance 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](#) - \$!d\$

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



The screenshot shows the 'Service Provider Metadata Registration' screen. At the top is a dark blue header with the text 'ZXID IdP Circle of Trust Manager' in white. Below the header is the title 'Service Provider Metadata Registration'. Underneath is the instruction 'Paste metadata here:' followed by a large, empty white text area. Below the text area is a button labeled 'Submit Metadata'. At the bottom of the screen is a dark blue footer containing navigation links: 'ZXID.org | TAS3.eu -- Top | Register Metadata | View Metadata | Register Web Service | View Discovery'.

Figure 32: Metadata upload screen

The screenshot shows the 'Web Service Discovery Registration' screen. At the top is a dark blue header with the text 'ZXID IdP Circle of Trust Manager' in white. Below the header is the title 'Web Service Discovery Registration'. Underneath are four input fields with labels: 'Endpoint URL', 'Abstract', 'Entity ID', and 'Service Type (URN)'. Each label is in a light blue box, and each has an adjacent empty white input field. Below the input fields is a button labeled 'Submit Discovery Registration'. At the bottom of the screen is a dark blue footer containing navigation links: '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			
<i>This listing reflects the Service Providers known to us, i.e. in our Circle of Trust.</i>			
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	xsKJr3DL7sUPDdbdggC2H_eP-UM	Tue Nov 10 08:43:31 2009	-
http://localhost:8082/pdmail.pl?o=B	9RHlaxHzbMXxKpOuQI4H_bIQzso	Tue May 18 14:35:51 2010	-
http://other.zxidp.org:8080/zxidervlet/wspleaf?o=B	AsKqjEQ0W6eohmyzwLRbbND1I3Y	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.

ZXID IdP Circle of Trust Manager		
Web Service Discovery Registration Listing		
<i>This listing reflects the web services known to us, i.e. the ones that are discoverable.</i>		
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_0C31ioZtDCOKbp1ljo	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-652lJbx6UgpBNX8S8	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-lkn1ZylScA	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,NNSeTYwDoGOF6kF7KDE8HEg1YVq	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,vpVccylDZ2Hp7qPBN2okajgRuzM	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

765 2.19 New User Intake

766 2.19.1 zxidp.org

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

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

ZXID IdP New User Creation

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

* 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](#) - \$/d\$

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.

771 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 ▾

 **Sampo @ TAS3**

Profile | Network | Status Updates | Labels | Watches | Drafts | Settings

Personal

* Full Name
Email
Phone
IM
Website
About Me

Company

Position
Department
Location

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

772 **2.20 Self Audit Business Process**

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

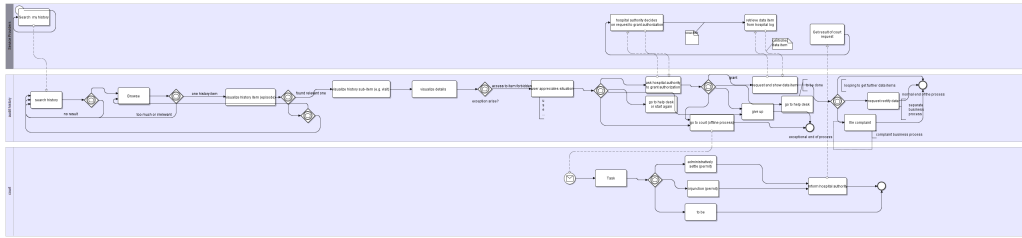


Figure 38: Business Process Model for Self Audit (too small, we know, access the version on the web!).

775 **2.21 Other Use Case Work**

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

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

780 **2.22 Future Use Case Work**

781 Some other User Cases we may elaborate on, or that will be elaborated in other
782 TAS³ deliverables, include:

- 783 • Full elaboration of the Trust and Privacy Negotiation Use Case(s)
- 784 • SP BPel4People UI
- 785 • Trust Guarantor UI
- 786 • Bulletin board UI's
- 787 • Statistical services from anonymised data UI
- 788 • Situation where additional data request deep in the recursive Web Services
789 or business process requires Step-Up authentication
- 790 • Processes that may take long time and have start stop states taking longer
791 than a web service call can be reasonably expected to take.
- 792 BPEL engine can monitor this: any timeout is service failure and recorded
793 as such. All service providers must agree to terms SLA on sign up to TAS³
794 network and a key element of this will be service reliability and perfor-
795 mance.
 - 796 - Human steps in process flow can be slow (e.g. process can be waiting
797 sometimes for days / weeks)
- 798 • Use case: User wants to audit and complain
 - 799 - like on ebay give negative feedback and influence reputation of Service
800 Provider
 - 801 - Complaining to wrong entity
 - 802 - Misidentifying probable cause
 - 803 - Ability trace all the way to the legal evidence

REFERENCES

- 804 • 3rd party wants to audit or demonstrate that something happened,
 - 805 - nonrepudiation
 - 806 - articulation to proof in law suits
- 807 • Registering a new service to the trust network

808 References

- 809 [FMC03] Frank Keller, Siegfried Wendt: "FMC: An Approach Towards
810 Architecture-Centric System Development", Hasso Plattner In-
811 stitute for Software Systems Engineering, 2003.
- 812 [FMCWeb] "Fundamental Modeling Concepts" <http://fmc-modeling.org/>
- 813 [UML2] http://www.sparxsystems.com.au/resources/uml2_tutorial/
- 814 [Wharton94] C. Wharton et al. "The cognitive walkthrough method: a prac-
815 titioner's guide" in J. Nielsen & R. Mack "Usability Inspection
816 Methods" pp. 105-140, Wiley, 1994.
- 817 [CogWalkthruWeb] <http://www.cc.gatech.edu/classes/cs3302/documents/cog.walk.html>
- 818 [IDWSF2IOP] Eric Tiffany, ed.: "Liberty ID-WSF 2.0 Interoperabil-
819 ity Testing Procedures", Version Draft 1.0-01, 16. Aug.
820 2006. File: ID-WSF-2-0-TestProcedures-v1-01.pdf, from
821 <http://projectliberty.org/>
- 822 [IDWSF2MRD] "Liberty ID-WSF 2.0 Marketing Requirements Document", Lib-
823 erty Alliance, 2006. File: liberty-idwsf-2.0-mrd-v1.0.pdf (from
824 http://projectliberty.org/liberty/strategic_initiatives/requirements/)
- 825 [TAS3BIZ] Sampo Kellomäki (EIFEL), ed.: "TAS3 Business Model", TAS3
826 Consortium, 2009. Document: tas3-biz-model-2009-v05.pdf
- 827 [RFC2119] S. Bradner, ed.: "Key words for use in RFCs to Indicate Require-
828 ment Levels", Harvard University, 1997.
- 829 [TAS3D42Repo] David Chadwick, ed.: "Specification of information containers
830 and authentic repositories", TAS3 Deliverable 4.2, 2009.
- 831 [TAS3D14Req] TAS3 Deliverable 1.4, 2009.

REFERENCES

832 **Revision History**

833 **10** 9.9.2010 Sampo

- 834 • Added real world screen shots

835 **09** 28.4.2010 Sampo

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

839 **08** 4.4.2009 Sampo

- 840 • NOT PUB
841 • Incorporated comments from David and Luk

842 **07** 3.4.2009 Sampo

- 843 • First draft out of blue

844 **Document ID** tas3-user-inteface-v10.pdf

845 **Repository path** repo.tas3.eu:/var/lib/tas3repo/arch/tas3-user-interface.pd
846 (1.4)

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

852 **URL path** <https://portal.tas3.eu/arch/review/tas3-user-interface-v10.pdf>

853 **Commenting**

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