TAS$^3$: User Interface Contribution (to be integrated in Architecture)

Editor: Sampo Kellomäki (sampo@symlabs.com), EIfEL

January 20, 2010

Disclaimer: This document has not been reviewed or approved by European Commission.

Contributors
David Chadwick, Kent
Luk Vervenne, Synergetics
CONTENTS

Contents

1 Intro 3

2 Generalized Use Cases 3

2.1 User Uses Service (First Time in the Session) 4

2.2 Already-Logged-in Optimization (SSO) 6

2.3 User Uses Dashboard 6

2.4 IdP Detected-Optimization (SSO) 11

2.5 User Uses Service, Identity Selector Case 11

2.6 User Uses Service, Local Login Case 11

2.7 User Uses Service, Proxy IdP Case 13

2.8 Consenting to PII Release or Manipulation 13

2.8.1 Interaction on Front Channel 14

2.8.2 Interaction on side channel 14

2.8.3 Interaction via Dashboard 17

2.9 Using Linking Service 18

2.10 Choosing among Multiple Service Providers 19

2.10.1 Simple Choice of Provider 19

2.10.2 Trust and Privacy Negotiation Assisted by User Interaction 21

2.11 User-Not-Present Transaction 22

2.12 User Present Delegation 23

2.13 User-Not-Present Delegation 23

2.14 Other Use Case Work 23

2.15 Future Use Case Work 24
1 Intro

(placeholder to get numbering to match tas3-arch document)

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 choices 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 TAS³ 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.

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.
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.

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
2.1 User Uses Service (First Time in the Session)

dialog is presented asking for authentication so that authorization can be
granted. User will consider engaging in this dialog because they feel the
system is trustworthy, based on the Trust Seals and based on past success-
ful experiences.

Available and understandable User will be guided by modality of the inter-
action 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 IdP selec-
tion as a major problem. 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 moti-
vated 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
2.2 Already-Logged-in Optimization (SSO)

step if he reasonably can. This mind set is reinforced by IdP providing feedback as to what task requires the authentication.

Biggest challenge and inconvenience 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.

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.

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)
2.3 User Uses Dashboard

![Diagram of user dashboard and single sign-on (SSO)]

Figure 3: Story board: Using further services after logging in at IdP - Single Sign-On (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 noise 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
2.3 User Uses Dashboard

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-4 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 hierarchy 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 detail and request audit item from Front End**

**Motivation** User needs to get evidence about a step of a process

6. **View audit item** (not depicted in the figure)

7. **Escalate** (not depicted in the figure) (Req. *D1.2-6.9-Complaint*)
2.4 IdP Detected-Optimization (SSO)

This flow, see Fig. 5, 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

In the Identity Selector flow, see Fig. 6, 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.

2.6 User Uses Service, Local Login Case

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.
2.6 User Uses Service, Local Login Case

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

Figure 6: Story board: Identity Selector provides IdP User Interface.

Figure 7: Story board: Using services with local login (not recommended).
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.

2.7 User Uses Service, Proxy IdP Case

This sequence, see Fig. 8, 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.

![Diagram](image)

Figure 8: 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 Consenting to PII Release or Manipulation

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.9 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
Consenting to PII Release or Manipulation

Figure 9: Story board: Presenting a PII consent question in Front Channel interaction.

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...
2.8 Consenting to PII Release or Manipulation

Figure 10: 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 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.
2.9 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).
2.10 Choosing among Multiple Service Providers

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 among 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
2.10 Choosing among Multiple Service Providers

Figure 11: 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
2.11 User-Not-Present Transaction

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 Trust 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 TAS³ 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.
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 authorized, indirectly, the transaction. Audit trail MUST show this authorization.

Figure 12: Story board: Trust and Privacy Negotiation with User Interaction.
2.12 User Present Delegation

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-13.

- 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).

2.14 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.
2.15 Future Use Case Work

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

- Full elaboration of the Trust and Privacy Negotiation Use Case(s)
• SP BPel4People UI
• Trust Guarantor UI
• SP registration process 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 TAS³ 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

References


Revision History

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-interface-v08.pdf

Repository path repo.tas3.eu:/var/lib/tas3repo/arch/tas3-user-interface.pdf (1.23)
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-v08.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.