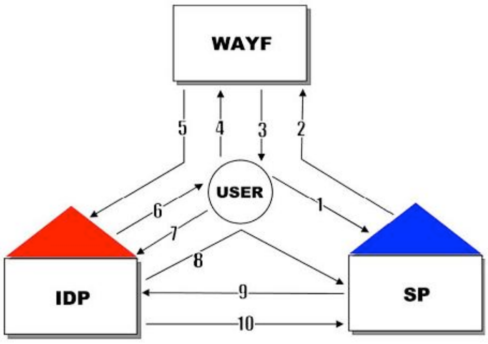
Shintau Demonstration
User Guide

Background

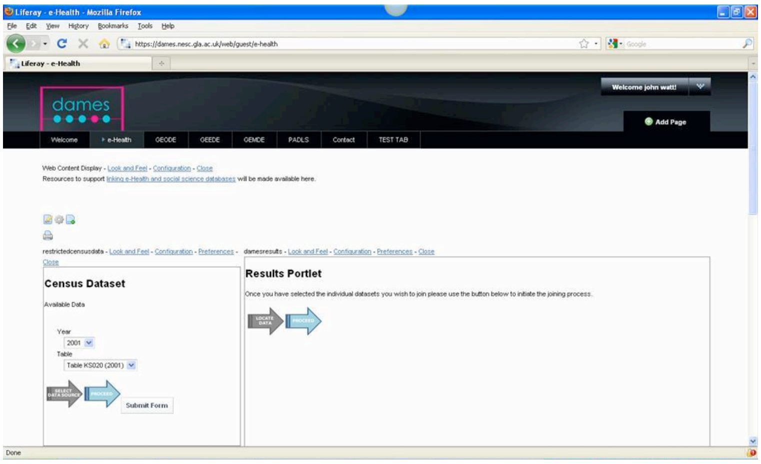
The Shibboleth software implements federated authentication, which means that a user's credentials at their local institution may be trusted as a source of authentication for external, non-local services. This allows a user to only need one credential to access a variety of services, plus movement between these services will not require any further logins (single sign-on). Shibboleth defines a group of trusting services as a *federation*, and defines various entities within this grouping, the most important of which here is the Identity Provider (IdP), which is a source of user information within a federation. The other entities are the Where-Are-You-From (WAYF) service, which allows a user to select their home institution in the federation, and the Service Provider (SP) which protects the web resource (web page/portal). The flow of user interaction is shown below.



A trusted institution can reliably assert the identities of its users through an institutional IdP, however services usually require extra information (roles, attributes or licences) to grant access to specific parts of services. Often this information is not provided by the primary IdP, so some mechanism of remote authorisation information extraction is needed. With the standard Shibboleth software, there exists no easy way of merging remote information with the authentication assertion. One way is to collect all the attributes at the IdP first – but this approach requires continuous configuration changes to the IdP software, and is in general not supported by institutions. Another approach is to have the service itself contact extra IdPs to extract the information they need, but this would be impossible without user interaction.

The Shintau project provides software which allows a user to merge information about themselves from multiple IdP using a Linking Service. A user will log into the Linking Service, select which IdPs will be required to access a specific service, and save this information at the Linking Service. Any subsequent visits to the service will now only require logging in at the primary IdP, and the Linking Service will contact the other IdPs for the rest of the attributes.

Demonstration Scenario



Web Content Display - Look and Feel - Configuration - Close

Resources to support linking e-Health and social science databases will be made available here.

restrictedcensusdata - Look and Feel - Configuration - Preferences - Close

damesresults - Look and Feel - Configuration - Preferences - Close

Census Dataset

Available Data

Year: 2001

Table: Table KS020 (2001)

Results Portlet

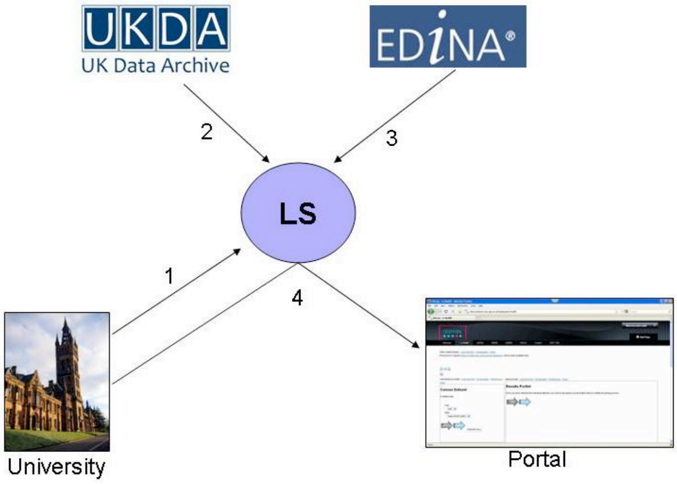
Once you have selected the individual datasets you wish to join please use the button below to initiate the joining process.

The Shintau demonstration shows how access to a social science data portal (like the one above) which requires licenses from the UK Data Archive and EDINA UK Borders can be achieved with only a single University login through a prepared Linking Service.

All users of the Shintau demonstration are registered in the fictional Shintau University, which has its own IdP which is used as the primary authentication source. Like a real-life institutional IdP, it is hooked up to the staff/student registry and provides authentic, accountable logins for all of its users.

When requesting access to real UKDA data sets, users visit their web site and register for an account. The user then goes through the list of data sets they provide and selects which ones they require a license for. These licenses allow the user to download data sets from various UK DA web sites upon providing the correct registration username/password. For the Shintau demonstration, we have created a Shintau-enabled IdP for the UK DA, which will assert the licenses the user has signed up for when requested by the portal.

EDINA, which provides the UK Borders data sets, has a similar registration procedure, and we have set up a Shintau IdP for their licences also.



To recap, we have three distinct IdPs, the University, the UKDA and EDINA. Without some way to link the information these entities provide, it would be necessary to login to each of the three IdPs every time we wish to access the portal. Using Shintau, we are going to show how this only needs to be done once with a Linking Service. Once this is set up for the portal service, subsequent visits to the portal will only require logging in to the primary IdP (the University), and Shintau will collect the rest of the attributes/licences on your behalf from your specified IdPs.

Operation

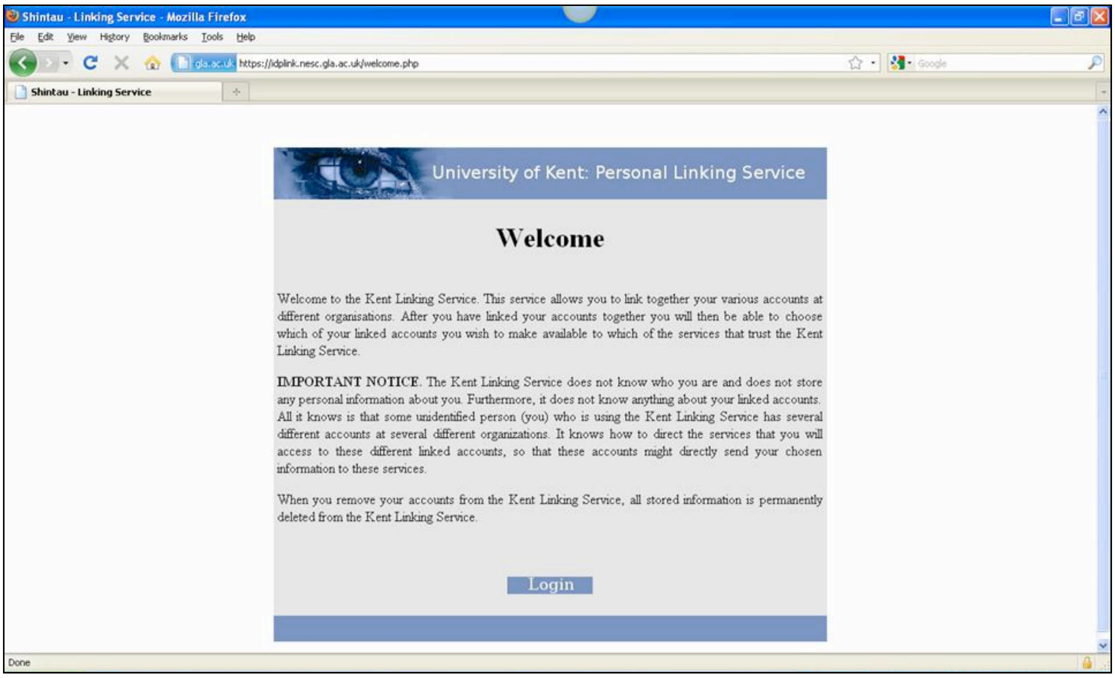
It is a good idea to save a couple of URLs as "Favourites" in your browser. This will mean less typing when moving between services:

https://idplink.nesc.gla.ac.uk - The Shintau Linking Service
http://terra.nesc.gla.ac.uk/shintau - The Shintau Portal Gateway

Also remember that, depending on your browser set up, Shibboleth may retain session information while your browser is open. To clear any session info, simply close all your browser windows.

You will have been emailed login credentials for use with this demonstration. For ease of use, your username and password are the same at the University of Shintau, the UKDA and EDINA. Note this will almost certainly not be the case in real life!

The first step is to set up the Linking Service for the portal…


Shintau - Linking Service - Mozilla Firefox
File Edit View History Bookmarks Tools Help
gla.ac.uk https://idplink.nesc.gla.ac.uk/welcome.php
Google
Shintau - Linking Service
Done

University of Kent: Personal Linking Service

Welcome

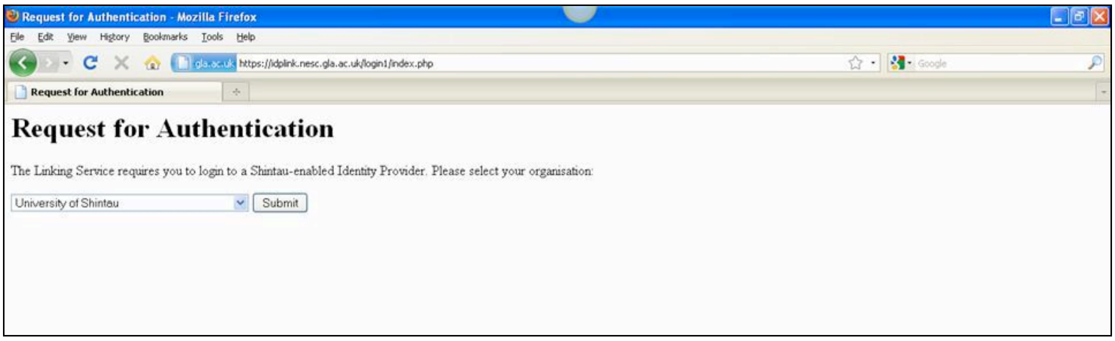
Welcome to the Kent Linking Service. This service allows you to link together your various accounts at different organisations. After you have linked your accounts together you will then be able to choose which of your linked accounts you wish to make available to which of the services that trust the Kent Linking Service.

IMPORTANT NOTICE. The Kent Linking Service does not know who you are and does not store any personal information about you. Furthermore, it does not know anything about your linked accounts. All it knows is that some unidentified person (you) who is using the Kent Linking Service has several different accounts at several different organizations. It knows how to direct the services that you will access to these different linked accounts, so that these accounts might directly send your chosen information to these services.

When you remove your accounts from the Kent Linking Service, all stored information is permanently deleted from the Kent Linking Service.

Figure 1: The Shintau Linking Service Welcome screen

Open a browser and point it at the Shintau Linking Service (URL saved above). You will see a Welcome screen with some explanatory text and a “Login” button (Figure 1). Click the Login button and you will be directed to the “Authentication Request” screen (This screen mimics the Where-Are-You-From (WAYF) service in use by national federations like the UK Access Management Federation). We are going to use the University login to authenticate to the Linking Service, so select “University of Shintau” IdP from the drop-down list (Figure 2).


Request for Authentication - Mozilla Firefox
File Edit View History Bookmarks Tools Help
gla.ac.uk https://idplink.nesc.gla.ac.uk/login1/index.php
Google
Request for Authentication

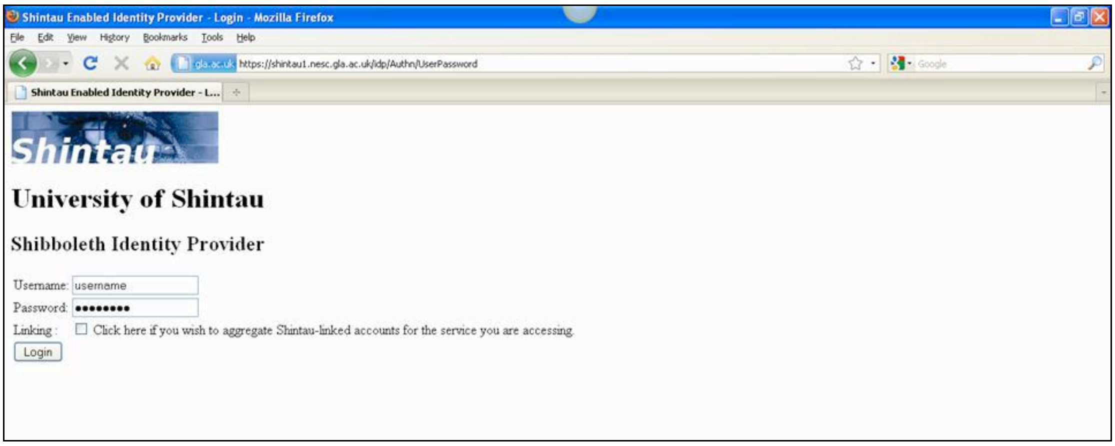
Request for Authentication

The Linking Service requires you to login to a Shintau-enabled Identity Provider. Please select your organisation:

University of Shintau

Figure 2: IdP selection screen

Shibboleth will then forward you to the University IdP, where you should enter your username and password to log in (Figure 3). Note that you shouldn’t click the attribute aggregation checkbox just yet, this is used after the Linking Service has been setup to tell the portal to merge the remote licences.


Shintau Enabled Identity Provider - Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://shintau1.nesc.gla.ac.uk/idp/Authn/UserPassword
Shintau

University of Shintau

Shibboleth Identity Provider

Username: username

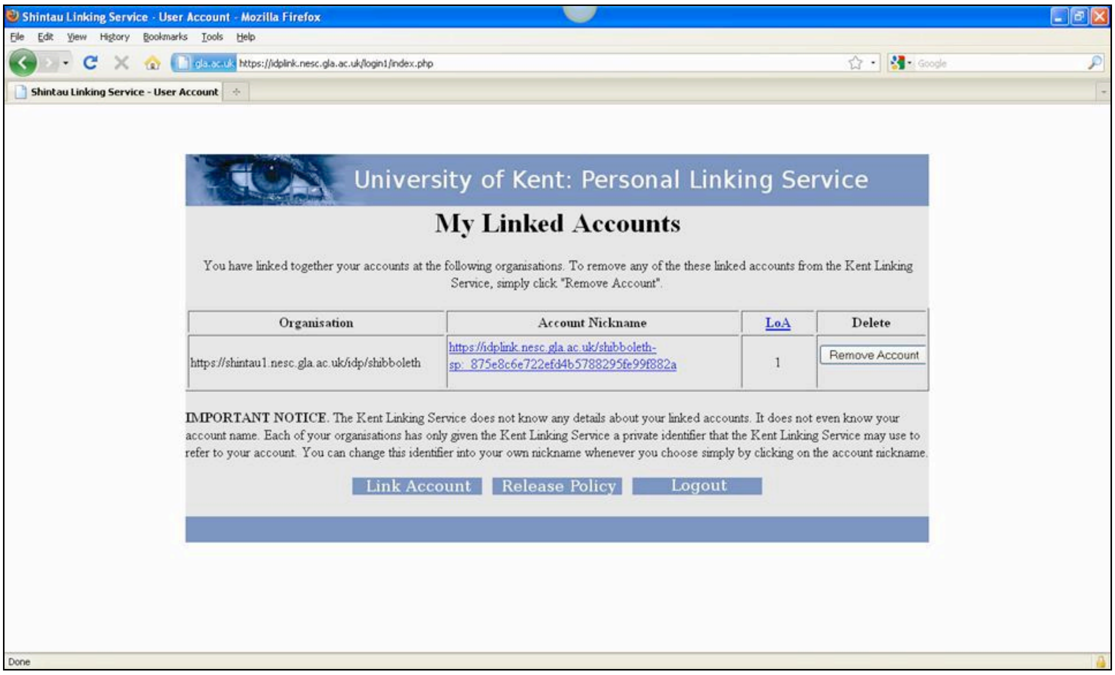
Password: ●●●●●●●●

Linking : □ Click here if you wish to aggregate Shintau-linked accounts for the service you are accessing.

Login

Figure 3: Authenticating at the University of Shintau IdP

You should now be back at the Linking Service, and you should have one entry in the Linked account list (Figure 4). This means that the University IdP you just signed into can be linked with any other accounts now.


Shintau Linking Service - User Account - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://idplink.nesc.gla.ac.uk/login1/index.php
Done

University of Kent: Personal Linking Service

My Linked Accounts

You have linked together your accounts at the following organisations. To remove any of the these linked accounts from the Kent Linking Service, simply click "Remove Account".

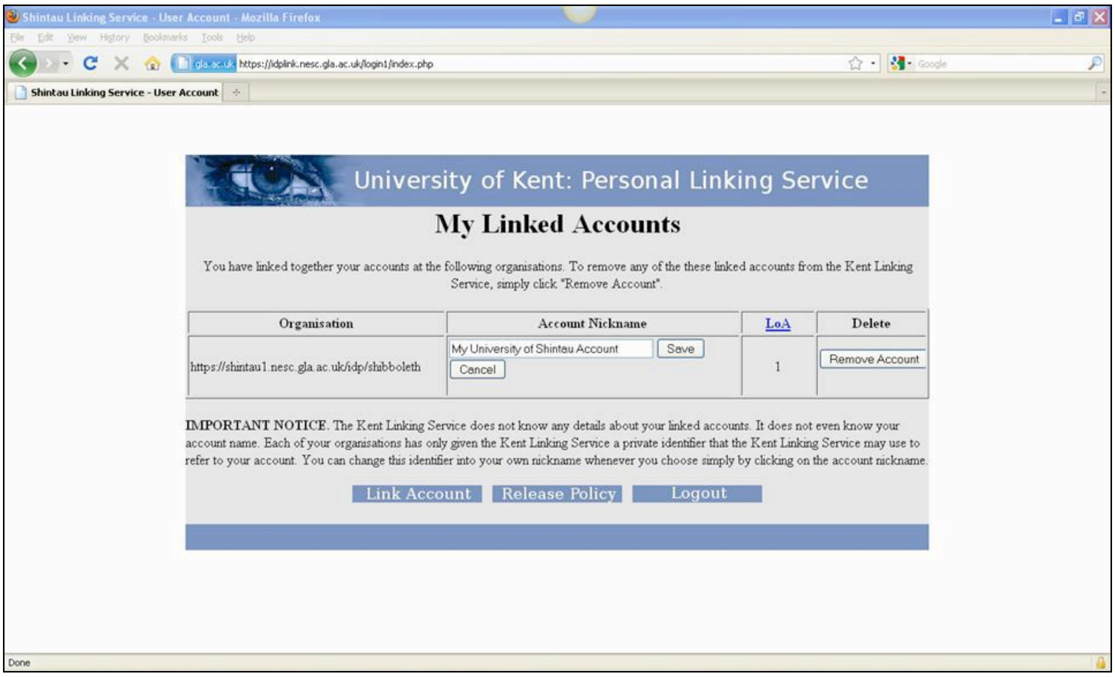
Organisation	Account Nickname	LoA	Delete
https://shintau1.nesc.gla.ac.uk/idp/shibboleth	https://idplink.nesc.gla.ac.uk/shibboleth-sp: 875e8c6e722efd4b5788295fe99f882a	1	Remove Account

IMPORTANT NOTICE. The Kent Linking Service does not know any details about your linked accounts. It does not even know your account name. Each of your organisations has only given the Kent Linking Service a private identifier that the Kent Linking Service may use to refer to your account. You can change this identifier into your own nickname whenever you choose simply by clicking on the account nickname.

Link Account Release Policy Logout

Figure 4: First account is now registered in the Linking Service

The personal identifier field has a strange looking string in it which Shintau uses to anonymously identify you, but you can provide a nickname for it to keep track of the accounts you want to link. Click on the string and change it to "University of Shintau" or something similar, then click "Save" (Figure 5).


Shintau Linking Service - User Account - Mozilla Firefox
File Edit View History Bookmarks Tools Help
gla.ac.uk https://idplink.nesc.gla.ac.uk/login1/index.php
Google
Shintau Linking Service - User Account
Done

University of Kent: Personal Linking Service

My Linked Accounts

You have linked together your accounts at the following organisations. To remove any of the these linked accounts from the Kent Linking Service, simply click "Remove Account".

Organisation	Account Nickname	LoA	Delete
https://shintau1.nesc.gla.ac.uk/idp/shibboleth	My University of Shintau Account Save Cancel	1	Remove Account

IMPORTANT NOTICE. The Kent Linking Service does not know any details about your linked accounts. It does not even know your account name. Each of your organisations has only given the Kent Linking Service a private identifier that the Kent Linking Service may use to refer to your account. You can change this identifier into your own nickname whenever you choose simply by clicking on the account nickname.

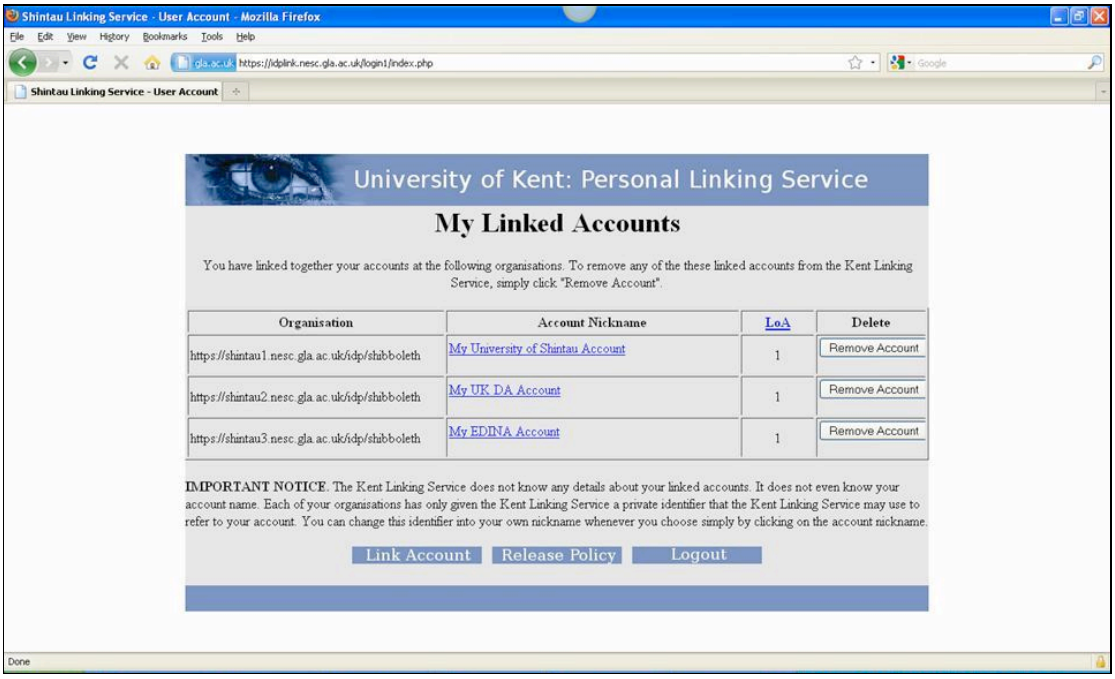
Link Account | Release Policy | Logout

Figure 5: Changing the account identifier to a recognisable nickname

We now want to get the UKDA and EDINA accounts in this list, so click on "Link Account" at the bottom of the screen, and you should find yourself back at the "Authentication Request" screen. We now want to link your UKDA account, so select that from the drop-down list and hit 'Select'. You will now be forwarded to the UKDA IdP, where you should supply your credentials. After authentication, you will be back at the Linking Service, and your UKDA account will now be present in the Linked Account list. Supply the nickname "UK Data Archive" in the same way as before and 'Save'.

Link the EDINA account to the Linking Service following the guide above, and supply a nickname (e.g. EDINA).

You should now have three accounts registered in your Linking Service (Figure 6). We will now do the final mapping of accounts to the portal service so we can test the Shintau aggregation.


Shintau Linking Service - User Account - Mozilla Firefox
File Edit View History Bookmarks Tools Help
gla.ac.uk https://idplink.nesc.gla.ac.uk/login1/index.php
Google
Shintau Linking Service - User Account
Done

University of Kent: Personal Linking Service

My Linked Accounts

You have linked together your accounts at the following organisations. To remove any of the these linked accounts from the Kent Linking Service, simply click "Remove Account".

Organisation	Account Nickname	LoA	Delete
https://shintau1.nesc.gla.ac.uk/idp/shibboleth	My University of Shintau Account	1	Remove Account
https://shintau2.nesc.gla.ac.uk/idp/shibboleth	My UK DA Account	1	Remove Account
https://shintau3.nesc.gla.ac.uk/idp/shibboleth	My EDINA Account	1	Remove Account

IMPORTANT NOTICE. The Kent Linking Service does not know any details about your linked accounts. It does not even know your account name. Each of your organisations has only given the Kent Linking Service a private identifier that the Kent Linking Service may use to refer to your account. You can change this identifier into your own nickname whenever you choose simply by clicking on the account nickname.

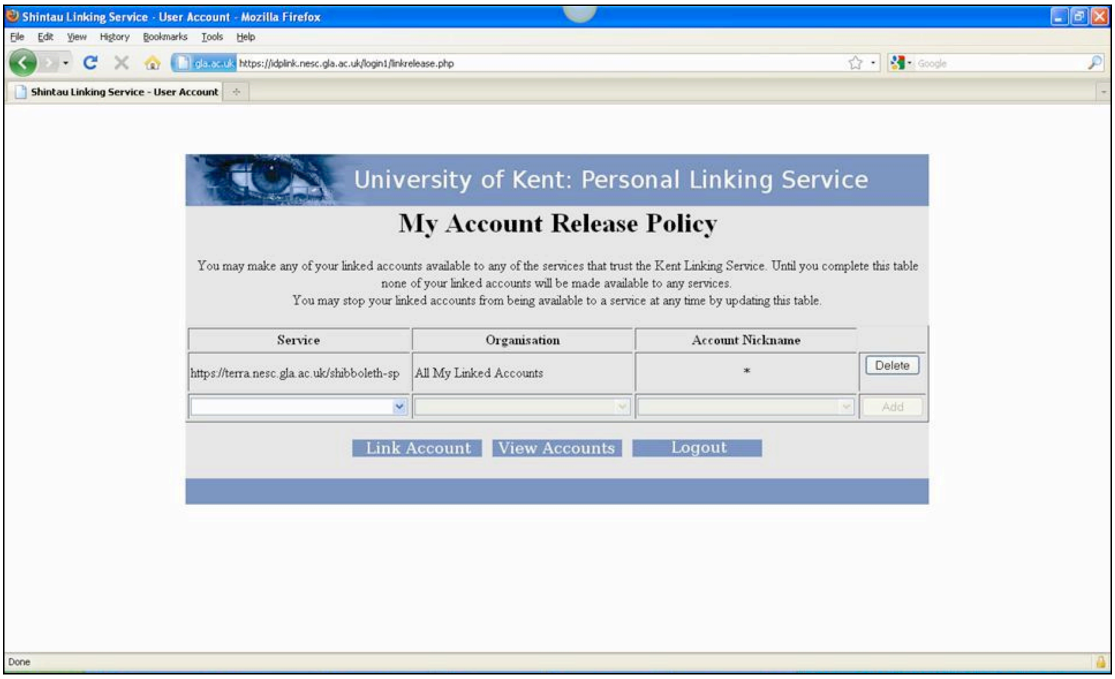
Figure 6: All IdPs now registered with Linking Service

Click on "Release Policy" at the bottom of the screen. A new Linking Service page appears, where the accounts you have registered may be associated with a particular service. Click on the "Service" drop down box, you will notice a massive list of Shibboleth Service Providers (these are the current TestShib SPs). Our social science portal is hosted on terra.nesc.gla.ac.uk, so search the menu for:

https://terra.nesc.gla.ac.uk/shibboleth-sp

and select it.

We will now associate your registered accounts with this service. Click the "Organisation" drop-down box. In our case, we need authentication and licenses from the university, UKDA and EDINA, so select "All Linked Accounts". You don't need to bother with a nickname here. Once all accounts are associated with the portal location, click "Add" (Figure 7).



Shintau Linking Service - User Account - Mozilla Firefox
File Edit View History Bookmarks Tools Help
gla.ac.uk https://idplink.nesc.gla.ac.uk/login1/linkrelease.php
Google
Shintau Linking Service - User Account
Done

University of Kent: Personal Linking Service

My Account Release Policy

You may make any of your linked accounts available to any of the services that trust the Kent Linking Service. Until you complete this table none of your linked accounts will be made available to any services.
You may stop your linked accounts from being available to a service at any time by updating this table.

Service	Organisation	Account Nickname	
https://terra.nesc.gla.ac.uk/shibboleth-sp	All My Linked Accounts	*	Delete
			Add

Figure 7: Associate all linked accounts with the Portal Gateway service

You have now setup Shintau aggregation on the portal! Any attempts to access this portal through Shintau will only require you to login using the University credential, and the Linking Service will grab the UKDA and EDINA licenses for you, as you have requested. Click the ‘Logout’ button at the foot of the page. Then close your browser windows.

We can demonstrate how simply logging in to the portal using the University credential WITHOUT Shintau will result in you being refused access. Open a browser and visit the Shintau Portal Gateway. You will be forwarded automatically to the University IdP. Supply your credentials to the portal and click the button, noting that the Shintau checkbox is not selected. Upon logging in you will be forwarded to an error page, which means you haven’t supplied the necessary licences (UKDA and EDINA) to gain access. Close this window now.

To successfully log in to the portal gateway, follow the steps outlined in the previous paragraph, but this time make sure the aggregation checkbox is selected. When you login, you will notice a larger time delay (around 5 seconds) while your licenses are extracted from UKDA and EDINA by the Linking Service. You should then be forwarded to the Gateway page, which confirms you have supplied the correct licenses before providing a link to the portal (in this case the DAMES project portal).