Attribute Aggregation in Federated Identity Management

David Chadwick, **George Inman,** Stijn Lievens
University of Kent

Acknowledgements

- Project originally funded by UK JISC, called Shintau
  - http://sec.cs.kent.ac.uk/shintau/
- Now continuing to be funded under EC TAS3 project (will be doing a CardSpace integration next)

Contents

- What is Attribute Aggregation?
- Demo
- The technical bits

Attribute Aggregation

- Users typically have lots of different attributes from different providers
- User is usually known by different IDs at the different IdPs/AAs
- Only the user knows what these IDs are
- User might wish to benefit from using these multiple attributes at an SP, but how will SP know that all these different IDs belong to the same real worldperson?

E.g. Use IEEE membership and credit card when purchasing a book

Using the LS for Aggregation

1. User connects to Linking Service Home Page
2. User is given confidence his privacy will be protected
3. User is invited to Login
4. User is then invited to select his IdP for authentication
5. User is redirected to his chosen IdP to login
6. User logs in and is redirected back to Linking Service where his linked accounts are displayed
7. Optionally the user sets a user friendly nickname for the account (otherwise the PID is used)

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.

Login


University of Kent: Personal Linking Service
Account Login
The Kent Linking Service requires you to login to one of your organisation accounts before proceeding.
Please select one of your organizations from the list below.
issrg-identity-1
Submit


University of Kent: Personal Linking Service
Account Login
The Kent Linking Service requires you to login to one of your organisation accounts before proceeding.
Please select one of your organizations from the list below.
issrg-identity-2
issrg-identity-1
issrg-identity-2
issrg-identity-3
issrg-identity-4

issrg-identity.cs.kent.ac.uk - LoA 2

Username: User0

Password: •••••

☐ Do you wish to aggregate attributes from other linked accounts

Login

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://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth	https://129.12.41.112/shibboleth-sp:_6f092289ee09bbd1fcedfb08118ecec4	2	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

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://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth	User0 - idp 2 Save Cancel	2	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

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".

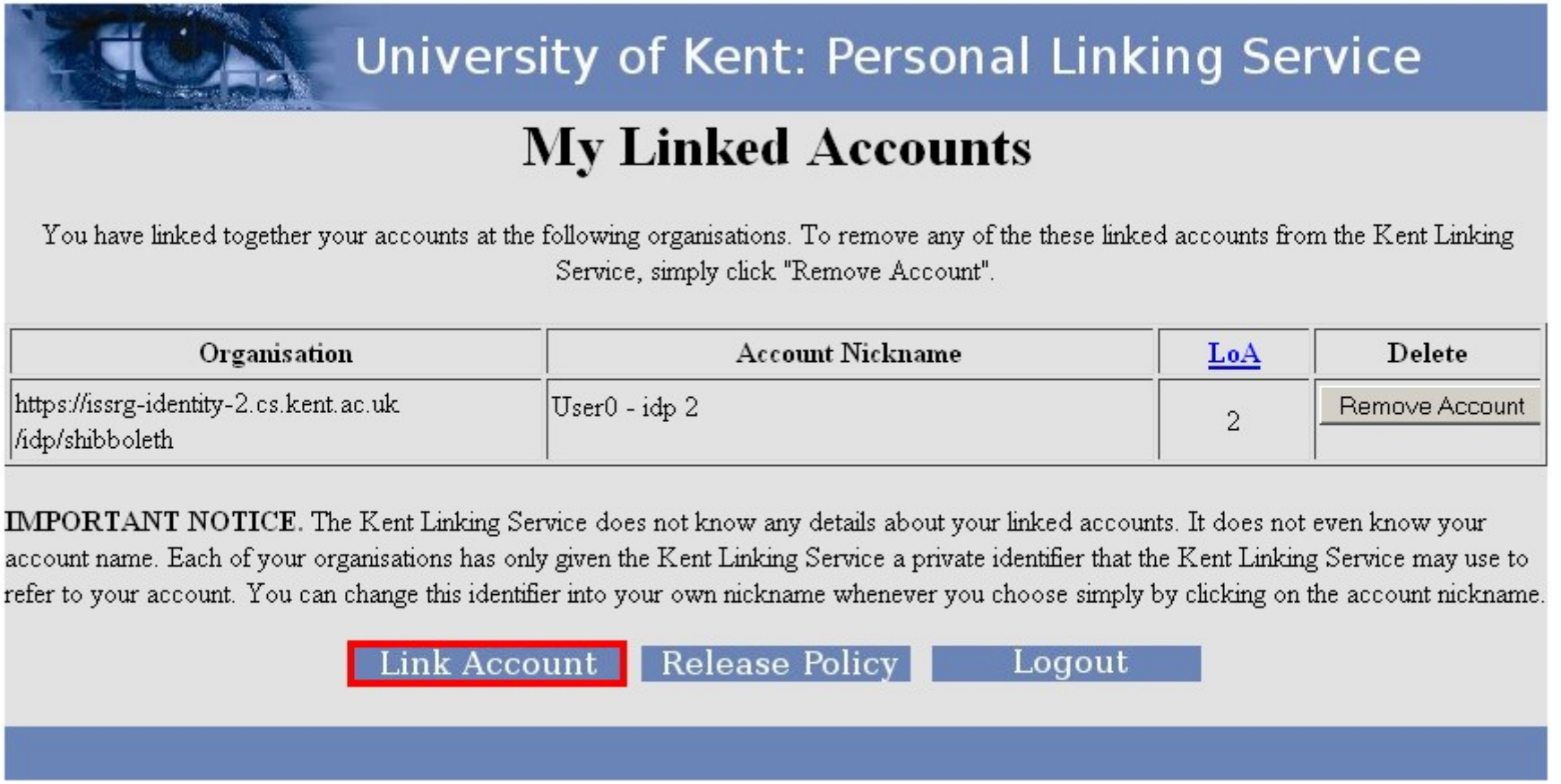
Organisation	Account Nickname	LoA	Delete
https://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth	User0 - idp 2	2	Remove Account

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

Adding New Linked Accounts

1. The user selects the Link Account button and is taken back to the Login page
2. The user chooses a different IdP this time around and is redirected there
3. The user is shown the IdP's login page and authenticates
4. The user is redirected back the Linking Services Linked Accounts page, and starts this whole process again
5. The next screen shows 2 linked accounts, at different IdPs


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://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth
User0 - idp 2
2
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


University of Kent: Personal Linking Service
Account Login
The Kent Linking Service requires you to login to one of your organisation accounts before proceeding.
Please select one of your organizations from the list below.
issrg-identity-1
issrg-identity-1
issrg-identity-2
issrg-identity-3
issrg-identity-4

issrg-identity-3.cs.kent.ac.uk - LoA 3

Username: User0

Password: •••••

Do you wish to aggregate attributes from other linked accounts

Login

University of Kent: Personal Linking Service

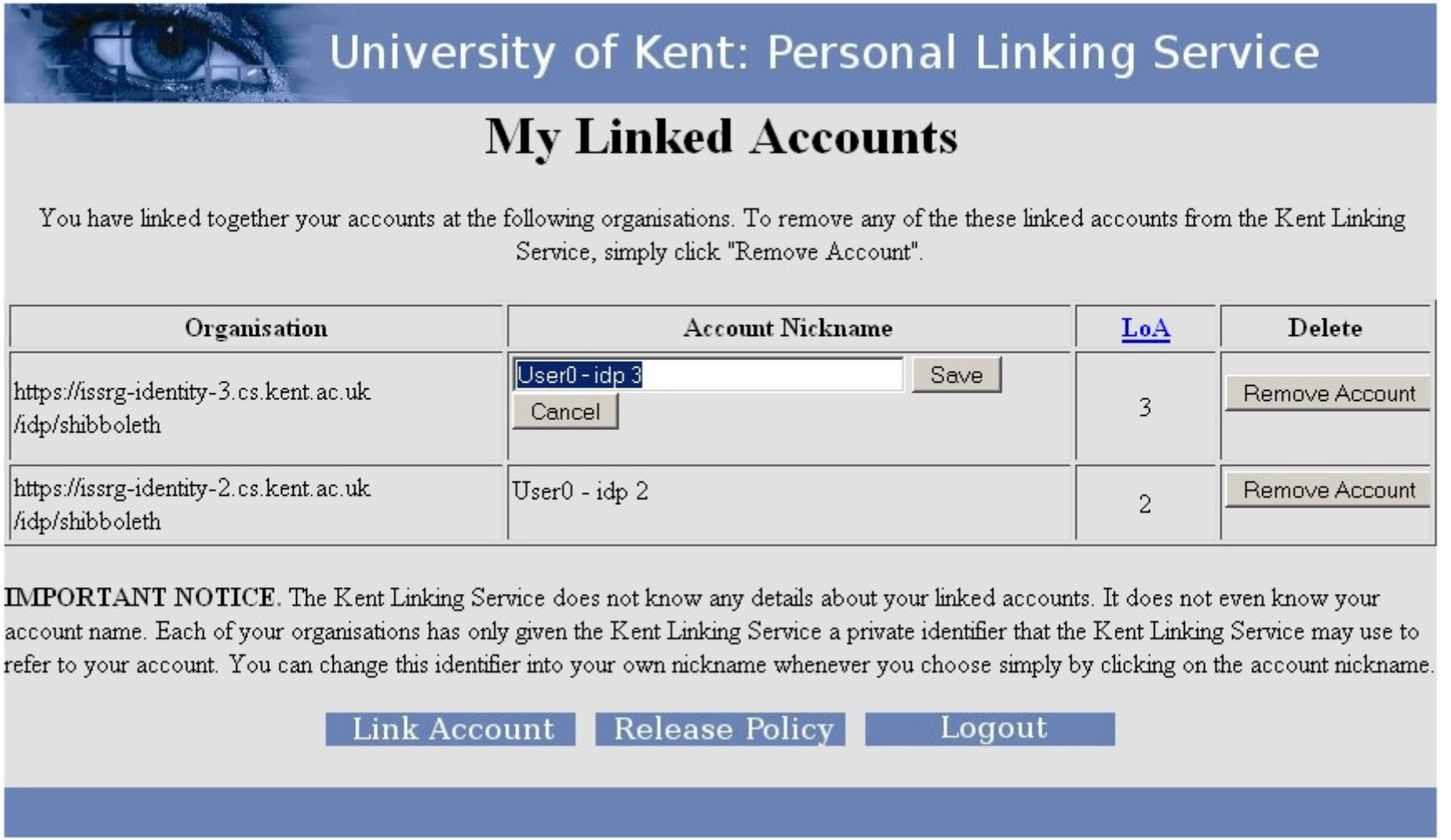
My Linked Accounts

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://issrg-identity-3.cs.kent.ac.uk /idp/shibboleth	https://129.12.41.112/shibboleth-sp:_d6c9c3865e2e5640ea6ec63a9af1cc85	3	Remove Account
https://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth	User0 - idp 2	2	Remove Account

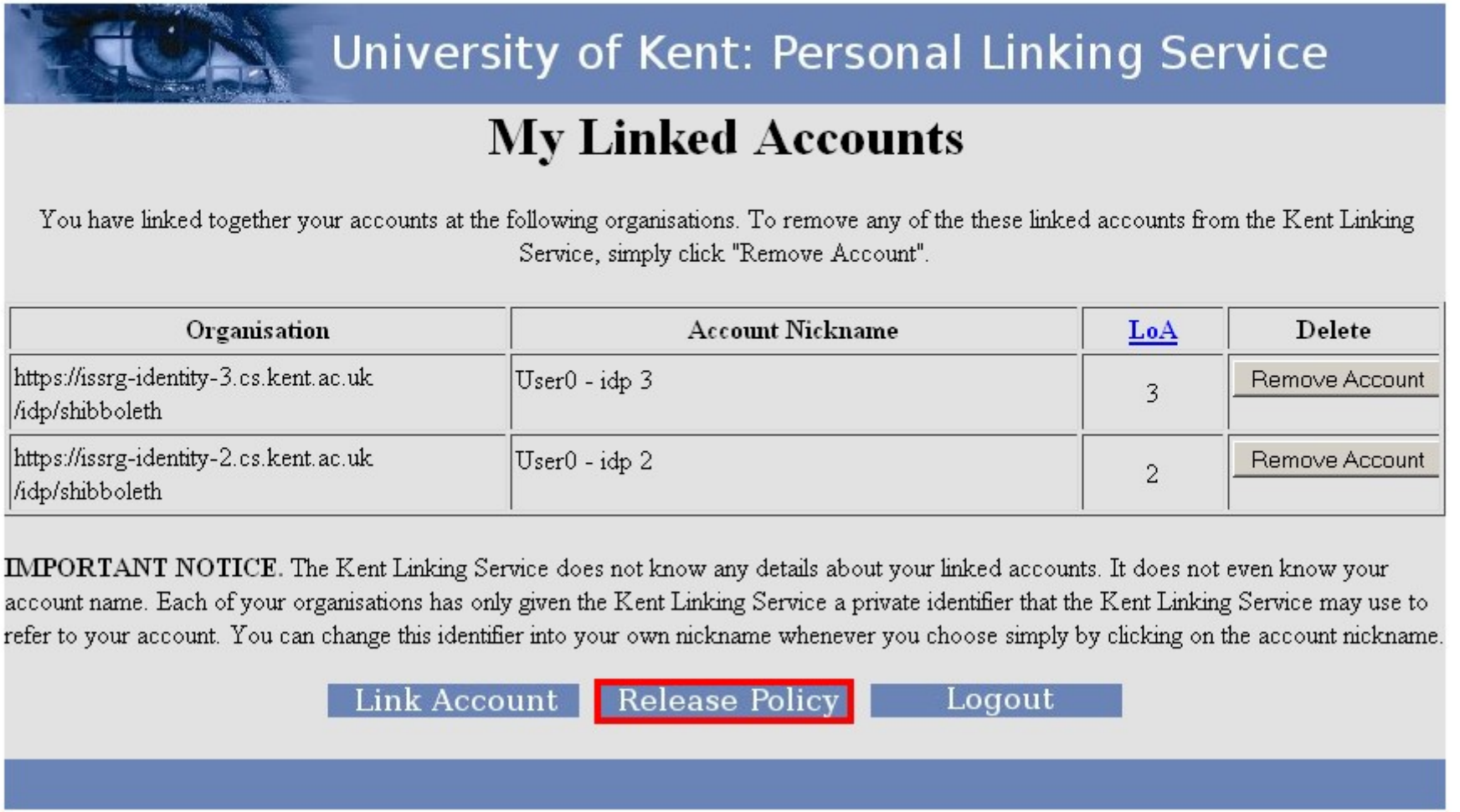
IMPORTANT NOTICE. The Kent Linking Service does not know any details about your linked accounts. It does not even know your account name. Each of your organisations has only given the Kent Linking Service a private identifier that the Kent Linking Service may use to refer to your account. You can change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

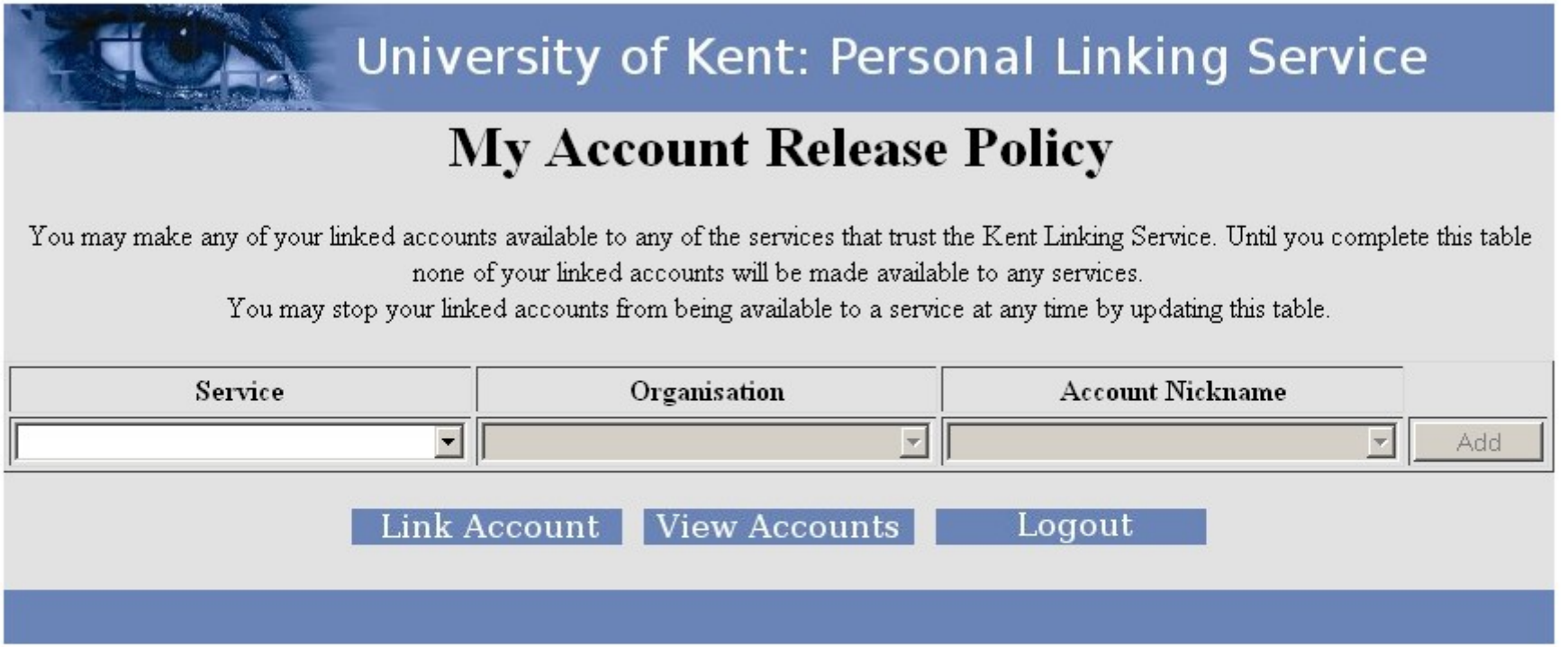
Link Account | Release Policy | Logout

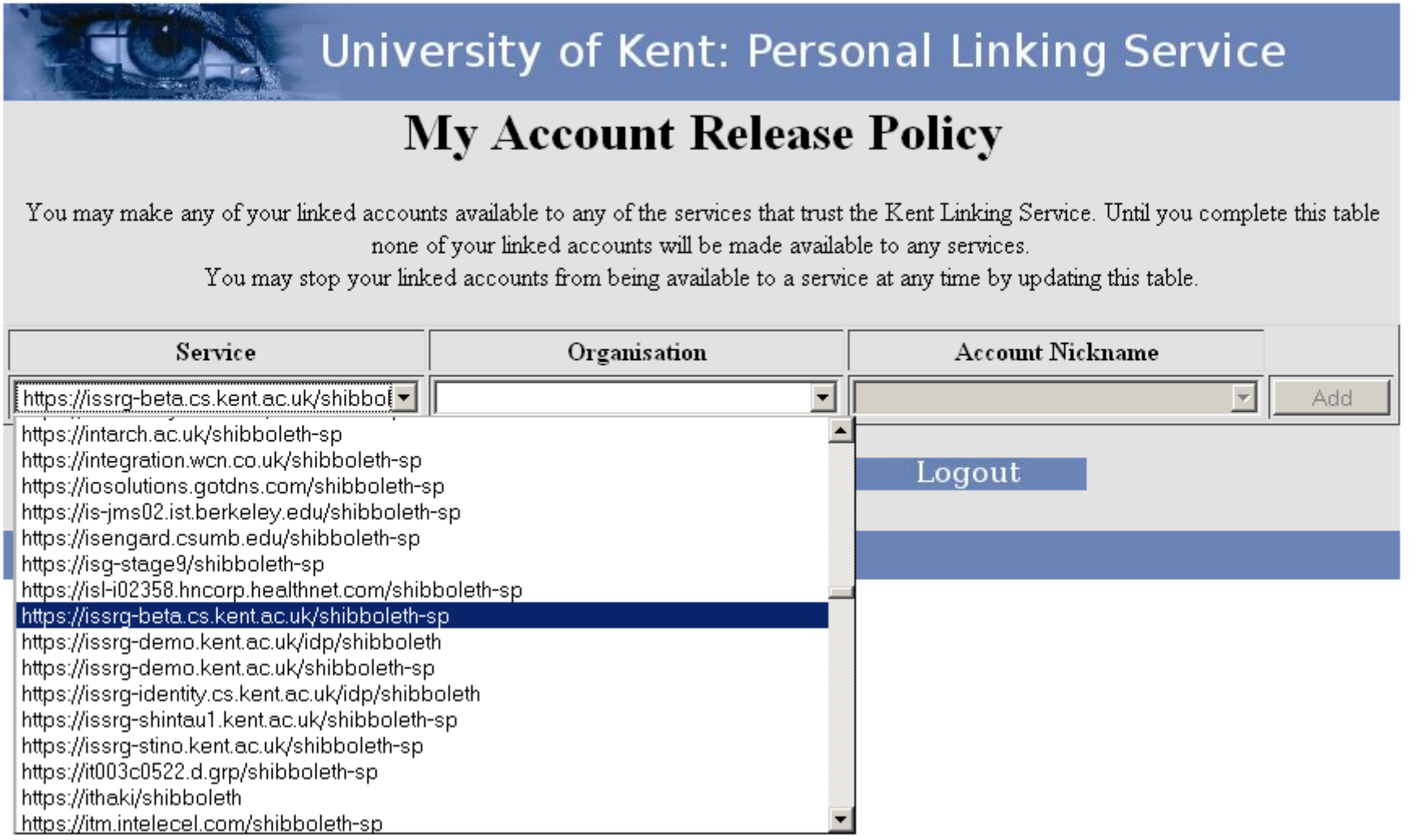

University of Kent: Personal Linking Service
My Linked Accounts
You have linked together your accounts at the following organisations. To remove any of the these linked accounts from the Kent Linking Service, simply click "Remove Account".
Organisation
Account Nickname
LoA
Delete
https://issrg-identity-3.cs.kent.ac.uk /idp/shibboleth
User0 - idp 3
Save
Cancel
3
Remove Account
https://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth
User0 - idp 2
2
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

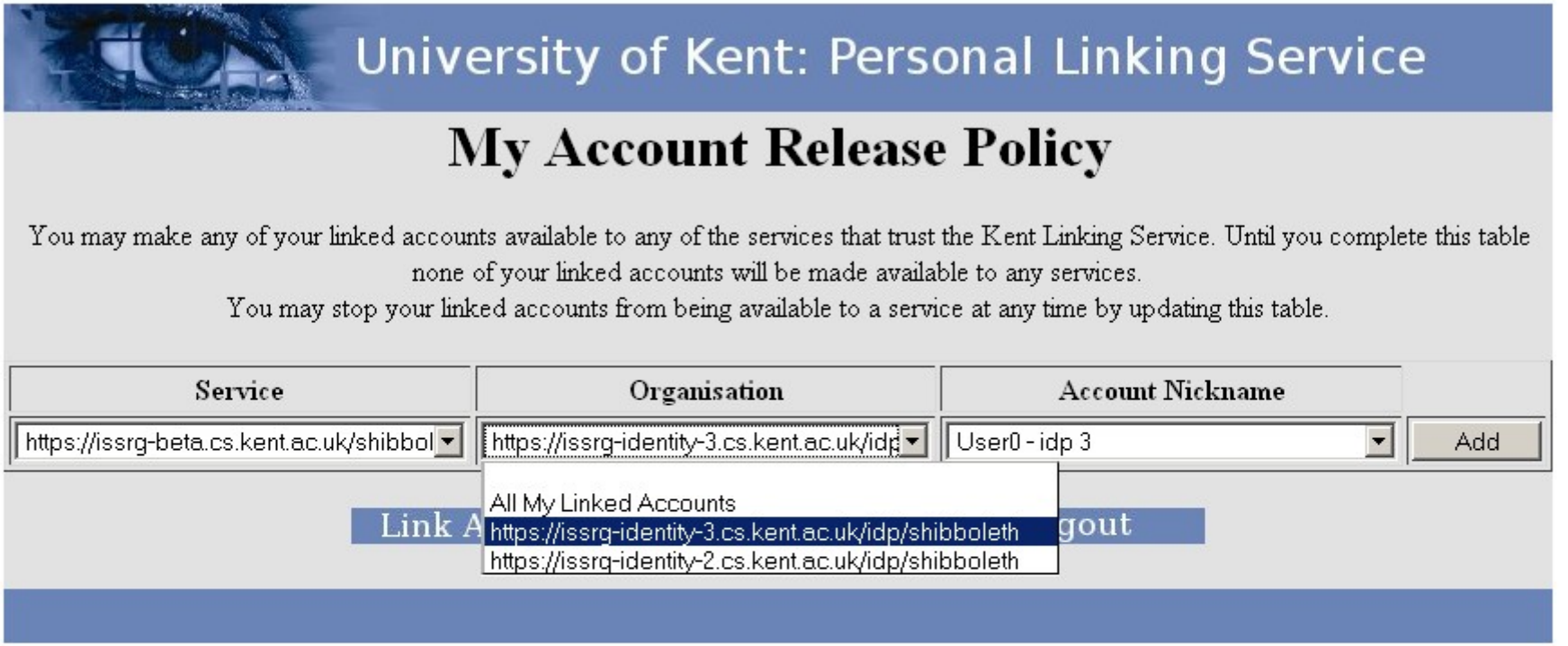
Setting up the Link Release Policy

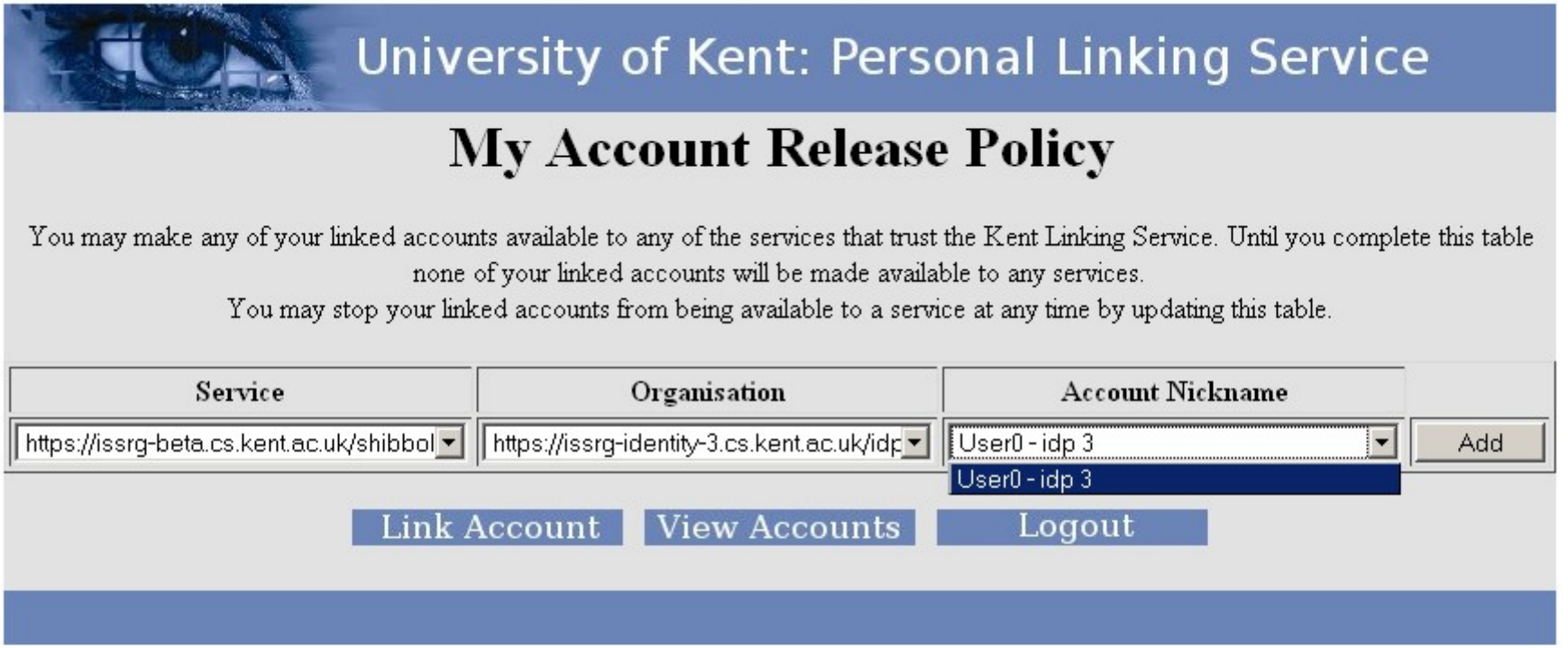
1. The user selects the Release Policy button and is taken to the Link Release Policy screen.
2. The user chooses the service provider who is to receive the attributes from the linked accounts
3. The user chooses the IdPs whose attributes are to be sent to the SP
4. The user chooses the nickname to use (only applicable if the user has 2 or more accounts at the same IdP)
5. The user clicks on Add, which creates the policy rule
6. The user repeats the whole process for each SP that is to receive a linked account

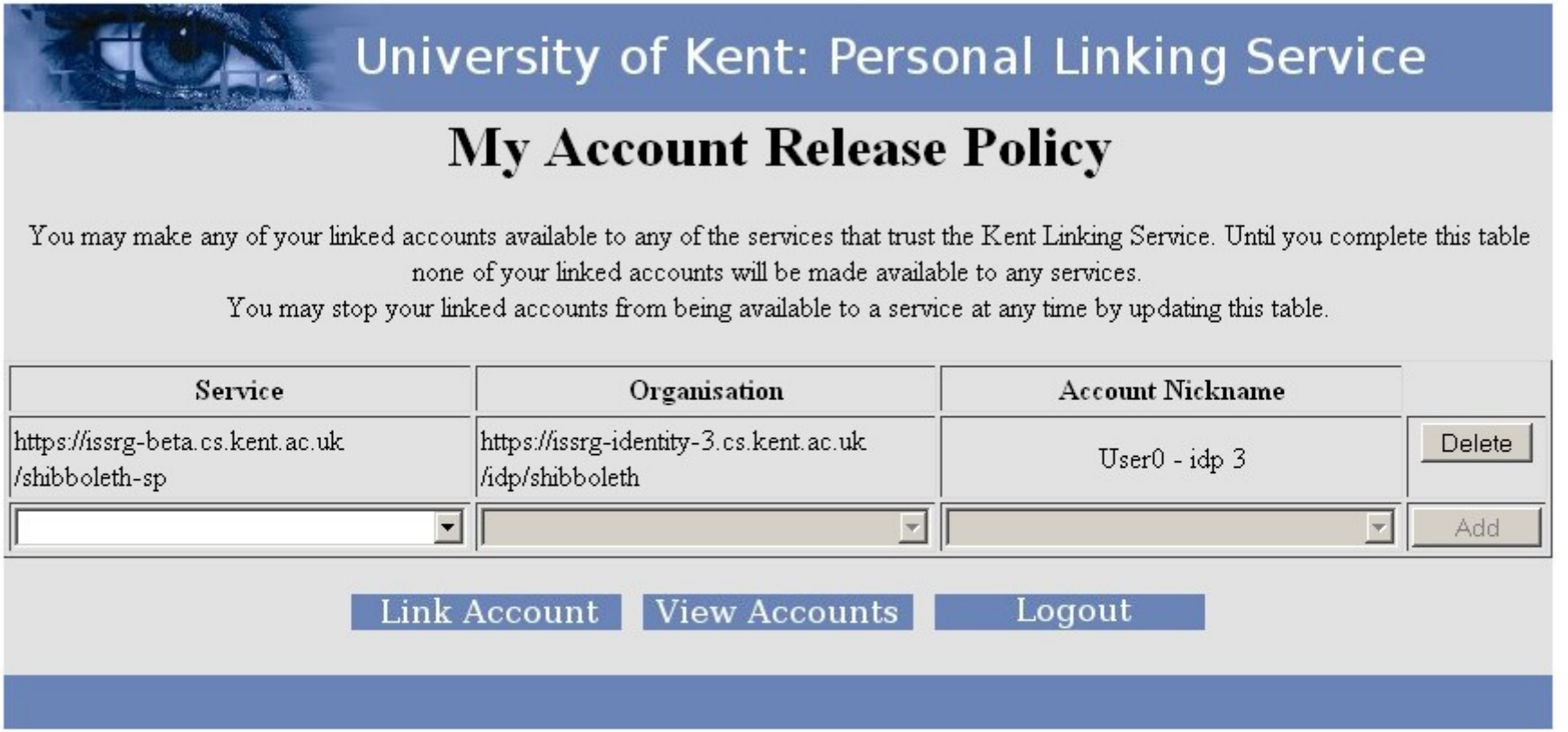

University of Kent: Personal Linking Service
My Linked Accounts
You have linked together your accounts at the following organisations. To remove any of the these linked accounts from the Kent Linking Service, simply click "Remove Account".
Organisation
Account Nickname
LoA
Delete
https://issrg-identity-3.cs.kent.ac.uk /idp/shibboleth
User0 - idp 3
3
Remove Account
https://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth
User0 - idp 2
2
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

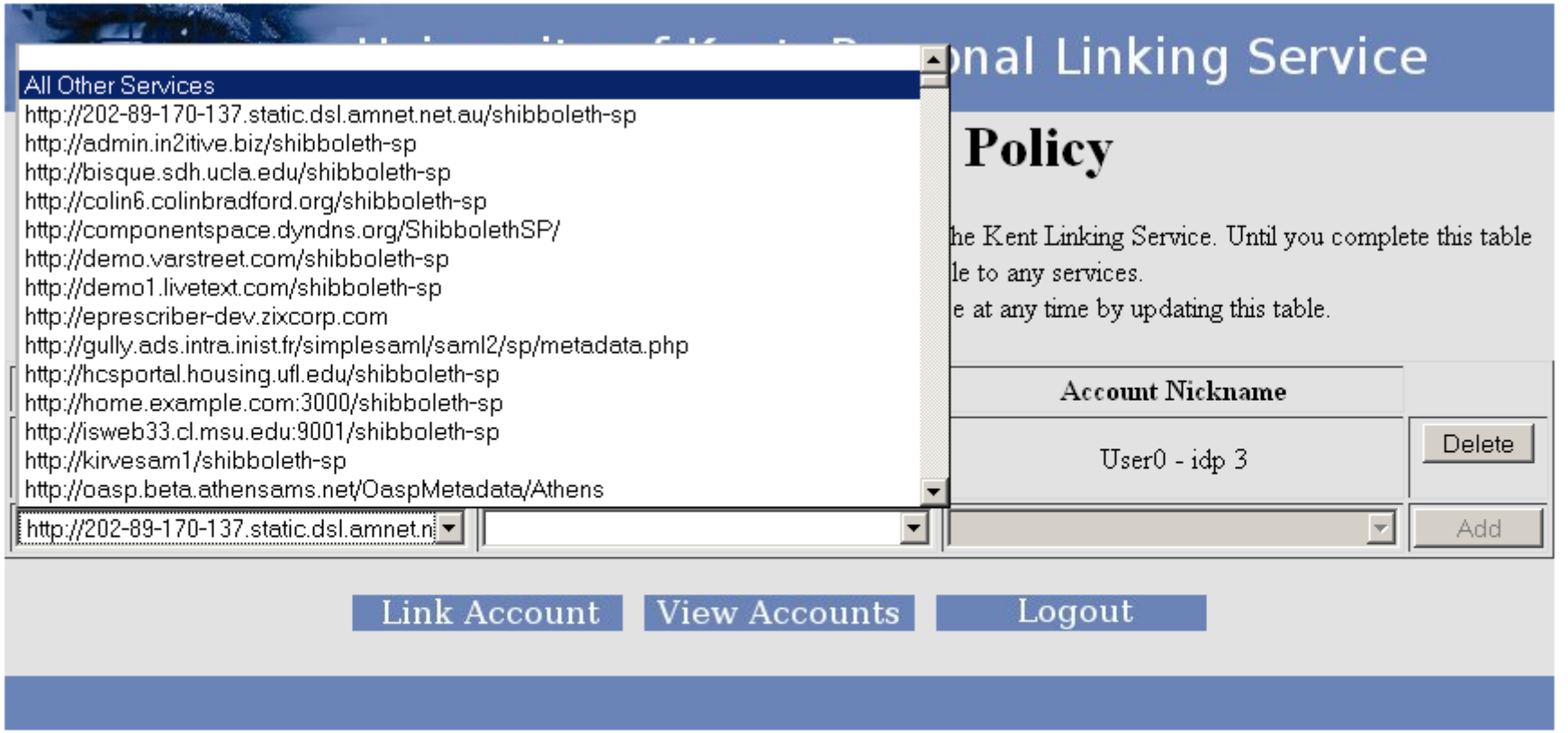

University of Kent: Personal Linking Service
My Account Release Policy
You may make any of your linked accounts available to any of the services that trust the Kent Linking Service. Until you complete this table none of your linked accounts will be made available to any services.
You may stop your linked accounts from being available to a service at any time by updating this table.
Service
Organisation
Account Nickname
Add
Link Account
View Accounts
Logout

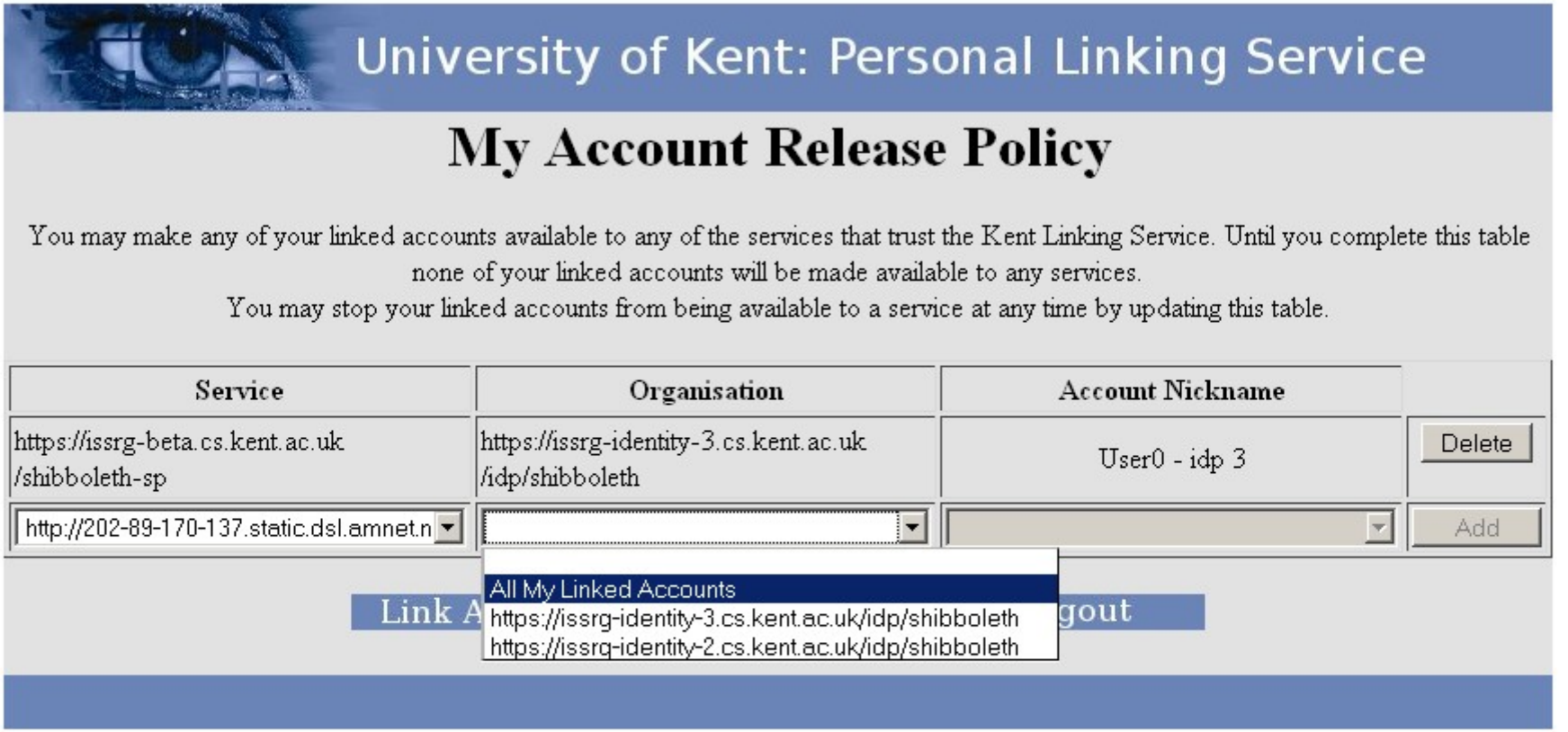

University of Kent: Personal Linking Service
My Account Release Policy
You may make any of your linked accounts available to any of the services that trust the Kent Linking Service. Until you complete this table none of your linked accounts will be made available to any services.
You may stop your linked accounts from being available to a service at any time by updating this table.
Service
Organisation
Account Nickname
https://issrg-beta.cs.kent.ac.uk/shibbol
Add
https://intarch.ac.uk/shibboleth-sp
https://integration.wcn.co.uk/shibboleth-sp
https://iosolutions.gotdns.com/shibboleth-sp
https://is-jms02.ist.berkeley.edu/shibboleth-sp
https://isengard.csumb.edu/shibboleth-sp
https://isg-stage9/shibboleth-sp
https://isl-i02358.hncorp.healthnet.com/shibboleth-sp
https://issrg-beta.cs.kent.ac.uk/shibboleth-sp
https://issrg-demo.kent.ac.uk/idp/shibboleth
https://issrg-demo.kent.ac.uk/shibboleth-sp
https://issrg-identity.cs.kent.ac.uk/idp/shibboleth
https://issrg-shintau1.kent.ac.uk/shibboleth-sp
https://issrg-stino.kent.ac.uk/shibboleth-sp
https://it003c0522.d.grp/shibboleth-sp
https://ithaki/shibboleth
https://itm.intelecel.com/shibboleth-sp
Logout

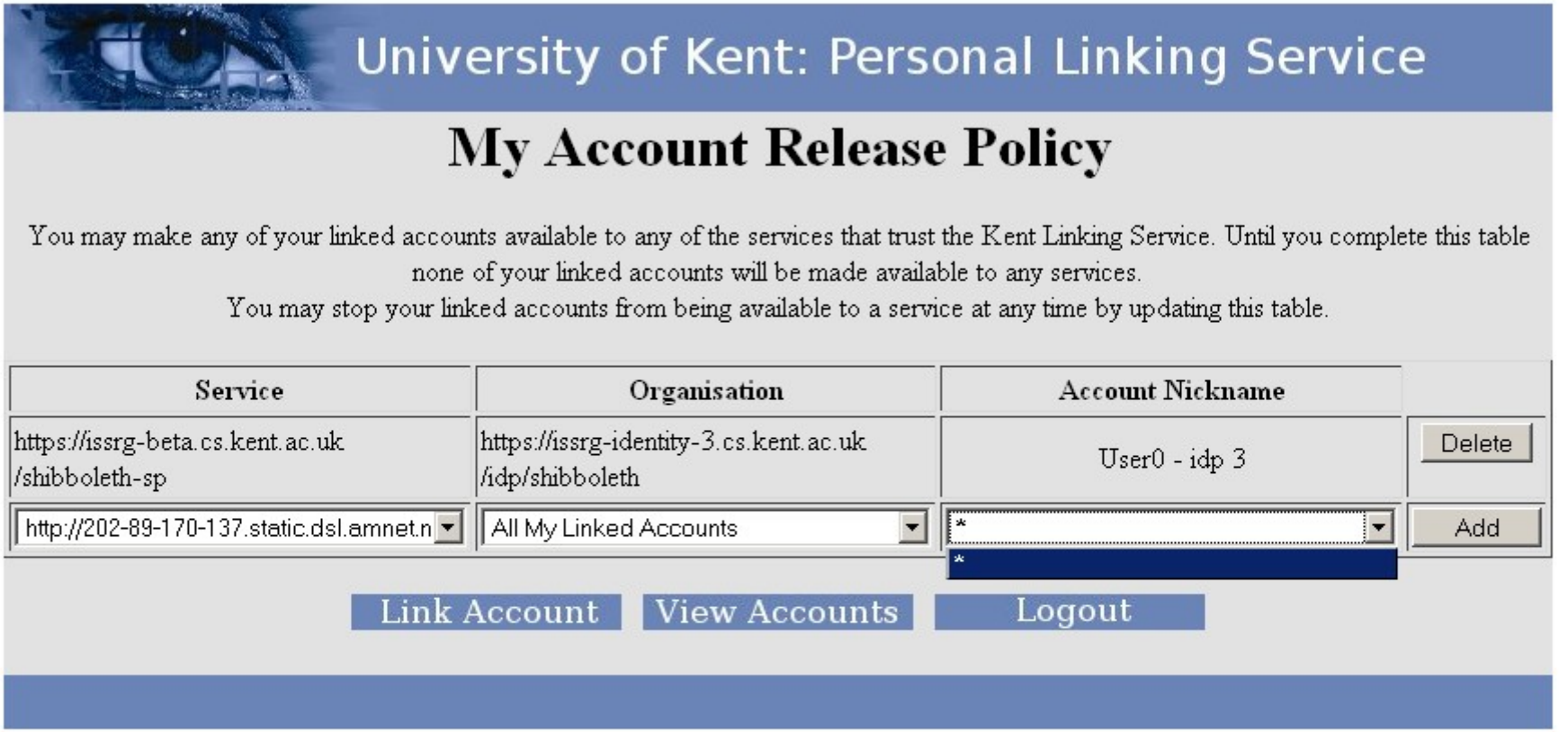

University of Kent: Personal Linking Service
My Account Release Policy
You may make any of your linked accounts available to any of the services that trust the Kent Linking Service. Until you complete this table none of your linked accounts will be made available to any services.
You may stop your linked accounts from being available to a service at any time by updating this table.
Service
Organisation
Account Nickname
https://issrg-beta.cs.kent.ac.uk/shibbol
https://issrg-identity-3.cs.kent.ac.uk/idp
User0 - idp 3
Add
All My Linked Accounts
https://issrg-identity-3.cs.kent.ac.uk/idp/shibboleth
https://issrg-identity-2.cs.kent.ac.uk/idp/shibboleth
Link A
gout


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://issrg-beta.cs.kent.ac.uk/shibbol
https://issrg-identity-3.cs.kent.ac.uk/idp
User0 - idp 3
User0 - idp 3
Add
Link Account
View Accounts
Logout


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://issrg-beta.cs.kent.ac.uk /shibboleth-sp
https://issrg-identity-3.cs.kent.ac.uk /idp/shibboleth
User0 - idp 3
Delete
Add
Link Account
View Accounts
Logout

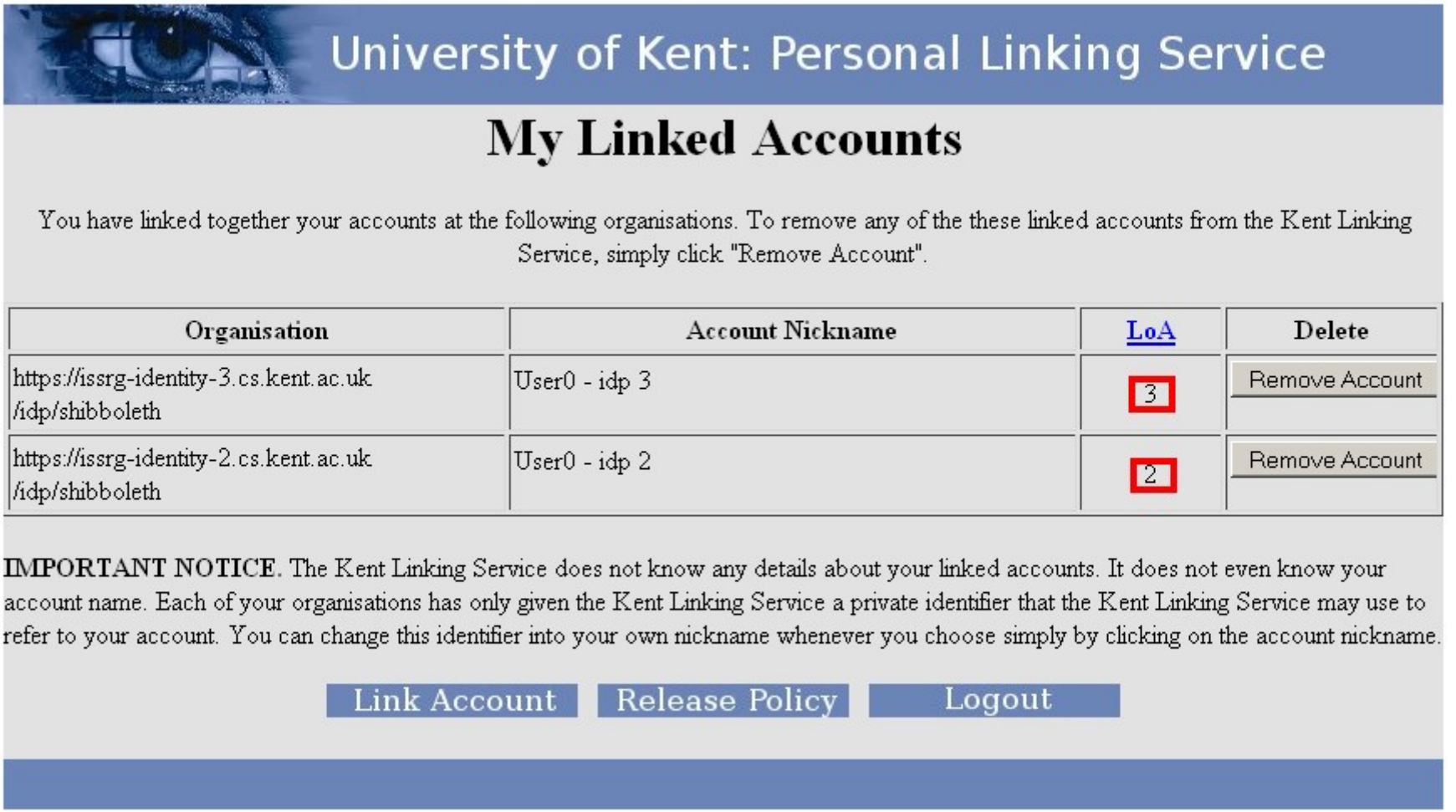

nal Linking Service
All Other Services
http://202-89-170-137.static.dsl.amnet.net.au/shibboleth-sp
http://admin.in2itive.biz/shibboleth-sp
http://bisque.sdh.ucla.edu/shibboleth-sp
http://colin6.colinbradford.org/shibboleth-sp
http://componentspace.dyndns.org/ShibbolethSP/
http://demo.varstreet.com/shibboleth-sp
http://demo1.livetext.com/shibboleth-sp
http://eprescriber-dev.zixcorp.com
http://gully.ads.intra.inist.fr/simplesaml/saml2/sp/metadata.php
http://hcsportal.housing.ufl.edu/shibboleth-sp
http://home.example.com:3000/shibboleth-sp
http://isweb33.cl.msu.edu:9001/shibboleth-sp
http://kirvesam1/shibboleth-sp
http://oasp.beta.athensams.net/OaspMetadata/Athens
Policy
he Kent Linking Service. Until you complete this table
le to any services.
e at any time by updating this table.
Account Nickname
User0 - idp 3
Delete
http://202-89-170-137.static.dsl.amnet.n
Add
Link Account
View Accounts
Logout


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://issrg-beta.cs.kent.ac.uk /shibboleth-sp
https://issrg-identity-3.cs.kent.ac.uk /idp/shibboleth
User0 - idp 3
Delete
http://202-89-170-137.static.dsl.amnet.n
Add
All My Linked Accounts
https://issrg-identity-3.cs.kent.ac.uk/idp/shibboleth
https://issrg-identity-2.cs.kent.ac.uk/idp/shibboleth
Link A
gout


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://issrg-beta.cs.kent.ac.uk /shibboleth-sp
https://issrg-identity-3.cs.kent.ac.uk /idp/shibboleth
User0 - idp 3
Delete
http://202-89-170-137.static.dsl.amnet.n
All My Linked Accounts
*
*
Add
Link Account
View Accounts
Logout

Use of LoA when Linking

- When linking an account identifier at the LS we also register the numeric LoA level of the authentication method as the PIDs registration LoA
  - The IdP replaces the AuthnContextClass SAML authn element with a class urn that identifies the LoA as described in the SAML LoA specification.
  - The LS looks up the value of the AuthnContextClass in the SSO assertion and stores this value as the registration LoA


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://issrg-identity-3.cs.kent.ac.uk /idp/shibboleth
User0 - idp 3
3
Remove Account
https://issrg-identity-2.cs.kent.ac.uk /idp/shibboleth
User0 - idp 2
2
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

Types of LoA at Service Provision

- Three types of loa
  - Registration LoA – How confident the IdP/LS is that the attributes it stores are accurate
    - Web registration may have an LoA of 1 but meeting the user and viewing their passport may be 4
  - Authentication LoA – The strength of the authentication at service provision
    - Username and password may have an LoA of 1 whereas Smart Cards may be 4
  - Minimum LoA level – What level of authentication LoA is required for the IdP to release additional attributes to the aggregating entity

Using the Linking Service at Service Provision time

- The Shibboleth login screen is modified to allow the user to select attribute aggregation (via a tick box)
- If the user does not tick the aggregation box, then Shibboleth works just as now (with no aggregation)
- Sites that require multiple attributes from multiple IdPs will reject access

Account Login

In order to access this resouce you must login to one of your organisation accounts before proceeding.
Please select one of your organizations from the list below.

issrg-identity-1

Submit

issrg-identity.cs.kent.ac.uk - LoA 2

Username: User0

Password: •••••

Do you wish to aggregate attributes from other linked accounts

Login

Resource Requiring Attributes from a single IdP

It works!

This page is protected by Shibboleth and PERMIS

Resource Requiring Attributes from Multiple IdPs

Authorization Required

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

Apache/2.0.63 (Unix) DAV/2 PHP/5.2.6 Server at issrg-beta.cs.kent.ac.uk Port 8080

Using the Linking Service at Service Provision time

- If the user selects attribute aggregation but did not set up a Link Release Policy with the Linking Service then he will still be refused access as no linked attributes will be returned by the Linking Service
- Any linked accounts with a lower registration LoA than the session IdP are not returned by the LS.
- Similarly if an IdP receives an LoA value which is higher than an Attribute's registration LoA or lower than the minimum LoA then it is not returned.

issrg-identity.cs.kent.ac.uk - LoA 2

Username: User0

Password: •••••

☑ Do you wish to aggregate attributes from other linked accounts

Login

Authorization Required

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

Using the Linking Service at Service Provision time

- If the user selects attribute aggregation and has set up a correct Link Release Policy with the Linking Service then he will be granted access to the service

issrg-identity.cs.kent.ac.uk - LoA 2

Username: User0

Password: •••••

☑ Do you wish to aggregate attributes from other linked accounts

Login

It works!

This page is protected by Shintau and PERMIS

And now the technical stuff

- User authentication to the Linking Service is a standard SAMLv2.0 request in which a permanent id (PID) is requested
  - <NameIdPolicy> element is set to “urn:oasis:names:tc:SAML:2.0:nameid-format:persistent,”
  - allow-Create attribute of the <NameIdPolicy> element is set to true
- LOA is returned using draft OASIS spec *Level of Assurance Authentication Context Profiles for SAML 2.0*

Service Provision

- SP redirects user to IdP and asks for transient ID in authn response (standard Shib)
- If user requests attribute aggregation then IdP returns a referral to the Linking Service (LS) along with the authn statement containing Session LOA and the attribute statement
  - otherwise IdP behaves as now (no referrals)
- Referral is encoded as a Liberty Alliance ID-WSF endpoint reference (EPR).
- EPR's <sec:Token> contains the encrypted PID of the user shared between IdP and LS
- If SP has enough attributes from attribute statement then it ignores the referral and gives the user acces, otherwise it acts on referral

SP -> LS

- Uses LA Discovery Service. SP sends Discovery Query to LS asking for the user's linked IdPs' discovery services
- Query Message contains the <sec:Token> copied from the referral EPR, an optional "aggregate" Boolean and the initial authentication assertion in the message's SOAP header. This is the only nonstandard part of the protocol; in the original SOAP binding only the <sec:Token> would be present

Action by LS

- LS decrypts the <sec:Token>, looks up the PID and gets all the user's linked IDPs
- LS checks if the user's Link Release Policy allows these links to be returned to the SP
- LS checks if the Session LOA is LE to stored LOAs. Only links with equal or higher LOAs are returned
  - Don't want user to assert an attribute at a higher level than it was registered
- If Boolean is missing or false then SP is performing aggregation, and LS returns a Discovery QueryResponse to SP containing referral EPRs to the discovery services of the user's linked IdPs
- The SP then sends a DiscoveryQuery message to each IdP's discovery service, requesting the EPR of the user's attribute authority
  - Query contains <sec:Token> and Authn statement
- If LS is performing the aggregation, it sends the same message to each IdP

Action by Linked IdP

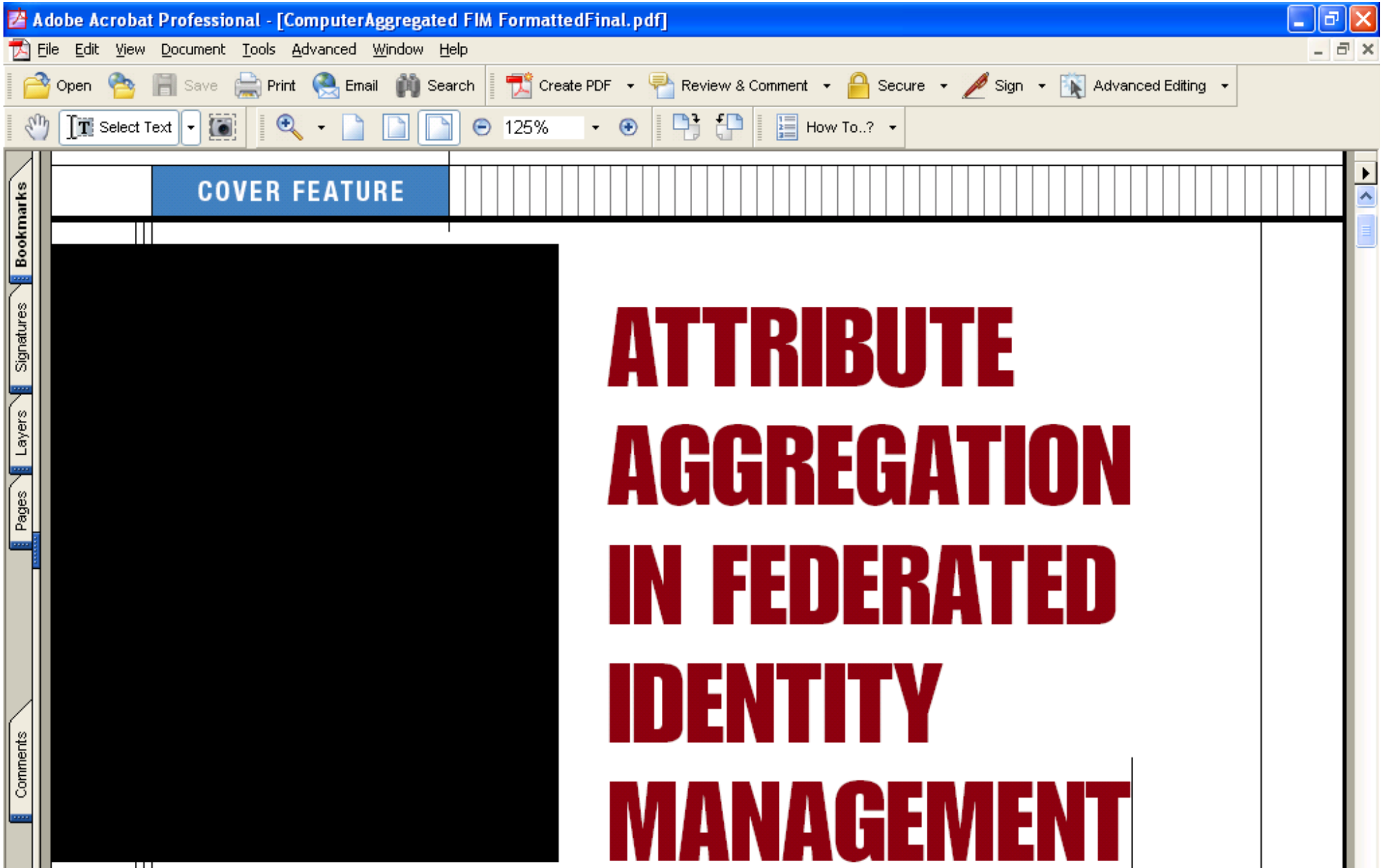
- Decrypts the <sec:Token>, locates the user's account from the PID
- If the user's registration LOA is GE to the session LOA, it maps the random identifier from the authentication assertion into the user's account.
  - it wont return attributes at a higher Session LOA than its stored attributes
- The IdP returns a Disco QueryResponse containing the EPR of the attribute authority where the random ID is now valid (or null if the Query is erroneous)
- The requestor then sends a SAML Attribute Query to this EPR and the IDP returns a response containing the user's random ID and attributes, signed and encrypted to the SP

Features

- The SP gets an authentication statement and set of attribute statements all containing the same user ID and all signed by their authoritative sources
- The user remains in full control and provides his consent every time. Also sets his own release policies.
- User friendly (we hope). The user only authenticates to one IdP for service provision and it can be any from the set of linked IdPs. Linking is also pretty easy
- The user's privacy is protected as the SP does not know the identity of the user unless the user wishes to release a unique identity attribute to it
- Fully standards compliant with only one minor change to Disco protocol
  - Uses Connor Cahill's open source Disco Service and Internet 2 Shibboleth software
- Will be released as Open Source (BSD License) to the community in 3 months time after validation/user trials are completed by University of Glasgow

Finally

- You can read all about this in May's edition of IEEE Computer Magazine



Any Questions?