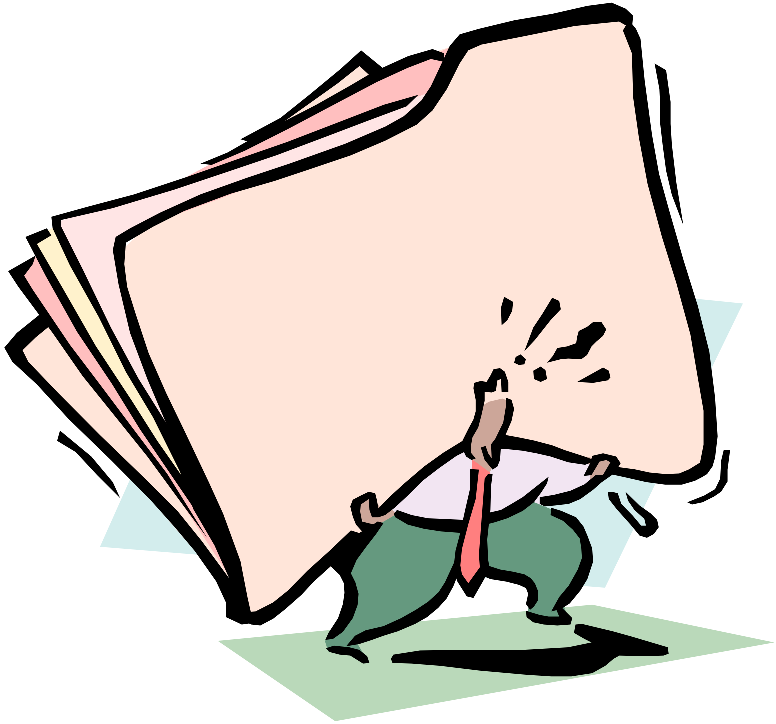
CardSpace in the Cloud

David Chadwick, George Inman

University of Kent

Hypothesis

- (Nearly?) All current Identity Management models today are inadequate/broken



Why Inadequate?

- Do not fit current use model of plastic cards
- We have multiple cards in our wallet and may need to present several of them in a single transaction

  e.g. Credit Card and Rail Card; Hotel Loyalty Card and Frequent Flyer Card
- along with self asserted data
- The identity management models today assume that in *any given transaction* the user has one ***Identity Provider*** that will provide ***ALL*** his/her attributes to the Service Provider
  - E.g. in CardSpace the user can only select a single card, in SAML/Liberty/Shibboleth the user is redirected to a single IDP to login which provides all his/her attributes

What is the Reality?

- Users have no identity providers (as such)
- They only have dozens of different service providers

- Take a look in your wallet at all the plastic cards you have.
- Which is from an identity provider?
- Which are from service providers?
- Even passports are from SPs!
  - – If you don't travel abroad you don't have one

Why is this?

- Because organisations don’t just issue cards for the fun of it (what is the business model of being purely an identity provider?)
- They provide you with a service and issue cards as a by-product in order to increase their service offerings to you
- Some service providers may accept the cards from other service providers in order to entice you to take their services
- There is usually a cost to them in doing this, but the benefit is extra business for them

How many attributes are on a Card?

- The vast majority of cards only contain a single authorisation attribute about you
- The rest of the information on the card is usually
  - Details about the issuer
  - Validity Time of the card
  - A unique card number
  - Name/Identifier of the subject
  - Information to allow the subject to be authenticated by relying parties (signature, picture, age etc.)
- Consequently the current IdM models are totally inadequate since they expect each identity provider to present ALL your authorisation attributes
  - Why should anyone trust my university to assert my credit card number, my address etc.
  - More importantly, my university would never take responsibility for asserting my credit card number to anyone

Proposed IDM Solution

- A user should be able to combine the attributes he has from multiple providers (lets call them Attribute Authorities) into a single session with the current service provider, in order to gain a rich quality of service.
  - E.g. book a hotel room online and present your credit card, hotel loyalty card and frequent flyer card in order to pay, get a free room upgrade and acquire points with your airline,
- User should only have to authenticate once in order to do this

This presents a number of ***Challenges***

- Users are typically known by different identifiers at each of their service providers
  – No common globally unique identifier for the user
- No service provider knows all the other service providers that a user has relationships with.
  – Only the user knows this
- To ensure privacy protection we would like to keep it this way
- So how can a service provider have confidence that all these attributes belong to the same user?

Technically Speaking

- The service provider should receive digitally signed attribute assertions from multiple authorities which
  - All belong to the same end user
  - Give assurance that the person at the other end of the Internet is this end user (and is not a dog)
- Without requiring the user to have to login to each of the attribute authorities

"On the Internet, nobody knows you're a dog."

3-D Secure

- The nearest we have to this today is 3-D Secure from Visa and MasterCard
- User logs into Service Provider and is authenticated
- User provides credit card number to SP then issuing bank asks the user to enter a password to confirm that (s)he is the owner of the credit card
- Time consuming and tedious for the user, but it does provide a bit of extra security

Now extend this to 2 or more cards

- Would the user accept having to authenticate to multiple card providers in the same session with the service provider?
- Probably not
- So what do we propose?

Attribute Aggregation

- The process of obtaining attribute assertions from different attribute authorities, within a single session, to prove to the service provider that the service requestor is the rightful subject of all of the assertions
- The user should only need to authenticate once during the session (to either the service provider or one of the attribute authorities) and trust relationships should be sufficient for the other parties to confirm who the user is

Current State of the Art

- SAML, Liberty Alliance and Shibboleth all recognise that the user has different identifiers at different attribute authorities and that these identifiers should be privacy protected ✓
- SAML allows new identifiers (random or permanent) to be created between pairs of attribute authorities (or identity providers) and service providers ✓
- But the protocol flow typically only goes between a single IDP/AA and a service provider, so there is no support for attribute aggregation ✗
- And there is no dynamic protocol support for the set of attributes that the service providers requires ✗

Information Cards/CardSpace

- Provides the user with a visual representation of his/her attributes ✓
- Allows the service provider to dynamically send its policy for which attributes it requires ✓
- Only allows the user to choose one card in one session ✗

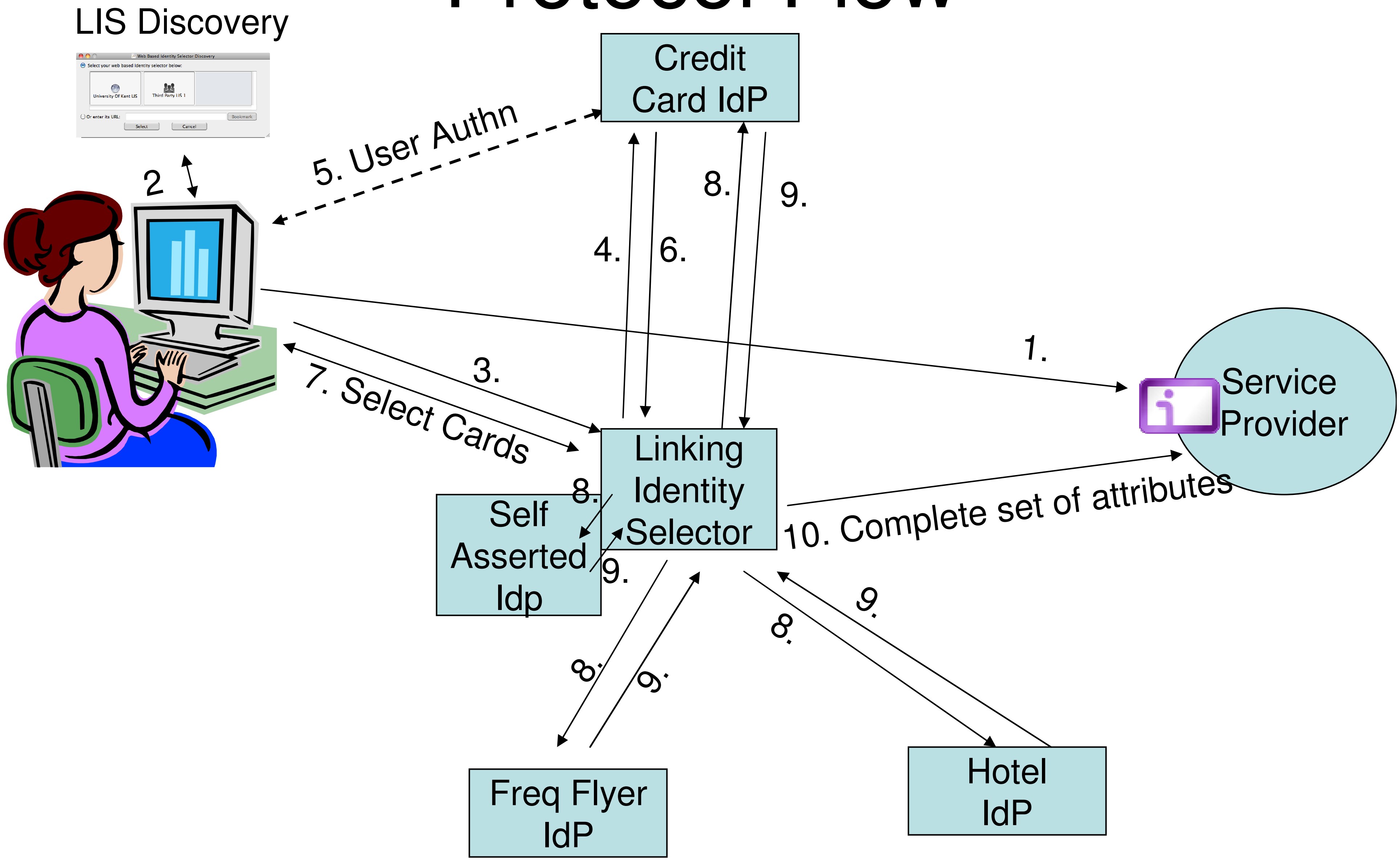
Combining the two together

- Recognise that the user has many different attribute authorities with different identifiers at each that should be privacy protected
- Allows new identifiers (random or permanent) to be created between pairs of attribute authorities (or identity providers) and service providers
- Provide the user with a trusted service for aggregating these AAs together
- Provide the user with a visual representation of his/her attributes and allow her to give consent each time they are released
- Only require the user to authenticate once to the aggregated system and allow the protocol flow and trust relationships to support the attribute aggregation
- Allow the service provider to dynamically send its policy for which attributes it requires i.e. dynamic protocol support for the set of attributes that the service providers requires

CardSpace in the Cloud Implementation

- Introduce a trusted service, the Linking Identity Selector (LIS), to replace the CardSpace desktop Identity Selector
- The LIS is controlled by the user, but does not know who the user is, apart from the minimal details it holds about the user's different attribute types at various attribute authorities/IdPs
  - Note. The LIS never knows any attribute values apart from user self asserted ones which the user provides to the LIS for storage
- Attribute authorities/IdPs have trust relationships with the LIS, with each other, and with the SP (as they determine)
- When the user logs in to one IdP, other IdPs may also be prepared to release their attributes to the SP for this user
- The SP receives digitally signed assertions from each IdP, each asserting different attributes for the same user.
- Each attribute is encrypted to the SP, so no data leakage
- The user is identified by a random number in each assertion, so no permanent identifiers of the user are released.

Protocol Flow



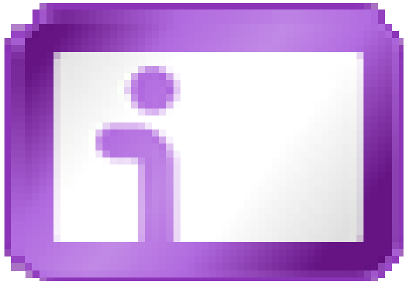
Web Based Identity Selector Discovery

○ Select your web based identity selector below:

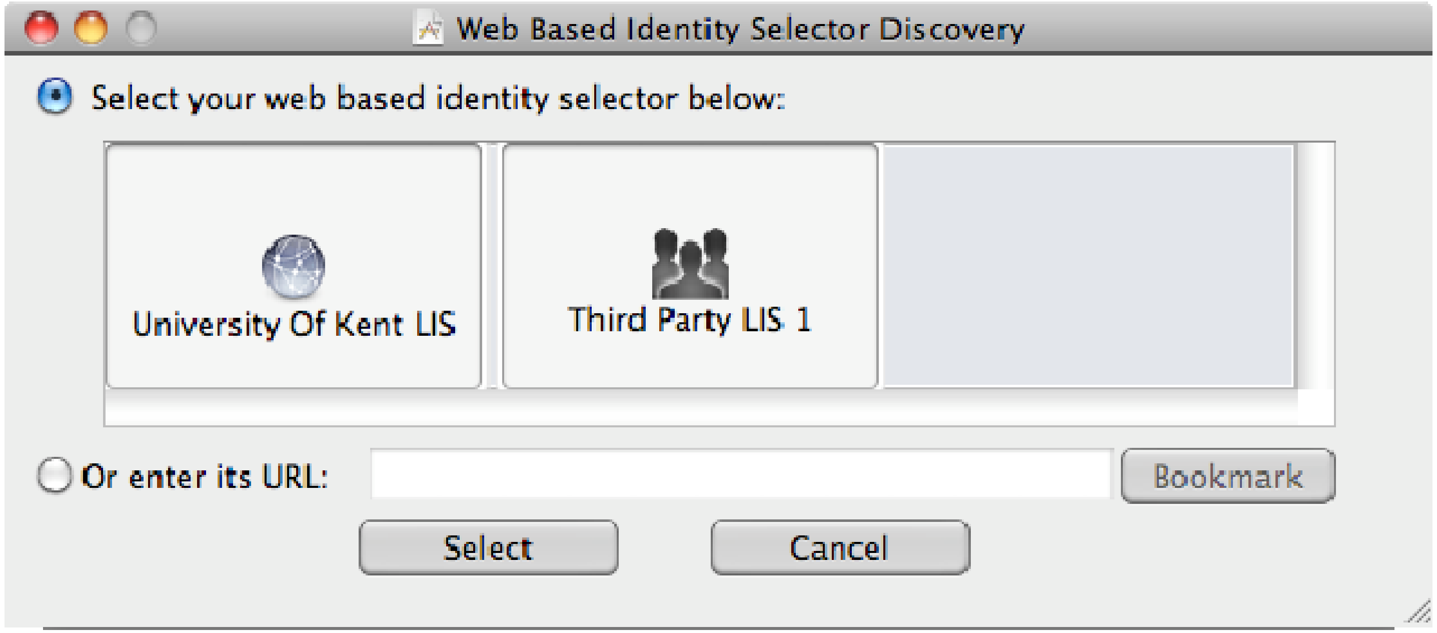
○ Or enter its URL:

User Experience

- User visits a secured web site and sees the CardSpace icon
- User clicks on the icon
- Browser displays the LIS Discovery window



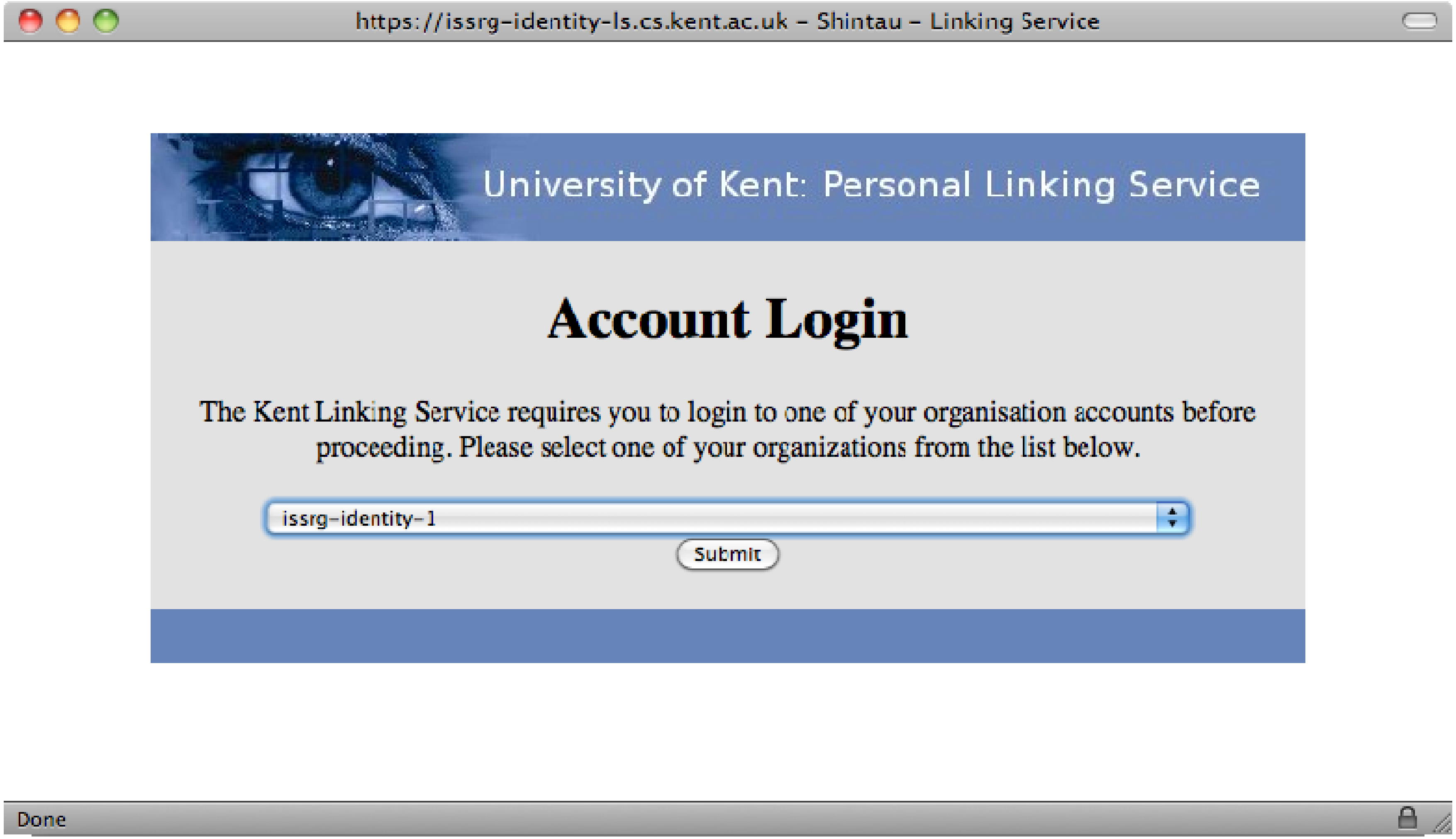
Browser LIS Discovery Window



Web Based Identity Selector Discovery
● Select your web based identity selector below:
University Of Kent LIS
Third Party LIS 1
○ Or enter its URL:
Bookmark
Select
Cancel

- Protects against Phishing attacks, since user must enter the location of the LIS herself
- User selects a LIS and is presented with Login Screen

Logging in to the LIS



https://issrg-identity-ls.cs.kent.ac.uk - Shintau - Linking Service
University of Kent: Personal Linking Service

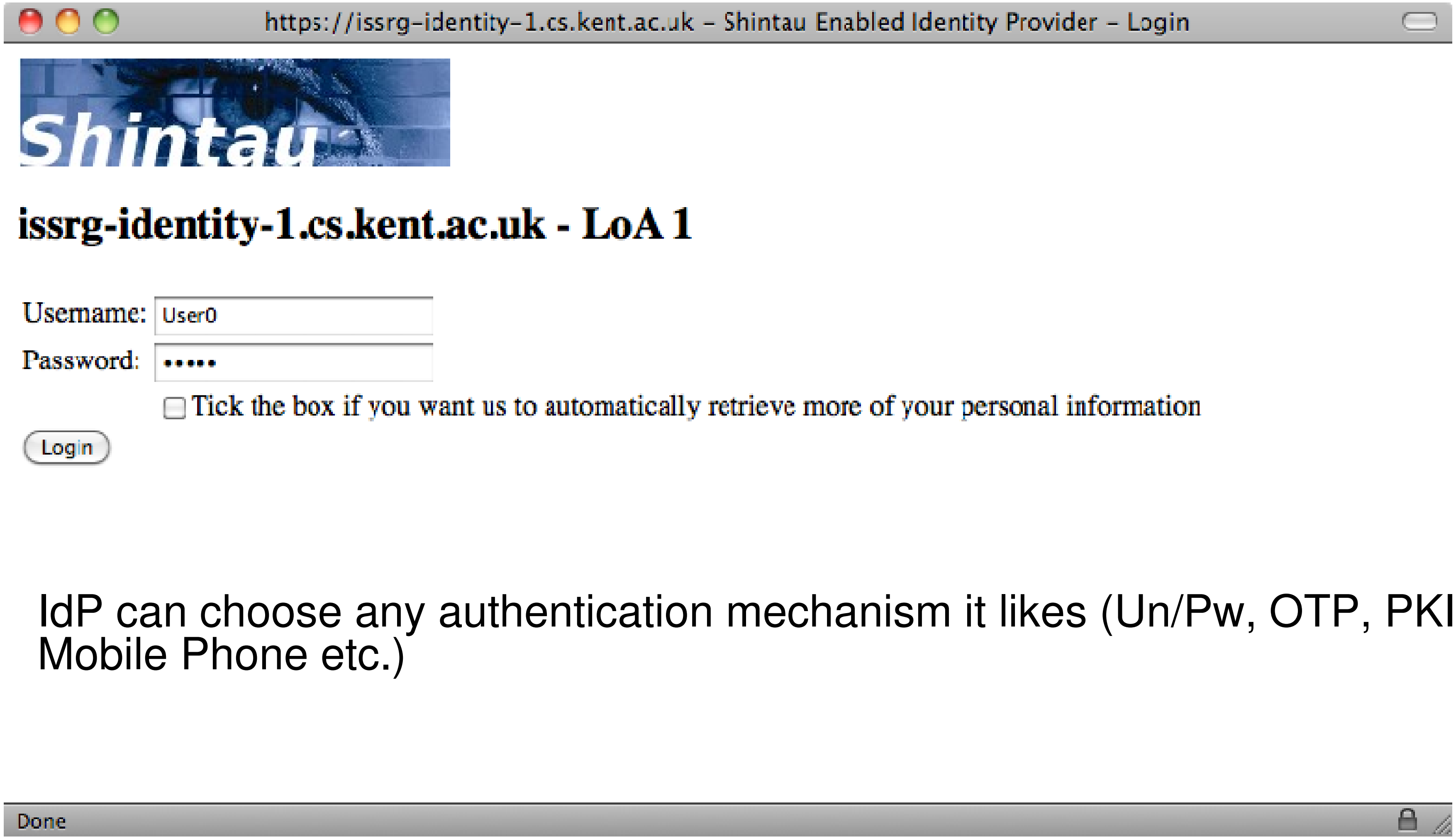
Account Login

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

- User selects his IdP from a picking list and is redirected there

User Authenticates to IdP



https://issrg-identity-1.cs.kent.ac.uk – Shintau Enabled Identity Provider – Login

issrg-identity-1.cs.kent.ac.uk - LoA 1

Username: User0

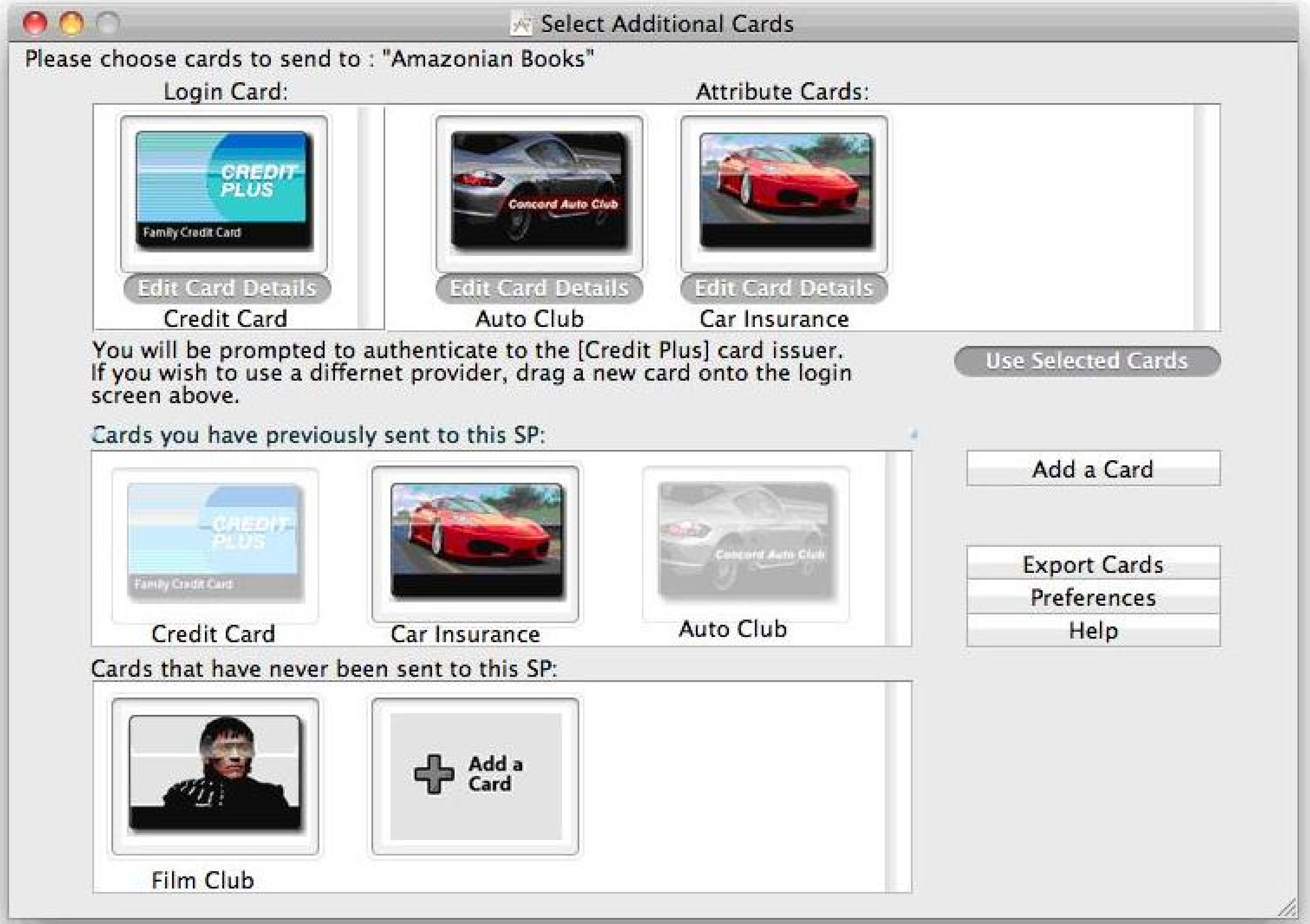
Password: •••••

□ Tick the box if you want us to automatically retrieve more of your personal information

- IdP can choose any authentication mechanism it likes (Un/Pw, OTP, PKI, Mobile Phone etc.)

- User is redirected back to the LIS, which displays his/her cards which match the SP's policy

Linking Identity Selector

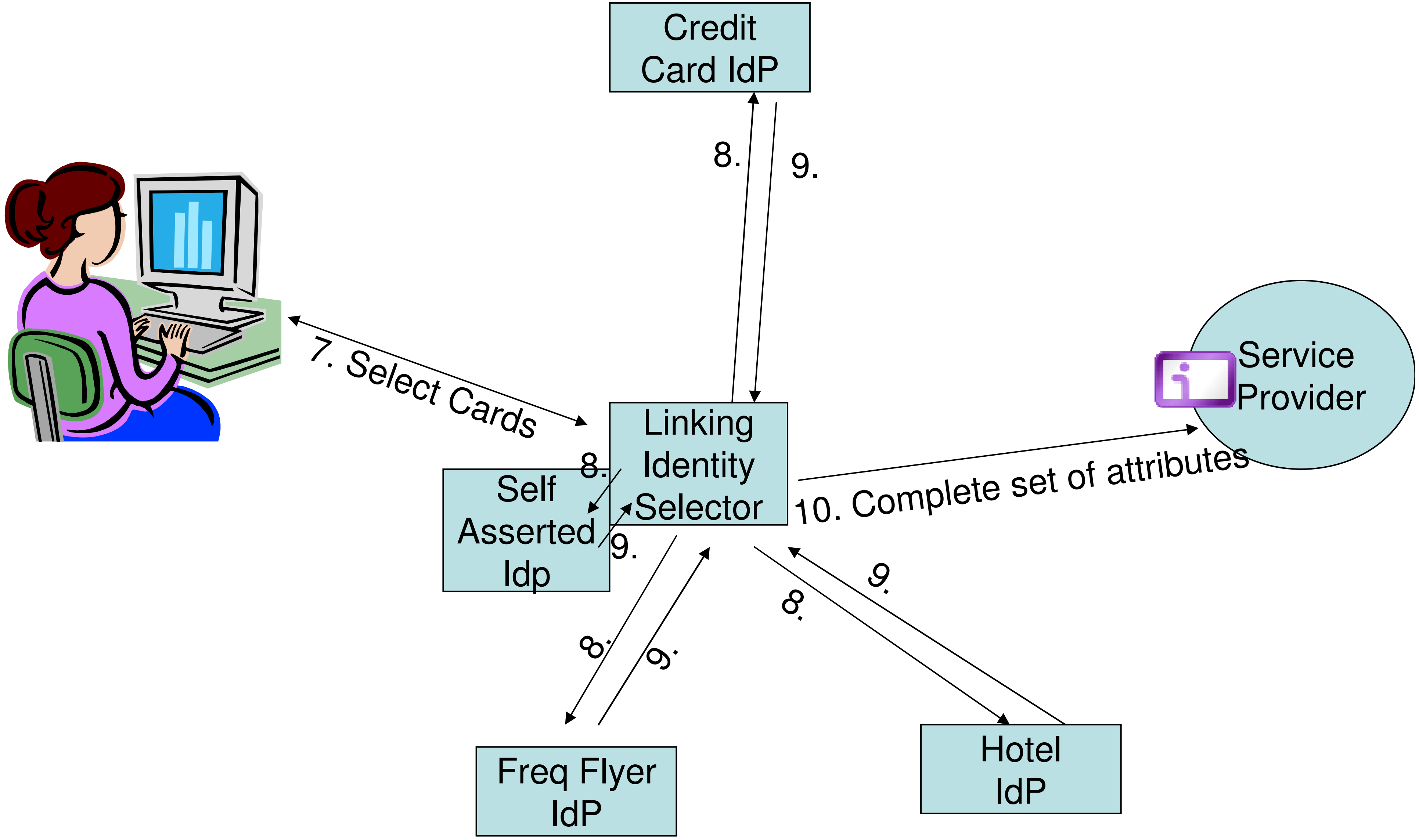


Please choose cards to send to : "Amazonian Books"

You will be prompted to authenticate to the [Credit Plus] card issuer. If you wish to use a differnet provider, drag a new card onto the login screen above.

- Users select the cards they want to send and these move up to the top window
- Bottom two windows are the existing CardSpace windows

Protocol Flow



Protocol Technicalities

- All protocol interactions between the LIS, IdPs and SP are SAMLv2
- The authenticating IdP uses a random ID to identify the user, and includes a referral to the user’s account at the LIS
  - This is our main extension to existing protocols
- The referral is a Liberty Alliance Endpoint Reference
  - Contains the PID of the user encrypted to the recipient
- The SP policy schema needs enhancing to support multiple IdP/card selection

Next Steps

- Complete the implementation
- Perform user trials
- Publish results
- Get the protocol extensions standardised

Thankyou

- ANY QUESTIONS????????????