

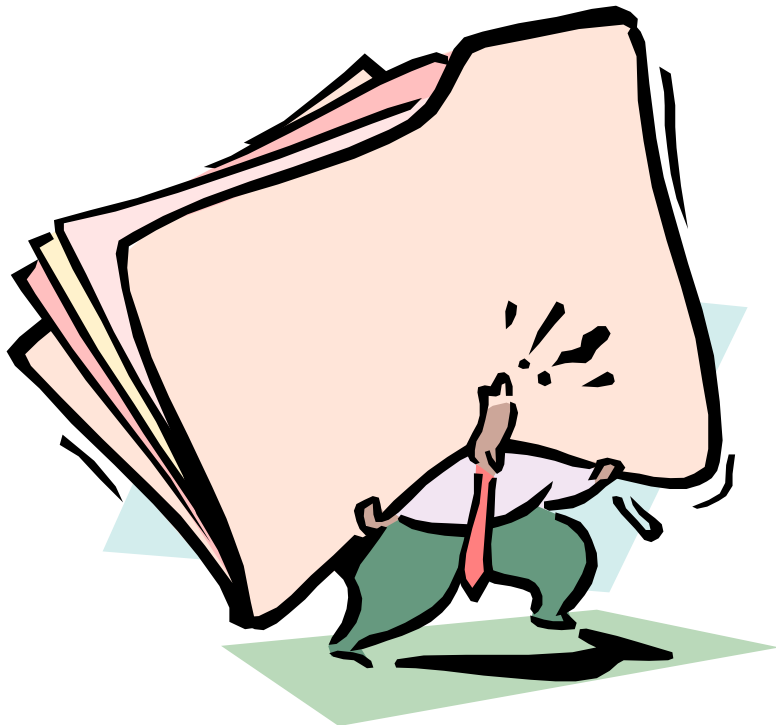
The Trusted Attribute Aggregation Service (TAAS)

Providing an attribute aggregation layer for
federated identity management

David W Chadwick, George Inman
University of Kent

Hypothesis

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



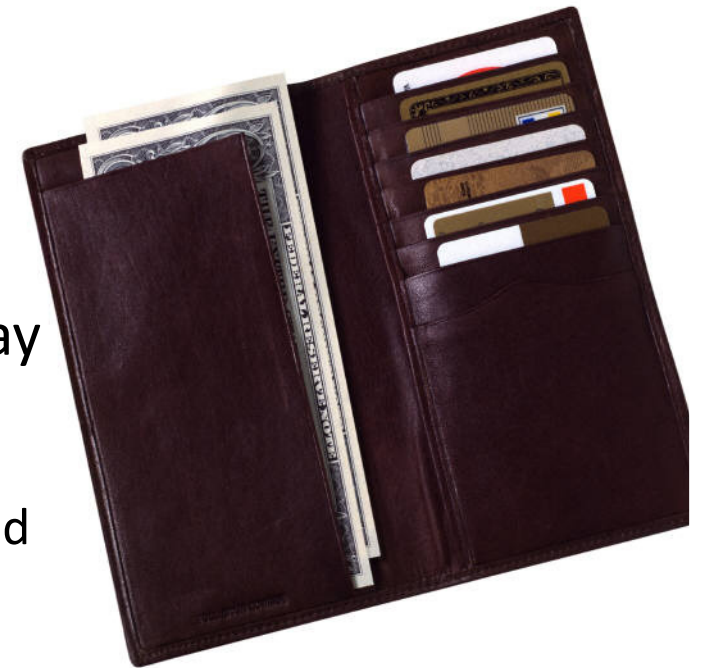
© 2013 University of Kent



ARE

Why Inadequate/broken?

- 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** (IdP) that will provide **ALL** his/her attributes to the Service Provider (SP)
 - 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
- They are open to phishing attacks, since the SP redirects the user's browser to his IdP



How many attributes are on a Card?

- The vast majority of cards typically 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

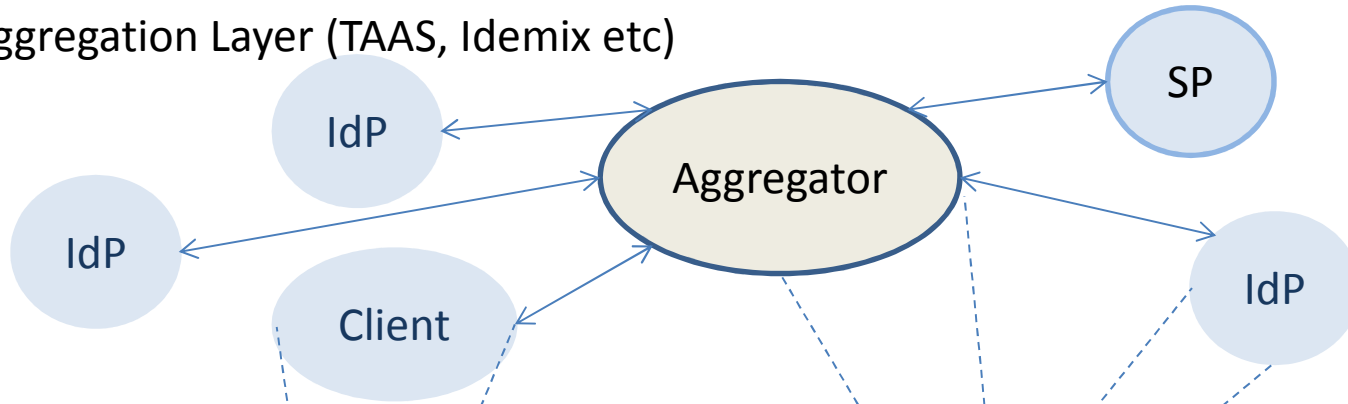
Proposed IDM Solution

- SPs should **inform users** which attributes they need or desire at the time authorisation is needed, along with the **assurance level**, and should be able to **alter this mid-session**.
- A user should be able to combine the attributes he has from **multiple providers** (IdPs/ Attribute Authorities) into a single session with the current service provider, along with **self asserted attributes**, 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 have **complete control, visibility and consent** over attribute release, and otherwise be privacy protected
- User should only have to **authenticate once** in order to do this
- System should be **resilient to phishing attacks**

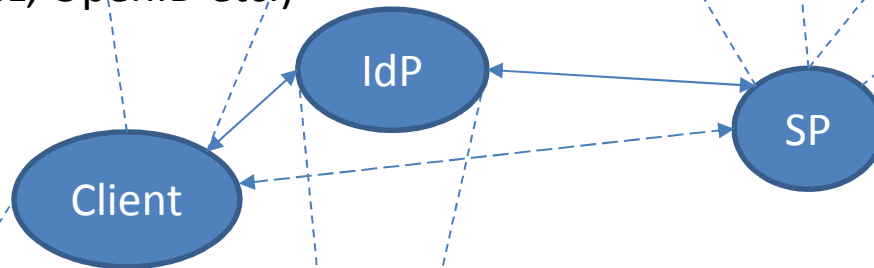
Our Proposal

- To add an attribute authorisation and aggregation layer above the existing federation layer
- Purpose: to provide user attribute aggregation, selection and consent at multiple points during a session with a SP, as the user accesses different protected resource requiring different permissions (attributes and LoAs)

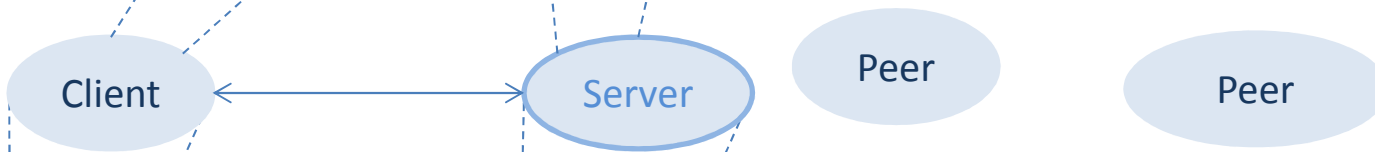
Attribute Aggregation Layer (TAAS, Idemix etc)



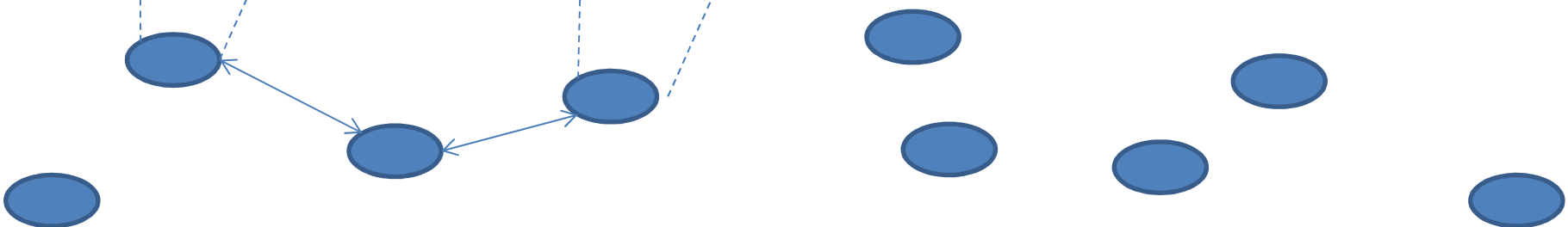
Federated Layer (SAML, OpenID etc.)



Authentication Layer (UN-PW, PKI etc)



Connectivity Layer (TCP-IP)

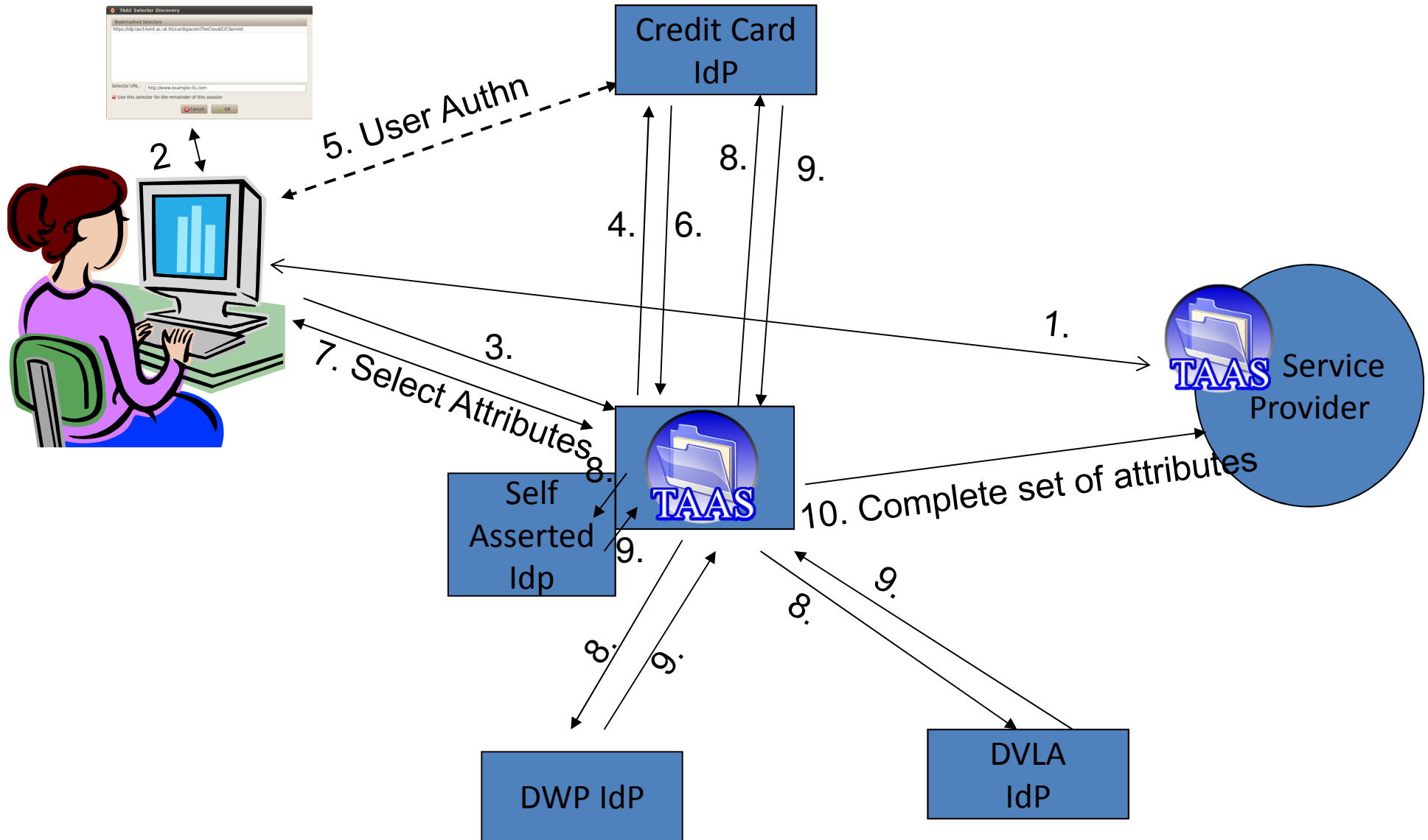


Technically Speaking

- The service provider should receive digitally signed attribute assertions from multiple attribute authorities which
 - All belong to the same end user
 - Only release the attributes the user consents to release
 - 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
- We propose a Trusted Attribute Aggregation Service for this, which is under the control of the user

TAAS Protocol Flow

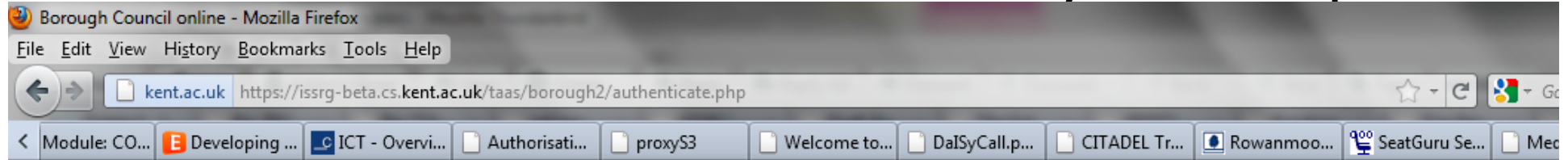
TAAS Discovery



Live Demo of TAAS

- The live demo is publicly accessible and is available from here
- <http://sec.cs.kent.ac.uk/demos>
- Select demo 5, Trusted Attribute Aggregation Service
- There are 3 demos available:
 - e-government, buying a car parking permit
 - e-business, online shopping for books
 - e-learning, downloading a peer-reviewed paper

Users are shown which attributes they have to provide



Borough City Council Online

You Are Here: >> [Home](#) >> [Parking](#) >> [Buy Parking Permit](#)

Before proceeding with your purchase we require you to login with a security level of 2  and provide all of the following information:



Proof of **Car Ownership** issued by the **DVLA**



Proof of **Name** and **Address** issued by the **DWP**



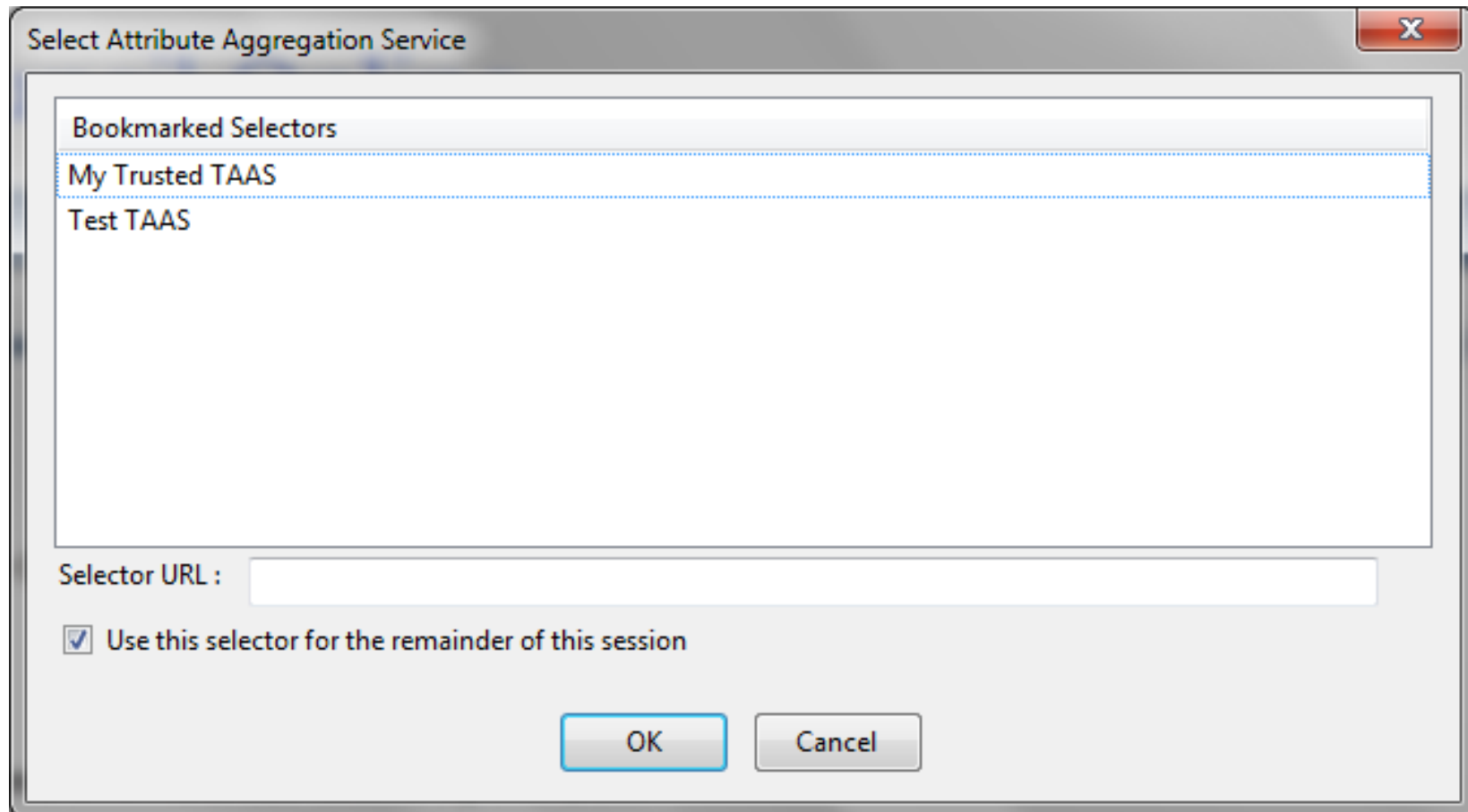
A **Credit Card** issued by **Visa**, **Mastercard** or **American Express**

User clicks on TAAS icon



User is asked to select his/her aggregation service

- Users can click on a bookmarked URL (e.g. stored on their own PC)
- Or enter a new URL (e.g. if in Internet café)




TAAS now asks user to select an IdP for authn

TAAS

Select your identity provider

Please select the identity provider where you want to authenticate:

Remember my choice

Department of Work & Pensions (DWP) 

Select

Big Bank

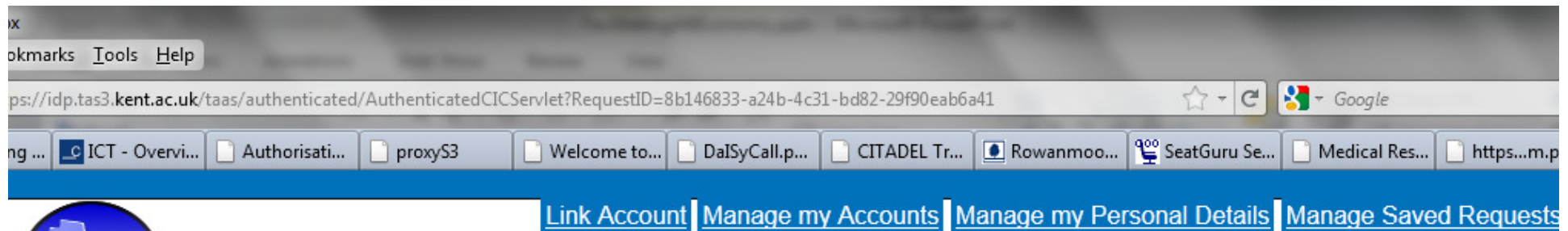
Select

The University of Kent

Select

Driver & Vehicle Licensing Agency (DVLA)

TAAS filters user's available attribute types against SP's policy



Please choose which of the following you want to use for borough-council2.gov

Cancel

Credit Card

Required

Choose

Car Registration

Required

Choose

Name

Required

Choose

Address

Required

Choose

Don't bother me again

Save and Submit

Submit

Allowing user to select which values he/she wants to use

The screenshot shows a web browser window with the URL `https://idp.tas3.kent.ac.uk/taas/authenticated/AuthenticatedCICServlet?RequestID=b642c49f-43ce-409f-a513-70dd0c1eb0f9`. The browser tabs include "University o...", "ACE-CSR.p...", "Living Inves...", "Authorisati...", "TAAS Demo...", "CardSele...", "Module: CO...", "Developing ...", "ICT - Overvi...", and "Authorisati...".

The main content area features a navigation bar with links: [Link Account](#), [Manage my Accounts](#), [Manage my Personal Details](#), and [Manage Saved Requests](#). Below this is the TAAS logo and a heading: "Please choose which of the following you want to use for borough-council.gov".

The interface displays several selection options:

- Credit Card**: Marked as ***Required*** with a "Choose" button and a card icon.
- CarRegistration issued by dvla.gov**: Marked as ***Required*** with a "Change" button and a "(X.50)" label.
- Name issued by dwp.gov**: No specific action button is visible.
- Address issued by dwp.gov**: No specific action button is visible.

A modal dialog is open over the "Credit Card" option, titled "Please choose your preferred Credit Card" with a red "X" icon. It contains two options:

- VisaCard issued by bigbank.com
- MasterCard issued by bigbank.com

Each option has a small card icon with a red ribbon. A "Submit" button is located at the bottom right of the modal.

At the bottom of the main page, there is a checkbox labeled "Don't bother me again" and two buttons: "Save and Submit" and "Submit". A "Cancel" button is also visible in the top right corner of the main content area.

After completing selection, user submits to SP

Firefox
Bookmarks Tools Help
https://idp.tas3.kent.ac.uk/taas/authenticated/AuthenticatedCICServlet?RequestID=b642c49f-43ce-409f-a513-70dd0c1eb0f9
Google
University o... ACE-CSR.p... Living Inves... Authorisati... TAAS Demo... CardSele... x Module: CO... Developing ... ICT - Overvi... Authorisati...

[Link Account](#) | [Manage my Accounts](#) | [Manage my Personal Details](#) | [Manage Saved Requests](#)

TAAS

Please choose which of the following you want to use for borough-council.gov

Cancel

VisaCard issued by bigbank.com (SomeRandomVisa)
Required
Change

CarRegistration issued by dvla.gov (X.500 DSA)
Required
Change

Name issued by dwp.gov (David W Chadwick)
Required
Change

Address issued by dwp.gov (1 Some Street...)
Required
Change

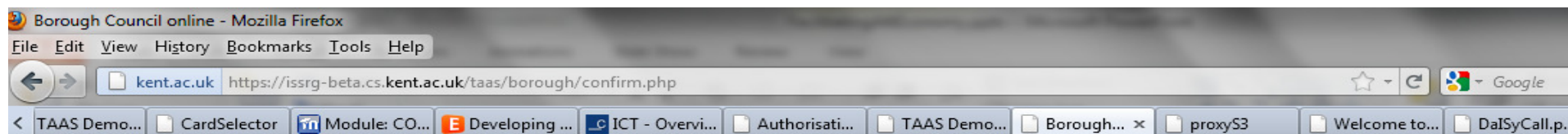
Don't bother me again

Save and Submit Submit

If user selects this, the saved selection will always be used in future without showing this screen to the user again

User can choose to save selection for next time or submit without saving

SP confirms to the user all the actual aggregated attribute values it received from the IdPs



Borough City Council Online

You Are Here: >> [Home](#) >> [Parking](#) >> [Payment Confirmation](#)

Payment Confirmation

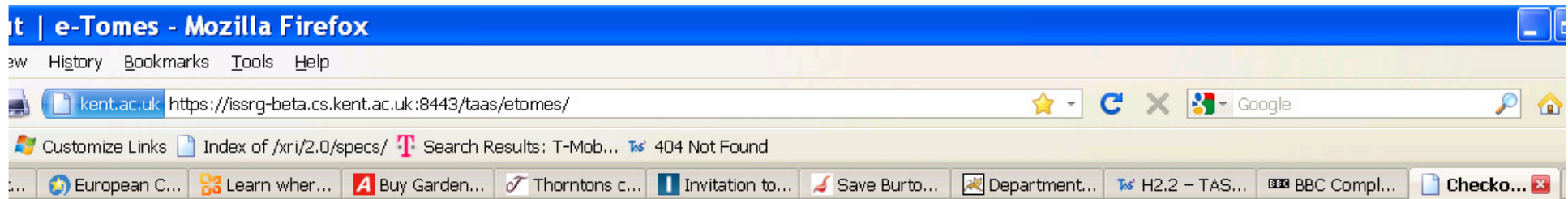
A summary of your order is displayed below, please verify that your details are correct before submitting your order.

Name:	David W Chadwick
Address:	1 Some Street Some Area Borough BR68LU
Item: Car Reg:	Limited Parking Permit X.500 DSA
Price:	£23.00

[Submit](#)

[Cancel](#)

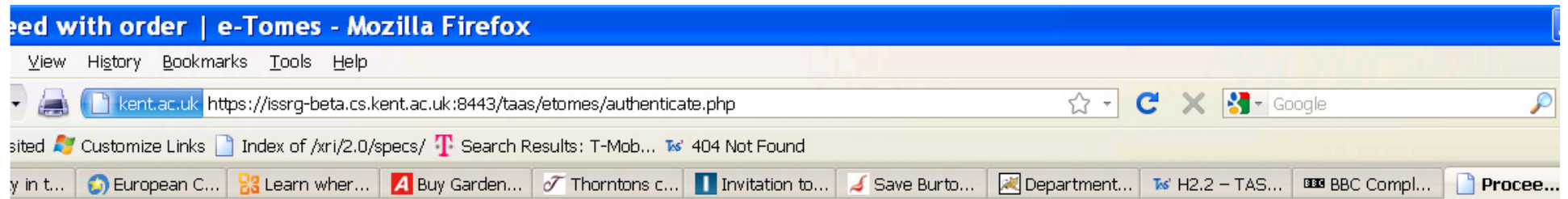
e-Shopping example



e-Tomes
weighty reading for the Electronic Age

	Item	Price	Qty
<input type="button" value="Delete"/>	Finnegans Wake - James Joyce	£5.99	<input type="text" value="1"/>
	Student Discount	-£0.59	
			Total: £5.40

Site shows its Attribute Requirements



Before you proceed with your purchase we require you to login with an authentication level of 1 and supply us with the following information :

- A Credit Card issued by **Visa**, **Mastercard** or **American Express**
- A **Postal address** provided by you
- A **Recipient name** provided by you
- A **Student Card** provided by a university



User is Asked to Choose Her Attributes

or - Mozilla Firefox


History Bookmarks Tools Help

kent.ac.uk https://idp.tas3.kent.ac.uk/taas/authenticated/AuthenticatedCICServlet

Customize Links Index of /xri/2.0/specs/ Search Results: T-Mob... 404 Not Found




European C... Learn wher... Buy Garden... Thorntons c... Invitation to... Save Burto... Department... H2.2 - TAS... BBC BBC Compl...

[Link Account](#) [Manage my Accounts](#) [Manage my Own Attributes](#)



Please choose one of your attributes to match each of https://e-tomes.com's requirements

Requested Attributes

 <p>*Required* <input type="button" value="Choose"/> Credit Card</p>	 <p>*Required* <input type="button" value="Choose"/> Name</p>	 <p>*Required* <input type="button" value="Choose"/> Address</p>
--	---	---

03/10/2013 © 2011 University of Kent 20

User Can Have Many Self Asserted Values


Firefox - Mozilla Firefox

History Bookmarks Tools Help

kent.ac.uk https://idp.tas3.kent.ac.uk/taas/authenticated/AuthenticatedCICServlet


Customize Links Index of /xri/2.0/specs/ Search Results: T-Mob... 404 Not Found

European C... Learn wher... Buy Garden... Thorntons c... Invitation to... Save Burto... Department... H2.2 - TAS... BBC BBC Cor







Please choose one of your attributes to match each of https://e-tomes.com's requirements

Requested Attributes

 ***Required***

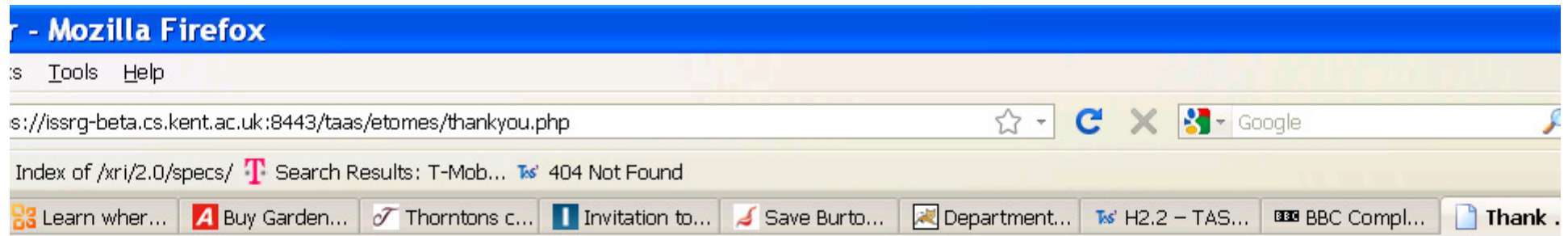
VisaCard from bigbank.com

Please choose your preferred Name 

 <p>Name from dwp.gov</p>	 <p>Name from Self Value: David Chadwick</p>	 <p>Name from Self Value: Bill Gates</p>
--	---	---

03/10/2013 © 2011 University of Kent 21

Transaction Successful

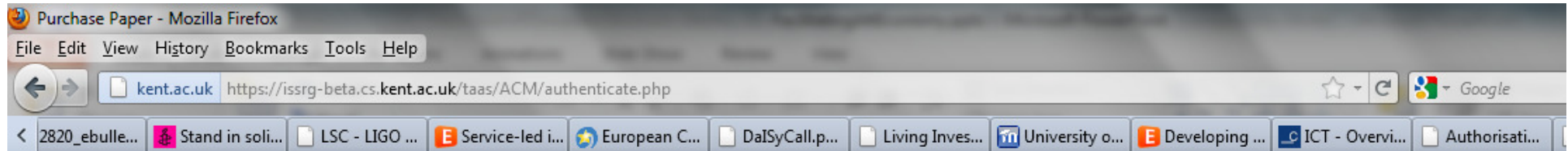


Thank you for your order!

Your order number is XXX1234, please keep a record of this


[Continue Shopping](#)

A Disjunctive Policy



ACM Digital Library

You Are Here: >> Home >> Academic Papers >> Purchase Paper

Before proceeding with your purchase we require you to login with a security level of 1  and provide:

Either



A **Credit Card** issued by **Visa**

There is a cost of \$25 to download this paper

Or



Proof of **affiliation** with a **UK University**

Papers can be downloaded free by members of participating universities

Summary of Usability Features

- Allows SP to display/set its policy for both the LoA and its mandatory and optional attributes, so users know what is required from them
- Allows user to select attributes from multiple IdPs as well as his own provided values (if SP's policy allows it)
- TAAS automatically filters SP's policy against user's attributes and does not show ones that don't match
- TAAS allows users to dynamically add new attributes and links to IDP attributes in the middle of a transaction
- Allows user to add his own attribute types and values
- Allows user mobility and use from Internet cafes
- TAAS will remember a user's choices so they don't have to
- Users never need to enter credit card numbers again

Summary of Security/Privacy Features

- Built on top of SAML so inherits its security and privacy features
- Ensures users consent to each attribute release
- TAAS does not know who the user is
 - It only gets PIDs from IDPs and user self asserted attributes (if any)
- TAAS never sees any IDP provided attribute values
 - They are encrypted end to end from IDP to SP
- TAAS stops phishing attacks by evil SPs and evil emails
 - Users provides their own URLs of their own TAASs
- TAAS stops all storage and theft of credit card numbers from SP sites
 - Users never enter their credit card numbers. Card Issuer sends one time encrypted value to the SP for use in current transaction
- The SP receives digitally signed assertions from each IdP, each asserting different attributes for the same user (identified by a Random ID)
- Uses standard protocols throughout (SAMLv2, LA ID-WSF EPRs)
- Requires trust between various components
- Provides very similar functionality to U-Prove and Idemix tokens, but with today's technologies.

Trust Requirements

- SP must trust authenticating IDP to authenticate user correctly
- SP must trust IDPs for attributes they issue
- IDPs must trust authenticating IDP to authenticate user correctly
- SPs and IDPs must trust TAAS not to mix up user PIDs and to only release PIDs back to their issuing IDPs

Conclusions

- Leveraging Trust reduces the cost of doing business
- We introduce a Trusted Attribute Aggregation Service that facilitates trust between users, SPs and IDPs and allows attribute aggregation, user consent and user choice over which attributes to release
- The standardisation activities that are still required are
- The content of the SP's policy
- The profiles for use of SAMLv2, LA and HTTP/post protocols