The Trusted Attribute Aggregation Service (TAAS)

Privacy Protected Identity Management with User Consent, Minimum Disclosure and Unlinkability

David W Chadwick, George Inman, Kristy Siu

University of Kent
### e-Shopping example

A screenshot of an e-commerce website, e-Tomes, with a purchase order for a book titled "Finnegans Wake - James Joyce." The price is £5.99, and the quantity is 1. There is a student discount of £0.59, making the total £5.40. Options to place the order or cancel are displayed.
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
Browser Pop Up Ask User for Her TAAS

You proceed with your payment.

Credit Card issued by Visa, M.
Postal address provided by y
Recipient name provided by w
Student Card provided by a

Select Attribute Aggregation Service

Bookmarked Selectors
My Trusted TAAS

Selector URL:

Use this selector for the remainder of this session

OK Cancel

Get Information

21/05/2011 © 2011 University of Kent
TAAS Asks User to Authenticate

Account Login

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

Big Bank

Submit
User Logs In to Her Chosen IdP

My Big Bank Login Page

Username: David
Password: *********

Login

Disclaimer: This login page is for demonstration purposes only. My Big Bank is purely fictitious and any resemblance to real entities is coincidental.
User is Asked to Choose Her Attributes

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

Requested Attributes

- **Credit Card**
  - Required
  - Choose

- **Name**
  - Required
  - Choose

- **Address**
  - Required
  - Choose

21/05/2011 © 2011 University of Kent
User Chooses Her Preferred Attribute/IdP
User Can Have Many Self Asserted Values

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

Requested Attributes

VisaCard from bigbank.com

Please choose your preferred Name

Name from dwp.gov
Name from Self Value: David Chadwick
Name from Self Value: Bill Gates
After All Are Chosen She Can Submit (and Save)
Transaction Successful

Thank you for your order!

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

Continue Shopping
Now to demo 1-Click on subsequent buying.
Selection from last time was Saved by User

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

Requested Attributes

- VisaCard from bigbank.com
- Name from Self Value: Bill Gates
- Address from Self Value: 1 Short Ave

Save and Submit  Submit
Thank you for your order!

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

Continue Shopping
Borough City Council Online

You Are Here: >> Home >> Parking >> Residents Parking

Parking Permits

Residents Off-Street Parking

Residents in Borough, who live in the vicinity of a public car park, can buy permits allowing them to park free without any additional charge. Permit cost £23.00 and allows the holder to park at all times.

Apply For Parking Permit
Council Displays Its Attribute Requirements

Before proceeding with your purchase we require you to login with an authentication 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 Chooses Her TAAS

When making a purchase, we require you to login with an authentication level of 2 and provide all of the following in a SAML assertion:

- Proof of e-mail
- Proof of address
- A credit card

When you login to the TAAS service, you can select from the following predefined selectors:

- Bookmarked Selectors
- My Trusted TAAS

You can choose the Use this selector for the remainder of this session option.
User Chooses Her IDP
User Logs In

The Driver and Vehicle Licensing Agency Login Page

The Driver and Vehicle Licensing Agency Login to Service Provider "Kent Trusted Aggregation Service"

Username: 
Password: 
Login

Disclaimer:
This login page is for demonstration purposes only, it should not be confused with the official DVLA
User is Asked to Choose Attributes

Please choose one of your attributes to match each of https://borough-council.gov's requirements

Requested Attributes

- 'Required' Credit Card
- 'Required' Car Registration
- 'Required' Name
- 'Required' Address

[Buttons: Save and Submit, Submit]
Note that Self Asserted Names are Not Allowed by SP
User Chooses and then Submits
Site Confirms User’s Attributes

---

**City Council Online**

---

**Payment Confirmation**

Your order is displayed below. Please verify that your details are correct before submitting your order.

<table>
<thead>
<tr>
<th>Name:</th>
<th>David W Chadwick</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address:</td>
<td>1 Some Street</td>
</tr>
<tr>
<td></td>
<td>Some Area</td>
</tr>
<tr>
<td></td>
<td>Borough</td>
</tr>
<tr>
<td></td>
<td>BR68LU</td>
</tr>
<tr>
<td>Item:</td>
<td>Limited Parking Permit</td>
</tr>
<tr>
<td>Car Reg:</td>
<td>X.500 DSA</td>
</tr>
<tr>
<td>Price:</td>
<td>£23.00</td>
</tr>
</tbody>
</table>

---

Submit  Cancel
Summary of Features

- Uses standard SAMLv2 protocol for transferring claims/attribute assertions
- Prevents phishing attacks since user chooses where to go to for claims
- SP shows its attribute policy to user prior to aggregation so user knows what is required
- TAAS re-displays SP’s policy with user’s attributes that match each element so user can select each attribute one by one
- User chooses and consents to all attribute releases
- Minimum disclosure of user attributes and unlinkability of transactions (unless user chooses linkable attributes)
- User can self assert attribute values if SP’s policy allows it
- Simplifies user experience down to 1-click attribute selection and never having to enter credit card numbers
- Privacy protects user. TAAS never sees any IdP claim values and does not know who the user is. SP is never given a user identifier by any IdP (random ID is used)
- Ensures SP’s don’t need to store or see credit card numbers as claims can use unique 1-time numbers which are different for each transaction