Privacy Preservation through good AIM

Dr Rhys Smith
Dr John Chapman

October 2014
Today’s story

1. What we want and why
2. Where are we now?
3. Where we’re going
Prologue
Janet – the UK’s research & education network

• Janet, a part of Jisc, is a not-for-profit company that works on behalf of the UK’s R&E community
• Janet’s service portfolio includes the high speed network, and other services that build on it
• This includes a portfolio of Trust & Identity services, and related service development activity
• Janet has approximately 18 million eligible users, from UK schools, HE, FE and ACL programmes
Target Audience

New to the AIM area?
  • Overview of the everything

Have experience in one particular area?
  • Understand the other areas

Establishing a federation?
  • Understand privacy implications of design choice

Everyone
  • See where we’re heading…
Act I:
What we want and why
Context & Motivation

• Hypothesis:
  – Individual privacy is under attack

• But?
  – Do people care?

• Well
  – I care!
  – Every little helps
  – Higher assurance data is worth $$$
  – R&E specifically – anonymous browsing may have real business benefits
Privacy?

- Privacy is an overloaded term.
- Today I’m talking about:
  - Anonymous/pseudonymous access to resources
  - Only releasing PII with appropriate policy and/or consent.
- Some good general, relevant, privacy principles are...
Privacy by Design

• Privacy is usually very hard to retrofit properly
• Take privacy into account during the whole design & engineering process
Data Protection != Privacy Protection

- EU privacy laws are somewhat over effective
  - Good, obviously, but hinders usefulness

- UK seems to be slowly moving towards more of a risk based approach rather than black/white
  - ICO guidance

- What does this mean?
Privacy vs Utility

- Constant battle (especially in EU)
  - Protect individual & organisational privacy
  - Whilst also retaining usefulness of federated identity (rich attribute ecosystem)
  - Boils down to Trust vs Privacy

- Striking a balance is hard!
  - Different answer for every context
Act II:
Where are we now
State of the Union

• Let’s have a look at where we are with the various AIM services:
  – Web federations
  – Network federations
State of the Union – SAML federations

• Web SSO
  – E-journals
  – Web systems
  – Learning platforms
  – Etc
• Many R&E federations
• Gov federations
• Commercial uses
• And beyond…
R&E federations worldwide (a selection)
SAML federations

<table>
<thead>
<tr>
<th>IdPs</th>
<th>RPs</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Server" /></td>
<td><img src="image2.png" alt="Server" /></td>
</tr>
<tr>
<td><img src="image3.png" alt="Server" /></td>
<td><img src="image4.png" alt="Server" /></td>
</tr>
<tr>
<td><img src="image5.png" alt="Server" /></td>
<td><img src="image6.png" alt="Server" /></td>
</tr>
<tr>
<td><img src="image7.png" alt="Server" /></td>
<td><img src="image8.png" alt="Server" /></td>
</tr>
<tr>
<td><img src="image9.png" alt="Server" /></td>
<td><img src="image10.png" alt="Server" /></td>
</tr>
</tbody>
</table>
Mesh Federation

IdPs

RPs
Privacy and Utility in a Mesh World

**User:**
- Can remain anonymous to the service

**IdP:**
- Tailor attribute release per RP
- Traceability
- Sees which RPs the user uses

**RP:**
- Anonymous personalisation
- Sees which IdP the user came from
Privacy in a Mesh World

- Anonymity (or pseudonymity) is easy
  - Opaque identifiers targeted per RP
- Non PII attributes released
- PII attributes destroy anonymity, so only released with specific purposes and trust base
Privacy in a Hub & Spoke world

**User:**
- Can remain anonymous to the service

**IdP:**
- Doesn’t know what services user is using

**Hub:**
- Sees everything
- Traceability
- Tailor release policy to RP

**RP:**
- Anonymous personalisation
- Doesn’t know user or IdP
Privacy in a Hub & Spoke world

• Double Blind
  – Better privacy guarantees than Mesh… assuming you trust the Hub (!!!?)

• Triple Blind
  – New cryptographic techniques meaning no single entity has full picture
State of the Union – eduroam
Eduroam all the way down
Eduroam meshed up (RadSec / DD)
Privacy in the hierarchical eduroam world

User:
• Remains anonymous (to the service and to eduroam)

AP / RP:
• Can see which realm user came from

Eduroam
• Can see which realms people are roaming from/to
  • (RadSec/DD removes this)

IdP:
• Sees where user is roaming
• Traceability
Act III:
Where we’re going
• If privacy protection is the goal, then we’ve largely achieved it!

• Problem is – a bit too well, in many contexts
  – Utility has suffered which may affect take up of services

• So looking to shift the balance slightly
(EU) DP CoC

• An attempt to help increase utility
  – help the lack of attributes problem

• Services sign up to a promise to respect data privacy
  – Makes use of EU DP “code of conduct” allowances
Entity Categories

• Mark particular entities with annotations
  – Shows entity is a member of a particular category
  – Can be used to help attribute release, influence UI, etc

• Research & Scholarship category
  – Attempt to help attribute release for the R&S world
    • “Service Providers that support research and scholarship interaction, collaboration or management as an essential component”
Improving the current - eduroam

• Eduroam works pretty well actually
  – Good levels of privacy - user anonymity
  – But also good utility

• Some small tweaks
  – CUI (a pseudonymous identifier) – helps with traceability

• But is the utility stretching a bit thin?
  – School / other gov use cases who want some more attribute information
Next Gen - Moonshot

• Moonshot
  – Federated Access for anything
  – EAP/RadSec & SAML & GSS-API & Trust Router

• UK pilot
  – April 2013 -> Dec 2014
  – Focus on research community requirements (SSH, etc)

• GÉANT pilot
  – March 2013 -> March 2015
  – Focus on interfederation from the start with Trust Router
Privacy in the Moonshot world

• Just like everything else – depends on deployment model

• Assuming common deployment model will be mesh
  – Similar privacy properties
  – But a few minor tweaks to enhance utility
Trust Router

• How do entities find each other?
  – No metadata like SAML
  – No heirarchy like eduroam

• Trust Router
  – Allows Moonshot entities to securely locate each other and communicate.
  – Multi-layered trust network
Trust Router - Communities

Policy coming from community requirements. Could include:
- Registration LoA
- AuthN LoA
- Operational Practices
- User behaviour
- Attribute release (RADIUS & SAML)
- Etc.

Authentication Policy Community / (Community of Registration)

Organisation validation to APC’s defined standards
Whole Trust Network
Community A
Moonshot/TR – Pseudonymous Identifiers

• Generally, federated AuthN has been accepted as useful, but federated AuthZ is another matter
  – IdPs don’t want to take responsibility
  – RPs don’t want to delegate responsibility

• So, want to enable pseudonymous federated AuthN

• Existing deployment typically hampered by “flatness”:
  – pseudonymous identifiers per RP
  – Attribute release per RP

• But, Moonshot is less flat. So we’ve defined three levels
RP Targeted Identifier

- Different for every RP
  - No collusion
  - But no (good) linking either
Realm Targeted Identifier

- Different for every realm
  - No collusion across realms
  - Linkability between RPs in same realm
Community Targeted Identifier

- Different for every community
  - No collusion across communities
  - Linkability between RPs in same community
Community Policy

• Enables account linking across realms, or whole communities.

• Communities with the need for this, or with the need for PII, can write the requirements into their policies
  – And have content that will constrain its usage and meet DP law
Epilogue
In Conclusion

• Privacy is an important fundamental human right
• Federated AIM services can help preserve (a bit) of individual / organisational privacy
  – every little helps!

• When deploying:
  – Carefully consider your deployment model as it will have lasting privacy implications that may be hard to change later
Questions?