Consent-Informed Attribute Release (CAR)
Scalable Consent and Consent-Informed Attribute Release (CAR)

- The problem set and resulting requirements
- The Scalable Consent work
- The CAR architecture – a brief look under the hood and at the two user UX
- Unexpected outcomes
- CAR Management capabilities – how it performs
- Demos
  - Intercept UI
  - Self-service UI
- The Duke experience
- Next steps
A growing set of federated identity challenges
- Attribute release for R&S and other needs
- GDPR, the EU privacy regulations
- Institutional desires for transparency
- Providing the capstone UI for federated identity

Results in a set of requirements that motivates CAR
- Consent-informed attribute release as an IAM service, with tight integration points to Shib IdP
- Integration of institutional and individual release preferences in a flexible manner
- A well-engineered UX that allows users and organizations effective, but not intrusive, tools for managing consent decisions both in real-time and while they are away
GDPR (General Data Protection Regulation)

- Created by EU to manage data protection uniformly across the EU
  - Is binding for every member EU nation
  - With many global impacts
- Covers a vast waterfront of issues from tracking to attribute release to right to be forgotten to data breaches to . . .
- Consists of a set of rules (Articles) and then example interpretations of the rules in key areas (Recitations)
- Penalties of up to 4% of global revenue
- Identifies six reasons for attribute release, including contract, consent, national security, legal interest, etc.
  - Specifies when consent is not to be used, when it should be used, the quality of the consent, etc.
- If you do business in the EU, this impacts your organization
Consent-Informed Attribute Release (CAR)

- A system of components that serves attribute release and consent needs across all protocols – OIDC and OAuth as well as Shib/SAML.
  - Integrates organizational and individual choices for attribute release
  - Support for user consent decisions that are informed, effective, revocable, accessible, etc.
- Includes UI/UX, enterprise and individual attribute release policy stores, individual and organizational admin interfaces, etc, all accessed through the CARMA API.
Under the hood: CAR in SAML use
Under the hood: CAR in OAuth use
User Experience

• UI/UX well researched, well-designed and well-tested. Includes:
  – Adaptive, mobile-friendly, accessible design. i18n and locale support.
  – Fine-grain controls on attribute release (down to value level of multi-valued attributes), explanations, reconsent options, friendly names and values, etc.
  – Capabilities to handle a wide range of policies, such as GDPR

• Two UI for the standard user
  – Intercept – the standard “transaction” interaction, with options to manage suppression of consent for the site going forward
  – Self-service – users manage their set of consent policies, including revocation, templates for new sites, and “while I’m away” options
Review what you are releasing to CIlogon

CIlogon is requesting information about you from your TIER record.

You may update your settings for CIlogon:

- PERMIT  Email Address (kjk@tier.internet2.edu)
- PERMIT  Legal Name - Last/First (Klingenstein)
- PERMIT  Name - First/Given (Legal) (Ken)
- PERMIT  Name - Full (Preferred) (Ken Klingenstein)
- PERMIT  Scoped NetID (kjk1@tier.internet2.edu)

EDIT THESE CHOICES  CONTINUE WITHOUT EDITING  

CIlogon

CIlogon facilitates secure access to Cyberinfrastructure (CI).

privacy policy

Update your preferences: Consent Manager
Review what you are releasing to CIlogon

CIlogon is requesting information about you from your TIER record.

<table>
<thead>
<tr>
<th>What would you like to release to CIlogon?</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="permit" alt="permit" /> <img src="deny" alt="deny" /></td>
</tr>
<tr>
<td><img src="permit" alt="permit" /> <img src="deny" alt="deny" /></td>
</tr>
<tr>
<td><img src="permit" alt="permit" /> <img src="deny" alt="deny" /></td>
</tr>
<tr>
<td><img src="permit" alt="permit" /> <img src="deny" alt="deny" /></td>
</tr>
<tr>
<td><img src="permit" alt="permit" /> <img src="deny" alt="deny" /></td>
</tr>
</tbody>
</table>

Choose one:
- ![perm](permit) Save my choices; don't show me this screen again unless necessary.
- ![perm](permit) Save my choices, but show me this screen next time.
- ![perm](permit) Don't save the choices I made just now. Show me this screen next time.

CANCEL   ACCEPT AND CONTINUE

CILogon

CILogon facilitates secure access to Cyberinfrastructure (CI).

privacy policy

Update your preferences: Consent Manager
### My Sites

Manage what information will be shared with these sites:

<table>
<thead>
<tr>
<th>Name</th>
<th>URL</th>
<th>Updated</th>
<th>Manage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI Logon</td>
<td>cilogon.org</td>
<td>05/30/2017</td>
<td>manage</td>
</tr>
<tr>
<td>G7NANT Service Provider Proxy</td>
<td>terena.org</td>
<td>05/01/2017</td>
<td>manage</td>
</tr>
<tr>
<td>Internet2 Collaboration Wiki Spaces</td>
<td>spaces.internet2.edu</td>
<td>05/18/2017</td>
<td>manage</td>
</tr>
<tr>
<td>LIGO Wiki</td>
<td>wiki.ligo.org</td>
<td>05/02/2017</td>
<td>manage</td>
</tr>
<tr>
<td>TIER CARMA</td>
<td>carma.testbed.tier.internet2.edu</td>
<td>06/15/2017</td>
<td>manage</td>
</tr>
</tbody>
</table>

### New Site Policy

Manage defaults for what information is shared with new sites.
Manage information sharing for CILogon

Information Requested by CILogon

You can choose whether the following information is shared with CILogon:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Current Value</th>
<th>Current Choice</th>
<th>Duke Recommends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name - Full (Preferred)</td>
<td>Ken Klingenstein</td>
<td>permit</td>
<td>permit</td>
</tr>
<tr>
<td>Scoped NetID</td>
<td><a href="mailto:kjk1@tier.internet2.edu">kjk1@tier.internet2.edu</a></td>
<td>permit</td>
<td>permit</td>
</tr>
<tr>
<td>Name - First/Given (Legal)</td>
<td>Ken</td>
<td>permit</td>
<td>permit</td>
</tr>
<tr>
<td>Email Address</td>
<td><a href="mailto:kjk@internet2.edu">kjk@internet2.edu</a></td>
<td>permit</td>
<td>permit</td>
</tr>
<tr>
<td>Legal Name - Last/Family</td>
<td>Klingenstein</td>
<td>permit</td>
<td>permit</td>
</tr>
</tbody>
</table>

Additional Settings

- **All other information**
  - If CILogon requests information not listed above
    - (any values) askMe askMe

- **While I'm Away**
  - If your choice above is "askMe" but you're not available to answer when CILogon requests information about you
    - (any values) deny deny
What is Informed Content

• The fuel that drives effective and informed user consent decisions
• Obtained from federation, client registration, well-known URL’s, etc.
• Limited, though extensible sets of marks, assessments, policies, etc. that are part of the UX
  – Icons for IdP and SP
  – SP IsRequired and Optional Attribute Needs
  – Display-names and display-values for attributes
  – Trustmark information
  – Explanatory application-specific dialogue boxes (e.g., why attribute is needed)
  – Privacy and third-party use policy pointer
  – Additional user-centric information feeds
    • Vetted, self-asserted, reputation systems, etc.
Unexpected Outcomes

- Initiating important policy conversations on campus
- Allowing users to manage consent across applications and consent as a service
  - Ability to offer organizational advice to user during consent
- Consistent, informed user consent experience across a variety of platforms and protocols
  - Good feedback from successive rounds of user testing
- * Potential integration of institutional and individual attributes
  - Location, Emergency contact and medical information, etc.
- Providing new options for accessibility
  - Accessibility with Privacy
- * Extending organizational attribute release policy from directory/IdP to other systems of record with bio-demographic attributes.
  - Creates institutional policy repository and service for attribute release
  - Illuminating the intra-organizational policy swamp
Status and Next Steps

- CAR is readily integrated into the Shibboleth IdP v3, with it being called for institutional attribute release policy editing and as the decision point for attribute release per transaction.
- Enhancements await – e.g. policy editors, more informed content.
- The deployment is in production but the code is in pre-production stage.
  - Central functionalities implemented and tested
  - First screens (MFA) rolled out
  - End-user UI under tweaking; admin and superadmin UI under development
Organizational Management for Consent

- **Policy administration tool**
  - Will allow editing of organizational attribute release policies within a decentralized authority environment.
  - Who sees consent when, for what attributes, with what defaults
  - Aimed for use by policy administrators, sysadmins of SOR
  - Raises the need to resolve policy conflicts (e.g., DENY trumps RELEASE, rank ordering, etc.)

- **Superadmin tool**
  - Will manage institution-wide settings
    - Logos and skinning
    - Managing when to reconsent – e.g. change in value being released; change in RP privacy policy
    - Managing opaque values, sensitive attributes and values, blacklist and persona non grata attributes, friendly names and values
  - Aimed for use by IdP/CAR sysadmins and Resource Server (OAUTH/OIDC) admins

- **Migration/maintenance toolkit**
  - Repeatable mining/updating of informed content from SAML metadata
  - Generate “starter policies” from IDP configs (attribute-filter.xml)
Adding the RP/client registration and informed content layer

Informed Content is gathered from SAML metadata, OpenId client registration, well-known URL’s, OpenId software statements to come, etc.
Turning the consent management knobs

- Sample student policy:
  - “All students need to visit this alcohol education site. Only FERPA students need to see consent for this site, and we can present advice to them on what to consent to.”

- Policies can be set in a distributed fashion
  - E.g., students on a “manage as a VIP” list can be done by the person who handles students who are children of VIP’s and so subject to special considerations
  - The person who handles GDPR issues (e.g., sensitive attributes) can control those release/presentation issues.

- Time stamps and audit logs to document consent
Consent challenges

- Friendly names for extensible attribute values
- Data minimization for applications
  - Required vs optional attributes and the process to determine that
  - And inform users of the consequence of not consenting
- Purpose of consent fields – can users distinguish
- Sensitivity of log files – avoiding sensitive info kept in logs
- Cognitive load on users
  - How to include trustmarks
  - User feedback
- The politics of introducing consent to existing flows
CAR Next steps – technology

• V1.0 – a Docker container (TIER packaging standards) + a Shib integration guide
  – Include admin and superadmin UI
  – End of Year
• Sustaining and enhancements – 2018 and beyond
  – UMA and Oauth Guide
  – Measurements and instrumentation
    • What to measure
    • How to anonymize
    • How to distribute and share
  – Better policy editors and maybe a more expressive policy language
Closing thoughts

- Privacy is even more complex than security. (Nuance, cultures and laws, etc.)
- Scalable consent is viable.
  - User and institutional feedback has been and understanding positive
- We need research and metrics into managing the issues in good consent
  - The goal is effective informed consent, not fast or deceptive or ignored
  - Qualitative measures must augment current quantitative views (e.g. dwell time)
- The work is capstone to federated identity
- The work is bedrock to sovereign identity