Roadmap

• A Brief Recap of CAR
• CARMA Components
• GDPR & Duke: Challenges for IAM
• Demo
• Deployment Schedule
• Questions/Discussion
CAR: A Brief Recap
CAR: A Brief Recap

WHAT IT IS

Consent-informed Attribute Release (CAR) is a system that serves as a consent-enabled policy decision point for personal information sharing across institutional and affiliated or federated sites and services. CAR is built to handle a range of contexts (authentication, offline requests) and deciding authorities (the institution or a part of it, the user in question), allowing for consistent presentation and enforcement of nuanced policies.

WHY IT’S RELEVANT

New privacy regulations (such as EU-GDPR or CCPA) have resulted in increased interest and inquiries pertaining to data use. As IAM professionals, we need to be prepared to quickly respond to these queries, as well as policy mandates that result from them, and to provide tools that inform users about their privacy.
Acknowledgements

Much of the design and early implementation work for CAR was supported by Internet2 via a grant from the National Institute for Standards and Technology (NIST), under the auspices of the National Strategy for Trusted Identities in Cyberspace (NSTIC) program.

Components of the CAR design were informed by work begun at Carnegie-Mellon University under various grants from the National Science Foundation, including work on CMU’s Privacy Lens project.

The CAR Team:

Rob Carter (Duke University) - architect, developer
Marlena Erdos (independent) - lead architect
Ken Klingenstein (Internet2) - PI, evangelist
Mary McKee (Duke University) - interface design, product development
Shilen Patel (Duke University) - integration development
CARMA: Components
Interface:

**Intercept (or “Inline”)**

- Real-time prompt for transparency or consent

- Users interact with one consent interface regardless of underlying technology (Shibboleth, OAuth, etc.)

- User chooses how often to see this, has option to default to institutional recommendation.
Interface:

Self-Service

• Review the *whats*, *whos*, and *whys* of access to your information.

• Express preferences about how your information is used.

• Manage settings about how you’d like to be notified about actions that impact privacy.
Interface:

System Configuration

- Register Resource Holders, Relying Parties, and information items
  - Import scripts available

- Manage language support (i18n), institutional language (display names, etc.), and branding (colors, fonts, images).

- Manage extended properties
Interface:
Policy Admin

• Create institutional and meta-policies

• Drag-and-drop management of priorities and application order

• Manage legal bases for information release.
GDPR & Duke: Challenges for IAM
Duke’s GDPR Strategy

• Meeting with inside and outside counsel
• Naming Data Protection Officer(s)
• Article 30 Records of Processing
• Privacy Office
  • Guiding Departmental Reviews
  • Managing User Requests
Privacy Office: What parties are holding information on Jane Doe?
On what basis has that information been collected/held?
What is Jane’s relationship to Duke?
What business impact would result from forgetting Jane?

Departments: Can you help us with our Article 30 Record of Processing?
What are we getting from you and why? I’m new here.

What This Means for IAM

Systems of Record: So um…what are you all doing about GDPR?
How are you protecting the data you get from me?

Senior Leadership: How are you supporting our departments with GDPR?
Group X doesn’t have the resources to answer these questions.
Can’t you work with their vendor?
Many areas of your institution will need to account for complicated flows between data controllers and data processors.

Now, where would they find that kind of expertise?

Y’all. This is IAM’s time to shine.
CAR supports

- Point-in-time informed, revokable, granular, audit-friendly consent
- GDPR-compatible handling of declared-“sensitive” data
- Transparency of information sharing for users, administrators, and data stewards across contexts
- Both interactive and “batch processing” information flows
- Granular “legal basis” and intended use/purpose tracking

Consent is not a major part of Duke’s GDPR strategy. CAR is.
Demo
CAR Deployment Schedule
## Deployment Schedule

<table>
<thead>
<tr>
<th>Phase</th>
<th>Scope</th>
<th>Status</th>
<th>Available</th>
</tr>
</thead>
</table>
| **Alpha**         | Pilot Intercept  
Pilot System Admin  
Pilot Self-Service          | Complete | Now (at Duke)      |
| **Beta**          | Expanded pilot (opt-in)  
UX testing and final interface adjustments  
Performance testing, Duke rollout  
Launch branding console  | In Progress | December (at Duke) |
| **General Availability** | Deployment guides, docs and repackaging  
Reporting enhancements  
Additional integrations, integration tools  
Source release (probably under LGPL2) | Planned | January 2019      |
Questions?
{here are some you might start with}

How does policy by value work?
How does CAR handle internationalization?
How does CAR handle FERPA?
How can my institution use CAR without implementing consent?
How does CAR handle sensitive values? Sensitive attributes?
What can CAR offer data owners outside of IAM?
How do users revoke consent? Institutions?
How do you measure informedness of consent?
What kind of resources does CAR need? How about a cloud solution?
What can metrics tell us about how people interact with privacy information?
How the heck does one consent to [very large number] of [attributes | values]?
How can I get my hands on the source code?
Thank You!

Rob Carter
robert.carter@duke.edu

Mary McKee
mary.mckee@duke.edu

https://spaces.at.internet2.edu/display/CAR/
Architecture

- Policy stores
  - COPSU - User policy
  - ARPSI - Institutional policy

- CARMA
  - Meta policy management
    - Ask it anything!
  - UIs for user self-service, policy and system admin, intercept/inline prompts