CAR: Consent-informed Attribute Release system

Background: At many universities and colleges today, a user doesn't have say in the release of their personal information (e.g. email address) to a vendor site that is in a relationship with the institution.

The CAR system:

- **enables user choice (“consent”) about release of their personal information on a per vendor site basis.**
- **balances institutional policies with a user's policies.**
- **works across all browsers and devices.**
- **is protocol agnostic: can work with SAML-based Identity Providers and OAUTH/OIDC Resource Servers**
- **can be used in a variety of "user not present" scenarios, including bulk feeds to external providers, provisioning, and scientific batch programs.**
- **is open-source; currently being deployed at a major US University.**

This site offers information about CAR. Most of the information is intended for people who already are familiar with "identity management," but we give a bit more background for normal people immediately below. We follow the background material with a brief overview of CAR's component services. The bottom of the pages contains links to in-depth technical information about CAR (e.g architecture and policy language documents).

The user's policy choices are permit, deny, "ask me" and "use my institution's advice." For example:

- "permit release of my email address to LibrarySite"
- "ask me about release of my surname to LearningManagementVendor"
- "use my institution's advice about release of my faculty role to SomeOtherSite"
- etc

The institution's policy choices are permit and deny.

- if the user's choice "wins," the institutional decision of permit or deny becomes "advice" the user can see and choose to use or not.
- institutional policy allows for groupings of vendors and groupings of users for ease of administration. For example:
  - "permit release of email for students to all Research & Scholarship vendors"
  - "deny release of given name and surname for staff and faculty to all other sites"

CAR's policy language document describes the policy statements in glorious, geeky detail.

- initially designed to be a policy service about the **release** of **personal information** typically stored by higher education institutions in their campus directories.
  - Each directory item (e.g. email) about a given user is called an "attribute" – hence CAR's name "Consent-informed Attribute Release."
- extended early on to work as an authorization service for many types of user resources and operations (e.g. "view selfies").
- works both for the user present and user-offline cases.
  - user-chosen "While I'm away" setting fills in for the "ask me" choices if the user is not present.
- provides policy decisions of "permit" or "deny" to the holder of the user's resource (or its proxy), be it a directory, a photo service, etc.
- the holding service – the "Resource Holder" in CAR terminology – makes the final choice as to whether to enforce the decision from CAR.

- currently under development at Duke University through the auspices of Internet2.
- catalyzed by a grant from NSTIC grant from NIST.
- CAR Architecture & Implementation Team: Rob Carter (Implementation Lead, Contributing Architect), Marlena Erdos (Architecture Lead), Ken Klingenstein (CAR Evangelist & Project Manager), Mary McKee (UI Lead, and Duke University Liaison/Evangelist), Shilen Patel (Shibboleth Integration).

CAR Components: three separate, but interacting services. These are:

Consent Policy Service For Users (COPSU):

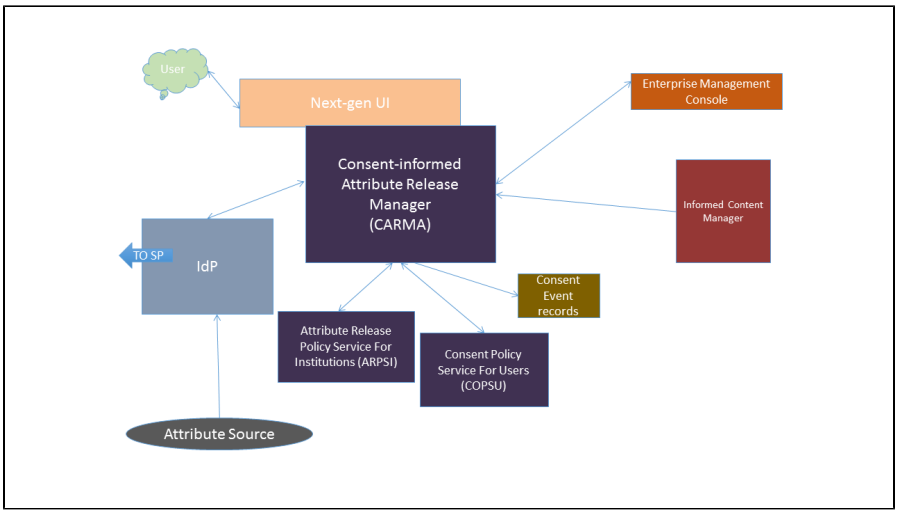
- Stores user policies (including “ask me”) with respect to release of specific values of attributes– or OAUTH scopes or OIDC claims – to specific relying parties (RPs).
- Answers queries about a given user’s choices with respect to a given RP, and a specific set of attributes/scopes/claims.
- Doesn’t hold a user's actual attribute values; instead holds the release policy around the attributes and their values.

Attribute Release Policy Service For Institutions (ARPSI):

- Stores Institutional attribute release policies about users, attributes, values, and relying parties (RPs).
- Answers queries about the institutional choices with respect to a given user, a given RP, and a specific set of attributes.

Consent-informed Attribute Release Manager (CARMA)

- Handles all UI interactions with end users on their policy choices
- Handles all UI interactions with administrators who set institutional or user attribute release policies.
- Handles requests for decisions on attribute release from callers (e.g. IdPs) via requests to the ARPSI and COPSU.
- Holds and applies a "meta policy" to decide what to do when institutional and user policies conflict.
- Takes care of authenticating and authorizing identity providers, users, and admins, so that the COPSU and ARPSI don't have to.



Architecture Document

Policy Language Document

Requirements-Connected-To-Use-Cases

User Attributes: Policy & UI Designations (aka "Taxonomy")

CAR & OIDC/OAUTH: Integration Discussion

CAR Architecture In-Depth (PDF diagram)

Please see the Scalable Consent site.