



CARMA:
Consent-Informed Attribute Release
Manager

Key points - Consent-Informed Attribute System (CAR)

- Serves attribute release and consent needs across all protocols – OIDC and OAuth as well as Shib/SAML.
 - Integrates institutional and individual choices for attribute release
 - Support for user consent decisions that are informed, effective, revocable, accessible, etc.
- Integrates nicely with Shibboleth v3 IdP, replacing v3 attribute policy editing and end-user consent modules.
- Catalyzed by multi-year NIST grant to Internet2 and now a TIER component
- Will be available as a solid TIER component – already HA, already Dockerable. Scheduled to go through alpha/beta/1.0 over the next 6-12 months. Duke has a go-live date of July 1 with over 2000 SP's.
- Device and browser independent. In fact, device adaptive. Works well with mobile apps.
- UI/UX well researched (CMU, Duke) and well-designed (Duke) and well-implemented (Duke). Includes
 - Fine-grain controls on attribute release (down to value level of multi-valued attributes), explanations, re-consent options, friendly names and values, etc.
 - User self-serve for bulk management, revocation, etc.
 - i18n and locale adaptive.
- Depends on informed content as user fuel for consent

Kim Cameron's Laws of Identity

Kim Cameron's Laws of Identity

1 User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

2 Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3 Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4 Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 Human Integration

The universal identity metasytem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7 Consistent Experience Across Contexts

The unifying identity metasytem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.



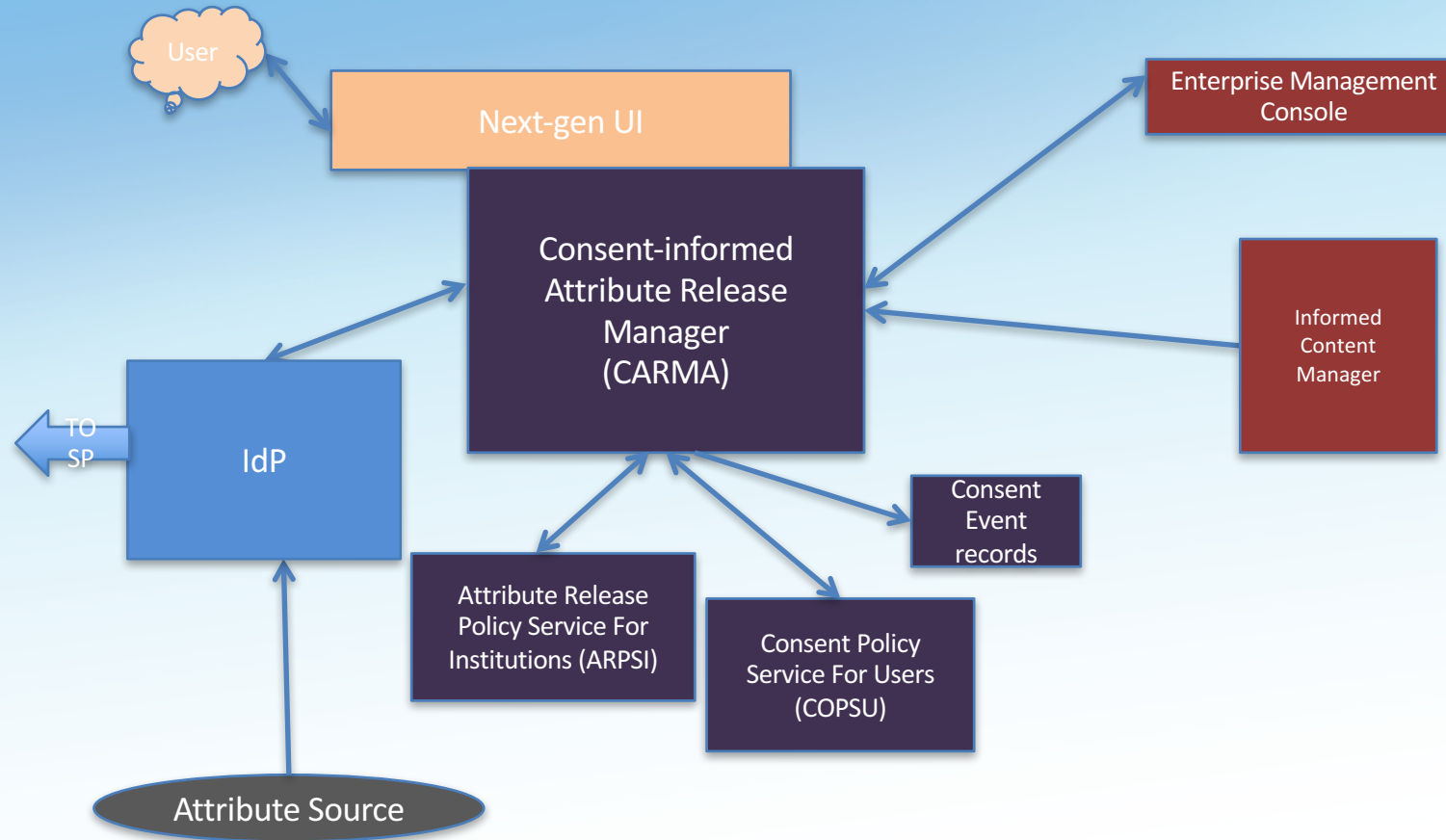
Flickr: Allatan

[Download](#) the poster. [Read the explanation](#) of the Laws of Identity.

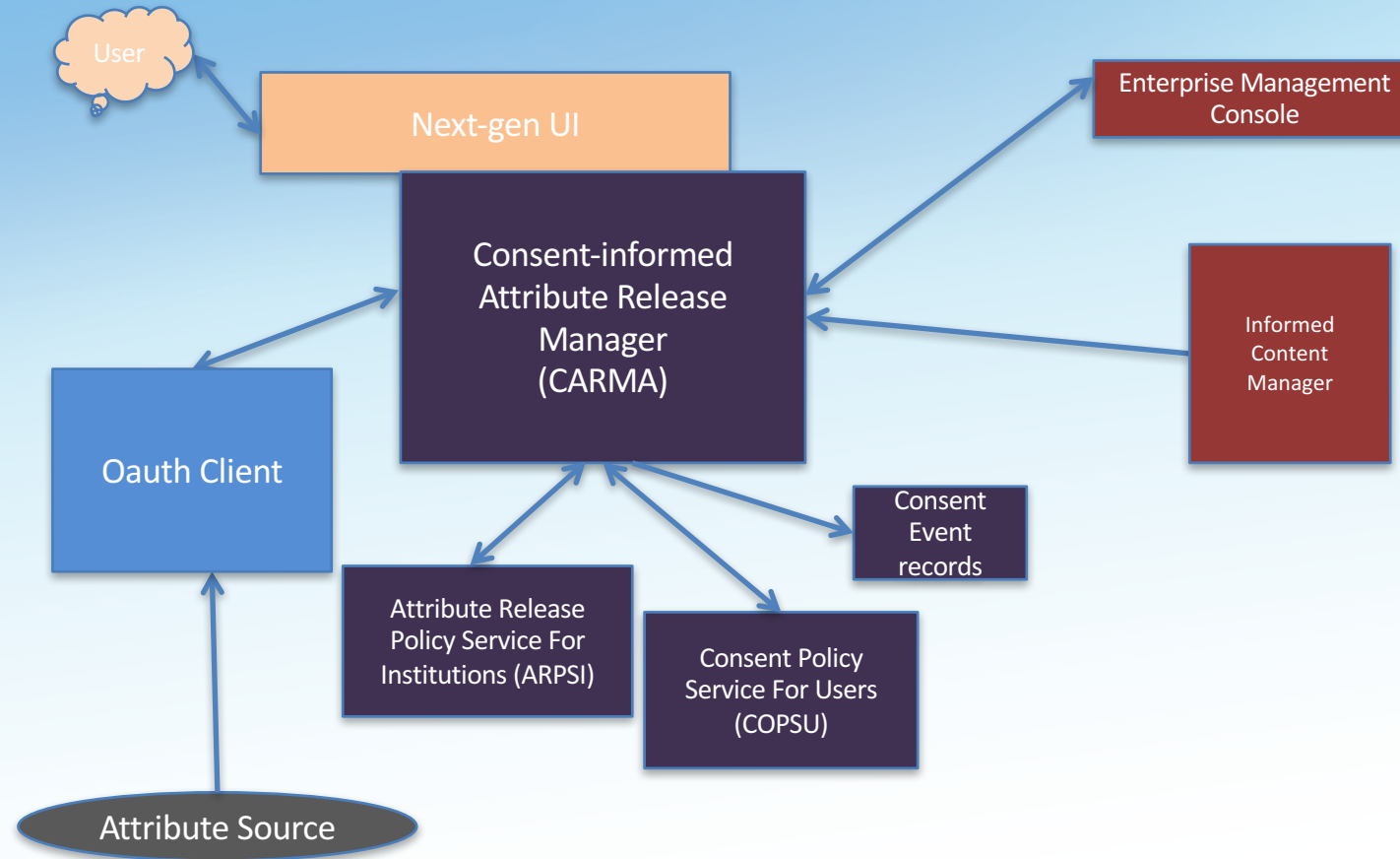
Consent-Informed Attribute Release Manager (CARMA)

- CARMA is the entryway for organizations and users to manage attribute release; applications invoke CARMA to get consent and attributes or information items.
- CARMA is instantiated as:
 - a published API (ICM API) and
 - HA code as a VM within a Docker container that implements the API
- Includes UI for end-users in a variety of use cases (in-line, off-line, persistent) and management UI for end-user self-service, policy administrators, configuration, etc.
- Includes admin and super-admin consoles
- <https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home>

CARMA in SAML flow



CARMA in OAuth flow



Getting the right user experience

- "You are what you release"
- Blind click through is not the goal; An informed and effective decision is.
 - Good first time dwell experience; good further suppression or revocation options
- Original next-gen interface designed by CMU Researchers in Usable Privacy
- Adapted and enhanced by Duke UI/UX group with iterative user testing
 - <http://people.duke.edu/~mkm16/projects/consent/>
- Some surprising results
 - Users understand what's happening
 - In both US and European testing, users show interest in controlling consent

CARMA opening up new capabilities

- Consistent, informed user experience across a variety of platforms and protocols
- Integration of institutional and individual attributes
 - Location
 - Emergency contact and medical information
 - Personal schedules
- Teaching students how to manage their privacy
 - Well-designed approaches appear to be well-received
 - By shaping their expectations, we help them shape a marketplace
- 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

What is Informed Content

- The fuel that drives effective and informed user consent decisions
- 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
 - Far-reaching insights - <https://arxiv.org/abs/1608.05661>

Sources and needed functions

- Sources
 - SAML metadata
 - Well-known URI's
 - Resolvable attributes
 - Publish and subscribe mechanisms
 - OIDC metadata statements
 - Others might work as well
- Functions
 - Attribute names and values translations
 - Message code support

CARMA UI Localizations

- Skinning, language and “locale”
- Attribute name and value translations
- Explanatory dialogues (privacy policies, local recommendations)
- Informed Content API-based services
- Special attribute handling
 - <http://www.commonaccord.org/index.php?action=doc&file=Wx/eu/europa/eur-lex/GDPR/PrivacyPolicy/Form/0.md>