Consent-informed Attribute Release (CAR): Fixing the Attribute Crisis

IAM Online – June 28, 2017

Rob Carter, Duke University

Ken Klingenstein, Internet2

Topics

---- Ken ---------

- The problem set and resulting requirements
- The Scalable Consent work
- The CAR architecture – a brief look under the hood and at the two UX
- Positive outcomes
- CAR Management capabilities – how it performs

---- Rob ---------

- Demos
  - CIlogon – key national cyberinfrastructure and an attribute responsive app
  - LIGO wiki – an international collaboration
  - User managing their consent choices
- The Duke experience

---- Questions ---------

The Problem Set

- A growing set of federated identity challenges
  - Attribute release for R&S and other needs
  - GDPR, the EU privacy regulations
  - Institutional desires for transparency
  - Serving other consent needs, such as in Oauth and OpenId
  - Providing the capstone UI for federated identity – the original placemat
- Results in a set of requirements that motivates CAR
  - Consent-informed attribute release as a 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
- Passed in 2016, becomes operational May 25, 2018.
- 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 actions, etc.
  - Specifies when consent is not to be used, when it should be used, the quality of the consent, etc.
- It affects many, perhaps most, US institutions.

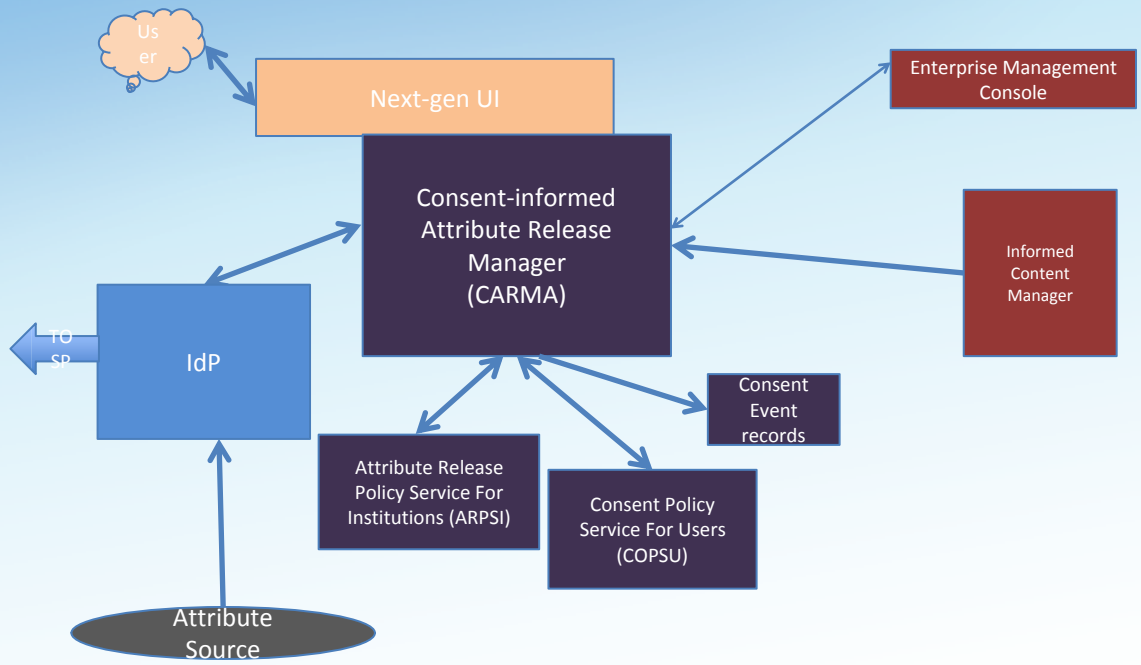
Scalable Privacy

- Multi-year grant by NIST to Internet2 as part of the NSTIC program
- Built on the approach of generalizing the R&E approach to federation and attributes e.g. MFA, citizen schema, fine-grain attribute release, scalable consent, etc.
- Helped drive MFA adoption in R&E
- Catalyzed CAR (Consent Informed Attribute Release)
- May have had influence on the plenary of NSTIC (IDESG) and the revised NIST 800-63 series
- https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home

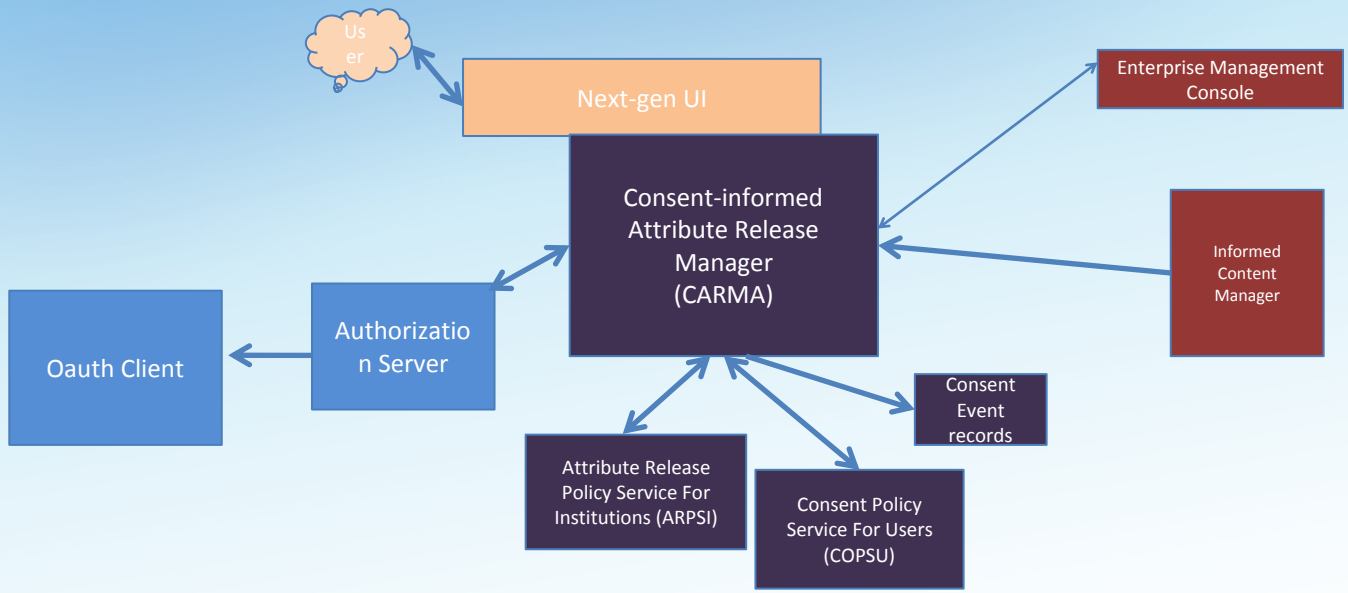
Consent-Informed Attribute Release (CAR)

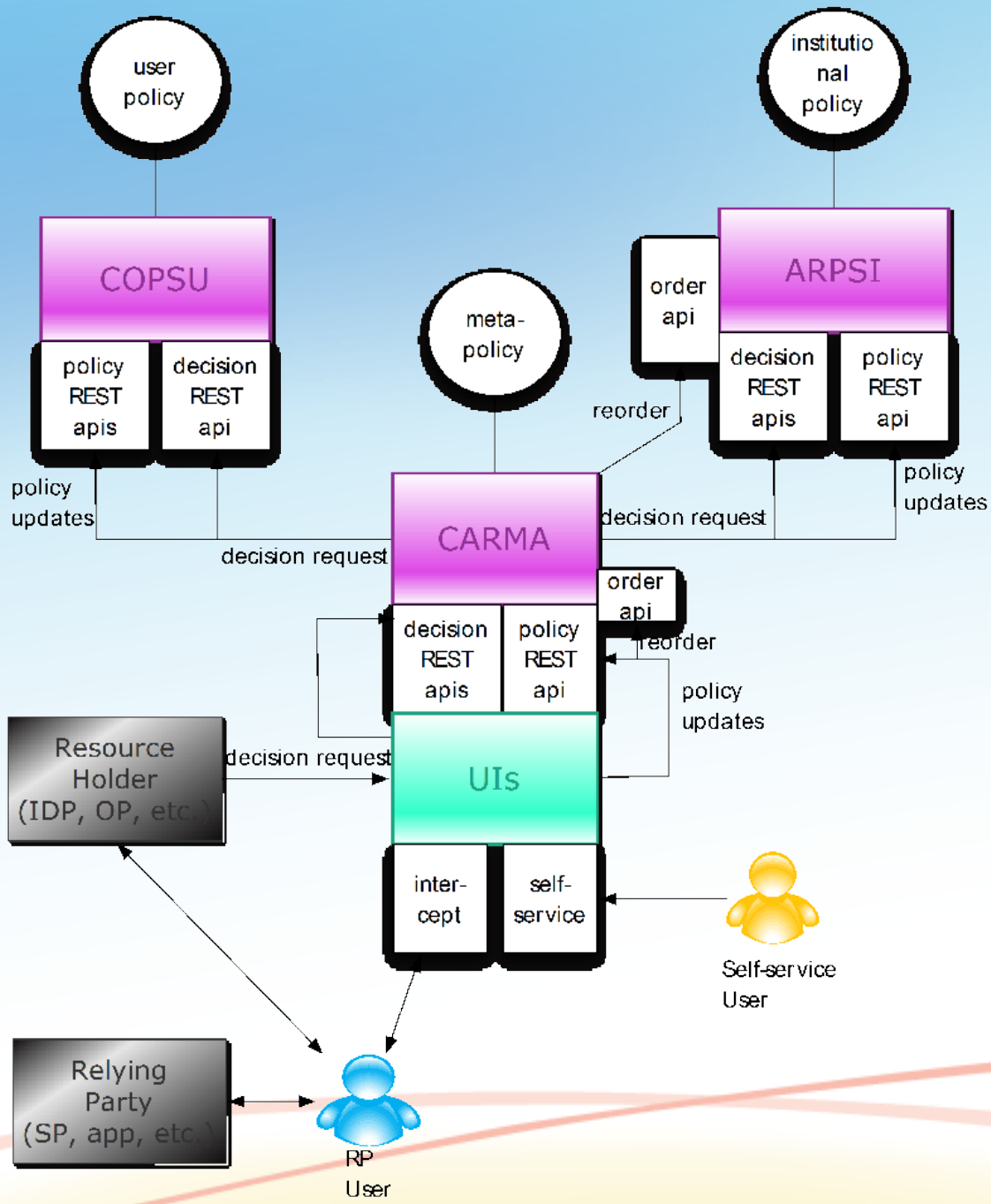
- A system of components that serves attribute release and consent needs across all protocols – OIDC and OAuth as well as Shib/SAML.
  - Integrates organizational and individual choices for attribute release
  - Support for user consent decisions that are informed, effective, revocable, accessible, etc.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

Under the hood: CAR in SAML use



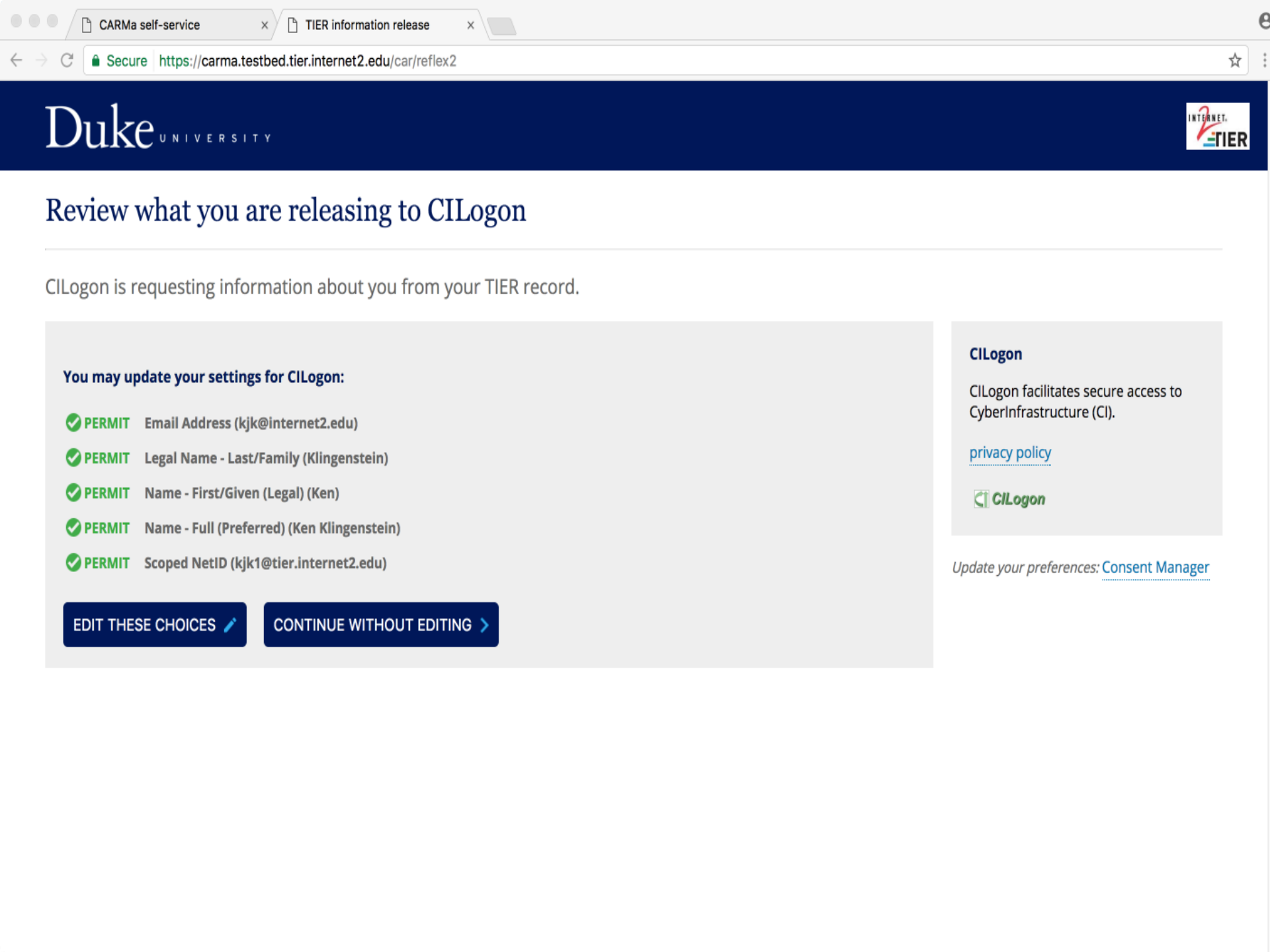
Under the hood: CAR in OAuth use




user policy
institutional policy
COPSU
policy REST apis
decision REST api
meta-policy
order api
ARPSI
decision REST apis
policy REST api
reorder
policy updates
decision request
CARMA
order api
reorder
decision REST apis
policy REST api
policy updates
Resource Holder (IDP, OP, etc.)
decision request
UIs
inter-cept
self-service
Self-service User
Relying Party (SP, app, etc.)
RP User

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 again
  - Self-service – users manage their set of consent policies, including revocation, templates for new sites, and “while I’m away” options


CARMa self-service
TIER information release
Secure https://carma.testbed.tier.internet2.edu/car/reflex2
Duke UNIVERSITY
INTERNET2 TIER
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@internet2.edu)
PERMIT Legal Name - Last/Family (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
CILogon
Update your preferences: Consent Manager

Secure https://carma.testbed.tier.internet2.edu/car/reflex2

Review what you are releasing to CILogon

CILogon is requesting information about you from your TIER record.

What would you like to release to CILogon?

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

Hide -

Choose one:

- (•) Save my choices; don't show me this screen again unless necessary.
- ( ) Save my choices, but show me this screen next time.
- ( ) Don't save the choices I made just now. Show me this screen next time.

CANCEL X ACCEPT AND CONTINUE >

CILogon

CILogon facilitates secure access to CyberInfrastructure (CI).

privacy policy

CILogon

Update your preferences: Consent Manager

CARMa self-service | https://carma.testbed.tier.inter

Secure https://carma.testbed.tier.internet2.edu/car/carma/selfservice

Duke UNIVERSITY

INTERNET2 TIER

My Sites

logged in as kjk1@tier.internet2.edu

Manage what information will be shared with these sites:

TIER

Name	URL	Updated	
CILogon	cilogon.org	05/30/2017	manage
G??ANT Service Provider Proxy	terena.org	05/01/2017	manage
Internet2 Collaboration Wiki Spaces	spaces.internet2.edu	05/18/2017	manage
LIGO Wiki	wiki.ligo.org	05/02/2017	manage
TIER CARMA	carma.testbed.tier.internet2.edu	06/15/2017	manage

New Site Policy

Manage defaults for what information is shared with new sites

Duke UNIVERSITY

Manage information sharing for CILogon

Information Requested by CILogon

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

Attribute	Current Value	Current Choice	Duke Recommends
Name - Full (Preferred)	Ken Klingenstein	permit	permit
Scoped NetID	kjk1@tier.internet2.edu	permit	permit
Name - First/Given (Legal)	Ken	permit	permit
Email Address	kjk@internet2.edu	permit	permit
Legal Name - Last/Family	Klingenstein	permit	permit
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

EDIT CANCEL

CILogon

CILogon facilitates secure access to CyberInfrastructure (CI).

privacy policy

Policy History

Updated: 05-30-17 09:46:16 AM

Policy Version: 5

CILogon

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

Positive 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

Status and Next Steps

- HA, packaged in standard TIER Docker containers. Scheduled to go through alpha/beta/1.0 over the next 6-12 months. Moving from NIST supported down the path towards TIER support.
- 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 code is in pre-production stage.
  - Central functionalities implemented and tested
  - End-user UI under tweaking; admin and superadmin UI under development
- An operational version is available now for demos. A dabble version should be available by late summer. A deployable version should be available by TechEx, but expect the usual chop at that point

Organizational Management for consent

- Policy administration tool
  - Will allow editing of organizational attribute release policies within a decentralized authority environment.
  - Aimed at use by policy administrators, sysadmins of SOR
- 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
  - Can have additional layers of security
  - Aimed for use by IdP/CAR sysadmins and Resource Server (OAUTH/OIDC) admins

Organizational Management for consent

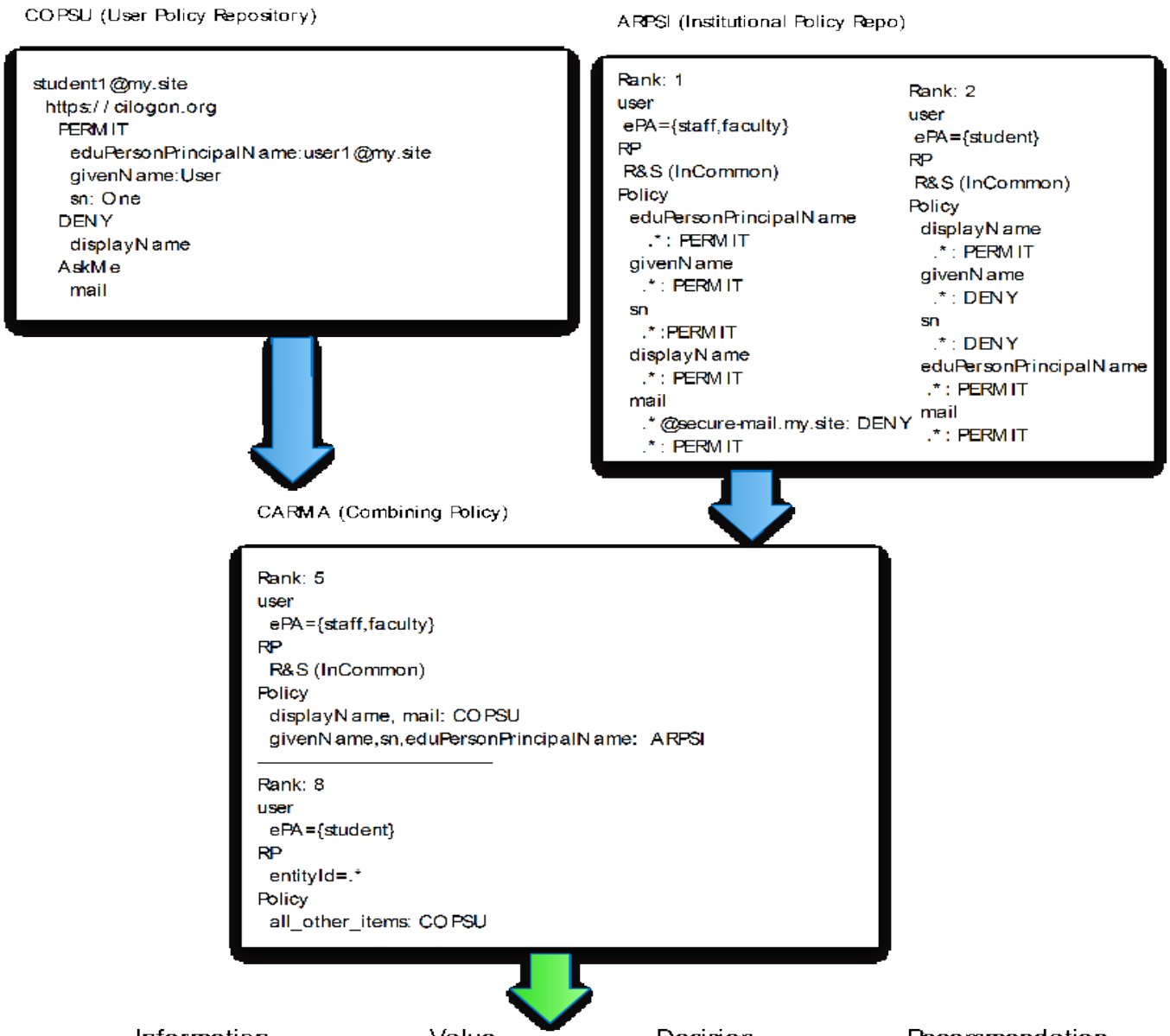
- Migration/maintenance toolkit
  - Repeatable mining/updating of informed content from SAML metadata
  - Generate “starter policies” from IDP configs (attribute-filter.xml)

Managing how to serve R&S and other release needs

- Sample R&S policy:
  - Faculty: Release by default to R&S RP; inform once; provide revocation options
  - Students: Use consent, with recommendations set by the institution
    - Recommendations can vary by student role, group membership, etc.
    - Provide management and revocation options
- 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."

Managing how to serve R&S and other release needs

- 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



Information	Value	Decision	Recommendation
UserName	student1@my.site	PERMIT	PERMIT
First Name	User	PERMIT	DENY
Last Name	One	PERMIT	DENY
Preferred Name	Yullie One	DENY	PERMIT
Email	123@my.site	ASK	PERMIT

Additional information

- Web sites –
  - CAR
    - https://spaces.internet2.edu/display/CAR/CAR%3A+Consent-informed+Attribute+Release
  - Scalable Consent
    - https://spaces.internet2.edu/display/ScalableConsent/Scalable+Consent+Home
  - TIER
    - https://spaces.internet2.edu/display/TWGH/TIER+Working+Groups+Home
- The CAR Team – Marlena Erdos, Rob Carter, Mary McKee, Ken Klingenstein

Evaluate Today's IAM Online

https://www.surveymonkey.com/r/IAM-Online-June-2017

24

2017 Technology Exchange

October 15-19, 2017

San Francisco, California

Note the Trust and Identity Track runs through *Noon Thursday, October 19*

https://meetings.internet2.edu/2017-technology-exchange/

25