opencapereo2013

Serving the Academic Mission

Internet2 Scalable Privacy project update

Agenda

- Introduction
- Overview of NSTIC & Scalable Privacy
- Key Deliverables & Example Use Cases
- Promotion of multi-factor authentication (MFA)
- Citizen-centric attribute work
- Privacy Manager
- Anonymous Credentials
- Metadata, trust, attribute bundles and certification marks (attribute ecosystem)
- How to stay informed

Introduction

- Mike Grady
  - For this talk, Coordinator/Project Management with the Internet2 Scalable Privacy project, assisting Ken Klingenstein (Internet2 and the Primary Investigator on the grant funding this effort) as needed. (Contract with Unicon)
  - Senior IAM Consultant with Unicon

Overview: NSTIC

The National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative is a "White House initiative to work collaboratively with the private sector, advocacy groups and public-sector agencies" with the goal of advancing the "NSTIC vision that individuals and organizations adopt secure, efficient, easy-to-use, and interoperable identity credentials to access online services in a way that promotes confidence, privacy, choice and innovation." The Internet2 Scalable Privacy Project (**ScalePriv**) is one of five pilot projects to receive funding from the first round of pilot funding in September 2012.

Overview: Scalable Privacy project

Objective: Help create the key components needed to build an authentication and attribute ecosystem that supports privacy in access control and transactional use cases through the following key elements:

- Multi-factor Authentication (MFA) deployment in Higher Education
- Citizen-centric attribute work
- Privacy manager for attribute release, authorization settings, etc.
- Integrated use of anonymous credentials at scale
- Work in metadata, trust, attribute bundles and certification marks

Overview: Scalable Privacy

- Two year grant (second year pending) to Internet2/InCommon
- Actually, a “Cooperative Agreement” with NIST
- Key partners include:
  - Internet2 and InCommon
  - Developers at CMU (Privacy Manager), Brown U (Anonymous Credentials), U Wisconsin-Madison (Citizen-centric work)
  - Three (3) primary pilot institutions for MFA deployment: University of Texas System, MIT, University of Utah
  - 35+ institutions in the MFA Cohortium
  - A lead set of institutions to advise and test components, individually and integrated (still to be assembled)
  - Internationalization and standardization via Kantara, Refeds, ISOC, etc.

Key deliverables

- Promotion of two factor authentication
  - Good privacy begins with good security
- Citizen-centric attribute activities
  - For transactions, for accessibility, for social government
- Privacy Manager
  - Build tool for user consent for attribute release based on research
  - Put the “informed” into informed consent
- Anonymous credentials
  - Special credentials issued by attribute authorities that allow for minimum disclosure of attributes of bearer
  - Integrated at key junctions into the ecosystem, leveraging existing infrastructure, working out policy, mobility, software issues
- Trusted metadata, promotion of attribute bundles and certification marks, and pushing policy issues

Example Use Cases

- This user has authenticated with multiple types of factors/"strong authentication".
- The holder of this credential has the following preferences for presentation of the content on this device.
- The holder of this token is a registered citizen, living in a specific precinct, with permits issued for activities such as parking/shared cars, zoning exceptions, etc.
- This user has been presented a clear and understandable summary of the personal data they are about to release and how it will be used by the service requesting that data.
- Is the user associated with this token over 18? (legal age) Is the user between 11 and 13? (entrance into COPPA-compliant sites).
- Is the user associated with this attribute a resident of dorm? Does the holder of this attribute attend University X?

Example Use Cases

- With your paper diploma and your identity-rich e-transcript, you get issued an anonymous token asserting affirmation of graduation and degree, year, honors, major.
- A user, in their context as a worker, uses a privacy manager to release anonymous credentials (such as security clearances and personal medical information) to third party contractors.
- A parent uses a privacy manager to manage their children's on-line privileges to COPPA-compliant applications.
- The holder of the token is a certified first responder with special training in a specified set of skills.
- A user, in their context as a citizen, uses a privacy manager to release sufficient residence information that allows them to then anonymously post to the neighborhood-only wiki.
- Does the user have a security clearance of level at least X?

Promotion of multi-factor authentication (MFA)

- Good privacy begins with good security
- MFA addresses a significant number of security threats
- A variety of second factor alternatives are now viable – USB devices, NFC devices, cell phones, certificates, etc., and technology can bridge across them
- Advantages of MFA and Federated identity
  - Combining MFA with WebSSO and federated identity allows MFA to be leveraged by many services/SPs
  - If biometric factors are used, “privacy spillage” limited to IdP
  - Can help achieve higher levels of assurance

MFA: Two major thrusts

- MFA Pilot Institutions: help support wide-scale deployments of MFA technologies at three institutions:
  - Massachusetts Institute of Technology (MIT)
  - University of Texas System
  - University of Utah

- MFA Cohortium: Create and facilitate a cohort of additional institutions, establishing a collaborative environment for sharing questions, requirements, planning, expertise, experience, artifacts, etc. related to deploying and supporting MFA, leveraging the pilot institution activities.

The MFA Pilot Institutions

- Project funds Duo licenses for wide-scale deployment
- Diverse environments, services, planning approaches, deployment approaches, etc.
- Pilot deployment plans include a focus on integration of MFA into federated identity and SSO environments (Shibboleth IdP, CAS).
- The broader outcome of this work will be documents, artifacts, and possible presentations of deployment experiences for the solutions utilized
- Some deployment has begun, hope for widespread use by Spring 2014
- Technology work enabling flexible MFA use with Shibboleth (& CAS) beginning Summer 2013 and completing before end of year (and to be MFA technology agnostic)

Expected MFA Pilot Outcomes

- Support for flexible MFA integration with the Shibboleth IdP and CAS
- Planning documents
- End-user experience
- Observed risks
- Performance impacts and scalability
- Lessons learned
- Issues specific to the use of MFA within an identity federation
- Recommendations for future deployments by other institutions

The MFA Cohortium

- A focused and facilitated initiative to help scores of institutions move along with multifactor authentication
- Experiences and artifacts from pilot institutions will provide one key source of input into the Cohortium
- Comprehensive approach
  - Technology and Policy
  - Deployment and Maintenance
- Large scale but finite length initiative (15 month)
- MFA technology agnostic
- Project provides facilitation & collaboration environment

The MFA Cohortium (continued)

- Collect and create extensive set of resources and artifacts on “all things MFA planning and deployment” for Higher Ed
  - Plans, ROI, Rollout Strategies, etc.
  - Critical code contributions (e.g. Shib and CAS login handlers, InCert)
- Build public web site to serve as lasting (and hopefully living) resource site
- 35+ institutions, first meeting was May 29, 2013
- Door is still open for more schools to join

Citizen-centric attribute deliverables

- Schema Catalog and Attribute Registry
  - Version 1.0 February 2013; expand and enhance over course of project
  - Browsable/searchable schema and attribute reference
- GPII Proof of concept
- Attribute annotated Use-Cases
- Cookbook “To Serve Citizens” ☺
- Engagement with the privacy manager
- Bindings and refactoring

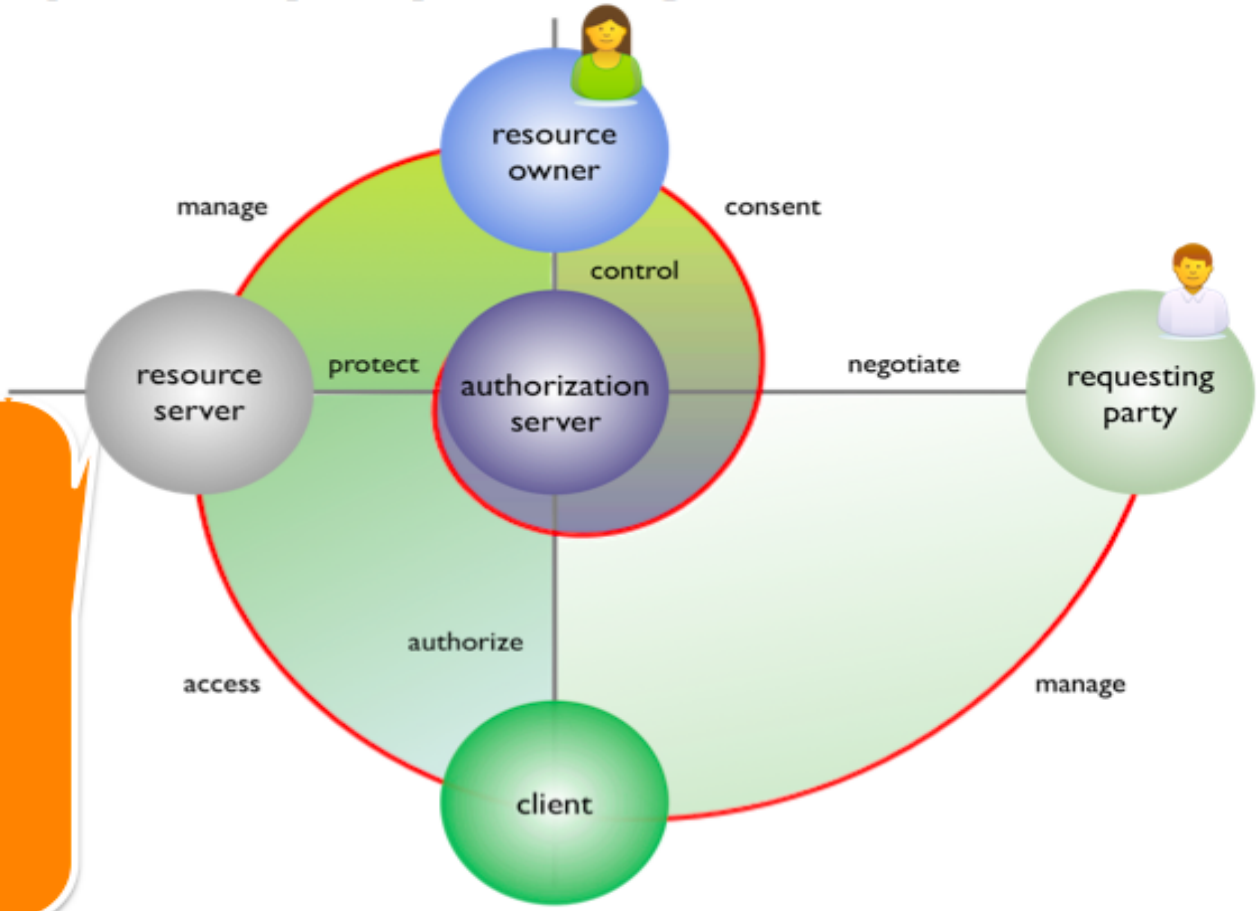
GPII Proof of Concept

- Collaborate with the Global Public Inclusive Infrastructure (GPII) project, whose purpose is to ensure that everyone who faces accessibility barriers due to ***disability***, ***literacy***, ***digital literacy,*** or ***aging***, regardless of ***economic resources***, can access and use the Internet and all its information, communities, and services for education, employment, daily living, civic participation, health, and safety
- Automatic personalization of user interfaces and user context adaptation based on user preferences, across platforms
- Schema standard is AccessForAll (ISO/IEC JTC1 24751)
- Proof of concept will establish user preferences stored in an authorization server being used with open credentials to adaptively present content

GPII Proof of Concept

- **Case Study: Management and Sharing of Personal Accessibility Needs and Preferences: http://tinyurl.com/cn48bgl**
- Madeline's campus supports tools/wizard to build content presentation preferences profile (AccessForAll), and store on UMA Authorization Manager (AM)
- Madeline can control access rights to her AM-hosted profile
- She has color blindness, impaired fine motor control, and impaired hearing
- Her modal logic class is using eText book, and she'd like relevant presentation preferences made available to adjust presentation of the eText
- Campus could release attribute identifying location of her profile on AM
- eText service then communicates with AM under appropriately controlled access to obtain and act upon relevant preferences

UMA turns online sharing into a privacy-by-design solution



- Historical
- Municipal
- Financial
- Vocational
- Artistic
- Social
- Geolocation
- Computational
- Genealogical
- Biological
- Legal
- ...

Citizen-centric milestones & timelines

- Pilot user-managed delivery of GPII/AccessForAll information supporting accessibility needs and preferences, April 2013 – August 2013
- Demonstrate end-to-end support for GPII, August 2013 through Spring 2014.
- Guidance on handling attribute ecosystem aspects of selected use cases in the citizen to government (local, state, federal) and other civic spaces, Spring 2013 and through duration of project
- Publish training materials to disseminate good practices: "Building Services that Address Privacy and Accessibility by Design" by Fall 2014. ("To Serve Citizens").

Attribute-annotated use cases

- Use cases often focus on a transaction level description and don't address/identify details about the attributes involved etc.
- Example: https://spaces.internet2.edu/x/qwROAg
- Attribute annotation will ask/identify questions such as:
  - Attributes/claims RP needs, and the categories of those attributes
  - Who are the Attribute Provider(s)?
  - What if attributes not available?
  - Does the user have a say in whether RP gets the attributes
  - Will RP accept the attributes without further verification?
  - If not, who would RP expect to verify?
  - One-time only, or can RP ask for them again? Is user in that loop?
  - Is anonymity, unlinkability, and/or unobservability required?
  - Protocol stack, bindings, what's in-band vs. out-of-band vs. dynamic

Categories of use cases for annotation

- Accessibility
  - Physical, cognitive, age-related, etc.
  - Global Publically Inclusive Internet (gpii.net)
- Operational Government
  - Transaction based, May be out of scope
- "Social Government"
  - Community wikis, on-line discussions, news feeds, etc.
  - Generally local in nature, often requiring anonymous but attribute-controlled access (e.g. resident, registered voter, over legal age, etc.)
- Envision It Scenarios
  - Contained in Full NSTIC Strategy (April 2011)
- UMA developed
- IDESG provided

To Serve Citizens

- Publish training materials to disseminate good practices: “Building Services that Address Privacy and Accessibility by Design” by Fall 2014.
- A guide to using the materials, including an overview of the major schema and attributes, methodology for annotating use cases, approaches to extensions and good design considerations for subspaces, etc.
- Materials on how to build an online service that addresses privacy and accessibility concerns by design
- Will be accompanied by outreach to relevant standard organizations and community organizations, such as ISOC, Kantara, IDESG, Refeds, etc.

Privacy manager (PM)

- Prof. Lujo Bauer of Carnegie Mellon University and their Center for Usable Privacy and Security, with help from central IT
- Consoles to help users manage the release of attributes
- Can leverage trust, informed consent, default settings and preferences, etc.
- Must be carefully engineered
  - Across the variety of contexts
  - Across a variety of credential types
  - In ways that are user-effective
- Set of leader universities to review design, drive policy, test and deploy

PM: Key design considerations

- Usability
- CMU Tech Report, Warning Design Guidelines, Bauer et al
- Fit into Shibboleth IdP as first deployment model
- Further studies on what users understand about privacy and controls over such
- Informed consent
- GPII
- Awareness of out-of-band considerations
- Minimal disclosure for constrained purpose

PM: Milestones & timelines

- Year one – basic research, development of basic PM
- Will also produce publications on user understanding of privacy and use and management of options to control access and sharing of personal information over the course of the pilot project
- Runnable prototype of PM by Fall 2013, Production version by end of 2013 (coding is just starting now)
- Year 2 – advanced research, feedback-based research, evolution of PM (spanning technologies) pilots
- Incorporate anonymous credentials, perhaps MFA, starting by end of 2013

Anonymous Credentials (AC)

- Special credentials issued by attribute authorities
- Allows for minimum disclosure of attributes of bearer
  - Over legal age; graduate of university in year X; resident; first-responder certifications; access to age-restricted services; etc
- Built on several similar technologies, including ABC4Trust (open source from IBM) and uProve (from Microsoft)
- Tamper-proof, Unobservable
- Long-time cool technology in search of use cases and modern enhancements (mobility, informed consent, etc.)
- Our work is being led by Brown University

AC: Milestones & timelines

- Year 1
  - technology evaluation and integration architecture development
  - use case development
  - start of creating working prototypes
- Year 2 – finish prototypes and test integrations and deployments

AC: Deployment Models

- Classic ABC4Trust, Idemix, etc.
  - Credentials held in a cert store on the user's desktop or smart card
  - RPs accessed via Web Browser
  - Processing done in User's desktop by previously downloaded plugins
- Enterprise-based
  - Credentials held in enterprise directory
  - Processing still done in desktop
  - Addresses mobility
  - May serve important enterprise needs
- Cloud-based
  - Processing and storage moved to the cloud
  - Addresses mobility issues

Metadata and trust implications

- At scale, there needs to be ways to establish and convey trusted information about applications and services to users
  - Implies "vetting" or auditing processes for services
  - Implies metadata that can convey this information in real time to users
  - Implies trust in the metadata
- Dynamic metadata services
  - Work is already underway on this in other places
- Federation operations need to evolve
- Auditing applications
  - For "privacy-preserving" approaches (minimal attribute requests, informed consent, proper handling and disposal, etc.), for COPPA compliance, for …
  - Prototype approaches are successful; market needs to grow

The Attribute Ecosystem

- Those parts of the identity ecosystem that focus on attributes in the ecosystem
- Centers on the creation, exchange and use of attributes associated with those in the identity ecosystem
- Critical to privacy, scalable access control, etc.
- Depends heavily on other aspects of the identity ecosystem, including authentication, trust, etc.
- The relatively unexplored part of the landscape.

Elements of the Attribute Ecosystem

(an evolving understanding)

- IdPs
- SPs
- Attribute authorities and providers
- Attribute verifiers
- Trust frameworks and trust framework providers
- Third parties, portals, etc.
- Federation operators
- Application auditors
- The user, and, if applicable, the subject

What Flows Within the Ecosystem

- Attributes
  - May be externally asserted (e.g. student, citizenship), self-asserted (e.g. preferred language), third party asserted (e.g. resident of a town), etc.
- Management of attributes
  - Trust, certification marks and vetted application information, user consent flows, etc.
  - Can flow as metadata or in-stream
- Others?
  - Liability,

Types of attributes (by authority)

- Enterprise/employer-asserted
- Self-asserted
- Reputation systems asserted
- Government asserted
- Third-party asserted
  - Business
  - Certification authority
  - Device asserted?

How to stay informed and participate

- The web site:

  https://spaces.internet2.edu/display/scalepriv
- Join the ongoing processes:
  - Track the Cohortium and start some local work
  - https://spaces.internet2.edu/display/mfacohortium
- Try the products when available:
  - CAS and Shib login handlers, InCert