



**Scalable Privacy:  
An NSTIC grant for the Identity  
Ecosystem**

# Scalable Privacy

- Grant Basics
- Key deliverables
- How the pieces fit together and create infrastructure

# Basics

- Part of the Identity Ecosystem initiative (NSTIC)
  - Governance – the IdESG
  - Pilots to inform and advance the ecosystem
  - Scoped to US but with global implications
  - <http://nist.gov/nstic/>
- Two year grant (second year pending)
  - Activity centers are Brown (anonymous credentials), CMU (Privacy Manager), Wisconsin (citizen-centric schema), along with a set of campuses for leadership in the spectrum of scalable privacy issues
  - A small group of MFA Pilots and a large scale MFA Cohortium
- Pilot is distinct from but actively engaged with IdESG

# Key deliverables

- Promotion of two factor authentication
  - Good privacy begins with good security
- Schema for common use
  - A user-manageable but broadly useful set of attributes
- Privacy managers
  - For users to control the release of attributes
  - Putting the informed into informed consent
- Implementing anonymous credentials at scale
  - Engineering into infrastructure privacy protecting technologies
- An attribute ecosystems and metadata strategies to support the above

# 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.
- Grant will support wide-scale deployments of different technologies at three lead schools (MIT, Utah, Texas) with harvesting of planning processes
- Facilitation will support a cohort of additional schools with their deployments, leveraging the lead school activities.

# The MFA Cohortium

- A focused and facilitated initiative to help scores of institutions move along with multifactor authentication
- Comprehensive approach
  - Technology and Policy
  - Deployment and Maintenance
- Large scale but finite length initiative (18 mo)
- MFA Technology agnostic
- Leaving behind key artifacts
  - Plans, ROI, Rollout Strategies, etc
  - Critical code contributions (e.g. Shib and CAS login handlers)
- Will leverage Net+ security service offerings where possible

# Privacy foundational elements

- Common attributes and schema
- Privacy managers
  - Controls the release of personal attributes
  - Spans user contexts
  - Relies on the trusted metadata for informed consent
- Trusted meta-data
  - About the relying party and the IdP
  - Vetted by the federation and by third-parties
- Anonymous credentials
  - Integrated at key junctions into the ecosystem, leveraging existing infrastructure
  - In software, use of metadata, and user experience
- Pushing policy issues

# The User and Roles

- A person operates in one of several roles when on-line:
  - As a citizen
    - At local, state and national levels
  - As a worker-employee
    - With other businesses, with governments, with consumers
  - As a consumer
  - As a physical entity
    - Geolocation, age, personal preferences, etc
  - Maybe one or two others
- In managing their privacy, what parts of the user experience should be consistent between roles and what may be different?



# Common attributes, schema and bundles

- A small set of attributes, organized into schema and bundles, that span the needs of a broad range of applications
- Primarily “citizen” oriented, but with significant value to many other use cases, including consumer and business.
- Intended to be user-manageable
  - Through privacy managers
  - With informed consent
  - Leveraging existing and emerging trust and security infrastructure

# Of contexts, credentials, and bundles



# Privacy managers (Carnegie-Mellon Univ)

- 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
- Similar, less leveraged approaches are successfully deployed in a few settings.

# Attribute authorities

- Entities that generate additional attributes about an individual (but do not provide other identity services)
- Examples include: Agencies (grant information, security clearances, etc) identifier services (ORCID, SSN, Driver's licenses, etc), auditors and compliance organizations, etc
- Many open issues exist:
  - Linking between attribute authority and {IdP, RP, third party, etc}, including LOA
  - Uni-directional or bi-directional, One time vs regular vs upon-change
  - Policy and contractual frameworks

# Anonymous Credentials (Brown University)

- Special credentials issued by attribute authorities
  - Encrypted at rest; reduces privacy spills
  - When queried by RP, will do minimal disclosure of encoded attributes
    - E.g. Over 18, True/False on specific sets of attributes, such as citizen, medical, IMBY discussions, etc.
  - Can be done so that IdP does not know either the values being released or the RP's requesting information
- Need infrastructure to support deployment at scale
  - Delivering credentials to user and storing, scalable query controls, audit, policy issues, integrating with privacy management

# 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

# Significant pilots and testbeds

- Intent is to facilitate significant deployments through:
  - Three partially supported leadership deployments of MFA at MIT, Texas, and Utah
  - Focus testing of privacy managers through development cycles
  - Identify and leverage existing IdM consortia to pilot, with active support and facilitation, both privacy managers and anonymous credentials
  - Create a broader cadre of observing institutions that participate in the planning and deploys, including attribute/schema development
- Work actively with related communities, from registrars to researchers, to help them understand the issues and opportunities

# How it all fits together

- A user, in their context as a university student, uses a privacy manager to release their institutional affiliation to student discount services
- 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.
- A user, in their context as a consumer, uses a privacy manager to manage the release of preferences (e.g. zip code, preferred language, geolocation, etc) to customize commercial services while preserving privacy
- 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