DHS Science and Technology Directorate
Identity and Access Management Engine

Technology Engines Context

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) launched a series of high-profile, high-impact Apex programs to look strategically at the nation's security and address future challenges while supporting today's operational needs. S&T Engines were created to meet cross-cutting needs for all Apex programs.

Impact and Vision

The Identity and Access Management Engine (IDAM-E) will help the Homeland Security Enterprise (HSE) enable identity and access management solutions via stakeholder engagement, problem identification, projects, and research and development (R&D) investments.

Description and Approach

IDAM-E will bring expertise, technologies, tools, capabilities and approaches from government (U.S. and international) as well as external scientific, technical, industrial and academic sources to bear on identity, cyber and privacy problems identified by the Apex programs, IDAM-E, and DHS components. When capabilities do not exist, we build them via investments in research, prototypes, etc.

Key Activities

- Leverage expertise and relationships that span the public and private sector to bring identity, information security and privacy capabilities to meet Apex program and HSE needs.
- Provide test-bed infrastructure and test and evaluation expertise to prototype, evaluate and validate technologies.
- Make R&D investments to close technology gaps in areas of importance to the HSE.

Engine Service Offerings

Expertise

- Subject matter expertise
- Ideation workshops
- Analysis of alternatives
- Mapping technology to needs

Testbed Infrastructure

- Prototyping
- Proof of concepts
- Technology validation

Research and Development Investments

- To mature technology
- To provide open standards
- To provide multiple implementation choices
- To encourage private sector investment priorities

Engine Competency and R&D Focus Areas

1. Authentication of people and non-person entities
2. Risk based confirmation of identity that leads to trust
3. Data and application security at rest and in transit
4. Access control at the point of need
5. User experience that incorporates security, privacy and informed consent

Key Successes

- **Technology identifies fraud in data sets while ensuring privacy of law abiding individuals.** IDAM-E worked with Rutgers University to develop a prototype of a privacy respecting screening capability to detect individuals, behaviors, areas, or data samples of high interest. It can be used to detect fraudulent activity on the web (relevant to the NGCI Financial Sector customers) and suspicious air travelers for high-risk screening based on their TSA relevant travel data.
- **Mobile credentialing technology that validates trusted credentials, enabling faster crises response.** IDAM-E collaborated on a mobile capability to present credentials ("I am a Doctor") at incident scenes, while assuring information security, the device it is deployed on, and the authority vouching for the information. The Next Generation First Responder program is interested in the technology and it has applicability to the trusted traveler re-engineering programs pursued by Customs and Border Protection. It also has wider HSE utility (e.g., delivery of benefits to veterans).
- **Secure Mobile Authentication to Physical Access Control Systems.** IDAM-E is developing technology to enable the usage of a credential stored within a phone over a secure NFC channel for physical access control. This capability can be used to ensure emergency responders and other authorized personnel can use their mobile device to authenticate themselves and have access to buildings and building control systems using technology they carry with them at all times.

Homeland Security
Science and Technology

To learn more about the S&T IDAM Engine, contact the IDAM-E@hq.dhs.gov

2017-06-08