Department of Homeland Security

Trusted Identity Exchange (TIE) Initiative

The Department of Homeland Security (DHS) consists of numerous different programs and agencies such as FEMA, TSA, US Borders and Protection Agencies, to name a few. Yet, federal employees, both old and new, needed basic access to the DHS network for email, facility control, training, and time and attendance systems. Granting secure access, while preserving a high level of access control, was tricky because employee identity and attribute data were scattered across the multiple different data repositories of the various agencies. **In order to provide fast and secure access, DHS needed a way to simplify its identity infrastructure.** The following description of their solution is based on the Privacy Impact Assessment for the DHS Trusted Identity Exchange.*

The Challenge

DHS's identity infrastructure was fragmented and not flexible enough to incorporate change. The existing process to add new employees required multiple paper forms to be generated and sent via email or faxed to a number of individuals who must then hand-enter Personally Identifiable Information (PII) from paper forms, or look up necessary information in other systems and copy and paste information into the systems for which the new employee needs access.

In addition, every internal system, or "consuming" application, uses a unique collection of the user's digital identity and credential data to manage access to protected resources, such as federally managed facilities, information systems, and data. Consuming applications may range from a physical building door reader to a computer connected to the DHS network, or to any application that resides on the DHS technical environment. Keeping a high degree of access control over this wide array of application types and points of entry presents a constant challenge to the DHS's IT personnel.

The Solution

To help aggregate all these identities for proper authentication and authorization for its consuming applications, DHS set up the Trusted Identity Exchange or TIE. TIE enables and manages the digital flow of identity, credential, and access-management data for DHS employees and contractors. The technology behind TIE is RadiantOne federated identity and directory service based on virtualization. It establishes connections to various internal authoritative data sources and provides a secure, digital interface to other internal DHS consuming applications, a 'one-stop-shop' of trusted information about the people that access DHS applications and data.

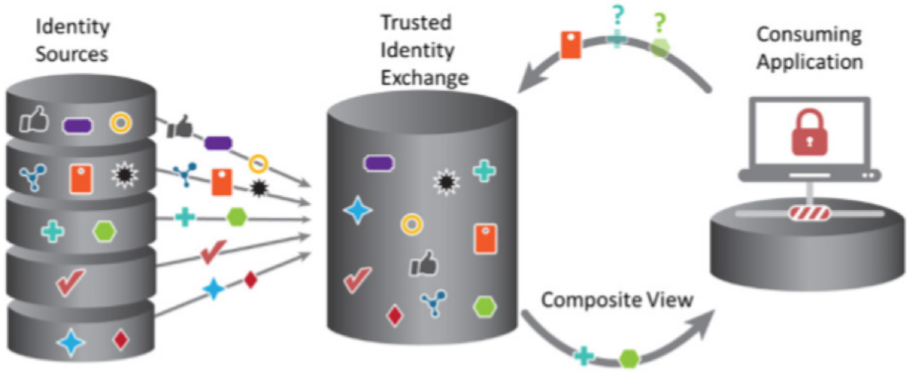

Figure 1: Graphical Overview of TIE Functionality

The Results

RadiantOne provides the integration layer for TIE that aggregates and rationalizes the data to create a central identity hub that contains all the identity data for each user. It can then produce the specific composite views required by each consuming application. RadiantOne supports many important consuming applications, such as SailPoint and TSA Pre-Check for DHS employees, making it a key enabler to many important DHS initiatives. These initiatives include the DHS Data Framework, Personal Identity Verification (PIV) Smart Card usage, Single Sign-On (SSO), and fine-grained authorization (also known as Attribute Based Access Control).

The following describe how TIE impacts each initiative.

DHS Data Framework

The DHS Data Framework is a scalable information technology platform with built-in advanced data security and access controls. TIE was developed to meet the DHS Data Framework access control requirements. As the technology behind TIE, RadiantOne brokers connectivity to the variety of authoritative identity data sources and integrates the information in a way that facilitates the authorization required by the Framework.

PIV Smart Cards

Federal employees and contractors are issued PIV smart cards, which are secure credentials, and are required for use to access federally managed facilities and information systems. For these smart cards to be used as required by policy, TIE is required to broker connectivity between PIV authoritative sources and consuming applications to create an association between a person's PIV card and the related user account on any given system. The data attributes and PII required to provision and de-provision access accounts and entitlements is often moved via emails, spreadsheets, comma-separated value (CSV) files, and sometimes via fax. When a person uses his or her PIV card to log-on to the DHS network (Windows), data about the PIV card must be provisioned to Active Directory (AD).

Previously, this was accomplished through a variety of manual processes, including several stop-gap solutions through which the provisioning took place well after a person's AD account was created. In some instances, more information than was necessary may have been transmitted between consumer and source systems to provision or de-provision access. These manual processes not only elevated the risk of exposing sensitive PII to unauthorized personnel, but also prohibit or hinder the efficient transfer of data required to securely grant access to users within the DHS infrastructure. As TIE, RadiantOne serves as the identity information broker required to support automation of PIV and all other access entitlement provisioning and de-provisioning, thus eliminating costly, inefficient business processes. This facet of TIE also mitigates privacy risk by reducing the risk of exposure when PII is passed via less secure email or paper-based processes.

Single Sign-On (SSO)

SSO enhances a user's PIV log-on experience by enabling seamless, "one-click" access to applications, following use of the PIV card to log-on to the DHS network. SSO reduces DHS's dependence on passwords for access to sensitive systems, while achieving PIV compliance. SSO enables an end-user experience that combines previously mentioned initiatives, such as PIV smart card usage, provisioning automation, and fine-grained authorization, and is a strategic initiative for DHS. TIE (RadiantOne) must be in place to support PIV, provisioning, and fine-grained authorization use cases to achieve the SSO user experience for all targeted applications.

Fine Grained Authorization

Fine-grained authorization (which sometimes materializes as ABAC) describes an IT system's ability to make a final access determination based on near real-time information from authoritative identity sources. Because DHS has numerous authoritative identity sources used by numerous consuming applications, TIE is necessary to provide a single interface (acting as a broker) for consuming applications to request the information required to make such a dynamic decision.

Thanks to RadiantOne and the TIE initiative, DHS simplified its identity infrastructure, enabling more efficient and secure operations and easier, more streamlined experience for its users, no matter which DHS-affiliated program or agency employs them.

About Radiant Logic

As the market-leading provider of identity virtualization solutions, Radiant Logic delivers simple, logical, and standards-based access to all identity within an organization. RadiantOne FID, our federated identity and directory service, enables customizable identity views built from disparate data silos, driving critical authentication and authorization decisions for WAM, federation, and cloud deployments. Fortune 1000 companies rely on RadiantOne to deliver quick ROI by reducing administrative effort, simplifying integration, and building a flexible infrastructure to meet changing business demands.

Contact Us

To find out more about Radiant Logic, please call us at **877.727.6442**, email us at info@radiantlogic.com, or visit www.radiantlogic.com.

*www.dhs.gov/sites/default/files/publications/privacy-pia-dhsall050-tie-february2018.pdf