

Federated Identity for Federal Agencies

Identity Virtualization Enables the Future, Respects the Legacy

Federal agencies face a major dilemma — how to meet future demands of the Continuous Diagnostics and Mitigation (CDM) program without impairing mission-critical legacy systems. For many agencies, identities are fragmented across a complex array of silos, and every new application or initiative requires significant integration into these legacy systems for user authentication and authorization decisions.

These agencies face challenges and opportunities:

- mandates for certificate-based strong authentication
- collaboration and information sharing around identity across agencies
- implementation of dynamic authorization, providing access only to needed resources

Identity Integration

Many agencies mandated to implement common access card (CAC), personal identity verification (PIV) or other certification-based strong authentication are scrambling to upgrade legacy systems needed to meet those standards.

Upgrading an existing identity system based on outdated authentication methods — such as usernames and passwords — to a

stronger, certificate-based method requires manually replacing user names and passwords with tamperproof identity attributes implemented by the certificate. This demands reaching into fragmented identity sources to create a common form of identity

“With identity-as-a-service, I can plug in my application and know that I will get the right data for authentication and authorization.”

– Dieter Schuller, Vice President, Sales and Business Development, Radiant Logic

representation, thereby integrating users' attributes and providing a global identity profile. This unified view forms the basis for single sign-on and, more importantly, granular authorization and access.

Without this unified view, end users wrangle with multiple usernames and

passwords, and agencies can't deploy the mandated strong authentication methods. Some users can't get access to the systems they need, while others get access to what they shouldn't have.


“When you build your own authentication and authorization functions into each application, things become even more siloed,” said Dieter Schuller, vice president, business development, at Radiant Logic. “Each new initiative involves an unanticipated project within a project, and identity integration becomes the roadblock to all of these new initiatives.”

Just Say No?

Overextending access rights is every cybersecurity pro's nightmare. Given the sensitivity of the material, granular authorization is a must-have in the federal sector. An overabundance of caution about access, though, can wall off functionality and cause unnecessary user delays.

“The easiest way to provide security is to simply say ‘no’ — and that is often what happens. People cannot get access,” Schuller said.

With fine-grained, dynamic authorization, policy engines ensure that users can access what they need at the right time — and nothing more. Modern authorization methods, such as ABAC, rely on a rich supply of user



attributes, objects and context to grant or withhold resources — and to reflect changes in the system as they happen. If critical user information is locked in silos, there's no way to build a complete picture of the user. Granular authorization becomes impossible.

Manage Globally, Act Locally

Today's systems may need to tap multiple identity sources — Active Directory, other LDAP directories, SQL databases, and other APIs and Web Services — to get to a single user's data. The RadiantOne federated identity and directory service (FID) uses a new approach to identity that consolidates and rationalizes disparate identity data, providing a single access point for authentication, authorization and information sharing projects.

The highly distributed environments of federal agencies require each agency to enforce security at the local level (acting locally) while delivering the identity data they own into a larger environment so it can be shared with another agency that needs it (managing globally).

Agencies must be able to quickly integrate disparate user populations and various aspects of a user's profile across different authoritative sources — and deliver identity-as-a-service to consuming applications and other agencies. This requires a platform that can connect to existing silos of identity, understand the local data model, create a common data model, and deliver (publish) the right data in the right protocol, schema and structure. It must have the ability to rationalize data and correlate/disambiguate the user across different systems to create a 360-degree view of each user.

“Today, when you plug in your computer, you know that you will get electricity from the wall outlet in the right wattage. When you plug in your phone, you know you will get a dial tone,” Schuller said. “With identity-as-a-service, I can plug in my application and know that I will get the right data for authentication and authorization.”

A Moving Target

Identity is a moving target. Emerging rules and changing technologies will necessitate changes in authentication and authorization methods and protocols. By abstracting and federating the identity function, organizations can create a core of identity that is flexible enough to deliver in whatever form an application needs.

“In a move to the cloud, IT just needs to take the virtualized image and configure it to match what is

expected by the cloud provider,” Schuller said. “You have a simple point-to-point sync that anyone can do, without lots of complex additional business logic.”

For IT leaders, this loosely coupled architecture enables new levels of agility, making it easier to build and deploy systems in response to emerging needs.

“When you virtualize and rationalize your existing identity silos, your identity consumers can go to one place instead of many places,” Schuller said. “Once you prove to application owners that they can consume identity-as-a-service, you've effectively freed them up to focus on the business aspects of the application. You've solved a problem for them.”

To learn more about a federated identity and directory service, visit www.radiantlogic.com

Moving Forward

Many government agencies are already using this approach.

- **The Department of Homeland Security (DHS)** has identity data scattered across multiple repositories: FEMA, TSA, US Borders and Protection Agencies, etc. To grant secure access while preserving a high level of access control, DHS set up a Trusted Identity Exchange or TIE based on RadiantOne. The solution provides a secure ‘one-stop-shop’ of trusted information about people who access DHS applications and data, allowing agencies to collaborate and share data and increase effectiveness, and respond more quickly in emergencies.
- **NIST's National Cybersecurity Center of Excellence (NCCOE)** is a public-private partnership for businesses and government agencies to address pressing cybersecurity issues. RadiantOne FID, a key component of its reference architecture for Access Rights Management (ARM) in the financial services sector, improves security, flexibility and speed in the identity infrastructure.