
Experts See Big Push Toward Cloud-Based Architectures, Enhanced Data Privacy


“Federal agencies are facing new Identity and Security challenges as they transition many workloads to cloud-based platforms,” said Gerry Gebel, President Axiomatics Federal, Inc. “Federal agencies require modern tools and techniques to protect sensitive digital assets, but also must appropriately share the right data across departments, across agencies and with citizens.”

Axiomatics Federal, Inc. security leaders compiled six trends government agencies should follow heading into 2020, including:

Moving Toward Cloud Hosted Data Systems
Federal agencies are migrating their data and other application resources to the cloud because cloud platforms provide simple, flexible and affordable data storage systems compared to legacy database solutions. Platform specific security capabilities may not be sufficient to address all requirements, particularly for agencies/departments that adopt a multi-cloud architecture. Dynamic Authorization implementations provide a common and consistent access model across and within cloud platforms.

APIs and Microservices Security
Leveraging microservices, service meshes and APIs to access sensitive or confidential data is now commonplace in government applications. Scenarios that require fine-grained access can utilize a comprehensive approach to access control by combining OAuth and Dynamic Authorization. Working together, OAuth and Dynamic Authorization enable the proper management and governance of access scopes and cleaner APIs that are not overloaded with security logic. Authorization deployed as a microservice is also an advantage for government agencies because it fits well within a DevSecOps process.

The Data Privacy Movement
GDPR set off a data privacy evolution globally when it went into effect in May 2018. Now government agencies across various states and countries are implementing laws with GDPR’s data privacy standards in mind. These new regulatory requirements drive organizations to implement new security controls that protect citizens’ privacy through a context-sensitive and risk-based access control model.

PKI transitions to OIDC?
PKI based authentication has been the mainstay for strong authentication in government applications for many years. The capability to cryptographically link user authentication and system access in an unbroken chain of custody is a capability where PKI excels. However, PKI technology is also associated with a high cost to acquire and maintain, is not easy for end-users, and is not flexible enough for many use cases.

“Going forward, we can expect to see more adoption of authentication capabilities based on standards like OpenID Connect (OIDC),” said Gebel. “OIDC is easier to implement, simpler to use and accommodates modern applications and use cases.
Zero Trust Network Access
The concept of Zero Trust is gaining momentum across the IT landscape. With Zero Trust, users and devices face stronger validation before being allowed on the network, replacing past mechanisms that granted broader access once someone was remotely connected to a network segment. In many ways, Dynamic Authorization is similar to Zero Trust in that every access attempt is validated against current access policies – and access policies can be specific to enable access only to the resources needed for a specific job function.

Bridging the IT Skills Gap
The IT skills gap across federal agencies makes it critical for government employees to understand how to utilize a variety of modern technologies to gain a competitive advantage. Take, for example, Identity and Access Management (IAM) tools. Leveraging different IAM tools requires diverse expertise for each one. Users need training to understand these tools and ensure that unauthorized users don’t access data. Organizations like IDPRo address this challenge by turning federal employees into digital identity professionals.

“As federal agencies modernize technologies and train employees, data security is a top priority. Managing and verifying who should have access to data is key to data security,” said Gebel. “By choosing technologies like Dynamic Authorization delivered with Attribute Based Access Control (ABAC), federal agencies can better disseminate and share actionable intelligence across agencies.”


About Axiomatics Federal, Inc.
Axiomatics Federal, Inc., a wholly owned subsidiary of Axiomatics Inc., is a U.S. company with offices in Reston, Virginia. The federal team works closely with customers and partners of the federal government to meet mission-critical access control needs with a policy-based approach delivery through externalized dynamic authorization management.

About Axiomatics
Axiomatics is the leading provider of fine-grained access control. Axiomatics' solutions are utilized by government agencies and Global Fortune 1000 companies around the world to enable digital transformation: share and safeguard sensitive information, meet compliance requirements and minimize data fraud. Axiomatics provides Attribute Based Access Control (ABAC) for applications, databases, Big Data, APIs and microservices. To learn more, please visit http://www.axiomatics.com or @axiomatics.
Contact Information
Derek Cnota
Axiomatics Federal Inc.
(630) 639-2456

Online Web 2.0 Version
You can read the online version of this press release here.