FedRAMP and DoD IL5 Solutions for Government

Cloud Identity for Federal Agencies

SOLUTION BRIEF

Old Technology Can't Support Your New Challenges

As your agency shifts to telework and cloud computing, you experience firsthand the limitations of legacy identity, credential, access and management (ICAM) tools. As you're tasked to secure access for your increasingly remote workforce and support connectivity with mission partners and other organizations, you realize that outdated identity security technology just wasn't designed for today's threat landscape. Nor can it support the increasing number of FedRAMP authorized cloud service offerings you may be adopting.

At the same time, the ever-present threat of bad actors looking to compromise government and private sector networks reveals growing gaps in agencies' federal Identity, Credential and Access Management (ICAM) programs. To address these new and evolving challenges, many agencies are moving towards a Zero Trust security posture in which you assume a state of breach, there is no implicit network trust and all access requests are verified based on dynamic context and risk. This transformation requires that you establish an identity-centric control plane for access security.

72% of government executives say that outdated IT systems are hurting their ability to respond to changing demands, and 79% say the age of their IT systems negatively impacts their mission.

Source: Modern Government: Connected. Powered. Trusted. KPMG, Feb 2021

Modern Identity Supports Your Mission-critical Requirements

Build the Foundation for Zero Trust Security

Zero Trust requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they're sitting within or outside of the network perimeter. Your workforce authentication authority from Ping delivers an identity control plane so you can secure access for every user population, asset, environment and endpoint across your hybrid, multi-cloud and on prem architectures.

Increase Cloud Adoption Flexibility

Not every cloud solution is a viable option. Ping's cloud identity and access management solutions are available on a DOD IL5, FedRAMP High Authorized environment, helping you secure, modernize and future-proof your hybrid IT environment according to federal standards. And if you leverage DevOps practices, Ping delivers cloud-ready containerized software that can be automated to deploy anywhere and everywhere across your multi-cloud, air-gapped, hybrid environment.

Prevent Identity Silos

Cloud shouldn't be viewed as a separate component of your IT architecture, and it definitely shouldn't require new cloud identities for your users. You don't need more identity silos; you need a single source of truth that gives you the ability to manage identities and access with a cloud identity control plane. Ping's cloud-based workforce authentication authority solution lets you break down the identity silos and overcome hybrid IT challenges.

Uplevel ICAM Initiatives

You already rely on PIV/CAC cards to strengthen authentication, but you need a way to expand their reach to secure every digital asset, especially those in the cloud. Your IT organization can accelerate work-from-anywhere and cloud initiatives by upleveling your federal ICAM/FICAM program with modern federation, identity management and access management from Ping Identity.

Ping Government Identity Cloud and Software Solutions

Welcome to a central authentication authority that empowers you to secure access for every user population, asset, environment and endpoint. Deployment options including cloud, software and hybrid give you the flexibility to modernize legacy without disruption, while FedRAMP High and DoD IL5 authorizations ensure compliance with all required security controls.

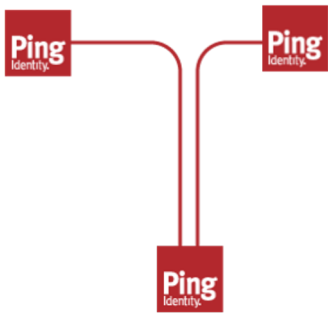
Identity, Credential and Access Management (ICAM)

Identity Management

- Streamlined identity management with efficient provisioning and deprovisioning of access
- Secured and personalized registration, login, and self-service journeys
- Detailed audit trails of all identity related activities

Credential Management

We integrate with authoritative PIV and CAC credential management data sources and can connect with automated identity and access lifecycle management systems. We also support standards-based verifiable credentials.



Federation

- Federated authentication and single sign-on
- Standards-based signed assertions (tokens)
- Adaptive authentication polices
- Pre-built adaptors

Access Management

- Centralized access security for web apps and APIs
- Comprehensive policy engine and session management
- Enforces authorized user access to the right resources
- Gateway and agent-based deployment options

Governance

- Access request workflows with automated provisioning
- Access review certification management
- Separation of duties checks and enforcement
- Analytics and Reporting

FICAM is the Federal Government's implementation of Identity, Credential, and Access Management (ICAM). ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives.

Get the latest FICAM Architecture at:
https://www.idmanagement.gov/arch/

Secure and Streamline Access for the Good of the Nation

Secure Remote Access

Your ability to provide secure and seamless access to digital assets from anywhere is mission-critical. With Ping, you can confidently ensure and enforce that the right people are accessing the right resources at the right time and for the right reasons.

Accelerate Cloud Initiatives

Abandon the notion that "cloud" is separate and requires new cloud identities. Embrace cloud-smart initiatives with an identity platform that keeps you in control, lets you manage access to all resources across your hybrid IT environment, and meet the federal government's required security controls.

Protect Every Mission-Critical Asset

Ultimately, all assets are protected by identity, and not just cloud ones. So it's critical to choose an identity security provider that can connect all your multi-generational assets, no matter where they're hosted, using out of the box standards and integration kits.

Lay the Foundation for Zero Trust and Passwordless

An authentication authority provides a solid foundation for a Zero Trust security posture, lessens password dependence and enables more secure passwordless authentication methods.

Learn more about Ping's government solutions today.