Ping Government Identity Cloud

Ping Government Identity Cloud is

FedRAMP High, IL5 Authorized

Ping Government Identity Cloud

DATASHEET

Ping Government Identity Cloud is a FedRAMP High, DOD IL5 authorized cloud identity and access management (IAM) solution for government agencies and suppliers that need to modernize their identity infrastructure in compliance with federal regulations. It provides federation, access management, authorization, and directory capabilities hosted in a fully managed, dedicated cloud environment with data and resource isolation. With our FedRAMP solutions, federal agencies and suppliers can facilitate secure access for federal employees, mission partners and citizens to all resources across their hybrid IT environments.

Key Features

- FedRAMP High, DOD IL5 authorized
- Based on identity standards
- Centralizes policy management for attribute-based access control
- Flexible federation hub
- Lightweight, scalable master user record
- Supports X.509 PKI certificates
- Stores structured and unstructured data
- Manages web and API access

Benefits

- Comply with federal regulations and mandates (e.g., FedRAMP, EO 14028, OMB M-22-09)
- Improve interoperability with agencies, mission partners and suppliers
- Integrate with existing ICAM infrastructures
- Secure access to all resources
- Optimize operational performance
- Decrease IT costs
- Extend your investment using standard operating procedures with the ability to deploy instances of this same cloud identity technology as software in on-premises, air-gapped, and hybrid environments

Workforce

Partner

Citizen

Ping Government Identity Cloud

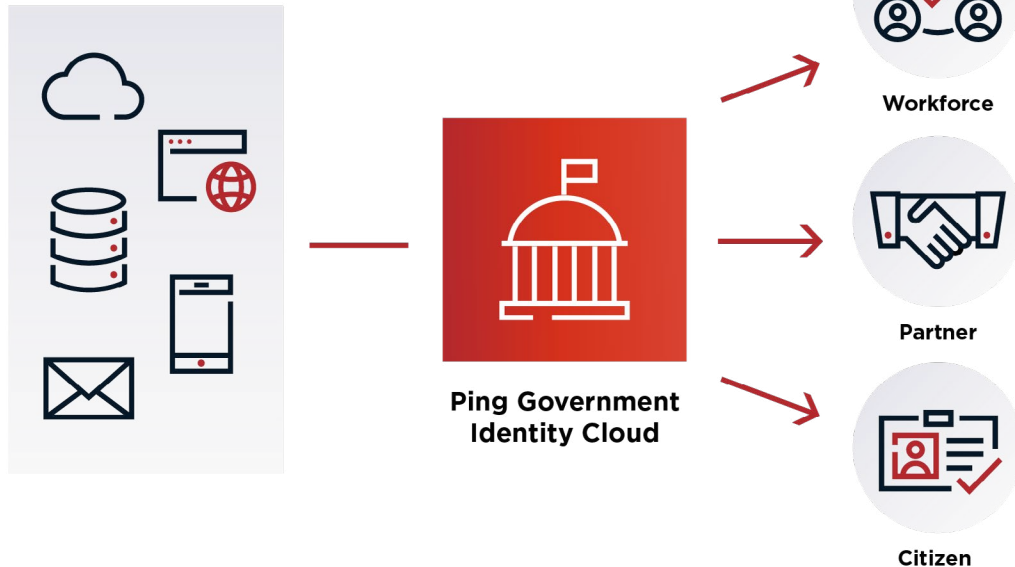**DATASHEET** — **Ping Government Identity Cloud**

Ping Government Identity Cloud

Ping Government Identity Cloud is a FedRAMP High, DOD IL5 authorized cloud identity and access management (IAM) solution for government agencies and suppliers that need to modernize their identity infrastructure in compliance with federal regulations. It provides federation, access management, authorization, and directory capabilities hosted in a fully-managed, dedicated cloud environment with data and resource isolation. With our FedRAMP solutions, federal agencies and suppliers can facilitate secure access for federal employees, mission partners and citizens to all resources across their hybrid IT environments.

Ping Government Identity Cloud

Workforce

Partner

Citizen

Key Features

- FedRAMP High, DOD IL5 authorized
- Based on identity standards
- Centralizes policy management for attribute-based access control
- Flexible federation hub
- Lightweight, scalable master user record
- Supports X.509 PKI certificates
- Stores structured and unstructured data
- Manages web and API access

Benefits

- Comply with federal regulations and mandates (e.g., FedRAMP, EO 14028, OMB M-22-09)
- Improve interoperability with agencies, mission partners and suppliers
- Integrate with existing ICAM infrastructures
- Secure access to all resources
- Optimize operational performance
- Decrease IT costs
- Extend your investment using standard operating procedures with the ability to deploy instances of this same cloud identity technology as software in on-premises, air-gapped, and hybrid environments

Proven Capabilities Delivered in the Cloud

Federation Hub

An enterprise federation server for user authentication and standards-based single sign-on (SSO). It serves as a global authentication authority that allows employees, mission partners and suppliers to securely access all the applications they need from any device, without the need to copy existing user data.

Attribute-Based Access Control (ABAC)

A centralized access security solution with a comprehensive policy engine.
It provides secure access to applications and APIs down to the URL level and ensures authorized users access only the resources they need.

Orchestration

A flexible, low-code adaptive integration framework to create cross-channel seamless identity experiences. Simply drag and drop flow connectors to achieve authentication experiences right for your organization and risk thresholds.

Lifecycle & Relationship Management

Automated identity management that helps with onboarding and account claiming to provision the right user access at the right time and to quickly disable accounts that are no longer needed. Serve your evolving needs with flexible identity data models and custom relationships between objects.

Identity Governance & Administration (IGA)

Streamlined access request, access review, and segregation of duties allows organizations to quickly grant the right permissions/entitlements, prevent inappropriate access, and comply with a complex web of regulations.

Phishing-Resistant MFA

A secure authentication method with adaptive policies for countering phishing attacks. It ensures that users are verified through multiple layers of protection, with a diverse set of use-cases including onboard, progressive profiling, and passwordless authentication.
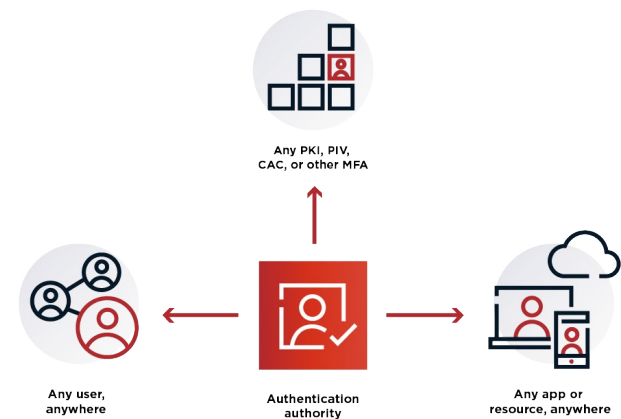
Master User Record

A high-performance, scalable directory for identity and rich profile data. It allows enterprises to expose a master user record to all applications, manage millions of identities and billions of attributes and protect data with encryption in every state: at rest, in motion and in use.

Modernize Federal ICAM With Open Standards

Ping Government Identity Cloud is built on open standards, making it easy to modernize IAM components within existing Federal Identity, Credential, and Access Management (ICAM) architectures. This is because standards-based technologies easily co-exist and integrate with other technologies in your environment. Whether your architecture needs a greater overhaul or you're simply looking to augment select capabilities, Ping Government Identity Cloud can help you uplevel ICAM capabilities—without ripping and replacing your existing investments—and lay the foundation for other modernization initiatives, like Zero Trust.

Comply With FedRAMP

Federal agencies and suppliers have compliance mandates they must meet to demonstrate they are keeping Federal data secure when using cloud solutions. A solution that has gone through the FedRAMP process has demonstrated it meets the Federal Government's required security controls. This allows agencies and suppliers to purchase and implement the solution without performing their own assessment to confirm it abides by those security controls. It also expedites audits, saving an immense amount of time and budget.

Any PKI, PIV, CAC, or other MFA

Any user, anywhere

Authentication authority

Any app or resource, anywhere

Take the next step with Ping

Learn More | **Contact Us**

Ping
Identity.

Thank you for downloading this Ping Identity Datasheet. Carahsoft is the master government aggregator and distributor for Ping Identity's Cybersecurity solutions available via GSA 2GIT, CMAS, Educational Software Solutions and Services – OMNIA Partners, Public Sector, and other contract vehicles. To learn how to take the next step toward acquiring Ping Identity's solutions, please check out the following resources and information:

For additional resources:

carah.io/PingIdentityResources

For additional Ping News:

carah.io/PingIdentityNews

To purchase, check out the contract vehicles available for procurement:

carah.io/PingIdentityContracts

For upcoming events:

carah.io/PingIdentityEvents

For additional CyberSecurity solutions:

carah.io/CyberSecuritySolutions

To set up a meeting:

PingIdentity@carahsoft.com
703-871-8505