BRING FRAGMENTED IDENTITY ECOSYSTEMS TOGETHER WITH A FEDERATION HUB

A decades-old timekeeping application was all that stood in the way of transitioning to passwordless authentication for one Federal agency. The disk operating system-based application required directory-based username and passwords, and configuring it to function in a public key infrastructure (PKI) environment proved difficult.

This agency's challenge is just one example of the historical struggle with technical debt and fragmented security infrastructures across the Federal government. As agencies work to meet the cybersecurity standards set forth by the Office of Management and Budget memorandum M-22-09[1] on Federal zero trust architecture strategy and the Department of Defense Zero Trust Strategy[2], many are working to retire legacy systems and processes, break down silos, and enable interoperability.

Zero trust is the identity-centric security framework that assumes the network is hostile and that users cannot be implicitly trusted. It requires strict identity verification and explicit authentication and authorization for every person and device trying to access resources. Crucially, users can only receive access to resources if they can continuously verify that they are who they say they are.

LEGACY AND FRAGMENTED INFRASTRUCTURES STALL ZERO TRUST TRANSFORMATION

Legacy identity, credential, and access management (ICAM) infrastructures do not enable the sophisticated authentication and authorization mechanisms needed to align with current zero trust best practices.

For example, with zero trust, identity assurance and identity-device pairing are just as important as the authenticator itself. In other words, to enable zero trust priorities such as federated single sign-on (SSO), ICAM systems need to be able to perform more than simple authentication.

Legacy technologies and approaches to cybersecurity stall cross-agency collaboration – ultimately hindering the government's ability to adequately respond to mission needs, citizen service priorities, or even national security emergencies – because they prohibit individual agencies from validating the digital identities of workers and mission partners from other agencies.

Fragmented systems have proliferated due to a lack of universal acceptance of identity federation and SSO. A recent National Security Agency/Central Security Service report[3] highlights the security criticality of identity federation and SSO.

A FEDERATION HUB BREAKS DOWN AUTHENTICATION SILOS

To enable interoperable trust across the government and modernize ICAM systems, agencies can employ identity federation, which breaks down silos between user stores and authentication systems to enable users in multiple organizations to access the same networks, applications, and resources with one set of credentials.

A robust, standards-based federation hub can bridge older authentication sources and multiple standards, including the X.509 standard that powers certificates at the center of PKI authenticators. It can integrate with legacy and modern applications, third-party authentication sources, diverse user directories, and existing identity and access management systems.

With enterprise-wide SSO, a federation hub extends agency resources to mission partners for secure collaboration on joint initiatives. A federation hub also integrates with any application, so all applications across the environment can go directly to a single federation hub to confirm the user's identity and grant access. The result is secure enterprise-wide SSO.

A federation hub can extend to mission partners for secure collaboration on joint initiatives. Partners can securely access an agency's resources, even when the partner's authentication methods differ from the agency's.

SECURITY AND TRUST PROVIDE THE FOUNDATION FOR INTEROPERABILITY

Interoperability is the ultimate goal, but there is no standard syntax across government security infrastructures, which complicates authentication. Ping Identity's Federation Hub addresses this challenge by enabling attribute mapping on an application-by-application basis. It can also apply logic to change syntax or format.

In addition, Ping's Federation Hub also supports translation between identity federation protocols, which specify how authentication is conveyed from an organization's identity provider to specific applications. Supported federation protocols include Security Assertion Markup Language (SAML), OpenID Connect (OIDC), WS-Federation, as well as other options for legacy systems.

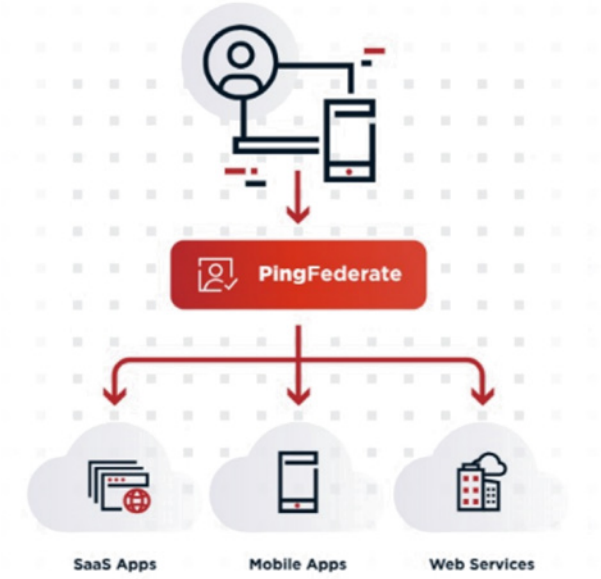
Ping's Federation Hub securely enables translation between federations by only sending information in the federation as an assertion or token that is necessary to establish the connection. Additional information, such as the contextual attributes needed to establish fine-grained authorizations to resources, can be sent via secure, back-channel communication. This creates additional layers between network traffic and any potential attackers.

To comply with the security requirements of the defense and intelligence communities, Ping utilizes encryption where applicable. In addition, Ping's Federation Hub can be configured to use a hardware security module (HSM), which stores private keys and their corresponding certificate. For even stronger security, related signing and decryption operations are processed in the HSM. Additionally, if needed, Ping's Federation Hub can provide bearer of key assertions, in accordance with Federation Assurance Level 3 (FAL3) of NIST SP 800-63.

Ping's capabilities include use cases around collaboration with international partners, where trusted sharing of information is essential. This trust could erode if U.S. agencies were required to open their systems to audit to prove that user data from foreign partners is protected under international regulations. To address this issue, Ping's Federation Hub decouples identity data storage from access controls and policies and employs access control solutions that do not require persistent storage of user data. With the hub-and-spoke model employed by Ping Identity, the agency sets and controls access policy, even when the source of the identity data resides with a partner organization.

BREAK DOWN AUTHENTICATION SILOS WITH PING IDENTITY

Ping Identity believes that digital experiences should be both secure and seamless for all users, without compromise. We enable enterprises to combine our best-in-class identity solutions with third-party services they already use to support zero trust, passwordless authentication, threat detection, and more.

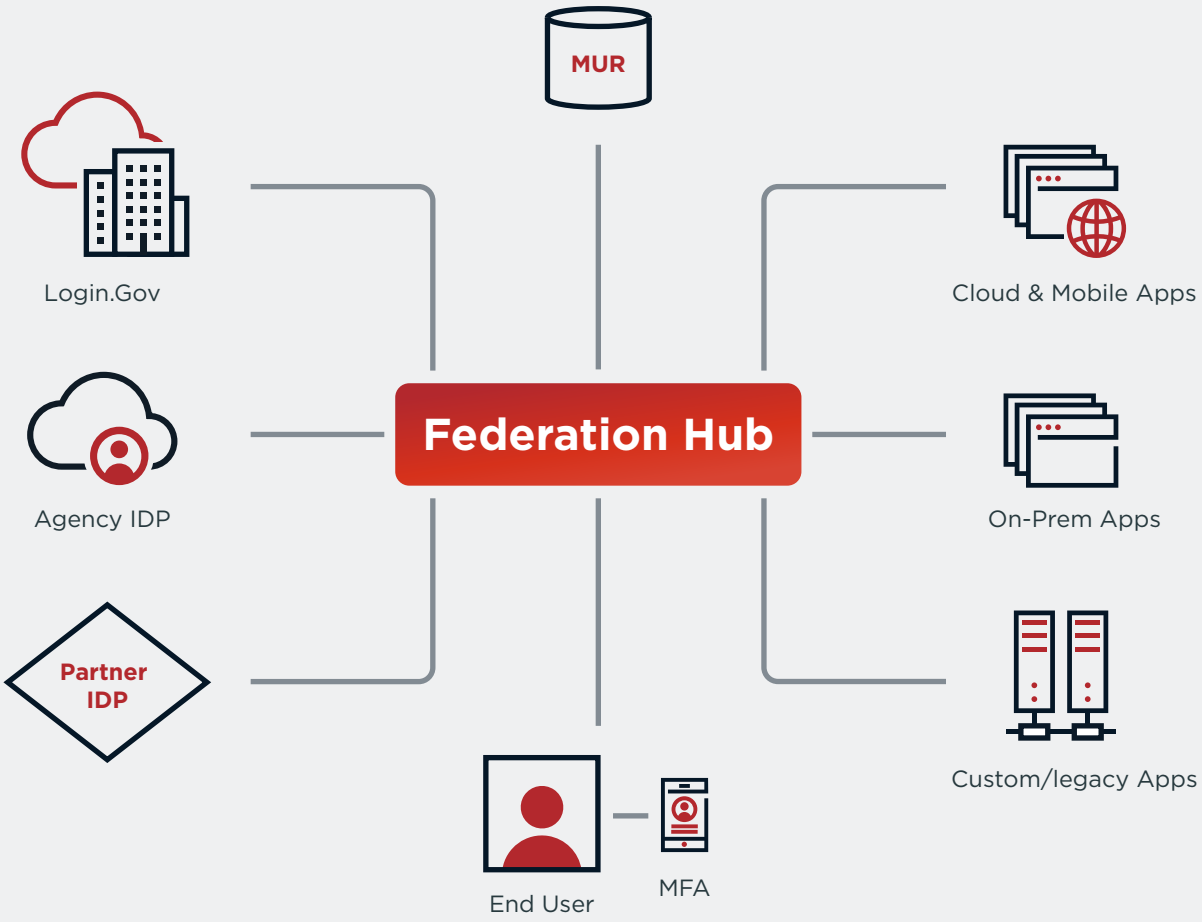


OPEN STANDARDS ENABLE INTEROPERABILITY

Ping Identity has a long history of commitment to open standards for authentication systems to achieve interoperability and scalability. In fact, we coined the term "federation." We have been involved in the creation of many open identity standards, including OIDC. We are a sustaining member of the OpenID Foundation's board of directors and have helped shape the strategy of the foundation since 2010. We are also involved with the Kantara Initiative, a community focused on improving the trustworthy use of identity and personal data.

Why? Because open standards are the foundation of interoperability – they eliminate vendor silos and create bridges across departments, agencies, and international partners. As agencies move toward zero trust, open standards help them to enhance and extend existing technologies, instead of ripping and replacing them.

With FedRAMP High authorization[4], Ping Identity's cloud solutions for government have full feature parity in hybrid; on-premises; disrupted, disconnected, intermittent, and low-bandwidth (DDIL); air-gapped; and now FedRAMP High, DOD IL5 environments.



Learn more about how we enable authentication interoperability and scalability:

pingidentity.com/en/solutions/industry/government.html

[1] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[2] https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[3] https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3547453/nsa-and-esf-partners-release-report-on-mfa-and-sso-challenges

[4] https://press.pingidentity.com/2023-10-31-Ping-Identity-Achieves-FedRAMP-High-Certification

Ping Identity