High assurance security for Ping Identity federated identity management

Standards-based single sign-on solution with FIPS certified cryptography for access to on-premises and cloud-based resources
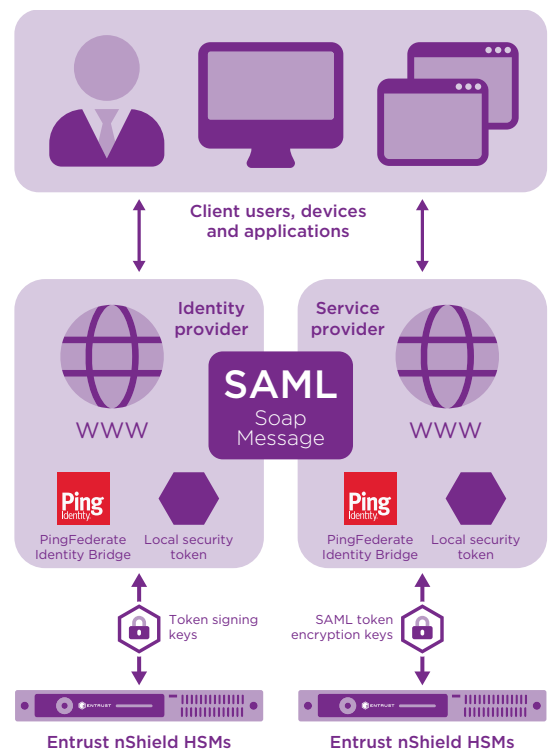
HIGHLIGHTS

- Enables managed access to resources across the enterprise

- Removes the need for multiple sign-on to on-premise or cloud-based enterprise services

- Enables rapid deployment and scalability with an off-the-shelf multi-domain access solution

- Enhances trust with FIPS and Common Criteria-certified standards-based single sign-on

- Delivers best-of-class identity management with protected token signing and encryption

The problem: providing users with easy and secure access to their information and applications – from anywhere and on any device

From smartphones to tablets to cloud-based applications, today's enterprise users have more ways to access their data than ever before – and they expect to get access

quickly and easily. To satisfy enterprise security requirements and user demands, organizations require a comprehensive identity management system.

Client users, devices and applications

Identity provider

Service provider

SAML
Soap Message

WWW

WWW

PingFederate Identity Bridge

Local security token

PingFederate Identity Bridge

Local security token

Token signing keys

SAML token encryption keys

Entrust nShield HSMs

Entrust nShield HSMs

Entrust nShield Connect HSMs integrate with the PingFederate enterprise identity bridge to protect the SAML token signing and encryption keys within a high assurance environment, enabling keys to be exchanged between Web servers using Simple Object Access Protocol (SOAP).

LEARN MORE AT ENTRUST.COM/HSM

Entrust high assurance for Ping Identity federated identity management

The challenge: single sign-on solutions across a federated environment require stronger security

Single sign-on solutions give users seamless access to any application from any device. But managing the identities of employees, customers, and partners access across different domains requires stronger security than what these solutions are designed to deliver, particularly when many identities exist in the cloud. As users increasingly bring their own devices to the organizational environment, this presents additional challenges in keeping business and personal data secure and private. Since single sign-on solutions contain an increasing number of user credentials under one umbrella, they have become a highly valuable target that must be protected. Compromise of the system can have far-reaching corporate consequences and service interruptions can result in a widespread denial of access. Ping Identity and Entrust deliver centrally managed secure identity management with strong authentication and authorization for enterprise services, networks and applications

The solution: Ping Identity and Entrust hardware security modules (HSMs) deliver a high performance solution for managing access

PingFederate supports single sign-on, providing enterprise users easy access to their information and applications. It eliminates the need for multiple sign-on usernames and passwords and allows users to share their identities between web applications and organizations.

PingFederate complies with single sign-on and federated identity standards including Security Assertion Markup Language (SAML), WS-Federation, WS-*, OAuth, OpenID, OpenID Connect and System for Cross-domain Identity Management (SCIM). Leveraging these identity standards, PingFederate secures user access to enterprise and cloud-based resources across organizational domains and via mobile devices.

For the highest levels of identity security, PingFederate can be deployed with an Entrust network-based nShield® Connect hardware security module (HSM). nShield Connect HSMs are high-performance network-attached and tamper-resistant devices that deliver secure cryptographic services. The devices enable organizations to sign and encrypt tokens that supplement SAML token processing and generation. The HSM provides strong integrity and authenticity to protect critical signing and SSL keys, ensuring that keys are never exposed to unauthorized entities. In addition, nShield HSMs provide centralized key management and can be configured for high availability failover and load balancing. Integration of PingFederate with nShield Connect provides FIPS 140-2 Level 3 and Common Criteria EAL4+ certified protection.

Entrust high assurance for Ping Identity federated identity management

Why are HSMs critical to identity management?

While it's possible to deploy an identity management platform in a purely software-based system, this approach is inherently less secure. Token signing and encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that could compromise the token signing and distribution process. HSMs are the only proven and auditable way to secure valuable cryptographic material and deliver FIPS-approved hardware protection.

nShield HSMs enable your enterprise to:

- Secure token signing keys within carefully designed cryptographic boundaries, employing robust access control mechanisms with enforced separation of duties in order to ensure that keys are only used by authorized entities

- Ensure availability by using sophisticated key management, storage and redundancy features

- Deliver high performance to support increasingly demanding enterprise requirements for access to resources from different devices and locations

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Ping Identity

PingFederate enables SSO and Identity Management for Customers, Partners and Employees. It is a lightweight and powerful identity bridge that delivers a comprehensive identity management solution for federated access to applications using existing identity infrastructure.

- Provides 80 pre-packaged integration kits

- Connects to any identity store and application, on-premises and in the cloud

- Deploys anywhere in less than a day

www.pingidentity.com

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com