OneSpan and Entrust secure lifecycle of user credentials and authentication devices

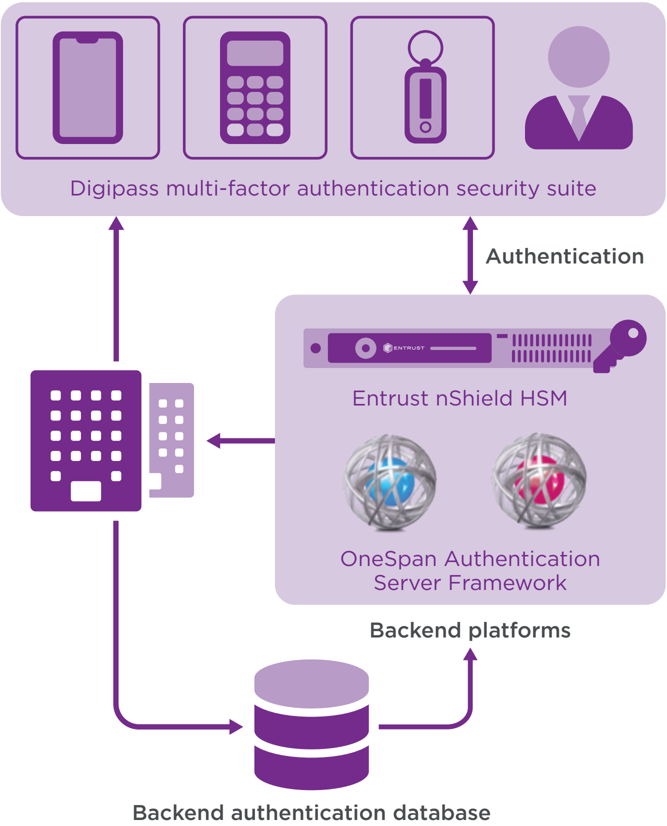
Protecting online identities with OneSpan dynamic password authentication and Entrust hardware security modules

HIGHLIGHTS

- Enable robust two-factor authentication of users
- Protect wide range of authentication devices
- Afford full lifecycle cryptographic key management
- Store keys in FIPS 140-2 Level 3 validated module
- Simplify PCI DSS auditing and reduce compliance costs.

The problem: online applications are increasingly vulnerable to unauthorized access

Unauthorized user access to online applications is a persistent problem for organizations. To mitigate risks, security mechanisms such as two-factor authentication and diverse regulations have been put in place across many industries. With security and regulatory compliance driving implementation of this technology, organizations must recognize what they are trying to protect and how to deploy the technology to avert targeted attacks.


Digipass multi-factor authentication security suite
Authentication
Entrust nShield HSM
OneSpan Authentication Server Framework
Backend platforms
Backend authentication database

Entrust nShield HSMs safeguard and manage the master keys used to protect secrets injected into end-user authentication devices and the backend files used to validate them.

OneSpan and Entrust secure lifecycle of user credentials and authentication devices

The challenge: deploying two-factor authentication without introducing an unnecessary burden on users andthe IT system

Cyber-attacks targeted specifically at defeating two-factor authentication solutions can render security measures ineffective, compromise confidential data, undermine customer trust, and create a public relations nightmare. To safeguard against these threats, the security of user credentials and authentication devices is critical. Equally important is the protection and management of the underpinning cryptographic keys used for provisioning and authentication.

The solution: scalable issuance and enrollment of strong authentication devices to protect against stolen user identities

OneSpan Authentication Server Framework is the backend platforms for the Digipass multi-factor authentication and e-signature security suite. The platforms processes login requests to ensure that only authenticated Digipass users obtain access to protected online applications.

Entrust nShield® Connect hardware security modules (HSMs) integrate with the OneSpan Authentication Server Framework to protect and manage the cryptographic keys used during the provisioning of Digipass devices. The combined solution ensures that Digipass keys are never exposed on the host, and enables organizations to combat advance persistent threats (APTs) on stored authentication data.

Natively integrating with the platform, nShield allows Digipass secret value keys to be protected at all times throughout transport, storage, and use during cryptographic operations.

OneSpan world class application security and identity protection platforms, in combination with Entrust nShield HSMs provide a trusted key management system that delivers a complete end to end solution against unauthorized user access.

Why Entrust nShield Connect HSM with OneSpan Authentication Server Framework and Digipass

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to a security compromise. HSMs are the only proven and auditable way to secure valuable cryptographic material. By providing a mechanism to enforce security policies and a secure tamper resistant environment for backend decryption and key management, the combined solution delivers a best-in-class method for enforcing the security policies underpinning critical components of the enterprisesecurity strategy.

OneSpan and Entrust secure lifecycle of user credentials and authentication devices

Entrust nShield Connect HSMs enable OneSpan customers to:

- Secure keys within carefully designed cryptographic boundaries with robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability with sophisticated management, storage, and redundancy features to guarantee keys are always accessible when needed by OneSpan Authentication Server Framework
- Combat APT attacks on stored authentication data
- Prevent reverse engineering of cryptographic keys and algorithms

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.

OneSpan

OneSpan's security and e-signature solutions protect people, devices and transactions from fraud, providing rock-solid security and a frictionless customer experience. This enables even the most regulated companies to drive bold digital transformation and deliver powerful digital interactions with their customers.

www.onespan.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