Prime Factors EncryptRIGHT and Entrust nShield solution

Prime Factors EncryptRIGHT and Entrust nShield provide a comprehensive and flexible encryption and tokenization solution

HIGHLIGHTS

- Protect data across the enterprise
- Support both encryption and tokenization
- Secure keys within a tamper resistant FIPS 140-2 certified security module
- Simplify policy definition and key management
- Speed deployment with simplified setup
- Facilitate security auditing and compliance
- Support multiple environments from PCs to mainframes

The challenges of data protection

Organizations that want to achieve the highest levels of data protection face an uphill challenge. Data volumes are increasing. Threats are continuously evolving. New technologies and mobile devices are creating more ways for users to access information. And regulations governing data security seem to constantly proliferate.

To reduce risk and demonstrate and descope compliance, more organizations are considering encryption and tokenization solutions. However, these technologies can be costly, difficult to deploy and scale, support limited use cases, and be complicated to manage.

Prime Factors EncryptRIGHT and Entrust nShield solution

A flexible data protection solution

Prime Factors EncryptRIGHT data protection software enables users to easily deploy encryption and tokenization, protecting data at the file, database, or application level. EncryptRIGHT can be deployed on a range of platforms from PCs to mainframes and can span multiple data protection requirements simultaneously. When enhanced level of assurance is required, the solution can be hardened with an nShield hardware security module (HSM), a FIPS-certified device that protects against tampering and is designed to provide the highest level of protection for keys and cryptographic processes.

Speed deployment. Simplify management. Protect system performance.

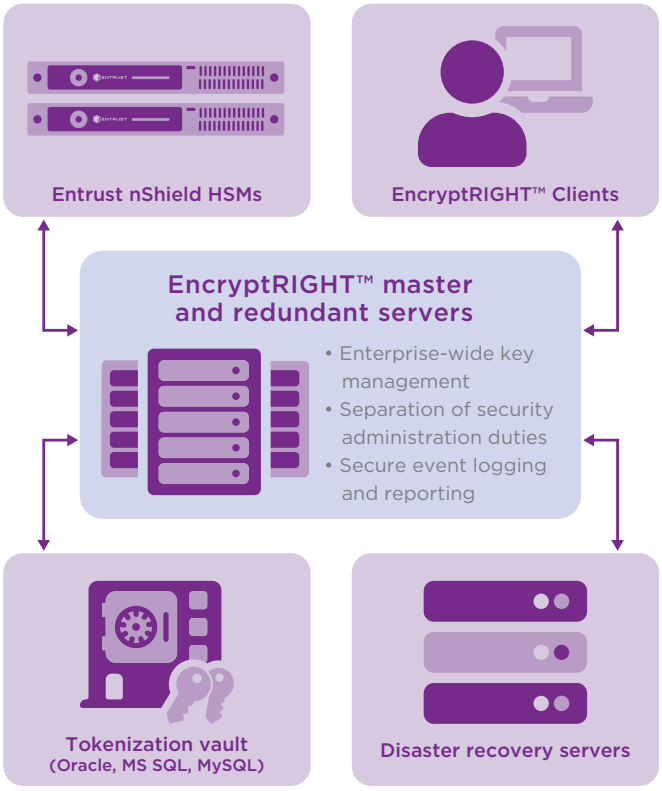
With a consistent approach to setting policies for data protection, the Prime Factors/Entrust solution deploys quickly and easily. EncryptRIGHT's encryption and tokenization processes can preserve data formatting to minimize impact on existing applications and significantly reduce implementation timeframes. The solution is centrally managed to maximize scalability and enable support for mixed environments including z/OS, OS/400, Solaris, AIX, Linux, and Windows operating systems.

EncryptRIGHT embodies the latest in best practices for cryptographic systems and key management and simplifies deployment through an innovative wizard and automated policy configuration. The EncryptRIGHT data protection API provides application developers with a reduced command set to request data to be protected and unprotected in a simple, easy to use toolkit that requires little or no knowledge of cryptography.

Primary features

Designed for maximum flexibility, this joint solution lets organizations choose how best to encrypt or tokenize data without disrupting operations. Features include:

- Cryptography and key management
- Optional high-assurance security using nShield HSMs
- Reports and audit trails
- Broad platform support from PC to Mainframe
- A simple management console and API for application integration
- Application level, file, and database encryption



nShield Connect HSMs integrate with Prime Factors EncryptRIGHT to safeguard and manage underpinning master keys used to protect data. nShield can be deployed on-premises or as a service.

LEARN MORE AT ENTRUST.COM/HSM

Prime Factors EncryptRIGHT and Entrust nShield solution

Reduce the cost of compliance and audits

Designed to help organizations meet regulatory requirements such as PCI DSS, GDPR, HIPAA, and data breach disclosure laws, EncryptRIGHT comes bundled with key management, secure audit logs, and predefined PCI DSS reporting capabilities. Comprehensive central key management, policy definition, and integration with nShield HSMs for enhanced key and cryptographic process protection make it easy to comply with PCI key management requirements for key generation, distribution, storage, rotation, and replacement.

Optional tokenization

EncryptRIGHT includes an optional tokenization capability that helps reduce the PCI DSS footprint and therefore scope and cost of PCI audits. Following industry best practices for token generation and secure storage, the software supports multiple methods of token generation including random tokenization and tokenization by encryption. Token generation uses a FIPS 140-2 compliant random number generator. Tokenization by encryption uses EncryptRIGHT's key management and encryption to generate tokens.

Format preservation

EncryptRIGHT's format-preserving encryption and tokenization processes create encrypted data and tokens with the same formats and data types as the original values. This is a significant deployment advantage that eliminates the need for developers to change applications and/or databases, and can reduce implementation timeframes from months to weeks.

Scalability and resilience

This joint solution provides flexible capabilities to replicate and back up keys in accordance with customer requirements to ensure both security and long-term data availability. Both manual and automated methods are available to back up the internal EncryptRIGHT database. Multiple master and slave servers can be configured to help ensure client access to key values when needed. The internal EncryptRIGHT database can also be synchronized with assigned redundant servers and clients for local processing to protect against bandwidth or other throughput challenges.

About nShield

Deployed on-premises or as a service, nShield HSMs provide a proven, hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. Certified to FIPS 140-2 Level 3, they allow organizations to deploy incremental levels of assurance via standards-based integration with leading applications including Prime Factors EncryptRIGHT for encryption and tokenization.

EncryptRIGHT creates hardware master keys (HMKs) in the nShield HSM and uses them to protect data keys. New key values are exported from the nShield HSM as HMK-encrypted values for storage in the EncryptRIGHT key database. For added protection against illicit database replication, the EncryptRIGHT database itself is also encrypted with its own hardware local master key.

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**

Visit Prime Factors at **primefactors.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