SOLUTION BRIEF

# Prime Factors EncryptRIGHT and Entrust nShield Solution

## Reduce the Cost and Complexity of Protecting Data Where It Is Most at Risk

### HIGHLIGHTS

- Broad-spectrum data protection functionality in a single code base
- Centralized control and distributed enforcement of data security policies
- FIPS 140-3 certified tamper-resistant root of trust
- Crypto-agile data protection to simplify application-level security on-prem or in the cloud

## The Challenge of Protecting Data Where It's Most at Risk

Protecting data at rest is no longer enough. Regulations like PCI DSS now require enterprises to secure sensitive data beyond storage databases and enforce protection and privacy everywhere data is moved or used. However, the traditional approach to protecting data at the application layer is complex and time-consuming, requiring security to be interwoven into applications by developers with specific cryptography expertise. And changes to data protection requirements can add complexity and compound costs. This leaves many organizations searching for an approach that balances risk, cost, and speed – particularly as regulations and business priorities continue to evolve. To enforce data protection and privacy, organizations need a broad spectrum of security techniques that can simplify data protection when requirements change – a concept the industry calls crypto-agility.

## Simplified Data Protection at the Application Layer

EncryptRIGHT is designed to transform data, structured or unstructured, into secured and revealed states, leveraging data security techniques, including encryption, tokenization, masking, digital signing, and hashing. The solution provides an abstracted data protection orchestration layer that secures sensitive data on behalf of applications, transforming data as defined by a central security policy to ensure only the right users can access the data at the right time for the right reasons. EncryptRIGHT's centralized policy engine is agnostic to platforms and technology, consistently enforcing data protection controls wherever data is moved, used, or stored. Integration with nShield HSM establishes a certified root of trust and tamper-resistant environment for keys protecting the policy engine and the data processed by applications.



PrimeFactors™ APPLIED DATA PROTECTION

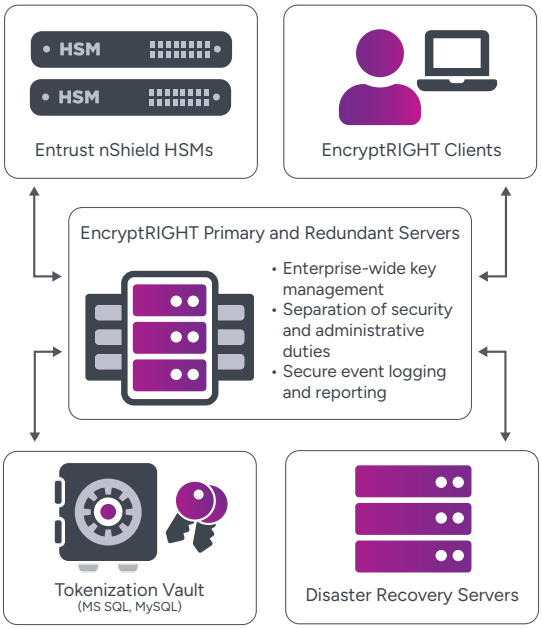
ENTRUST SECURING A WORLD IN MOTION

## Faster Deployment. Lower Costs. Reduced Risk.

Instead of integrating data security into applications, applications can request EncryptRIGHT services using native and web APIs, enabling fast and streamlined implementation in any common programming language or operating system, from Windows to mainframe. Applications don't need to know specifics or access controls to protect the data, resulting in faster deployment, less complexity, and reduced risk.

Primary Features:

- Broad-spectrum security functionality including encryption, tokenization, masking, digital signing, hashing, and OpenPGP
- Crypto-agile architecture, centralized security policy control, and distributed enforcement
- All the functionality of an enterprise key manager to protect and manage critical keys
- Granular role-based access controls to enforce data privacy and permissions
- Audit logs and reporting functionality with SYSLOG support
- Flexible deployment on premises, in the cloud, or across hybrid environments
- High-assurance security using an nShield HSM root of trust




Using pre-built integrations with nShield, EncryptRIGHT can leverage all the benefits of an HSM root of trust without having to re-architect applications.

## Crypto-Agile Architecture

EncryptRIGHT lowers total cost of ownership by empowering enterprises to quickly adapt to evolving threats without costly and time-intensive application re-architecture. The data protection-agile architecture not only enables enterprises to easily transition to new cryptographic keys or quantum-resistant algorithms but also allows them to seamlessly adjust their data security posture to meet new vulnerabilities on the fly. When operational demands shift and regulatory requirements change, enterprises can quickly and easily swap algorithms and keys without facing long development timelines and expensive rework.

## Simplified Compliance

Leverage integrated role-based access controls to support data protection compliance. Built-in secure audit logs, predefined PCI DSS reporting, and SYSLOG facilitate compliance with regulatory requirements. Comprehensive central key management, policy definition, and integration with nShield HSMs enhance key and cryptographic process protection, helping meet PCI requirements for key generation, distribution, storage, rotation, and replacement.

## Robust Tokenization Functionality

EncryptRIGHT delivers tokenization functionally to reduce attack surface and scope audit for PDI DSS compliance, with support for both algorithmic derived tokens and random number generated tokens. The method supports format-preservation and format-targeting to facilitate implementation, eliminating the need for developers to change applications and/or databases and significantly reducing deployment timeframes. Other tokenization features include support for numeric and alphanumeric tokens, single and multi-use tokens, collision avoidance, and partial tokenization. A seamless combination of tokenization enforces privacy for de-tokenization with dynamic masking, and Luhn checks for credit card numbers are also available, together with an integrated PCI-Compliance report to facilitate auditing.

## Better Management

Supporting OpenPGP is complex, but EncryptRIGHT helps enterprises seamlessly manage all the keys and file encryption in support of the OpenPGP standard for secure file transfers. This enables an enterprise-wide key management solution for PGP keys. Organizations can generate public/private key pairs for use with PGP without the need for individual key rings for each user/installation. Existing key pairs can also be imported for continued use of legacy PGP keys after migrating to EncryptRIGHT.

## Scalability and Resilience

EncryptRIGHT is built to provide resiliency with flexible capabilities to replicate and back up keys in accordance with customer requirements to ensure security and long-term data availability. Both manual and automated methods are available to back up the internal EncryptRIGHT database. Redundant 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 Entrust Corporation

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.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 learn more about how to simplify protecting data where it is most at risk, visit primefactors.com.



entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION