PrimeFactors™
APPLIED DATA PROTECTION

EncryptRIGHT®

Application Level Data Protection Simplified

Traditional data protection solutions that protect sensitive data at the disk, database, or file structure level typically leave data exposed in the clear at the application level – the place where most successful data breaches occur. This gap in protecting sensitive information has been difficult to address because application level data protection is messy, complex, and impractical – until now.

EncryptRIGHT provides data encryption, tokenization, data masking, key management, audit-logging, and reporting functionality to protect Personally Identifiable Information (PII) and other sensitive data of global customers across many industries, including financial services, healthcare, global logistics, manufacturing, energy, and more. Whether complying with global data protection regulations or industry standards, reducing the scope of PCI-DSS audits, protecting privacy, pseudonymizing or anonymizing data, managing data sovereignty, or subpoena-proofing the cloud, EncryptRIGHT delivers a seamless data protection solution where data is most at risk of being breached.

EncryptRIGHT Features & Capabilities:

- **Speed of Integration** - Application-native data protection in as little as 3 lines of code
- **Encryption** – Application-level encryption, file encryption and Transparent Database Encryption (TDE)
- **Tokenization** – Random-number generation or encryption generated, single- or multi-use tokens
- **Data Masking** – Static or dynamic data masks applied based on predefined user permissions
- **Role-Based Access Controls** – Define users' level of access to data – full, partial, or no access
- **Data-Centric Security Architecture** – Data Protection Policies (DPP)s that bind to the data itself
- **Broad Compatibility** – Out-of-the-box functionality for every common enterprise operating system
- **Centralized Key Management** – Key generation, rotation, exchange, revocation, and expiration
- **Audit Logging & Alerts** – Reports and audit trails for assessment and verification processes
- **Deployment Flexibility** – Deploys on premise, in private or public cloud, or in hybrid environments

Data Security Governance Approach

Data protection in modern enterprises demands more than just cryptography. EncryptRIGHT leverages a data security governance approach to protect sensitive data, supporting data policy management, data protection management, data access management and cryptographic key management. EncryptRIGHT delivers application level data security governance by coupling a data-centric security architecture with role-based access controls to govern how sensitive data is protected, who may access the data, and how the data will be presented when access is granted – in the clear, partially masked, or no access at all.

Simplified Deployment

Unlike traditional application-level data security products that interweave cryptographic libraries and data protection functionality into an application, EncryptRIGHT Data Protection Policies leverage a data-centric security architecture to bind to the data itself. This approach separates functional application calls to EncryptRIGHT from the specifics of how the data is actually protected, which means quicker deployments with less programming, without the need for cryptographic expertise. EncryptRIGHT protects data where it is most susceptible to breach, providing application-native data protection in as little as 3 lines of code!

Tokenization

The EncryptRIGHT tokenization solution offers robust data security functionality for protecting sensitive data by substituting surrogate data elements in place of sensitive data, helping enterprises reduce potential audit scopes, comply with regulations and industry standards, reduce contingent liability associated with potential data breaches, and increase the tangible effects of data protection altogether. For improved security and flexibility, EncryptRIGHT tokenization can utilize Oracle or Microsoft SQL Server as a secure database or 'token vault' or can deploy in a vaultless environment. The use of random number generators as well as encryption techniques can be leveraged to create format-preserved or format-targeted tokens.

Centralized Key Management

EncryptRIGHT replaces ad hoc key management policies with automated, centralized key management with support for key generation, distribution, storage, rotation, revocation, and expiration, along with extensive audit capabilities. Keys as well as cryptographic operations can be protected through an optional integration with a FIPS 140-2 certified Hardware Security Module (HSM) using the PKCS#11 standard, such as the nCipher nShield. EncryptRIGHT has optional support for Key Management Interoperability Protocol (KMIP) clients and OpenPGP standard for securing file transfers.

Audit and Alerts

EncryptRIGHT includes flexible audit logging and reporting functionality to support traceability, alerting and compliance. Virtually every relevant system event can be monitored to establish detailed audit trails, and logging and reporting can be configured to meet the specific need of an enterprise. Designated users can generate reports showing every administrative change a specific user has executed or reports that identify every user that touched an item, such as a specific cryptographic key. Reports can draw from a single audit log or pull from multiple audit logs over time to provide additional visibility into an EncryptRIGHT deployment. A PCI Compliance Report details the options in EncryptRIGHT that especially relate to the PCI Data Security Standard (PCI-DSS) for compliance and best practices. Audit log entries may be automatically sent to an exportable file or a SYSLOG server to integrate with a Security Information and Event Management (SIEM) system for unified reporting and monitoring.

Dynamic Data Masking

Often, different people in an organization require different levels of access to data based upon their role. EncryptRIGHT can apply any number of data masks in real time to obfuscate some or all of the authentic piece of data in a manner that protects the actual data from being fully viewed. Data masks can be full (concealing all of the original data characters), partial (obscuring only some of the data characters) or clear (allowing the original data to be viewed), based upon the role of the user accessing the data – this is known as Dynamic Data Masking. Many different masks can be configured for different groups of users or for specific data to meet the various data privacy needs of a business.

Flexibility and Scale

EncryptRIGHT was built to scale from a single desktop application to an enterprise-wide data protection solution on premise, in private or public cloud, or in a hybrid deployment environment. The modular client-server architecture allows EncryptRIGHT to expand almost endlessly to meet the need of any size enterprise and the redundancy to assure business continuity in hardware failure or disaster recovery situations. Client-embedded APIs and web APIs supporting calls in a variety of programming languages, from COBOL to C# and Java, allow application programmers to leverage the interfaces with which they are most familiar.

Algorithms, Interfaces, and Platforms

Protect, authenticate and digitally sign data with standards such as Triple DES (2-key and 3-key), AES (128, 192, 256 bits), X9.71 HMAC, OpenPGP, RMD160, and RSA public key algorithms. Strong hashing is provided using SHA-2 or SHA-3. Public keys can be up to 4096 bits.

EncryptRIGHT Supports several common application interfaces, including REST, PHP, Java, VB/.NET, C/C++/C#, PL/SQL, COBOL, CICS, RPG or CLI.

EncryptRIGHT works out-of-the-box on a wide range of operating systems, including z/OS, IBM i (AS/400), Oracle Solaris (SPARC), AIX, Linux and Windows.

To Learn More, Visit:

PrimeFactors™
Applied Data Protection

www.primefactors.com

DS-ER-20200214