ENCRYPTION & KEY MANAGEMENT FOR DRUPAL

NIST Compliant AES Encryption | FIPS 140-2 Compliant Key Management

ENCRYPT

The Encrypt module creates an API for performing symmetric encryption and decryption of data within Drupal. It provides a plugin-based system for encryption methods and key providers, allowing the ability to choose how to encrypt data and where the key should be stored. Contributed modules can integrate with Encrypt to provide encryption functionality for specific kinds of data.

KEY

The Key module gives site developers the ability to store and manage encryption keys and API passwords outside of Drupal. Storing these critical items within the Drupal database, settings file,or a protected file on the server (as many modules commonly do) does not meet security best practices or compliance requirements.

TOWNSEND SECURITY KEY CONNECTION

Townsend Security's Key Connection provides integration between the Encryption and Key modules with Townsend Security's Alliance Key Manager (AKM) solution to provide NIST-compliant encryption and FIPS 140-2 compliant key management.

ALLIANCE KEY MANAGER PLATFORMS

amazon web services™

Microsoft Azure

vmware

ADDITIONAL MODULES WITH INTEGRATION

ENCRYPT USER

Encrypt User allows site administrators to encrypt certain user- related data, such as email address, user name, and password by leveraging Encrypt's API.

ENCRYPT FORM API

Encrypt Form API adds the ability for site builders to encrypt data entered in supported Form API elements. It requires the Encrypt module to do the actual encryption and decryption.

ENCRYPTED FILES

Encrypted Files allows files uploaded to the server to be encrypted for secure storage. It is currently being rewritten to use Encrypt's API.

FIELD ENCRYPTION

Allows users to encrypt Field data in Drupal.

WEBFORM ENCRYPT

Allows users to encrypt Webform data in Drupal.

Townsend SECURITY

www.townsendsecurity.com