Townsend SECURITY

Modules for Securing Data in Drupal

Encryption, Key Management & API Key Security

Data security can be a challenge for Drupal Developers. Townsend Security is helping the community by sponsoring a suite of modules that allow developers to meet compliance (PCI DSS, HIPAA, FISMA, etc.), manage risk of a data breach, as well as protect sensitive API keys.

KEY

Key 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.

ENCRYPT

Encrypt 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 that integrate with Encrypt to provide encryption functionality for specific kinds of data include Encrypt User, Encrypt Form API, Field Encrypt, Encrypted Files, and Webform Encrypt.

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.

WHY ENCRYPTION?

- Protect Personally Identifiable Information (PII) such as usernames, email addresses, ZIP codes, etc.
- Meet compliance requirements (PCI DSS, HIPAA, FISMA, etc.)
- Hosting provider compliance does not make your site compliant

IMPORTANCE OF KEY MANAGEMENT

- Hackers don't break encryption, they find encryption keys
- Compliance regulations require encryption key management
- Protect API keys to prevent anuathorized access to web services
- Manage risk of a data breach with a defense-in-depth security strategy

TOWNSEND SECURITY
townsendsecurity.com | 800.357.1019 | 360.359.4400

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.

ENCRYPT 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 ENCRYPT & WEBFORM ENCRYPT

These two modules integrate with Encrypt to allow encryption of Field data and Webform data.

TOWNSEND SECURITY KEY CONNECTION

Townsend Security's Key Connection provides integration between the aforementioned encryption and key modules with Townsend Security's Alliance Key Manager (AKM) solution to provide secure and regulation-compliant encryption.

HACKERS DON'T BREAK ENCRYPTION. THEY FIND KEYS.

Most users who are currently encrypting sensitive data are storing the encryption key locally in either a file on the server, in the database, or in Drupal's settings file. None of these methods meet data security best practices or compliance regulations such as PCI DSS, HIPAA/HITECH, state privacy laws, etc.

Enterprises that need to meet compliance requirements or are taking a defense-in-depth strategy to data security rely on an external key manager.

In addition to sponsoring numerous encryption and key management modules, Townsend Security offers the only FIPS 140-2 compliant key management solution with Drupal integrations.

Alliance Key Manager for Drupal

Alliance Key Manager by Townsend Security is a FIPS 140-2 compliant key management solution. Additionally, the solution supports on-appliance encryption and decryption services so that encryption keys are always kept separate from the data they protect.

Alliance Key Manager is available as a Hardware Security Module (HSM), Cloud HSM, VMware OVA, or in the cloud (AWS and Microsoft Azure). Townsend Security offers a free developer license for their key manager as part of their Developer Program.

Townsend Security

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security's NIST compliant and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, DIACAP, SOX, and other regulatory compliance requirements. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.

LEARN MORE

Visit www.townsendsecurity.com and find the following resources for securing data in Drupal:

White Paper
What Data Needs To Be Encrypted In Drupal?

Compliance Brief
Meeting Data Privacy Compliance Within Drupal

Developer Program
Free developer licenses for Alliance Key Manager