

Encrypting Sensitive Data in DB2 for IBM i (AS400)

Field and Column-level Encryption using FIELDPROC



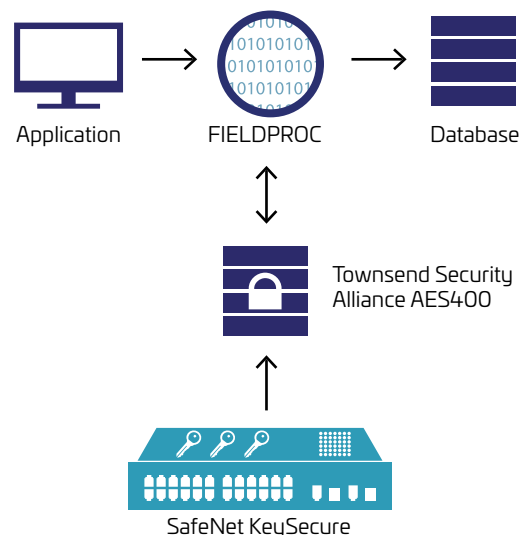
For organizations that store sensitive structured data and personally identifiable information—such as credit card numbers, social security numbers, birth dates, addresses or account numbers—the threat of a security breach—and the damage it can cause—has never been greater. Encrypting this high-value data provides protection in the event of a breach, while enabling organizations to meet various government and compliance regulations. However, traditional database encryption solutions often require changes to the database table format and can slow performance. Enterprises need a solution that secures sensitive data that is critical to their business operations without costly and time-consuming investments.

The Thales and IBM Solution

Thales and Townsend Security can solve the challenges faced by organizations that need an efficient and effective method to encrypt sensitive data in their DB2 databases on IBM i. SafeNet KeySecure with Townsend Security Alliance AES400 encrypts data instantly at the field and column-level using the FIELDPROC or “Field Procedure” exit program for DB2 on the IBM i operating system. With Townsend Security and FIELDPROC, there is no need to modify applications or databases to accommodate encrypted data. Using a set of APIs, application data is encrypted before it is written to the field, making security and access transparent with no impact to the end user. Organizations encrypting data with Townsend Security Alliance AES400 using FIELDPROC in DB2 for IBM i minimize the risk to high-value data across its entire lifecycle while avoiding resource-intensive modifications to the database at the core of their operations.

DB2 on IBM i for Power Systems

DB2 for IBM i is an advanced relational database management system (RDBMS) that is pre-installed on the IBM i operating system. It supports applications and development environments running on the IBM i platform and uses several IBM Power System features, such as Dynamic Logical Partitioning, costbased query optimizer, Capacity Upgrade on Demand, and PowerVM virtualization. The new FIELDPROC exit point in DB2 for IBM i allows users to secure sensitive application data with **transparent encryption using third-party encryption APIs**.



Thales KeySecure with Townsend Security Alliance AES400

Townsend Security Alliance AES400 is an application encryption solution that integrates with DB2 for IBM i to encrypt data at the field and column level without requiring changes to the database or the format of the fields it secures. SafeNet KeySecure also centralizes application encryption policy and key management to increase the level of control that administrators have over their data. Encryption and decryption are transparent to the enduser and doesn't require changes to the application calling the FIELDPROC exit point.

Key Benefits

- **Immediate encryption:** The sooner a sensitive asset is encrypted, the less chance that asset has to be exposed.
- **A Scalable Solution:** DB2 for IBM i's use of Power System features allow it to scale nearly linearly. SafeNet KeySecure's consolidated key management streamlines not only the keys for DB2 encryption, but also for other databases, applications, and KMIP-compatible encryption solutions.
- **Secure data throughout its lifecycle:** Once application data is encrypted, it does not matter if it is backed up on-premises, replicated, or stolen. Only authorized users holding the appropriate encryption keys will be able to view and access the data. Even data encrypted and stored in virtual machines will remain secured in the event the image is copied or stolen.
- **Key management simplified:** Townsend Security Alliance AES400 interfaces with KeySecure for centralized key management to reduce the strain on administrative resources. Administrators can manage the entire security infrastructure's keys from one location to reduce both complexity and the amount of time needed for management and oversight.

Key Features

Centralized Key Management

Thales KeySecure centralizes cryptographic key storage and management in a secure, FIPS 140-2 Level 3-validated, tamperproof appliance. Management tools and capabilities, such as key versioning, streamline key rotation and other time-consuming tasks to make encryption management for DB2 for IBM i databases more efficient and secure. KeySecure enables enterprise key management for Townsend Security Alliance AES400 encryption, the entire portfolio of Thales encryption products, as well as a growing list of third-party solutions supporting the OASIS Key Management Interoperability Protocol (KMIP) standard. Centralized administration of keys, policies, logging, auditing, and reporting functions with KeySecure simplifies management, helps ensure regulatory compliance, and maximizes security.

Policy Management and Separation of Duties

Administrators can set authentication and authorization policies that dictate which fields or columns can be accessed in the clear by a particular user or set of users. These controls provide administrators with tighter governance of sensitive data. Policy driven security

using granular access controls provides a vital separation of duties between IT and security administrators that is required in many security mandates.

Logging, Auditing, and Reporting

Thales KeySecure records all key state changes in centralized logs, simplifying auditing and reporting access to data and encryption keys. By tracking this information from one platform, organizations increase security around their data and can readily demonstrate their compliance with industry mandates and government regulations.

Secure cryptographic processing in a hardware appliance

- When Townsend Security Alliance AES400 encryption is deployed with Thales KeySecure, all cryptographic processing is securely conducted on the KeySecure appliance.
- The appliance is built specifically for optimizing the performance and security of processing-intensive cryptographic operations. By conducting all operations on the appliance, and never letting encryption keys leave the hardware, Thales preserves the integrity of the organization's cryptographic infrastructure. Administrators can account for their keys at all times, and trust that unauthorized users won't ever have access to encryption processes.
- In addition, KeySecure offers load balancing, connection pooling, SSL connections, and key caching to optimize scalability and throughput to reduce the impact on overall performance.

Conclusion: Best-in-Class Security Intelligence and Key Management





Thales and IBM make securing databases easy so organizations' sensitive information is protected from increasingly sophisticated attacks. This solution ensures that data is always secure and the encryption is thoroughly monitored throughout its lifecycle so potential threats are addressed before they become a problem. Organizations now have an effective, powerful, and scalable database that can be easily and efficiently secured through the use of encryption and centralized key management.

To learn more, visit cpl.thalesgroup.com/partners/ibm-0

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> cpl.thalesgroup.com <    

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: apacsales.cpl@thalesgroup.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-eseurity.com