cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales Key Management for Precisely Encryption of DB2 for IBM i (AS400)

Key Management and Field and Column-level Encryption using FIELDPROC

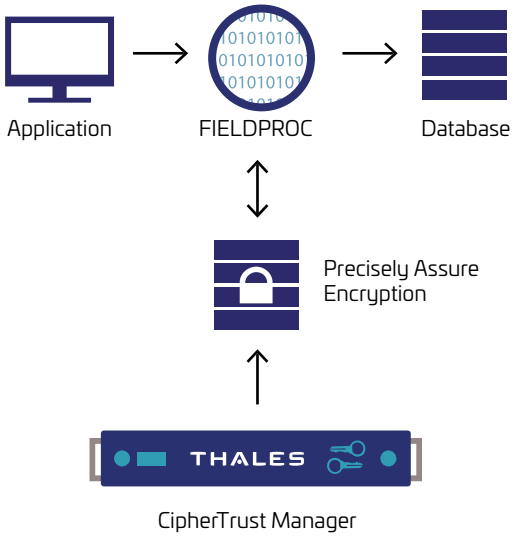
For organizations that store sensitive structured data and personally identifiable information—such as credit card numbers, social security numbers, birth dates, addresses or account numbers—the threat of a security breach—and the damage it can cause—has never been greater. Encrypting this high-value 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 Precisely Solution

Thales and Precisely 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. Precisely Assure Encryption 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 Precisely Assure Encryption 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 Assure Encryption using FIELDPROC 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 CipherTrust Manager with Precisely Assure Encryption

Precisely Assure Encryption 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. CipherTrust Manager centralizes key management externally from the encryption to increase the level of control that administrators have over their data. Encryption and decryption are transparent to the enduser and do not require changes to the application calling the FIELDPROC exit point.

Key Benefits

- **A Scalable Solution:** CipherTrust Manager'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 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.
- **Achieve Regulatory Compliance:** Precisely Assure Encryption and CipherTrust Manager allow organizations to both secure their data and demonstrate control of that data per governmental and industry regulations such as PCI DSS, GDPR, LGPD, and the CCPA.

Key Features

Centralized Key Management

Thales CipherTrust Manager 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. CipherTrust Manager enables enterprise key management for Precisely Assure Encryption, the entire CipherTrust Data Security Portfolio, 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 CipherTrust Manager 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

CipherTrust Manager 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 Precisely Assure Encryption is deployed with CipherTrust Manager, all cryptographic processing is securely conducted on the CipherTrust Manager 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, CipherTrust Manager 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 Precisely make securing DB2 databases on IBM i 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.