MySQL Enterprise Encryption

Only available in select Commercial Editions

To protect sensitive data throughout its lifecycle, MySQL Enterprise Encryption provides industry standard functionality for asymmetric encryption (Public Key Cryptography). MySQL Enterprise Encryption provides encryption, key generation, digital signatures and other cryptographic features to help organizations protect confidential data and comply with regulatory requirements including HIPAA, Sarbanes-Oxley, and the PCI Data Security Standard.

MySQL Enterprise Encryption gives DBAs and Developers the tools they need for:

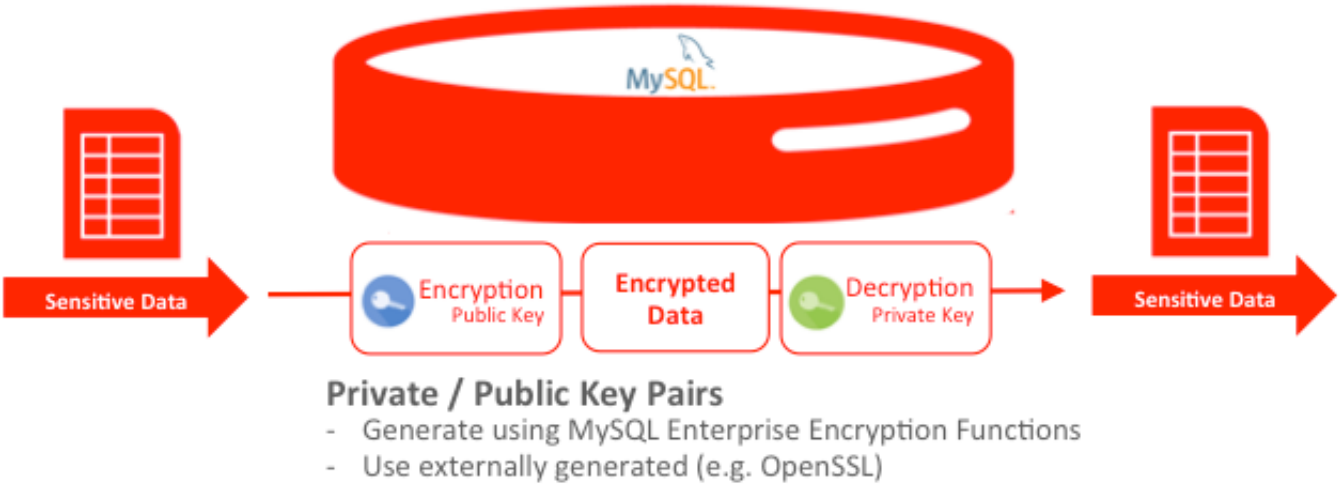
- Asymmetric Public Key Encryption (RSA)
- Asymmetric Private Key Decryption (RSA)
- Generate Public/Private Key (RSA, DSA, DH)
- Derive Symmetric Keys from Public and Private Key pairs (DH)
- Digitally Sign Data (RSA, DSA)
- Verify Data Signature (RSA, DSA)
- Validation Data Authenticity (RSA, DSA)

This enables software developers to encrypt data by using RDS, DHS and DH encryption algorithms easily.

MySQL Enterprise Edition

- Oracle Enterprise Manager
- MySQL Enterprise Monitor
- MySQL Enterprise Backup
- MySQL Enterprise HA
- MySQL Enterprise Scalability
- MySQL Enterprise Authentication
- MySQL Enterprise Encryption
- MySQL Enterprise Firewall
- MySQL Enterprise Audit
- White Papers
- Contact MySQL Sales
- Buy Now
- Demos

Download Now »



MySQL Enterprise Encryption provides industry standard functionality for asymmetric encryption.

MySQL Enterprise Encryption allows your enterprise to:

- **Secure data using combination of public, private, and symmetric keys** to encrypt and decrypt data.
- **Encrypt data stored in MySQL** using RSA, DSA, or DH encryption algorithms.
- **Protect replicated data** by encrypting the MySQL Binlog and Redo Logs.
- **Digitally sign messages to confirm the authenticity** of the sender (non-repudiation) and the integrity of the message.
- **Eliminate unnecessary exposure to data** by enabling DBAs to manage encrypted data.
- **Interoperate with other cryptographic systems** and appliances without changing existing applications.

- **Avoid exposure of asymmetric keys** within client applications or on disk.