DbEncrypt™

A flexible solution providing a means of encrypting columns in a database.

In contrast to bulk file or network-based encryption, DbEncrypt secures data at the column level on the production database. Far more than an encryption toolkit, DbEncrypt includes a robust key management system, templates to ease deployment, and supports a variety of strong encryption algorithms—all from a point-and-click interface. Encryption at the column-level with DbEncrypt is as simple as: 1) Connecting to the database, 2) Picking which column(s) to encrypt, 3) Selecting which user(s) can decrypt, and 4) Selecting the desired algorithm.

KEY FEATURES

- Column-level encryption on production databases
- Robust key management to support granular/flexible privileges (e.g., denying administrators the ability to decrypt)
- Broad algorithm support
- Auditing functionality
- Restoration Key Account Split capability

Customer Privacy & Regulatory Compliance

With DbEncrypt, organizations can easily implement a last line of defense for their most sensitive information—whether the threats come from outside or inside, with administrative privileges or otherwise, mission-critical data remains safe. By extending security measures to include production data on production systems, DbEncrypt not only tightens security for the most sensitive information, but in doing so enhances customer privacy and regulatory compliance efforts.

Authentication, Encryption, and Data Integrity

To enable strong authentication as well as encryption and data integrity, DbEncrypt includes pre-built templates which can be easily customized for specific needs. Interfaces are available to a group of both low- and high-level encryption functions as well as to generate secure random numbers, strong encryption keys, and initialization vectors.

World-Class Protection

DbEncrypt provides enterprise-strength protection for your database through its support for a wide variety of block and stream ciphers, public key algorithms, message authentication codes, and one-way hash functions.

AVAILABLE ENCRYPTION ALGORITHMS

Modes of Operation Include:

- Cipher Block Chaining, CBC
- Electronic Code Book, ECB

Symmetric Algorithms:

- AES
- RC4 (Compatible)
- CAST-128
- CAST-256
- DES
- Triple DES
- SkipJack
- Serpent
- Twofish
- Blowfish (for Oracle)
- RC2 (Compatible) (for Oracle)

Hash Algorithms:

- HMAC_SHA1
- MD5
- RSA
- SHA1

APPLICATION SECURITY, INC.

DbEncrypt™

SYSTEM REQUIREMENTS

Server-Side Module Requirements

For Oracle

- Oracle8i & 9i Enterprise Edition
- Oracle9i Standard Edition
- **Operating System:** Sun Solaris, Linux, Windows NT/2000

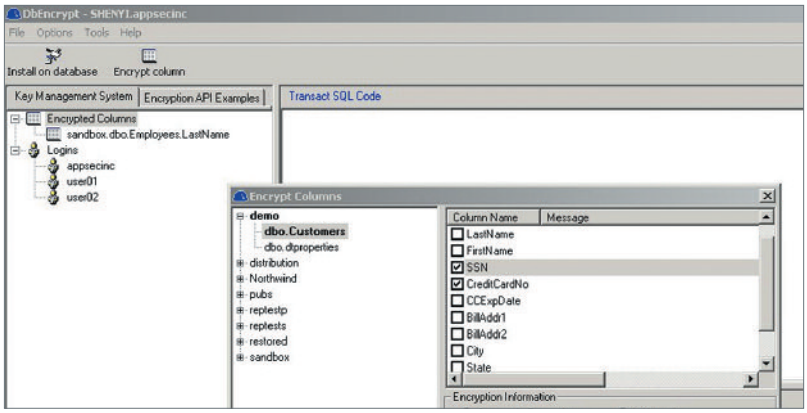
For Microsoft SQL Server

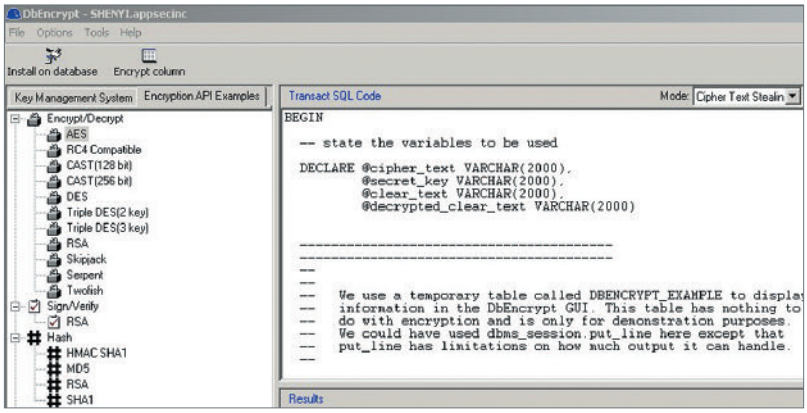
- Microsoft SQL Server 2000
- MSDE 2000
- **Operating System:** Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows NT 4.0 SP3
- **RAM:** Additional 150k per concurrent client that will use DbEncrypt
- **Hard Drive:** Minimal

Console (GUI Interface)

- **Operating System for Microsoft SQL Server:** Microsoft Windows 2000, Windows XP, Windows Server 2003
- **Operating System for Oracle:** Windows NT 4.0 SP3, Windows 2000, Windows XP
- **RAM:** Additional 150k per concurrent client that will use DbEncrypt (for Microsoft SQL Server only)
- **Hard Drive:** 10MB of free disk space

Note: In order to install the server-side module, perform key management, or run any encryption scripts, you must be able to connect an Oracle or Microsoft SQL Server database. Typically, in Microsoft SQL Server, this is done through Windows' built in ODBC drivers. For Oracle, you must install Oracle Objects for OLE on the client where the DbEncrypt Console will reside.





DbEncrypt's point-and-click interface allows enterprises to easily adopt a column-level encryption solution that is transparent to the application without disrupting day-to-day business transactions with active data on production databases.

ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is the leading provider of database security solutions for the enterprise. AppSecInc products proactively secure enterprise applications at more than 250 organizations around the world by discovering, assessing, and protecting the database against rapidly changing security threats. By securing data at its source, we enable organizations to more confidently extend their business with customers, partners and suppliers. Our security experts, combined with our strong support team, deliver up-to-date application safeguards that minimize risk and eliminate its impact on business. Please contact us at 1-866-927-7732 to learn more, or visit us on the web at www.appsecinc.com.

APPLICATION SECURITY, INC.

www.appsecinc.com

575 8th Avenue, Suite 1220, New York, NY 10018 TOLL FREE 866 9APPSEC MAIN +1 212 947 8787 FAX +1 212 947 8788