



## » SERVICES



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
INTERNATIONAL TRADE  
2007



AWARDS  
2008  
EUROPE  
WINNER

Category 'Best  
Security Company'

# Cryptography Evaluation

There are many considerations involved in evaluating the appropriateness of a database encryption product. All considerations must be evaluated against the criteria specified by the prospective purchaser and consequently there are no right or wrong solutions, just products that minimise the level of risk at an acceptable cost. Utilising established implementation assessment methodologies, NGSConsulting are confident that they can uncover the security flaws that will affect the security and integrity of data protected by database encryption products.

In evaluating any database security product, the product undergoes an exhaustive testing phase to identify any implementation issues that could be used to circumvent security. Input into the solution would be tested for its ability to cope with malformed data, all communications would be monitored for leakage of information, and the use of any third-party software would be determined to see if any known flaws in it could be used against the database encryption solution.

The evaluation of a database encryption product involves analysis of its design and implementation from various points of view, the key areas of focus include Architecture, Technical Areas and Implementation. Two of these areas are expanded on in the next sections to demonstrate the topics that NGSConsulting can extensively cover whilst evaluating a product.

## » Architecture

The architectural design of a database encryption product dictates the features it can offer. Below are the key areas that can be evaluated for the security functionality they allow:

- » **Key Management** - This is one of the most fundamental and difficult issues to be examined in any encryption security product encryption. There are many considerations involved in key management, but the key areas for evaluation are; the secure storage of keys (either in the database, elsewhere in the network, on secured hardware, in smartcards etc), creation of keys, separate keys for different resources, location of keys, implication of compromised keys, access of keys by users and administrators, and expiration of keys. If any public key cryptography is being used then more issues such as; issuing keys to users, revocation of keys, key transport, resetting keys etc., are all features that may need evaluation.
- » **Trust Management** - All databases have administrators who have greater privileges for administering the database; from a security point of view this means they are potentially more trusted than the average user. The approach to trust management of a database encryption product will determine how secure the product is in the face of an 'inside' attacker or a compromised user. Identification of specific accounts, roles and privileges need to be made in order to understand the impact of a security breach. The trust in an encryption product can be delegated to the database administrator, or to a separate database security administrator, a combination of them both, or a combination of many administrators. The trust model can also affect the usability of the database from an end user perspective. Trust management and Key management are closely tied - as those that manage the keys usually have the most trust placed in them.
- » **Encryption** - The architectural perspective on encryption focuses on what layer the encryption occurs at. It can occur at the Disk layer, the Operating System layer, the File layer, the Database layer or the Application layer. Depending on the needs of the customer each layer has its benefits and constraints. Of equal importance is what needs to be encrypted in the database, whether this is the entire database, certain tables, columns, rows or individual fields. This evaluation is closely tied to the technical considerations of encryption.
- » **Negotiation** - In many cases strong encryption processes can be bypassed through optional negotiation or hand-shaking protocols. Numerous flaws have been discovered in the past where client-side negotiation can force server systems to utilise low strength or null encryption schemes.
- » **Database Design** - Databases are not static devices; they evolve over time as requirements change. Integrating an encryption solution into a database can seriously limit the ease at which a database design can change; the change in design extends from a schema change to a change in size and database migration issues. This issue then affects the cost of maintaining the database. Depending on requirements, considerations include; the need to change the database design just to incorporate the encryption product and then the ability to change the design once incorporated, changing indexes or data types, changing stored procedures or triggers etc.
- » **Performance** - The database layer of a business application can contain a vast amount of information, and retrieving that information in a timely fashion is often a key business requirement. Incorporating an encryption product will affect performance, and this degradation needs to be evaluated. Adding special hardware to reduce the performance hit is an option offered by some products, but other potential impacts need to be evaluated, and justification for the extra expense usually requires verification.
- » **Scalability** - Databases can be extremely large, quite small and everywhere in between, so the scalability of the encryption solution is very important. Not only can performance can be affected, but the cost of integrating the solution and the future maintenance costs of a solution must be carefully evaluated.
- » **Auditing** - If security is compromised then an audit trail is vital in tracking down the means of entry and the culprit. An audit log can also provide information to an attacker looking to break into a system. Both the effectiveness of any audit features offered and the security implications need to be evaluated.



## » SERVICES



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
INTERNATIONAL TRADE  
2007



AWARDS  
2008  
EUROPE  
WINNER

Category 'Best  
Security Company'

## Cryptography Evaluation

### » Architecture

» Recovery - Things can go wrong; it is the nature of encryption to stop those who do not possess the correct keys from being able to decipher information. While closely related to Key management, this area also includes how the encryption solution handles the creation of backup databases and the security of these backup databases, together with any features that may be offered to make recovery easier to manage and perform.

» Interoperability - Is the solution available for all database products on all operating systems and, if not, how could this affect an enterprise installation of the encryption product? Does the solution have support for industry standards for databases, cryptographic algorithms, and communication protocols? For related features offered by an encryption product these questions should be answered as they can affect security and maintainability.

### » Technical Areas

The technical area of evaluation of database encryption products focuses specifically on the technologies used. Generally this is limited to cryptographic algorithms and communication algorithms, but can include such things as key storage, storage formats and reliance on third-party software.

The encryption technologies offered by a solution are clearly of fundamental importance. The choice of algorithms made available by a solution should include industry standards such as the Advanced Encryption Standard (AES) and 3DES for symmetric ciphers and RSA for asymmetric ciphers. Too many choices for encryption algorithms can work against security for the administrator with minimal security knowledge. The source of the implementation of any encryption algorithm is also extremely important as this affects the amount of trust we should place in whether the implementation is correct or not. In-house implementations require scrutiny to determine if they comply with standards, whereas 3rd party implementations from reputable security vendors offer more assurance. Certainly any database encryption product touting proprietary encryption algorithms be considered flawed until thoroughly researched.

For symmetric encryption algorithms the options available for configuring the algorithms need to be examined; the mode of operation, the use and source of initialisation vectors and the generation of keys etc. are all aspects to be looked at.

For asymmetric encryption algorithms, the key size and key management processes need to be examined along with any message encoding that occurs. These can be verified against applicable industry standards (like PKCS from RSA Security). The use of certificates with asymmetric encryption would also be evaluated, with such things as, the issuing of certificates, root certificates, chains of trust involved, revocation of certificates, encryption and hashing algorithms used, naming used, the use of the certificate to confirm identity, credentials or just provide a public key. A lot of these issues fall into the area of a Public Key Infrastructure (PKI), which is commonly a very difficult system to set up - but is the environment public key certificates were designed to be used in - hence the way in which certificates are used outside such an environment needs to be carefully examined.

All other cryptographic algorithms used in the encryption solution would need evaluation. This would include signature algorithms, hashing algorithms, secret sharing schemes, MAC's, key agreement protocols, key distribution protocols, and access control schemes.

The security of the data on the wire is also extremely important, the use of Secure Sockets Layer (SSL) is commonplace for this purpose, but it is a protocol that is quite configurable and hence if it is used by a solution then its configuration options must be evaluated.

Another important technical area is randomness. Many cryptographic algorithms rely on the availability of random numbers, in fact their entire security depends on it. If a solution requires random numbers it is important to evaluate the actual quality and source of random numbers being produced. Pseudo-random numbers are often used in place of actual random numbers, without the security implications being considered.

### » Contact Details

Web: [www.ngssoftware.com](http://www.ngssoftware.com)

Support: [support@ngssoftware.com](mailto:support@ngssoftware.com)

Sales: [sales@ngssoftware.com](mailto:sales@ngssoftware.com)

UK Head Office (London)  
Next Generation Security Software Ltd  
52 Throwley Way  
Sutton  
Surrey, SM1 4BF  
United Kingdom

Australian Office (Sydney)  
Next Generation Security Software Pty Ltd  
Level 19, 2 Market Street  
Sydney, NSW, 2000  
Australia  
ABN: 83 119804803  
Regional Web: [www.ngssoftware.com/au](http://www.ngssoftware.com/au)  
Regional Sales: [australiasales@ngssoftware.com](mailto:australiasales@ngssoftware.com)

Tel: +44 (0)208 401 0070  
Fax: +44 (0)208 401 0076

Tel: +61 (0) 448 692 022