To encrypt or not to encrypt? That is not the question.

There are several areas of encryption that can be deployed in Record Management System, namely encryption of the database, encryption of the network, encryption of individual documents, as well as Digital Rights Management.

— by Fong Khai Yin, CTO

SQLView Making Enterprises Smarter KRS

Before jumping into when to encrypt and when not to encrypt, it is worth taking a closer look at the several types of encryption that can be deployed in a record management system.

Encryption of the database

Database backups, and archives are normally stored on backup media like disks, backup tapes.

People having access to these backups and archives can be restored and browse the database content on another machine.

Database can be encrypted to ensure that backup media cannot be restored and browse so easily.

Encryption of the database ensures the protection sensitive data on backup media. There is a trade-off of security verses performance that needs to be considered to implement Database encryption.

There is also a need to instill proper key management to ensure proper key access when needed.

Encryption of the network

There are two types of network encryption normally used:

- Encryption of the traffic between the browser and Web server. The most common form used is SSL (Secure Sockets Layer). SSL provides a secure connection between Internet browsers and websites, allowing transmission of private data online. SSL prevent the inspection of network traffic between Internet browsers and web server via net sniffers.

- Encryption of traffic between servers. Although most Application Server, Database Server, etc, are behind the firewall, we may want to ensure that no third party or Trojan virus may eavesdrop or tamper with any message between servers using TLS (Transport Layer Security). TLS is the successor to the Secure Sockets Layer (SSL), but its main use is largely between servers.

Encryption of individual documents

Documents can be selectively encrypted when stored on the servers based on security grading.

When these documents are retrieved, it is the encrypted documents that is transmitted over the network and a local applet in the local retrieval station that does the decryption. This provides an extra layer of security.

Digital Rights Management

Sometimes, we want to distribute documents to other users, and we want to protect users from being able to copy, print, re-transmit documents retrieved. This is where Digital Rights Management can be deployed.

Documents can be tagged with usage policy of who, what, when and where before transmission. And when these documents are access, it will always be checked against the usage policy.

SQL View's KRIS e-RM solution is designed with security in mind and supports encryption in all of the above areas.

SQLView Making Enterprises Smarter KRIS