University College Cork

Encryption Guidelines

Version 1

UCC

University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Information for the University community regarding the protection of stored electronic information and information in transit.

Document Location

http://www.ucc.ie/en/it-policies/guidelines

Revision History

Date of this revision: 02/08/2013	Date of next review: 2/08/2014

Version Number/Revision Number	Revision Date	Summary of Changes

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date

Encryption Guideline

Encryption can play an important role in the protection of stored electronic information and information in transit. It is also used for authentication and validation.

The effectiveness of encryption depends on

- the strength of the algorithms,
- the size and secrecy of the encryption keys,
- and the quality of the implementation.

For this reason, only good, internationally tried-and-tested algorithms should be deployed. For a given algorithm, a key size appropriate to intended application should be used. The implementation should come from a reliable source and should be maintained.

The following is a list of the MINIMUM standards we would recommend. This level of functionality is available with many "off the shelf" products and services. If you have more demanding requirements or need to preserve confidentiality for along time into the future, you should, at the very least, consider using the larger key sizes available.

Symmetric Encryption

- AES 128, 192 or 256 bit keys.
- Triple DEA a.k.a. Triple Des (specifically 3TDEA)

Asymmetric

- DSA 2048
- RSA 2048
- Elliptic Curve DSA - ECDSA 224 bit keys
- Hashing/Digest functions (often used in conjunction with the foregoing)SHA-224, SHA-256, SHA-384 or SHA-512

Any other proposed encryption methods should have at least equivalent strength and reliability to those on the list above. Precautions should be taken to ensure that keys are kept secret. Computers and other devices which hold such keys should be properly protected, configured and maintained so to avoid compromise.

Lost keys or corrupted files will result in encrypted data being unusable. You should keep a backup copy of your encryption key(s) in a secure place. Good reliability and error-correction capabilities on the storage device(s) will reduce the risk of file corruption, but you should nevertheless maintain a secure backup of the encrypted files.

Finally, encryption has a chequered legal history. You should be aware that in Ireland, in certain circumstances, you may be required by law to decrypt your encrypted files. For travel outside the jurisdiction you should take into account that the laws regarding encryption vary widely from state to state. This may manifest itself in restrictions on the possession, use or import/export of encryption technology or in mandatory decryption of files for customs or security purposes.