

# P Cryptography

This document is part of the *UCISA Information Security Toolkit* providing guidance on the policies and processes needed to implement an organisational information security policy. To use the Toolkit effectively it should be read alongside the Toolkit *Introduction* and the *How to use* guide and then used to develop appropriate information security elements for inclusion in your organisation's policies.

## 1. Introduction

The Cryptography Policy sets out when and how encryption should (or should not) be used. It includes protection of sensitive information and communications, key management, and procedures to ensure encrypted information can be recovered by the organisation if necessary.

## 2. BS 7799 definitions and numbering

Cryptography issues relating to information security are covered by section 12.3 and control 15.1.6 of the standards document.

### 12.3 Cryptographic controls

**Objective:** To protect the confidentiality, authenticity or integrity of information by cryptographic means.

#### Controls

#### 12.3.1 Policy on the use of cryptographic controls

A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

#### 12.3.2 Key management

Key management shall be in place to support the organisation's use of cryptographic techniques.

### 15.1 Compliance with legal requirements

**Objective:** To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

#### Controls

#### 15.1.6 Regulation of cryptographic controls

Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

## 3. Interrelationship between policies in this document and related BS 7799 references

In this Toolkit, each subsection addresses a number of cryptography controls from the standard. All of the controls from sections 12.3 and 15.1.6 are covered.

Toolkit subsection	Control(s)
Cryptography and compliance	12.3.1 Policy on the use of cryptographic controls 15.1.6 Regulation of cryptographic controls
Use of encryption	12.3.1 Policy on the use of cryptographic controls
Managing electronic keys	12.3.2 Key management
Using and receiving electronic signatures	12.3.1 Policy on the use of cryptographic controls

## 4. Guidelines for use

### Data encryption

All organisations should establish a procedure for identifying the security risks associated with the ways that confidential or sensitive information is used and evaluate where those risks might effectively be reduced by the use of encryption. For example, additional protection might be given by encryption of sensitive information which, during normal business activities, might temporarily need to be in a less secure environment than normal, (and thereby exposed to greater risks from accidental or malicious threats): this might occur where information is accessed remotely across an insecure network; transferred to a third party (possibly as an email attachment), or loaded on a laptop being used away from the office. Encrypted storage might also be considered for highly sensitive information where there is a risk that the device or media holding it could be accessed or stolen by others. Where the risks are sufficiently great, encryption might be used to complement and strengthen other security measures.

Data encryption should only be considered for sensitive or confidential data. Also, the procedures for key management and the chosen encryption algorithm should reflect the level of sensitivity of the data.

### Transferring data

Any agreements for the exchange of sensitive or confidential data, whether transported manually or electronically (including an attachment to email), must specify security controls that reflect the sensitivity of the information involved and the risks to the data during its transfer. This might include a requirement for encryption, which could be satisfied by electronic transfer over an encrypted data-link or by manually encrypting the file at source and decrypting it at the destination. Clearly, for a file to be decrypted a key needs to be communicated and any key management procedures need to ensure that the source of the key is trustworthy. Keys need to be communicated securely and kept confidential.

### Digital signatures, integrity and authenticity

Consideration should be given to employing digital signatures when embarking on any form of e-Commerce (online booking of distance learning, acceptance of electronic invoices, e-Procurement) or where reliance might be placed on the authenticity and integrity of information received.

In information security terms, a digital signature is a form of electronic signature that has been encoded using public key or asymmetric cryptography, where there are two keys: a private key and a related but different public key. Digital signatures may be added to any document being processed or transferred electronically, whether the document itself is encrypted or not.

Decrypting the digital signature with the published public key will verify that it was signed with the secure private key of the sender. To be truly confident of the authenticity of the signature, it is essential that an organisation can be sure that the public key used belongs to a particular person or identity. For this, key management procedures need to ensure that keys are communicated by reliable and secure methods or only relied upon if received in certificates from trusted third parties.

To address any issue of possible alteration, it is common for a digital signature to include, within it, a message digest, which is a value determined by applying a hash-function to the contents of the document. Once the digital signature has been decrypted, the recipient may confirm the integrity of the document by computing their own message digest and comparing it with the one extracted from the signature.

### Remote network access

Facilities for connection to the organisation's IT facilities via networks not fully within the control of the organisation's security management (e.g. the internet or wireless access), may provide a means of unauthorised access to business applications or confidential information.

When appropriate, and at a pertinent level, controls that include a requirement for encryption should be established to safeguard the confidentiality and integrity of data passing over public networks. Where relevant, risk assessments should be undertaken to assess security implications and, in general, best practice guidelines should be adopted; for example, passwords should not be transmitted unencrypted and applications that require this should either be withdrawn or given additional protection, SSH (if permitted at all) should be promoted instead of telnet, and all VPN connections should be encrypted.

## 5. Cryptography and compliance

### i. Suggested Policy Statement

*“A policy on cryptographic controls will be developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.”*

#### Explanatory notes

Whilst the initial reason for embarking on a cryptography policy might be the protection of confidential information, cryptography also offers benefits in such areas as e-Commerce.

Consideration should always be given to the procedures to be used between the sending and recipient parties and any possible legal or contractual issues arising from using encryption techniques. The introduction of e-Commerce (e.g. online purchasing or electronic invoicing) needs to be done within the emerging regulatory and contractual framework but cryptography, in the form of digital signatures, can be used to confirm the necessary authenticity and integrity of a document.

## 6. Use of encryption

### ii. Suggested Policy Statement

*“Confidential information shall only be taken for use away from the organisation in an encrypted form unless its confidentiality can otherwise be assured.”*

#### Explanatory notes

Confidential information on a laptop taken from the office, for a meeting or to work at home, is exposed to greater security threats – the laptop may be stolen or a family member might use it.

Also, data on PCs used in external events, such as student enrolments at partner organisations, might also be at risk. Information security risks should be assessed and encryption employed where it is found appropriate.

### iii. Suggested Policy Statement

*“Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.”*

#### Explanatory notes

In the normal course of business it might be desirable for a member of staff to hold some important confidential data securely in an encrypted form. It is often essential, however, that this data remains accessible in their absence. Staff might be required to use a shared group passphrase to protect such data, a record of pass-phrases could be held in a secure repository, or staff may be required to encrypt using an organisational public key as well as their own.

### iv. Suggested Policy Statement

*“The confidentiality of information being transferred on portable media or across networks, must be protected by use of appropriate encryption techniques.”*

#### Explanatory notes

Confidential data distributed across networks (both public and private) and by other means, e.g. tapes, disks, CDs and USB keys, needs appropriate protection to assure confidentiality and integrity.

Information security issues to be considered when implementing your policy include the following:

- Weak administration and procedures surrounding the encryption keys can limit the effectiveness of this security measure. Confidential information might inadvertently be compromised or encrypted information may prove to be inaccessible where keys are poorly managed.
- Where security measures have not been adequately deployed, sensitive information may be accessed by unauthorised persons.
- Processor capacity (overhead) is used in the process of encryption and decryption.
- Lack of available capacity could lead to the data being effectively unavailable when actually needed.
- When sending encrypted data outside the UK, cognisance should be taken of any regulatory regime in the destination country.
- The recipient of your data may have adopted information security standards that are incompatible with yours. This constitutes a weak link in your security, which could be exploited.

## v. Suggested Policy Statement

*“Encryption shall be used whenever appropriate on all remote access connections to the organisation’s network and resources.”*

### Explanatory notes

Remote users, either teleworkers or personnel on business trips etc., may need to communicate directly with their organisations’ systems to receive/send data and updates. Such users are physically remote and often connecting through public (insecure) networks. This increases the threat of unauthorised access. Remote access was traditionally provided by means of dial-up or leased phone lines. Today, however, VPNs provide access across public networks, e.g. the internet.

Information security issues to be considered when implementing your policy include the following:

- Inadequate internet security safeguards can allow unauthorised access to your network, with potentially disastrous consequences.
- Weak dial-in security standards can give unauthorised access to your network, the consequences of which could be very serious.

## 7. Managing electronic keys

### vi. Suggested Policy Statement

*“A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.”*

### Explanatory notes

Electronic keys are used to encrypt and decrypt messages or digital signatures on messages sent between one or more parties. The management of the electronic keys is critical if confidentiality, authenticity and integrity are to be preserved.

Information security issues to be considered when implementing your policy include the following:

- The source of a key must be trustworthy so that it may be reliably associated with a particular person or organisation.
- Keys need to be communicated by reliable and secure methods and kept confidential.
- If a private key becomes compromised, invalid messages could be sent which forge the identity of an organisation. Such security breaches could result in substantial fraud. A process to cancel compromised keys to prevent their further use is therefore required.
- Failure to manage the keys of the various senders of encrypted data may result in a failure to decrypt an incoming message, with potential costly delays.

## 8. Using and receiving digital signatures

### vii. Suggested Policy Statement

*“Important business information being communicated electronically shall be authenticated by the use of digital signatures; information received without a digital signature shall not be relied upon.”*

### Explanatory notes

The option of using digital signatures in electronic documents can provide a means of introducing a high degree of authenticity and integrity to an otherwise insecure communications medium. Confidence can be had in an email sent using an appropriate digital signature – its contents only need encrypting if it is also confidential. The content of emails received without signatures may be considered unreliable.

When using digital signatures, consideration should be given to any relevant legislation that describes the conditions under which a digital signature is legally binding.

Information security issues to be considered when implementing your policy include the following:

- Even signed documents cannot be relied upon unless the keys being used are trustworthy.
- Relying upon unsigned email, whilst acceptable in many circumstances, carries a risk, as source and destination fields can be readily forged.
- Receiving email via unsecured public lines (e.g. the internet) can compromise the confidentiality and integrity of the contents.
- Important electronic mail communications might not be authenticated, which could result in unauthorised instructions being issued.

## Specimen Information Security Elements of a Cryptography Policy

A policy on cryptographic controls will be developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.

Confidential information shall only be taken for use away from the organisation in an encrypted form unless its confidentiality can otherwise be assured.

Procedures shall be established to ensure that authorised staff may gain access, when needed, to any important business information being held in encrypted form.

The confidentiality of information being transferred on portable media or across networks, must be protected by use of appropriate encryption techniques.

Encryption shall be used whenever appropriate on all remote access connections to the organisation's network and resources.

A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.

Important business information being communicated electronically shall be authenticated by the use of digital signatures; information received without a digital signature shall not be relied upon.

These specimen policy elements are intended only as a guide and should be adapted for individual organisations.

The implementation of a cryptography policy will also require the development of processes and procedures. Documentary evidence of these will be required to satisfy an external party, such as an auditor, that the policy has been fully implemented.

