Cryptography

# Cryptography

## The base principles

* All data **must** employ adequate and proportionate cryptography to preserve confidentiality and integrity whether data is at-rest or in-transit.
* Existing cryptographic algorithms (and implementations thereof) should be used - at the highest possible abstraction level.

## In-transit

In-transit encryption techniques can both protect data during transit through cryptography but also help facilitate the establishing of identity of devices on one or more sides of the connection.

### Transport Layer Security (TLS)

The [National Cyber Security Centre (NCSC)](https://www.ncsc.gov.uk/) have published information on good TLS configurations <https://www.ncsc.gov.uk/guidance/tls-external-facing-services>.

In general, subject to document exceptions (such as end-user needs and required legacy backwards compatiability)

### Testing

Tools such as [Qualys SSL Server Test](https://www.ssllabs.com/ssltest/) and Check TLS services from [checktls.com](http://www.checktls.com/index.html) **must** be used where applicable to help identify most common issues and configuration problems.

While these tools are not a replacement for skilled testing, the outputs of these tools can help you identify inefficient or insecure configurations which should be considered for remediation.

Configurations should be periodically re-validated.

### Internet protocol security (IPsec)

NCSC have published information on good IPsec configurations <https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data>.

## At-rest

At-rest encryption techniques can protect data while being stored and even during some processing. At-rest techniques usually protect against physical theft or attack methods.

### Server-based

Local storage (such as operating system locations) and filestores (such as storage area networks) should be considered for at-rest encryption to help mitigate again physical interception (such as theft) threats.

Given the autonomous nature of server provisioning and management, it may not always be technically practical to implement such encryption (particularly when a physical server restart would require human intervention with a decryption passphrase).

In general, at-rest encryption **must** always be proportionally considered, even if documented as not reasonable to implement.

#### Cloud-based

Vendor managed at-rest encryption **must** be enabled by default unless there is a good reason not to (for example, licensing restrictions or severe performance issues).

Vendor managed at-rest encryption (the vendor will typically managed encryption keys, on-the-fly encryption and decryption) is preferred, shifting management to the vendor under the shared responsibility model.

In some circumstances, it *may* be reasonable to self-managed encryption keys but should be relatively rare.

### End-User Device based

Native at-rest encryption such as [Apple macOS FileVault](https://en.wikipedia.org/wiki/FileVault), [Apple APFS](https://en.wikipedia.org/wiki/Apple_File_System) or [Microsoft Windows BitLocker](https://en.wikipedia.org/wiki/BitLocker) **must** be used, preferably controlled by central enterprise device management and key management systems.

The NCSC have published [end-user device guidance](https://www.ncsc.gov.uk/index/guidance?f%5B0%5D=field_topics%253Aname%3AEnd%20user%20technology) that discusses such technologies.

### Portable storage

Portable storage such as CDs, DVDs and USB sticks can be safely used to move data. As usual, data must be adequately protected based on the overall governance and information risk requirements.

While the following certifications are preferred, they may not be required based on the data and data methods being stored or transported.

* [FIPS 140-2 Level 3](https://en.wikipedia.org/wiki/FIPS_140-2)
* [NCSC CPA](https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa)
* [NATO Restricted Level Certified](https://www.ia.nato.int/NIAPC/)

The Ministry of Justice (MoJ) prefers the use of network-based transfers compared to the use of portable storage (even if the portable storage is encrypted).

### Portable end-user devices

Portable end-user devices such as laptops, tablets and smart phones must utilised at-rest encryption to protect on-board data (and subsequent configured accounts) while the device is 'locked' or powered down.

The [NCSC End-user Device Security Collection](https://www.ncsc.gov.uk/guidance/end-user-device-security) discusses per-platform configuration advice.

Summarily, native at-rest encryption must be enabled with a suitable and proportional decryption code (typically, a password) and hardware-backed cryptography is preferred.

### Hashing

Data that should be kept confidential or is worthwhile to otherwise obfuscate should be hashed. This **must** apply where authentication credentials are stored, such as a password.

The published [MoJ Password Standard](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/password-standard/) has a section on hashing as part of password storage.