Secrets management

# Secrets management

A 'secret' is defined here as a sensitive piece of information that should be kept private. A secret usually has a technical system or user focus, for example a password, OAuth token or 'private key'. Private keys are secrets associated with SSH network connections, certificates, etc.

A 'secret' **not** the same as a SECRET classification.

## The base principle

All secrets **must** be adequately protected from a loss of confidentiality or integrity. Secrets, much like other confidential data, must be controlled so they can only be viewed or influenced by authorised parties.

## Application & infrastructure secrets

All secrets should be adequately protected and suitably stored.

Where possible, use infrastructure-based secrets management services such as [AWS Key Management Service](https://aws.amazon.com/kms/), [AWS Systems Manager Parameter Store](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-paramstore.html), [Microsoft Azure Key Vault](https://azure.microsoft.com/en-gb/services/key-vault/) or [Kubernetes Secrets](https://kubernetes.io/docs/concepts/configuration/secret/) on Ministry of Justice (MoJ) Cloud Platforms.

It should be rare and exceptional to store secrets within code repositories, such as in Github.com. Where secrets must be stored, they must be protected to control who has the ability to view or use those secrets. For example, to store a secret on GitHub you must use a tool such as [git-crypt](https://github.com/AGWA/git-crypt) to encrypt the secret.

Secrets must never be stored in plain-text. This also applies to code repositories, even when the repository is set to a private mode.

Secrets for managing infrastructure must be issued as user authentication secrets, not a single shared secret.

## User authentication secrets

User authentication secrets such as SSH private keys or tokens must be generated for each purpose and kept private.

Unless by intended design, authentication secrets should never be shared or published.

SSH private keys should be password protected where practical to do so.