Multi-Factor Authentication (MFA) Guide

# Multi-Factor Authentication (MFA) Guide

## Introduction

This Multi-Factor Authentication (MFA) guide explains how MFA can be used to ensure that users are only granted access to Ministry of Justice (MoJ) information once their identity is confirmed. This is a sub-page to the [Access Control Guide](access-control-guide.html).

## MFA

Users should have their identity authenticated through the following methods:

* something they know (such as a password)
* something they have (such as a mobile phone or smart card), and/or
* something they are (biometric authentication such as a fingerprint).

MFA can be used as a possession-based factor for authentication, by checking for something 'you have'. MFA is sometimes referred to as Two-Factor Authentication (2FA) if it involves a second form of authentication. MFA is referred to as 3, 4, or 5 Factor Authentication if it includes additional authentication requirements. Different methods of additional authentication identify users with varying degrees of accuracy. Care should be taken to ensure true MFA. For example, password and security questions are both dependent 'something the user knows' and therefore are just one factor of authentication.

The list below identifies the MoJ's preference for MFA methods, with 1 ranked the highest. These methods can be used for 2, 3, 4, or 5 Factor Authentication as required.

Note:

* MFA Type 1 may not be suitable for all systems. In that case, other methods of delivering MFA should be considered to provide additional protection beyond single sign on.
* MFA types 5 and 8 should only be used when no other MFA method is appropriate as these methods can be easily spoofed or circumvented.

|  |  |
| --- | --- |
| Preference | Type |
| 1. | Hardware-based (for example, Yubikeys or TPM enabled devices) |
| 2. | Software-based (for example, [Google Prompt](https://support.google.com/accounts/answer/6361026?co=GENIE.Platform%3DAndroid&hl=en) on a mobile device) |
| 3. | Time-based One Time Password (TOTP)-based (the code is held by a dedicated app such as Google Authenticator on a mobile device) |
| 4. | [TOTP](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm)-based (the code is held within a multi-purpose app, for example, a password manager app that also holds other factor information) |
| 5. | Certificate-based (a digital certificate used to authenticate a user) |
| 6. | Email-based (a one-time code/link sent to the registered on-file email address) |
| 7. | SMS-based (a one-time code sent via SMS) |
| 8. | Phone-call based (a phone call providing a one-time code or password) |

The [MoJ Password Guide](https://intranet.justice.gov.uk/guidance/security/it-computer-security/passwords/) provides more information on the use of MFA.

## Contact details

For any further questions relating to security, contact: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [itpolicycontent@digital.justice.gov.uk](mailto:itpolicycontent@digital.justice.gov.uk).