Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# Implementing Multi-Factor Authentication

**First published**: January 2012
**Last updated:** November 2023

## Introduction

Multi-factor authentication is one of the most effective controls an organisation can implement to prevent malicious actors from gaining access to online services, systems or data repositories and accessing sensitive data. When implemented correctly, multi-factor authentication can also make it more difficult for malicious actors to steal legitimate credentials to facilitate further malicious activities. Due to its effectiveness, multi-factor authentication is one of the Essential Eight from the *Strategies to Mitigate Cyber Security Incidents*.

This publication has been developed to provide guidance on what multi-factor authentication is, different multi-factor authentication methods that exist and why some multi-factor authentication methods are more secure, and therefore more effective, than others. It also discusses how multi-factor authentication is different to multi-step authentication.

Phishing-resistant multi-factor authentication should be implemented for all online services (including online customer services), systems and data repositories. Using phishing-resistant multi-factor authentication provides a secure authentication mechanism that is not as susceptible to brute force attacks and machine-in-the-middle attacks as traditional single-factor authentication methods, such as those that use passwords or passphrases, or weaker multi-factor authentication implementations, such as those that rely on the use of Short Message Service (SMS) messages, emails or voice calls.

## Why multi-factor authentication is important?

Malicious actors frequently attempt to steal legitimate user credentials when they compromise a system. These credentials, depending on the access they grant, may allow them to easily propagate within a network and conduct malicious activities without additional exploits, thereby reducing the likelihood of detection. Malicious actors will also try to gain user credentials for online services, such as remote access solutions (including Virtual Private Networks [VPNs]), as such access can further mask their activities and reduce the likelihood of being detected.

When implementing multi-factor authentication, it is essential that it is done so correctly to minimise vulnerabilities and to avoid a false sense of security that could leave a system vulnerable. For example, when multi-factor authentication is used for remote access solutions in an organisation, but not for corporate workstations, malicious actors could compromise the username/passphrase from a device used for remote access and then use it to authenticate either locally to a corporate workstation or to propagate within a network after compromising an initial workstation on the network via spear phishing techniques. In such a scenario, multi-factor authentication for remote access is significantly better than single-factor authentication but does not negate the requirement for appropriately hardened devices to be used as part of a comprehensive remote access solution.

# What is multi-factor authentication?

Multi-factor authentication is defined as 'a method of authentication that uses two or more authentication factors to authenticate a single claimant to a single authentication verifier'.

Authentication factors that make up a multi-factor authentication request must come from two or more of the following:

- something the claimant knows, such as a memorised secret (i.e. a personal identification number [PIN], password or passphrase)
- something the claimant has, such as a security key, smart card, software certificate, physical one-time password (OTP) token, smartphone
- something the claimant is, such as a fingerprint pattern or their facial geometry.

The claimant being authenticated may be a person, device, service, application or any other security principal that can be authenticated within the system.

An authentication verifier is an entry point to a confined sub-system where a single technical authentication policy is enforced.

Multi-factor authentication often involves the use of passphrases in addition to one or more of the following multi-factor authentication methods:

- security keys
- smart cards
- software certificates
- physical OTP tokens
- mobile apps
- SMS messages, emails or voice calls
- biometrics.

If an authentication method at any time offers the ability to reduce the number of authentication factors to a single factor it is by definition no longer a multi-factor authentication method. A common example of this is when a user is offered the ability to 'remember this computer' for a public web resource. In such a scenario, a user may be authenticated initially using multi-factor authentication but a token is then set on their device such that subsequent authentications use a single factor (usually a passphrase) as long as the token on their device is accessible and valid. In this scenario, the claimant verified by the token is the user's web browser rather than the user. As such, it violates the requirement for two or more authentication factors to authenticate a single claimant to a single authentication verifier. Furthermore, the token has characteristics more akin to a session token than an authentication factor, which makes it unsuitable for the purposes of authentication.

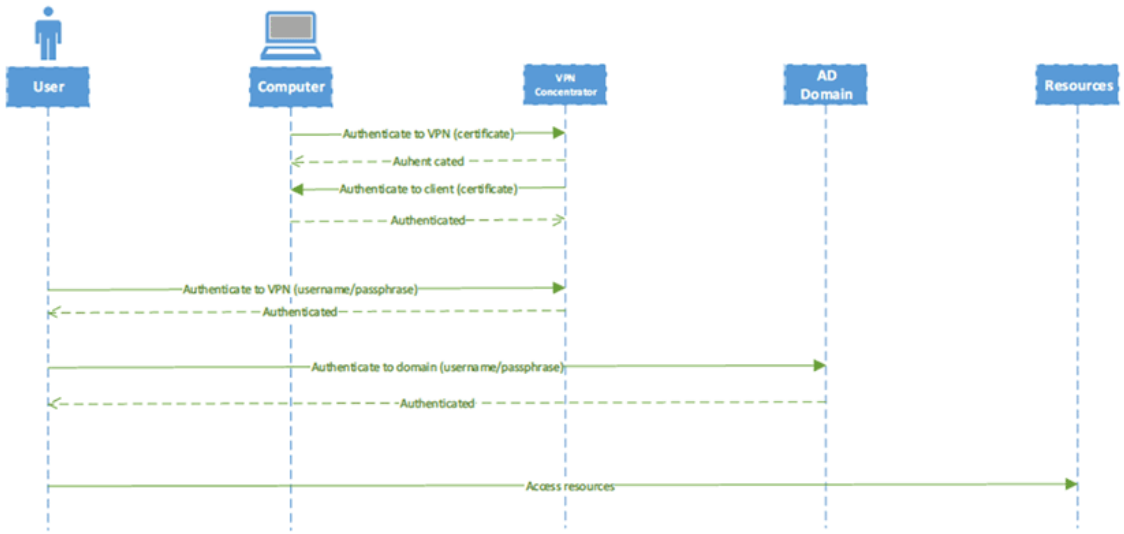
# Multi-factor authentication versus multi-step authentication

A common authentication approach often confused with multi-factor authentication is multi-step authentication. Multi-step authentication is an architectural approach to accessing resources sequentially through multiple authentication verifiers. Each authentication verifier grants access to increasingly privileged areas of the system until access to the desired resources is achieved. Authentication verifiers may be single-factor or multi-factor in nature.

While multi-step authentication may significantly improve the security of a system, it is easier for malicious actors to bypass than multi-factor authentication as there is no single point within the system that uses two or more authentication factors to authenticate a single claimant to a single authentication verifier. As a result, malicious actors can incrementally compromise a system, gaining ever increasing access while never having to overcome the requirement for multi-factor authentication. For this reason, multi-step authentication is not a suitable substitute for multi-factor authentication.

Consider a remote access solution. In this scenario (see diagram below), a computer has an Internet Protocol Security (IPsec) certificate that authenticates the computer to the VPN concentrator, a user has a passphrase that authenticates them to the VPN concentrator and then a passphrase that authenticates them to the Active Directory (AD) domain.

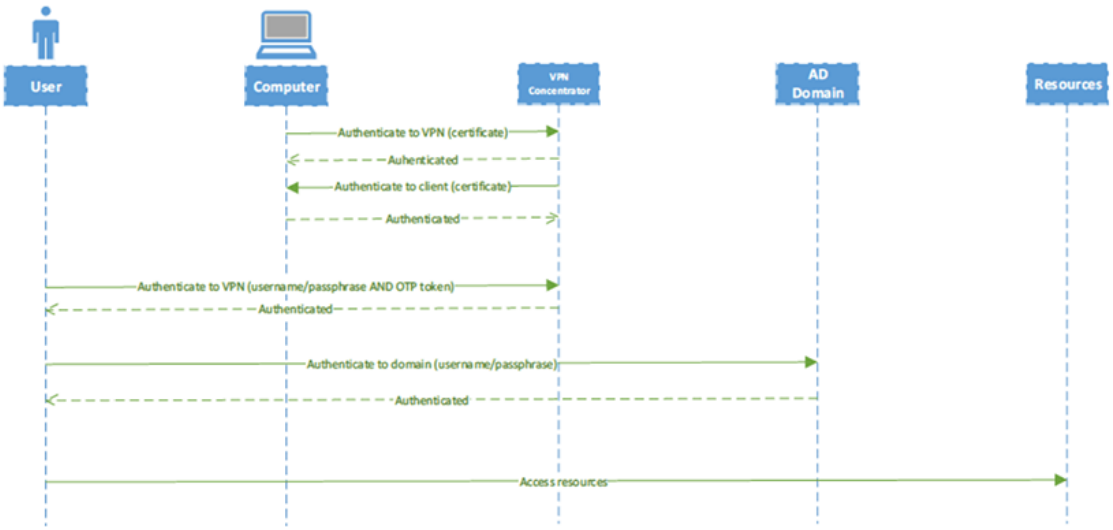
This scenario demonstrates multi-step authentication; however, there is no multi-factor authentication implemented in this scenario. When authenticating to the VPN concentrator, the user and computer are considered separate claimants, therefore the computer's IPsec certificate and the user's passphrase are not a form of multi-factor authentication. Furthermore, the user authenticates separately to the VPN concentrator and to the AD domain. These authentications take place on different authentication verifiers and fail to use different types of authentication factors; therefore, this approach is also not multi-factor authentication.




The risk associated with this scenario is that malicious actors may be able to compromise the computer's IPsec certificate at one point in time, compromise the passphrase the user uses to authenticate to the VPN concentrator at another point in time and, finally, compromise the user's AD credentials at yet another point in time. In this way malicious actors are able to increase their access over time, which increases the level of risk associated with this approach.

Consider a second remote access solution. In this scenario (see diagram below), the user is authenticated to the VPN concentrator using a passphrase and an OTP token. All other authentication steps are the same as in the previous scenario.

This scenario demonstrates a relatively secure remote authentication architecture with a multi-factor authentication method used to authenticate the user to the VPN concentrator. In this case, the computer is authenticated with single-factor authentication in the form of the computer's IPsec certificate. The multi-factor authentication takes place on entry into the remote access environment (using the user's passphrase and OTP token), which verifies access through to the corporate environment, which remains protected by single-factor authentication in the form of the user's passphrase.




# Are all multi-factor authentication methods equally effective?

While all forms of multi-factor authentication listed in this publication provide significant advantages over single-factor authentication, some methods are more effective than others. Notably, multi-factor authentication is most effective when one of the authentication factors uses public key cryptography and is physically separate from the device from which the user is accessing the system or resource, such as using a security key rather than a physical OTP token. Alternatively, a private key, used by public key cryptography, may be stored in a Trusted Platform Module (TPM) on a device with access to the private key protected by either a memorised secret or biometrics, such as with Windows Hello for Business and passkey implementations.

To maximise the security effectiveness of any multi-factor authentication method chosen, the authentication service (if a dedicated authentication server) should be hardened and isolated from the rest of the network as much as possible. This can be achieved by (at a minimum) applying any specific hardening advice provided by vendors and implementing appropriate network segmentation and segregation to limit the types of network traffic to and from the authentication service to only traffic required for its proper operation, with particular care paid to which devices and users on the network that can access the authentication service directly.

# Multi-factor authentication methods

## Security keys

This multi-factor authentication method uses a small physical device (often in the form of a USB device) as a second factor. Software on the user's device prompts the user to either press a button on the security key (when connected to the user's device via a USB port), tap it using Near Field Communication (NFC) or unlock it using biometrics (such as a fingerprint pattern). In doing so, the security key uses public key cryptography to verify the user's identity by signing a challenge-response request from a service which had been passed through via a web browser or mobile app. The service then verifies that the response is signed by the valid and correct private key for that service, and grants or denies access to resources.

For maximum security and effectiveness, the following supplementary security measures should be implemented when using this multi-factor authentication method:

- ensure users do not store security keys with their devices, especially those with NFC capabilities
- ensure users receive a visual notification each time an authentication request is generated that requires them to authenticate using their security key
- use security keys that have been certified to the latest FIDO2 specification
- instruct users to report any lost or missing security keys as soon as practical.

## Smart cards

This multi-factor authentication method uses a private key stored on a smart card as a second factor. Software on the user's device prompts the user to unlock the smart card by entering a PIN or password. When the smart card is successfully unlocked, the software on the device verifies the user's identity by signing an authentication request with the user's private key. The authentication service then verifies that the authentication request is signed by the valid and correct private key, and grants or denies access to resources.

Unfortunately, this multi-factor authentication method has the potential for vulnerabilities due to the software involved in interacting with the smart card. If the user's device is compromised and malicious actors gain elevated privileges, they can potentially intercept and replay legitimate authentication requests or initiate fraudulent authentication requests on the user's behalf – within the limitations of any anti-replay measures.

For maximum security and effectiveness, the following supplementary security measures should be implemented when using this multi-factor authentication method:

- ensure that any patches or updates for smart card software are applied to users' devices as soon as possible, especially if vulnerabilities have been identified as critical by vendors or working exploits exist
- ensure users do not store smart cards with their devices
- ensure users receive a visual notification each time an authentication request is generated that requires them to unlock their smart card
- instruct users to not leave their smart card inserted into their device and unlocked
- instruct users to report any lost or missing smart cards as soon as practical.

## Software certificates

This multi-factor authentication method uses a software certificate stored within a TPM of a device as a second factor. When the user wishes to authenticate, the system attempts to access the user's software certificate, which should require the user to first provide a password or biometric data to unlock the TPM. If successful, the software certificate assists the user to verify their identity by signing an authentication request with the user's private key. The authentication service then verifies that the authentication request is signed by the valid and correct private key, and grants or denies access to resources. Common implementations of this multi-factor authentication method are Windows Hello for Business and passkeys.

For maximum security and effectiveness, the following supplementary security measures should be implemented when using this multi-factor authentication method:

- ensure that software certificates are never stored outside of a device's TPM
- ensure that a password or biometric data is required to unlock access to a device's TPM
- ensure users receive a visual notification each time an authentication request is generated that requires them to enter their PIN or password to access their software certificate
- instruct users to report the theft or loss of their device, even if it is a personal device, as soon as practical.

## Physical OTP tokens

This multi-factor authentication method uses a physical token that displays a time-limited OTP (generally in the form of a six-digit number) on its screen as a second factor. Alternatively, the user may be required to press a button on a physical token, which is connected to their device, to submit the OTP on their behalf. The time on both the physical token and the authentication service are synchronised and the authentication service knows what OTP should be used by all physical tokens that it services at a particular time. When the user authenticates with a passphrase and OTP, the authentication service verifies that all details are correct for that user and grants or denies access to resources.

For maximum security and effectiveness, the following supplementary security measures should be implemented when using this multi-factor authentication method:

- ensure users do not store physical OTP tokens with their devices
- set the expiry time of the OTP generated by physical OTP tokens to the lowest practical value (e.g. 60 seconds)
- instruct users to report any lost or missing physical OTP tokens as soon as practical
- ensure users know that they should never provide details (such as the serial number) of their physical OTP token unless they are certain it is being requested by their ICT support staff.

## Mobile apps

This multi-factor authentication method uses a time-limited OTP provided via a mobile app as a second factor. When the user enrols they either scan a QR code or provide a phone number or an email address so that an OTP can be provided to them to register the mobile app.

During the logon process, the user requests the mobile app to provide them with an OTP in order to complete the authentication process. The user then provides this information to the authentication service, which verifies that all details are correct for that user and grants or denies access to resources.

The advantage of this multi-factor authentication method is that it uses a second factor that the user already has and therefore minimises the cost to the system owner; however, there are also a number of disadvantages, namely:

- use of devices for web browsing or reading emails may mean that the device running the mobile app may no longer be secure
- many devices are not secure and a device can be compromised by motivated and competent malicious actors, particularly when travelling overseas.

For maximum security and effectiveness, the following supplementary security measures should be implemented when using this multi-factor authentication method:

- ensure the expiry time of the OTP generated via the mobile app is set to the lowest practical value (e.g. 60 seconds)
- instruct users to report the theft or loss of a device running the mobile app, even if it is a personal device, as soon as practical.

## SMS messages, emails or voice calls

This multi-factor authentication method uses a time-limited OTP provided via an SMS message, email or voice call as a second factor. When the user enrols they provide a phone number or an email address so that an OTP can be provided to them to register.

During the logon process, the user requests that the authentication service provide them with an OTP in order to complete the authentication process. The user then provides this information to the authentication service, which verifies that all details are correct for that user and grants or denies access to resources.

The advantage of this multi-factor authentication method is that it uses a second factor that the user already has and therefore minimises the cost to the system owner; however, there are also a number of disadvantages, namely:

- depending on the user's location, telecommunication networks may have degraded service or no service at all, which may affect the availability to receive an OTP
- use of devices for web browsing or reading emails may mean that an SMS message, email or voice call containing the OTP may no longer be secure, particularly when SMS messages are delivered via VoIP or internet messaging platforms
- many devices are not secure and a device can be compromised by motivated and competent malicious actors, particularly when travelling overseas
- telecommunication networks do not provide end-to-end security and an SMS message, email or voice call may be intercepted by motivated and competent malicious actors, particularly when travelling overseas.

For maximum security and effectiveness, the following supplementary security measures should be implemented when using this multi-factor authentication method:

- set the expiry time of the OTP provided via an SMS message, email or voice call to the lowest practical value (e.g. 60 seconds)
- instruct users to report the theft or loss of their device, even if it is a personal device, as soon as practical.

### Biometrics

This multi-factor authentication method uses biometrics, such as a fingerprint or iris scan, as a second factor. When the user enrols they provide a scan of the appropriate biometric as a reference point for the authentication service to compare to. When the user authenticates they provide a passphrase along with their biometric data, the authentication service verifies both the passphrase and the biometric data with those provided at enrolment, and grants or denies access to resources. It should be noted though, that for every biometric mechanism, due to the wide range of differences between individuals, some of the potential users will not be able to successfully enrol.

There are, however, potential vulnerabilities in this multi-factor authentication method caused by the fact that biometric characteristics are not secrets (especially if the biometric reader converts biometric data into a hashed form), biometric matching is probabilistic rather than deterministic, and there is a reliance on the biometric capture software installed on the user's device. If malicious actors compromise the user's device and gain elevated privileges, then it is possible for them to use the services provided by the biometric capture software to intercept and replay legitimate authentication requests or initiate fraudulent authentication requests on the user's behalf – within the limitations of any anti-replay measures. Furthermore, the effectiveness of biometrics is reliant on the quality of the biometric readers and capture software to ensure that false negatives (denying access when it should be allowed) and, more importantly, false positives (granting access when it should have been denied) provide an appropriate trade-off.

For the above reasons, the use of a memorised secret and biometrics is not recognised as a suitable form of multi-factor authentication. However, biometrics can be used to unlock access to another authentication factor, such as a private key stored in a TPM on a user's device.

For maximum security and effectiveness, the following supplementary security measures should be implemented when using this multi-factor authentication method:

- ensure users receive a visual notification each time an authentication request is generated that requires them to provide their biometric data
- ensure an alternative authentication method, including supplementary security measures, is implemented for cases where users cannot successfully enrol using biometrics.

# Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

# Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

**Disclaimer**

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.



## For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)


**Australian Government**

**Australian Signals Directorate**