Choosing an MFA solution

Token	Description	Pro's	Con's
SMS	Good old-fashioned SMS or TXT messages; these require you to have a mobile phone number associated with your account so a 6-digit code can be SMS's to you when logging in.	• No additional physical token to carry around • No mobile token software to install • Works on ANY phone (even a Nokia 3210)	• Weak security; SMS messages are clear text so any app on your phone which has access to messages (and there an alarming amount) can read these and transmit them to an attacker if compromised • Typically, people like the convenience of seeing messages or part of messages on their lock screen or wearable, leaving the code exposed to should surfing • In some cases, the code doesn't expire until they have been used • Open to social engineering attacks; there has been a growing trend of SIM jacking, this is where an attacker contacts your mobile vendor to request a new SIM card and port the victim's number so they can receive the SMS code • Won't work without a mobile phone signal • Depending on your carrier this may create complications & cost when abroad • No centralised control from the business/IT • May require disclosure of staff's personal mobile phone numbers (if they are not issued with business devices) which adds to the point above as well as present considerations around personal privacy • No temporary token option; if users forget their phone, they either need to be re-enrolled on another device (which can be time consuming or less secure as it may be a desk phone) or their account is left temporarily un-protected before re-enrolling their old token • Most security organisations & large enterprises plan to decommission SMS mid to long term due to the weak security and on-going high-profile breaches associated to it. As such this methodology may be short lived for a business and require further investment to replace

Telephony	Similar to SMS this methodology makes a call to an associated telephone number and the user authorises by answering the call and pressing #	• No additional physical token to carry around • No mobile token software to install • Works on ANY phone (even a Nokia 3210) • Good for situations where a shared account is used; the DDI of a particular department can be used to answer the call and approve the MFA request	• Weak security; this token relies on physical security of the phone(s) or phone system but does mean anyone with physical access to the phones or phone system can intercept the prompt • Open to social engineering attacks; fake diversion or changes to hunt groups can be made to the person(s) who administer the telephony system • Won't work if the phone line or phone system are down • Can complicate the administration and audit trail as the IT/security team may not be responsible for the telephone system (or may have to learn this additional set of skills) creating admin delays • Most security organisations & large enterprises plan to decommission this token type mid to long term due to the weak security and on-going high-profile breaches associated to it. As such this methodology may be short lived for a business and require further investment to replace • Sharing of administration accounts and associated MFA is terrible practice from a compliance point of view as its harder to ensure authorised access and audit access requests and investigate incidents
OTP	OTP or One Time Passcode is similar to SMS in that it's typically a 6 digit code, the main differentiator is that the code is held/generated either via a hardware device (key fob) or a piece of software (most commonly on a mobile phone); the Google Authenticator is a good example of this - check out the Hardware & Mobile sections below when considering OTP	• Simple to use • Most OTP's expire within 30-60 seconds giving potential attackers a very small window of opportunity • Can be used off-line	• In some cases, tokens do not expire until they are used • Often these solutions do not have a central management console, users imply enrol with a given token which can lead to overheads if tokens need to be retired or reissued • Can be laborious to type codes in for some users • Some solutions do not offer a temporary token option if users forget their token, meaning they either need to be re-enrolled (which can be time consuming) or their account is left temporarily un-protected before re-enrolling their old token • OTP is susceptible to shoulder surfing
Hardware	Hardware tokens come in several forms but in essence can be boiled down to devices which need to be connected to	• Simple to use • Physical access to the fob or card is required	• Hardware tokens can be lost more easily due to their size • Hardware tokens require a battery replacement/full on replacement periodically

	a device such as USB or smart card or a Key fob which displays an OTP code	• Code algorithm is difficult to crack • Hardware tokens can be difficult to clone	
Mobile	Mobile tokens are typically applications which utilise the OTP algorithm	• More convenient as users only need their mobile phone with them • Software based OTP's can be backed up making device swapping easier for the user(s) • Services like Google Authenticator are free and widely used	• Some applications offer weak security allowing a compromised device to copy the OTP code and send it to an attacker via the clipboard or screen shot ◦ Some applications can also be cloned or have their backup mechanism exploited to 'recover' the MFA token to another device • Some OTP applications offer no in-app security so a poorly secured phone can be physically accessed, and tokens obtained
Push-Based	This again uses a mobile phone but utilises a push service; what this means is there is an application on the device which has been registered against the MFA solution and the user will receive a pop-up message for them to approve (or deny) when they login	• Considered the most secure option within the industry • Quicker & simpler than OTP • Harder to crack or intercept on the device • Can act as an early warning if users receive a prompt when not logging in • Convenient as users only need their mobile phone with them • Typically offer in-app protection; securing access to the app even if the phone is unlocked • Can be backed up/migrated to a new device • Token has a short life span reducing the window of opportunity for an attacker • Most often compatible with wearables for convenience and added security if user's	• Requires connectivity to the MFA solution/internet • Some push-based apps can be quicker to exploit than OTP if the user's device is unlocked and a prompt comes in • Some solutions have no temporary token option; if users forget their phone, they either need to be re-enrolled on another device (which can be time consuming or not possible) or their account is left temporarily un-protected before re-enrolling their old token

		device is unlocked & out of sight	
QR Code Based	QR based token require a user to scan a QR code then type the OTP code which is generated	• Works off-line • Convenient as users only need their mobile phone with them • Difficult to intercept or crack • Token has a short life span reducing the window of opportunity for an attacker	• Can be a slow login experience which may frustrate some users. This in turn can hamper productivity, especially if the users need to re-authenticate multiple times due to locking their screen, etc • Some solutions have no temporary token option; if users forget their phone, they either need to be re-enrolled on another device (which can be time consuming or not possible) or their account is left temporarily un-protected before re-enrolling their old token • Camera issues can affect the performance of QR based solutions • Use of cameras within an office/area may be undesirable for other security & compliance reasons