SecurEnvoy
A Shearwater Group plc Company

Multi-Factor Authentication Buyers Guide

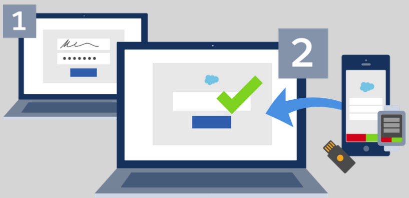
A Guide to Multi-Factor Authentication Options and Features

Introduction

In this informational document, we will examine the possible options and features available to prospective MFA buyers. Their respective purposes, advantages, disadvantages and our recommendations to help you make the most informed choices when buying and implementing an MFA solution.

What is MFA?

MFA or multi-factor authentication is the process of authenticating a user account using both something you know (your password/PIN) and something you own (a device such as a plastic token or mobile phone). IT security experts universally recommend the implementation of MFA, particularly for public-facing portals, as it reduces the risk of unauthorised access due to threats such as password theft, shoulder surfing and password guessing.



In recent years, the use of MFA has become widespread. The most common example of this is the adoption of MFA in the online banking industry. The low cost of MFA implementation versus the reduction in fraud has meant it is almost impossible to find a bank, public-sector organisation or email provider offering just a single-factor of authentication.

On-Premise vs Hosted vs Cloud

MFA solutions are often available in a variety of architectural formats. An on-premise MFA solution requires an existing server and operating system to install management software onto, meaning all the all responsibility for upgrades, maintenance and on-going management your own. On-premise solutions are popular with organisations who see risk in outsourcing security solutions or wish to have full control of the cryptographic key used in calculating MFA OTPs (One Time Password).

A hosted solution is one held and managed by a third-party on your behalf. Also known as a managed service, there is a reduced cost due to the pooling of resources such as server space and administration staff. Upgrades and maintenance tasks are the responsibility of the managed service provider and may incur a per change cost. In addition, the key used to calculate the MFA OTP may be shared among all the managed service provider's customers.

Cloud-based solutions are commonly hosted by the MFA vendor using a subscription cost model. Maintenance and upgrades to the solution are handled by the vendor, however unlike a hosted solution, the on-going management is made available to you via a web-based portal. Often cheaper and benefiting from global resources, cloud deployments are a popular choice. For the security conscious, there are challenges around the ownership of the cryptographic key and how to securely synchronise internal user repositories (for example, Microsoft Active Directory) with the cloud.

The MFA industry has been witness to more cloud and hosted adoption in the past few years. In particular small to medium sized businesses view the cost saving opportunities as attractive. The larger and more heavily regulated have been slower to succumb to change, sometimes unhappy with the additional risk of not hosting the solution themselves. All three options are likely to stay with us for some time, giving you the flexibility of choice. As a recommendation, consider choosing a vendor who supports multiple formats and allows you to move easily between the: today's choices may not reflect tomorrows challenges.

Hardware or Software Tokens

Since the early days of the MFA industry, it has been common to distribute a small plastic token device as the "something you own" element. This device has a small screen presenting a numeric code which has been uniquely calculated, at an interval, by that device alone. Presenting that token value is used to prove the holder of the device and ultimately authenticate the user account.

Today, hardware tokens are still available as an option, however the same technology has been reproduced for mobile phones in the format of apps, SMS and voice calls.

Software token options are undeniably cheaper with no additional equipment to supply as the token is stored on a mobile phone. Benefiting from the care afforded to a personal phone, software tokens are less likely to be lost or broken without hastily being replaced. In addition, software tokens are viewed as more flexible as they are available in a number of formats and can be moved between those formats using wizard drive enrolment portals. Large IT providers such as Microsoft and Google focus on software tokens solely due to their simple use and quick distribution.

Hardware tokens have been witness to their own evolution of late, with the introduction of the YubiKey. A USB based one-key keyboard which injects an OTP into the field of focus. Negating the need to copy a numeric value from a screen to a prompt and making the token smaller has proven popular with those organisations using hardware tokens.

Both supporters of hardware and software options point to the advantages and disadvantages of both solutions as a reason to justify their choices. Yet, as a recommendation the low cost, simplicity and ease of software tokens means they are an irresistible and sensible choice for any organisation. In cases where there is resistance to use a mobile device or other prohibitive circumstances, the use of a YubiKey is an innovative option.

Choose a solution which gives the option of both software and hardware tokens dependent on the needs of the user and the organisations security policy.

PIN or Password

When thinking about the second factor of authentication, you must also consider your first factor, or the "something you know" element.

Some MFA providers request entry of a static PIN along with the dynamic MFA OTP. This PIN serves as the something you know element as it is a static value known by the authenticating user. This option has always been popular with hardware token systems as it forces the entire authentication stream through one solution thus making the overall solution architecturally simpler.

Modern solutions view this as more complicated for users as they now have to remember both a password and PIN, plus in which instances they must present either option. Instead replacing the need for a PIN with the password from a universal user repository, such as Microsoft Active Directory, meets the same MFA requirements.

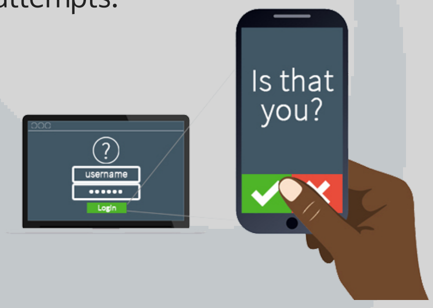
It is recommended to use a solution which utilises password as the "something you know" element. The adoption of solutions by users is reliant on its ease of use, complicating the use of solutions such as MFA will hamper its adoption and result in an increase in IT help-desk requests.

Software Token Options

Software tokens are available in a number of different formats, from smartphone app to NFC to SMS and push-notification.

For those without smartphones, or those who do not want to add an app to their phones, OTPs can be delivered by both email and SMS. These low-touch options can be both real-time, with the OTP arriving at the time of need, or pre-loaded, whereby the OTP is delivered after the last authentication attempt. The latter approach guarantees an OTP despite network coverage during the next attempt. In 2016, NIST (National Institute of Standards and Technology) issued guidance against the use of SMS for delivery of OTPs as it can be intercepted, however those who prefer OOB (Out of Band) methods of delivery persist.

More popular is the use of a smartphone app which replicates the function of a hardware token by displaying a uniquely calculated OTP on the screen of a mobile phone. Apps are free and usually downloaded from a mobile phone manufacturer app store which will require subsequent enrolment to synchronise it with your cryptographic key. Such is the popularity of smartphone apps, the MFA industry has introduced an extension by way of a push notification feature. Instead of copying an OTP from mobile phone to authentication prompt. A prompt is displayed on the mobile phone asking is attempting to authentication. A positive response transfers the OTP in the background. The simplification of push-notifications has a notable effect on successful authentication attempts.



When looking ahead to future trends within the MFA industry, NFC (Near Field Communication) stands out as an option being adopted by some vendors. Using both the NFC components in the mobile phone and the the device you are using to facilitate the authentication request. An OTP can be passed by just moving the two within close proximity. Similar to push-notification, NFC is preferred by some as it requires the mobile phone to be nearby, reducing remote hijacking. Unfortunately, at time of writing this technology has seen slow uptake, mainly due to Apple keeping its NFC API (Application Programming Interface) proprietary. Negating the need to copy a numeric value from a screen to a prompt and making the token smaller has proven popular with those organisations using hardware tokens.

Choose a solution which can provide not only a solution for today but one fit for tomorrow. Todays users of smartphone tokens, may be tomorrow's NFC fans.

Bio-Metrics - The 3rd Factor

Once upon a time, bio-metrics was a subject reserved for Hollywood science fiction, now it is a feature offered in many a MFA solution. Often thought as the 3rd factor of "something you are", bio-metrics allow you to positively identify the authenticating user using a physical attribute such as fingerprint, voice analysis or iris scan.

For all but door entry systems, bio-metrics is handled by a mobile phone app which makes use of the built-in camera or fingerprint reader. In the case Apple iOS, finger print analysis by an MFA solution is a misnomer. The fingerprint is not used to authenticate the user against the MFA solution, rather it is used to unlock the phone. The iOS architecture places the fingerprint into a special on-board chip called the secure enclave which is not accessible to apps or APIs. When a fingerprint is presented, this is compared with the contents of the secure enclave, upon a match the phone is unlocked, providing access to the MFA app or OTP. Therefore bio-metric controls are provided by the mobile phone as opposed to the MFA provider.

Additional layers of authentication undoubtedly reduce the risk of unauthorised access. However, this must be balanced with a degree of usability, which is reduced when another authentication stage is added.

Our recommendation is to focus on ensuring mobile phones have a PIN applied through an MDM solution or ActiveSync policy. If this is not possible then ensure the MFA app is protected by a bio-metric method.

Geo-fencing & Locating

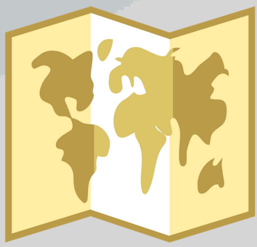
Geo-fencing capabilities allow administrators and IT security teams to limit or modify authentication policies based on the location of the authenticating user.

If your user base is primarily located in one geographical region, anything outside of this region can be considered suspicious leading to a denial of entry or requiring additional stages of authentication to further identify the request.

This style of adaptive and contextual authentication is popular with some, however there are two disadvantages to consider.

Very few auditors consider geo-fencing to have any real defensive value and critically do not count it as an additional factor of authentication. In addition to this, geo-fencing often becomes an unintended barrier. For example, if a user is travelling, using a VPN or tethering their device, they can appear in an unusual location leading to prevented access or additional authentication they are unfamiliar with.

In an ever shrinking world, our recommendation would be to avoid such controls. The added complexity is difficult for administrators to control and confusing for users when they are presented with new prompts or rejection notices. Instead focus on strong authentication



solutions, firewall policies, privilege access management and incident response.

Databases and AD

When choosing an on-premise MFA solution, you may be offered the option of installing a database, for example Microsoft SQL Server, for the purpose of storing authentication information about each user account. This a normal model for most IT applications which has been replicated for years.

Some MFA vendors negate the need for a database and instead opt for storing the same parameters with the user accounts, in AD (Microsoft Active Directory). This model keeps the MFA application requirements smaller by removing the need for a separate database. In addition it benefits from the exiting LDAP replication process by moving those parameters to each domain controller in the domain or forest.

How this is stored in AD differs between vendors. Some choose to modify the schema in order to add additional custom fields. Others elect to use existing empty fields instead. Modifying the schema is a topic which attracts much debate. It means that the MFA application data is kept separate to other attributes, however it can mean your AD database is no longer supported by Microsoft.

It is therefore recommended that whilst AD is used as a storage medium to keep things small, you should not modify your schema. Not only does this potentially put you into conflict with Microsoft, but it also puts your schema into a permanent posture for a single solution.

Licensing

The bottom line for some organisations is the on-going cost of an MFA solution. Some vendors will offer a flat subscription or ownership model.

Ownership models are simple, in exchange for a fixed yearly cost, the software and solution belongs to you.

Subscription can come in various models. More commonly they are split into per month or per authentication plans. Monthly plans will include an unlimited number authentications for a fixed monthly cost. Authentication plans will charge per authentication, regardless of success. If carefully managed and limited to small set of user accounts, a per authentication model can work out as more cost effective. However, it can also spiral out of control if not managed carefully. In addition, it is worth considering the cost in the event an attacker or bot is able to continually attempt authentication.

In both subscription models you may also be expected to purchase a version based on the features you require. This is often multi-tiered, with the cost rising as more features are made available. The cheaper tiers are attractive, however they rarely include features required by the majority of organisations, such as cloud authentication and auditing.

We recommend that you choose an MFA vendor which keeps costs flat and simple, avoiding tiered models entirely. Tailored and use base models appear small on paper but have a tendency to increase sharply overtime as authentication increases and additional features are required. Keeping costs predictable keeps board rooms and budget holders content and more willing to fund future projects.

SecurEnvoy

A Shearwater Group plc Company

+44 (0) 845 260 0010
info@securenvoy.com
https://www.securenvoy.com