# PASSWORDLESS AUTHENTICATION
## – a Technical Viewpoint from WinMagic

Passwordless authentication is held out as the ultimate solution to the many operational, usability and security issues imposed upon us by the traditional password. We agree but there are gaps in the passwordless solutions that are available today and there appears to be a long road ahead to get from where we are today to a passwordless future.

### The Situation today:

- With username and password authentication, you must remember many long passwords, one for each server or website (And, if they are not different passwords then that is a security problem, as a breach at one web site could impact many others)
- This leads to workarounds like password managers that can remember many long and complex passwords in a vault on your computing device or even in the cloud
- Identity theft is still on the rise. Despite use of a good computing device and a password manager, passwords can still be stolen, for example through phishing and man-in the middle attacks Passwords are static, thus can be stolen and reused. One remedy for the static password is to add a dynamic factor, which cannot be replayed or reused. This leads to the One Time Password (OTP) token, or SMS message. These "passwords" – which are usually a 6-digit PIN and change every time – cannot be reused. In addition, with the use of the extra token or the phone people achieve the long-desired "multi-factor authentication" (MFA)
- Even though not static, OTP and SMS still have vulnerabilities:
    a. There are well known SIM swapping attacks where the attacker convinces your carrier to switch your phone number over to a SIM card they own and then intercept the SMS message
    b. And because OTP is based on a shared secret, as is password authentication, it also has vulnerability to attack on the server side just like passwords do
- The extra physical factor can also be inconvenient. Not everyone wants to put a company approved OTP authentication app on their personal phone and not everyone wants to carry around an extra hardware token. It is just one more thing to lose and then must replace

**So, to recap:**

Business users just wants to get some work done on their laptop but the problems with passwords have led to work arounds with password managers and then MFA solutions which have the extra complication of a phone or hardware token to deal this. So, things are even more complex to deal with and yet not necessarily as secure as they should be.

### The solution, Passwordless Authentication, comes with complications

The solution for the password problems with secure remote authentication is passwordless authentication.

Passwordless Authentication prevents the data breaches that are caused by credential and identity theft occurring through phishing and malware attacks. This has given rise to the Passwordless movement, with the result that security professionals and most organizations are starting to adopt and learn how to use Passwordless as their next technology. Most organizations (including your own) will start to investigate options for Passwordless Authentication and to develop a plan for the transition, because passwordless has gaps and complications too.

The complications with passwordless authentication:

- Passwordless authentication can be achieved with a hardware token, but a passwordless hardware token has some of the same issues an OTP hardware token. Users need to carry something extra around with them and companies still need to buy these tokens, keep track of them, distribute them and replace them if they are lost. In fact, one common strategy is to dispense two tokens to each user in case they lose one so that they are not locked out. So passwordless with hardware tokens does not solve the overhead problem.
- The phone is also a passwordless option, usually called "Mobile Push", but it too has some of the same issues as an OTP mobile app. To make use of mobile push, companies must either purchase expensive mobile phone hardware for their users or demand control of users' personal phones. Not all employees are keen to have company-mandated apps on their phones. From a security perspective it is all too easy to automatically press "accept" on the app and, before you know it, the user is a victim of a "push" attack.
- Then there is **Windows Hello for Business (WHfB)**. WHfB can use the TPM and thus does not require an external factor such as a hardware token or phone. However, WHfB only supports Windows 10 devices and has a long list of pre-requisites, including requiring licenses for Azure AD and InTune, making it difficult and expensive to setup and manage.
- Due to complex deployment and lack of support for other platforms, WHfB is not getting the market traction today. WinMagic believes our nimbleness and focus on providing solutions based on industry standards and advancements for non-Web applications like VPN, legacy, rich-client applications will help businesses well beyond what are being offered today.

## “Passwordless” Authentication

**Passwordless:** No centrally managed passwords.

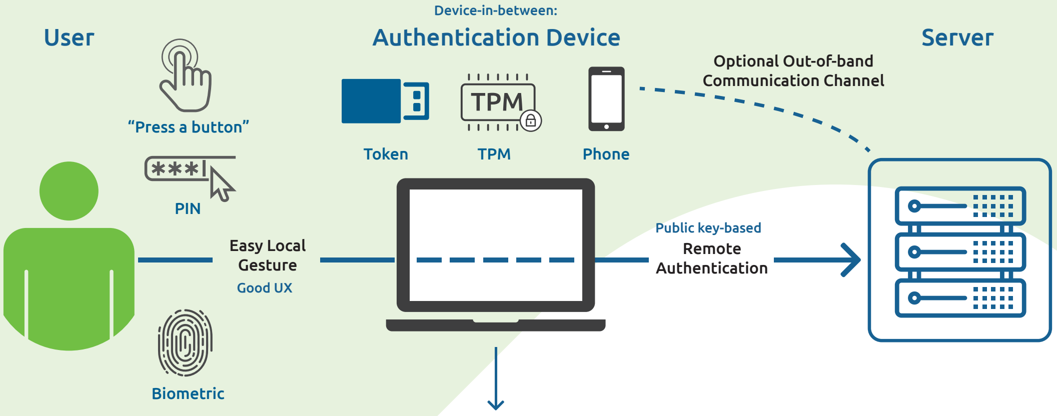

*Figure 1* *The authentication device in-between performs strong authentication to the remote server. Without possession of the authentication device - the private key - no one can login as this user!*

## The Recommendation

The business user just wants to get work on their primary work device but without the complication of an extra factor, such as a phone or a hardware token. The device that they are already doing their work on, a laptop, MAC or phone can be the second factor and provide the most secure authentication. There is no need to carry an extra token or to fiddle with a phone with it because the computer is the MFA, and can log users into a remote server. You are already using your computer at that time. For the server, your computer is the MFA. Between you and the device/the computer, you only need to provide a “local gesture” to confirm your intention to login to the remote server. This “local gesture” can include biometrics (easy), a short PIN, pressing <Enter> or even nothing. You ARE USING the device already. WinMagic makes this easy with our software technology.

MFA is indeed useful when you login to your computer. Note that login at the local device (the computer) is not in the context of the “passwordless” movements the industry is pushing for. However, it should be considered and WinMagic is probably the only vendor working on MFA for pre-boot authentication. WinMagic’s SecureDoc Pre-Boot can also manage authentication/access to BitLocker-encrypted devices and to Self-Encrypting Drives, which we feel are well-positioned to be the preferred disk encryption layers in the future. Regardless how the disk is encrypted, our Pre-Boot, supports MFA like the YubiKey token, PIV, and smartcards. We are the only vendors currently offering MFA at preboot and we can include that in your passwordless journey.

On the server/application side what you must change is that the remote authentication no longer uses a username and password. WinMagic will help you to determine where you can start changing it, i.e. out of the 20 applications currently using remote authentication, WinMagic can help determine which applications you can start using Passwordless Authentication to start. Which applications to start on may be determined by how often users use the application, and which solutions are early adopters of Passwordless authentication. With companies like Microsoft, Google, and Apple behind FIDO (the leading passwordless authentication standard) more and more remote apps will support passwordless. This will enable the phasing out of OTP hardware tokens and phone apps.

**Interested in the 5 Steps to ease enterprises on their passwordless journey? Read our web version HERE**

Passwordless authentication from the perspective of the remote server or application is the act of the server verifying a user without relying on a shared secret. The most common shared secret is a password. With passwordless authentication there are no passwords (or hashes of passwords) stored on the server or shared with the end user. From the user perspective, as seen in Figure 1, the user authenticates locally to the device with a local gesture such as a PIN, Biometric, external hardware token, or out of band with a mobile phone. Then it is this device in-between the user and the server that authenticates to the server. The PIN, Biometric data, etc. are NOT transmitted to the server. Instead the device uses public key cryptography to prove to the server that it is in possession of the corresponding private key that only exists on the user’s device. WinMagic is a FIDO Alliance member. The FIDO Alliance is the leading organization in the passwordless authentication space. The FIDO Alliance is an open industry association with a focused mission: authentication standards to reduce the world’s over-reliance on passwords.

FIDO Authentication is an approach to strong authentication that uses standard public key cryptography techniques - instead of shared secrets - to provide stronger authentication and protection from phishing and other attacks.

fido ALLIANCE