SECRET DOUBLE OCTOPUS

How to Choose an MFA Method?

Trust in users' identities is essential to the value of IAM - Identity and Access Management. User authentication supports IAM functions such as audit, analytics, and authorization, and is important to IAM leaders and to security & risk management leaders alike. While not independently sufficient, it's necessary to provide network control, application and data security, and fraud reduction.

Usability and security are equally essential, and neither should be compromised to meet the needs of the other. Usability, cost, and security must be balanced to provide security that does not impact the user experience.

Currently, the most commonly used authentication methods are:

- **OTP hardware token**
- **OTP soft token applications**
- **OTP via SMS**
- **Push notification**
- **Biometric**

In this document, we will map these popular authentication solutions based on the most relevant decision points: level of security and user experience.

OTP hardware token

With this authentication method, the user possesses a hardware token in addition to knowledge of their account's username and password. This token creates a time-limited or event based One-Time Password (OTP). While authenticating, the user supplies the code of the token or app to the authentication portal after the username and the password.

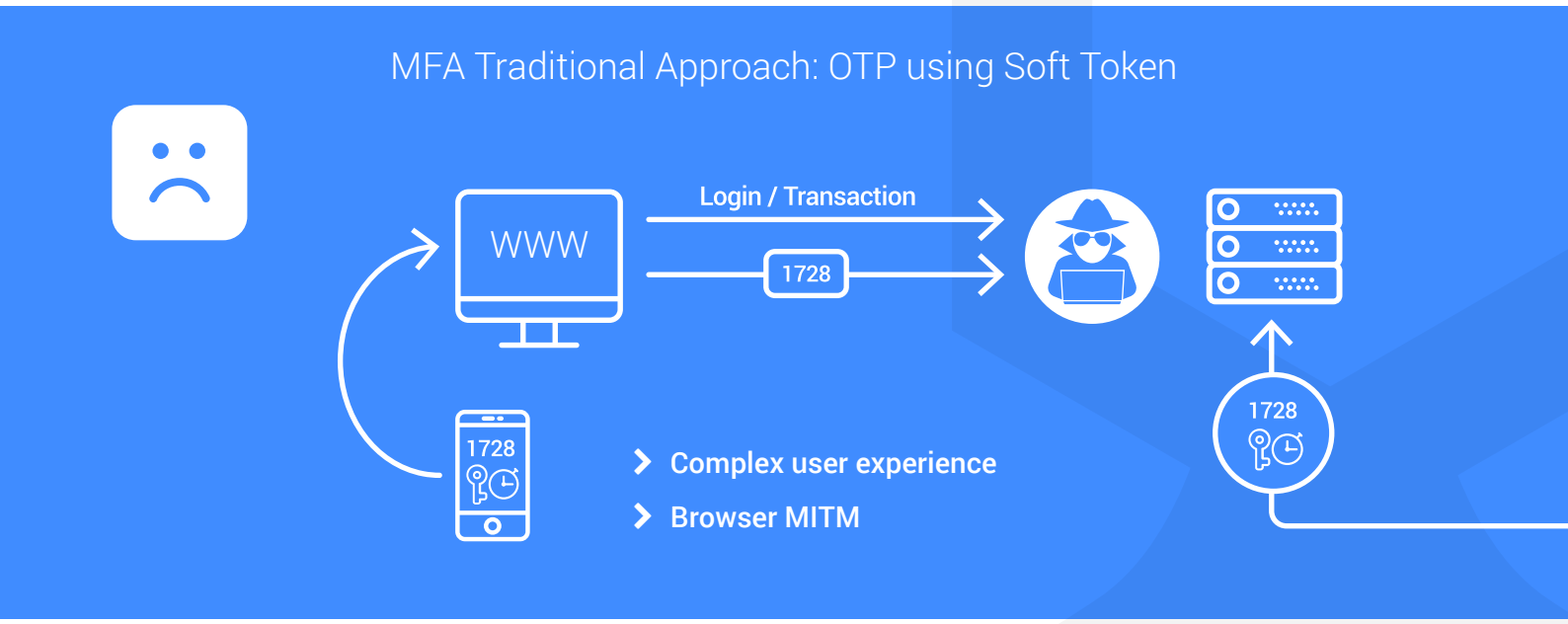
Both server and token hold the same seed and, therefore, generate the same code at each time. The purpose of hardware tokens is that they prove possession of the second factor – it is something you physically possess rather than something received, as in SMS. The user experience, however, suffers as users must carry a hardware token, which is naturally inconvenient.

Hardware tokens contain a secret seed value that must be protected. Those secret values can be stolen from the server or from the hardware token vendor. Token provider RSA, for example, was breached[1] with millions of token serial numbers stolen, exposing customers to hack attacks.

OTP soft token applications

With this method, a user receives an OTP from a pre-installed application. The user then inserts this password into the authentication form.

Soft token applications are more convenient than hardware tokens, in not requiring users to carry additional hardware. Their advantages and disadvantages are otherwise similar to hardware tokens, except that the seed value is vulnerable to theft by mobile malware. When the seed value is stolen, the same soft token can be replicated on the malicious actor's phone.



1 Security Firm Offers to Replace Tokens After Attack, The New York Times, June 6,2011

OTP via SMS

With OTP via Out of Band (OOB) SMS, the user receives an SMS text message with a random code (time-limited OTP). The user then needs to enter the code into the same authentication portal or application in which he or she has entered the user name and password.

SMS as an authentication method may not feature in future releases of the NIST guidance

The traditional and arguably the most common OOB MFA method is OTP via SMS sent to a mobile device[2]. This method is the most vulnerable, however, with security flaws and a less than desirable user experience.

Through 2019, Gartner predicts, enterprises using legacy OOB SMS will suffer more than twice the number of authentication-related breaches than those using mobile push[3].

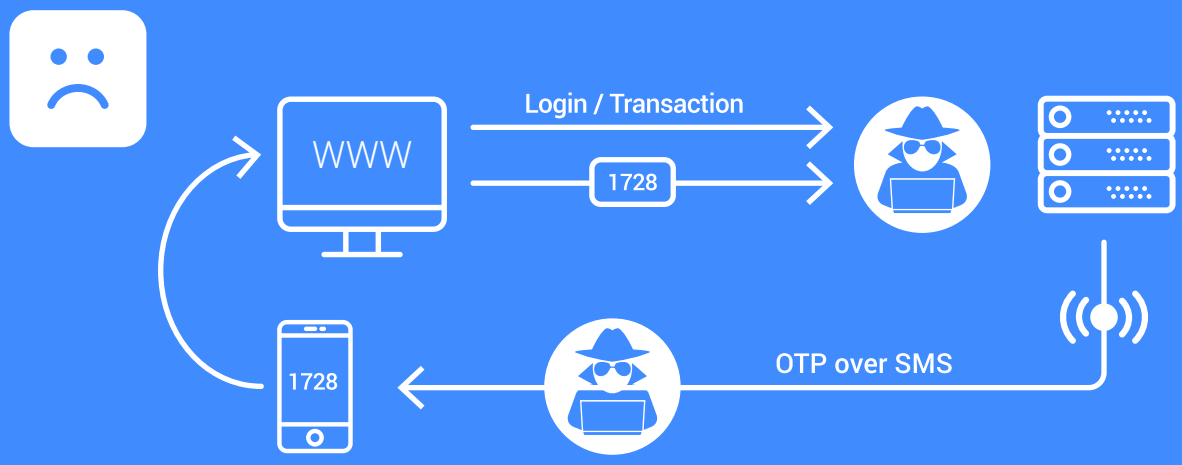
In regard to security, SMS text messages are the weakest link in MFA. Attacks on political activists in Iran, Russia, and in the US have shown that determined hackers can hijack SMS messages in transit[4 5]. Another weakness is that the expecting user is open to receive SMS from anyone – and fraudulent authentication messages are a popular tactic in phishing attacks.

Mobile network operators are not guaranteed to run secure networks, and roaming further reduces the chances for strong security. Moreover, encryption used on cellular networks is known to be weak[5].

Recently, NIST published an authentication guide[6] that discouraged SMS use, and it seems that SMS as an authentication method may not feature in future releases of the guidance.

The SMS user experience is inconvenient, as many users will attest to. When using SMS OTPs, users must copy the OTP information from the receiving device to the login form. As a result, it must be a short 'typeable' string, which reduces security.

MFA Traditional Approach: OTP using Soft Token



2 Technology Insight for Phone-as-a-Token Authentication, Gartner, p.11, March 10, 2017, ID: G00319826
3 Technology Insight for Phone-as-a-Token Authentication, Gartner, p.3, March 10, 2017, ID: G00319826
4 So Hey You Should Stop Using Texts for Two-Factor Authentication, WEIRD magazine, Jun 26, 2016
5 More than 86% of the world's iPhones can still be hacked with just a text, Business Insider, Aug. 29, 2016
6 DRAFT Special Publication 800-63B, Digital Identity Guidelines, NIST, Apr 30 2017

Biometric factor authentication

Another option is biometric authentication. This can be static biometric, such as fingerprint, or dynamic, such as behavioral biometric factors. Static biometric is considered relatively inaccurate. According to NIST[6], "Biometric false match rates, and false non-match rates do not provide confidence in the authentication of the subscriber". For example, security researchers claimed to have cloned the thumbprint of the German Defense Minister by photographing her hand at a press conference[7].

Individual behavioral biometric factors are more difficult to copy. Behavioral biometrics solutions can create a more accurate picture of the user by examining a range of behavioral patterns, and this picture is continuously improved. However, since at the time of login, the application has no behavioral data to analyze, behavioral biometric has been less useful for authentication and is finding its niche in fraud detection instead.

Since at the time of login there is no data to analyze, behavioral biometric is less useful for authentication

Another aspect of biometric factors is where information is stored. Usually authentication is local, such as a user to their device using Apple fingerprint. The reason that biometric data is not stored on a server is derived from a wider question of how secure it is to centralize confidential and sensitive data.

Push notification

The main advantage of push notification is that only the owner of the application can send the notification and, therefore, a phishing attack cannot be generated by a third-party.

By the end of 2019, 50% of all enterprises using phone authentication will move towards push authentication

Push strikes the ultimate balance between a secure and a convenient user experience. As opposed to SMS and biometrics, NIST[6] suggests that push authentication is acceptable as an authentication system.

According to Gartner, by the end of 2019, 50% of all enterprises using phone authentication will move towards push authentication over other methods (such as a one-time-password and SMS), compared to less than 10% today – a 500% growth. It's a trend that is set to grow significantly in 2017.

The problem with push notification is that the encryption is done in two stages: service provider to push server (e.g. Apple or Google) and push server to mobile device. The plain data is revealed at the push server, which means confidential data, including OTP, cannot be sent over push notification. Push notification should only be used to wake up the application so it can send an inquiry to the server. In which case, the authentication would use PKI, but this in turn is vulnerable to SSL weaknesses. Octopus Authenticator addresses this and other MFA vulnerabilities.

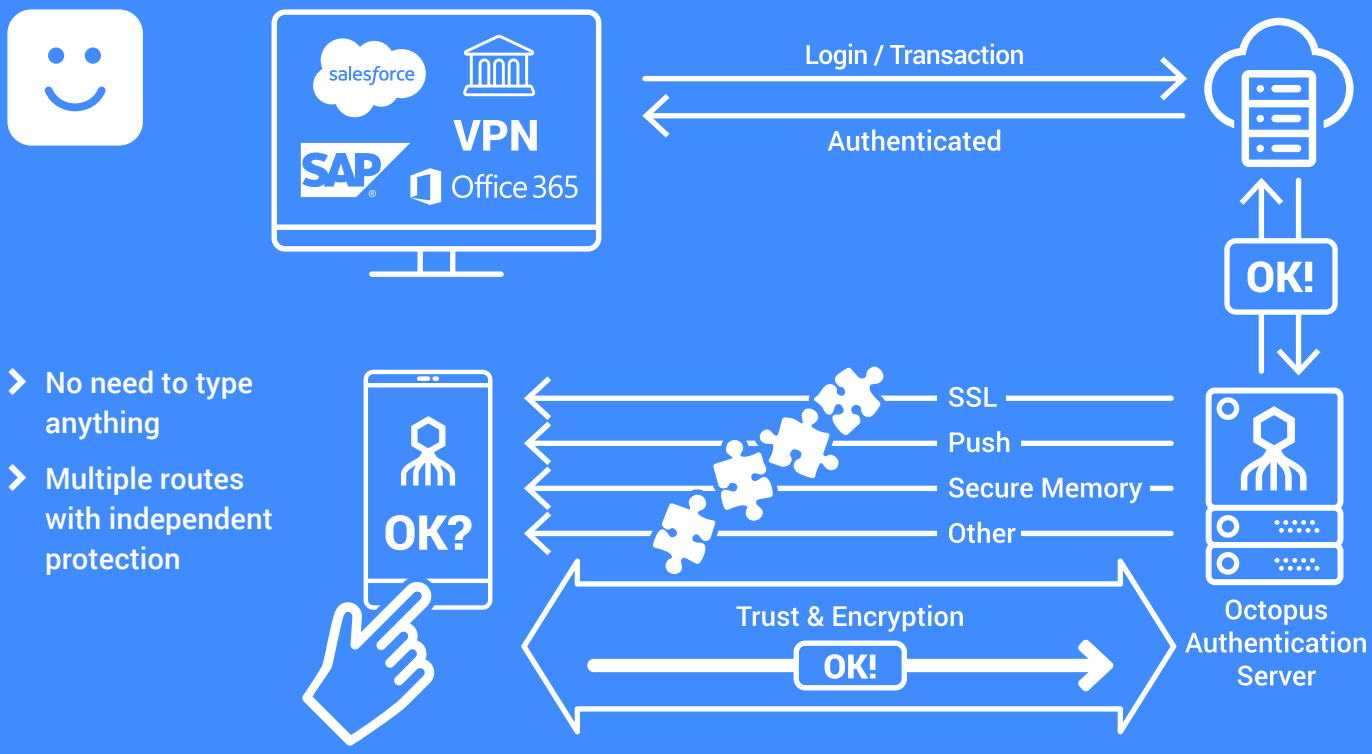
6 DRAFT Special Publication 800-63B, Digital Identity Guidelines, NIST, Apr 30 2017

7 Politician's fingerprint 'cloned from photos' by hacker, BBC News, Dec 29, 2014

Octopus Authenticator

Octopus Authenticator by Secret Double Octopus Is state of the art push mode authentication – and the only market solution that uses secret sharing to eliminate any single point of security failure. Key theft, enrollment eavesdropping, and other MITM attacks yield insufficient information for any successful attack. While the security level is significantly increased, the complexity is completely concealed from the user, and approval is given with a single tap in response to a clear and meaningful push notification.

Octopus Authenticator - Multi-shield protection



- No need to type anything
- Multiple routes with independent protection

As experts in authentication, we can help businesses ensure that their systems are as secure as possible and make the shift towards the industry's most advanced authentication method.

Secret Double Octopus has developed the world's only keyless multi-layer authentication technology to protect identity and data across cloud, mobile and IoT environments. Based on Secret Sharing algorithms, originally developed to protect nuclear launch codes, Secret Double Octopus' technology prevents cyber attackers from accessing enough critical information to be useful for attacks, eliminating brute force, man-in-the-middle, PKI manipulation, key theft and certificate authority weaknesses.

SECRET DOUBLE OCTOPUS

For more information, contact us:
contact@doubleoctopus.com
www.doubleoctopus.com