

SDI vs MFA vs Passkey

SDI vs MFA with Traditional Credentials

	SDI	MFA with Traditional Credentials
Identity verification	A nonce (big number used once), similar to OTP (One Time Password), but 32-bytes long, is sent encrypted to the user, and the user's device must decrypt it. <u><i>Phishing or spoofing is ineffective, as the nonce originates from a server, and it must be decrypted before it can be sent back.</i></u>	Shared secrets (passwords, tokens) that are sent over the network for comparison. <u><i>Phishing or spoofing is effective as the password originates from the user, and it doesn't change often, if ever.</i></u>
Password-less operation	Requires a passphrase to decrypt the user's PCM, but that passphrase never traverses any network. Once the PCM is on a device, authorizations with service providers are password-less. <u><i>Single Sign-On (SSO) with PCM cached on a device. Authorizations are fully password-less.</i></u>	It is password-based. <u><i>No</i></u>
ZTA (Zero Trust Architecture) friendly	Can be triggered to authenticate by push notifications or by the 3 rd party app that is SDI-ready. <u><i>Operates seamlessly with ZTA.</i></u>	Traditional credentials are prohibitively cumbersome in that environment, and MFA only makes the process more difficult. <u><i>Practically useless with ZTA.</i></u>
Authenticated transaction	Transaction content (directive) that is bundled with a nonce and signed. This allows sending critical information locked with an authenticating component, e.g., the amount paid or the action to be performed. <u><i>This allows for quick confirmation, denial, or request of action when controlling especially tangible assets, like cars, buildings, etc.</i></u>	<u><i>Non-existent</i></u>
Robustness against phishing	There is nothing to phish as there are no credentials in use. The malicious server will fail to provide the nonce that can be decrypted. Even if the encrypted nonce is stolen, it will not be accepted by the legitimate server upon decryption. With a malicious proxy server, the dynamic certificate pinning will detect the intrusion. <u><i>Provides robust protection against phishing.</i></u>	Verification codes that are sent via email or SMS can be stolen when in motion due to security weaknesses in both methods. Authenticators generating the codes on a separate device have the same problem, as the codes can be stolen on a spoofing server. <u><i>Adds complexity without the necessary robustness.</i></u>

Spoofing detection	The same as above in “Robustness against phishing”.	The same as above in “Robustness against phishing”.
Registration vulnerabilities	It recommends in-person verification of users to obtain the authentication account by issuing a one-time activation code. It is to prevent registration with stolen identity data. Authorization registration is automated because it involves attestation with the authentication service. However, it also requires an activation code. <u>Impersonation is possible but difficult and depends on how robust the admission of new users is.</u>	Knowledge of a password is assumed as original verification. <u>Once a password is stolen (phished, spoofed, etc.), impersonation is easy.</u>
Robustness to device theft	It has two types of kill switches: one on the user’s side, which can trigger their account into a panic mode, and the other is available in each authorization service and can be used to permanently disable the user’s account. Re-registration is not possible unless the account is deleted and a new activation code is issued. <u>There is a small chance that a stolen and active device with the SDI app turned on can be used to impersonate the owner. However, that window is limited to the time when the owner logs in from a different device with panic mode, which will eventually disable the SDI app on a stolen device.</u>	There is no protection against the consequences of theft of a device, except for the user calling the services that had the email or mobile number registered as the second factor of authentication. <u>There is virtually no effective protection.</u>
User friendliness	Device independence makes it easier to communicate even if the preferred device is not available or broken. Each transaction is almost seamless to the user. <u>Ease of use with improved security.</u>	Complex operation using traditional credentials with an additional step and delay in handling verification codes, and the registered device must be available and operational for the communication to succeed. <u>Adds complexity without the expected security.</u>

SDI vs Passkey/FIDO

	SDI	Passkey/FIDO
Identity verification	A nonce (big number used once), similar to OTP (One Time Password), but 32-bytes long, is sent encrypted to the user, and the user’s device must decrypt it. <u>Since the public key is used as a shared secret, the origin of a nonce comes with verification of whether it can be decrypted.</u>	A signature over a challenge that the user’s device receives from a server. <u>There is no verification that the challenge came from the legitimate server, except for the response URL.</u>

Password-less operation	Requires a passphrase to decrypt the user's PCM, but that passphrase never traverses any network. Once the PCM is on a device, authorizations with service providers are password-less. <u>Single Sign-On (SSO) with PCM cached on a device. Authorizations are fully password-less.</u>	Once set up, it can operate password-less, despite being considered the second factor of authentication. However, when a device must be changed, especially to a different brand, the registration process of the new device must be repeated, and the password used. The password is still in use and should be different for each site. <u>Storage and maintenance of passwords remains so is potential for phishing or spoofing.</u>
ZTA (Zero Trust Architecture) friendly	Can be triggered to authenticate by push notifications or by the 3rd party app that is SDI-ready. <u>Operates seamlessly with ZTA.</u>	Auto re-authentication is built into the FIDO protocol, so if it is used as the primary authentication, it can operate in the ZTA environment. <u>Can operate in the ZTA environment, though it was not intended to.</u>
Authenticated transaction	Transaction content (directive) that is bundled with a nonce and signed. This allows sending critical information locked with an authenticating component, e.g., the amount paid or the action to be performed. <u>This allows for quick confirmation, denial, or request of action when controlling especially tangible assets, like cars, buildings, etc.</u>	<u>Non-existent</u>
Robustness against phishing	There is nothing to phish as there are no credentials in use. The malicious server will fail to provide the nonce that can be decrypted. Even if the encrypted nonce is stolen, it will not be accepted by the legitimate server upon decryption. With a malicious proxy server, the dynamic certificate pinning will detect the intrusion. <u>Provides robust protection against phishing.</u>	It is robust against phishing during normal operation. However, since the password is still needed for the registration of new devices, the user can still be tricked into a phishing scheme. <u>It improves robustness against phishing, though still vulnerable.</u>
Spoofing detection	The user's device may generate a nonce and request the server to decrypt it, thus providing stronger verification of the server. In addition, the user's device may request the SDI server to provide its certificate that can be compared with the one received by TLS (Transport Layer Security). <u>Robust detection, even in attacks with a malicious proxy server.</u>	Matching response URL. <u>Weak detection, especially with hacked DNS.</u>

Registration vulnerabilities	It recommends in-person verification of users to obtain the authentication account by issuing the one-time activation code. It is to prevent registration with stolen identity data. Authorization registration is automated because it involves attestation with the authentication service. However, it also requires an activation code. <u><i>Impersonation is possible but difficult and depends on how robust is the admission of new users.</i></u>	Attestation focuses on a device, though it is very weak due to batching of certificates, but it is also unnecessary. It assumes that if the user knows the password, the user is legitimate. Registration with stolen identities is not even considered. A criminal can steal a password and register their device as legitimate. <u><i>Prone to stolen identities.</i></u>
Robustness to device theft	It has two types of kill switches: one on the user's side, which can trigger their account into a panic mode, and the other is available in each authorization service and can be used to permanently disable the user's account. Re-registration is not possible unless the account is deleted and a new activation code is issued. <u><i>There is a small chance that a stolen and active device with the SDI app turned on can be used to impersonate the owner. However, that window is limited to the time when the owner logs in from a different device with panic mode, which will eventually disable the SDI app on a stolen device.</i></u>	Just like with MFA and traditional credentials, there is no protection against the consequences of theft of a device, except for the user calling the services that had accepted the device as an authenticator. <u><i>There is virtually no effective protection.</i></u>
User friendliness	Device independence makes it easier to communicate even if the preferred device is not available or broken. Each transaction is almost seamless to the user. <u><i>Ease of use with improved security.</i></u>	Once set up, it is very user-friendly to operate. However, users still need to maintain their collection of passwords. In addition, a broken or lost device can create a real problem, as the keys are lost if not backed up, the backup is not up to date, or the user wants to upgrade to a different brand of device. <u><i>It is easier in day-to-day operations, though it adds another layer of concern.</i></u>

Summary

It is important to emphasize here that although in cybersecurity an authenticator on a separate device owned by the user is considered as an additional factor of authentication, it actually isn't, because it doesn't eliminate the vulnerability to phishing even with Passkey. Hackers can easily forward the QR code to be scanned by the authenticator, so the authentication succeeds, despite that the user is connected to a malicious server, and the criminals can take over the session. Passkey is only effective if it is in the same app, not just the same device, and under the condition that the DNS wasn't hacked.

	SDI	Passkey/FIDO
Password-less?	Authentication: Single Sign-On Authorizations: password-less	Authentication to a device and password-less authorizations.
A new device	A new Single Sign-On	New registrations with passwords to all service providers.
Is phishing resistant	It is because there is nothing to phish.	It is still vulnerable to phishing because passwords are needed for the registration of new devices.
Can a hacker register their device?	Very unlikely since the original registration blocks further registrations. New devices must obtain keys from the authentication service regardless of their brand.	A hacker can phish a password and register their device as legitimate and then continue to impersonate the original user. This feature is by design.
My device was lost or stolen	Log in to your authentication account from another device set to panic mode. Buy a new device and log in to your authentication account set to normal mode, but do it about an hour after the panic was set, and you are ready.	Call all service providers to remove registrations of your device. Buy a new device and register with all service providers (using your passwords).
My device broke	Buy a new device and log in to your authentication account, and you are ready.	Buy a new device and restore your keys if the device is compatible and the backup is current. Otherwise, register the new device with all service providers (using your passwords).
I'm not sure if I was connected to the right site	Don't worry, dynamic certificate pinning would detect a malicious site.	Call your DNS provider. They may thank you for telling them that they were hacked.