12.12.2024

Multi-factor authentication and passkeys

In a digital environment, it is critical to protect your user accounts. By combining several security factors, multi-factor authentication (MFA) offers greater protection than traditional passwords.

Multi-factor authentication (MFA) is a security method best known currently under the sub-term “two-factor authentication” (2FA). MFA is more comprehensive and describes all authentication methods requiring two security factors or more though. In the process, it combines authentication factors such as knowledge (e.g. a password), ownership (e. g. a smartphone) and inherence (e.g. fingerprints). The aim is to create a multi-layered defence and better protect user accounts against the most common threats such as phishing and password theft.

In doing so, MFA solves some central security problems: Even if a password, i.e. one factor, is stolen or compromised, attackers still cannot gain access, since the other factors are missing. Combining several security factors significantly increases the level of protection and is essential nowadays.

A new approach for an easier, more user-friendly authentication technology consists of passkeys (https://www.ebas.ch/en/passkeys/) . Passkeys are meant to completely replace traditional passwords and are based on secure authentication methods such as biometric characteristics. MFA is already integrated into passkey technology. Instead of a password, users use a biometric characteristic or a PIN on their device where the private key remains safely stored on it and is never transmitted anywhere. Passkeys strengthen the password aspect of the log-in process and don’t add a further security layer via another authentication factor.

You can read up more extensively on this topic in our article on Passkeys. (https://www.ebas.ch/en/passkeys/)