At the core of FIDO2 lies the WebAuthn (Web Authentication) standard, which defines a number of requirements for a conforming website, browser and compatible authenticator. In essence it’s a public key-based security scheme, whereby one has to register a device that will function as the authenticator. This can be a laptop with a fingerprint scanner, Windows Hello, Apple FaceID, or a smartphone with such biometrics options. Alternatively a PIN code can be used instead of biometrics.

In addition to this, CTAP (Client To Authenticator Protocol) allows one to link a device like a smartphone with a laptop to act as an authenticator for the browser on the laptop using NFC, USB or BLE (if supported). Regardless of the setup, there’s always the remote service with which one registers or already has registered the authenticator device. This is similar to how one would register their public SSH key at a site like Github, yet this also means that you would want to register two or more authenticators for a service, in case one is lost, stolen or otherwise becomes unavailable.

Here the device is ‘What you have’, while biometrics would be ‘What you are’, or alternatively a PIN code or similar could provide ‘What you know’.