FIDO (Fast IDentity Online)

FIDO (*Fast IDentity Online*) je soubor otevřených technických standardů pro bezpečné ověřování uživatelů na internetu, vyvinutý a spravovaný aliancí FIDO Alliance (v úzké spolupráci s konsorciem W3C). Hlavním cílem standardů FIDO je eliminovat závislost na tradičních textových heslech, chránit uživatele před moderními formami phishingu a zjednodušit proces přihlašování pomocí bezheslové (*Passwordless*) autentizace.

Architektura a klíčové standardy

Základním stavebním kamenem FIDO je asymetrická kryptografie (kryptografie veřejného klíče). Místo odesílání a sdílení tajného hesla se serverem se při registraci vygeneruje unikátní pár klíčů – soukromý a veřejný.

FIDO U2F (Universal 2nd Factor)

Starší standard navržený primárně jako vysoce bezpečný druhý faktor (MFA) doplňující klasické heslo. Uživatel zadá heslo a následně potvrdí přihlášení fyzickým hardwarovým tokenem (např. přes USB nebo NFC). Zásadní výhodou oproti SMS nebo TOTP kódům z aplikací je kryptografické ověření domény, což zcela brání útokům typu AiTM phishing.

FIDO UAF (Universal Authentication Framework)

Standard zaměřený na zcela bezheslové přihlašování. Uživatel k přihlášení využívá biometrii (otisk prstu, rozpoznání obličeje) nebo lokální PIN přímo na svém koncovém zařízení (např. na chytrém telefonu). Zařízení po lokálním ověření uživatele kryptograficky potvrdí identitu serveru.

FIDO2 a WebAuthn

Nejnovější a nejdůležitější iterace, která plně integruje principy FIDO do webových prohlížečů a operačních systémů. Skládá se ze dvou klíčových komponent:

WebAuthn (Web Authentication API): Standard W3C, který jako webové API umožňuje aplikacím a stránkám komunikovat s autentizátory (hardwarovými zařízeními nebo softwarovými klíči) prostřednictvím běžného webového prohlížeče.

CTAP (Client to Authenticator Protocol): Protokol, který umožňuje externím autentizátorům (např. klíče YubiKey připojené přes USB, NFC nebo Bluetooth) bezpečně komunikovat s klientským zařízením (počítačem, telefonem).

Jak funguje proces ověření

Zásadním rozdílem oproti tradičnímu heslu je skutečnost, že při využití FIDO se na server nikdy nepřenáší žádné sdílené tajemství, které by šlo odposlechnout nebo ukrást.

Fáze registrace

Uživatel je webovou službou vyzván k vytvoření nového pověření (*Credential*).

Autentizátor (např. hardwarový klíč nebo Windows Hello na notebooku) vygeneruje nový, pro tuto konkrétní službu zcela unikátní pár kryptografických klíčů.

Soukromý klíč zůstává bezpečně uložen v hardwaru (např. TPM čip, Secure Enclave nebo kryptografický čip tokenu) a nikdy neopouští zařízení.

Veřejný klíč je odeslán na server služby, kde je v databázi spárován s uživatelským účtem.

Fáze přihlášení (Autentizace)

Webová služba vygeneruje unikátní výzvu (*Challenge*) a zašle ji prohlížeči uživatele.

Prohlížeč předá výzvu autentizátoru spolu s metadaty o aktuální doméně (např. `mojebanka.cz`).

Autentizátor vyzve uživatele k interakci (dotyk senzoru hardwarového klíče, skenování obličeje, zadání lokálního PINu). Tím uživatel potvrdí svou přítomnost a odemkne soukromý klíč.

Autentizátor podepíše přijatou výzvu svým soukromým klíčem a odešle kryptografický podpis zpět na server.

Server ověří platnost podpisu pomocí veřejného klíče uloženého při registraci. Pokud se podpisy shodují, je identita uživatele ověřena a získá přístup.

Hlavní výhody standardu FIDO

Absolutní odolnost vůči phishingu: Vzhledem k tomu, že prohlížeč automaticky předává autentizátoru informaci o přesné webové doméně (*Origin*), podepíše FIDO klíč výzvu výhradně pro legitimní web. Pokud je uživatel naveden na podvodnou stránku (např. `mojebamka.cz` s překlepem), klíč odmítne požadavek zpracovat, protože doména nesouhlasí s tou registrační.

Ochrana soukromí: Biometrická data a lokální PINy nikdy neopouštějí koncové zařízení uživatele. FIDO nebuduje ani nevyužívá žádnou centralizovanou databázi biometrických údajů; biometrie zde slouží striktně a pouze k lokálnímu zpřístupnění kryptografického klíče v zařízení.

Prevence následků úniků dat (Data Breaches): I kdyby se útočníkům podařilo napadnout databázi poskytovatele služby a celou ji stáhnout, získají pouze databázi veřejných klíčů. Ty jsou pro útočníka k přihlášení zcela bezcenné. Bez fyzického přístupu ke konkrétním zařízením (autentizátorům) uživatelů nelze vygenerovat platný přihlašovací podpis.

Passkeys (Přístupové klíče): Moderní rozšíření standardu FIDO2 prosazované společnostmi Apple, Google a Microsoft. Umožňuje bezpečné zálohování a synchronizaci FIDO pověření napříč zařízeními uživatele v rámci cloudového ekosystému (např. přes iCloud Keychain nebo Google Password Manager), čímž elegantně řeší obavy uživatelů ze ztráty fyzického hardwarového tokenu.