Ověřování uživatelů standardem WebAuthn

ESO9 international a.s.
U Mlýna 2305/22, 141 00 Praha 4 – Záběhlice
tel.: +420 228 809 000
e-mail: info@eso9.cz
www.eso9.cz

Zpracoval:	Urych Tomáš
Dne:	16.3.2023
Revize:	Urych Tomáš
Dne:	12.2.2024

Obsah

1. WebAuthn

Web Authentication (zkráceně WebAuthn) je standard ověřování uživatelů na webu, který vznikl ve spolupráci konsorcia W3C a aliance FIDO (Fast IDentity Online). FIDO Alliance je sdružení „velkých" hráčů v oblasti IT jako Google, Microsoft, Apple, Amazon nebo Intel. Standard WebAuthn tak podporují všechny významné webové prohlížeče (Google Chrome, MS Edge, Apple Safari) i operační systémy (Windows, Android, iOS).

Cílem standardu WebAuthn je zvýšení bezpečnosti na Internetu. Hlavním prostředkem je pak odstranění hesel pro přihlašování k webovým aplikacím a službám a jejich náhrada tzv. bezheslovou autentikací. Ta je založena principech asymetrické kryptografie, tj. použití veřejného a privátního klíče. Vlastní realizace pak spočívá nejčastěji v používání HW prostředků (tzv. autentikátorů), typicky čtečky otisků prstů, IR kamery pro rozpoznávání obličejů či USB/NFC/BLE tokenů. Ty jsou pak implementovány v technologiích jako Windows Hello či Apple Touch ID.

Hlavní výhodou oproti ověřování uživatelským jménem a heslem je fakt, že v tomto standardu uživatel nikde nezadává žádné ověřovací údaje, které lze zcizit či podvrhnout. Komunikačním kanálem mezi klientem a serverem (tj. Internetem) se posílají pouze veřejné klíče, které jsou ovšem bez privátních klíčů k ničemu. Privátní klíče přitom nikdy neopustí klientskou stanici. Vygenerovaná dvojice klíčů (veřejný a privátní) je vždy platná pouze pro zdrojový web, čímž se zároveň odstraňuje potenciální problém s phishingem.

Podrobnější informace ke standardu WebAuthn lze najít na https://webauthn.guide/ nebo https://fidoalliance.org/how-fido-works/.

2. Implementace WebAuthn v ESO9

2.1 Web pro autentikaci

Pro použití ověřování WebAuthn je třeba jednorázově nainstalovat a nakonfigurovat web pro autentikaci. Jeho instalace je součástí standardní distribuce ESO9. Web se instaluje na aplikačním serveru a při provozu ESO9 bude obsluhovat požadavky uživatelů na jejich registrace a přihlašování a to ze všech provozovaných aplikací (podobně, jako *Support web* obsahuje všechny skripty/styly/ikony všech provozovaných aplikací).

Web je vytvořený v prostředí *.NETu* (nikoli *.NET Frameworku*), pročež jej nelze instalovat automaticky s aplikačním serverem ESO9.

2.1.1 Protokol HTTPS

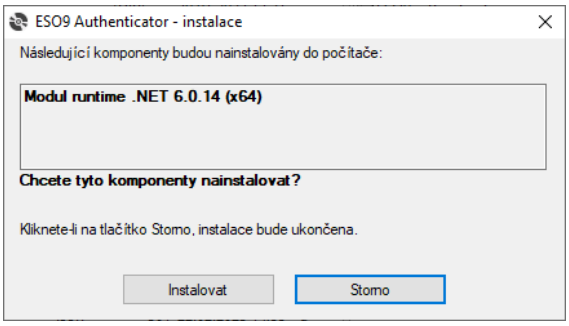
Web pro autentikaci musí být provozován na protokolu HTTPS, tj. website, který tento web hostuje, musí mít SSL certifikát. Tento certifikát musí být klientskými stanicemi považován za důvěryhodný. To znamená, že certifikát jeho vydavatele je na klientských stanicích zařazen ve skupině důvěryhodných kořenových certifikačních autorit. Self-signed TLS/SSL certifikáty proto nelze pro WebAuthn použít.

2.1.2 Instalace webu pro autentikaci

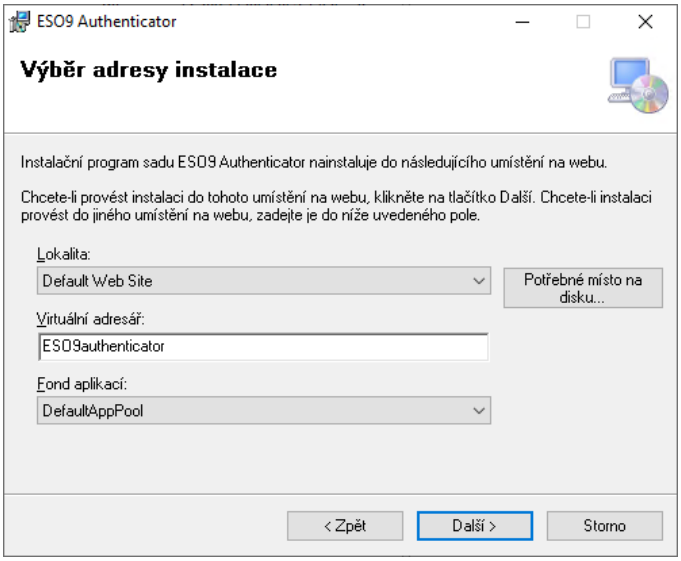
Instalace webu pro autentikaci se nachází ve složce *ESO9 Authenticator* ve standardní distribuci ESO9. Spouští se běžným způsobem, tj. spuštěním programu *setup.exe*.

Pro svou funkčnost web potřebuje programové prostředí *.NET 6*. To sestává z programového runtimu a podpory IIS; obě tyto části obsahuje tzv. *Hosting Bundle*, který lze stáhnout ze stránky https://dotnet.microsoft.com/en-us/download/dotnet/6.0.

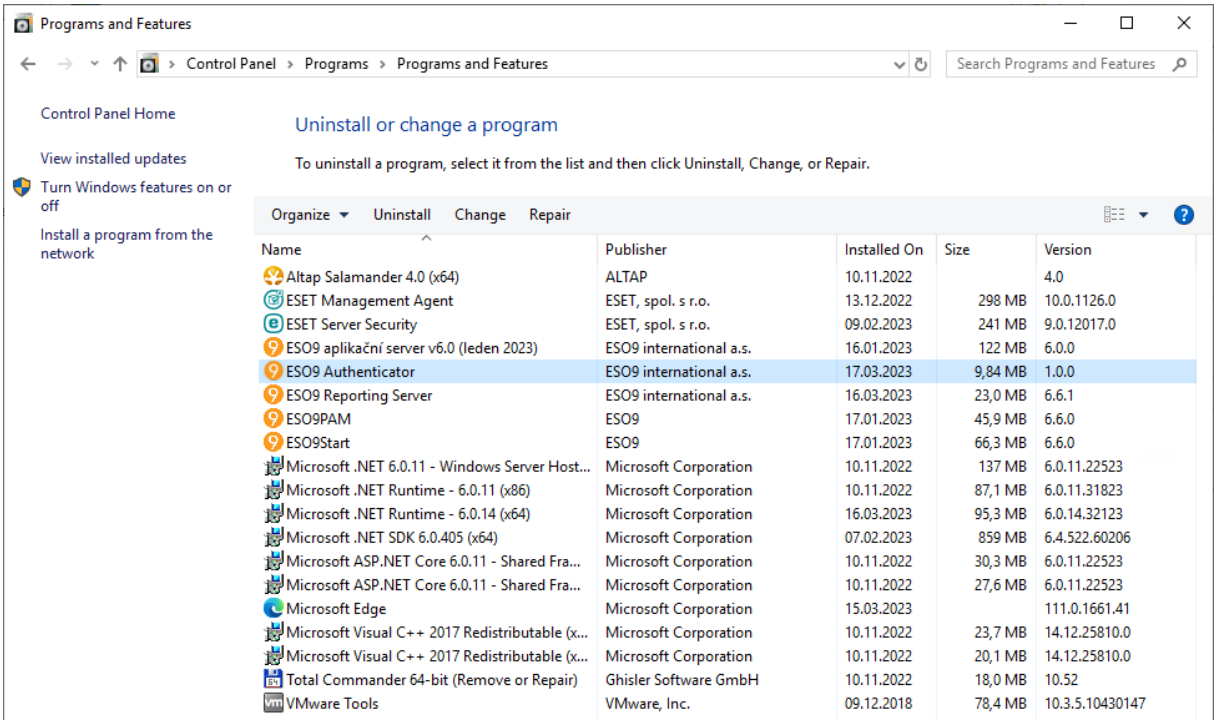
Přítomnost runtimu programového prostředí *.NET 6* kontroluje i instalační program. Je-li toto prostředí již nainstalované, spustí se rovnou instalace webu. Pokud není nainstalované, nabídne se jeho jednorázové stažení a instalace:



Po dokončení se spustí vlastní instalace webu. Během ní se zadává jméno webu a jméno aplikačního poolu (fondu aplikací). Jméno webu je pevně dané (*ESO9authenticator*), jméno aplikačního poolu lze zvolit libovolně:



Po úspěšné instalaci se web pro autentikaci objeví v konzoli IIS a v seznamu nainstalovaných programů:

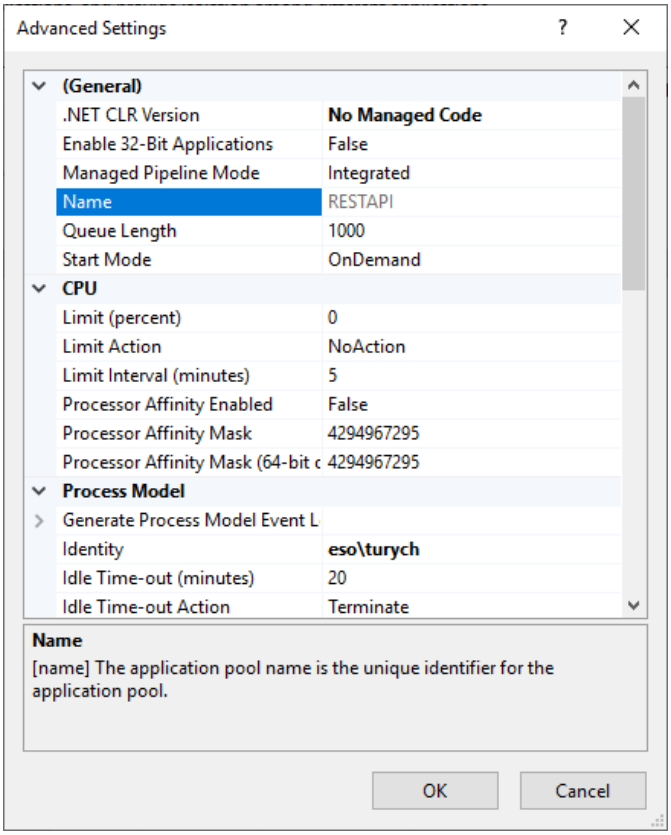


2.1.2.1 Aplikační pool

V konzoli pro správu webového serveru IIS založíme nový aplikační pool.

Klíčové vlastnosti budou:

- *.NET CLR Version* = No Managed Code
- *Managed pipeline mode* = Integrated
- *Load User Profile* = True
- *Identity* = uživatelský (Windows) účet, pod nímž běží na stejném serveru služba aplikačního serveru ESO9



2.1.3 Konfigurace webu pro ověření

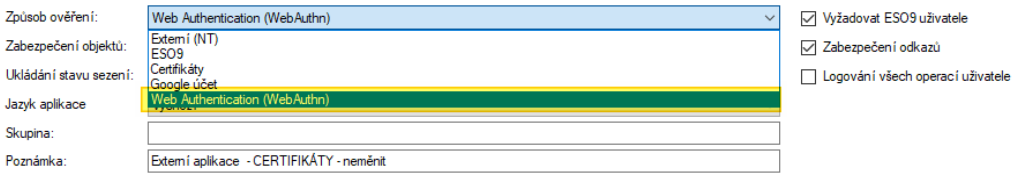
Po instalaci je třeba ještě dokončit konfiguraci webu pro autentikaci. Konfigurace se provádí v souboru *appsettings.json*. V souboru se upraví 2 položky:

```
"serverDomain": "example.com ",
"origins": [ "https://example.com" ],
```

- *serverDomain* – jméno serveru, na němž běží web pro autentikaci. Jméno je použito při tvorbě pověření. Oproti této doméně se registruje použitý autentikátor. Daný autentikátor může být pro danou doménu vždy pouze jeden.
- *origins* – URL adresa, z níž je server s webem pro ověření dostupný. Zadává se bez případného explicitního TCP portu a musí používat pouze HTTPS protokol s platným certifikátem. Používá se k ochraně proti phishingu.

2.2 Správce ESO9

Ve Správci ESO9 standardním způsobem nastavíme způsob autentikace ve vybrané aplikaci na *Web Authentication (WebAuthn)*:



3. Přihlašování uživatelů do aplikace ESO9

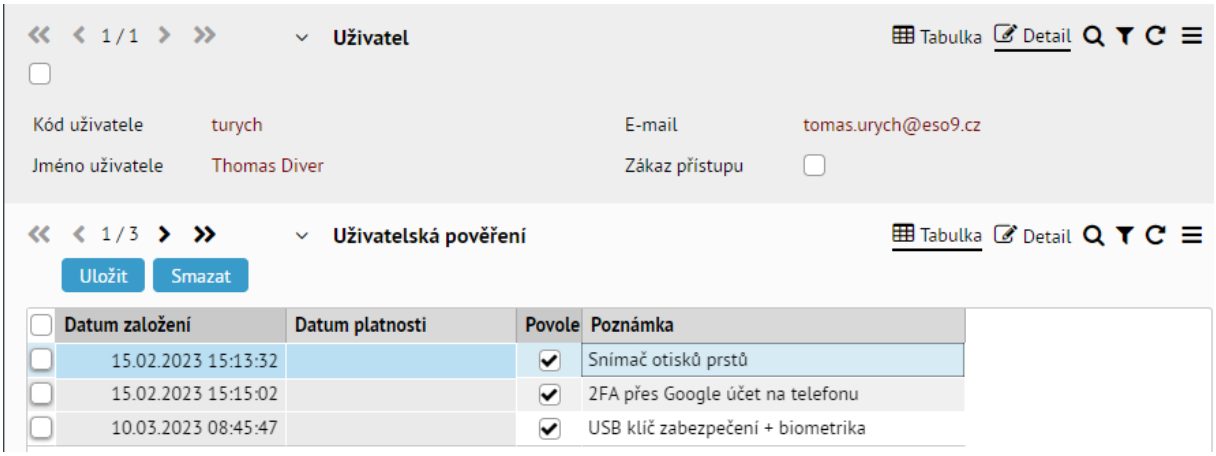
Uživatel se do aplikace přihlašuje běžným způsobem, tj. kliknutím na jméno aplikace ve vstupní stránce. Je-li v aplikaci nastaveno přihlašování přes WebAuthn, dojde k přesměrování na web *ESO9authenticator*, který jsme nainstalovali v kapitole 2.1.2.

3.1 Pověření uživatele

Oproti například formulářovému ověření, kde je uživatel ověřen vůči své identitě, tedy vůči jednomu záznamu v tabulce uživatelů, může mít uživatel při přihlašování standardem WebAuthn více tzv. pověření (credentials). Počet pověření je dán počtem autentikátorů a je přitom jedno, zda se jedná o více autentikátorů na jednom zařízení nebo více zařízeních.

V praxi tak uživatel zaregistruje jedno pověření ze čtečky otisků prstů na svém notebooku, další z rozpoznávání obličejů na svém mobilním telefonu a ještě další například ze svého USB tokenu, kterým se ad hoc přihlašuje z různých PC.

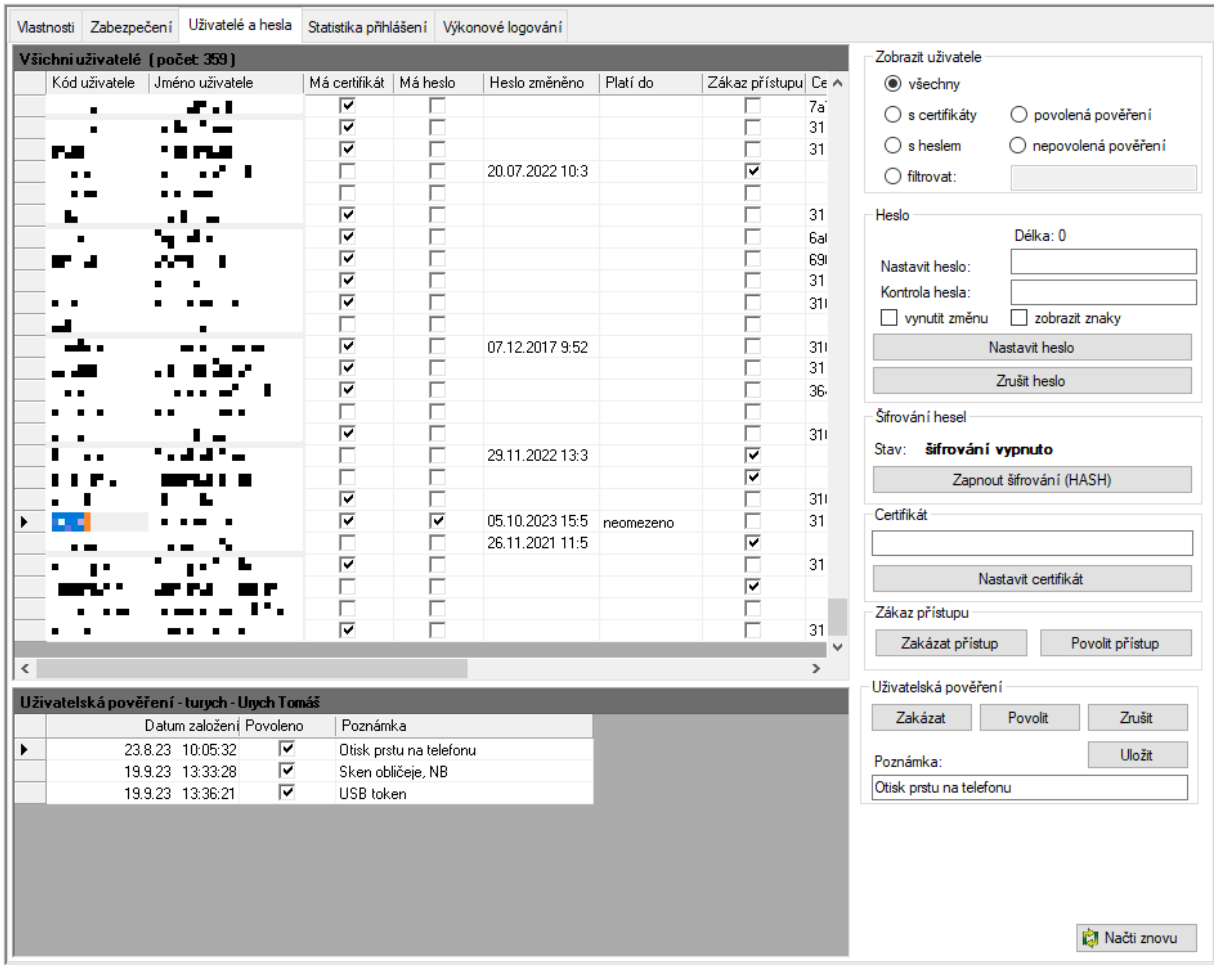
Všechna pověření jsou uložena v aplikační databázi v tabulce *WEBAUTHNCREDENTIALS*. Po registraci nového pověření je toto ve stavu „Zakázáno“, tj. není povoleno se jím do aplikace přihlásit. Povolení pro použití daného autentikátoru uděluje uživateli správce aplikace.



Jednotlivá pověření lze přenášet mezi aplikacemi (resp. databázemi). V případě přístupu jednoho uživatele do více aplikací tak není nutné jej registrovat vždy znovu do všech aplikací.

3.2 Pověření uživatele ve Správci ESO9

Ve Správci ESO9 lze s pověřeními pracovat stejně, jako přímo v aplikaci ESO9. Tj. jednotlivá zaregistrovaná pověření lze povolovat, zakazovat či mazat a lze u nich editovat poznámku o původu daného pověření.



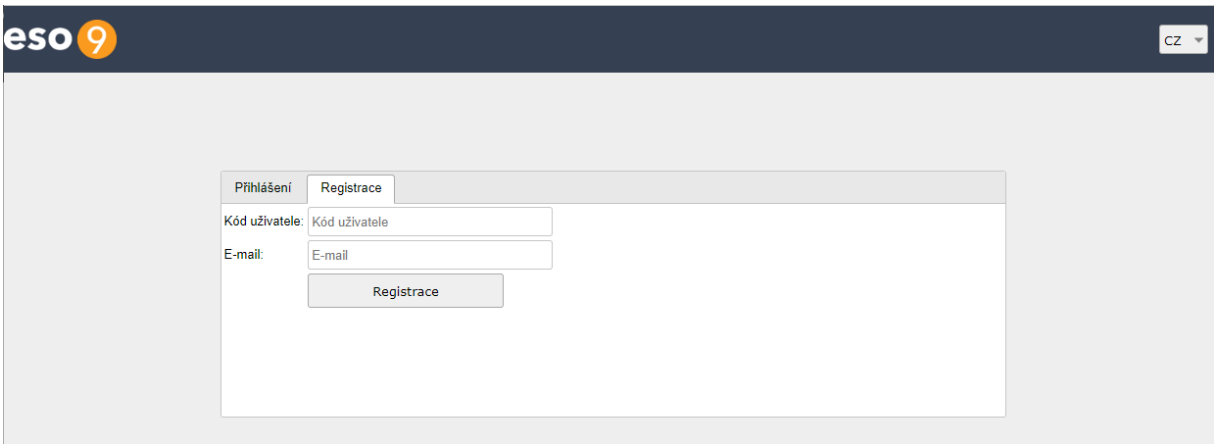
3.3 Web pro autentikaci

Web pro autentikaci (viz též kapitola 2.1) slouží zároveň pro registraci uživatelů i pro jejich přihlášení. Web neobsahuje žádné stránky či formuláře, pouze poskytuje programové služby pro registrace a přihlašování uživatelů.

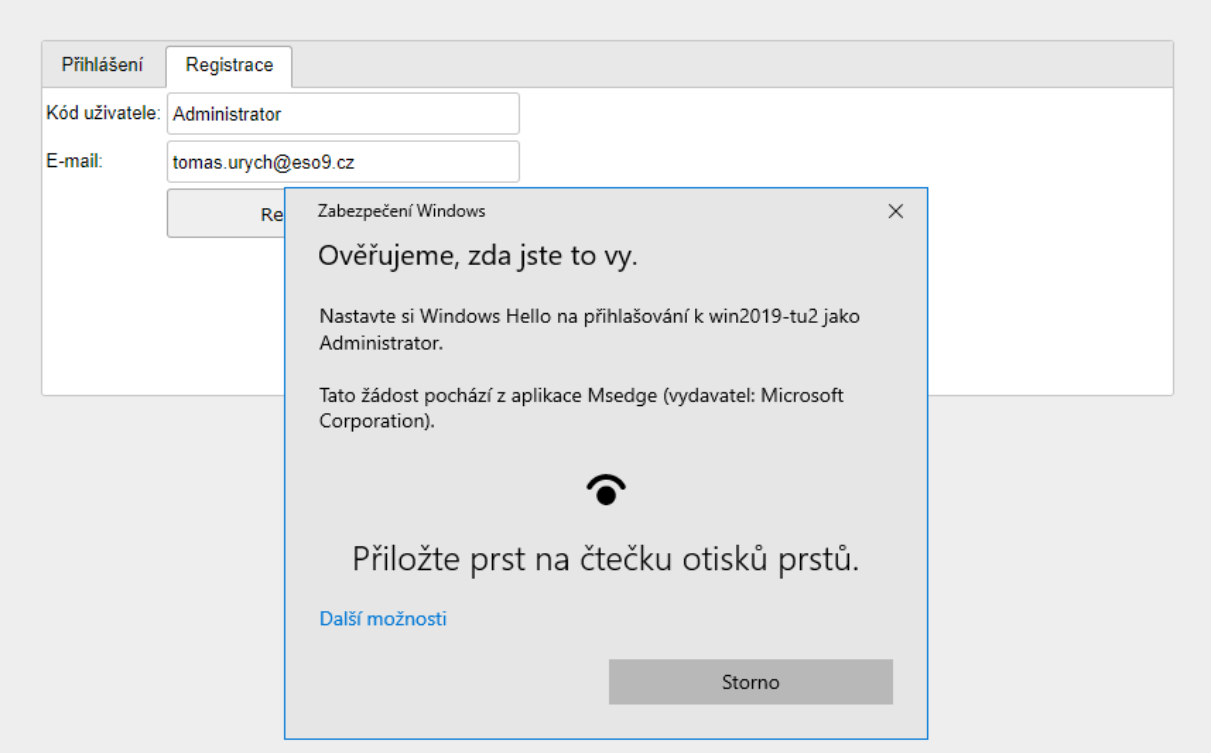
Web pro autentikaci je obsluhován z formulářů ve Start adresáři *webauth\login.htm* a *webauth\login.bs.htm*.

3.4 Registrace uživatele

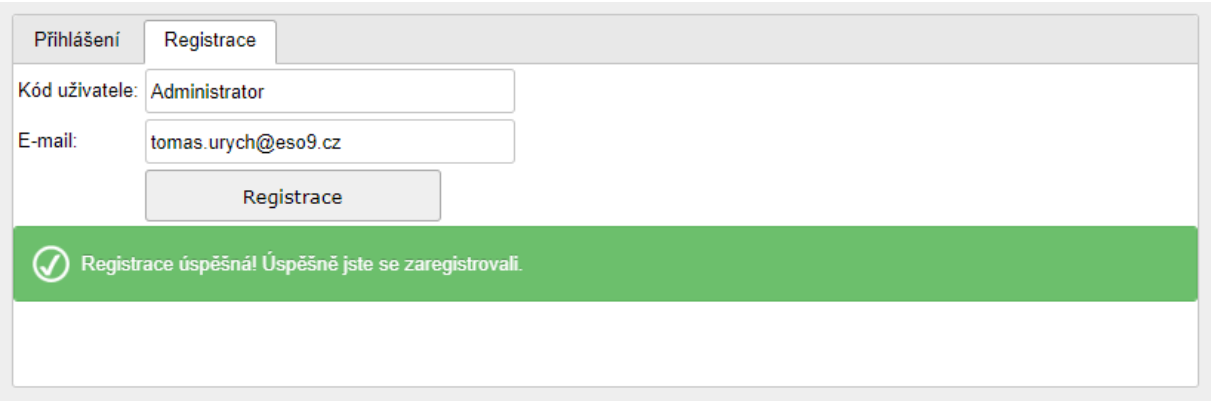
Každý uživatel si musí v aplikaci nejprve zaregistrovat své pověření. Pověření se registruje na záložce *„Registrace“* zadáním přístupového jména uživatele (resp. jeho kódu v tabulce uživatelů) a e-mailové adresy:



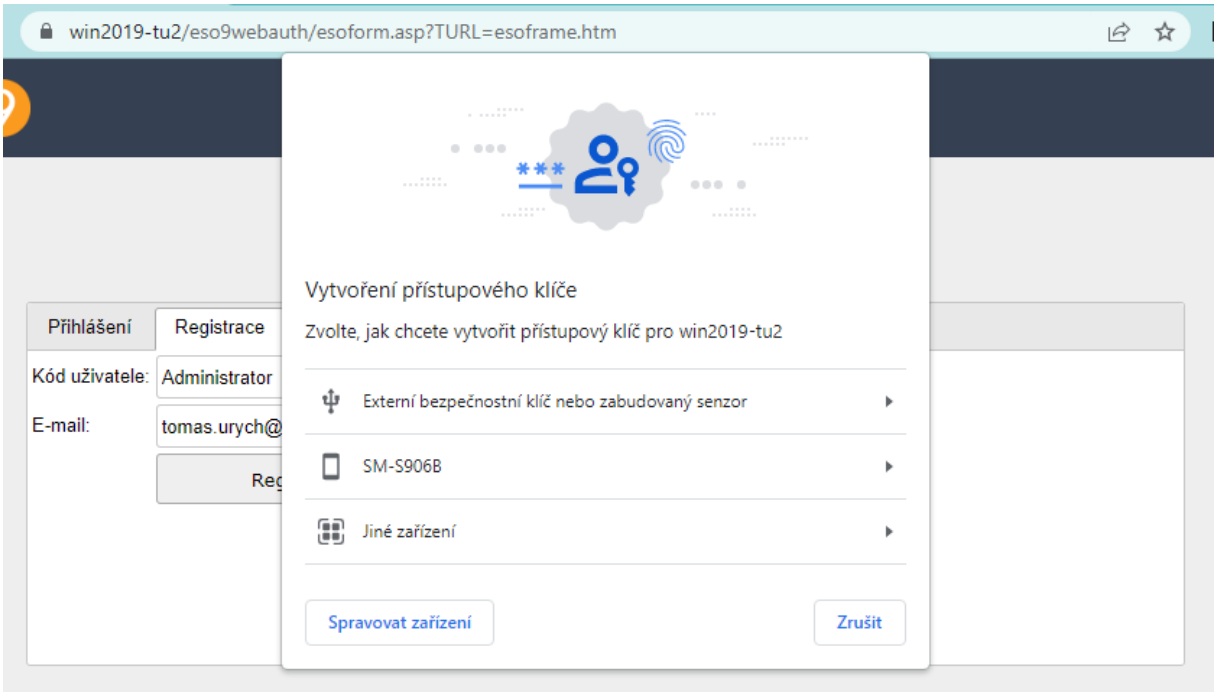
Pokud jsou zadané přístupové údaje v tabulce uživatelů nalezeny a jsou správné, nabídne se uživateli k registraci primárně dostupný autentikátor:



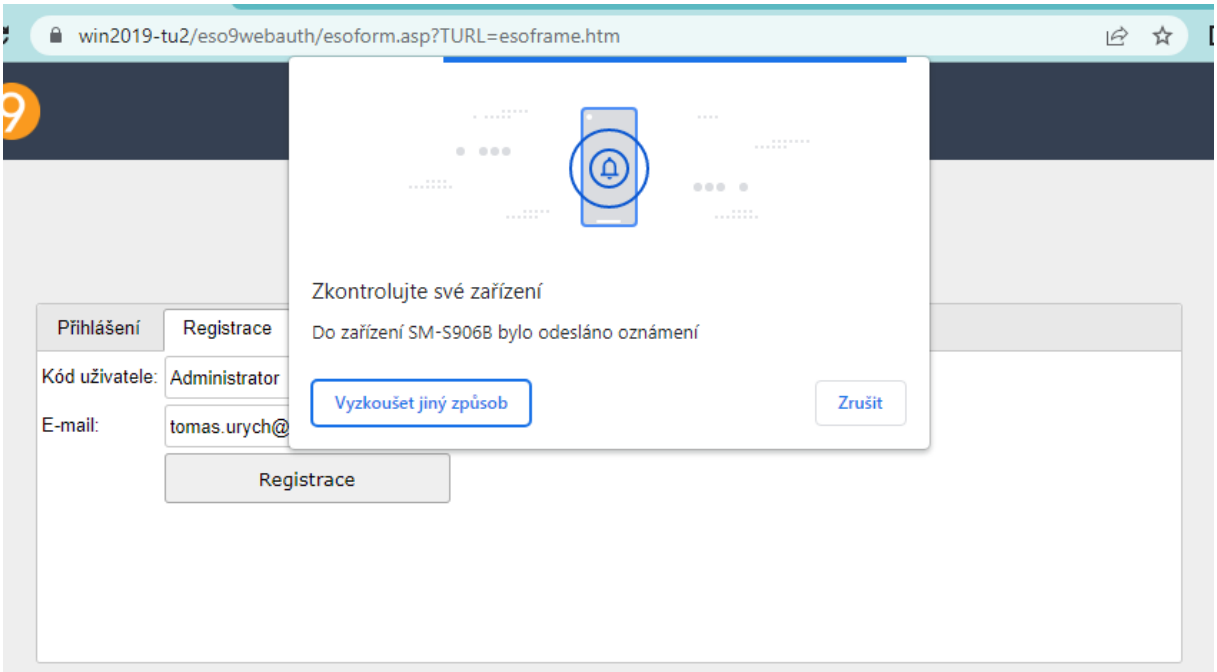
Po úspěšném ověření např. otisku prstu ve Windows Hello se objeví informace o registraci uživatelského pověření v aplikaci:



Uživatel si samozřejmě může vybrat z dalších autentikátorů, které má na daném zařízení dostupné. Pomocí prohlížeče Google Chrome a mobilního telefonu s Androidem lze např. zrealizovat i dvoufaktorové ověřování: uživatel si ve svém prohlížeči Chrome nastaví v sekci *ochrana soukromí a zabezpečení - telefon jako bezpečnostní klíč*. Následně se mu při registraci nebo přihlášení do ESO9 objeví v prohlížeči možnost použít jako klíč zabezpečení svůj mobilní telefon (zde *SM-S906B*):



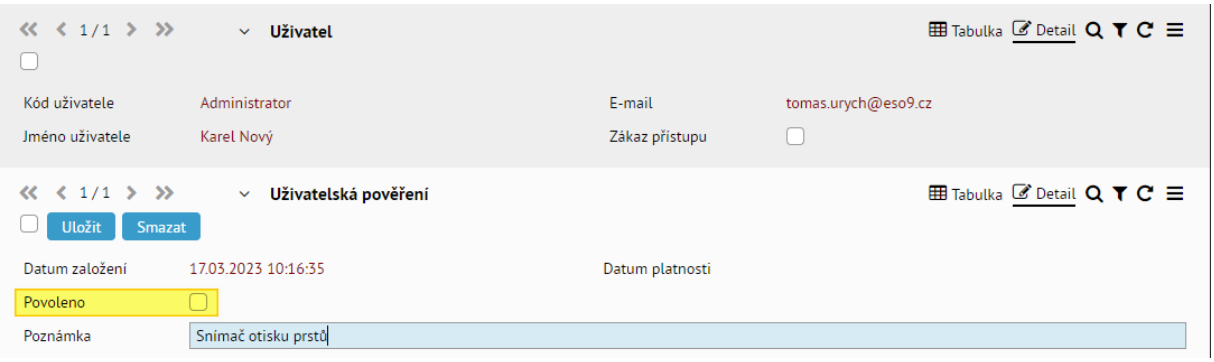
Prohlížeč odešle do telefonu požadavek na ověření uživatele:



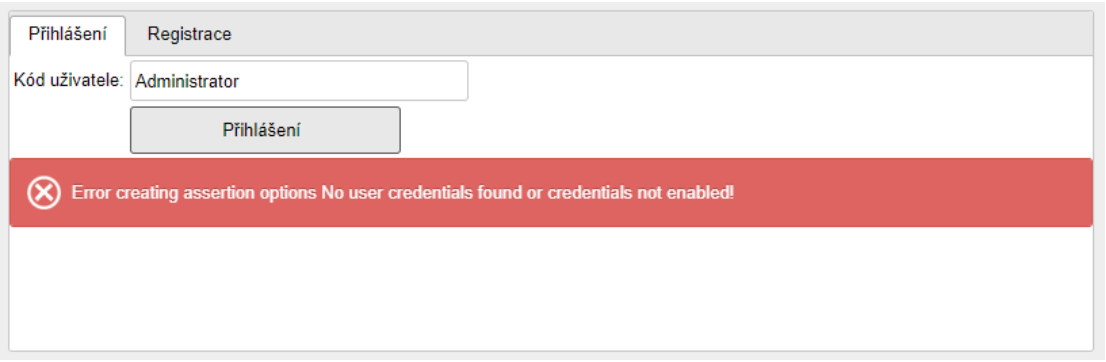
… a uživatel v mobilním telefonu potvrdí svou identitu obvyklým způsobem (otisk prstu, sken obličeje, gesto, …). Screenshot ověření identity zde bohužel nelze pořídit, výrobce OS tuto možnost z bezpečnostních důvodů zakázal.

3.5 Povolení používání pověření

Zaregistrované pověření nelze okamžitě začít používat, v aplikaci jej musí nejprve schválit její správce. Do poznámky si přitom může uložit např. jaký autentikátor byl pro vytvoření pověření použit. Správce schválí používání pověření zaškrtnutím volby *„Povoleno“*:



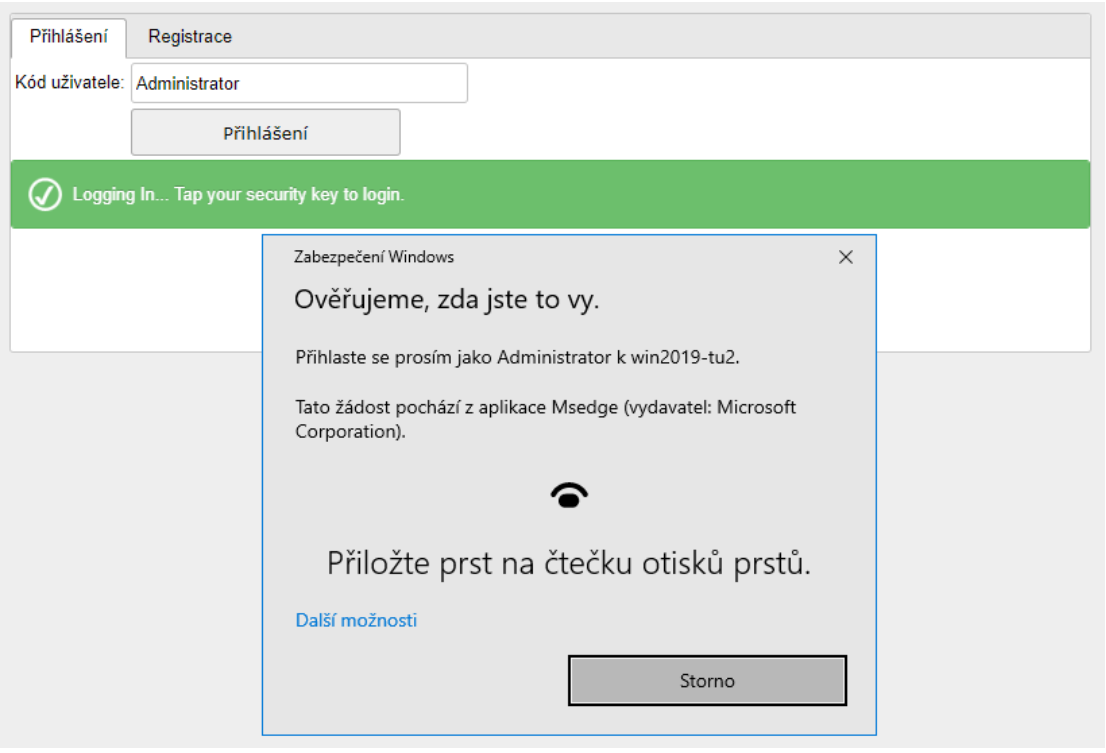
Pokud se uživatel pokusí použít k přihlášení neschválený autentikátor, objeví se chybové hlášení:



3.6 Přihlášení uživatele

Pokud má uživatel v aplikaci zaregistrováno povoleno alespoň jedno pověření, může se do aplikace přihlásit.

Přihlásí se zadáním svého přihlašovacího jména (resp. kódu uživatele) na záložce *„Přihlášení“*. Prohlížeč následně vyzve uživatele k použití autentikátoru, s nímž si uživatel zaregistroval své pověření:



Po úspěšném ověření autentikátorem je uživatel přesměrován zpět do aplikace ESO9.

3.7 Použití stejného autentikátoru ve více aplikacích

Pokud chceme použít stejný autentikátor ve více aplikacích na stejné aplikační doméně (tj. stejné doménové adrese), je třeba zajistit kopii pověření z aplikace, kde registrace vznikla, do všech dalších aplikací, do nichž se chceme přihlašovat stejným způsobem. Pokud si např. v ekonomické aplikaci zaregistrujeme otisk prstu z notebooku a následně si jej zaregistrujeme i ze mzdové aplikace běžící na stejné aplikační doméně, přihlášení bude funkční pouze ve mzdové aplikaci. Je to dáno tím, že operační systém si ukládá zaregistrovaná pověření (de facto digitální certifikáty) k aplikační doméně a nikoli k aplikaci (webu). Nová registrace stejného autentikátoru na stejné aplikační doméně pak vygeneruje nový klíč a zneplatní původní.

Pokud tedy stejný uživatel přistupuje do více aplikací (účetní firmy, holdingy), je třeba registrace nových uživatelů provádět jen v jedné z nich a vzniklá pověření pak kopírovat do všech ostatních.

Výjimkou jsou autentikátory, které mají klíč (certifikát) „vestavěný“ napevno v sobě; např. USB token. Takový autentikátor lze zaregistrovat do více aplikací na stejné aplikační doméně a přihlášení s ním bude fungovat ve všech.

3.8 Správa autentikačních klíčů

Pokud dojde např. po instalaci updatů operačního systémů k chybě ověřovacích klíčů zaregistrovaných k přihlašovaní v dané aplikaci, je nejjednodušší daný klíč smazat a nechat jej vygenerovat znovu. Pro jednu URL adresu totiž nelze vygenerovat více přihlašovacích účtů, tj. bez smazání stávajícího klíče si nelze vyžádat nový.

Způsob nalezení a smazání přístupových klíčů se liší dle operačního systému:

- Windows 10 – klíče nejsou dostupné v žádném UI dialogu nastavení, smazat je lze jen z příkazové řádky za použití některé z dostupných systémových utilit, např. https://github.com/passwordless/webauthn-fido2-key-remover.
- Windows 11 – klíče jsou dostupné v menu nastavení – účty – klíče.
- Apple iOS – klíče jsou dostupné v menu nastavení – hesla. Díky synchronizaci úložiště certifikátů v rámci uživatelského Apple účtu dojde při smazání klíče na jedné platformě (např. na mobilním telefonu) k výmazu stejného klíče i z ostatních platforem (desktopu či tabletu).