



Certifikátová autentikace v ESO9

ESO9 intranet a.s.
U Mlýna 2305/22, 141 Praha 4 – Záběhlice
tel.: +420 585 203 370-2
e-mail: info@eso9.cz
www.eso9.cz

Zpracoval: Tomáš Urych
Dne: 27.6.2008

Revize: Stanislav Havlena
Dne: 9.6.2011

Obsah

1.	ÚVOD.....	3
2.	PODMÍNKY PROVOZU.....	3
3.	NASTAVENÍ PŘÍSTUPU	3
3.1	INSTALACE SERVEROVÉHO CERTIFIKÁTU DO IIS.....	3
3.2	NASTAVENÍ PŘÍSTUPU V IIS.....	3
3.3	NASTAVENÍ PŘÍSTUPU V ESO9	4
3.4	NASTAVENÍ KLIENTA ESO9.....	4
4.	MOŽNÉ CHYBY A JEJICH ŘEŠENÍ	4

1. Úvod

Certifikátová autentikace je jednou ze třech možností ověření klienta ESO9 oproti aplikačnímu serveru. Je vhodná zejména tam, kde nelze použít NT autentikaci – tedy při přístupu vzdálených klientů přes Internet.

Výhodou provozu tohoto typu autentikace je jednak šifrovaný přenosový kanál (HTTPS komunikace) a jednak rychlejší přihlášení uživatele k aplikaci (na rozdíl od ESO9 autentikace není třeba zadávat jméno a heslo pro přihlášení se k aplikaci ESO9). Certifikátovou autentikaci lze na jednom IIS (Internetový informační server) kombinovat s dalšími dvěma způsoby autentikace v ESO9.

2. Podmínky provozu

K provozu certifikátové autentikace je zapotřebí mít nainstalovaný serverový certifikát na IIS serveru a klientské certifikáty na jednotlivých stanicích, které budou k takto zabezpečeným aplikacím ESO9 přistupovat.

Pro generování certifikátů je možné použít komerční certifikační autoritu, nebo je možné použít instalaci certifikační autority obsaženou ve Windows 2003/2008 serveru.

3. Nastavení přístupu

3.1 Instalace serverového certifikátu do IIS

- Spustit *Internet Information Services Manager* (Správce Internetové informační služby)
- Zvolit *Web Sites - Default Web Site* (Webové servery – Výchozí webový server)
- Zobrazit *Properties* (Vlastnosti)
- Přejít na záložku *Directory Security – Secure Communications - Server Certificate* (Zabezpečení adresáře – Zabezpečená komunikace – Certifikát server)
- Pokud již máte certifikát, vyberte možnost *Assign a new certificate* (Přiřadit existující certifikát), nebo *Import certificate* (Import certifikátu ze souboru PFX)
- V případě žádosti o nový certifikát, zvolit *Create a new certificate* (Vytvořit nový certifikát), potom *Prepare the request now* (Připravit žádost nyní), vyplnit požadované údaje a uložit do souboru.
- Soubor žádosti o certifikát doručit certifikační autoritě k vystavení certifikátu
- Po vystavení certifikátu pokračovat stejným postupem a volnou *Process the pending request* (Dokončit zpracování žádosti čekající na vyřízení) a nainstalovat certifikát.
- Restartovat službu IIS, případně celý server

3.2 Nastavení přístupu v IIS

Na aplikačních webech, využívajících certifikátovou autentikaci, je třeba provést následující nastavení:

- Zobrazit kartu s vlastnostmi požadovaného webu.
- Zvolit záložku *Directory Security* (zabezpečení adresáře).
- Tlačítkem *Edit* (upravit) zobrazit kartu s nastavením ověřování webu.
- Zaškrtnout pouze položku *Enable anonymous access* (anonymní přístup) a potvrdit dialogové okno.
- Na záložce *Directory Security* (zabezpečení adresáře) v sekci *Secure Communications* (zabezpečená komunikace) stisknout tlačítko *Edit* (upravit).

- V dialogovém okně *Secure Communications* (zabezpečená komunikace) zaškrtnout volbu *Require Secure Channel* a *Require 128-bit Encryption* (komunikační kanál bude šifrován 128 - bitovou šifrou).
- V sekci *Client Certificates* (klientské certifikáty) ve stejném okně zvolit položku *Require Client Certificates* (vyžadovat klientské certifikáty) a potvrdit dialogové okno.

3.3 Nastavení přístupu v ESO9

Nastavení se provádí na aplikačním serveru ve Správci ESO9. Na kartě s nastavením vlastností aplikace zvolit **způsob ověření – certifikáty**.

3.4 Nastavení klienta ESO9

Na klientské stanici je třeba nejprve korektně nainstalovat klientský certifikát:

- Pokud již máte vygenerovaný certifikát, uložený v souboru od certifikační autority, stačí jej pouze nainstalovat a zkontrolovat v *Internet Exploreru – Nástroje – Možnosti Internetu – záložka Obsah – Certifikáty – Osobní* zda je zde příslušný certifikát zobrazen.
- Pokud žádáte o nový certifikát je potřeba připravit žádost a poté provést instalaci certifikátu podle pokynů Certifikační autority.

Ke komunikaci s takto zabezpečenou webovou aplikací je třeba použít HTTPS protokol, tedy např.

<https://mujserver/mojeaplikace>.

Při prvním přístupu uživatele k aplikaci je třeba si zaregistrovat klientský certifikát v aplikaci ESO9 (tj. navázat daný certifikát na daného uživatele z tabulky uživatelů v ESO9). Tato akce předpokládá nastavení hesel pro všechny uživatele pracující s touto autentikací.

Vlastní registraci provede uživatel kliknutím na hyperlink *Registrace certifikátu*. Na následující stránce vyplní uživatel svůj kód uživatele a heslo v ESO9 a stiskne tlačítko *Registrovat*. Po úspěšné registraci je uživatel přesměrován na základní stránku v ESO9.

Při dalších přístupech (s již zaregistrovaným certifikátem) používá klient běžný přihlašovací mechanismus, tedy kliknutí na logo v úvodní stránce ESO9.

4. Možné chyby a jejich řešení

- Uživatel nemá v DB ESO9 žádné heslo (null) – nastavit.
- Uživatel již má v DB ESO9 přiděleno sériové číslo certifikátu – vymazat (např. pomocí Správce ESO9).
- Po instalaci certifikátu se uživateli nedaří registrace certifikátu v ESO9 (nepřenáší se mu jméno a heslo z registračního formuláře) – po instalaci certifikátu uzavřít Internet Explorer (všechny instance), spustit Internet Explorer a do adresního řádku ručně napsat adresu aplikačního serveru a kliknout na hyperlink *Registrace certifikátu*.
- Uživatel nemá aplikační server (přes HTTPS) v zóně důvěryhodných v Internet Exploreru - nastavit.
- Uživatel nemá svůj osobní certifikát v úložišti osobních certifikátů, tj. nemá se jak ověřit oproti IIS serveru – restartovat pracovní stanici, znovu nainstalovat certifikát.
- Nefunguje vyžádání si certifikátu přes web rozhraní – je třeba použít Internet Explorer (používá se ActiveX prvek)
- Uživatel zadává **http://** místo **https://** v adrese serveru