www.rexcontrols.cz/rex

RexSecurityConfig pro zabezpečení systému REX
Uživatelská příručka

REX Controls s.r.o.

Verze 2.50.2
Plzeň
26.1.2017

Obsah

Kapitola 1

Úvod

V některých případech je dobré zabezpečit svá data proti útoku zvenčí. Zabezpečení lze rozdělit na ochranu komunikace (například pomocí šifrování a podepisování) a na omezení přístupu k některým údajům pomocí autorizace a autentifikace.

Pro zabezpečení dat můžou řídící systém REX a OPC UA server používat šifrovanou SSL komunikaci. Aby však mohly tuto komunikaci používat, potřebují X509 certifikát, nejlépe vytvořený pomocí OpenSSL. OPC UA server může použít i autorizaci a autentifikaci, například na základě přihlašovacích údajů (další možnost je anonymní přihlášení a přihlášení pomocí certifikátu).

Program RexSecurityConfig je aplikace, v níž je jednoduché vytvořit OpenSSL X509 certifikát pro REX a pro OPC UA server pomocí jednoduchého dialogu. Navíc umožňuje upravovat přihlašovací údaje pro OPC UA server, kde je možné přidávat, mazat a upravovat jednotlivé uživatele.

Kapitola 2

Použití

Na úvodní obrazovce aplikace je přehled informací o souborech, které jsou důležité pro zabezpečení. Je zde zobrazena cesta k certifikátu a klíči pro REX Core, k certifikátu a klíči pro OPC UA server, k souboru s přihlašovacími údaji pro OPC UA server a ke složkám pro klientské certifikáty OPC UA serveru (viz obrázek 2.1).

Cesta pro certifikát a klíč pro REX Core je získána automaticky z cesty ke konfiguraci REX Core. Pokud tyto soubory neexistují, zobrazí se text polí červeně. Dialog tyto soubory poté umožní vygenerovat (viz obrázek 2.2).

Veškeré informace o souborech pro OPC UA server jsou získány z konfiguračního INI souboru. Pro běh serveru je nutné mít nastavenu cestu k certifikátu a klíči (APPLICATION_CERTIFICATE_PATH, APPLICATION_PRIVATE_KEY_PATH) a URI serveru (APPLICATION_URI). Nepovinný je soubor s přihlašovacími údaji (CREDENTIALS_INI_PATH), kódování hesel v souboru s přihlašovacími údaji (OPTIONAL_ENCODING_SALT) a složky pro klientské certifikáty (CERTIFICATE_TRUST_LIST_PATH, CERTIFICATE_REJECTED_LIST_PATH, CERTIFICATE_REVOCATION_LIST_PATH, CERTIFICATE_ISSUER_LIST_PATH). Pokud tyto soubory či složky neexistují, dialog je umožní vygenerovat a označí text políček červeně (viz obrázek 2.2).

Pokud neexistuje nebo není nastaven konfigurační INI soubor OPC UA serveru, není možné vygenerovat soubory pro OPC UA server (viz obrázek 2.3). Pokud ovšem konfigurační soubor existuje, ale neobsahuje například cestu k certifikátu nebo klíči, zobrazí se záložka se seznamem chyb (viz obrázek 2.4). Chyba se zobrazí i v případě, že je v konfiguraci nastaveno heslo pro soukromý klíč (APPLICATION_PRIVATE_KEY_PASSWORD), které ovšem k danému klíči nepatří. Nicméně tato aplikace nekontroluje celé nastavení konfiguračního souboru. Je například dobré zkontrolovat shodu URI certifikátu s parametrem APPLICATION_URI.

Aplikace po spuštění zjistí aktivní instanci REXu a použije její parametry. Instanci lze změnit v Nastavení. Výběr probíhá pomocí seznamu verzí. Při změně verze se v dalších dvou polích zobrazí cesta ke konfiguračnímu INI souboru OPC UA serveru a cesta k REXu (viz obrázek 2.5). Pokud konfigurační soubor neexistuje, zobrazí se tento text červeně.

2.1 Generování certifikátu

Pro generování certifikátu je třeba kliknout na tlačítko 'Generovat'. Otevře se dialog, který je třeba vyplnit. Povinná pole jsou označena černým popiskem, nepovinná jsou šedá. Certifikát může mít koncovku .cert, .cer, .crt, .der pro formát DER a .pem pro formát PEM. Soukromý klíč bude vždy ve formátu PEM a může mít koncovku .key nebo .pem.

Certifikát pro REX Core lze vygenerovat jednoduše, stačí mít vyplněná všechna povinná pole a mít nastavenu správnou cestu k certifikátu (viz obrázek 2.6).

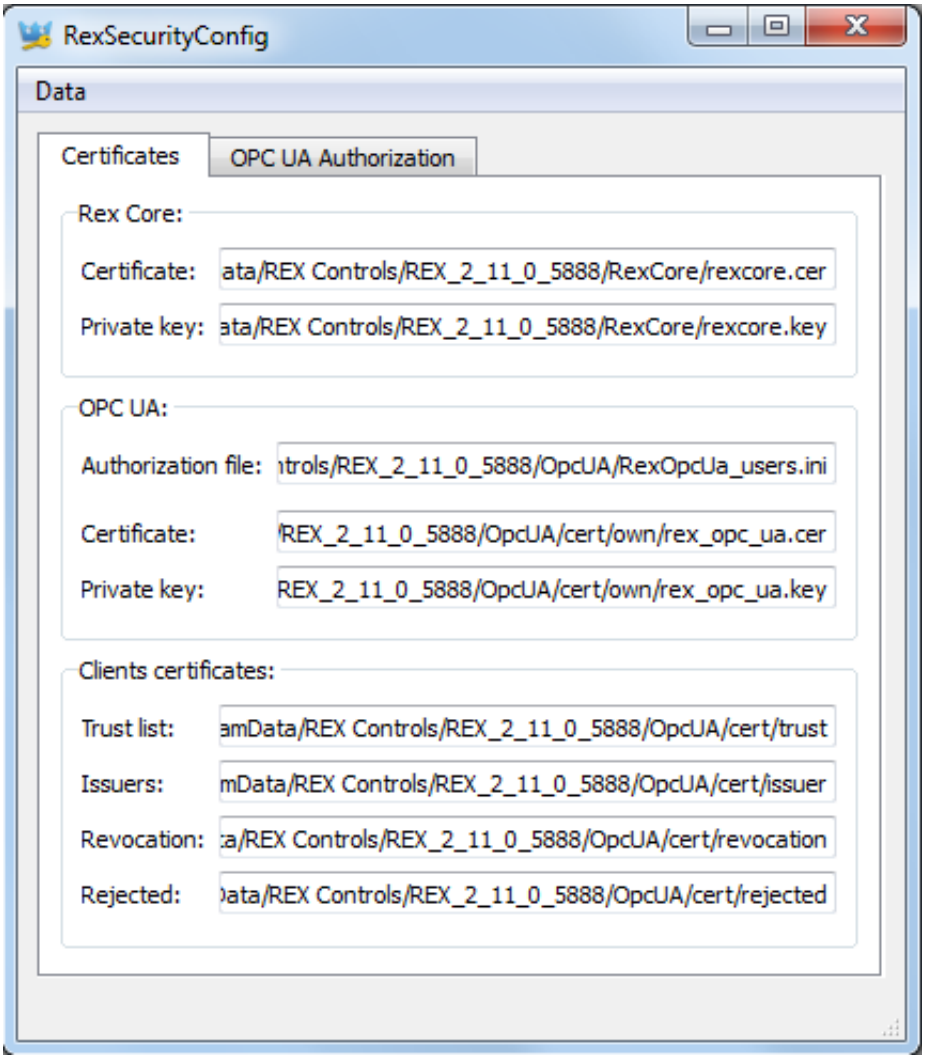
U certifikátu pro OPC UA server je třeba mít správně nastavené Application URI a heslo k soukromému klíči (viz obrázek 2.7). Tyto hodnoty musí být shodné s hodnotami APPLICATION_URI a APPLICATION_PRIVATE_KEY_PASSWORD v konfiguračním INI souboru OPC UA serveru, přičemž APPLICATION_PRIVATE_KEY_PASSWORD je nepovinné. Při otevření dialogu se jako heslo předvyplní právě tato hodnota z konfiguračního souboru.

2.2 Správa uživatelů

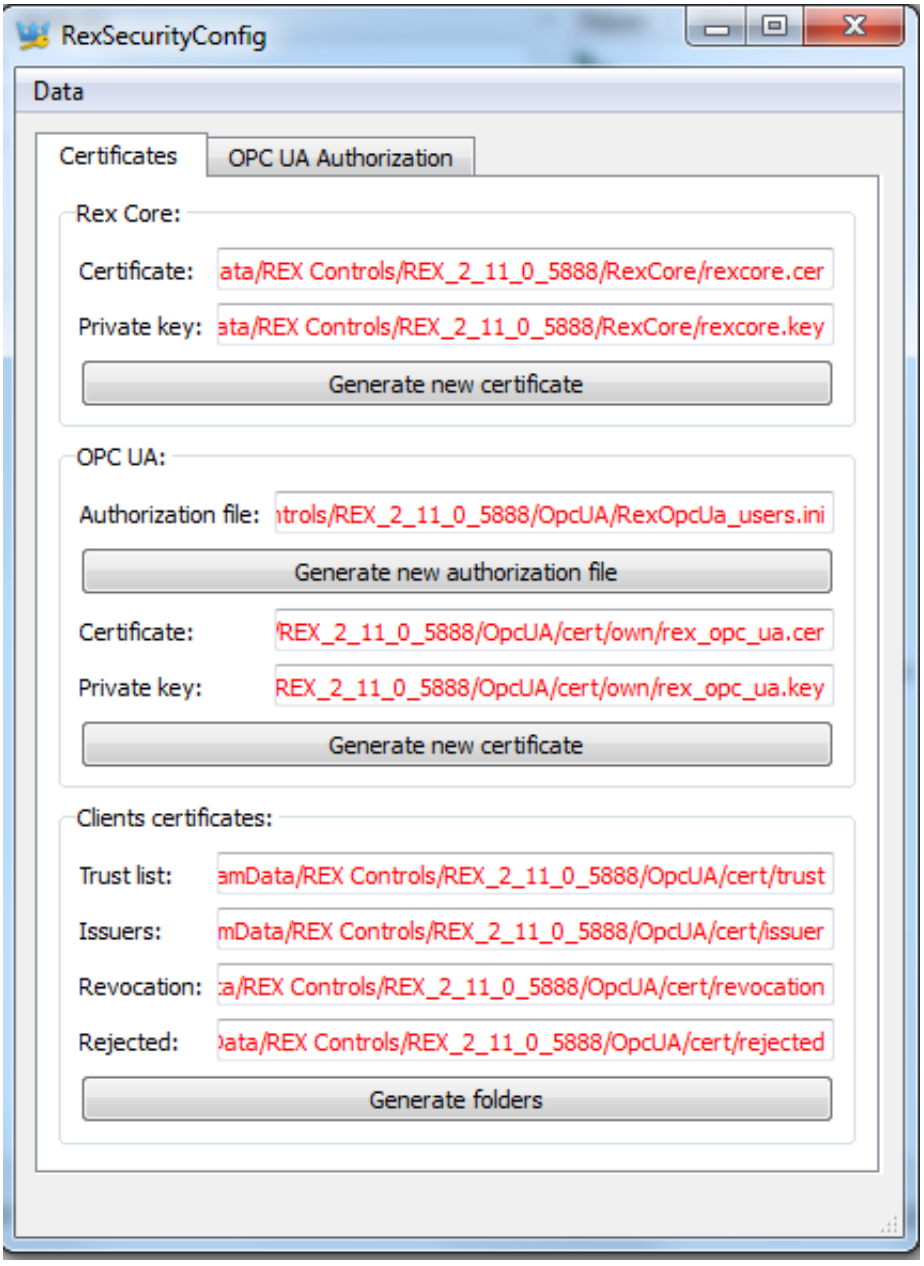
Pokud je vytvořen soubor s přihlašovacími údaji, lze ho na záložce 'OPC UA Authorization' upravovat. Na záložce je tabulka se seznamem uživatelů s jejich rolemi. Lze zde vytvořit nového uživatele a po označení řádku lze uživatele upravit nebo smazat (viz obrázek 2.8).

Novému uživateli je třeba zadat unikátní uživatelské jméno, heslo a patřičnou roli (viz obrázek 2.9). Pokud uživatele nelze vytvořit, dialog na to upozorní.

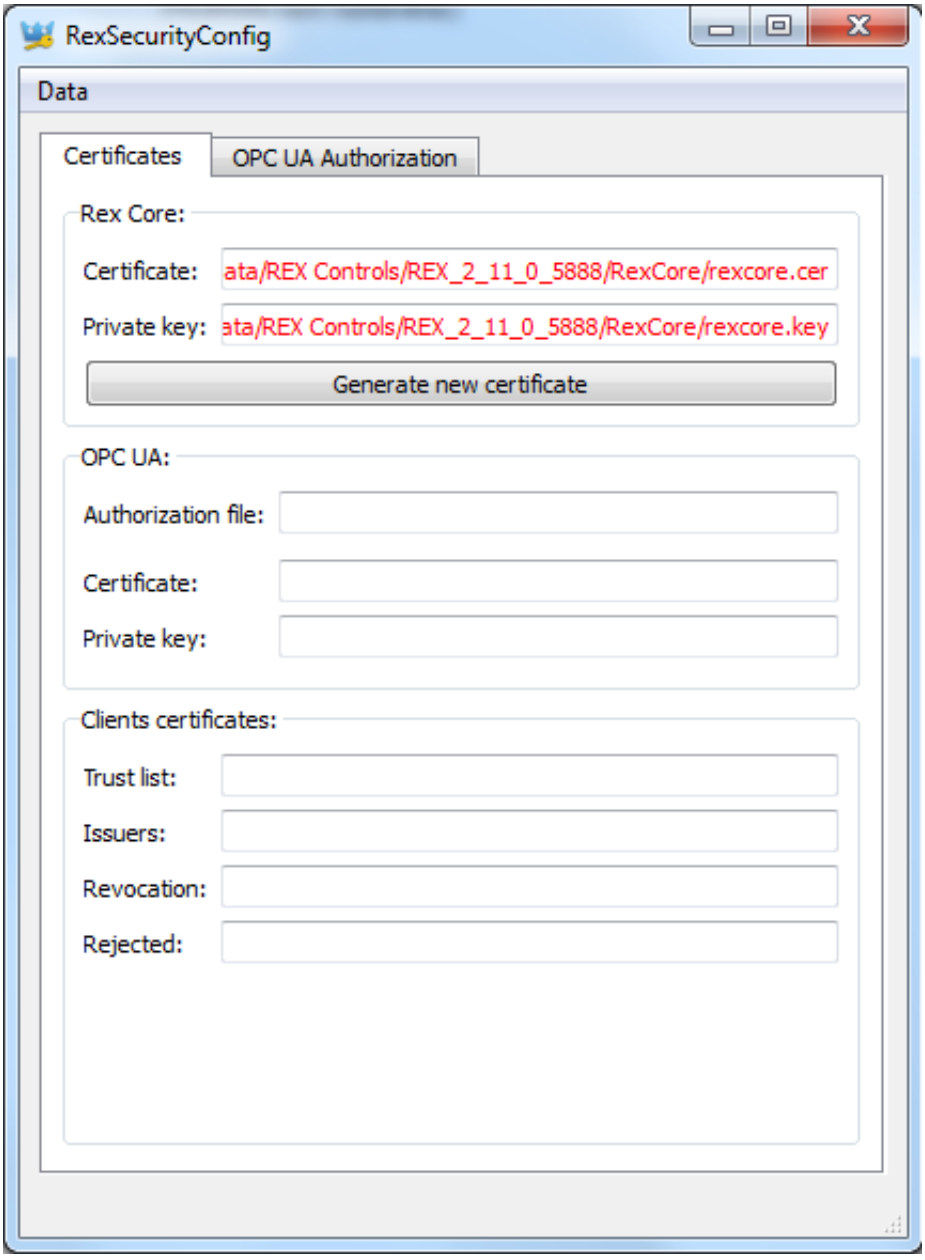
Při úpravě uživatele se dialog předvyplní (kromě pole pro heslo). Všechny změny, které budou ve formuláři provedeny a potvrzeny se poté uloží. Všechna pole, které se při potvrzení změní, jsou označeny tučným popiskem (viz obrázek 2.10).



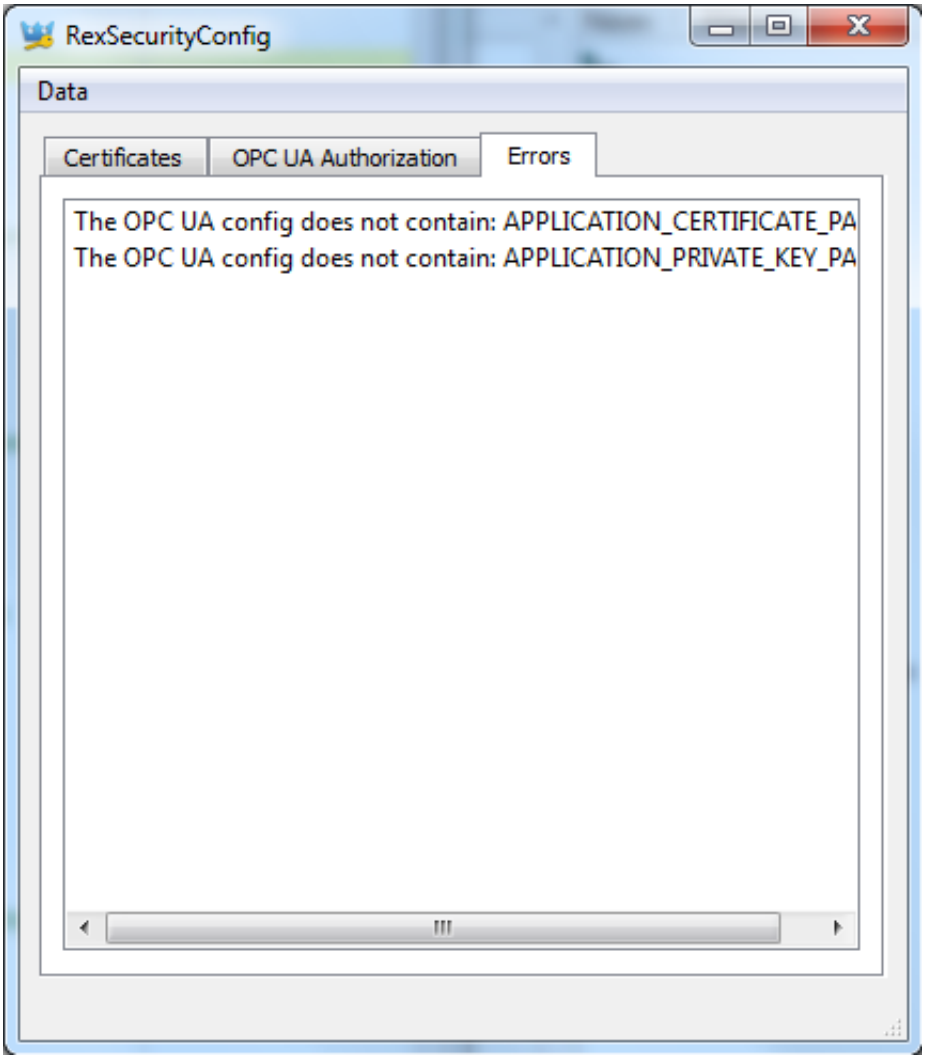
Obrázek 2.1: Program RexSecurityConfig



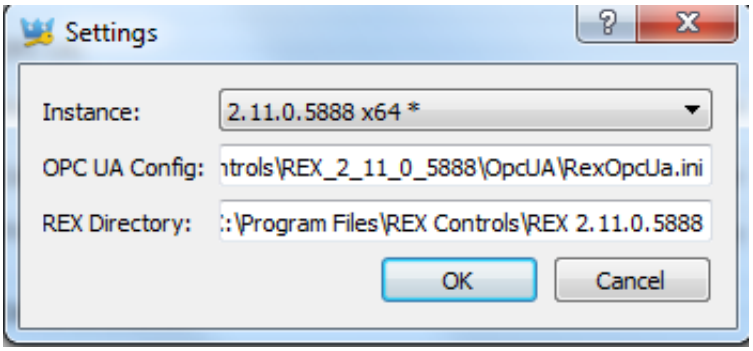
Obrázek 2.2: Chybějící soubory



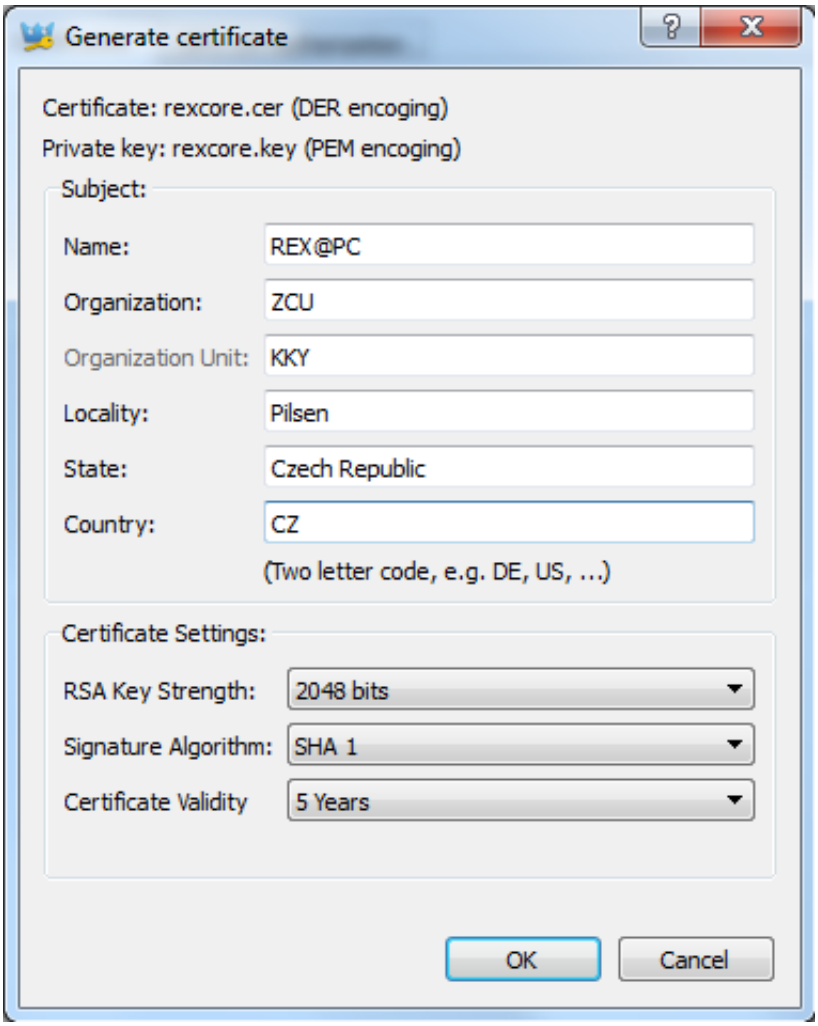
Obrázek 2.3: Instance bez konfiguračního souboru OPC UA serveru



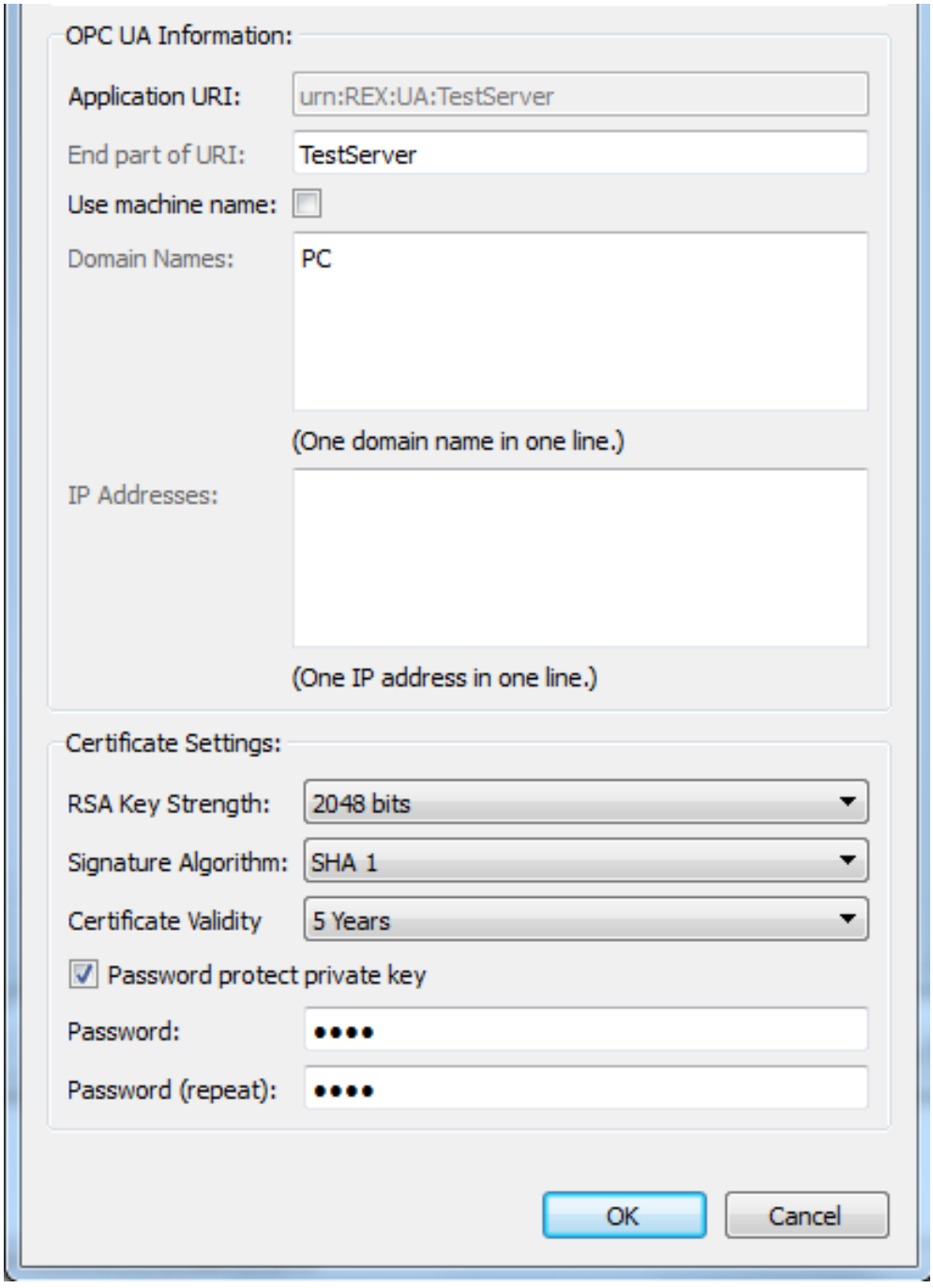
Obrázek 2.4: Chyby v konfiguraci



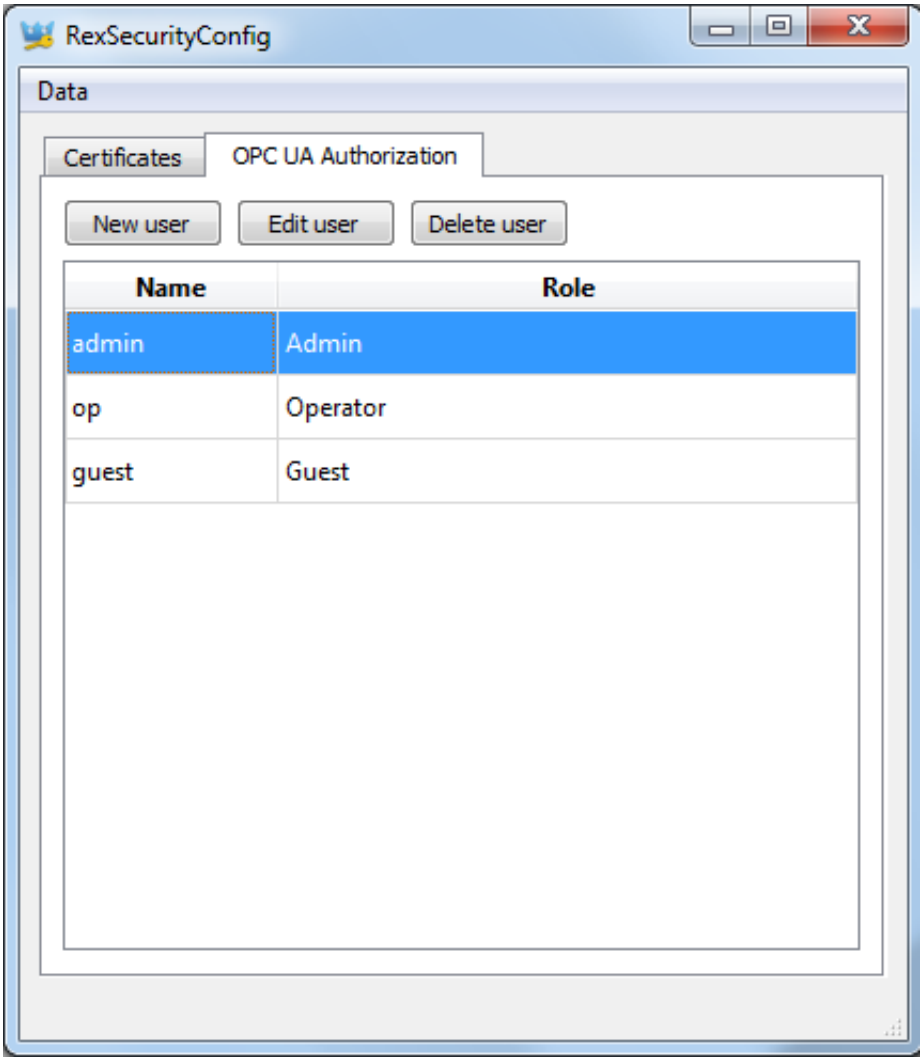
Obrázek 2.5: Výběr instance



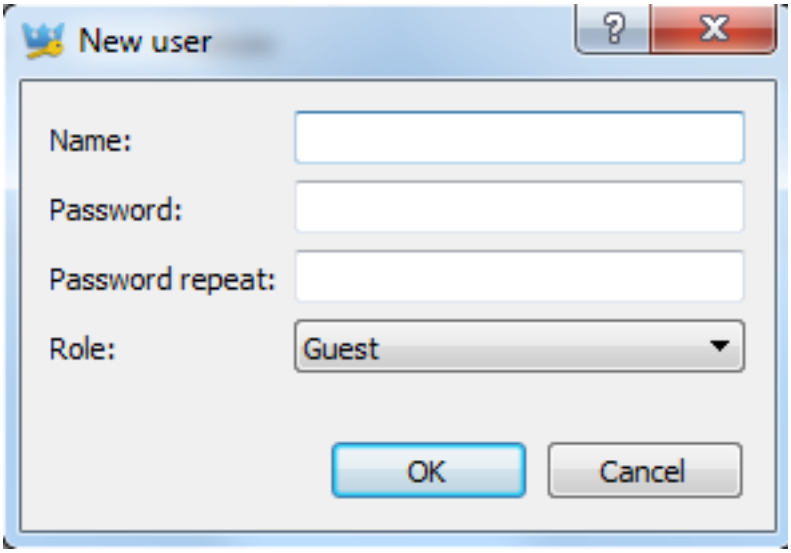
Obrázek 2.6: Generování X509 certifikátu pro REX



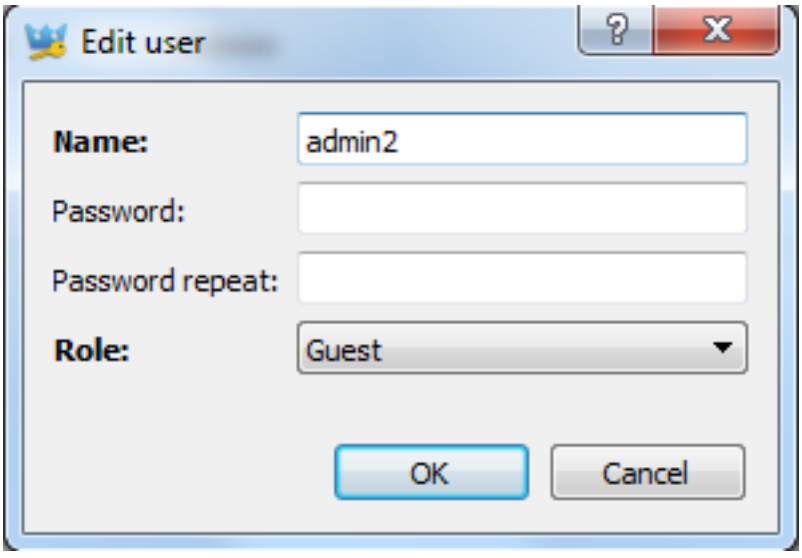
Obrázek 2.7: Generování X509 certifikátu pro OPC UA server



Obrázek 2.8: Seznam uživatelů



Obrázek 2.9: Nový uživatel



Obrázek 2.10: Úprava jména a role uživatele