

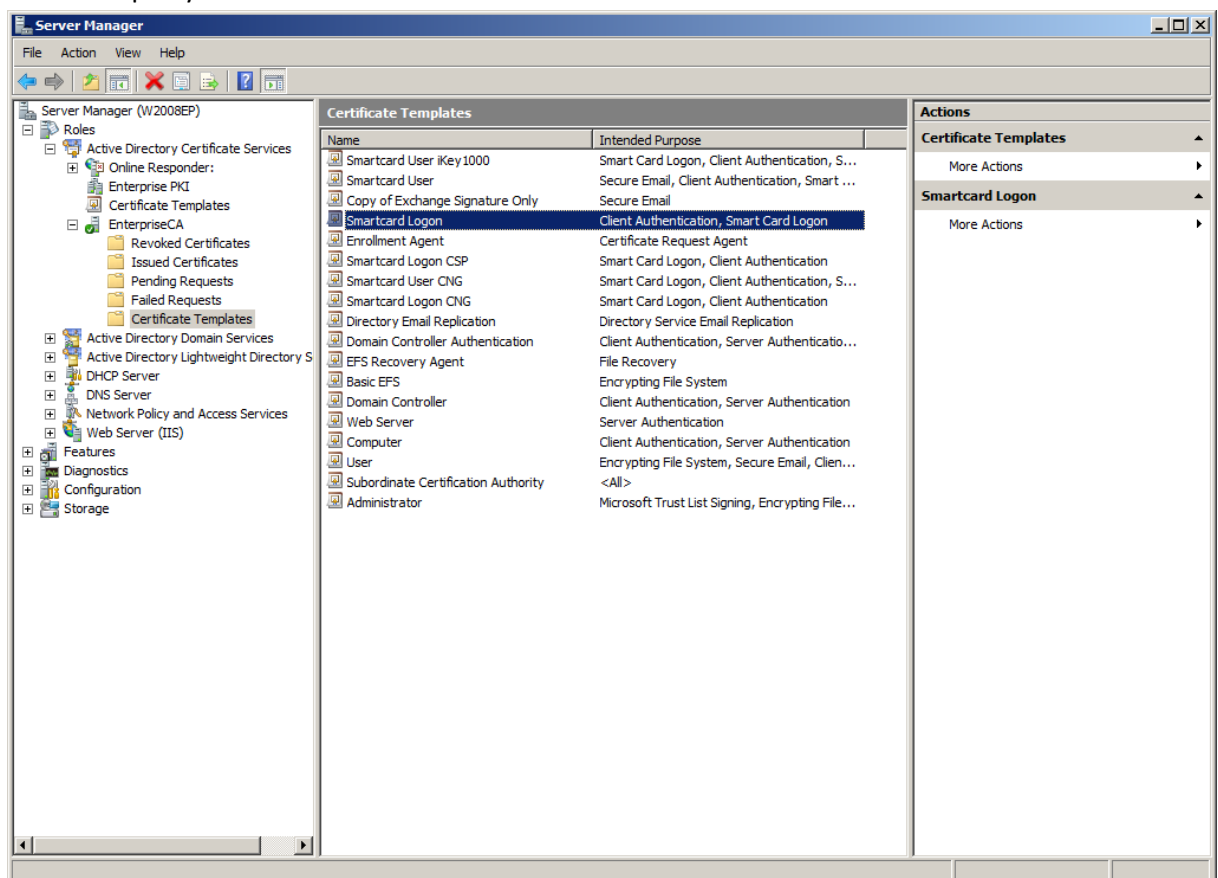
Generování certifikátu pro logon na tokenu

Předpoklady:

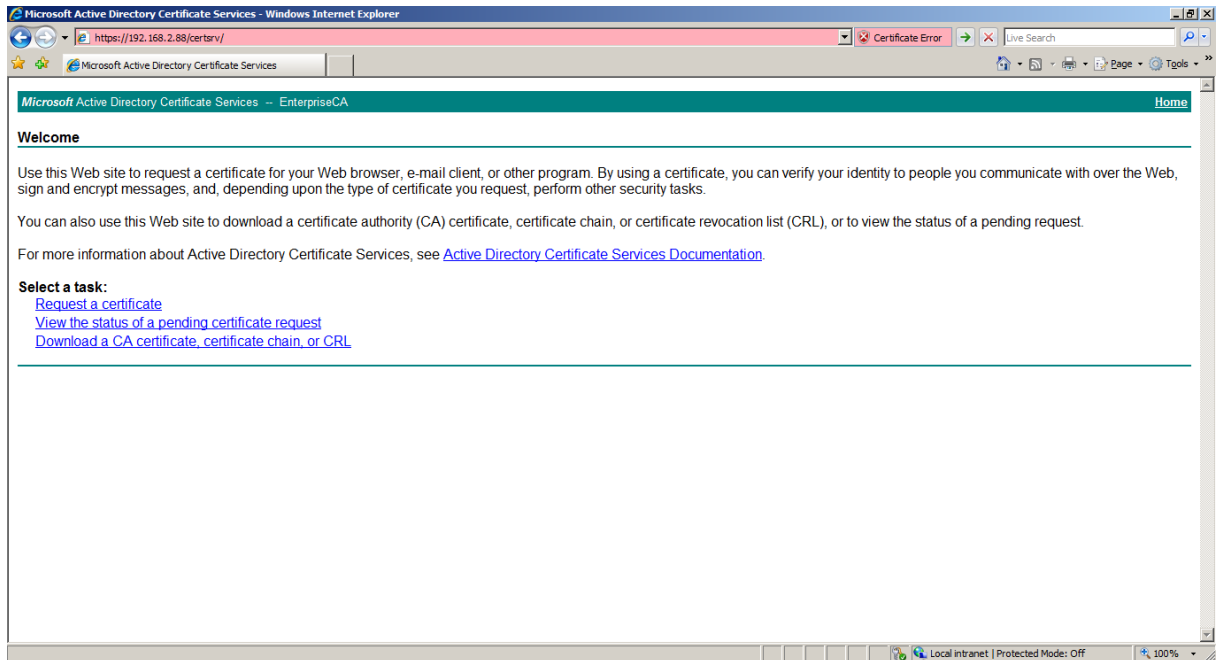
- Microsoft Server 2003/2008 s Active Directory a nainstalovanou certifikační autoritou s Web Enrollmentm (webová stránka zabezpečená SSL)
- klientské PC s Windows OS a nainstalovaným SafeNet Authentication Client 8.0 a vyšším
- token SafeNet s podporou PKI (eToken řady 4000, 4100, 5000, 5100, 5105, 5200, 7000, 7100, 7200)

Postup:

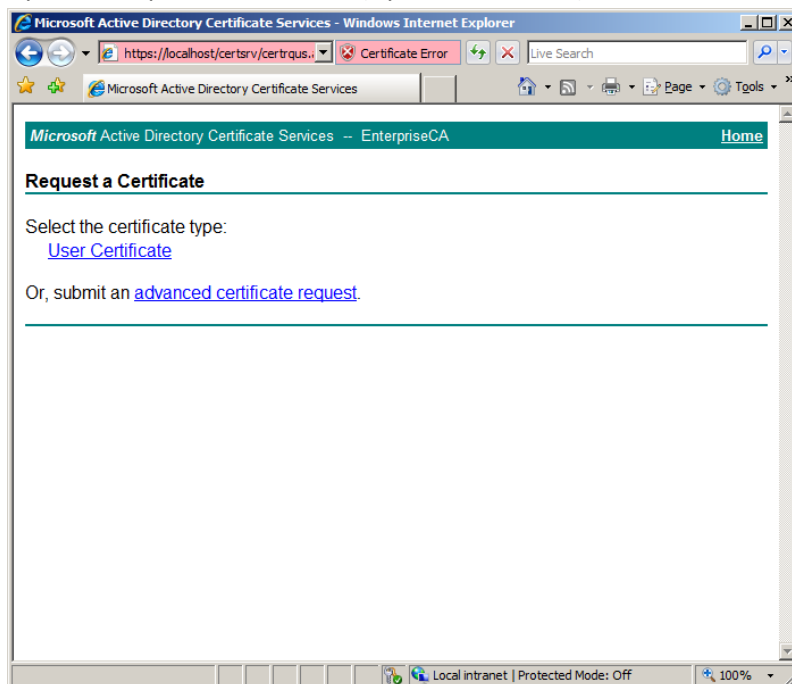
- 1) Zkontrolujte, jestli nainstalovaná MS certifikační autorita obsahuje požadovanou šablonu (v tomto návodu použijeme defaultní Smartcard Logon) a jestli je tato šablona připravená k vydání. Pod Certificate Templates jsou všechny šablony, které bychom (podle oprávnění) měli vidět při vytváření žádosti o certifikát.



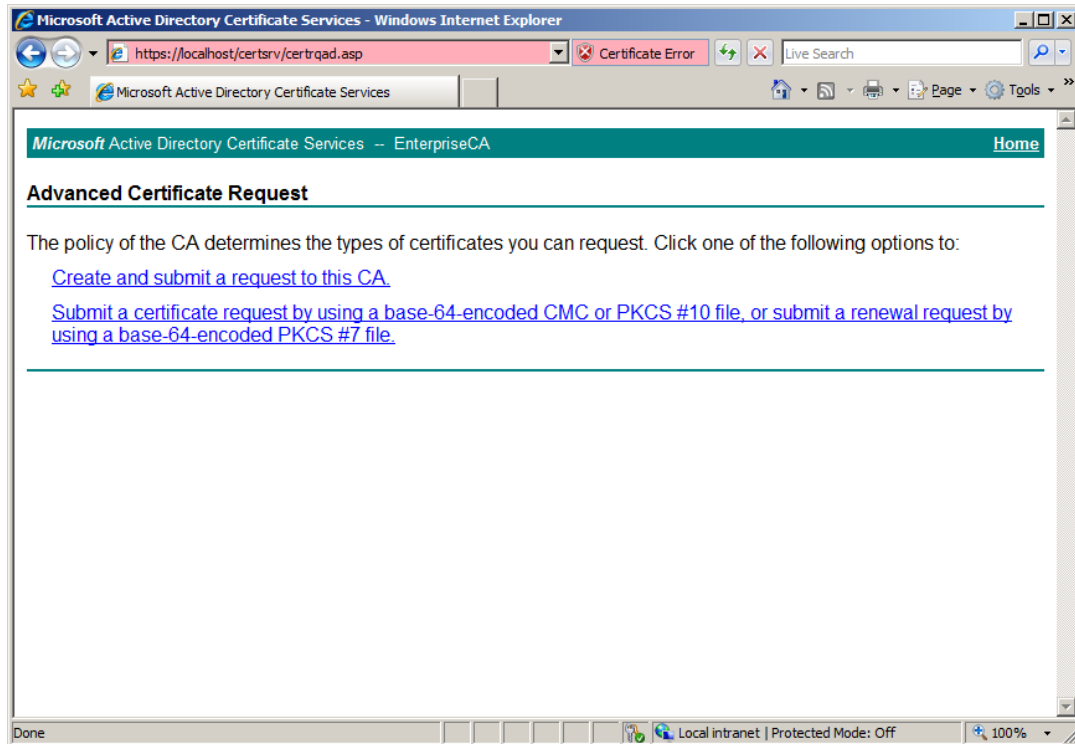
- 2) Na klientovi otevřete webový prohlížeč a zadejte adresu https://<IP_adresa_serveru_CA>/certsrv. Po kliknutí na pokračovat se objeví tato obrazovka:



3) Vyberte Request a certificate (Vyžadat certifikát)



- 4) Vyberte Advanced certificate request (rozšířený požadavek certifikátu)



- 5) Vyberte Create and submit a request to this CA (Vytvořit a odeslat žádost o certifikát této certifikační autoritě).

6) Vyplňte žádost o certifikát (např. podle následující obrazovky) a odešlete na CA (Submit)

The screenshot shows the 'Advanced Certificate Request' page in Internet Explorer. The browser address bar shows 'https://localhost/certsrv/certrqma.asp'. The page title is 'Microsoft Active Directory Certificate Services - EnterpriseCA'. The main content area is titled 'Advanced Certificate Request' and contains several sections:

- Certificate Template:** A dropdown menu is set to 'Smartcard Logon'.
- Key Options:**
 - Radio buttons for 'Create new key set' (selected) and 'Use existing key set'.
 - CSP: A dropdown menu is set to 'eToken Base Cryptographic Provider'.
 - Key Usage: Radio buttons for 'Exchange' (selected) and 'Other purposes'.
 - Key Size: A text box contains '1024'. Below it, 'Min:1024' and 'Max:2048' are shown, along with '(common key sizes: 1024 2048)'. There are also links for '1024' and '2048'.
 - Radio buttons for 'Automatic key container name' (selected) and 'User specified key container name'.
 - Checkboxes for 'Mark keys as exportable' (unchecked) and 'Enable strong private key protection' (unchecked).
- Additional Options:**
 - Request Format: Radio buttons for 'CMC' (selected) and 'PKCS10'.
 - Hash Algorithm: A dropdown menu is set to 'sha1'. Below it, the text 'Only used to sign request.' is displayed.
 - Checkbox for 'Save request' (unchecked).
 - Attributes: A list box with empty entries and scroll arrows.
 - Friendly Name: An empty text input field.

A 'Submit >' button is located at the bottom right of the form area. The status bar at the bottom of the browser shows 'Local intranet | Protected Mode: Off' and a zoom level of '100%'.

Důležitá pole:

Certificate Template – výběr šablon, které má autentizovaný uživatel k dispozici (Smartcard Logon)

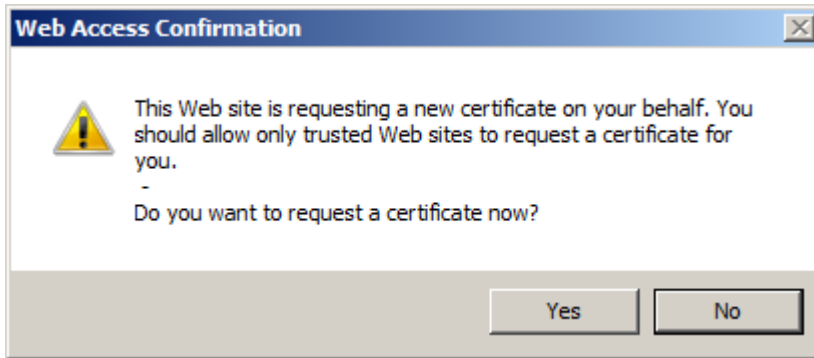
CSP – pro generování RSA klíčů na tokenu/čipové kartě SafeNet **musí být vybrán eToken Base Cryptographic Provider**

Key Size – vyberte velikost RSA klíče, pro token max 2048bit

Enable strong private key protection – ochrana silným privátním klíčem

Hash Algorithm – vyberte algoritmus hash pro podepsání požadavku podporovaný Vaším tokenem

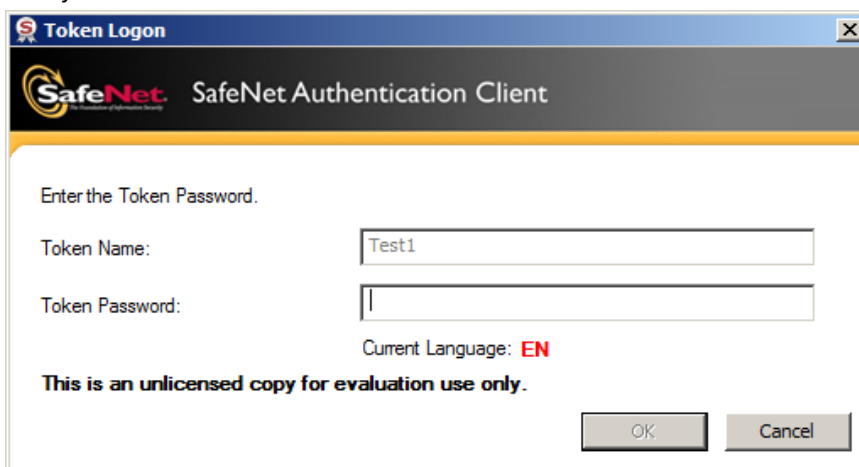
7) Potvrďte další okno stisknutím Yes/Ano.



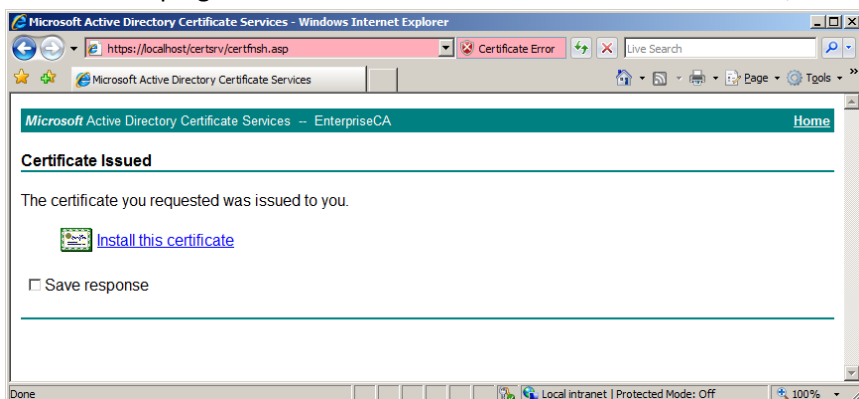
8) Potvrďte název připojeného tokenu/čipové karty



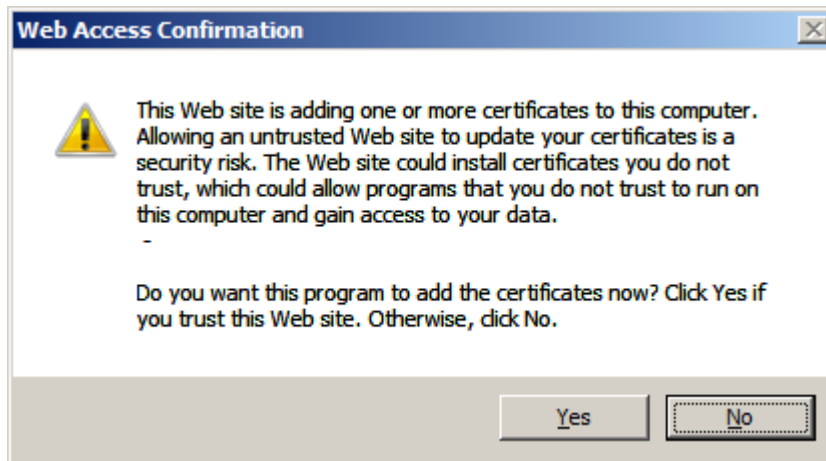
9) Zadejte PIN k tokenu



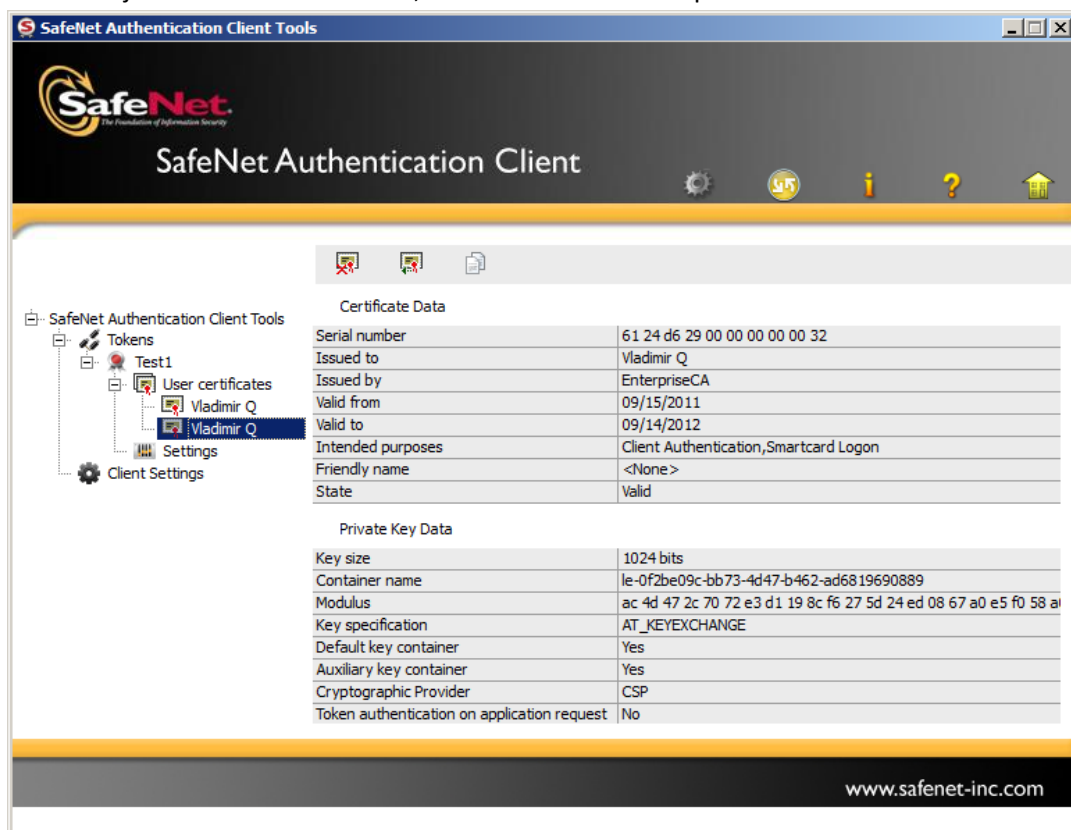
10) Klíče se generují na tokenu. Pokud je na CA nastaveno automatické vydávání certifikátů, bude možné hned po generování klíčů nainstalovat certifikát do tokenu/úložiště Windows.



11) Potvrďte důvěryhodnost webové stránky.



12) Certifikát je nainstalován v tokenu, můžete zkontrolovat spuštěním SAC Tools:



© 2011 ASKON INTERNATIONAL s.r.o., value added distributor společnosti SafeNet, Inc. pro Českou republiku a Slovenskou republiku. Všechna práva vyhrazena.

Tato dokumentace je určena pro zákazníky užívající produkty distribuované společností ASKON INTERNATIONAL s.r.o.

Další šíření této dokumentace nebo jejích částí je možné jen s výslovným písemným souhlasem ASKON INTERNATIONAL s.r.o.

V tomto materiálu uvedené názvy produktů jsou ochranné známky jejich vlastníků.