Lietotāja instrukcija
Konfigurācija ar REST

Izmaiņas domēna autentifikācijas konfigurēšanai
Pašapkalpošanās WEB

Horizon versija 3.450.450.

FMS
2014

SIA FMS
Kronvalda blv. 3/5
Rīgā, LV - 1010

Tālr.: 6711 6211
Fakss.: 6711 6212
E-pasts: fms@fms.lv

Saturs

Ievads

Lai nodrošinātu vidi REST lietojumiem no Pašapkalpošanās WEB, nepieciešams veikt šajā dokumentā aprakstītās darbības.

Nepieciešams:

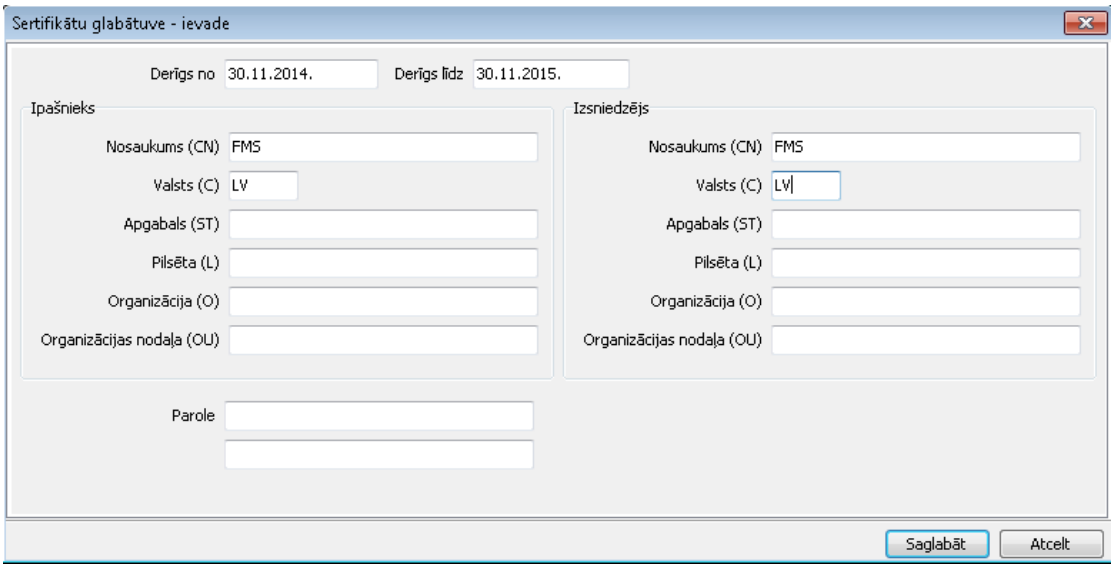
1) uzģenerēt sertifikātu pāri un Horizon sertifikātu glabātuvē (keystore) ieimportēt publisko sertifikātu;
2) datoram, uz kura atrodas IIS, iekonfigurēt privāto atslēgu.

Nākamajās sadaļās pa soļiem aprakstīts risinājums.

Sertifikāta ģenerēšana no Horizon

Izmantojot Horizon sertifikātu glabātuvi (*Sistēma -> Administrēt -> Sertifikātu glabātuve*) jāģenerē pašparakstīts sertifikāts. To veic, nospiežot pogu **Pievienot** un no piedāvātajām darbībām izvēloties darbību **Ģenerēt pašparakstītu sertifikātu**.

Tiks piedāvāts ievadlogs sertifikāta īpašnieka un izsniedzēja norādīšanai, kā arī paroles norādīšanai. Šeit var ievadīt vērtības, kas norādītas uzņēmuma aprakstā Horizon. Ja tiek norādīta parole, tad tā jāatceras, pretējā gadījumā, nezinot paroli, nebūs iespējams sertifikātu izmantot tālāk.



Darbības rezultātā Horizon sertifikātu glabātuvē ir izveidota publiskā atslēga un sertifikātu pāris izveidots.

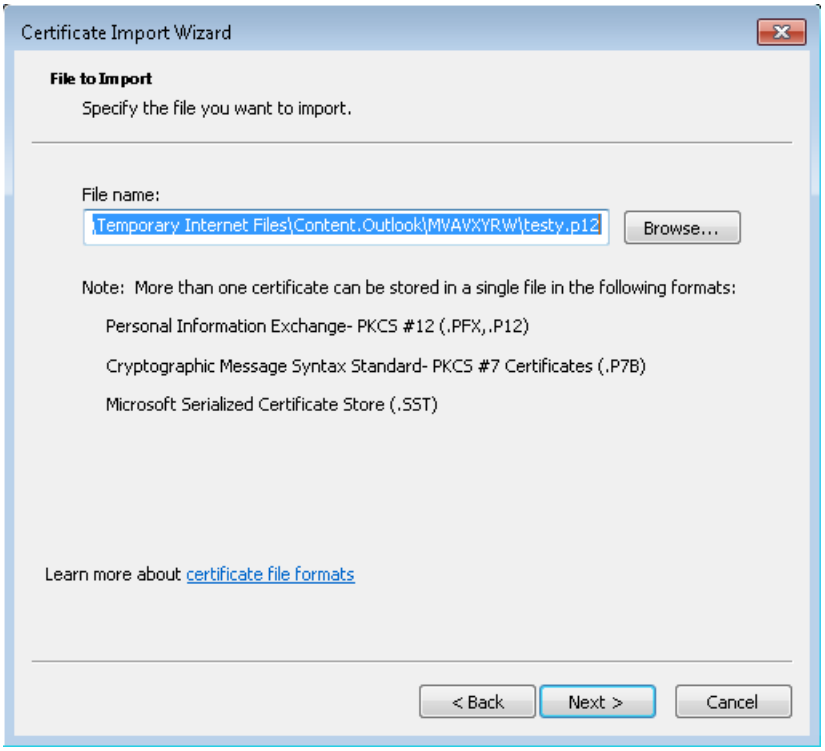
Uzģenerētā sertifikāta eksports

Izveidoto sertifikātu eksportē, izmantojot izvēlnē **Darbības** pieejamo darbību **Eksportēt sertifikāta failu**. Noklusētais eksporta formāts (.p12) ir derīgs importam Windows sertifikātu glabātuvē.

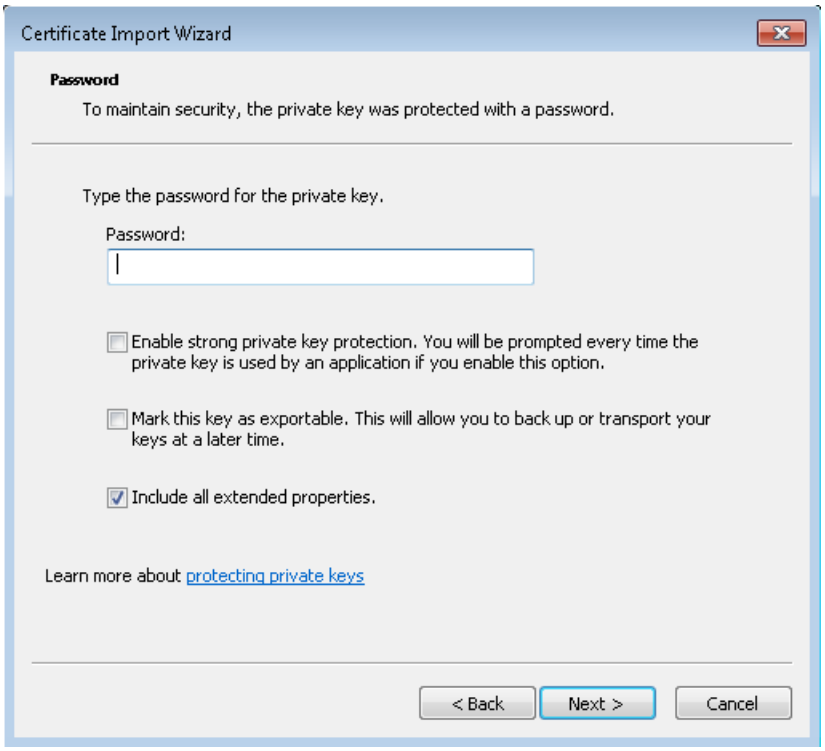
Sertifikāta imports Windows sertifikātu glabātuvē

Tālāk jāizmanto Windows standarta funkcija sertifikāta importam un jāimportē izveidotais sertifikāts Windows sertifikātu glabātuvē uz Web servera. To veic, uzklikšķinot uz eksportētā sertifikāta faila. Windows automātiski atpazīst formātu .p12 un iedarbina importa vedni. Tālāk pa soļiem jāseko importa vednim un jāspiež poga Next, lai pārietu uz nākamo soli.

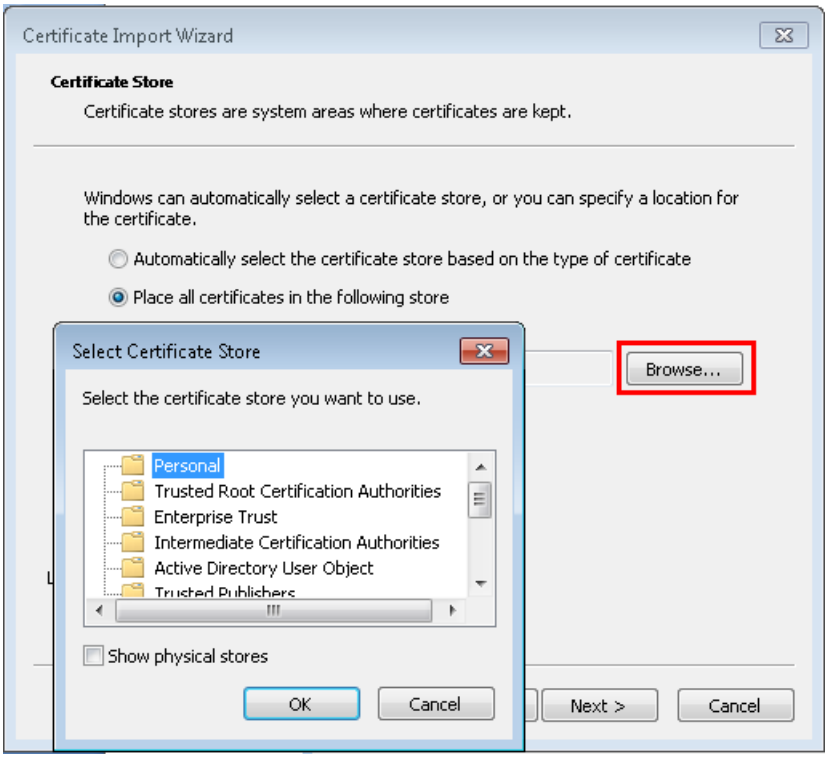
Jānorāda vieta un importējamais fails.



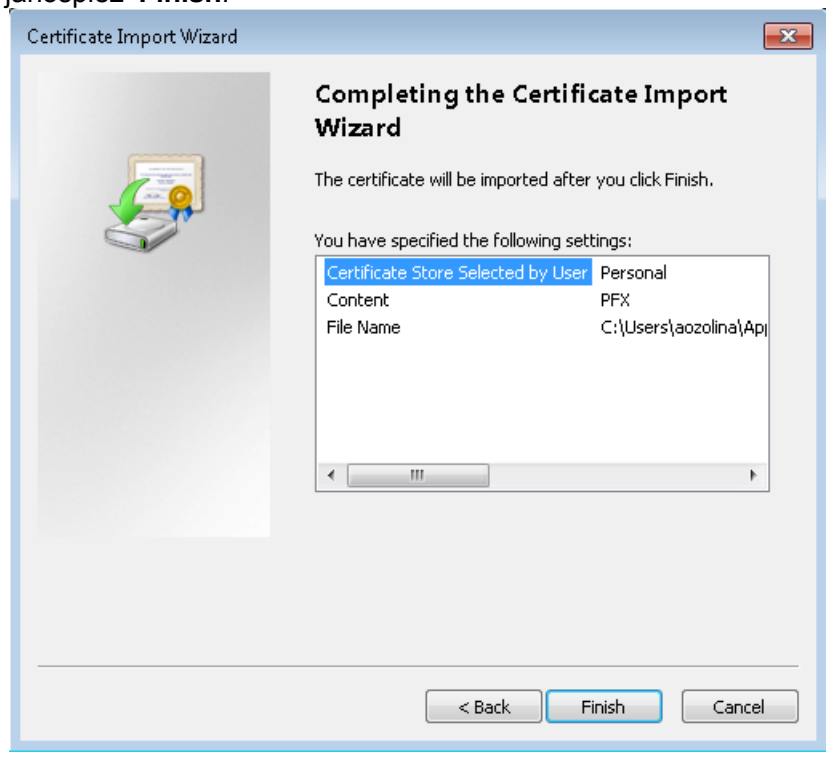
Nākamajā solī jānorāda parole, ar kuru ir aizsargāts sertifikāts. Ja sertifikāts nav aizsargāts ar paroli, tad tā nav jānorāda.



Sertifikāta faila novietošanai izvēlas „Place all sertificates in the following store” un nospiež „Browse”. Piedāvātajā lodziņā, kurā pieejams failu katalogs, norāda mapi, kur novietot sertifikātu. Iespējamās vietas: „Show physical stores”, „Personal”, „Local computer”.



Nākamais solis ir fināla solis, kurā redzami norādītie uzstādījumi. Lai pabeigtu importu, jānospiež **Finish**.



Par veiksmīgu sertifikāta importu liecina paziņojums:

Šī procesa rezultātā ir pabeigts sertifikāta imports.

Pašapkalpošanās WEB konfigurēšana

Pēc tam Pašapkalpošanās WEB konfigurācijas failā web.config jānorāda, kuru sertifikātu jāpaņem no Windows sertifikātu glabātuves, lai lietotājs varētu veikt sekmīgu autorizāciju HorizonWEB, izmantojot domēna autorizācijas iespēju.

To norāda, web.config failā pievienojot vai labojot atribūtu FTGRestCertificateName un norādot kā value vērtību to, kas tika ierakstīta laukā Nosaukums (CN), sertifikātu ģenerējot.

Izmaiņu lapa

Datums	Ver. Nr.	Izmaiņu apraksts	Autors
30.11.2014.	1.0	Izveidots jauns apraksts	A.Ozoliņa