

Упутство за инсталацију дигиталног сертификата

Сертификациони ауторитети

Када се користе Web апликације које од корисника очекују унос лозинки и других поверљивих информација, важно је да та комуникација буде поверљива, као и да је идентитет Web сервера коме се упућују поверљиве информације поуздано утврђен.

Сертификациони ауторитети (Certification Authority, скраћено CA) су организације и ентитети који јамче за идентитет сајтова на Интернету.

Ту функцију обезбеђују дигиталним потписом сертификата сајтова које корисници посећују. Оперативни систем и прегледач веб садржаја иницијално верују само дигиталним потписима велики комерцијалних сертификационих ауторитета, чији су сертификати саставни део инсталације оперативног система.

Потреба за додатном инсталацијом сертификата

Висока школа електротехнике и рачунарства има сопствено сертификационо тело које јамчи за идентитет наших сервера (студентски сервиси, Moodle, бежична мрежа...).

Пошто сертификат нашег локалног сертификационог ауторитета није део инсталације оперативног система корисника, у почетном стању, оперативни систем неће моћи са сигурношћу да утврди идентитет нашег сервера.

Проблем је у томе што оперативни систем сматра да за идентитет сервера јамчи тело које није препознато као валидни CA ауторитет.

Приликом покушаја креирања шифроване TLS сесије, веб прегледач ће одбити везу са сервером и приказати кориснику страницу са грешком.

Како би оперативни систем сматрао је дигитални потпис нашег CA ауторитета валидан, потребно је на сопственој радној станици инсталирати дигитални сертификат нашег сертификационог ауторитета.

Инсталација на Windows оперативном систему

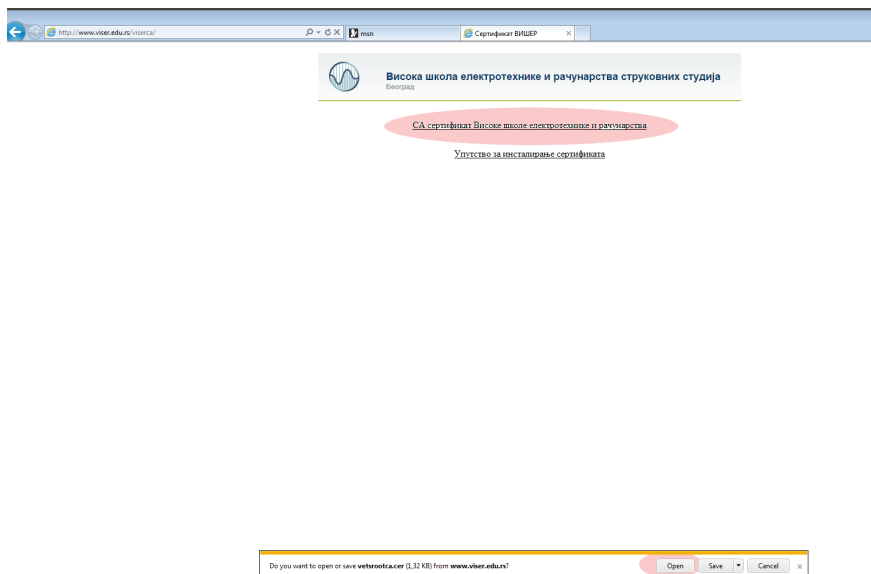
У примеру ће бити објашњена инсталација на Windows оперативном систему.

Сертификат који се увезе на овај начин је валидан и за Internet Explorer, Google Chrome, као и за подешавање бежичне мреже у школи. Ако се користи Mozilla Firefox, потребни су додатни кораци који су објашњени у документу.

Кораци у инсталацији

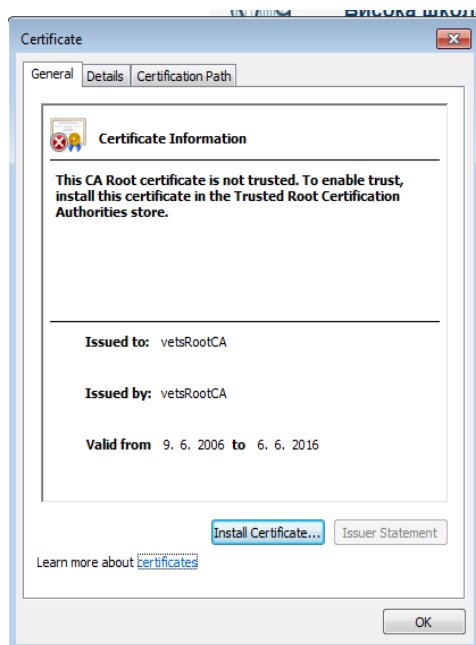
Користећи неки од прегледача веб садржаја (нпр. Internet Explorer) потребно је посетити страницу <http://www.viser.edu.rs/viserca>.

1. На страници је потребно изабрати прву везу („СА сертификат Високе школе електротехнике и рачунарства“), а затим отворити (опција „**Open**“) преузети фајл „vetsrootca.crt“.



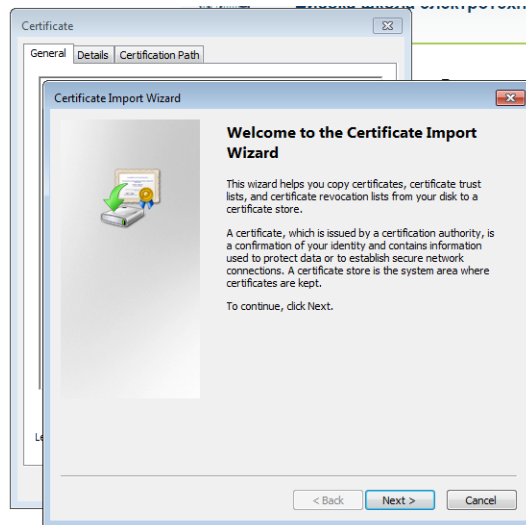
Илустрација 1: Страница за преузимање сертификата

2. Након отварања фајла приказаће се „**Certificate**“ дијалог прозор као на слици, са опцијом „**Install Certificate**“ коју треба изабрати



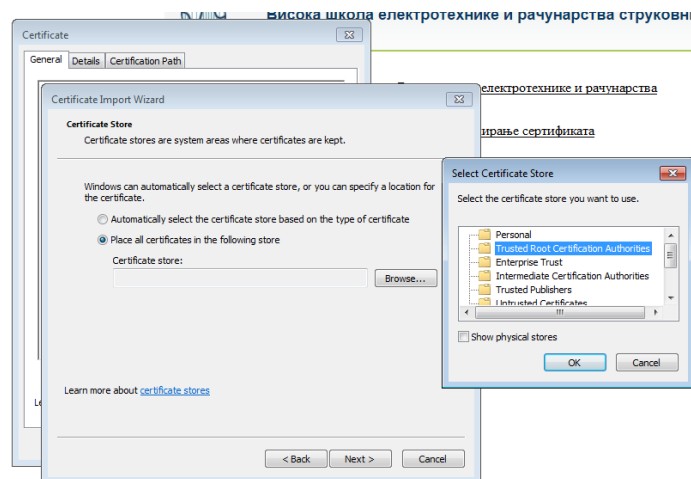
Илустрација 2: Отварање дијалог прозора са сертификатом

3. Након избора опције „**Install Certificate**“, покренуће се чаробњак за инсталацију сертификата. Потребно је изабрати опцију „**Next**“



Илустрација 3: Чаробњак за инсталацију

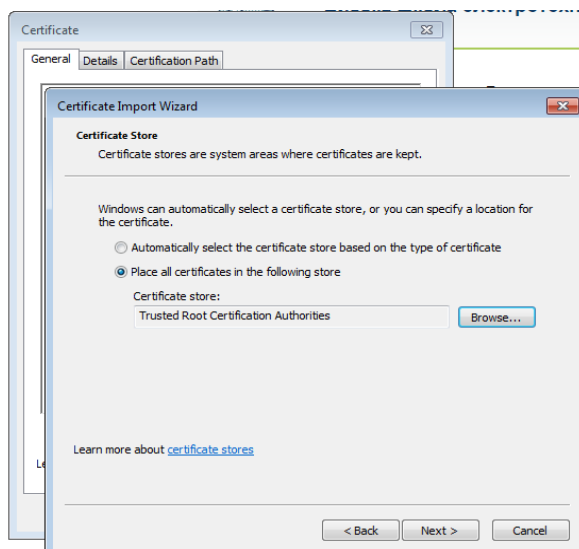
4. У следећем кораку потребно је изабрати складиште сертификата. Подразумевано је изабрана опција „Automatically select...“, што не треба користити, већ је потребно изабрати опцију „**Place all certificates in the following store**“, а затим изабрати тастер „**Browse**“ како би изабрали складиште.



Илустрација 4: Избор исправној складишту

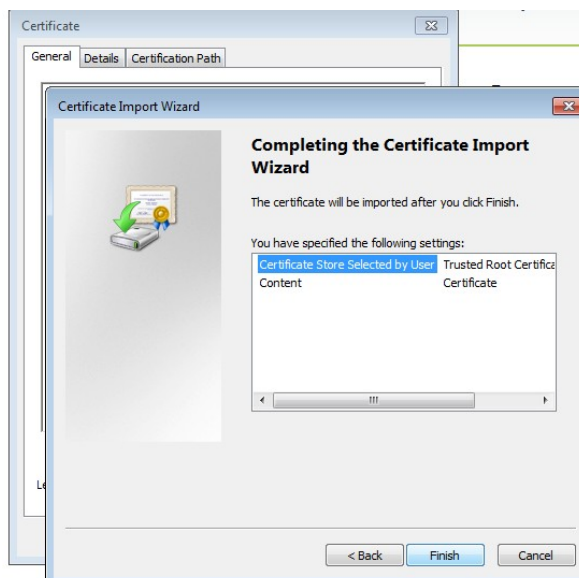
Овај сертификат је потребно инсталирати међу корене сертификационе ауторитете од поверења, па бирамо „**Trusted Root Certification Authorities**“, а зати избор потвдимо са „**OK**“.

5. Ако је изабрано исправно складиште као на слици, потребно је изабрати „**Next**“



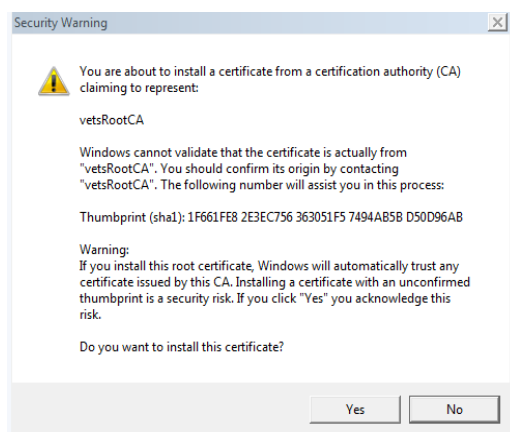
Илустрација 5: Складиште СА од поверења

6. Након што је чаробњак прикупио све потребне информације, приказаће се прозор као на слици. Потребно је изабрати „**Finish**“



Илустрација 6: Завршетак рада чаробњака

7. Након увоза, потребно је још једном додатно потвдити увоз сертификата



Илустрација 7: Потврђивање увоза сертификата

Потребно је изабрати опцију „Yes“

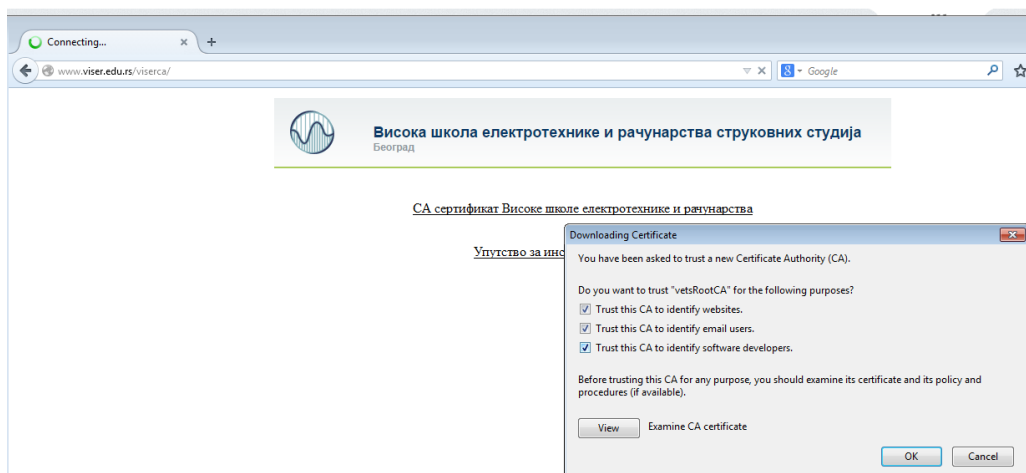
Након ових корака могуће је без упозоравајућих порука користи услуге школе који захтевају потвду идентитета сервера, користећи Google Chrome или Internet Explorer.

Инсталација за Mozilla Firefox прегледач

Firefox користи сопствено интерно складиште сертификата па је потребно увести СА сертификат Високе школе у нега.

Кораци у инсталацији за Mozilla Firefox

Користећи Mozilla Firefox, потребно је посетити страницу <http://www.viser.edu.rs/viserca>, а затим изабрати везу „СА сертификат Високе школе електротехнике и рачунарства“. Након тога, прегледач ће отворити дијалог прозор „**Downloading Certificate**“, као на слици:



Илустрација 8: Преузимање сертификата за Mozilla Firefox

У оквиру дијалог прозора, потребно је изабрати све три опције: „**Trust this CA to...**“ а затим изабрати „**ОК**“.

Након овог корака могуће је без упозоравајућих порука користи услуге школе који захтевају потвду идентитета сервера, користећи Mozilla Firefox.