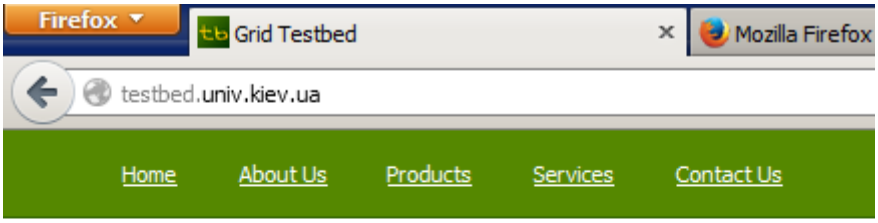
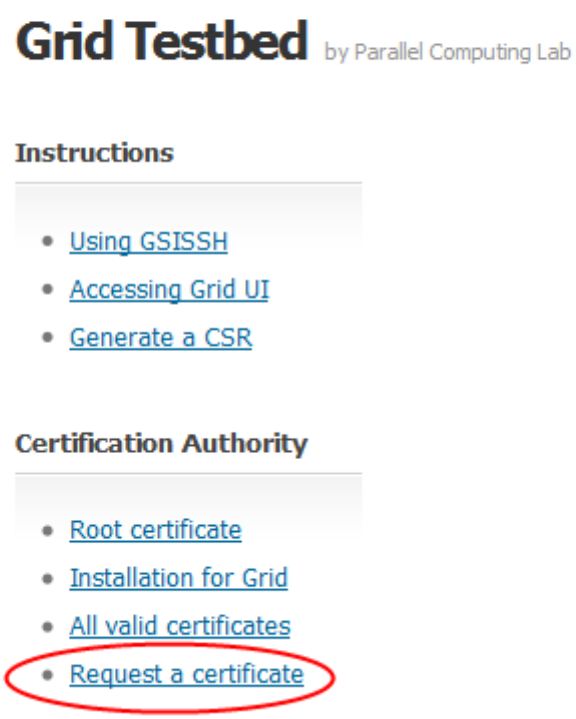
Лабораторна робота №1

Реєстрація та отримання доступу на обчислювальний кластер університету

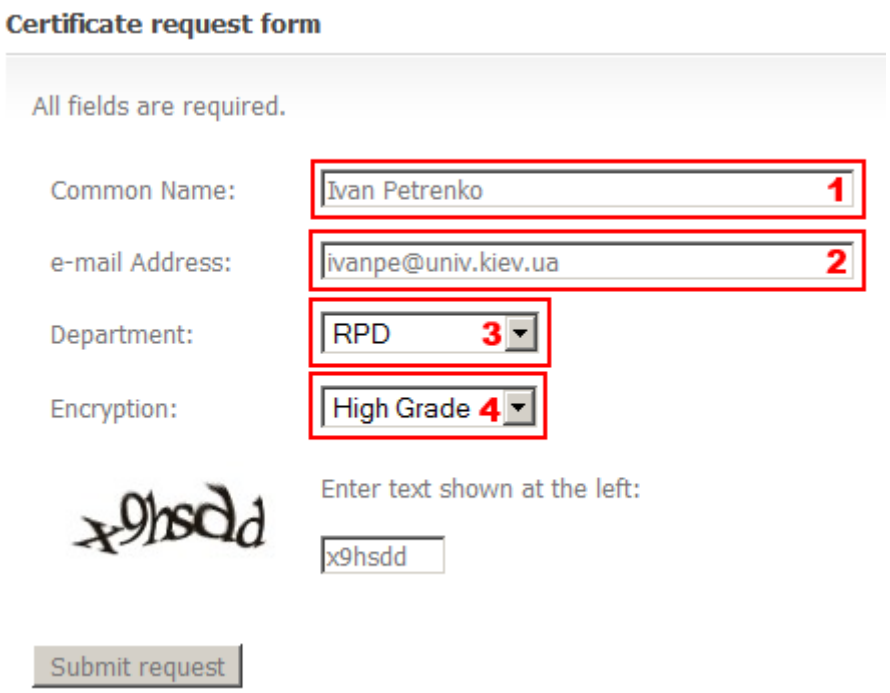
Отримання персонального сертифікату користувача

Завантажте портативну версію веб-браузера Firefox та встановіть її на змінний носій. Ця інсталяція буде необхідна для отримання персонального електронного сертифікату користувача. Спрямуйте ваш веб-браузер на сайт навчального центру сертифікації користувачів – http://testbed.univ.kiev.ua





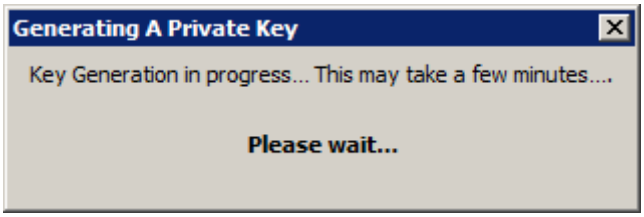
Оберіть функцію формування запиту для створення персонального сертифікату. Відкриється форма запиту.



Необхідно заповнити усі поля форми:

1) ім’я та прізвище у латинській транскрипції;
2) дійсна адреса електронної поштової скриньки;
3) підрозділ, для радіофізичного факультету необхідно обрати “RPD”;
4) потужність шифрування – оберіть “High Grade”, що відповідає 2048-бітному ключу RSA.

Після натискання на кнопку підтвердження, веб-браузер здійснить генерацію пари ключів RSA, що може зайняти від декількох секунд до хвилини. Під час генерації на екрані з’явиться відповідне повідомлення.



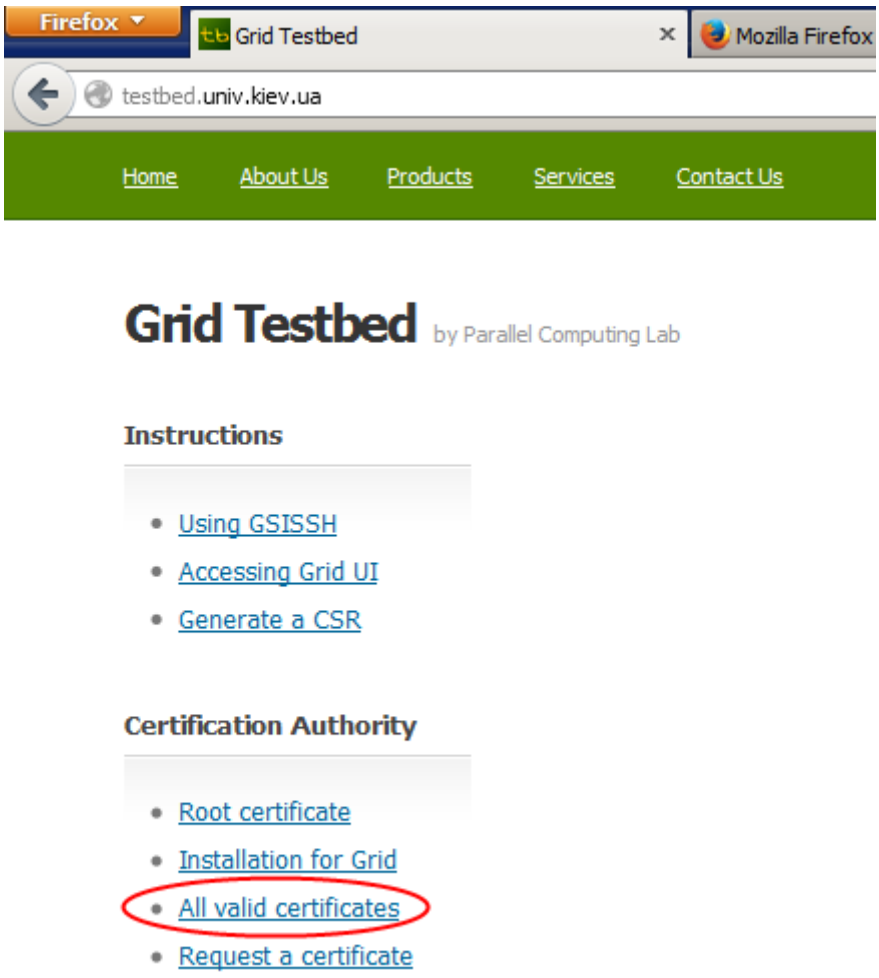
Довгий час генерації пов’язаний із необхідністю отримання великої кількості випадкових чисел, що генеруються із властивостей реальних подій, які реєструються операційною системою, наприклад, переміщення мишки, отримання пакетів із мережі, тощо.

Закритий ключ із згенерованої пари зберігається у профілі налаштувань веб-бреузера та ніколи не передається на віддалені сервери. Відкритий ключ разом із атрибутами, введеними у формі, відправляється на сервер центру сертифікації. Сервер підтверджує отримання запиту повідомленням “Request captured”.

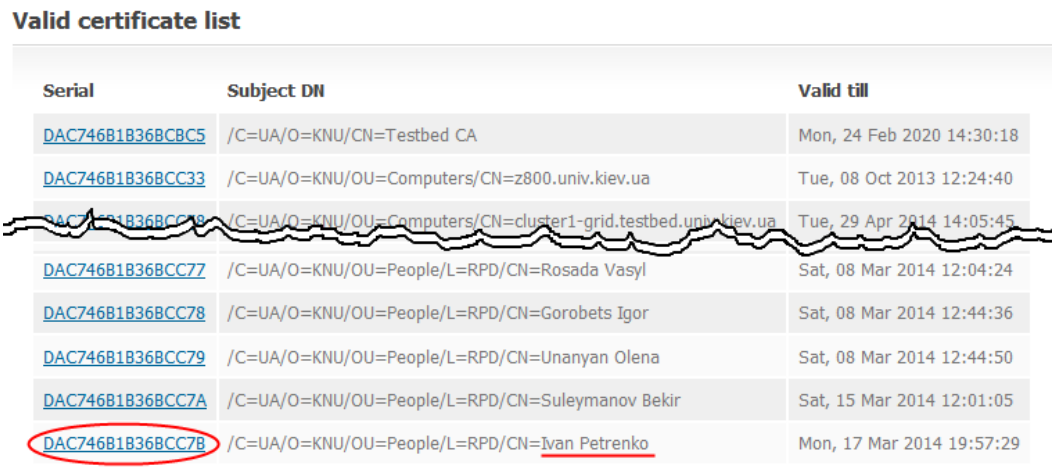
Повідомте викладача про завершення процедури формування запиту.

Якщо ваш запит був сформований задовільно, його буде підписано із використанням закритого ключа центру сертифікації. Ваш відкритий ключ разом із атрибутами, вказаним терміном дії та підписом довіреного центру сертифікації, що представлені у форматі X.509 і є ваш електронний персональний сертифікат. Проте, скористатися ним можна буде лише у випадку, коли у системі встановлена відповідність між власне сертифікатом та закритим ключем, комплементарним до того, який вказано в сертифікаті. Для цього необхідно виконати процедуру залучення сертифікату до вашого веб-браузера.

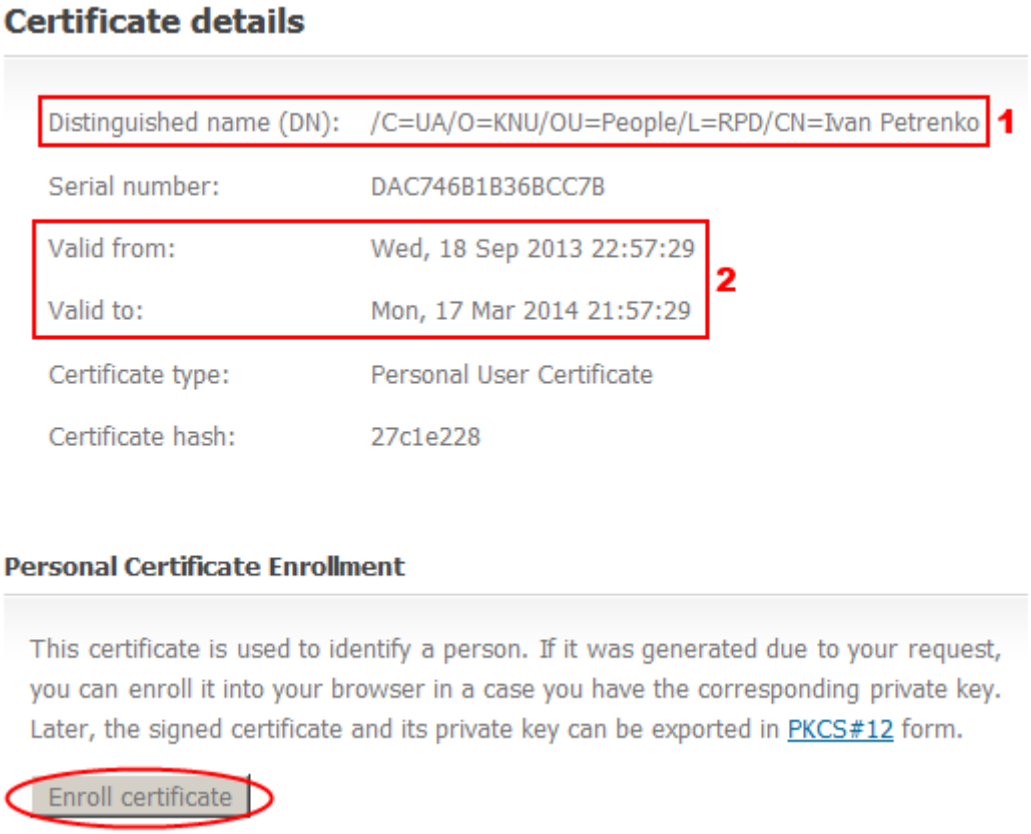
Оберіть на панелі меню зліва список усіх дійсних сертифікатів.



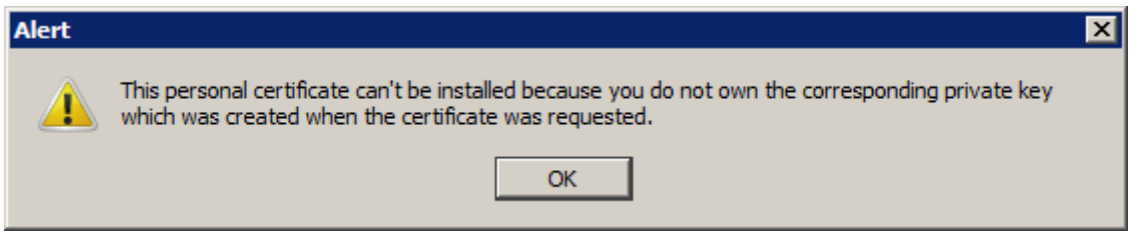
Знайдіть у списку запис із вашим іменем та натисніть на його серійний номер щоб переглянути інформацію про сертифікат. Якщо у вас були попередні спроби, то зазвичай необхідно обирати останній із записів.



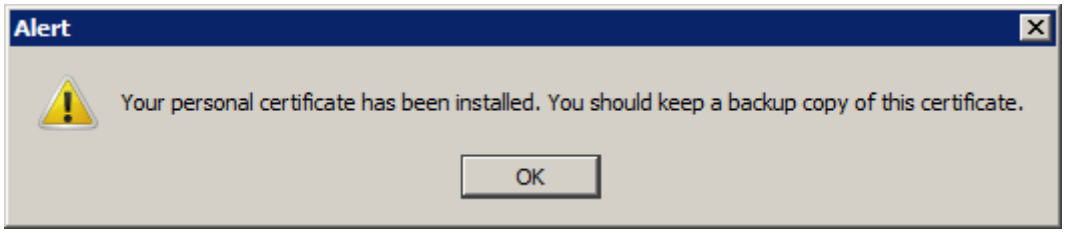
На сторінці інформації про сертифікат відображається його визначальний ідентифікатор – “Distinguished Name” (1), термін дії сертифікату (2) та інші відомості.



Для залучення сертифікату до браузера слід натиснути на кнопку “Enroll certificate”. Важливо, що залучення сертифікату є можливим лише до того ж профілю веб-браузера, у якому було попередньо згенеровано запит відповідного сертифікату та зберігається комплементарний до нього закритий ключ. У випадку використання іншого примірника веб-браузера чи вибору сертифікату іншої особи на попередньому кроці, при спробі залучення сертифікату буде неможливим, про що сповістить наступне повідомлення.



У випадку успішного залучення сертифікату веб-браузер також сповістить про це повідомленням.

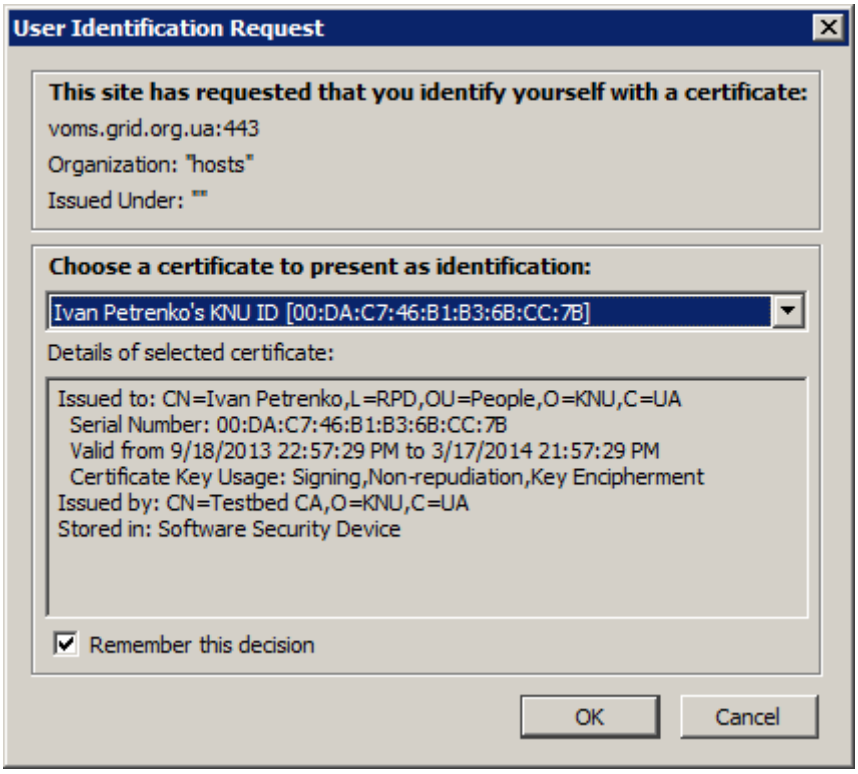


Реєстрація у віртуальній організації грід-інфраструктури

Для отримання інтерактивного доступу на обчислювальний кластер, а також для подальшого виконання лабораторних завдань із використанням обчислювальних кластерів Української національної грід-інфраструктури, необхідно вступити до спеціалізованої *віртуальної організації* (ВО) – об'єднання людей, що пов'язані єдиною метою чи напрямком досліджень. З метою навчання роботі у грід-середовищі було створено віртуальну організацію "testbed.univ.kiev.ua".

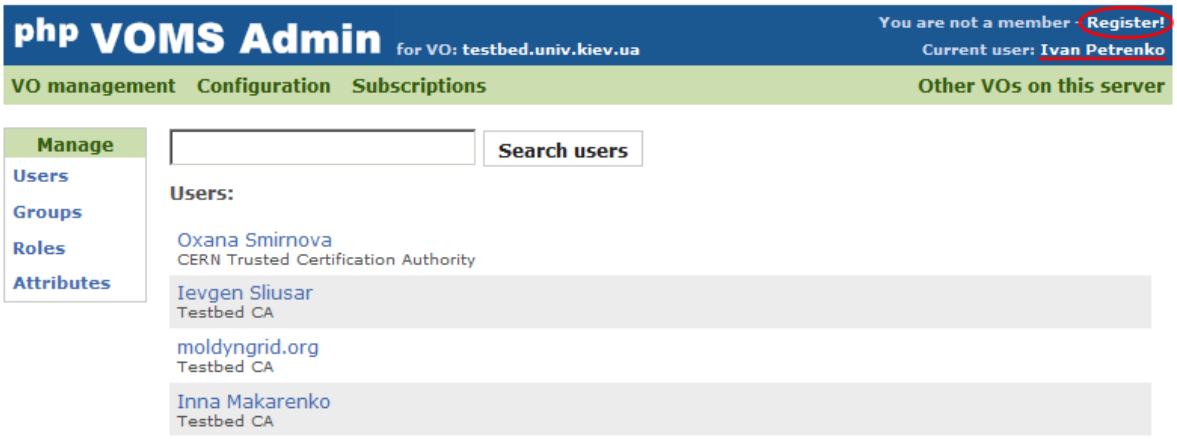
Керування участю у віртуальних організаціях технічно здійснюється за допомогою служби керування та засвідчення участі у ВО – Virtual Organization Membership Service (VOMS). Щоб подати заявку на вступ до ВО "testbed.univ.kiev.ua", необхідно скерувати веб-браузер на сторінку інтерфейсу керування служби VOMS: https://voms.grid.org.ua/voms/testbed.univ.kiev.ua/

При зверненні до сторінки, сервер здійснить спробу авторизації клієнта за допомогою персонального сертифіката. Якщо у вашому веб-браузері було успішно інстальовано ваш сертифікат, то буде виведено вікно підтвердження автентифікації. Необхідно підтвердити вибір сертифіката веб-браузером.

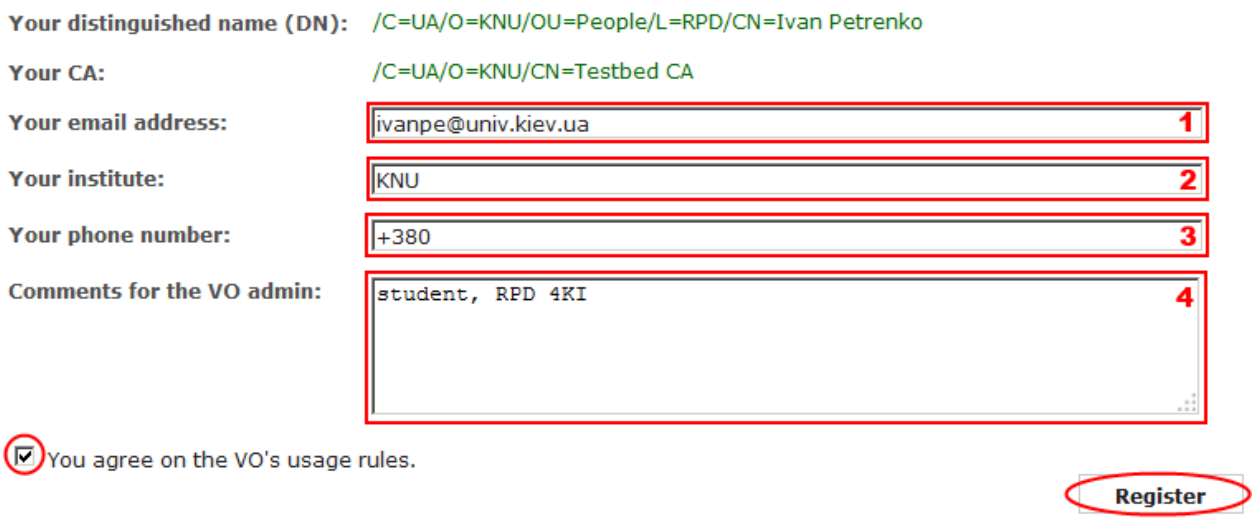


Веб-браузер може видати попередження про використання веб-сервером електронного сертифікату, що підписаний центром сертифікації без встановлених відношень довіри. У такому разі потрібно погодитись із попередженням та продовжити роботу попри можливі ризики.

На головній сторінці сервісу VOMS необхідно перевірити коректність визначення ідентифікації користувача та перейти за посиланням на форму реєстрації.



У формі реєстрації необхідно вказати дійсну адресу електронної поштової скриньки (1), зазначити назву організації (2), у нашому випадку – “KNU”, контактний телефон у міжнародному форматі без прогалин та дефісів (3). У примітці (4) для адміністратора ВО слід зазначити факультет, курс та групу. Також необхідно ознайомитись та підтвердити свою згоду із правилами використання ВО.



Якщо усі поля було заповнено коректно, сервер надішле на вказану електронну адресу листа із посиланням для підтвердження заявки. Електронний лист буде мати тему “Your membership request for VO testbed.univ.kiev.ua”.

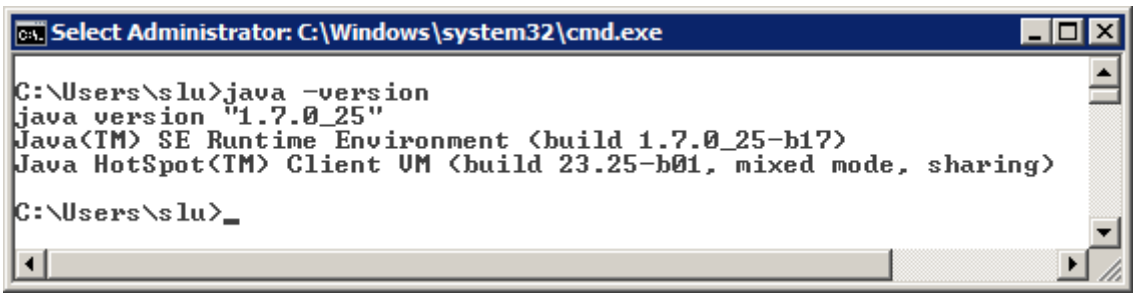
Після переходу за посиланням із електронного листа, служба VOMS передасть вашу заявку на розгляд адміністраторам ВО. Буде відображено повідомлення “Your request successfully confirmed”.

Повідомте викладача про успішно подану заявку на участь у ВО. Після того, як вашу заявку буде розглянуто та схвалено, ви отримаєте електронний лист-підтвердження. Лист матиме тему “Your membership request for VO testbed.univ.kiev.ua has been approved”.

Перед початком наступного етапу переконайтесь, що ви є у списку учасників ВО на головній сторінці віртуальної організації.

Отримання інтерактивного доступу до обчислювального кластера університету

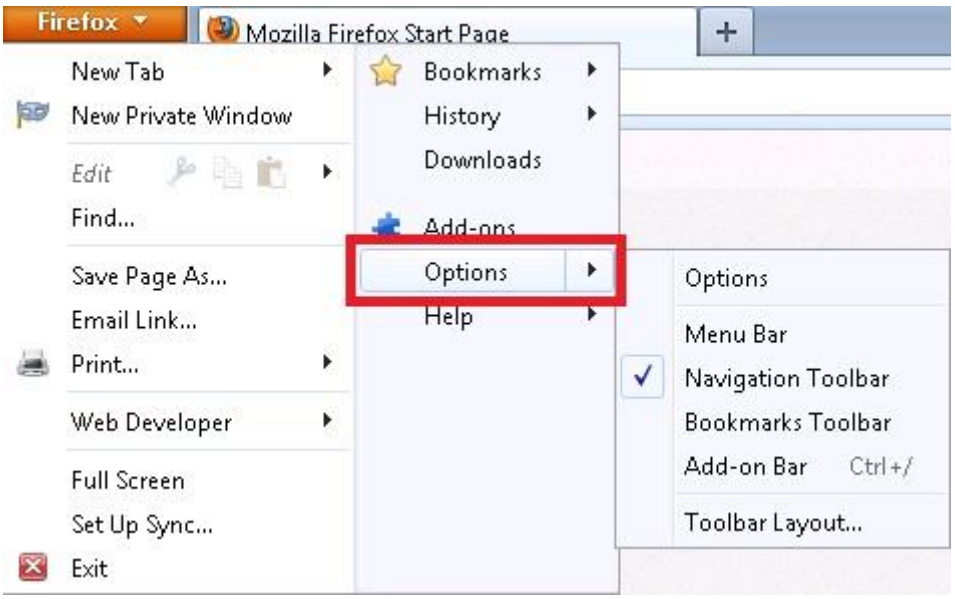
Для продовження вам знадобиться програмне забезпечення Java. Його можна завантажити та встановити на сайті http://java.com . Після встановлення переконайтесь що в командному рядку присутня команда “java” – це гарантуватиме правильне налаштування середовища для запуску програм.

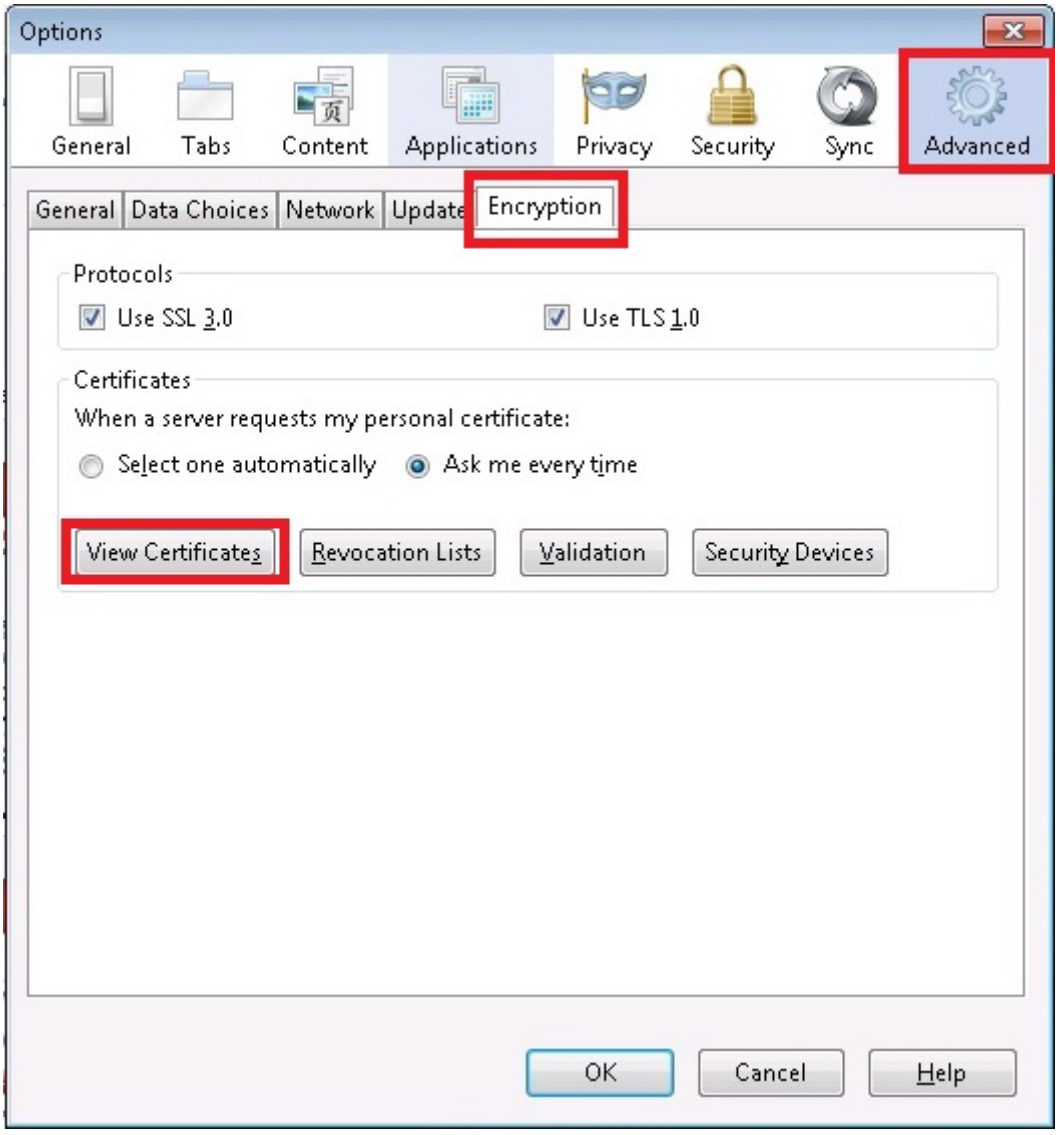


Більш детальні інструкції щодо встановлення Java та усунення проблем наведено на сторінці http://testbed.univ.kiev.ua/i_gsissh.php .

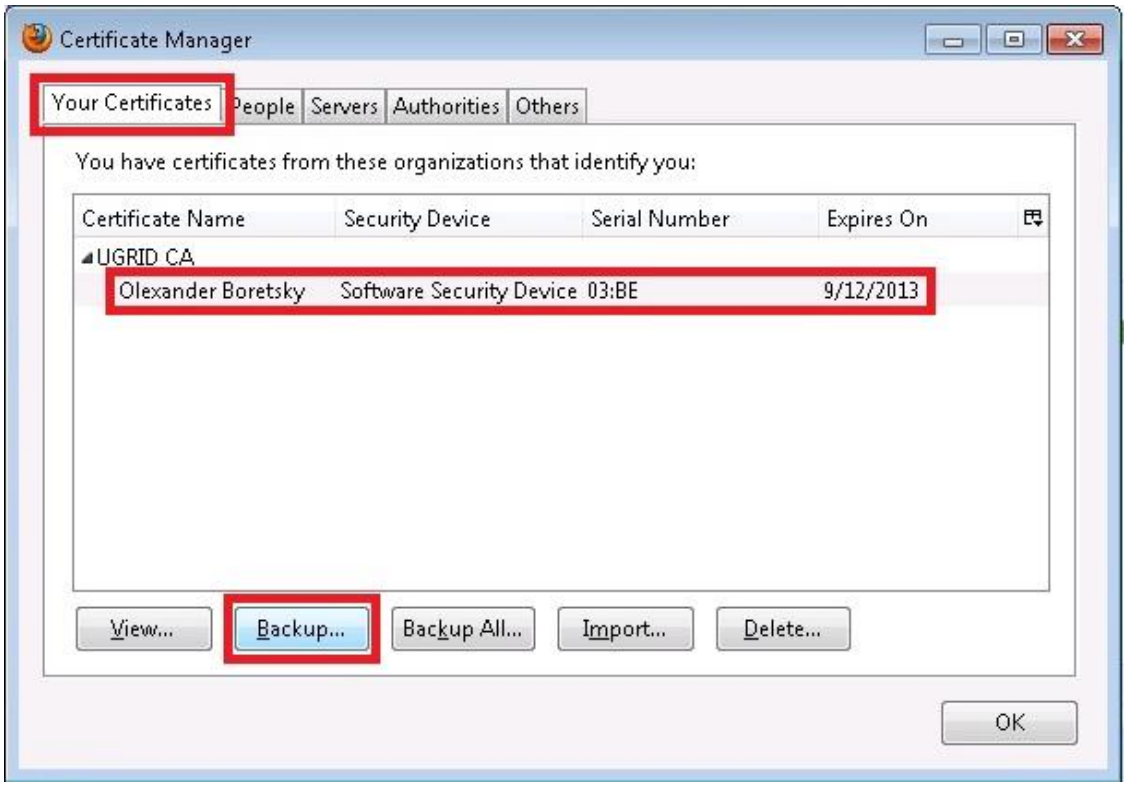
Для автентифікації користувачів при доступі до обчислювального кластеру використовується інфраструктура безпеки грід – Grid Security Infrastructure (GSI), що передбачає застосування персональних сертифікатів X.509. Для доступу буде використовуватись протокол емуляції терміналу Secure Shell (SSH).

Експорт персонального сертифікату та його закритого ключа із веб-браузера здійснюється за наступною процедурою. Сертифікат та закритий ключ запаковуються у файл-контейнер формату PKCS#12, що захищається ключовою фразою. У подальшому для використання сертифікату в інших програмах, необхідно буде вводити ключову фразу для розкриття контейнера.





Відкрийте вікно параметрів електронних сертифікатів. Перейдіть на закладку персональних сертифікатів та оберіть власний сертифікат, отриманий на попередніх етапах роботи.

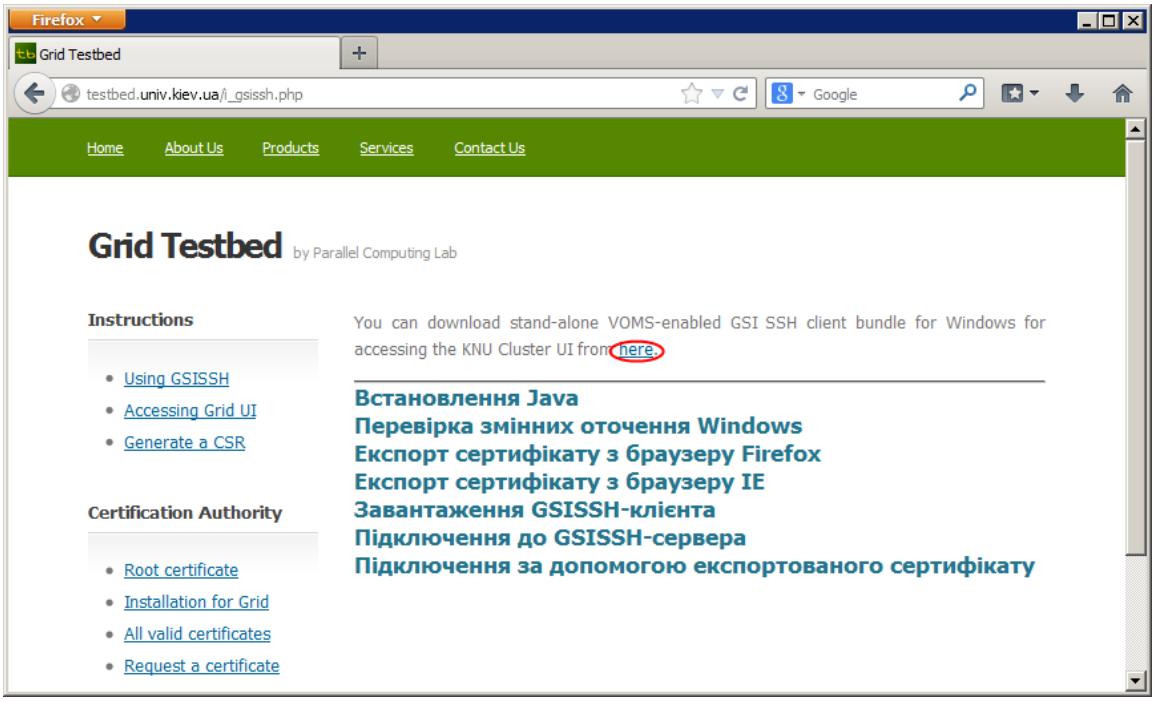


Натисніть на кнопку “Backup” та вкажіть місцезнаходження створюваного файла-контейнера PKCS#12. Він буде мати розширення “.p12”. У наступному вікні введіть бажану ключову фразу. Через експортні обмеження алгоритмів шифрування, що застосовуються у пакеті Java, довжина ключової фрази не має перевищувати 7 символів. Якщо ваша ключова фраза буде довшою, то доведеться додатково встановлювати модулі підвищення стійкості шифрування.

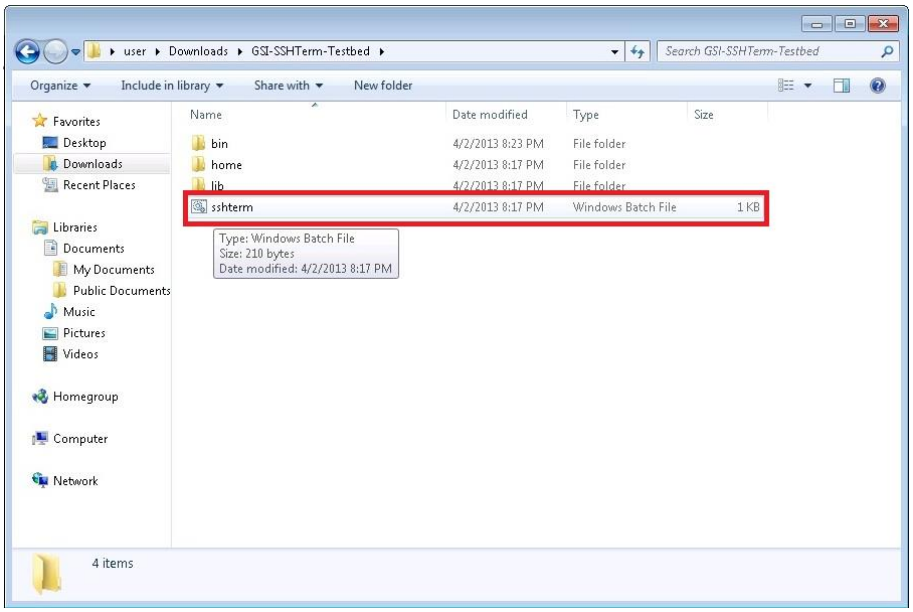
У випадку успішного експорту сертифікату, веб-браузер сповістить про це наступним повідомленням.

Збережіть одержаний файл (*.p12) на змінний носій поряд із портативною версією веб-браузера. Рекомендується скопіювати його на резервне сховище.

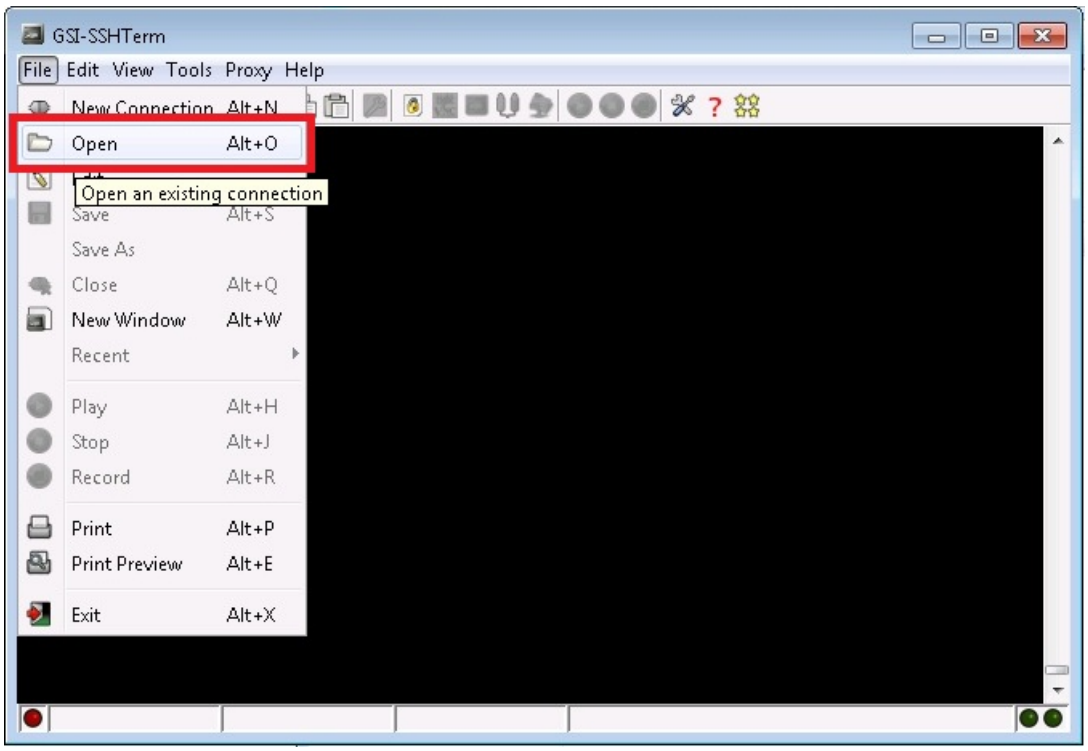
Завантажте спеціалізовану збірку пакету GSI-SSHTerm зі сторінки центру сертифікації користувачів http://testbed.univ.kiev.ua/i_gsissh.php .



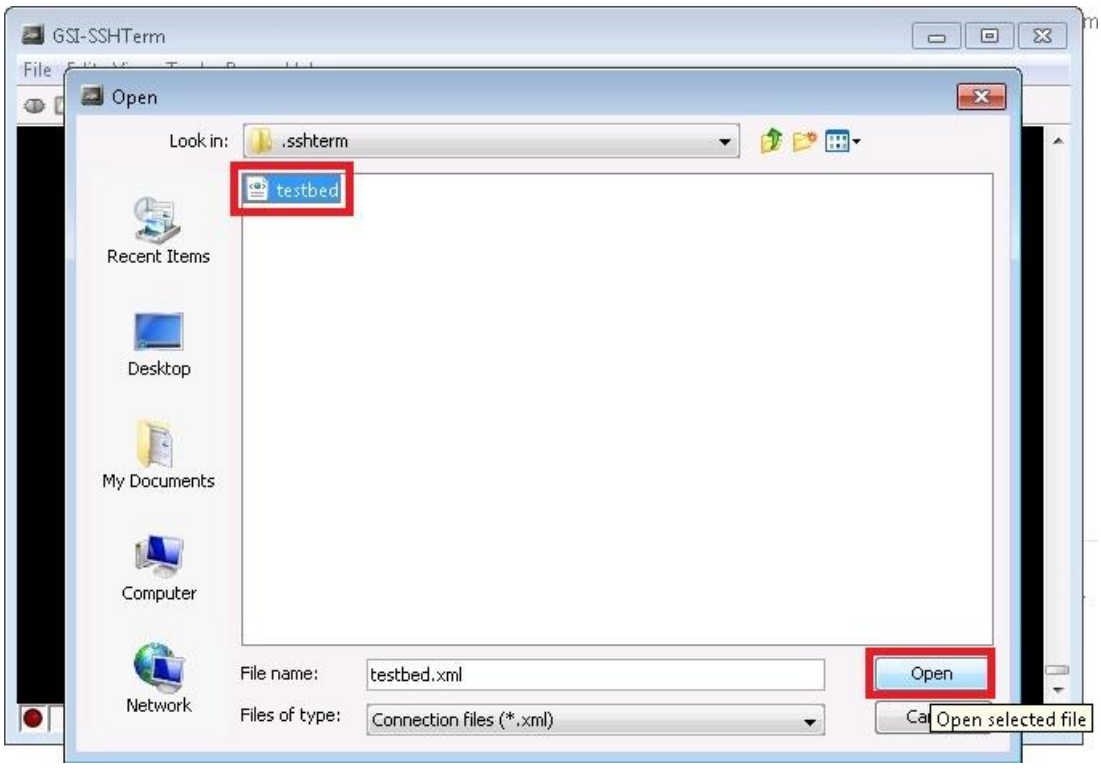
Розпакуйте архів поряд із портативною збіркою веб-браузера.



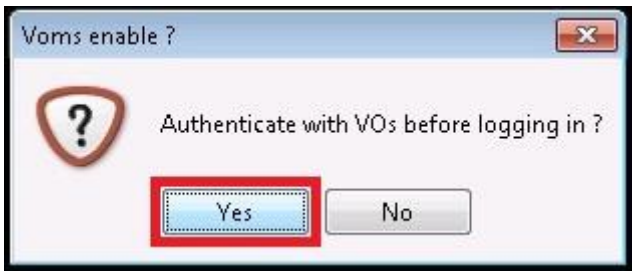
Запустіть на виконання файл “sshterm.bat”.



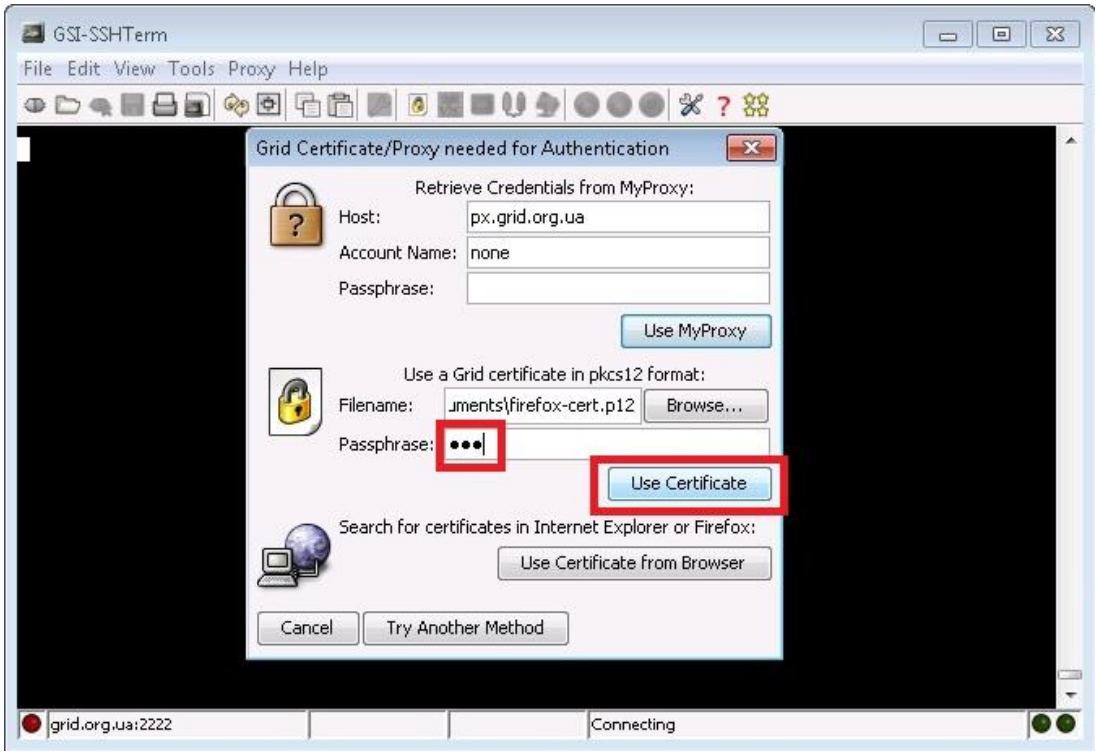
У вікні програми емуляції термінала “GSI-SSHTerm” оберіть відкриття профілю з’єднання та вкажіть готовий профіль “testbed.xml”.



Система видасть запит на використання служби VOMS для засвідчення участі у віртуальних організацях. Його необхідно підтвердити.

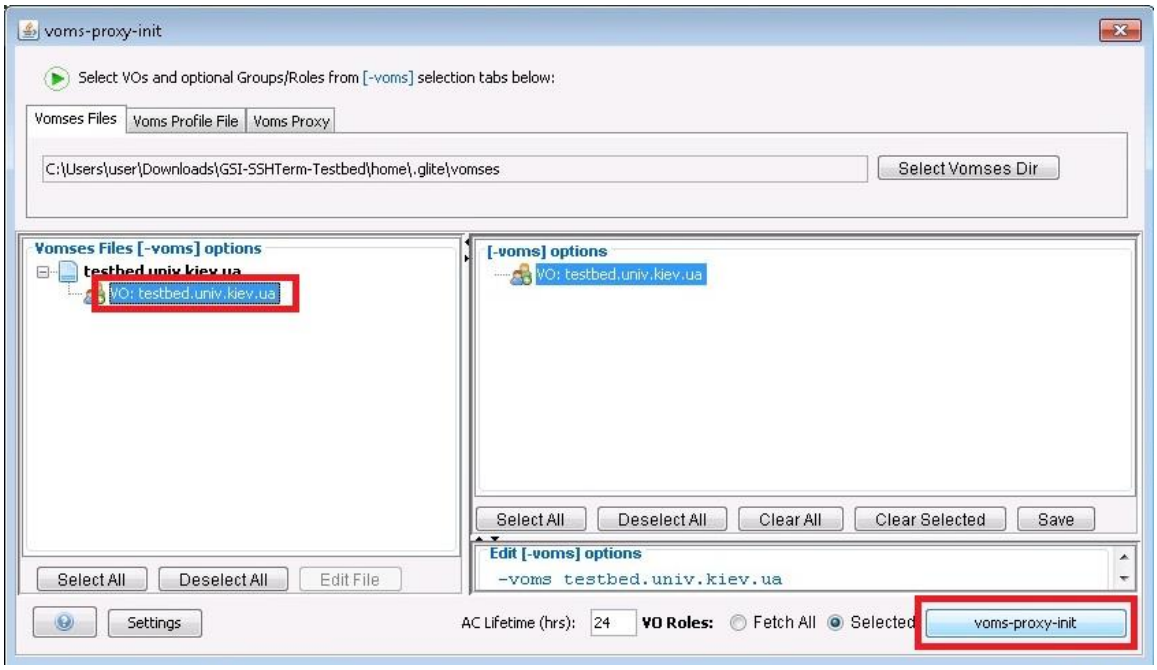


Для підключення необхідно вказати місцезнаходження шифрованого контейнера PKCS#12 із вашим персональним сертифікатом, а також ввести ключову фразу до нього.



Підтвердіть вибір сертифікату кнопкою “Use Certificate”.

Програма видасть форму засвідчення участі у віртуальних організаціях. Необхідно вказати ВО “testbed.univ.kiev.ua” та запустіть процедуру генерації проксі-сертифіката натисканням на кнопку “voms-proxy-init”.



У випадку успішного з’єднання із обчислювальним кластером буде виведено запрошення вводу команди у вікні термінала.