Інструкція з використання захищеного носія ключа eToken для Windows, установки драйвера та налаштування браузера Internet Explorer

АТ «Укрексімбанк»
2015

Зміст

Шановний клієнте!

Вітаємо Вас із початком використання цифрового сертифіката для здійснення платежів в Інтернет-банкінгу АТ «Укрексімбанк»!

Інформація в Інтернет-банкінгу захищена відповідно до сучасних світових стандартів захисту електронної інформації. Ваші платіжні документи підписуються електронно-цифровим підписом. Це робить неможливим підробку документів, гарантує їх авторство та цілісність за умови конфіденційного використання та зберігання носія ключа.

З умовами безпеки роботи в системі Ви маєте можливість ознайомитись за посиланням: http://www.eximb.com/ukr/personal/everyday/internet_banking/safety/

1. Для чого потрібен захищений носій ключа eToken

Ваш таємний ключ знаходяться на спеціальному захищеному носії ключа (далі – eToken). Захищений носій ключа eToken потрібен для створення і підпису платіжних документів. Таємний ключ і сертифікат створюються Вами в Банку.

Починати використання eToken можна тільки після установки на Вашому комп'ютері спеціальної програми-драйвера SafeNet. Програма SafeNet працює тільки в операційних системах **Windows** XP, Vista, Windows 7, Windows 8, браузері **Internet Explorer** 7.0 і вище.

Не підключайте eToken до комп'ютера поки успішно не завершиться встановлення програми SafeNet. Інакше, встановлення програми може пройти з помилками.

Використання eToken для створення платежів можливе лише у разі знання пін-коду. Пін-код створюється Вами в Банку при форматуванні eToken.

Не здійснюйте форматування eToken самостійно. Це призведе до видалення Вашого таємного ключа. Форматувати eToken можна тільки в Банку в присутності менеджера.

2. Перший сеанс роботи із захищеним носієм ключа eToken

Для першого сеансу роботи з eToken Вам необхідно:

2.1. Завантажити з веб-сайту Банку і встановити спеціальну програму-драйвер SafeNet;

2.2. Під'єднати eToken до USB порту комп'ютера;

2.3. Увійти до системи з використанням eToken.

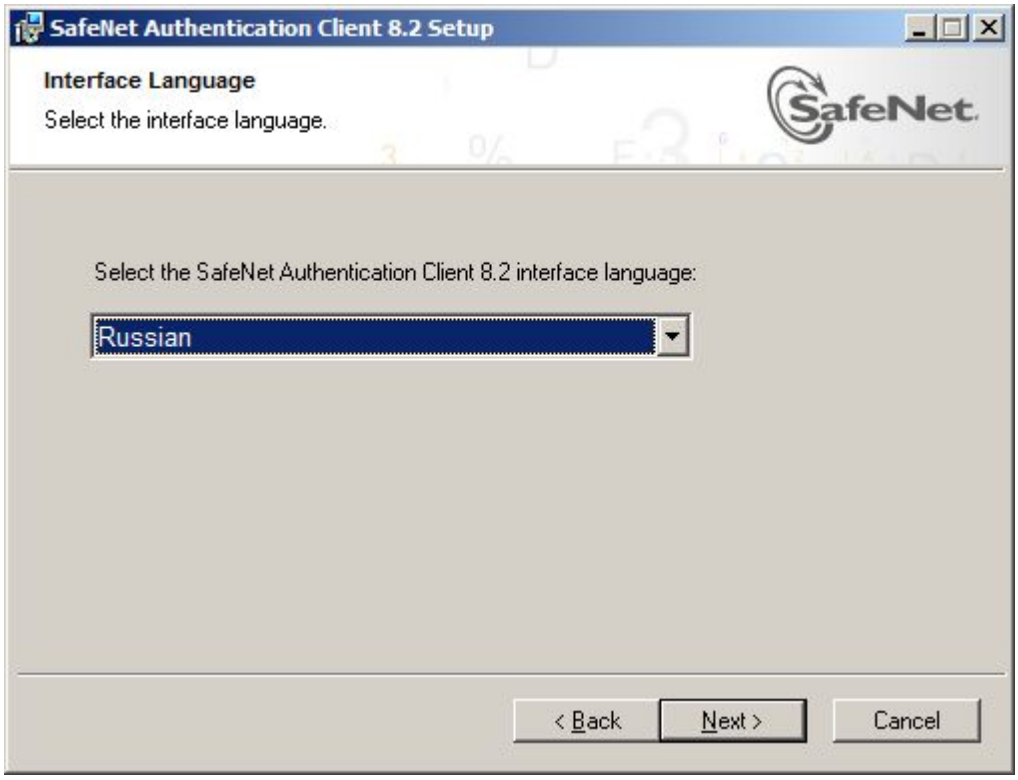
2.1. Встановлення спеціальної програми-драйвера SafeNet

1. Збережіть на комп'ютері та відкрийте архівний файл з програмою-драйвером. Файл-архів міститься за посиланням: *http://www.eximb.com/upload/portal/SAC-8.2.rar*

2. Виберіть файл SAC-8.2-x32.msi або SAC-8.2-x64.msi в залежності від розрядності Вашої операційної системи. Запустіть програму подвійним натисненням миші.

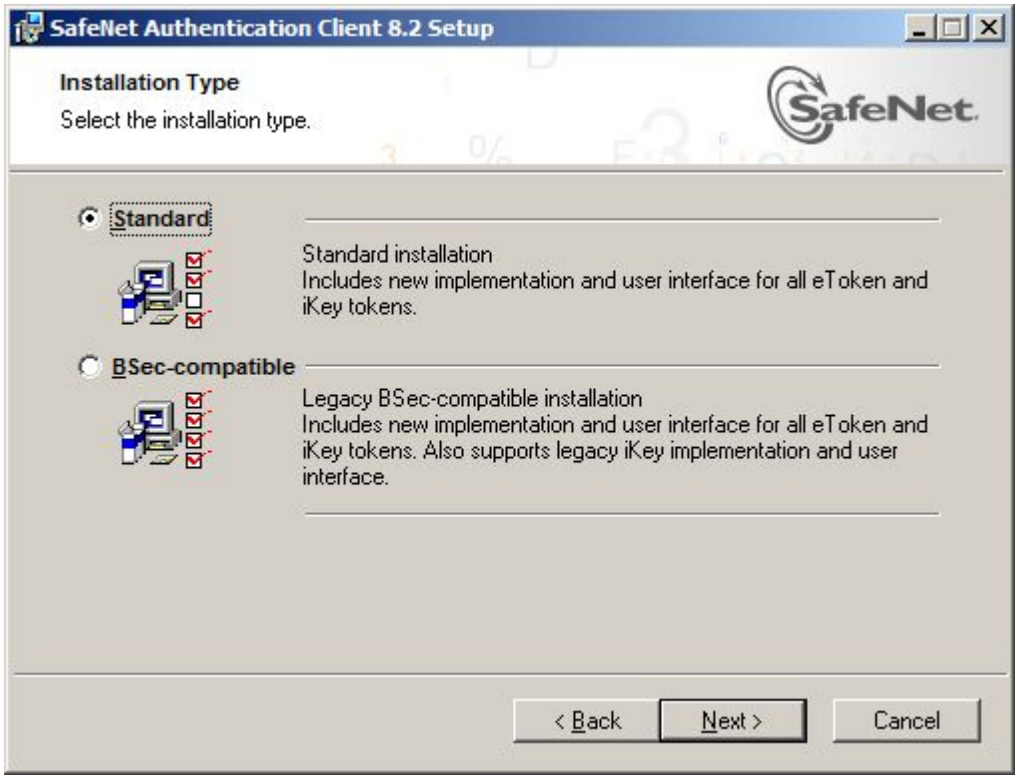
3. Програма розпочинає роботу з вікна привітання. Для початку встановлення драйвера натисніть кнопку *«Next»*.

4. Оберіть мову та натисніть кнопку *«Next»*.

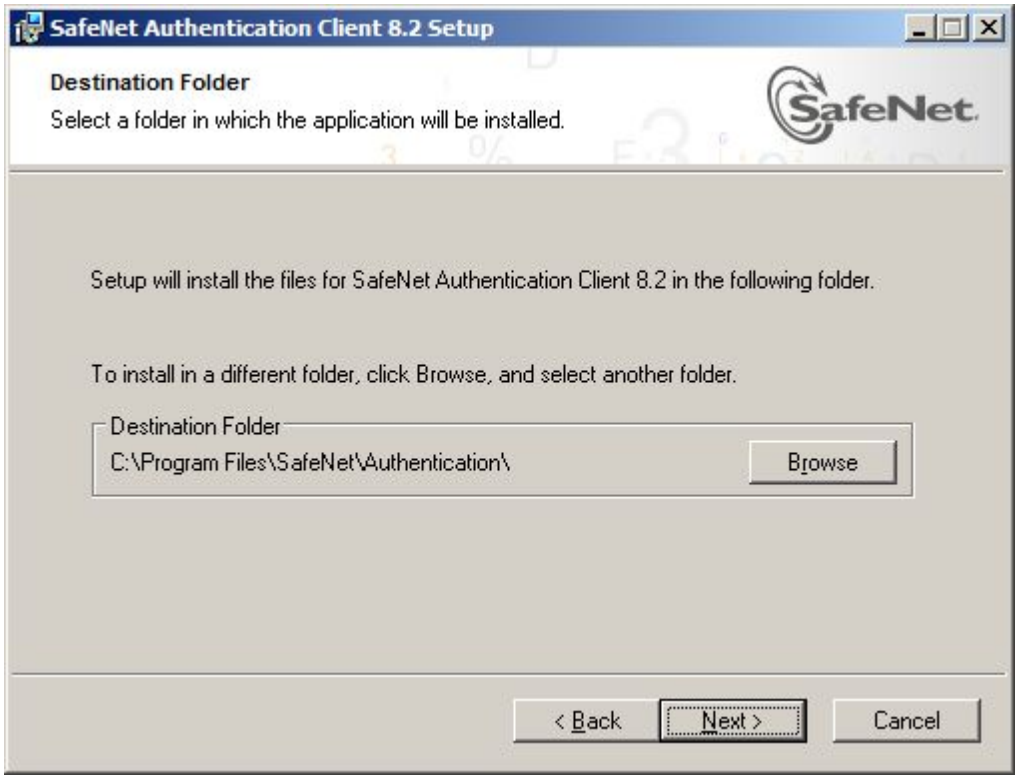


6. Ознайомтесь з Ліцензійною угодою та натисніть кнопку *«Next»*:

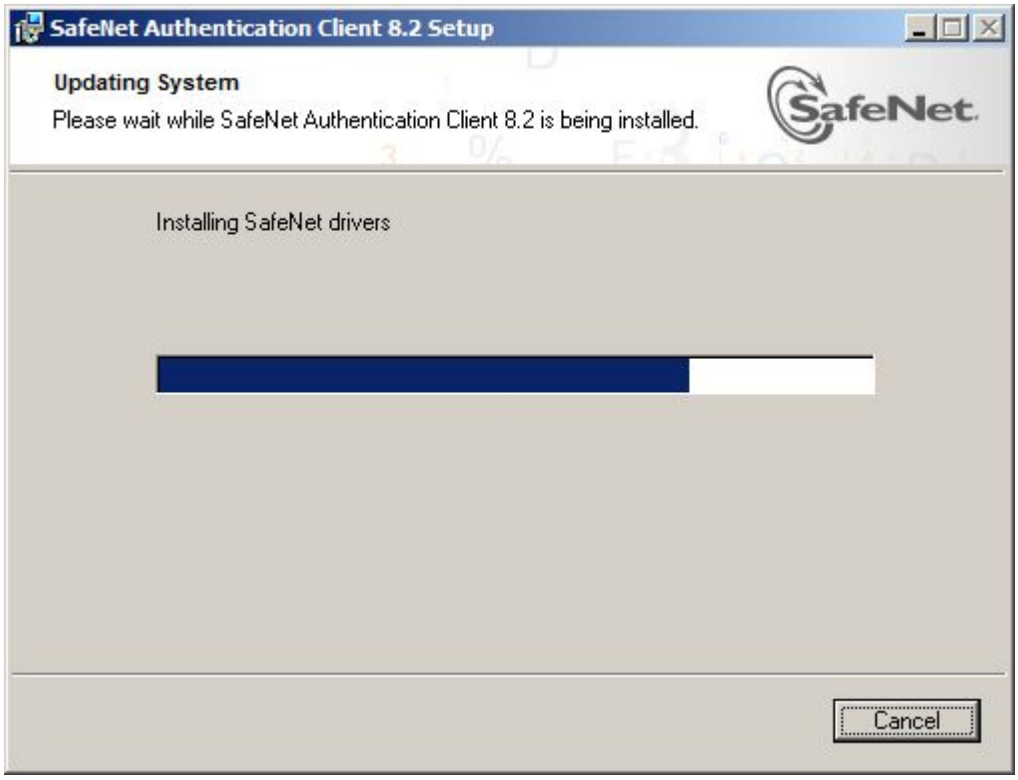
7. Натисніть кнопку *«Next»*:



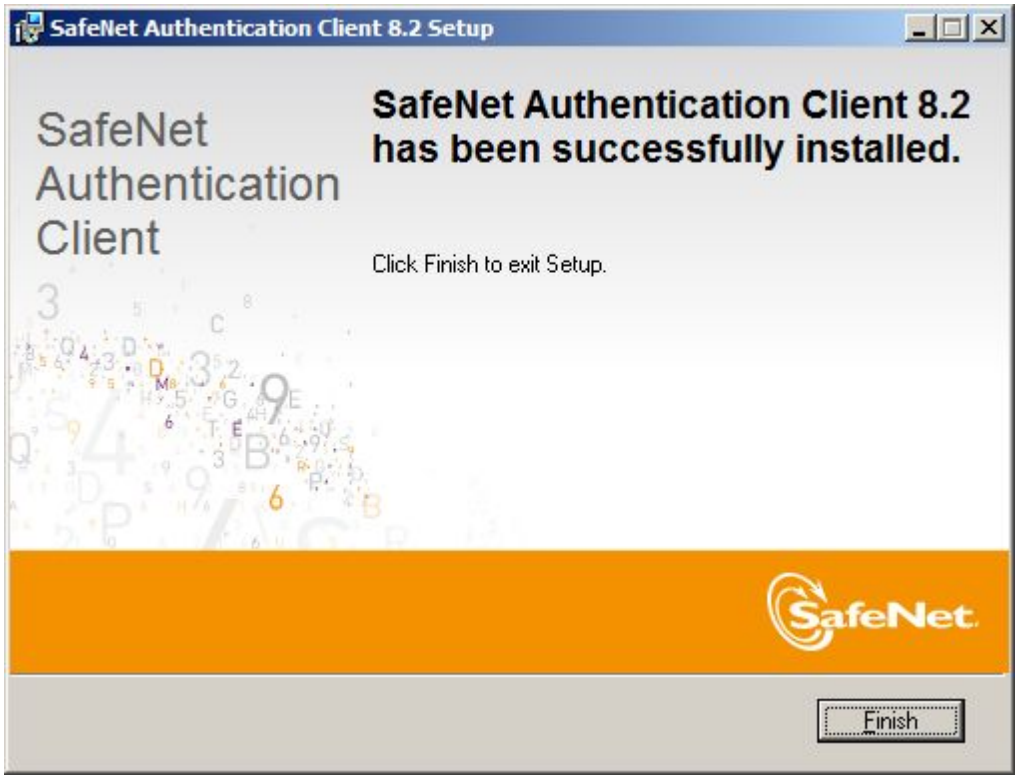
9. За замовчуванням драйвер буде встановлено в папку «Program Files», якщо є необхідність, Ви маєте можливість кнопкою «Browse» обрати іншу папку для встановлення драйверу. Далі натисніть кнопку *«Next»*:

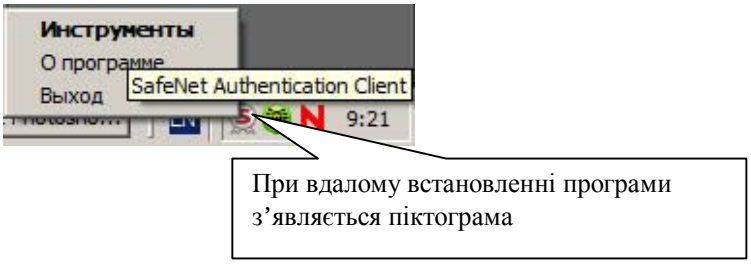


10. Вікно встановлення драйверу:



11. По завершенні інсталяції програмного забезпечення натисніть кнопку «Finish»:





Вітаємо з успішною установкою програми!

З цього моменту на Вашому комп'ютері є можливість використовувати в Інтернет-банкінгу цифровий сертифікат і ЕЦП. Не забудьте перевірити налаштування Internet Explorer для завантаження елементів ActiveX (п. 2.2 Інструкції).

2.2. Виконання налаштувань Internet Explorer для завантаження елементів ActiveX

На початку першого сеансу роботи в Інтернет-банкінгу з використанням сертифіката на Ваш комп'ютер буде автоматично встановлено елемент ActiveX.

Приналежність елемента ActiveX Банку посвідчена сертифікатом міжнародного сертифікаційного агентства Thawte. При наступних сеансах роботи елемент ActiveX повторно не встановлюється.

i **В налаштуваннях Internet Explorer повинні бути дозволені виконання, автоматичні запити та завантаження <u>підписаних</u> елементів ActiveX. Якщо налаштування цього не дозволяють, Internet Explorer видасть повідомлення *Error on Page* (Помилка на сторінці) у нижній лівій (*Status Bar*) частині екрана.**

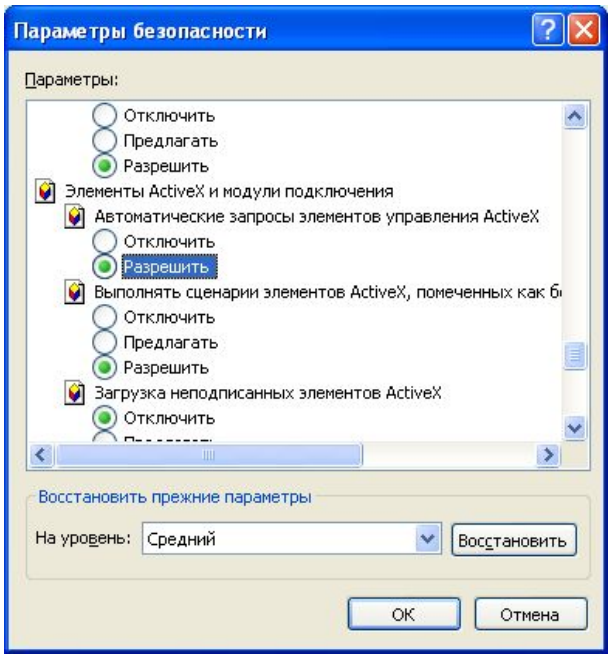
Налаштування розташовані в меню Internet Explorer: Tools (Сервис) > Internet Options (Свойства обозревателя) > закладка Security (Безопасность) > кнопка Custom Level (Другой), пункти розділу Active controls and plug-ins:

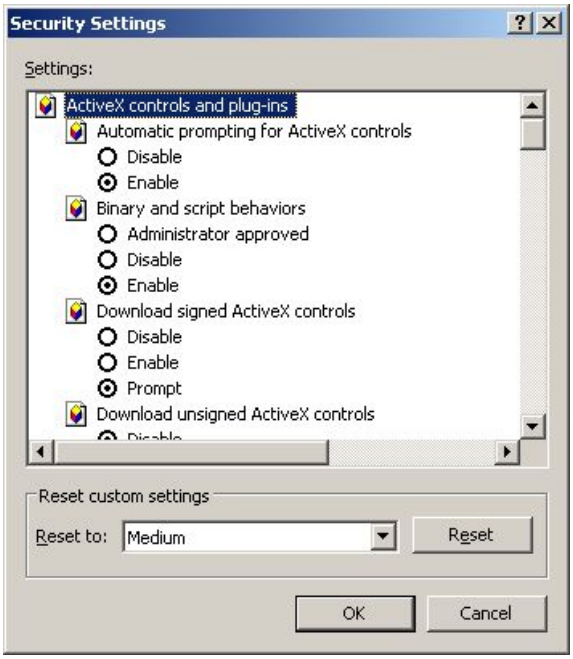
Якщо браузер на російській мові:

1. Автоматичні запити елементів управління ActiveX – вибрати Разрешить;
2. Виконати сценарії елементів ActiveX, помічених як безпечні – вибрати Разрешить;
3. Завантаження підписаних елементів ActiveX – вибрати Предлагать;
4. Запуск елементів ActiveX і модулів підключення – вибрати Разрешить.

Якщо браузер на англійській мові:

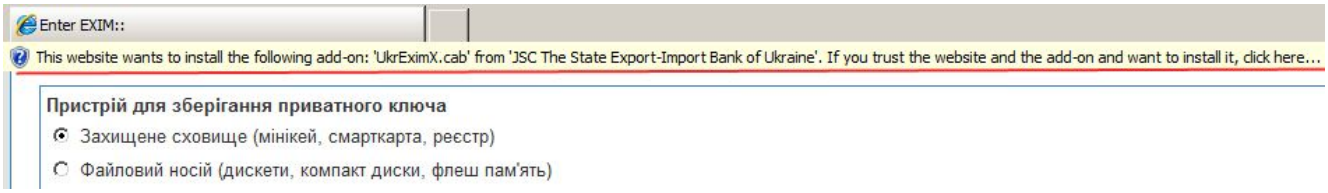
1. Automatic prompting for ActiveX controls – вибрати Enable;
2. Run Active controls and plug-ins – вибрати Enable;
3. Download signed Active controls – вибрати Prompt;
4. Binary and script behaviors – вибрати Enable.





Якщо повідомлення про установку ActiveX при першому сеансі роботи з сертифікатом не з'являється, зверніть увагу, що для установки елемента ActiveX користувачам необхідні права Адміністратора (принаймні для першого успішного сеансу роботи з використанням цифрового сертифіката). Для наступних сеансів роботи права Адміністратора непотрібні – елемент ActiveX зберігається на Вашому комп'ютері постійно.

Користувачі Windows XP Service Pack 2 бачать рядок попередження жовтого кольору у верхній частині екрана:



На запит Windows про дозвіл на установку елемента ActiveX, який належить JSC «Ukreximbank», відповідайте «Так»:

Додатково надаємо інформацію для адміністратора Вашого комп'ютера у випадку видалення або повторного встановлення елемента ActiveX.

Для видалення елемента ActiveX Банку виконайте команду (*Start* > *Run*) – *regsvr32.exe UkrExim.ocx /u*

Windows повідомить Вас про успішне виконання команди. Після видалення елемента ActiveX і входу до Інтернет-банкінгу з використанням цифрового сертифіката Вам буде повторно запропоновано встановити елемент ActiveX.

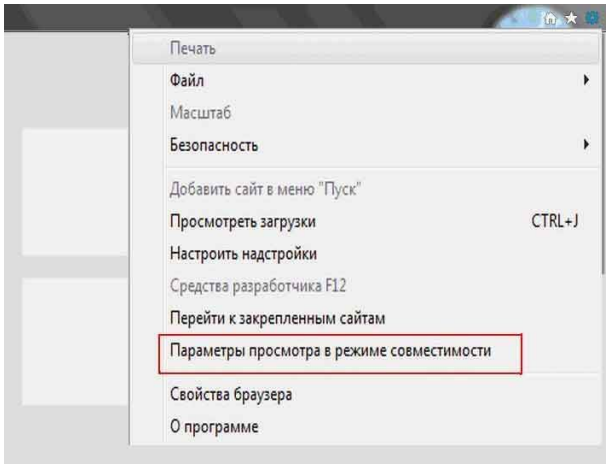
Якщо установка елемента ActiveX Банку не виконана, в нижній лівій частині екрана з'явиться повідомлення «Помилка на сторінці / Error on Page»:

При використанні у деяких операційних системах **Windows** необхідно провести такі налаштування в браузері Internet Explorer:

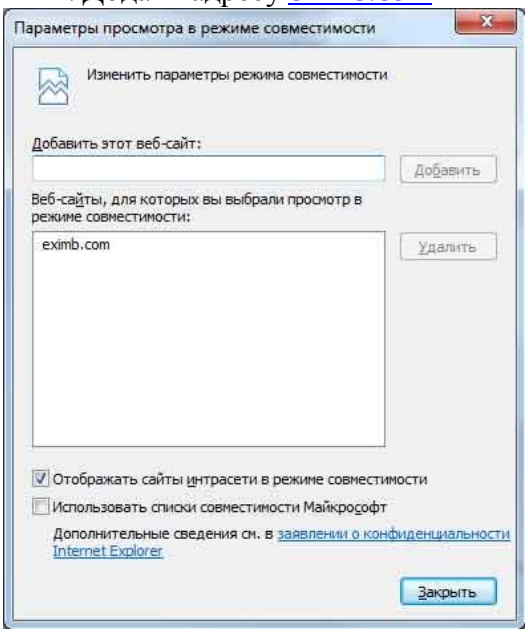
1. Вибрати меню «Tools (Сервис) > Internet Options (Свойства обозревателя)»;
2. У закладку «Privacy (Конфиденциальность) > Edit (Параметры)» додати www.eximb.com і https://bank.eximb.com;
3. У закладку «Security (Безопасность) > Trusted sites (Надежные узлы) > Sites (Узлы)» додати https://bank.eximb.com.

В браузері **Internet Explorer 11** потрібно здійснити наступні налаштування:

1. Обрати меню «Сервис» далі «Параметры просмотра в режиме совместимости**».**



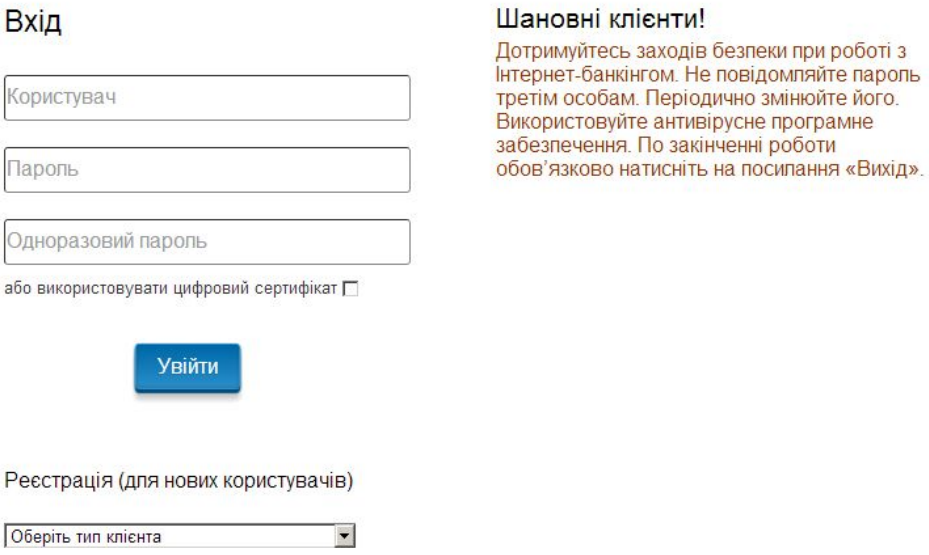
2. Додати адресу eximb.com



2.3. Вхід до Інтернет-банкінгу з використанням захищеного носія ключа eToken

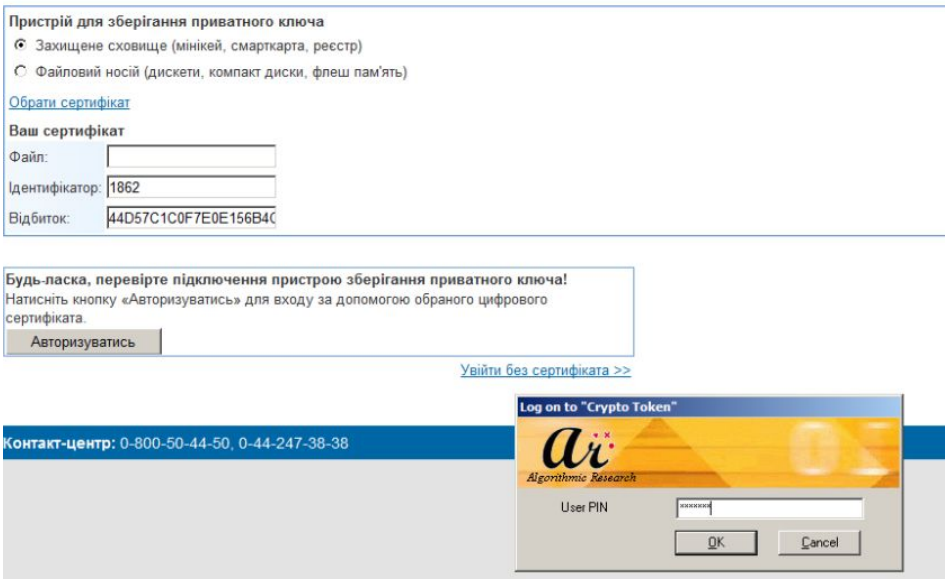
Входити до Інтернет-банкінгу з пристроєм eToken можна після успішної установки програми SafeNet (п. 2.1 Інструкції) і перевірки налаштувань браузера Internet Explorer (п. 2.2 Інструкції).

1. На сторінці входу до Інтернет-банкінгу введіть ім’я користувача і пароль. Поле «Одноразовий пароль» заповнювати непотрібно. Відмітьте на екрані поле «використовувати цифровий сертифікат»:



Якщо Ви вже увійшли з рівнем аутентифікації «Пароль», підключити цифровий сертифікат можна в меню Інтернет-банкінгу «*Налаштування* > *Підключити «Цифровий сертифікат»*.

2. Натиснувши на кнопку «Увійти», Ви переходите до сторінки підключення цифрового сертифіката.



Під’єднайте eToken до USB порту комп’ютера. При цьому індикатор на пристрої має засвітитися.

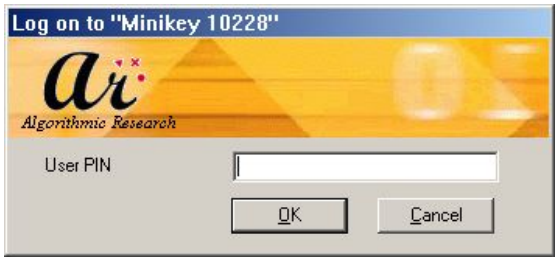
У блоці «Пристрій для зберігання приватного ключа» повинно бути відмічене поле «Захищене сховище (мінікей, смарткартка, реєстр)».

Якщо в блоці «Ваш сертифікат» поля «Ідентифікатор» і «Відбиток» не заповнені, натисніть на посилання «Обрати сертифікат», після чого поля «Ідентифікатор» і «Відбиток» повинні заповнитись автоматично.

Якщо поля «Ідентифікатор» і «Відбиток» не заповнюються, переконайтесь, що програму SafeNet встановлено коректно, установка елементів ActiveX дозволена (п. 2.2 Інструкції), eToken під’єднано до порту USB комп’ютера, а індикатор на пристрої світиться.

3. Після того, як поля «Ідентифікатор» та «Відбиток» вже заповнено, натисніть кнопку «Авторизуватись».

Вам буде запропоновано увести пін-код доступу до eToken. Пін-код створюється Вами в Банку при форматуванні eToken. Пін-код можна змінити самостійно. Якщо Ви забули пін-код, необхідно прийти до Банку для форматування eToken, створення нового пін-коду і нового сертифікату.



4. Після успішного входу в Інтернет-банкінг Ви можете працювати з платежами. У правому верхньому куті екрана буде стояти відмітка «Аутентифікація: Цифровий сертифікат».

2.4. Перевірка в браузері Internet Explorer наявності цифрового сертифіката і правильної роботи програми SafeNet

Ви можете перевірити правильність установки програми SafeNet та її роботи.

Перевірку необхідно виконати у випадку наявності помилок або повідомлення «У сховищі нема ключів для підпису або не обрано жодного ключа».

1. Увійдіть в меню Internet Explorer «Сервис (Tools) > Свойства обозревателя (Internet Options) > Содержимое (Content) > кнопка «Сертификаты» (Certificates)»:

2. У вікні «Сертификаты» повинно бути видно ім’я сертифіката. Ім’я сертифіката таке ж як і ім’я користувача (наприклад, sheva1010).

3. Під час перевірки програма SafeNet має бути встановлена, eToken має бути під’єднаний до USB порту комп’ютера, а індикатор на пристрої eToken має світитися.

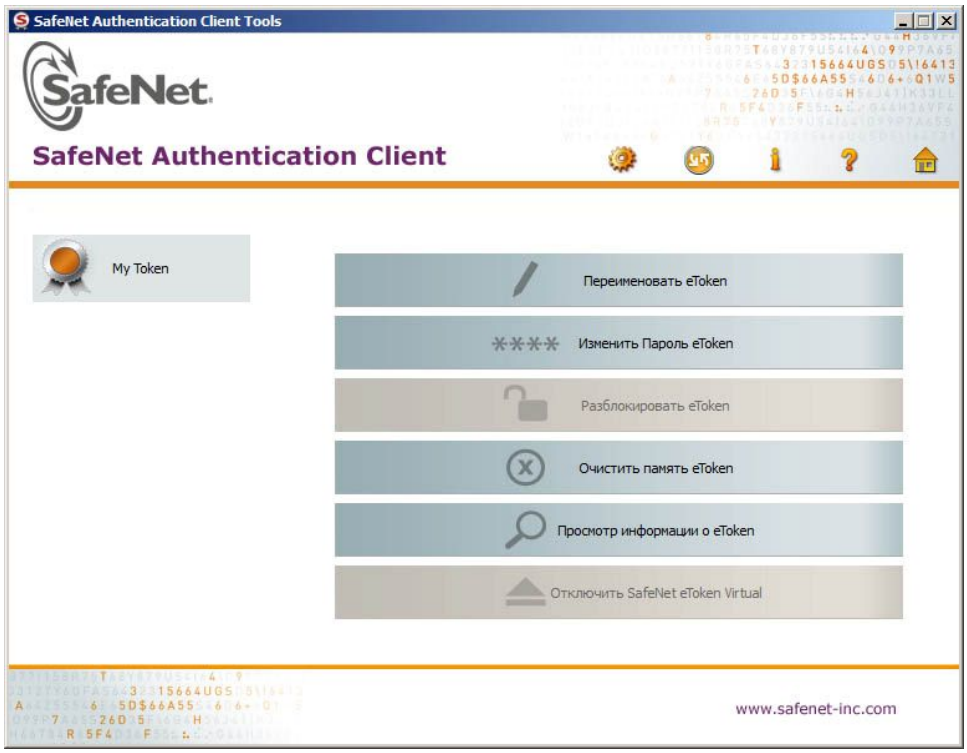
4. Якщо імені сертифіката не видно, це означає, що програма SafeNet встановлена неправильно або eToken не підключений до порту USB.

3. Зміна пін-коду до eToken.

Створювати і підписувати платежі з eToken можна тільки після введення пін-коду. Пін-код створюється Вами в Банку при форматуванні eToken. В подальшому **пін-код можна змінювати самостійно** (але не обов'язково). Для зміни пін-коду програма SafeNet вже повинна бути успішно встановлена на Вашому комп'ютері.

3.1. Підключіть eToken до порту USB. Індикатор на пристрої має світитися.

3.2. Натисніть в Windows кнопку «Пуск» і виберіть пункт меню «SafeNet» > «SafeNet Authentication Client» > «SafeNet Authentication Client Tools». З'явиться меню управління пристроєм.



За допомогою меню «Изменить пароль eToken» Ви маєте змогу змінити Пін-код пристрою.

4. Можливі проблеми і варіанти їх вирішення

Проблема	Вирішення
Після натискання на посилання «Вибрати цифровий сертифікат» поля «Ідентифікатор» і «Відбиток» не заповнюються. Після натискання на посилання «Вибрати цифровий сертифікат» або кнопки «Авторизуватися» з'являється повідомлення «У сховищі немає ключів для підпису або не обрано жодного ключа».	Після натискання на посилання «Вибрати цифровий сертифікат» поля «Ідентифікатор» і «Відбиток» повинні заповнюватися автоматично. Це відбувається при таких умовах: 1. Програму-драйвер SafeNet встановлено (п. 2.1 Інструкції); 2. Установку елементів ActiveX дозволено (п. 2.2 Інструкції); 3. Автоматичне встановлення елементів ActiveX виконано (п. 2.2 Інструкції); 4. eToken зі створеним у Банку сертифікатом

	під'єднано до USB порту комп'ютера, а індикатор eToken світиться.
У вікні Internet Explorer «Сервис > Свойства обозревателя > Содержание > Сертификаты» не видно назви сертифіката.	У вікні Internet Explorer «Сервис > Свойства обозревателя > Содержание > Сертификаты» назву сертифіката видно при таких умовах: 1. Програмау-драйвер SafeNet встановлено (п. 2.1 Інструкції); 2. eToken зі створеним у Банку сертифікатом під'єднано до USB порту комп'ютера.
Після відмітки позначки «Використовувати цифровий сертифікат» на екрані з'являється повідомлення «Вибраний рівень аутентифікації недоступний».	Ваш сертифікат не активовано в Банку. Будь ласка, повідомте про помилку менеджера Банку, який допомагав Вам створювати цифровий сертифікат.

5. Запитання та відповіді

Запитання	Відповідь
Чи можна використовувати один сертифікат на різних комп'ютерах?	Так, один сертифікат **можна використовувати на різних комп'ютерах.** Для цього на кожному комп'ютері повинен бути встановлений драйвер SafeNet і дозволені елементи ActiveX. Під'єднувати eToken до USB порту комп'ютера можна тільки після установки драйвера.
Що таке захищений носій ключа (eToken)?	**eToken** – це спеціальний невеликий пристрій, на якому зберігається таємний ключ і сертифікат клієнта. **eToken** виконує криптографічні перетворення з цим ключем для підпису платіжних доручень і забезпечує надійне зберігання таємного ключа без можливості його копіювання. eToken підключається до комп'ютера через USB порт. На цей криптографічний пристрій для захисту інформації в Інтернет-банкінгу **видано експертний висновок Служби безпеки України.**
Що таке генератор одноразових паролів?	**Генератор одноразових паролів –** пристрій, який приватні клієнти можуть використовувати для платежів замість eToken.  Юридичні особи можуть використовувати генератор одноразових паролів для створення платіжних доручень. **Переваги генератора**: пристрій не потрібно підключати до комп'ютера, не потрібно встановлювати спеціальний драйвер. Особливість генератора: сума і кількість платежів обмежені.