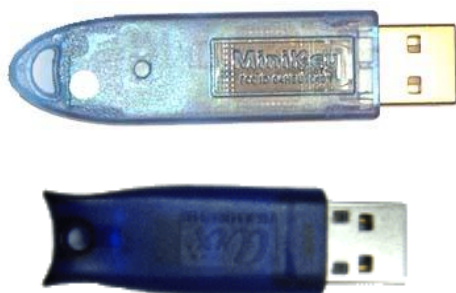




Інструкція з використання захищеного носія ключа MiniKey для Windows 7 (32-bit), установки драйвера та налаштування браузера Internet Explorer



Зміст

1. Для чого потрібен захищений носій ключа MiniKey	3
2. Перший сеанс роботи із захищеним носієм ключа MiniKey	3
2.1. Встановлення спеціальної програми-драйвера CryptoKit	3
2.2. Виконання налаштувань Internet Explorer для завантаження елементів ActiveX	7
2.3. Підтвердження успішності установки програми-драйвера CryptoKit	9
2.4. Вхід до Інтернет-банкінгу з використанням захищеного носія ключа MiniKey	11
2.5. Перевірка в браузері Internet Explorer наявності цифрового сертифіката і правильної роботи програми CryptoKit	12
3. Зміна пін-коду до MiniKey	13
4. Можливі проблеми і варіанти їх вирішення	15
5. Запитання та відповіді	15

Шановний клієнте!

Вітаємо Вас із початком використання цифрового сертифіката і здійсненням 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.

1. Для чого потрібен захищений носій ключа MiniKey

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

Починати використання MiniKey можна тільки після установки на Вашому комп'ютері спеціальної програми-драйвера CryptoKit (п. 2.1 Інструкції). Програма CryptoKit працює тільки в операційних системах **Windows**, браузері **Internet Explorer 7** і вище.



Не підключайте MiniKey до комп'ютера до успішної установки програми CryptoKit. Інакше, установка програми може пройти з помилками.

Використання MiniKey для створення платежів можливе лише у разі знання пін-коду. Пін-код створюється Вами в Банку при форматуванні MiniKey. Пін-код не можна забувати. Ви можете змінювати його самостійно (п. 3 Інструкції).



Не здійснюйте форматування MiniKey самостійно. Це призведе до видалення Вашого таємного ключа і цифрового сертифіката. Форматувати MiniKey можна тільки в Банку в присутності менеджера.

2. Перший сеанс роботи із захищеним носієм ключа MiniKey

Для першого сеансу роботи з MiniKey Вам необхідно:

1. «Скачати» з веб-сайту Банку і встановити спеціальну програму-драйвер CryptoKit (п. 2.1 Інструкції);
 2. Виконати налаштування Internet Explorer для завантаження елементів ActiveX (п. 2.2 Інструкції);
 3. Вставити MiniKey в порт USB комп'ютера;
 4. Увійти до Інтернет-банкінгу з використанням сертифіката (п. 2.4 Інструкції).
- При наступних сеансах роботи Вам достатньо виконувати пункти 3-4.

Якщо у Вас виникають помилки, Ви можете використовувати розділ «Можливі проблеми і варіанти їх вирішення» (п. 4 Інструкції).

2.1. Встановлення спеціальної програми-драйвера CryptoKit

1. Збережіть на комп'ютері і відкрийте файл-архів з програмою-драйвером. Файл-архів міститься на сторінці:

Для приватних клієнтів: Головна » Приватним клієнтам » Послуги » Інтернет-банкінг » Захист

http://www.eximb.com/ukr/personal/everyday/internet_banking/priladi/

Для малого та середнього бізнесу: Головна » Малому і середньому бізнесу » Послуги
» Інтернет-банкінг » Захист

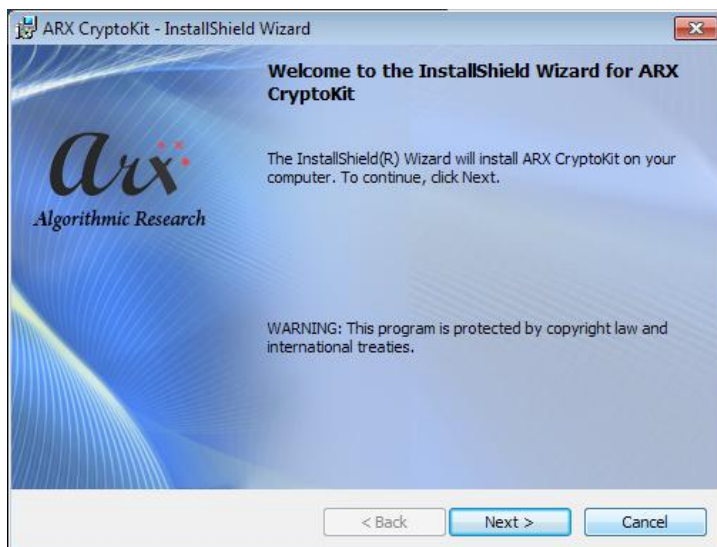
http://www.eximb.com/ukr/sme/everyday/internet_banking/priladi/

Для корпоративного бізнесу: Головна » Корпоративному бізнесу » Інтернет-банкінг »
Захист

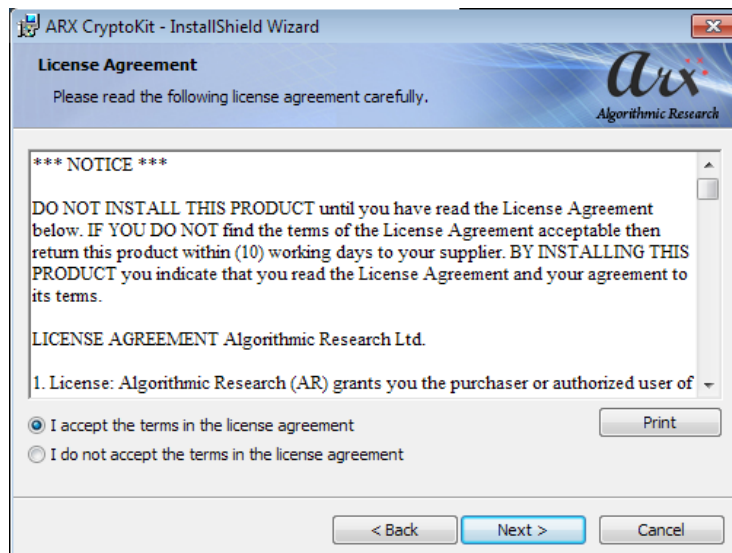
http://www.eximb.com/ukr/corporate/internet_banking/priladi/

2. Виберіть файл *ARX CryptoKit Runtime.msi* і запустіть програму подвійним натисненням миші.

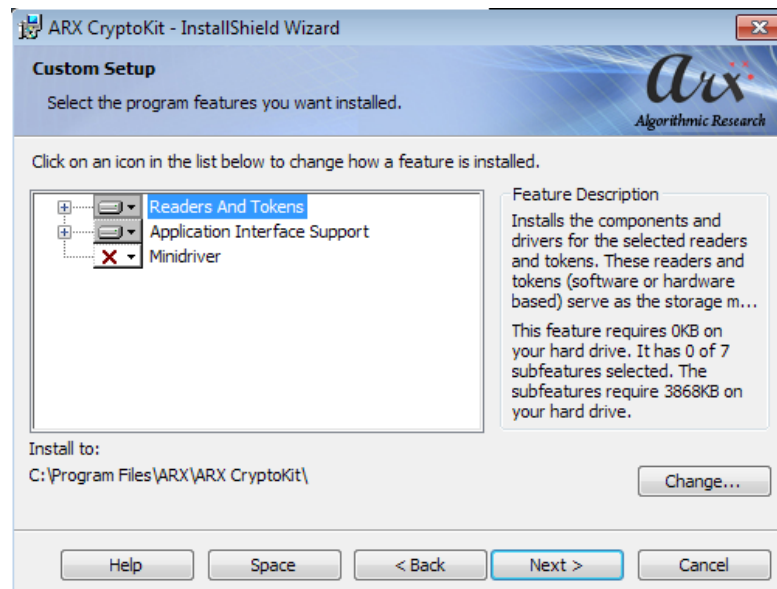
3. Програма починає роботу з вікна привітання. Для початку роботи натисніть на кнопку «Next»:



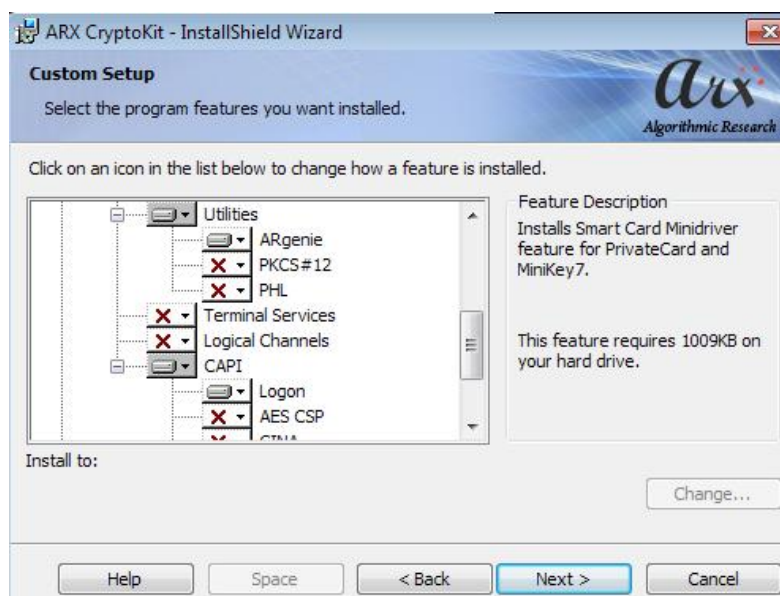
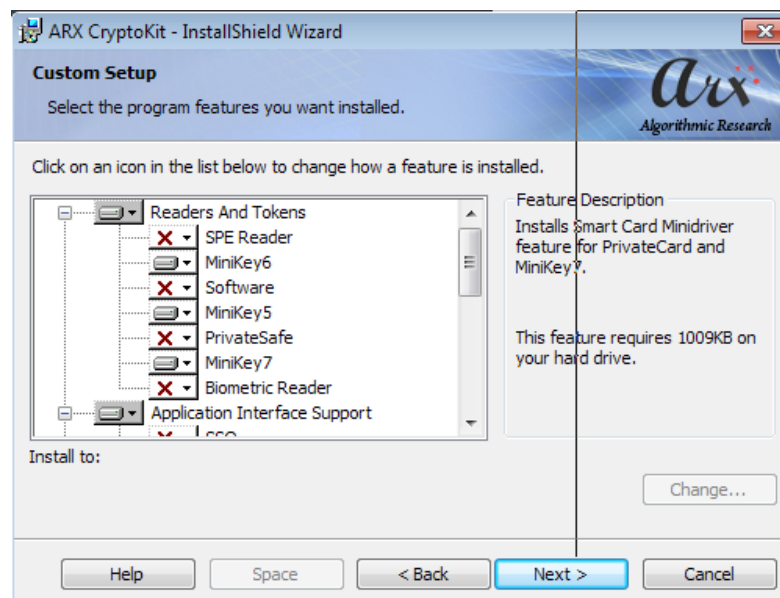
4. Ознайомтесь з Ліцензійною угодою і натисніть кнопку «Next»:



5. Натисніть на «+» розділу «Readers And Tokens» для розкриття списку компонентів:



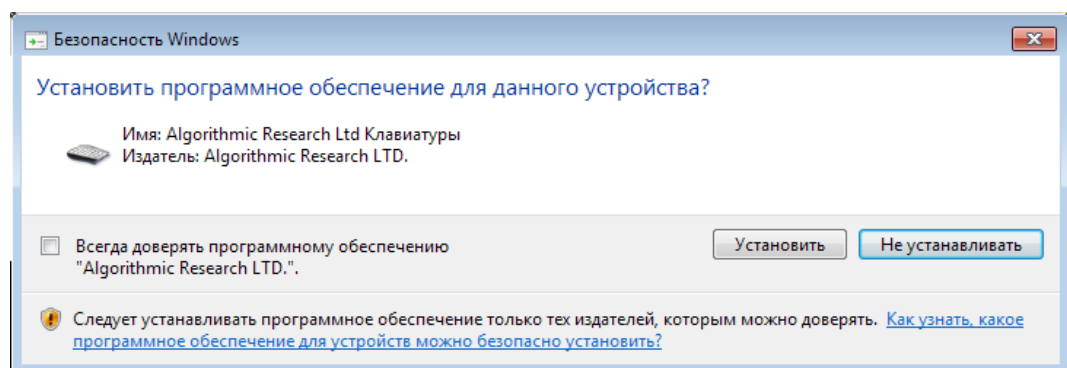
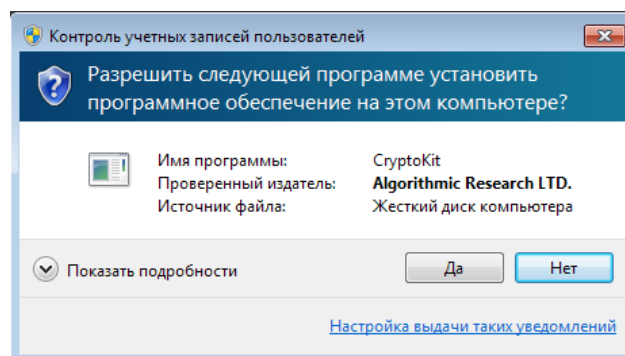
6. Зробіть вибір компонентів, як показано на малюнках:

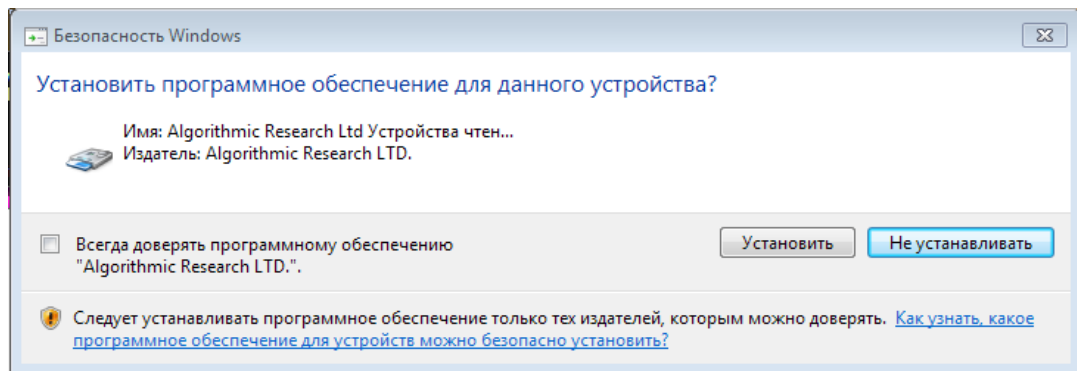


7. Для продовження натисніть кнопку «Next».
8. Натисніть кнопку «Install» для початку установки програми:



9. У процесі установки програми можуть з'явитися вікна із запитом на установку програмного забезпечення на Ваш комп'ютер, виберіть «Да» або «Установить»:

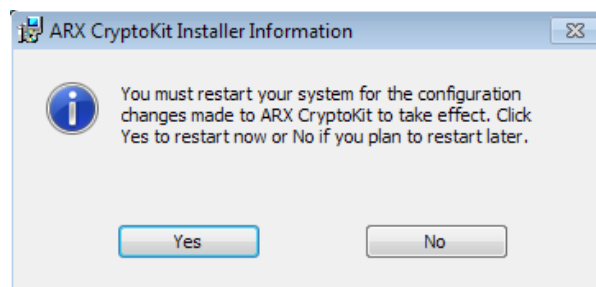




10. По завершенні установки натисніть кнопку «Finish»:



11. Після установки перезавантажите Ваш комп'ютер, натисніть кнопку «Yes»:



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.



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

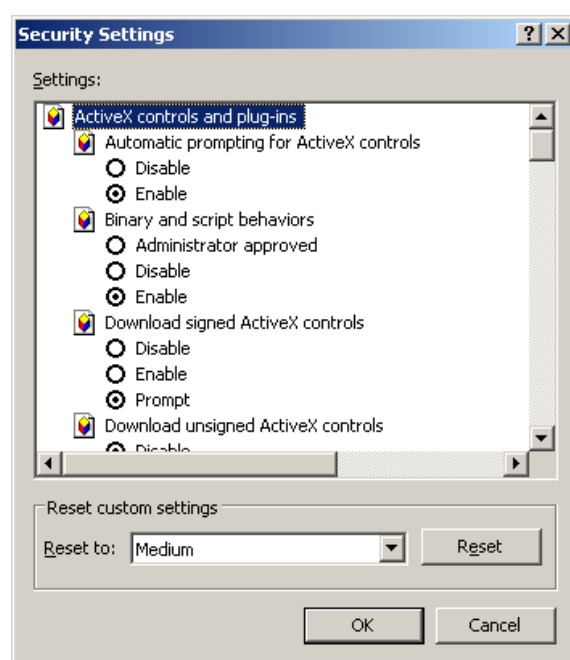
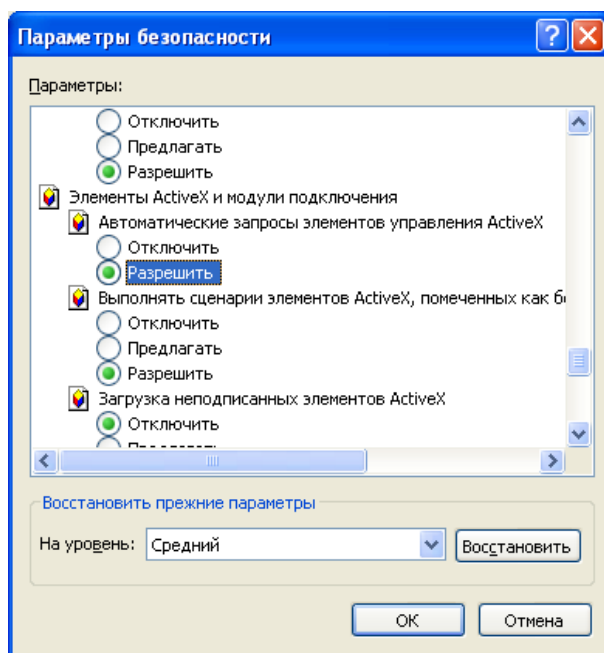
Налаштування розташовані в меню Internet Explorer: Tools (Сервис) » Internet Options (Свойства обозревателя) » закладка Security (Безопасность) » кнопка Custom Level (Другой), пункти розділу Active controls and plug-ins:

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.

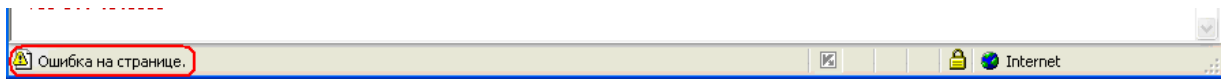


Додатково надаємо інформацію для адміністратора Вашого комп'ютера у випадку видалення або перевстановлення елемента ActiveX.

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

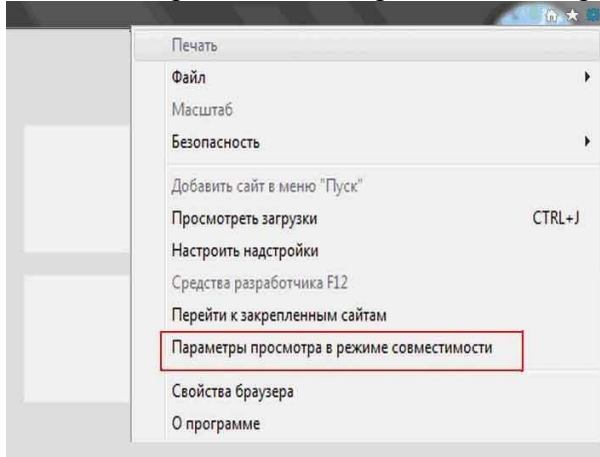
Windows повідомить Вас про успішне виконання команди. Після видалення елемента ActiveX і входу до Інтернет-банкінгу з використанням цифрового сертифіката Вам буде повторно запропоновано встановити елемент ActiveX.

При невиконаній установці елемента ActiveX Банку, в нижній лівій частині екрана з'явиться повідомлення «Помилка на сторінці / Error on Page»:

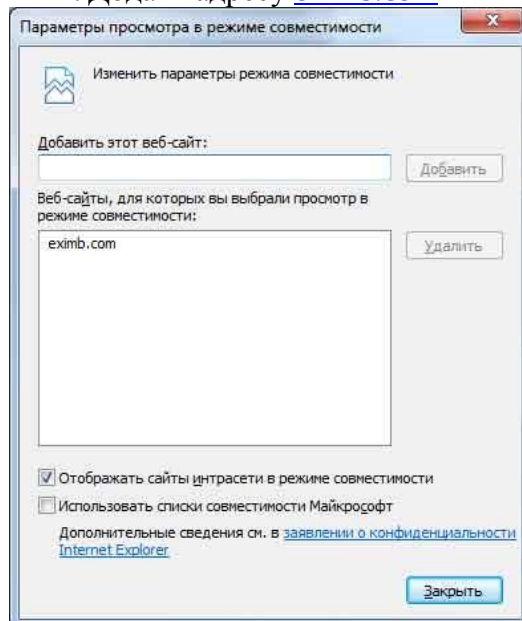


В браузері **Internet Explorer 11** потрібно здійснити наступні налаштування:

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

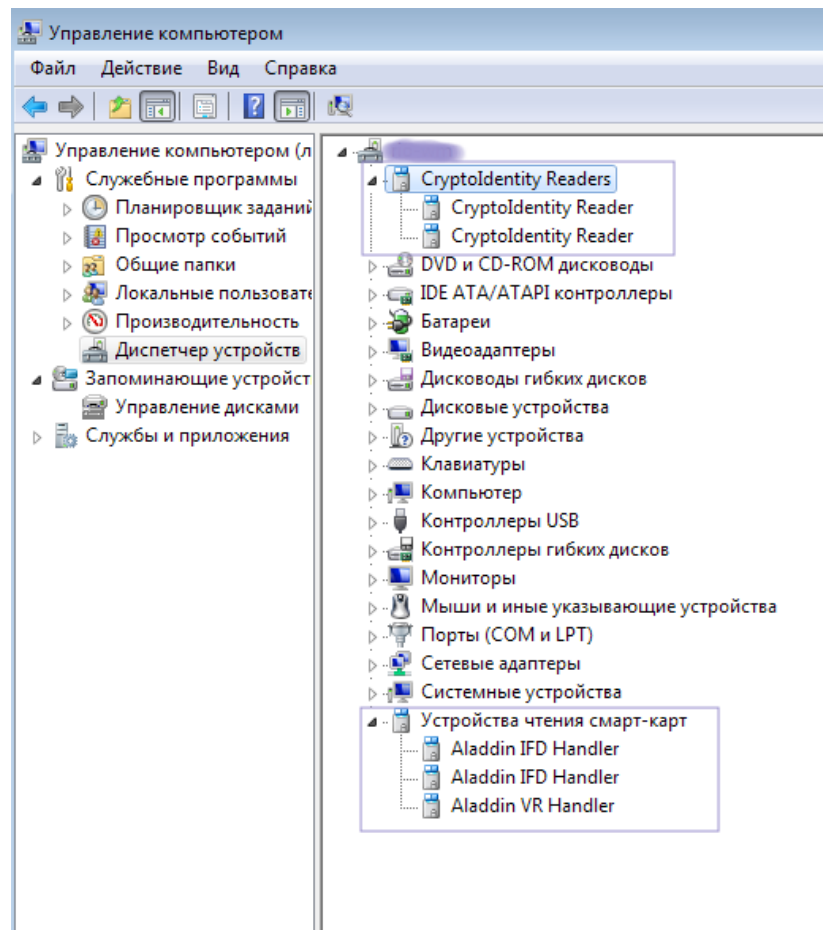


2. Додати адресу eximb.com

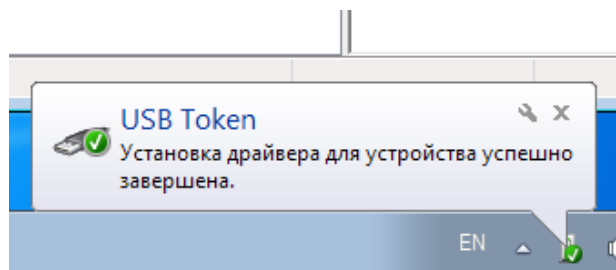


2.3. Підтвердження успішності установки програми-драйвера CryptoKit

Після перезавантаження з'являться нові пристрої:

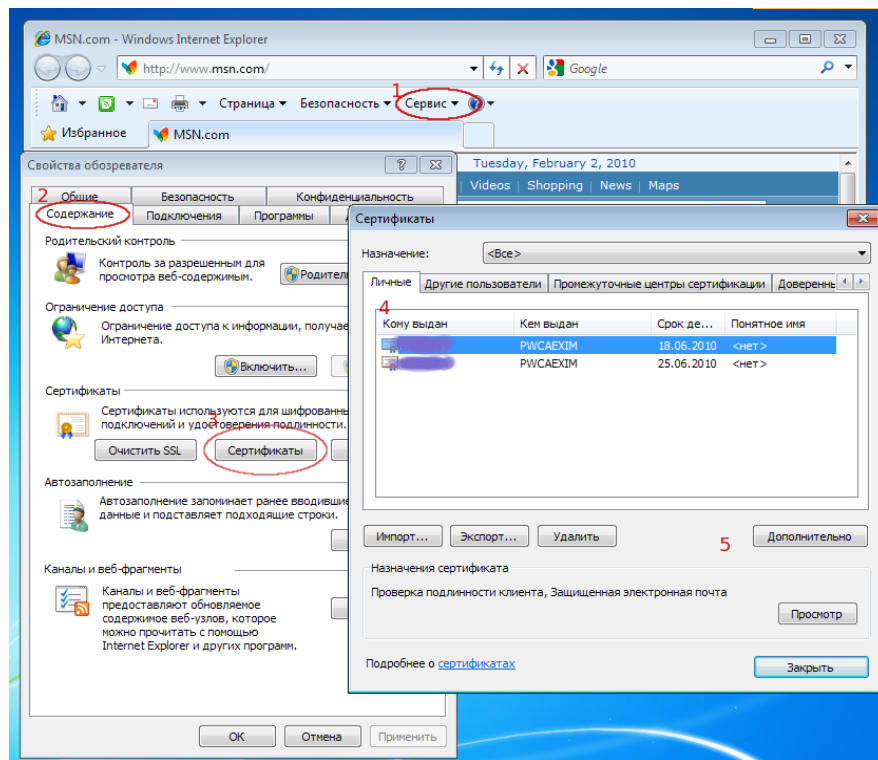


Далі необхідно вставити пристрій в USB роз'єм. З'явиться повідомлення про успішну установку драйвера:



Для здійснення перевірки сертифіката користувача в Internet Explorer необхідно виконати такі дії:

1. Вибрати меню «Сервис».
2. Вибрати меню «Содержание».
3. Натиснути на кнопку «Сертификаты».
4. Ви бачите один або декілька сертифікатів. Зверніть увагу на стовпчик «Срок действия». По закінченні терміну дії сертифіката Ви не зможете ним користуватися.
5. Натиснувши «Дополнительно» або «Просмотр», Ви зможете переглянути інформацію про сертифікат та його властивості.



2.4. Вхід до Інтернет-банкінгу з використанням захищеного носія ключа MiniKey

З MiniKey до Інтернет-банкінгу можна входити після успішної установки програми CryptoKit (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»:

Вхід

Користувач

Пароль

Одноразовий пароль

або використовувати цифровий сертифікат ☒

Важливо!

Пам'ятайте, для забезпечення безпеки Вам необхідно завершити сеанс роботи із Enter EXIM™ за допомогою команди «Вихід» та від'єднати пристрій із приватним ключем. Це не дозволить зловмисникам за Вашої відсутності скористатись Вашими повноваженнями.

Реєстрація

(для нових користувачів)

Оберіть

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.

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 CryptoKit встановлено правильно (п. 2.5 Інструкції), установка елементів ActiveX дозволена (п. 2.2 Інструкції), MiniKey вставлено в порт USB і індикатор світиться.

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

Вам буде запропоновано увести пін-код до MiniKey. Пін-код створюється Вами в Банку при форматуванні MiniKey. Пін-код не можна забувати і можна змінити самостійно (п. 3 Інструкції). Якщо Ви забули пін-код, необхідно прийти до Банку для форматування MiniKey, створення нового пін-коду і нового сертифіката.

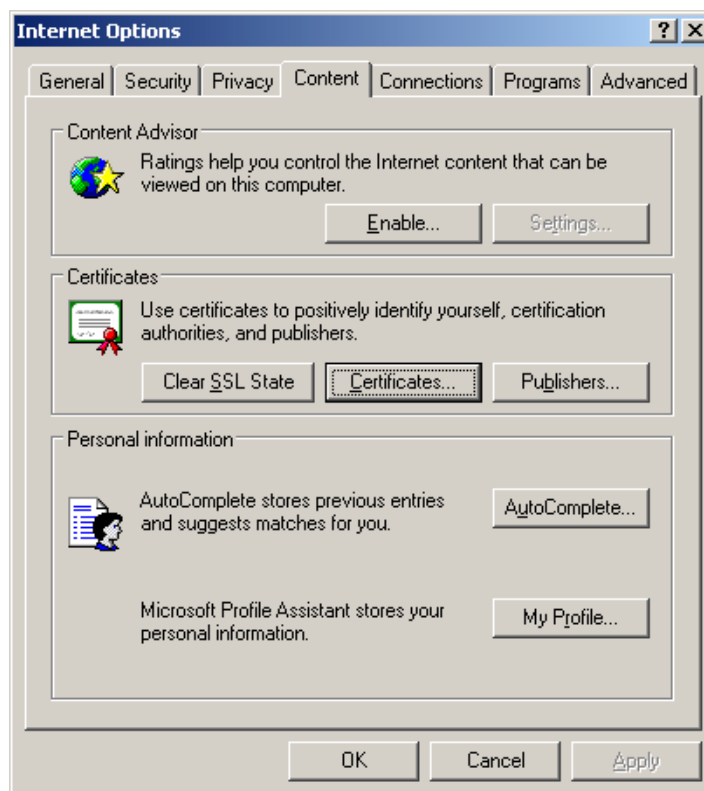
4. Після успішного входу в Інтернет-банкінг Ви можете працювати з платежами. У правому верхньому куті екрана буде стояти відмітка «Аутентифікація: Цифровий сертифікат».

2.5. Перевірка в браузері Internet Explorer наявності цифрового сертифіката і правильної роботи програми CryptoKit

Ви можете перевірити правильність установки програми CryptoKit 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 «Сервіс (Tools) » Свойства обозревателя (Internet Options) » Содержимое (Content) » кнопка «Сертификаты» (Certificates)»:



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

3. Під час перевірки програма CryptoKit повинна бути вже встановлена, MiniKey повинен бути підключений до порту USB і індикатор MiniKey повинен світитися.

4. Якщо імені сертифіката не видно, значить програма CryptoKit встановлена неправильно (і повинна бути переустановлена) або MiniKey не підключений до порту USB.

3. Зміна пін-коду до MiniKey

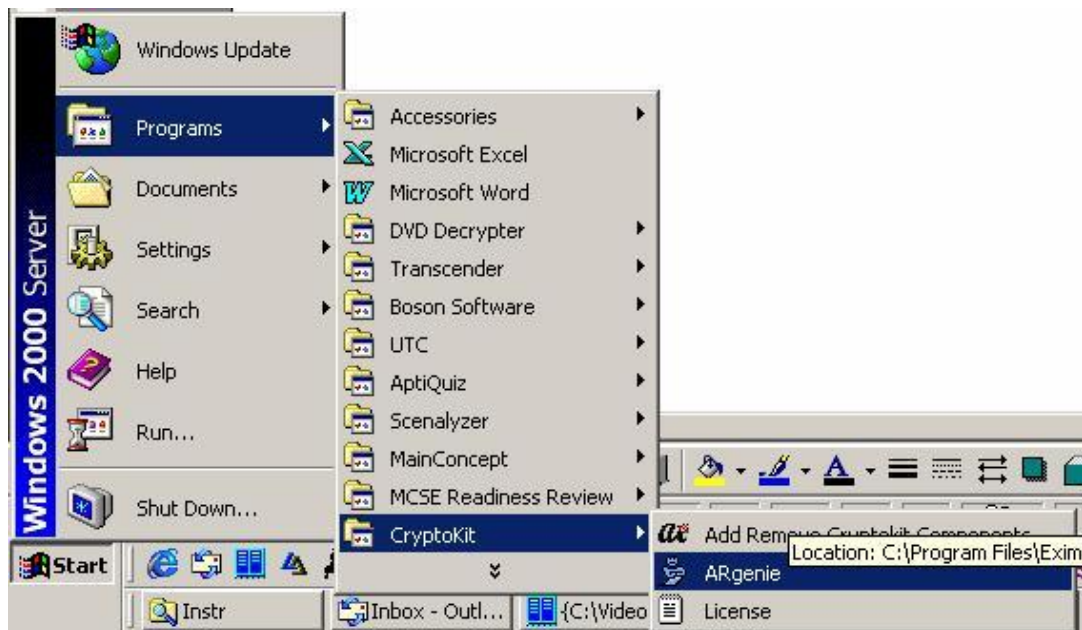
Створювати і підписувати платежі з MiniKey можна тільки після введення пін-коду. Пін-код створюється Вами в Банку при форматуванні MiniKey. В подальшому **пін-код можна змінювати самостійно (але не обов'язково)**. Для зміни пін-коду програма CryptoKit вже повинна бути успішно встановлена на Вашому комп'ютері (п. 2.1 Інструкції).

1. Підключіть MiniKey до порту USB. Індикатор повинен світитися зеленим і червоним кольорами.

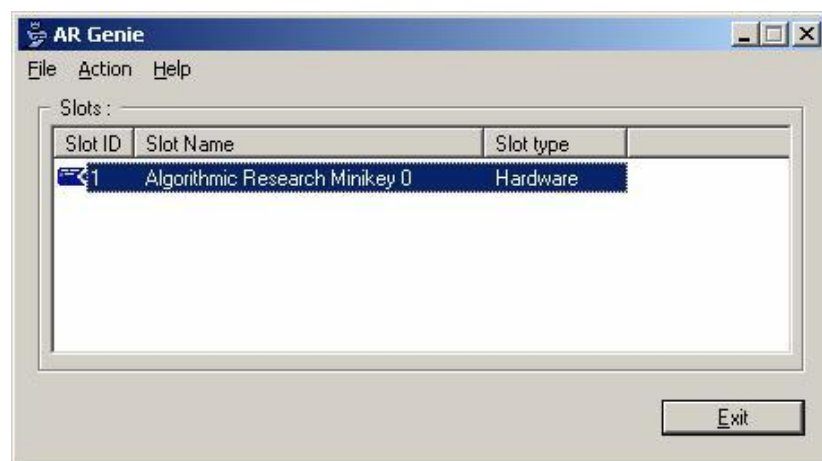
2. Про успішне виявлення MiniKey Вас повідомить вікно «Found New Hardware » Crypto USB Token».



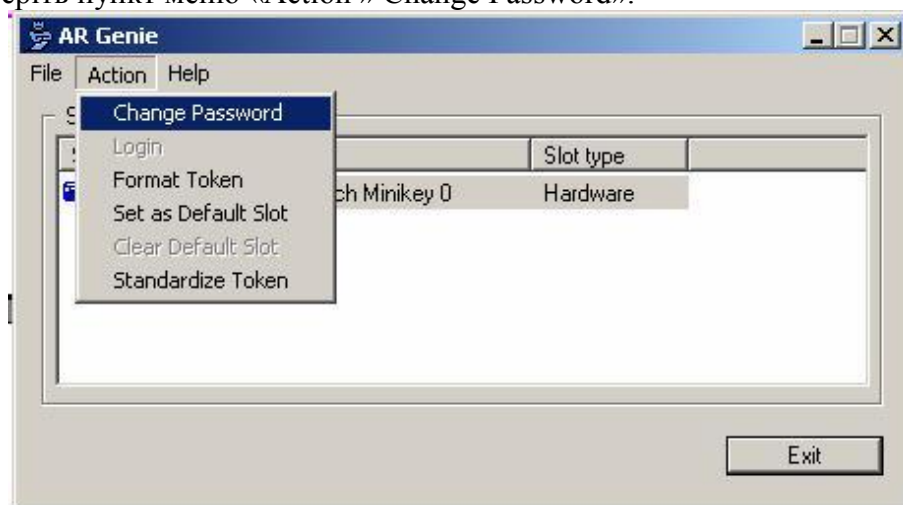
3. Натисніть в Windows кнопку «Пуск» і виберіть пункт меню «Пуск » Программы » CryptoKit » ARgenie».



4. Переконайтеся, що назва носія ключа (Algorithmic Research MiniKey) відображається у вікні програми.



5. Виберіть пункт меню «Action » Change Password».



6. У вікні «Log on to SmartCard» введіть існуючий пін-код, натисніть кнопку

7. У вікні «Change SmartCard PI» введіть існуючий пін-код, потім двічі новий

«Ok».



пін-код, натисніть кнопку «Ok».



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. Встановлено програму-драйвер CryptoKit (п. 2.1 Інструкції); 2. Дозволена установка елементів ActiveX (п. 2.2 Інструкції); 3. Виконано автоматичну установку елементів ActiveX (п. 2.2 Інструкції); 4. MiniKey зі створеним у Банку сертифікатом вставлено в комп'ютер USB і індикатор MiniKey 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. Встановлена програма-драйвер Cryptokit (п. 2.1 Інструкції); 2. MiniKey зі створеним у Банку сертифікатом вставлено в комп'ютер USB.
Після відмітки позначки «Використовувати цифровий сертифікат» на екрані з'являється повідомлення «Вибраний рівень автентифікації 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 CryptoKit і дозволені елементи ActiveX. Вставити MiniKey в порт USB можна тільки після установки драйвера.
Що таке захищений носій	MiniKey – це спеціальний невеликий пристрій, на

ключа (MiniKey)?	якому зберігаються таємний ключ і сертифікат клієнта. MiniKey виконує криптографічні перетворення з цим ключем для підпису платіжних доручень і забезпечує надійне зберігання таємного ключа без можливості його копіювання. MiniKey підключається до комп'ютера через порт USB. 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 MiniKey. 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. 