USER'S MANUAL

on generation of electronic digital signature keys using the "User's Account" of the Key Certification Center of JSC "PRAVEX BANK"

1. LIST OF ABBREVIATIONS

KCC administrator – authorized employee of JSC PRAVEX BANK
Bank – JSC "PRAVEX BANK"
EDS – electronic digital signature.
User's office – official resource of JSC "PRAVEX BANK" (https://ca.pravex.com.ua:444/).
PC – personal computer.
KCC – Key Certification Center of JSC "PRAVEX BANK".
USB-drive – flash drive.

2. USER'S ACCOUNT ASSIGNMENTS

The user's account of Key Certification Center (hereinafter referred to as the user's account) is the official resource of JSC "PRAVEX BANK" which provides:

- user registration;
- generation of user EDS keys;
- certification of public users EDS keys.

3. REGISTRATION IN THE USER'S ACCOUNT

1. In order to be able to generate a KCC EDS key, the Bank needs to register in the User's Account at https://ca.pravex.com.ua:444/ or on the Bank's official website in the section PRAVEXBANK BIZ \rightarrow *Generation of the Bank's KCC EDS key* (Fig. 1).

| 1 | Про Банк Про Банк Кар'єра в Банку Контактні та платіжні реквізити Family Banking Курси валют 🔇 Зворотній зв'язок |
|---------------------------------------|---|
| особам | |
| | Головна / PRAVEXBANK BIZ / Генерація ключа ЕЦП ЦСК Банку |
| Корпоративним клієнтам і банкам | Про систему Почати роботу Реєстрація нового клієнта Реєстрація нового ключа Генерація ключа ЕЦП ЦСК Банку |
| Платіжний портал | УВАГА! Шановні Клієнти! У зв'язку з встановленням оновлень змінився інтерфейс Кабінету користувача. Найближчим часом буде розміщена інструкція щодо реєстрації та генерації ключів ЕЦП за допомогою Кабінету користувача з урахуванням усіх змін сервісу. Приносимо вибачення за незручност! |
| | Робота в системі «PRAVEXBANK BIZ» можлива з використанням ключів ЕЦП, які було згенеровано ЦСК АТ «ПРАВЕКС БАНК» або в акредитованих центрах сертифікації ключів (АЦСК). |
| Відділення та | З метою генерації ключів ЦСК Банку необіхно використовувати сервіс «Кабінет користувача». |
| банкомати | Генерація ключа складається з двох кроків: |
| 8 | 1. Реєстрація в «Кабінеті користувача»; |
| ONLINE PRAVEX | 2. Генерація ключа ЕЦП. |
| i | Процедура реєстрації та генерації ключа ЕЦП ЦСК Банку описано в «Інструкції Клієнта по генерації ключів ЕЦП ЦСК Банку». |
| PRAVEXBANK BIZ | Реєстрація |
| Прес Центр | PDE |
| | Інструкція по генерації ключів ЕЦП ЦСК |
| Майно на продаж | Банку |

Fig. 1. Section "Generation of the Bank's KCC EDS key"

2. The standard view of the home page of the User's account is shown in Fig. 2.

| | Вхід користувача | |
|---------------------|-------------------------------|--------|
| Центр сертифікації | la'a: | |
| ключів | Пароль доступу: | |
| Кабінет користувача | | Увійти |
| | Відновлення паролю | |
| | Ресстрація нового користувача | |

Fig. 2. User's Account home page

3. For clients who are not registered in the User's account, you should go through the registration procedure by clicking the button Peccrpaus HOBORO KOPUCTYBANA .

4. Next, fill in the registration form with the user's details, selecting the user type "Legal entity". An example of filling in the registration form is given in Fig. 3.

| Реєстрація користуі | вача | |
|--|---|---|
| Для реєстрації користувача кабінету ЦС | (необхідно заповнити наступну форму заявкі | з інформацією про заявника (користувача) |
| | | |
| | Юридична особа | |
| Ім'я (Логін) * | Тестовий логін | |
| Адреса електронної пошти (e-mail) * | olga.dimpul@pravex.ua | |
| Пароль *: | | |
| Пароль (підтвердження) * | ••••• | |
| Прізвище *: | Тестове призвіще | |
| Ім'я та по батькові * | Тестове ім'я | |
| Місто (нас. пункт) * | Київ | |
| Область (регіон) * | | |
| | Для міст Київ або Севастополь поле 'Область | (регіон) не заповнюється |
| | | |
| Організація *: | Тестова компанія | |
| Підрозділ *: | Тестовий підрозділ | |
| Посада *: | Тестова посада | |
| | | |
| Адреса | | |
| Телефон : | | |
| Kon EURION * | 10245570 | |
| Kon /IPthO *** | 1234567900 | |
| | 1234367690 | |
| Код СПФМ | | |
| | | |
| | Я не робот послето и Каладината и Кала И Каладината и Каладина Каладината и Каладината и Каладина Каладината и Каладината и Каладината и Каладината и Каладин | |
| | | |
| | | Зарееструвати |
| • обое'язкові до заповнення поля ** - для фізичних осіб, які через свої рел ДРФО" вноситься серія та номер паспор | ігійні переконання відмовились від прийнятт ту. | з рестраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті у поле "Код |
| Примітка. Код підтвердження реєстр | ації буде відправлено на адресу електроні | итиопологи |

Fig. 3. User registration form in the User's account

Зареєструвати 5. Press the button

6. After that the message about the necessity to confirm the user registration by the link in the e-mail, which was specified during the registration (see Fig.4), will appear:

ПРАВЕКС БАНК КАБІНЕТ КОРИСТУВАЧА ЦСК

Реєстрація користувача

Реєстрацію завершено успішно. Для підтвердження реєстрації перейдіть за посиланням, що наведено у електронному листі.

Fig. 4. Message about the end of user registration

7. The following message will be sent to the e-mail address specified during registration (see Fig. 5):

| От: | 🗆 ca@pravex.ua |
|-------------------------------|--|
| Кому: | 🗷 Dimpul Olga Grygorivna |
| Копия: | |
| Тема: | EURegistration |
| На ваше | ім'я було зроблено запит на реєстрацію користувача Реєстраційні дані: |
| | |
| Тип кор | истувача: Юридична особа |
| Ім'я кор | истувача (логін): Тестовий логін |
| Користу | вач (Common name): Тестове призвіще Тестове ім\'я |
| Прізвиш | е: Тестове призвіще |
| Ім'я та п | о батькові: Тестове ім\'я |
| Місто (н | ас. пункт): Київ |
| Область | (регіон): |
| Адреса: | |
| Телефо | H: |
| Організа | ація: Тестова компанія |
| Підрозд | іл: Тестовий підрозділ |
| Посада: | Тестова посада |
| Адреса | електронної пошти: <u>olga.dimpul@pravex.ua</u> Ім'я (DNS чи інше): |
| Код ЕДР | INOY: 12345678 |
| Код ДРО | DO: 1234567890 |
| Ідентиф | ікатор НБУ: |
| Код СПФ | PM: |
| Для під <u>id=146&</u> | гвердження реєстрації необхідно перейти за посиланням: <u>https://ca.pravex.com.ua:444/registration-accept?</u> ac=2f9157160671ab2d47db892ac520d2e7ac7e4b5da645a944925f48c955c70d88103aff58479653c90533db18d309723b |
| I | Fig. E. Example of registration E mail confirmation |

Fig. 5. Example of registration E-mail confirmation

8. To confirm the registration, click on the link, and then the page with confirmation of registration and activation of the record will be automatically opened (see Fig. 6).

ПРАВЕКС БАНК КАБІНЕТ КОРИСТУВАЧА ЦСК

Реєстрація користувача

Вашу реєстрацію підтверджено, обліковий запис активовано.

Вхід до Кабінету користувача ЦСК

Fig. 6. Registration confirmation page in the User's account

9. Next you should press the button Bxia do KaGihery KopucryBava LCK, after that the user will be taken to the home page of the User's account, where it is necessary to login to the User's account under the username and password specified during registration (see Fig. 7).

| 🛅 ПРАВЕКС БАНК | | |
|---------------------|---------------------------------|--------|
| | Вхід користувача | |
| Центр сертифікації | ім'я (Логін): Тестовий догін | |
| ключів | Пароль доступу: | |
| Кабінет користувача | ••••• | Увійти |
| | Відновлення паролю | |
| | Реєстрація нового користувача | |

Fig. 7. Home page of the User's account

4. PERSONAL KEY GENERATION

1. The standard page of the User's account is shown on. Fig. 8.

| I IPABEKC DAHK | КАБІНЕТ КОРИС | ТУВАЧА ЦСК | Профі | ль Вихід з кабінету |
|---|---|---------------------------------------|---|---------------------|
| Про кабінет Завантажити Ге | енерація ключів Заявка на сертифікат | и Перегляд заявок Арх | <u>в заявок</u> | |
| Про кабінет корист | гувача центру серти | фікації ключів | | |
| Центр сертифікації ключів (ЦСК) забезпечує власний відокремлений пункт реєстрації ЦС | с обслуговування сертифікатів відкритих ключіє СК. | а користувачів розробників та інших к | ористувачів. Надає розробникам можливіс | ть створювати |
| Центр сертифікації ключів забезпечує: | | | | |
| обслуговування сертифікатів кори | стувачів, що включає: | | | |
| реєстрацію користувачів; | | | | |
| сертифікацію відкритих ключ | ів користувачів; | | | |
| розповсюдження сертифіка | ітів через інформаційний ресурс - web-сайт | та LDAP-каталог, а також за прото | околом СМР; | |
| управління статусом сертиф | рікатів та розповсюдження інформації про | статус сертифікатів через списки | зідкликаних сертифікатів на інформаці | йному ресурсі та за |
| hive normal user (the number of normality | | | | |
| фіксування часу (формування поз- | Harok racy). | | | |
| У засобах ЦСК реалізуються наступні н | криптографічні алгоритми та протоколи: | | | |
| шифрування за ДСТУ ГОСТ 28147 | 2009, TDEA ta AES 3a ISO/IEC 18033-3; | | | |
| ЕЦП за ДСТУ 4145-2002 та RSA з | a ISO/IEC 14888-2:2008 i PKCS#1; | | | |
| гешування за ГОСТ 34.311-95 та S | SHA 3a ISO/IEC 10118-3:2004; | | | |
| протокол розподілу ключових дан | их за ДСТУ ISO/IEC 15946-3 та вимог до фо | рматів криптографічних повідомл | энь. | |
| Засоби ЦСК підтримують наступні фор | мати даних та операційні протоколи взаєм | одії: | | |
| сертифікати та списки відкликани | х сертифікатів (CBC) згідно ISO/IEC 9594-8 | га державних вимог до надійних | засобів ЕЦП; | |
| особисті ключі згідно РКСЅ#8 та F | PKCS#12; | | | |
| протокол OCSP (визначення стату) | усу сертифіката) згідно RFC 2560 та та держ | авних вимог до надійних засобів В | ЕЦП; | |
| протокол TSP (фіксування часу) зг | rідно RFC 3161 та державних вимог до наді | йних засобів ЕЦП; | | |
| протокол СМР (управління сертиф | рікатами); | | | |
| протокол LDAP (доступ до LDAP-к | аталогу); | | | |
| підписані дані (дані з ЕЦП) згідно | ETSI TS 101 733 (CAdES), RFC 5652 та дер: | жавних вимог до надійних засобів | EUN; | |
| and the second second second second second | | | | |

Fig. 8. User's account

2. To generate an EDS key, select the corresponding section <u>Генерація ключів</u> (Fig. 9).

3. Key generation consists of two steps:

- personal key generation
- generation of a certificate request.

| ПРАВЕКС БАНК КАБІНЕТ КОРИСТУВАЧА ЦСК |
|--|
| <u>Про кабінет Завантажити Генерація ключів Заявка на сертифікати Перегляд заявок Архів заяво</u> |
| Крок 1 - Крок 2 Генерація особистого ключа <u>Формування запиту на створення сертификату</u> |
| Ключ ЕЦП буде автоматично записано в папку «Завантаження» на Вашому робочому ПК. Скопіюйте його на флеш-носій. Для генерації особистого ключа введіть пароль до нього за допомогою форми, що наведено нижче, та натисніть «Далі». |
| Генерувати ключі: |
| Пароль захисту особистого ключа: |
| Пароль захисту особистого ключа (підтвердження): |
| Далі |
| Fig. 9. "Key Generation" section |

4. The first step is to specify the **PASSWORD** for the personal key and confirm it.

Attention! When setting the password, the layout on the PC keyboard must be taken into account.

5. After clicking the button Далі automatic generation of the EDS key ("Key-6.dat" file) will be performed, which should be saved on the PC by selecting the following on the button ook (see Fig. 10). The default EDS key is saved in the *Downloads* folder on drive C:
 Открытие «Key-6.dat»
 Вы собираетесь открыть:
 Кеу-6.dat
 выприлицийся: dat File (946 байт)

| bbi coonpactices of tipbi | |
|-----------------------------|--|
| Key-6.dat | |
| являющийся: dat из blob: | : File (946 байт) |
| Как Firefox следует об | работать этот файл? |
| О О <u>т</u> крыть в | О <u>б</u> зор |
| Coxpанить фай | រែរ |
| В <u>ы</u> полнять авт | оматически для всех файлов данного типа. |
| | ОК Отмена |

Fig. 10. Save EDS key window

Attention! For further use of the EDS key in operation, copy it in the "Downloads" folder to the USB-drive.

| | 🔤 ПРАВЕКС БАНК 🛛 КА | БІНЕТ КОРИСТУВАЧА ЦСК | | Reciption Berlig a molivery |
|--------------|---|---|-------------------------------------|-----------------------------|
| | Roo kabiver Zasavravurtu Pavepau | n monula Zanasa na cepruplikatu Paparing kanaci Apula kanaci | | |
| | ПОДАННЯ ЗАЯВКИ НА СЕ Поданий заявки на формувания сертифікатів | ртифікати 20 цох | | |
| | Заявка на формування сертифікатів Для формування сертифікатів необхідно запо | енити наступну форму залаки з інформацією про заланима (користувана) та прикріпити файли із запитани | na dopujšamin cesnučkati | |
| | Saranuwa wasaa *: 'Te Agpeos enerstownol noume (e-mail) *: 'Dig Nyfonikyeank coprindpikat : | troe novalug Terroe inn s∂mpul@prevecue | | |
| | Rptinneue +: [Te w/in ta no 64544000 +: [Te Micro (nos. nyear) +: [An Otheran, (penton) +: [| toe norshun noes livin B | | |
| | Arr Agrece : Tenedow : | with fulls also Celescronomi none "Clearche (periow)" we sanoewoothick | | |
| | Oprenitaujie : [Te Pilopotojin : [Te Rocaya : [Te Mrte (DN 8 va insue) : | tosa koutakit Tosa hocuja | | |
| | Кад ЕДРПОУ - [12] Кад ДРФО: [12] (дентрийских ККУ - | 45573 | | |
| | 264, 6799 2649 - 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | INCOMPLANA ACCELEDA CONTENTARIA ACCELEDA ENTRE ALANA ACCELEDA INTERNA ACCE | | |
| | | | | Ngan Natagaras |
| | - odderhadel jo sandereten honn **- gin disevers oot, se vepes cool peninte | Fig. 11. Page "Ap | plication for certificates" | |
| 7. It is nec | cessary to check t | the data in the fields and | d click Подати ог Пове | рнутись, if the data is |
| incorrect. P | | КАБІНЕТ КОРИСТУВАЧ | а цск | Профіль Вихід з кабінету |
| | Про кабінет Завантажити | Генерація ключів Заявка на сертифікати Пери | егляд заявок Архів заявок | |
| | Подані заявки на | а формування сертифікатів | | |
| | Список заявок на формування се | ртифікатів, що сформовані користувачем та вже оброблен | і ЦСК чи знаходяться на обробці | Всього записів: 1 |
| | ПН Сформовано * * | Заявник (загальне ім'я) | Статус обробки Банком * * Оброблено | Перегляд/Друк |
| | | | | |

Fig. 12. "Display requests" section

8. Requests can be in several statuses:

• "Not processed" is under consideration of the KCC administrator;

- "*Rejected*" rejected by KCC administrator;
- "Processed" personal key certified by KCC administrator.

9. To certify the user's personal key, it is necessary to print out the "*Request to add JSC "PRAVEX BANK" keys*. To do this, next to the request with the "*Not processed*" status press the button +, then in the form "Request for certificate generation" (see Fig. 13) press the button Apyryesting and Repeated as East.

| Заявка на форму | вання сертифікатів |
|-----------------------------------|--|
| Інформація про стан обробки заявк | ки на формування сертифікатів та інформація про користувача, який її сформував |
| Інформація про заявку | |
| Сформована: | 27.08.2018 11:19 |
| | Друкувати для передачи в Банк |
| Статус: | Не оброблений |
| Інформація про користувача | |
| Загальна назва (ім'я): | Тестове призвіще Тестове ім'я |
| Прізвище: | Тестове призвіще |
| Ім'я та по батькові: | Тестове ім'я |
| Місто (нас. пункт): | Київ |
| Область (регіон): | |
| Організація: | Тестова компанія |
| Підрозділ: | Тестовий підрозділ |
| Посада: | Тестова посада |
| Адреса: | |
| Телефон: | |
| Адреса електронної пошти: | olga.dimpul@pravex.ua |
| Публікувати сертифікат: | M |
| Ken IBAO | 1234567890 |

10. Printed "Request to add JSC "PRAVEX BANK" keys" (in two copies) must be signed and stamped by the Client's authorized representative (see Fig. 14). *After that the original Requests should be handed over to the service department*.

ПРАВЕКС БАНК

Запит на додавання ключів АТ «ПРАВЕКС БАНК»

Замовлення на сертифікацію відкритої частини ключів ЕЦП (Протоколу розподілу ключів)

Произу сертяфікувати адприту частику ключа ВЦП (Протокалу рошоділу ключіа), першетри жого клаждної мижно Електроної платіжні документи, піцтисної за допомогою смеретної частини доного ключа, нажити дійствик.

| Номер запиту | 62 | |
|---|---|---|
| Дата отворения запиту | 27.08.2018 11:19 | |
| Загальна назва (ім'я): DIS максанта ЕШД | Tecrone monsume Tecrone info | |
| Населений пункт | Kais | |
| Область | | |
| Організація | Tecross sources is | |
| Підроздія | Тестовані підроздія | |
| Посада | Тастова посада | |
| Адрееа електронної пошти | olga.dimpul@praver.ua | |
| Криптографічні алгоритми | ДСТУ 4145-2002 та Даффі-Гелыан в гр. точки ЕК | |
| Відкритий ключ | 27 5C 04 11 A0 2F CF AC E0 2E 17 F5 19 B9 2A 85 C0 19 6C 28 F8 76 A6 D0 15 82 09 73 86 15 5A 20 00 | |
| Відкритий ключ проговопу розподілу | 41 00 90 D0 19 9F 78 33 99 51 CC E6 06 3F 31 FD 2F 8D F4 F7 A4 32 52 56 85 BE B9 97 79 73 91 40 FC 89 EC A4 19 B4 B5 51 84 E5 D2 EE 61 EE F3 B1 85 D0 20 61 1D 47 | |
| | | |
| | | |
| Ідентифікаційний кор | | |
| Ідеятифікаційний код Документ, що посвідчує особу | Cepix Hasep: | |
| Ідеятифікаційсякі код Документ, що посвідчує особу | Cepir Hoxep: Дога кадраі: | |
| Ідеятифікаційскі вад Документ, що посвідчує особу | Серіг Некер: Дега кадичі: Кок корзекіž | |
| Центифікаційний вод Довузанит, що посвідчує особу | Серія Нокер: Дага кадран: Кон каррынž | |
| Ідектаўізаційний кол Документ. що паскідчує особу Немер договору/дод угоди на обслугозувани в спотеля «URAVEXEANX: BEZ» | Серіг Немерл Дега кадачі: Кал каракиž | |
| Ідектаўізанійскі кол Документ. що паскідчує особу Немер договору'дод угодн на обслугозувани в спотока об'я AVEXEANK BIZO | Серіг Немер Дега кадачі: Ког карыкиž д | ; |
| Ідектаўляння кол Документ, пао посвідчує особу Немер договору/дод угодя на обслугозуваля в састемі «DRAVEXEANK BIZ» Особлагнай підпат, класкака БШП | Серіг Некер: Дега кадряці: Кон кадряцій га | |
| Ілектаўізаційний кол Далумент, що поскілчус особу Немер дагозору/дод угодн на обслугозуван в системі «URAVEXEANK BIZO Особластий підпяс власкака БЦП Достокурність прозеденна лённа пільернаму | Серіг Немерх Дега задачі: Кок задачі: в | |
| Ілектаўізаційний кол Долумент, що паскілчус особу Немер дагозору/дод угода на обслуговувана в система «ЛРА-VEXEAUX, БЕД» Особластий підпяс класкака БШП Достокірність призеленна люжа підпяеражу | Серіг Немерл Дега кадачі: Кыл кадамій а | |
| Ідектаўізаційний кол Далумент, що паскілчус особу Немер догозору/дод угодя на обслугозуванн в спотоль «ДРАЛИНХЕМИХ, ВІД» Особластий підпис: класкака БІДП Достокірність призеленна, підпершжу | Осріг Некерл Дега кодичі: Каг кодичиž п п | |
| Ідектаўізаційний кол Документ. що паскідчує особу Немер договору/дод угодя на обслуговувани в система «ОРАЛУЕХЕАНХ, ВЕД» Особластий підпас: класнака ЕЦП Достокірність призеленна пілизерску Коріанах: підпрачалета | Серіг Незер: Дега задачі: Как заракиž п | ; |
| Ілектаўіяллійскі кол Далумент, що паскілчус особу Немер дагозару/дод угодн на обслугозуваля в сястчая об'яліченням ВЕДО Особластий підпяс класснака БЕДП Достокірність призедення линно, пільзерныу Керіанах підпракаютва | Серіг Немерх Дета задачі: Т.ск. задачі: в в | ; |
| Ілектаўізаційскі кол Долумент, що паскілуу особу Немер догозору/дод угодн та обслугозуваля в системі «DRAVEXEANK BIZ» Особлитий підпях влескака ЕЦП Достокірність призелення піннэерску Корільнах підпрамяства Уполновалена особа балах | Серіг: Немерх Дега кадачі: Каг кадачій: а | |
| Ілектаўізаційний кол Далушент, що паскілчус особу Немер дагозору/дод угода на обслуговувана в система «ЛЕ-АУЧЕХЕРАУК БЕД» Особластий підпас класкама БШП Достокірність призеленна паная пілизеражу Карільнах підпрахнаства Уполазданена особа балку Дага прайоку малягу | Серіг Немерл Дега кадачі: Кат кадачій: а | |

Fig. 14. Example of request to add JSC "PRAVEX BANK" keys

11. After the KCC administration certifies the personal key, the status of the request will change to "Processed".

Заявка на формування сертифікатів

| Інформація про стан обробки заявки на формування сертифікатів та інформація про користувача, який ї сформував | |
|--|-----------------------|
| Інформація про заявку | |
| Сформована: | 10.07.2018 18:19 |
| | Друкувати |
| Статуе: | Оброблений |
| Час обробки: | 2018-07-10 18:55:04 |
| Сформовані сертифікати | |
| Сертифінат ЕЦЛ: | Зарантахити Друкурати |
| Сертифікат протоколу розподілу: | Завантакити Друдувати |
| Інформація про користувача | |
| Загальна назва (ім'я): | Тест4 Тест4 |
| Прізвище: | Тест4 |
| Ім'я та по батькові: | Тест4 |
| Місто (нас. пункт): | Київ |
| Область (регіон): | |
| Організація: | Фізична особа |
| Підрозділ: | Фізична особа |
| Посада: | Фізична особа |
| Адреса: | |
| Телефон: | |
| Адреса електронної пошти: | olga.dimpul@pravex.ua |
| Публікувати сертифікат: | 凶 |
| Код ДРФО: | 6644332211 |
| | |

Рис.15. Downloading a personal key certificate

RESULT:

- 1. Generated personal key (Key-6.dat file)
- 2. Downloaded personal key certificate

Personal key and certificate can be used to pre-register a new client or a new key in the PRAVEXBANK BIZ system!

Technical support is available at (044) 521-02-70 or at IKB-help@pravex.ua (9:00 – 18:00 on weekdays).