ПРАВЛІННЯ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

ПОСТАНОВА

11.07.2012 **м. Київ** **N 290**

Зареєстровано в Міністерстві юстиції України
17 вересня 2012 р. за N 1594/21906

Про затвердження Правил електронної взаємодії між респондентами та Національним банком України

Відповідно до статті 7 Закону України "Про Національний банк України", з метою підвищення рівня захисту інформації та встановлення єдиних правил обміну захищеними даними між Національним банком України та його респондентами Правління Національного банку України

ПОСТАНОВЛЯЄ:

1. Затвердити Правила електронної взаємодії між респондентами та Національним банком України, що додаються.

2. Контроль за виконанням цієї постанови покласти на заступника Голови Національного банку України Прохоренка В. П.

3. Ця постанова набирає чинності з дня її офіційного опублікування.

Голова **С. Г. Арбузов**

ПОГОДЖЕНО:

Голова Державної служби спеціального зв'язку та захисту інформації України **Г. А. Резніков**

ЗАТВЕРДЖЕНО
Постанова Правління Національного
банку України
11.07.2012 N 290

Зареєстровано
в Міністерстві юстиції України
17 вересня 2012 р. за N 1594/21906

Правила електронної взаємодії між респондентами та Національним банком України

I. Загальні положення

1.1. Ці Правила регламентують обмін захищеними електронними документами між респондентами та Національним банком України (далі - Національний банк) через мережу Інтернет та розроблені згідно із Законами України "Про Національний банк України", "Про банки і банківську діяльність", "Про електронний цифровий підпис" та "Про електронні документи та електронний документообіг".

1.2. У цих Правилах терміни вживаються в такому значенні:

електронна печатка - електронний цифровий підпис (далі - ЕЦП), який за правовим статусом прирівнюється до печатки з урахуванням вимог статті 3 Закону України "Про електронний цифровий підпис";

захищений електронний документ - електронний документ, зашифрований за допомогою засобу криптографічного захисту інформації (далі - КЗІ), що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації;

портал електронної взаємодії Національного банку (далі - портал Національного банку) - програмно-технічний засіб, розроблений з урахуванням цих Правил для обміну захищеними електронними документами між респондентами та Національним банком за допомогою електронної пошти (e-mail);

респондент Національного банку (далі - респондент) - особа - відправник захищеного електронного документа до Національного банку;

статус сертифіката - стан посиленого сертифіката ключа (чинний, блокований, скасований) на конкретний момент.

У цих Правилах інші терміни вживаються в значеннях, визначених у Законах України "Про електронний цифровий підпис", "Про електронні документи та електронний документообіг", Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу, затвердженому постановою Кабінету Міністрів України від 26.05.2004 N 680, Порядку акредитації центру сертифікації ключів, затвердженому постановою Кабінету Міністрів України від 13.07.2004 N 903.

II. Загальні вимоги до обміну даними

2.1. Національний банк визначає адресу електронної скриньки (e-mail) порталу Національного банку, телефони технічної підтримки та поширює цю інформацію через сторінки Офіційного інтернет-представництва Національного банку України (www.bank.gov.ua) у розділі "Портал електронної взаємодії".

2.2. Цикл обміну захищеними електронними документами (далі - файл обміну) складається з файла, який відправляється ініціатором обміну адресату (далі - файл повідомлення), повідомлення про доставку та двох квитанцій, які свідчать про результат отримання файла повідомлення.

Повідомлення про доставку свідчить про дату та час отримання файла повідомлення адресатом.

Перша квитанція (далі - квитанція N 1) свідчить про результат перевірки проходження автоматичного вхідного контролю файла повідомлення.

Друга квитанція (далі - квитанція N 2) свідчить про результат оброблення інформації з файла повідомлення.

2.3. Респонденту для обміну даними з Національним банком необхідно мати:

доступ до мережі Інтернет та можливість відправлення та приймання файлів обміну у форматі транспортного повідомлення (далі - ТП) згідно з розділом V цих Правил;

програмне забезпечення, призначене для створення і оброблення файлів обміну респондентом згідно з розділом III цих Правил;

засіб КЗІ, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

III. Формат файла обміну

3.1. Усі файли обміну мають формуватися як XML-документи відповідно до відкритого стандарту W3C (http://www.w3.org/TR/REC-xml) та кодуються у форматі "Windows 1251".

3.2. Для контролю за цілісністю структури та правильністю заповнення XML-документа використовується файл (далі - XML-схема), що відповідає стандарту W3C "XML Schema" (http://www.w3.org/2001/XMLSchema-instance) та має розширення XSD (XML Schema definition).

Кодування реквізитів у XML-схемі визначається шаблоном відображення кожного типу файла повідомлення. Усі шаблони надаються Національним банком у форматі Adobe Portable Document Format (PDF) і мають аналогічне до XML-схеми ім'я файла з розширенням PDF.

Порядок елементів у XML-документі повинен точно відповідати порядку, описаному XML-схемою.

3.3. Опис форматів файлів обміну наведено в додатку 1 до цих Правил.

Детальний опис та зміст файлів обміну, XML-схеми та шаблони відображення встановлюються Національним банком та поширюються через сторінки Офіційного інтернет-представництва Національного банку України в розділі "Портал електронної взаємодії".

IV. Вимоги до криптографічного захисту інформації

4.1. Створення файла обміну завершується накладанням електронного цифрового підпису з використанням надійного засобу електронного цифрового підпису (далі - ЕЦП).

4.2. Для перевірки ЕЦП використовується посилений сертифікат відкритого ключа (далі - сертифікат ключа), сформований акредитованим центром сертифікації ключів.

Статус сертифіката ключа перевіряється на момент, визначений позначкою часу, яка накладається на електронний документ, а у разі відсутності позначки часу - на момент отримання електронного документа.

4.3. Усі криптографічні перетворення виконуються засобами криптографічного захисту інформації, які повинні відповідати таким вимогам:

реалізовувати процедури формування й перевірки ЕЦП відповідно до національного стандарту України ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка", затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28.12.2002 N 31;

реалізовувати процедури відкритого розподілу ключів відповідно до національного стандарту України ДСТУ ISO IEC 15946-3:2006 "Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих", затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 03.10.2006 N 294;

реалізовувати процедури симетричного шифрування відповідно до міждержавного стандарту ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования", затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22.12.2008 N 495;

реалізовувати процедуру накладання позначки часу згідно з національним стандартом України ДСТУ ISO/IEC 18014-1:2006 "Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 1. Основні положення" (ISO/IEC 18014-1:2002, IDT), затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 27.12.2006 N 375;

мати сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Функції бібліотек криптографічних перетворень для сумісності з порталом Національного банку повинні відповідати специфікаціям криптографічних функцій, зазначеним у додатку 2 до цих Правил.

V. Формат ТП

5.1. ТП відповідає формату електронної пошти (MIME) згідно з міжнародним стандартом RFC-1521. Заголовки ТП кодуються у форматі "Windows 1251".

ТП складається з реквізитів ТП та транспортного контейнера (далі - ТК).

ТК входить у ТП як файл укладення.

ТК складається із заголовка та блока зашифрованих даних (реквізитів шифрування даних та зашифрованих даних).

Зашифровані дані містять зашифрований XML-файл з накладеними ЕЦП, а також набір додаткових даних, необхідних для перевірки ЕЦП та визнання його дійсності.

Перед зашифровуванням дані упаковуються архіватором ZIP, який у кореневому каталозі містить один підписаний XML-файл. Ім'я файла архіву збігається з ім'ям XML-файла.

Ім'я файла ТК збігається з ім'ям XML-файла та зазначається в полі "FILENAME" заголовка.

5.2. ТП може мати тільки одного одержувача.

Одне ТП повинно містити тільки один укладений у нього ТК. У разі прийняття ТП до оброблення ТК з тим самим ім'ям не може бути переданий вдруге.

Опис ТП наведено в додатку 3 до цих Правил.

VI. Найменування файлів обміну

6.1. Найменування файла обміну складається з назви файла та його розширення. Загальна довжина імені файла не може перевищувати 128 символів.

6.2. Назва файла обміну має таку структуру:

<код задачі (3 символи)><код підзадачі (5 символів)><унікальний ідентифікатор респондента><ggmmddNNN>, де:

код задачі, код підзадачі, унікальний ідентифікатор респондента визначає Національний банк;

ggmmdd - дата формування файла повідомлень (gg - дві останні цифри року та mmdd - місяць, день у 10-знаковій системі числення);

NNN - порядковий номер файла повідомлення протягом дня (3 символи).

Коди задачі і підзадачі доповнюються до потрібної довжини символом "0".

Назва файла повідомлення про доставку та назва файлів квитанції збігаються з назвою файла повідомлення, що квитується.

6.3. Розширення для відповідного файла обміну має значення:

XML - для файла повідомлення;

RPL - для повідомлення про доставку;

RP1 - для квитанції N 1;

RP2 - для квитанції N 2.

VII. Порядок подання файла повідомлення засобами телекомунікаційного зв'язку

7.1. Файл обміну на початку приймання перевіряється на допустиму назву і розширення (XML, RPL, RP1, RP2) файла та на коректність заповнення заголовка ТК. Якщо файл обміну не проходить перевірку, то він відхиляється, а на файл повідомлення адресат жодної відповіді не відсилає.

7.2. Файл обміну розшифровується, розпаковується з архіву, на нього накладається позначка часу адресатом, статус сертифіката ключа якого на момент накладання позначки часу має бути чинним, після чого він подається на зберігання до архіву. Структуру файла, який зберігається в архіві, зазначено в пункті 2.2 глави 2 додатка 3 до цих Правил. На файл повідомлення у відповідь адресат відсилає повідомлення про доставку.

7.3. Служба автоматичного вхідного контролю перевіряє ЕЦП електронного документа, у тому числі шляхом перевірки чинності відповідних посилених сертифікатів відкритих ключів, та відповідність електронного документа XML-схемі. На файл повідомлення адресат відсилає відправнику файла повідомлення квитанцію N 1.

7.4. Функціональна підсистема Національного банку відповідної задачі перевіряє зміст електронного документа. За результатами перевірки відправнику файла повідомлення формується квитанція N 2.

7.5. На файл повідомлення респондента до Національного банку накладається ЕЦП двох відповідальних осіб та електронна печатка респондента. Файл шифрується з використанням відкритого ключа порталу Національного банку.

На повідомлення про доставку та квитанції від Національного банку накладається ЕЦП порталу Національного банку. Файл шифрується з використанням відкритого ключа електронної печатки респондента.

Відкритий ключ електронної печатки респондента надається у сертифікаті ключа відповідного файла повідомлень, надісланого до Національного банку.

7.6. На файл повідомлення від Національного банку накладається ЕЦП відповідальної особи та порталу Національного банку. Файл шифрується з використанням відкритого ключа електронної печатки респондента.

На повідомлення про доставку та квитанції від респондента накладається електронна печатка респондента. Файл шифрується з використанням відкритого ключа порталу Національного банку.

Сертифікат ключа порталу Національного банку поширюється Національним банком через сторінки Офіційного інтернет-представництва Національного банку в розділі "Портал електронної взаємодії".

7.7. Національний банк надає повідомлення про доставку та квитанції респонденту на електронну поштову адресу, з якої надійшов файл повідомлення.

7.8. Дані приймаються до оброблення, якщо квитанції не містять кодів помилок. Дату та час надання файла повідомлення засвідчує отримане респондентом повідомлення про доставку, якщо всі квитанції на відповідний файл повідомлення не містять помилок.

7.9. Файли обміну зберігаються Національним банком та респондентом у розшифрованому вигляді з накладеними на них ЕЦП протягом п'яти років.

Заступник начальника
Управління захисту інформації **С. П. Гавриш**

Додаток 1
до Правил електронної взаємодії між респондентами та Національним банком України

1. Загальний опис формата файлів обміну

Структура файлів є уніфікованою та складається із елементів "DECLARHEAD" та "DECLARBODY".

Кореневим елементом є елемент з іменем "DECLAR", у якому зазначається посилання на схему контролю даних (XML-схему). У елементі "DECLARHEAD" розміщується інформація, що ідентифікує респондента, який надає звіт Національному банку. Зміст елемента "DECLARBODY" визначається окремими вимогами щодо надання інформації респондентами Національному банку.

Загальний вигляд схеми XML-файла:

<xs:element name="DECLAR" type="DeclarContent"/>

<xs:complexType name="DeclarContent">

<xs:sequence>

<xs:element name="DECLARHEAD" type="DHead"/>

<xs:element name="DECLARBODY" type="DBody"/>

</xs:sequence>

</xs:complexType>

2. Загальний опис файла повідомлення

2.1. Елемент "DECLARHEAD" містить ідентичний для всіх файлів повідомлень набір елементів. Опис елемента "DECLARHEAD" надано в таблиці 1:

Таблиця 1

Назва елемента	Зміст
1	2
FNAME	ім'я файла повідомлення

EDRPOU	код за ЄДРПОУ [реєстраційний номер облікової картки платника податків або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган державної податкової служби і мають відмітку у паспорті)];
IDBANK	ідентифікатор банку або фінансової установи
MFO	код банку
CDTASK	код задачі
CDSUB	код підзадачі
CDFORM	код шаблону документа
FILL_DATE	дата формування файла у форматі "ДД.ММ.РРРР", де ДД - день, ММ - місяць, РРРР - рік надання файла повідомлення
FILL_TIME	час формування файла у форматі "ЧЧХХ", де ЧЧ-час та ХХ-хвилини формування файла

2.2. XML-схема файла повідомлення, яка повинна включатися до всіх схем опису:

```
<?xml version = "1.0"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="DECLAR" type="DeclarContent"/>

<xs:simpleType name="DGDate">

  <xs:restriction base="xs:string">

    <xs:length value="10" />

     <xs:pattern value=" ((((0[1-9] | [1-2][0-9])\.(0(1 | [3-9]) | 1[0-2])) | (30\.(0(1 | [3-9]) | 1 [0-2])) | (31\.(01 | 03 | 05 | 07 | 08 | 10 | 12)))\.(19 | 20)\d{2}) | ((0 [1-9] | [1-2][0-9])\.02\.(19|20)(([0 | 2 | 4 | 6 | 8][0 | 4 | 8]) | ([1 | 3 | 5 | 7 | 9][2 | 6])) | (0[1-9] | [1-2][0-8] | 19)\.02\.(19 | 20) (([0|2|4|6|8][1-3|5-7|9]) | ([1|3|5|7|9][0-1 | 3-5 | 7-9])))"/>

  </xs:restriction>

</xs:simpleType>

<xs:simpleType name="DGTime" >

  <xs:restriction base="xs:string">

    <xs:length value="4"/>

      <xs:pattern value=" ((([0-1][0-9])|(2[0-3]))[0-5][0-9])"/>

  </xs:restriction>
```

```
</xs:simpleType>

<!--Загальний тип "код за ЄДРПОУ [реєстраційний номер облікової картки платника податків або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган державної податкової служби і мають відмітку у паспорті)]"-->

<xs:simpleType name="DGLong">

  <xs:restriction base="xs:string">

    <xs:maxLength value="10"/>

    <xs:pattern value="([0-9]{5,10}|[АБВГДЕЄЖЗИ_КЛМНОПРСТУФХЦЧШЩЮЯ]{2}[0-9]{6})"/>

  </xs:restriction>

</xs:simpleType>

<xs:complexType name="DeclarContent">

<xs:sequence>

    <xs:element name="HEAD" type="DHEAD" minOccurs="1" maxOccurs="1"/>

</xs:sequence>

</xs:complexType>

<xs:complexType name="DHEAD">

  <xs:sequence>

    <xs:element name="FNAME" minOccurs="1" maxOccurs="1"/>

      <xs:simpleType>

        <xs:restriction base="xs:string">

          <xs:length value="23"/>

        </xs:restriction>

      </xs:simpleType>

    </xs:element>

    <xs:element name="EDRPOU" type="DGLong" minOccurs="1" maxOccurs="1"/>

    <xs:element name="IDBANK" minOccurs="1" maxOccurs="1" nillable="true">

      <xs:simpleType>
```

```
    <xs:restriction base="xs:string">
     <xs:length value="3"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="MFO" type="xs:integer" minOccurs="1" maxOccurs="1" nillable="true"/>
<!-- Код задачі -->
<xs:element name="CDTASK" minOccurs="1" maxOccurs="1">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:length value="3"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<!-- Код під задачі -->
<xs:element name="CDSUB" minOccurs="1" maxOccurs="1" nillable="true">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:maxLength value="5"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<!-- Код шаблону документа -->
<xs:element name="CDFORM" minOccurs="1" maxOccurs="1">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:length value="8"/>
```

```
      </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element name="FILL_DATE" type="DGDate" minOccurs="1" maxOccurs="1"/>
      <xs:element name="FILL_TIME" type="DGTime" minOccurs="1" maxOccurs="1"/>
      <xs:element name="EI" nillable="true">
       <xs:simpleType>
        <xs:restriction base="xs:string">
         <xs:maxLength value="2"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
  </xs:schema>
```

3. Загальний опис повідомлення про доставку квитанцій N 1 та N 2:

3.1. XML структура повідомлення про доставку квитанцій N 1 та N 2:

```
<?xml version="1.0" encoding="windows-1251"?>
<DECLAR xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<DECLARHEAD>
 <FNAME>
Ім'я файла квитанції
 </FNAME>
<DOCFNAME>
Ім'я файла повідомлення, на який створено квитанцію
</DOCFNAME>
<RESULT>
Результат приймання файла повідомлення:
```

1 - успішно;

2 - виявлено помилки (документ не прийнятий);

3 - документ прийнятий із зауваженнями.

</RESULT>

<KVTDATE>

Дата створення квитанції у форматі "DD.MM.YYYY"

</KVTDATE>

<KVTTIME>

Час створення квитанції у форматі "HHMM"

</KVTTIME>

<KVTNUM>

Номер квитанції:

1 - повідомлення про доставку файла повідомлення;

2 - квитанція N 1;

3 - квитанція N 2.

</KVTNUM>

<DOCHEAD>

Дублюється зміст елемента "DECLARHEAD" прийнятого файла повідомлення

</DOCHEAD>

<TEXT>

Містить текст квитанції

</TEXT>

</DECLARHEAD>

<DECLARBODY>

Зміст елемента визначається розробником функціональної підсистеми відповідної задачі

</DECLARBODY>

</DECLAR>

3.2. XML схема повідомлення про доставку квитанцій N 1 та N 2, яка повинна включатись до всіх схем опису:

```
<?xml version="1.0"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="DECLAR">

 <xs:complexType>

 <xs:sequence>

  <xs:element name="DECLARHEAD">

   <xs:complexType>

    <xs:sequence>

     <xs:element name="FNAME" minOccurs="1" maxOccurs="1">

      <xs:simpleType>

       <xs:restriction base="xs:string">

        <xs:length value="23"/>

       </xs:restriction>

      </xs:simpleType>

    </xs:element>

    <xs:element name="DOCFNAME" type="xs:string"/>

    <xs:element name="RESULT" type="xs:integer"/>

    <xs:element name="KVTDATE" type="xs:string"/>

    <xs:element name="KVTTIME" type="xs:string"/>

    <xs:element name="KVTNUM" type="xs:integer"/>

    <xs:element name="DOCHEAD" type="xs:string"/>

    <xs:element name="TEXT" type="xs:string"/>

   </xs:sequence>

  </xs:complexType>

    </xs:element>

    <xs:element name="DECLARBODY" type="xs:string" nillable="true"/>
```

```
    </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Додаток 2
до Правил електронної взаємодії між респондентами та Національним банком України

Специфікація криптографічних функцій

1. Загальні вимоги

Загальні вимоги до бібліотеки криптографічних функцій:

робота в середовищі Microsoft Windows 98/2000/XP/Vista/7, Linux (RadHat, Suse);

багатопоточність;

бібліотека повинна поставлятися для апаратних платформ x86 та x64;

передача параметрів за угодою "__stdcall" згідно з описом функцій бібліотеки (пункт 3 додатка 3);

пам'ять під блоки з результатом роботи функцій надається прикладною програмою, яка використовує бібліотеку.

2. Вимоги до використання бібліотеки

Бібліотека надається у вигляді "dll" для "Windows"-середовищ та "so" для "Linux"-середовищ. Ім'я "dll" та "so": Crypt_XXX.dll та Crypt_XXX.so, де XXX - ім'я постачальника бібліотеки.

Доступ до функцій "dll" та "so" виконується функцією "GetProcAddress".

Бібліотека постачається разом із заголовними файлами з розширенням (*.h), що містять вичерпний опис функцій бібліотеки.

3. Функції бібліотеки

3.1. Функція накладання підпису:

а) без передачі сертифіката ключа:

int __stdcall MakeSign (const void* pkbuf, int pklen, const char* pwd, const void* docbuf, int doclen, void* outbuf, int* outlen), де:

Параметр	Опис
1	2
const void* pkbuf	буфер із секретним ключем
int pklen	розмір буфера із секретним ключем
const char* pwd	пароль секретного ключа, повинен закінчуватися символом "\0"
const void* docbuf	буфер із документом
int doclen	розмір буфера з документом
Void* outbuf	вихідний буфер, якщо "NULL" - в "outlen" повертається розмір вихідного буфера
int* outlen	розмір вихідного буфера

Функція зберігає в "outbuf" блок документа з підписом.

Функція повертає символ "\0", коли успішно виконано, або код помилки;

б) з передачею сертифіката ключа:

int __stdcall MakeSignC (const void* certbuf, int certlen, const void* pkbuf, int pklen, const char* pwd, const void* docbuf, int doclen, void* outbuf, int* outlen), де:

Параметр	Опис
const void* certbuf	буфер із сертифікатом ключа
int certlen	розмір буфера із сертифікатом ключа
const void* pkbuf	буфер із секретним ключем
int pklen	розмір буфера із секретним ключем
const char* pwd	пароль секретного ключа, повинен закінчуватися символом "\0"
const void* docbuf	буфер із документом
int doclen	розмір буфера з документом
Void* outbuf	вихідний буфер, якщо "NULL" - в "outlen" повертається розмір вихідного буфера
int* outlen	розмір вихідного буфера

Функція зберігає в "outbuf" блок документа з підписом.

Функція повертає символ "\0", коли успішно виконано, або код помилки.

3.2. Функція перевірки підпису:

int __stdcall VerifySign (const void* docbuf, int doclen, void* outbuf, int* outlen, void* certuf, int* certlen), де:

Параметр	Опис
const void* docbuf	буфер з документом
int doclen	розмір буфера з документом
Void* outbuf	вихідний буфер, якщо "NULL" - в "outlen" повертається розмір вихідного буфера
int* outlen	розмір вихідного буфера
Void* certbuf	буфер з сертифікатом ключа, якщо "NULL" - в "certlen" повертається розмір буфера з сертифікатом ключа
int* certlen	розмір буфера з сертифікатом ключа

Функція зберігає в "outbuf" блок документа без підпису.

Функція зберігає в "certbuf" блок сертифіката ключа підписувача.

Функція повертає символ "\0", якщо підпис вірний, або код помилки.

3.3. Функція перевірки сертифіката ключа:

int __stdcall VerifyCert (const void* certbuf, int certlen, const void* rootcbuf, int rootclen), де:

Параметр	Опис
const void* certbuf	буфер із сертифікатом ключа
int certlen	розмір буфера із сертифікатом ключа
const void* rootcbuf	буфер з сертифікатом ключа Акредитованого центра сертифікації ключів (далі - АЦСК) для перевірки сертифіката ключа, яким підписано електронний документ
int rootclen	розмір буфера сертифіката ключа АЦСК

Функція повертає символ "\0", якщо перевірка успішна, або код помилки.

3.4. Функція шифрування блоку даних:

int __stdcall Encrypt (const void* certbuf, int certlen, const void* pkbuf, int pklen, const char* pwd, const void* docbuf, int doclen, void* outbuf, int* outlen), де:

Параметр	Опис
const void* certbuf	буфер із сертифікатом ключа

int certlen	розмір буфера із сертифікатом ключа
const void* pkbuf	буфер із секретним ключем
int pklen	довжина буфера із секретним ключем
const char* pwd	пароль секретного ключа повинен закінчуватися символом "\0"
const void* docbuf	буфер із документом
int doclen	розмір буфера з документом
void* outbuf	вихідний буфер, якщо "NULL" - в "outlen" повертається розмір вихідного буфера
int* outlen	розмір вихідного буфера

Функція зберігає в "outbuf" зашифрований блок документа.

Функція повертає символ "\0", коли успішно зашифровано, або код помилки.

3.5. Функція розшифрування блоку даних:

int __stdcall Decrypt (const void* pkbuf, int pklen, const char* pwd, const void* certbuf, int certlen, const void* docbuf, int doclen, void* outbuf, int* outlen), де:

Параметр	Опис
1	2
const void* pkbuf	буфер із секретним ключем
int pklen	довжина буфера із секретним ключем
const char* pwd	пароль секретного ключа повинен закінчуватись символом "\0"
const void* certbuf	буфер із сертифікатом ключа
int certlen	розмір буфера із сертифікатом ключа
const void* docbuf	буфер із документом
int doclen	розмір буфера з документом
void* outbuf	вихідний буфер, якщо "NULL" - в "outlen" повертається розмір вихідного буфера
Int* outlen	розмір вихідного буфера

Функція зберігає в "outbuf " розшифрований блок документа.

Функція повертає символ "\0", коли успішно виконано, або код помилки.

3.6. Функція звірки сертифіката ключа із секретним ключем:

int __stdcall VerifyCertPKMatch (const void* certbuf, int certlen, const void* pkbuf, int pklen, const char* pwd), де:

Параметр	Опис
const void* certbuf	буфер із сертифікатом ключа
int certlen	розмір буфера із сертифікатом ключа
const void* pkbuf	буфер із секретним ключем
int pklen	розмір буфера із секретним ключем
const char* pwd	пароль секретного ключа повинен закінчуватися символом "\0"

Функція повертає символ "\0", коли сертифікат та секретний ключ є відповідними, або код помилки.

3.7. Функція отримання інформації із сертифіката ключа:

int __stdcall GetCertInfo (const void* certbuf, int certlen, UACertInfo* info), де:

Параметр	Опис
const void* certbuf	буфер із сертифікатом ключа
int certlen	довжина буфера із сертифікатом ключа
UACertInfo* info	структура з інформацією із сертифіката ключа (приведена нижче)

Функція повертає символ "\0", коли успішно виконано, або код помилки.

Структура "UACertInfo":

Поле	Опис
1	2
char Serial[64]	серійний номер сертифіката ключа
char EDRPOU[11]	код за ЄДРПОУ установи
char DRFO[11]	реєстраційний номер облікової картки платника податків або серія та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний орган державної податкової служби і мають відмітку у паспорті)
char Name[64]	прізвище, ім'я, по батькові особи або найменування установи
char Email[64]	електронна адреса
char Title[64]	посада

char PostalCode[7]	поштовий індекс
char Obl[64]	область
char Rayon[64]	район
char Adres[64]	адреса
char Tel[64]	телефон
time_t DtBeg	дата початку дії сертифіката ключа (4 байта)
time_t DtEnd	дата закінчення дії сертифіката ключа (4 байта)
char Issuer[64]	видавець (найменування)

Вирівнювання членів структури - 1 байт.

Розмір кожного строкового поля містить заключний символ "\0".

4. Коди помилок

0 - успішно;

1 - буфер порожній;

2 - DLL не ініціалізовано;

3 - помилка отримання інформації з сертифіката ключа;

4 - даний сертифікат ключа не може використовуватися для виконання операції;

5 - не збігається пара "сертифікат ключа - секретний ключ";

7 - некоректний формат секретного ключа;

8 - помилка підпису/шифрування, можливо вказано невірний пароль;

11- невірний підпис;

12 - внутрішня помилка перевірки підпису;

13 - помилка перевірки цілісності (пошкоджений буфер);

14 - функція не підтримується.

Додаток 3
до Правил електронної взаємодії між респондентами та Національним банком України

Опис транспортного повідомлення

Схему уніфікованого транспортного повідомлення (далі - ТП) представлено на рисунку 1:

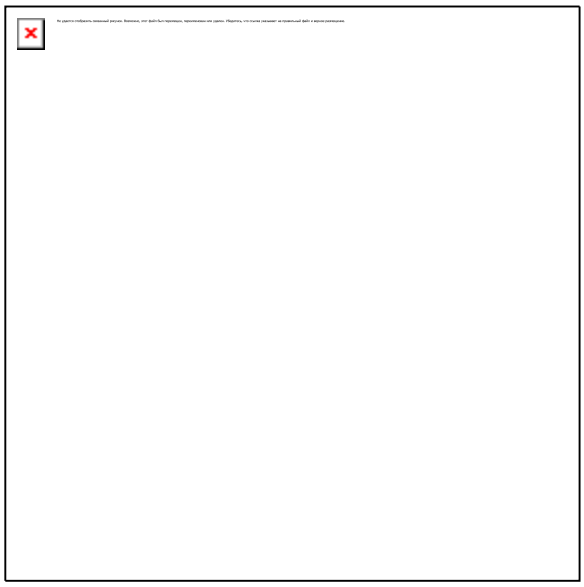

Рисунок 1. Схема уніфікованого ТП.

1. Опис ТК

1.1. Заголовок ТК.

Заголовок ТК містить інформацію про відправника та використовувану ним бібліотеку криптозахисту:

Елемент	Значення
Сигнатура	"TRANSPORTABLE"
0-символ	службовий символ
4-байтовий розмір заголовка контейнера	без урахування довжини сигнатури і "\0"-символа
CR/LF	символи повернення каретки (0D) і переводу рядка (0A)
Рядки <CR/LF>	послідовність вигляду <Тег>=<Значення>

Кожне значення тега заголовка ТК надається в кодуванні "Windows1251" та закінчується символом CHR(13) та CHR(10).

Перелік тегів заголовка ТК:

Найменування	Значення	Обов'язковість заповнення
FILENAME	ім'я файла контейнера у верхньому регістрі	так

EDRPOU	код респондента	так
PRG_TYPE	назва програмного забезпечення для накладання та перевірки ЕЦП відправника довжиною не більше десяти символів	так
PRG_VER	версія програмного забезпечення для накладання та перевірки ЕЦП відправника довжиною не більше десяти символів	ні
SUBJECT	найменування документа звітності	ні
RESULT	результат приймання повідомлення (0 успішно, 1 - помилка, 2 - попередження)	ні
KVTNUM	номер квитанції (1, 2, 3…)	ні
FINKVT	ознака фінальної квитанції (0/1)	ні

Теги заголовка ТК "PRG_VER", "SUBJECT", "RESULT", "KVTNUM", "FINKVT" надані для сумісності заголовка ТК портала Національного банку з порталами надання звітності інших державних установ.

1.2. Блок зашифрованих даних.

Формат блока зашифрованих даних:

Елемент	Значення
Сигнатура	"XXX_ CRYPT", де XXX - код Центру сертифікації ключів*
0-символ	службовий символ
4 байти	розмір зашифрованих даних
Зашифровані дані	

* Код Центру сертифікації ключів - послідовність із трьох прописних літер латинського алфавіту, яка однозначно ідентифікує Центр сертифікації ключів.

1.2.1. ЕЦП.

Формат підпису:

Елемент	Значення
Сигнатура	"XXX_SIGN", де XXX - код Центру сертифікації ключів

0-символ	Службовий символ
4 байти	розмір буфера підпису та підписаних даних
Буфер підпису та підписаних даних	

ЕЦП формуються послідовно, накладаючись один на одний.

Послідовність накладення ЕЦП секції "XXX_SIGN" для респондента:

а) накладання ЕЦП першої відповідальної особи;

б) накладання ЕЦП другої відповідальної особи;

в) накладання електронної печатки респондента.

Послідовність накладення ЕЦП для Національного банку:

а) накладання ЕЦП відповідальної особи;

б) накладання ЕЦП порталу Національного банку.

Розташування сертифікатів у блоці ЕЦП визначається постачальником криптографічної бібліотеки.

1.2.2. Позначка часу.

Позначка часу отримується з Акредитованого центру сертифікації ключів за протоколом TSP (Timestamp Protocol RFC 3161).

Формат позначки часу:

Елемент	Значення
Сигнатура	"XXX_STAMP", де XXX - код Центру сертифікації ключів
0-символ	службовий символ
4 байти	розмір хешу оригінального документа
хеш оригінального документа	
4 байти	розмір буфера позначки часу
Буфер позначки часу	
4 байти	розмір даних, на які накладено позначку часу
Блок даних, на які накладено позначку часу	

2. Формати повідомлень, які надсилаються в ТК

2.1. Формат повідомлення "Документ".

Повідомлення передається від респондента до порталу Національного банку.

Структура повідомлення:

заголовок ТК документа;

блок даних, зашифрований на одержувача, містить підписи респондента і документ у форматі XML.

2.2. Структура повідомлення "Документ з позначкою часу":

позначка часу на момент отримання документа від респондента;

підписи респондента;

документ у форматі XML.

2.3. Формат повідомлення "Документ від Національного банку".

Повідомлення передається від порталу Національного банку до респондента.

Структура повідомлення:

транспортний заголовок документа;

позначка часу;

підпис порталу Національного банку;

блок даних, зашифрований на респондента, який містить підписаний XML-файл Національного банку.

_____