ЗАТВЕРДЖЕНО
наказ ДПА України
від 12.07.10 № 499

Уніфікований формат транспортного повідомлення при інформаційній взаємодії платників податків і податкових органів в електронному вигляді телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису

Зміст

Уніфікований формат транспортного повідомлення для обміну інформацією між платниками податків і податковими органами в електронному вигляді з використанням електронного цифрового підпису (далі – Уніфікований формат транспортного повідомлення) застосовується для організації обміну електронними документами між платниками податків і податковими органами безпосередньо і телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису (далі – ЕЦП). Обмін електронними документами здійснюється за допомогою **транспортного повідомлення** (далі – ТП), складається з **реквізитів ТП** та **транспортного контейнера**, що містить зашифровані дані (електронні звіти, квитанції тощо).

Квитанції про приймання електронних документів, створені податковими органами, є електронними документами і передаються платнику податків в уніфікованому форматі транспортного повідомлення, який регламентовано у цьому документі.

1. Шляхи обміну інформацією

Обмін інформацією між платниками податків і податковими органами в електронному вигляді може проводитися двома шляхами:

- електронний документ передається безпосередньо до податкового органу на електронному носії інформації (дискета, флеш-накопичувач тощо);
- електронний документ передається до податкового органу телекомунікаційними каналами зв'язку.

2. Вимоги до криптографічного захисту інформації

Усі криптографічні перетворення виконуються засобами систем криптографічного захисту інформації (СКЗІ), які повинні відповідати таким вимогам:

реалізовувати процедури формування й перевірки ЕЦП відповідно до національного стандарту ДСТУ 4145-2002;

реалізовувати процедури відкритого розподілу ключів відповідно до національного стандарту ДСТУ ISO IEC 15946-3:2006;

реалізовувати процедури симетричного шифрування відповідно до регіонального ГОСТ 28147-89;

бути сертифікованими відповідно до законодавства України.

Функції бібліотек криптографічних перетворень, що надаються центрами сертифікації ключів для інтеграції у систему приймання та обробки податкової звітності, повинні відповідати специфікаціям криптографічних перетворень, викладених у додатку 3.

3. Уніфікований формат транспортного повідомлення

Уніфікований формат транспортного повідомлення підтримує всі діючі типи електронних документів інформаційної взаємодії, обумовлених порядком подання податкової звітності відповідно до чинного законодавства України та інших нормативних актів Державної податкової адміністрації України.

Схему уніфікованого транспортного повідомлення представлено на рис.1.

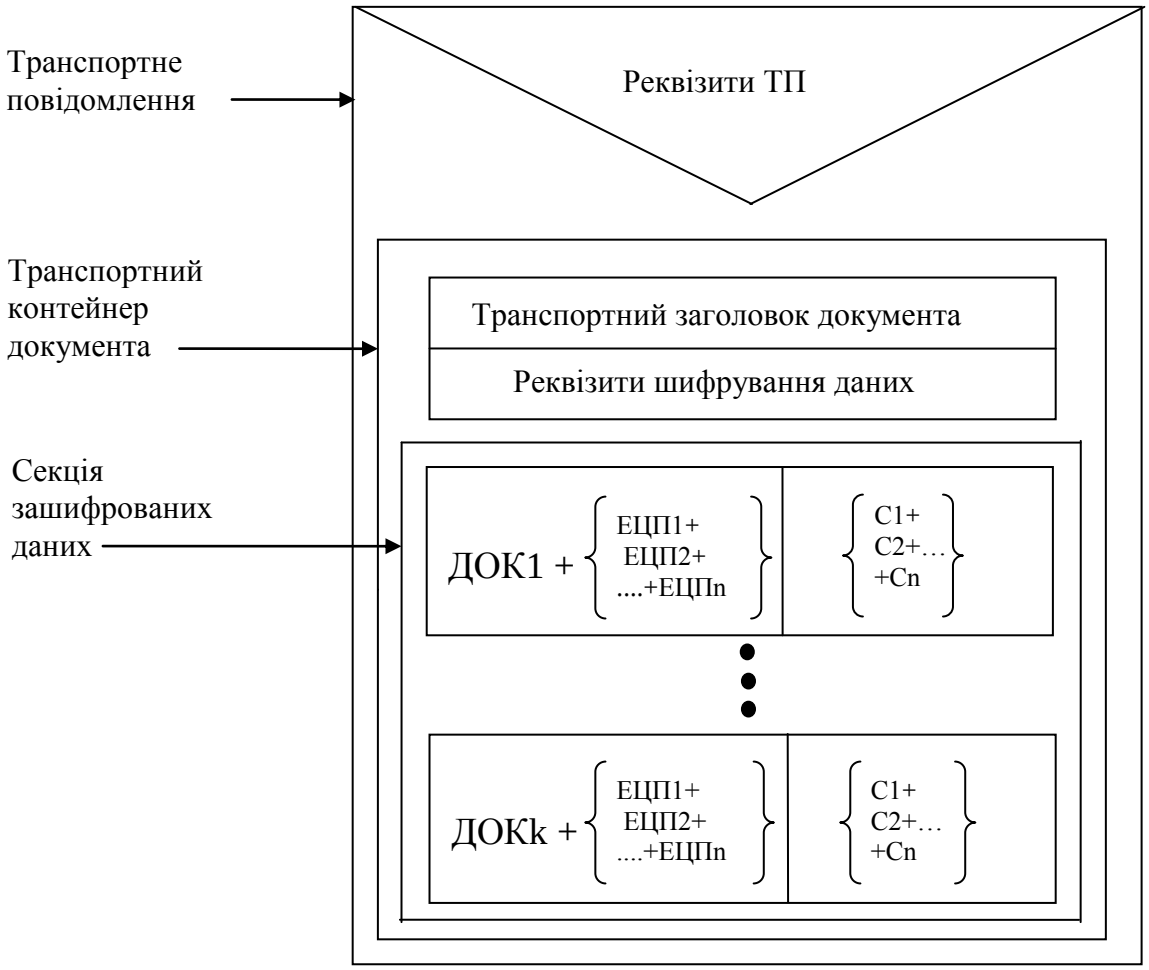

рис. 1

ДОК1, 2, …k – файл електронного документа;
ЕЦП1, 2, …n – один чи декілька електронно-цифрових підписів, якими засвідчений документ;
С1, 2, …n – один чи декілька блоків з сертифікатами ключів ЕЦП, якими засвідчений документ.

4. Вимоги до структури транспортного повідомлення, що передається телекомунікаційними каналами зв'язку

Транспортне повідомлення являє собою файл у форматі електронної пошти (MIME), оформлений за стандартом RFC-1521.

Файл, який вміщує транспортний контейнер, входить у транспортне повідомлення як файл-вкладення (**“Content-Disposition: attachment”**). Ім'я файла-вкладення зазначено в полі **“filename”.** Розмір файла транспортного контейнера не може бути нульовим.

Транспортне повідомлення може мати тільки одного одержувача.

Одне транспортне повідомлення повинно містити тільки один вкладений у нього транспортний контейнер. Розмір транспортного повідомлення не повинен перевищувати 10 Мбайт.

Ідентифікаційний код платника податків за ЄДРПОУ або індивідуальний податковий номер фізичної особи (далі – ЄДРПОУ).

Заголовок транспортного повідомлення повинен містити такі обов'язкові поля:

“From:” – поле, що містить ім'я відправника у кодуванні «Quoted Printable/Windows 1251» або «Base64/Windows 1251» й електронну адресу відправника, поміщену у кутові дужки <>;

“Reply-To:” – поле, що містить ім'я відправника в кодуванні «Quoted Printable/Windows 1251» або «Base64/Windows 1251» й електронну адресу відправника, поміщену у кутові дужки <>;

“To:” – поле, що містить ім'я одержувача в кодуванні «Quoted Printable/Windows 1251» або «Base64/Windows 1251» й електронну адресу одержувача, поміщену у кутові дужки <>;

“Message-ID:” – поле, що містить унікальний, у межах організації відправника, ідентифікатор повідомлення довільного формату з довжиною, що не перевищує 40 символів;

“Content-Transfer-Encoding:” – поле, що містить механізм кодування тіла повідомлення. Припустимі значення: «Quoted Printable/Windows 1251», «Base64».

Приєднаному файлу вкладення повинні відповідати поля:

“Content-Type:”, що містить ключове слово ”application/octet-stream” і параметр ”name=". Параметр ”name" повинен містити ім'я файла вкладення. Ім'я файла повинно кодуватися в Quoted Printable/Windows 1251 або Base64/Windows 1251.

“Content-Disposition:”, що містить ключове слово “attachment” і параметр “filename”. Ім'я файла повинно кодуватися в Quoted Printable/Windows 1251 або Base64/Windows 1251.

“Content-Length:”, що містить довжину вкладення.

“Subject:” – зміст поля представлений у кодуванні «Quoted Printable/Windows 1251» або «Base64/Windows 1251», визначається типом документа та ім'ям приєднаного транспортного контейнера.

Приклад транспортного повідомлення, що містить документ податкової звітності (розрахунку), наведено у додатку 1.

Приклад файла документа податкової звітності наведено у додатку 2.

5. Вимоги до структури транспортного контейнера для передачі документів до податкового органу

5.1. Узагальнений формат транспортного контейнера для передачі документів до податкового органу

Заголовок транспортного контейнера
Реквізити шифрування даних
Зашифровані дані

5.2. Перелік блоків даних транспортного контейнера для передачі документів до податкового органу

Зашифрований блок даних

Формат зашифрованого блоку даних:

Елемент	Значення
Сигнатура	" XXX_ CRYPT", де XXX – код Центру сертифікації електронних ключів: “A”, “B”, “C”, … – символьний ідентифікатор, привласнений АЦСК*
0-символ	
4 байти	розмір зашифрованого документа
Зашифрований документ	

* Символьний ідентифікатор, привласнений АЦСК, називається за порядком літер латинського алфавіту відповідно до черговості проходження акредитації в Україні. Тобто, першому акредитованому **ЦСК** в Україні буде привласнено символ «**A**», другому за часом акредитації - символ «**B**», третьому - «**C**», далі за латинським алфавітом.

Підпис

Формат підпису:

Елемент	Значення
Сигнатура	"XXX_SIGN", де XXX – код Центру сертифікації електронних ключів: “A”, “B”, “C”, … – символьний ідентифікатор, привласнений АЦСК*
0-символ	
4 байти	розмір буфера підпису та підписаних даних
Буфер підпису та підписаних даних	

* Символьний ідентифікатор, привласнений АЦСК, називається за порядком літер латинського алфавіту відповідно до черговості проходження ними акредитації в Україні. Тобто, першому акредитованому **ЦСК** в Україні буде привласнено символ «**A**», другому за часом акредитації - символ «**B**», третьому - «**C**», далі за латинським алфавітом.

Позначка часу

Позначка часу отримується з АЦСК за протоколом TSP (Timestamp Protocol).

Формат позначки часу:

Елемент	Значення
Сигнатура	"XXX_STAMP", де XXX – код Центру сертифікації електронних ключів: “A”, “B”, “C”, … – символьний ідентифікатор, привласнений АЦСК*
0-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	

* Символьний ідентифікатор, привласнений АЦСК, називається за порядком літер латинського алфавіту відповідно до черговості проходження акредитації в Україні. Тобто, першому акредитованому **ЦСК** в Україні буде привласнено символ «**A**», другому за часом акредитації - символ «**B**», третьому - «**C**», далі за латинським алфавітом.

Заголовок транспортного контейнера

Транспортний заголовок документа містить інформацію про передаваний документ.

Формат транспортного заголовка документа:

Елемент	Значення
Сигнатура	"TRANSPORTABLE"
0-символ	
4-байтовий розмір транспортного заголовка	без врахування довжини сигнатури і 0-символа
CR/LF	символи повернення каретки (0D) і переводу рядка (0A)
Рядок 1<CR/LF>	послідовність вигляду <Тег>=<Значення>
Рядок 2<CR/LF>	
…	
Рядок n<CR/LF>	

Теги, використовувані в транспортному заголовку документа:

Найменування	Значення	Обов'язковість заповнення
FILENAME	Ім'я файла у верхньому регістрі, що відправляє (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Так
SND_NAME	Найменування/ПІБ платника податків, що подає звіт (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Ні
SND_EMAIL	E-Mail відправника (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Ні
RCV_NAME	Найменування одержувача (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Ні
RCV_EMAIL	E-Mail одержувача (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Так
PRG_TYPE	Назва програмного забезпечення для накладання та перевірки ЕЦП відправника довжиною не більше десяти символів (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Так
PRG_VER	Версія програмного забезпечення для накладання та перевірки ЕЦП відправника довжиною не більше десяти символів (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Ні
SND_DATE	Дата і час відправки в форматі YYYYMMDDHHNNSS без розподільників та закінчується символом CHR(13) + CHR(10)	Так
CERTYPE	Символьний ідентифікатор, привласнений АЦСК (XXX) та закінчується символом CHR(13) + CHR(10)	Так
CRC32_SIGN	Контрольна сума згідно з алгоритмом CRC32 зашифрованого блоку даних та закінчується символом CHR(13) + CHR(10)	Так
CRC32_FILE	Контрольна сума згідно з алгоритмом CRC32 підписаного блоку даних та закінчується символом CHR(13) + CHR(10)	Так
SUBJECT	тип документа податкової звітності (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Так
GET_STAMP	Ознака необхідності передачі у відповідь позначки часу	Ні
RESULT	Результат прийому повідомлення (0 - успішно, 1 - помилка, 2 - попередження)	Ні

5.3. Формати повідомлень, які надсилаються в транспортному контейнері для передачі документів до податкового органу

Формат повідомлення „Документ"
Повідомлення передається від платника податків до податкового органу.
Структура:
1. Підпис відправника.
2. Транспортний заголовок документа.
3. Блок даних, зашифрований на одержувача, містить підписи платника податків і блок з документом у форматі XML.

Увага! Підписи платника повинні накладатися у такому порядку:
1. Підписана секція (XXX_SIGN) – підписана ключем головного бухгалтера (за умови наявності посади на підприємстві).
2. Підписана секція (XXX_SIGN) – підписана ключем директора (керівника) підприємства.
3. Підписана секція (XXX_SIGN) – підписана ключем цифрової печатки підприємства (за умови її наявності).
4. Підписана секція (XXX_SIGN) – підписана ключем цифрової печатки філіалу підприємства (за умови наявності філіалу на підприємстві).
5. Блок з документом у форматі XML.

Формат повідомлення „Документ з позначкою часу "
Повідомлення передається від податкового органу до платника податків.
Повідомлення є відповіддю податкового органу на запит документа.
Структура:
1.Транспортний заголовок документа.
2.Блок даних, зашифрований на одержувача:
2.1.Підпис податкового органу.
2.2.Позначка часу на момент отримання документа від платника податків.
2.3. Підписи платника податків.
2.4. Блок з документом у форматі XML.

Формат повідомлення „Відповідь на документ"
Повідомлення передається від податкового органу до платника податків.
Повідомлення є відповіддю податкового органу на переданий документ.
Наприклад, квитанція про призначення реєстраційного номера.
Структура:
1. Підпис податкового органу.
2. Транспортний заголовок документа.
3. Блок, зашифрований на платника податків, містить підписи і текст відповіді податкового органу.

Формат повідомлення „Відповідь на документ з позначкою часу"
Повідомлення передається від податкового органу до платника податків. Повідомлення є відповіддю податкового органу на переданий документ, якщо транспортний заголовок документа містить тег “ GET_STAMP=1”. Наприклад, квитанція про призначення реєстраційного номера.
Структура:
1. Позначка часу.
2. Підпис податкового органу.
3. Транспортний заголовок документа.
4. Блок, зашифрований на платника податків, містить підписи і текст відповіді податкового органу.

Додаток 1

до Уніфікованого формату транспортного повідомлення при інформаційній взаємодії платників податків і податкових органів в електронному вигляді телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису

Приклад транспортного повідомлення, що містить документ податкової звітності

```
From: "deklarenko@podatok.com" < deklarenko@podatok.com >
Subject: Zvit_to_STA_Report_Package:00000126
To: r2658@kyivsta.gov.ua
Content-Type: multipart/mixed; boundary="nKL74aFLyX=_quTCo1fSXn7ExWmSEcWQKL"
MIME-Version: 1.0
Reply-To: deklarenko@podatok.kiev.ua
Date: Tue, 8 Apr 2008 06:55:18 +0300
X-Mailer: Best Zvit MailAgent (v.08.001.0016)
Message-Id: <E1Jj7og-0005FF-PO@ podatok.kiev.ua>

This is a multi-part message in MIME format

--nKL74aFLyX=_quTCo1fSXn7ExWmSEcWQKL
Content-Type: text/plain; charset="windows-1251"
Content-Transfer-Encoding: 8bit

deklarenko@podatok.com
00000126
Закрите акціонерне товариство "Нагляд"
Петров Петро Петрович

--nKL74aFLyX=_quTCo1fSXn7ExWmSEcWQKL
Content-Type: application/octet-stream;
        name="26580000000126J020010610000132032008.XML"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="26580000000126J020010610000132032008.XML"

VFJBTlNQT1JUQUJMRQBsAQAARklMRU5BTUU9MjY1ODAwMDAwMDAxMjZKMDIwMDEwNjEwMDAwMTMy
MDMyMDA4LlhNTA0KRURSUE9VPTAwMDAwMTI2DQpTTkRfTkFNRT0gx+Dq8Ojy5SDg6vaz7u3l8O3l
IPLu4uDw6PHy4u4gIs3g4+v/5CINClNORF9FTUFJTD1jaGVwb3N0QGludGVsc2Vydi5raWV2LnVh
DQpSQ1ZfRU1BSUw9Y2hlcG9zdEBpbnRlbHNlcnYua2lldi51YQ0KUFJHX1RZUEU9QlpfUExVUw0K
UFJHX1ZFUj04NTQwMDANClNORF9EQVRFPTIwMDgwNDA4MTAwMDI2DQpDRVJUWVBFPVVTQw0KRFBB
X0NEPTI2NTgNCkNSQzMyX1NJR049Qzk1QjRCMDcNCkNSQzMyX0ZJTEU9NDFGNjgwNkQNClNVQkpF
Q1Q9x+Jp8u3gICDP7uTg8uru4uAg5OXq6+Dw4Paz/yDnIM/Ewg0KAFVTQ19DUllQVAAOAwAAMIID
CjCCArKgAwIBAgICIBcwDQYLKoYkAgEBAQEDAQEwTDELMAkGA1UEBhMCVUExETAPBgNVBAcMCNCa
0LjRl9CyMSowKAYDVQQDDCHQptCh0Jog0KLQntCSICLQo9Ch0KYiICjRgtC10YHRgikwHhcNMDcw
NDEzMDk0MjI5WhcNMDgwNDEyMDk0MjI5WjCB9DELMAkGA1UEBhMCVUExQjBABgNVBAoMOdCU0J9J
INCjINCh0J7Qm9Ce0Jwn0K/QndCh0KzQmtCe0JzQoyDQoC3QnUkg0Jwu0JrQmNCE0JLQkDERMA8G
A1UECwwIMjI2ODg4NjAxQjBABgNVBAMMOdCU0J9JINCjINCh0J7Qm9Ce0Jwn0K/QndCh0KzQmtCe
0JzQoyDQoC3QnUkg0Jwu0JrQmNCE0JLQkDE+MDwGA1UEEAw1MDMxNTEsINC8LtCa0LjRl9CyLCDQ
stGD0Lsu0KHQvNGW0LvRj9C90YHRjNC60LAsINCxLjYxCjAIBgNVBC4MATIwXTAgBg0qhiQCAQEB
AQMBAQEBMA8GDSqGJAIBAQEBAwEBAgkDOQAENggKYG8dpjombuOKKHjU8EmJs6mx7/i8jQBGRnXF
QewQfz6SWn2MACp4p10+cy9ycAdlwg8c66OB0zCB0DAfBgNVHREEGDAWgRRyMjY1OEBreWl2c3Rh
Lmdvdi51YTApBgNVHQ4EIgQgK9puJeBtvEuvL+x8hHjhyvDkJ2UhesH2WMHGDXFoMa0wJQYDVR0J
BB4wHDAaBgwqhiQCAQEBCwEEAgExChMIMjI2ODg4NjAwDgYDVR0PAQH/BAQDAgTwMB4GCCsGAQUF
BwEDAQH/BA8wDTALBgkqhiQCAQEBAgEwKwYDVR0jBCQwIoAg9ZI+eWr6Mnhv09/u27LVMD1lhQL/
rXDVIM01FUJHBvUwDQYLKoYkAgEBAQEDAQEDQwAEQEnfst10pV6MWBXYaHozzoxTBeEu9agZgOZS
GB3cO9ES9nNMtduBO/pBT0e8sK9hH63CrgHlIB21K3vvVdCHMjUMDQoOAAMIAgsEAQUPCQcGCgAB
DwsEDAMJAg0OBwYIBQ0FBAkOCwEABgwPCgIDCAcNAwwKAAQODwUIBgIBCwcJBQMJDwoLDAQHDg0C
AQAGCAUGDwILDQgKBA4BAAcDDAkGAg8KCA4MCQcBBQ0DAAQLDgMMCwkBDQUCAA8GBAgKB8a9JmfQ
ZultcgAAADBwBDZNCLod3+5SylvAYl8T4HxiXC5P493EjwKM0i1V1LCEKxNt142tBM+DPaIGWZoc
fh9EPcwCb+IENmf1eeElrJyJJ9/qoSOS2yVjFY4J2j54dbhLSkgi/Avpkxa6lt1VlT5kwnRoThIW
VyMmV/UCMAUfUgYOIYoMiQqr1QTC/LrhQ0KoOk2WEBClrANuM2LzPDfYSQYDngU+G8ou9mbSp05y
mTFYkq3n0/h+D1uQDZUAAAAABAsAABu8CngVM5kQtdMgX6Qi4jLsoMFaUwLfkkXU1o55ZV7JiyOw
f1SQdp4xaYonmxaJXiQBbvWoMsHfZIhtkHcHTroKR+SRuT4iORQMJ4M/66wkjrISwunbPBwmAk73
yBWAzfev17laDETqfqDK62xp9PgI+4WVtMV5pbIM8iYTblkpioy28WYhzzL2ITJwwoQgtZw+915z
PWX2IwnqSbq8TnzsUlQhxm5ZNIgI5eHwk4XIiHzaPd7hxoSXSAPFwybXnysQWHrDuNM+TtowaQ7Q
3onAPSqexqJjB+6RnEpKkQyyBT0pZ4a+FfbZ4OuWxVXsLTxSkWPZxkvZuJ3rN+gQN92GisT+wvwX
D/U2yvg6/q7jh7BmDdfaLI1eQlVcbjO3cXT9v2v7QmBbhvID12jGP2P3PT/BwUyzQQjBSuZXcpb9
w8J/ZdqL2S8GW16CsPAqq7Vu24ejfRa60wfMLWGsRZ9e0AKMNCBeTxDpaT/Atye1E1NiGKhjPGUJ
FlAVVgnqPsHwxVuPo2PRPys2Mzz6vPQkR/rIyaSWZbSY6jeRlbY/EGi72PELwACEjsQ2smeqrqN9
np1wswtZupOWazKP4GfSTMhR/vQd10FfPAKB5ggcY826bUPsPqWOtZ7PdMJCaItqTsywHRphwbPu
y2VeWunrb7jsyZvEeHkP1swe3hY/JajIuhnne6V4I7W6S6O/m/0JigLPhISth4wHxl47wwQE6cTw
2dJmrtAKxnGAN1AJxUHyiMKmwSR5MwVAqMffB8k56G+zcvfJDqY7t62IUaVrxLv8juEN5+k6ypY1
NnNoLJNVNZ1rSUturt9WiJTAlYARkX3lzQq94azUsv9N2kLPS0r9jSd9eBbhP51frA==
--nKL74aFLyX=_quTCo1fSXn7ExWmSEcWQKL--
```

Додаток 2

до Уніфікованого формату транспортного повідомлення при інформаційній взаємодії платників податків і податкових органів в електронному вигляді телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису

Приклад файла документа податкової звітності

Ім'я файла:

26580000000126J02001061000013405 2008.XML

Зміст файла:

```
<?xml version="1.0" encoding="windows-1251"?>
<DECLAR xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="J0200106.XSD">
<DECLARHEAD>
        <TIN>00000126</TIN>
        <C_DOC>J02</C_DOC>
        <C_DOC_SUB>001</C_DOC_SUB>
        <C_DOC_VER>6</C_DOC_VER>
        <C_DOC_TYPE>0</C_DOC_TYPE>
        <C_DOC_CNT>134</C_DOC_CNT>
        <C_REG>26</C_REG>
        <C_RAJ>58</C_RAJ>
        <PERIOD_MONTH>5</PERIOD_MONTH>
        <PERIOD_TYPE>1</PERIOD_TYPE>
        <PERIOD_YEAR>2008</PERIOD_YEAR>
        <C_DOC_STAN>1</C_DOC_STAN>
        <D_FILL>03042008</D_FILL>
<SOFTWARE/>
</DECLARHEAD>
<DECLARBODY>
        <HZ>1</HZ>
        <HZY>2008</HZY>
        <HZM>05</HZM>
        <HZYP xsi:nil="true"></HZYP>
        <HNAME> Закрите акц_онерне товариство &amp;quot;Нагляд&amp;quot;</HNAME>
        <HTINJ>00000126</HTINJ>
        <HDDGVSD xsi:nil="true"></HDDGVSD>
        <HNDGVSD xsi:nil="true"></HNDGVSD>
        <HNPDV>236476834278</HNPDV>
        <HNSPDV>3266664-ГГ</HNSPDV>
        <HLOC>12345, м.М.КИЇВ, Перемоги, б.32</HLOC>
        <HZIP>12345</HZIP>
        <HTEL>678876</HTEL>
        <HFAX xsi:nil="true"></HFAX>
        <HEMAIL>deklarenko@ podatok.kiev.ua</HEMAIL>
```

```
        <HSTI>ДП_ У СОЛОМ&amp;apos;ЯНСЬКОМУ Р-Н_ М.КИЄВА</HSTI>
        <R10GA>150</R10GA>
        <R10GB>30</R10GB>
        <R21GA xsi:nil="true"></R21GA>
        <R22GA xsi:nil="true"></R22GA>
        <R30GA xsi:nil="true"></R30GA>
        <R40GA xsi:nil="true"></R40GA>
        <R50GA>150</R50GA>
        <R52GA>150</R52GA>
        <R52GB xsi:nil="true"></R52GB>
        <R60GA xsi:nil="true"></R60GA>
        <R60GB>0</R60GB>
        <R60GAD xsi:nil="true"></R60GAD>
        <R70GA xsi:nil="true"></R70GA>
        <R70GB>0</R70GB>
        <R82GB>0</R82GB>
        <R83GA xsi:nil="true"></R83GA>
        <R83GB>0</R83GB>
        <R90GB>30</R90GB>
        <R101GB>0</R101GB>
        <R102GA xsi:nil="true"></R102GA>
        <R110GA>0</R110GA>
        <R121GB>0</R121GB>
        <R122GA xsi:nil="true"></R122GA>
        <R122GB>0</R122GB>
        <R123GA xsi:nil="true"></R123GA>
        <R124GA xsi:nil="true"></R124GA>
        <R124GB>0</R124GB>
        <R125GA xsi:nil="true"></R125GA>
        <R125GB>0</R125GB>
`       <R162GA xsi:nil="true"></R162GA>
        <R162GB>0</R162GB>
        <R163GB xsi:nil="true"></R163GB>
        <R170GB>0</R170GB>
        <R181GB>30</R181GB>
        <R182GB>0</R182GB>
        <R200GB>30</R200GB>
        <R210GB>0</R210GB>
        <R222GB>0</R222GB>
        <R230GB>0</R230GB>
        <R240GB>0</R240GB>
        <R260GB>0</R260GB>
        <R270GB>30</R270GB>
        <R20G16S xsi:nil="true"></R20G16S>
        <HFILL>03042008</HFILL>
        <HBOS> Петров Петро Петрович</HBOS>
        <HBUH>Ваніліна Олена Петрівна</HBUH>
        <HFO xsi:nil="true"></HFO>
</DECLARBODY>
<!-- YOUR_ID="58762" -->
</DECLAR>
```

Додаток 3

до Уніфікованого формату транспортного повідомлення при інформаційній взаємодії платників податків і податкових органів в електронному вигляді телекомунікаційними каналами зв'язку з використанням електронного цифрового підпису

Специфікація криптографічних функцій

1. Вступ

У документі надається опис уніфікованої бібліотеки функцій, призначених для криптографічних перетворень інформації. Бібліотека призначена для застосування при розробці програмного забезпечення у будь-якому середовищі розробки (Microsoft Visual C++, Visual Basic, C#, CodeGear RAD Studio тощо).

2. Загальні вимоги

1. Робота в середовищі Microsoft Windows 98/2000/XP/Vista/7, Linux (RadHat, Suse).
2. Багатопоточність.
3. Бібліотека повинна поставлятися для платформ x86 та x64.
4. Передача параметрів за угодою __stdcall.
5. Пам’ять під блоки з результатом роботи функцій виділяється визиваючою стороною.

3. Поставка бібліотеки

Бібліотека поставляється 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.

Бібліотеки постачаються разом з заголовними файлами з розширенням (*.h), що містять вичерпний опис функцій бібліотеки.

1. Функція накладання підпису

```
int __stdcall MakeSign (const void* pkbuf, int pklen, const char*
pwd, const void* hashbuf, void* signbuf, int* signlen);
```

Параметр	Опис
const void* pkbuf	Буфер з секретним ключем
int pklen	Розмір буфера з секретним ключем
const char* pwd	Пароль секретного ключа, повинен закінчуватись символом ‘\0’
const void* hashbuf	Буфер з хешем документа, розмір 32 байта
void* signbuf	Буфер для підпису, якщо NULL – в signlen повертається розмір
int* signlen	Розмір підпису в буфері

Функція повертає 0, коли успішно виконано, або код помилки.

2. Функція перевірки підпису

```
int __stdcall VerifySign (const void* certbuf, int certlen, const
void* hashbuf, const void* signbuf, int signlen);
```

Параметр	Опис
const void* certbuf	Буфер з сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* hashbuf	Буфер з хешем документа, розмір 32 байта
const void* signbuf	Буфер з підписом
int signlen	Розмір буфера з підписом

Функція повертає 0, якщо підпис вірний, або код помилки.

3. Функція перевірки сертифіката

```
int __stdcall VerifyCert (const void* certbuf, int certlen, const
void* rootcbuf, int rootclen);
```

Параметр	Опис
const void* certbuf	Буфер з сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* rootcbuf	Буфер з кореневим сертифікатом
int rootclen	Розмір буфера з кореневим сертифікатом

Функція повертає 0, коли сертифікат відповідає кореневому, або код помилки.

4. Функція шифрування блоку даних

```
int __stdcall Encrypt (const void* certbuf, int certlen, const
void* docbuf, int doclen, void* outbuf, int* outlen);
```

Параметр	Опис
const void* certbuf	Буфер з сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* pkbuf	Буфер з секретним ключем
int pklen	Довжина буфера з секретним ключем
const char* pwd	Пароль секретного ключа повинен закінчуватись символом ‘\0’
const void* docbuf	Буфер з документом
int doclen	Розмір буфера з документом
void* outbuf	Вихідний буфер, якщо NULL – в outlen повертається розмір
int* outlen	Розмір вихідного буфера

Функція повертає 0, коли успішно зашифровано, або код помилки.

5. Функція розшифрування блоку даних

```
int __stdcall Decrypt (const void* pkbuf, int pklen, const char*
pwd, const void* docbuf, int doclen, void* outbuf, int* outlen);
```

Параметр	Опис
const void* pkbuf	Буфер з секретним ключем
int pklen	Довжина буфера з секретним ключем
const char* pwd	Пароль секретного ключа повинен закінчуватись символом ‘\0’
const void* certbuf	Буфер з сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* docbuf	Буфер з документом
int docsize	Розмір буфера з документом
void* outbuf	Вихідний буфер, якщо NULL – в outlen повертається розмір
Int* outlen	Розмір вихідного буфера

Функція повертає 0, коли успішно виконано, або код помилки.

6. Функція звірки сертифіката з секретним ключем

```
int __stdcall VerifyCertPKMatch (const void* certbuf, int certlen,
const void* pkbuf, int pklen);
```

Параметр	Опис
const void* certbuf	Буфер з сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* pkbuf	Буфер з секретним ключем
int pklen	Розмір буфера з секретним ключем
const char* pwd	Пароль секретного ключа повинен закінчуватись символом ‘\0’

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

7. Функція отримання інформації з сертифіката

```
int __stdcall GetCertInfo (const void* certbuf, int certlen,
UACertInfo* info);
```

Параметр	Опис
const void* certbuf	Буфер з сертифікатом
int certlen	Довжина буфера з сертифікатом
UACertInfo* info	Структура з інформацією з сертифіката (приведена нижче)

Функція повертає 0, коли успішно виконано, або код помилки.

Структура UACertInfo

Поле	Опис
char Serial[64]	Серійний номер сертифіката
char EDRPOU[11]	ЄДРПОУ установи
char DRFO[11]	ДРФО особи
char Name[64]	ПІБ особи або найменування установи
char Email[64]	E-mail
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
time_t DtEnd	Дата закінчення дії сертифіката

Вирівнювання членів структури – 1 байт.
Розмір кожного строкового поля містить
завершуючий 0-символ.

4. Коди помилок

```
#define CRYPT_OK                0  // Успішно
#define CRYPT_BUFFER_EMPTY      1  // Буфер порожній
#define CRYPT_DLL_NOT_LOADED    2  // DLL не ініціалізовано
#define CRYPT_BAD_CERT          3  // Помилка отримання інформації з
                                      сертифіката
#define CRYPT_CERT_NOT_ALLOWED  4  // Даний сертифікат не може
                                      використовуватися для
                                      виконання операції
#define CRYPT_SK_NOT_MATCH      5  // Не збігається пара сертифікат
                                      - секретний ключ
#define CRYPT_SK_CORRUPT        7  // Некоректний формат секретного
                                      ключа
#define CRYPT_BAD_PASSWORD      8  // Помилка підпису/шифрування,
                                      можливо вказано невірний
                                      пароль
#define CRYPT_BAD_SIGN         11  // Невірний підпис
#define CRYPT_INTERNAL_ERR     12  // Внутрішня помилка перевірки
                                      підпису
#define CRYPT_BAD_CRC          13  // Помилка перевірки цілісності:
                                      буфер пошкоджено
#define CRYPT_NOT_SUPPORTED    14  // Функція не підтримується
```