ЗАТВЕРДЖЕНО

Наказ Державної служби
статистики України

_____ № _____

**Уніфікований формат транспортного повідомлення
при інформаційній взаємодії респондентів і органів державної статистики в
електронній формі електронними комунікаційними мережами
з використанням кваліфікованого електронного підпису**

Зміст

Уніфікований формат транспортного повідомлення для обміну інформацією в електронній формі між респондентами і органами державної статистики електронними комунікаційними мережами з використанням кваліфікованого електронного підпису (далі – Уніфікований формат транспортного повідомлення) застосовується для організації обміну електронними документами між респондентами й системою електронної звітності органів державної статистики (далі – СЕЗ ОДС) електронними комунікаційними мережами з використанням кваліфікованого електронного підпису (далі – КЕП). Обмін електронними документами здійснюється за допомогою **транспортного повідомлення** (далі – ТП), яке складається з реквізитів ТП і **транспортного контейнера**, що містить зашифровані дані (електронні звіти, квитанції тощо).

Квитанції про приймання електронних документів, створені СЕЗ ОДС, є електронними документами й передаються респонденту в уніфікованому форматі транспортного повідомлення, який регламентовано в цьому документі.

I. Шляхи обміну інформацією

Обмін інформацією між респондентами і СЕЗ ОДС в електронній формі може проводитися двома шляхами:

електронний документ передається до СЕЗ ОДС за допомогою посередника електронної звітності;

електронний документ передається за допомогою електронної пошти безпосередньо автором електронного документа до СЕЗ ОДС електронними комунікаційними мережами.

Цей документ описує уніфікований формат транспортного повідомлення для подання електронної звітності безпосередньо до СЕЗ ОДС електронними комунікаційними мережами.

II. Вимоги до криптографічного захисту інформації

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

реалізовувати процедури формування й перевірки КЕП 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 ДСТУ 7624:2014;

бути сертифікованими відповідно до законодавства України.

Функції бібліотек криптографічних перетворень, що надаються кваліфікованими надавачами електронних довірчих послуг (КНЕДП) для інтеграції в систему електронної звітності органів державної статистики, мають

відповідати специфікаціям криптографічних перетворень, викладених у додатку 3.

III. Уніфікований формат транспортного повідомлення

Уніфікований формат транспортного повідомлення підтримує всі діючі типи електронних документів інформаційної взаємодії відповідно до чинного законодавства України та обумовлених у Порядку подання електронної звітності до органів державної статистики, затвердженому наказом Держкомстатом від 12.01.2011 № 3 та зареєстрованому в Міністерстві юстиції України 29.03.2011 за № 408/19146.

Схему уніфікованого транспортного повідомлення представлено на рис.1.

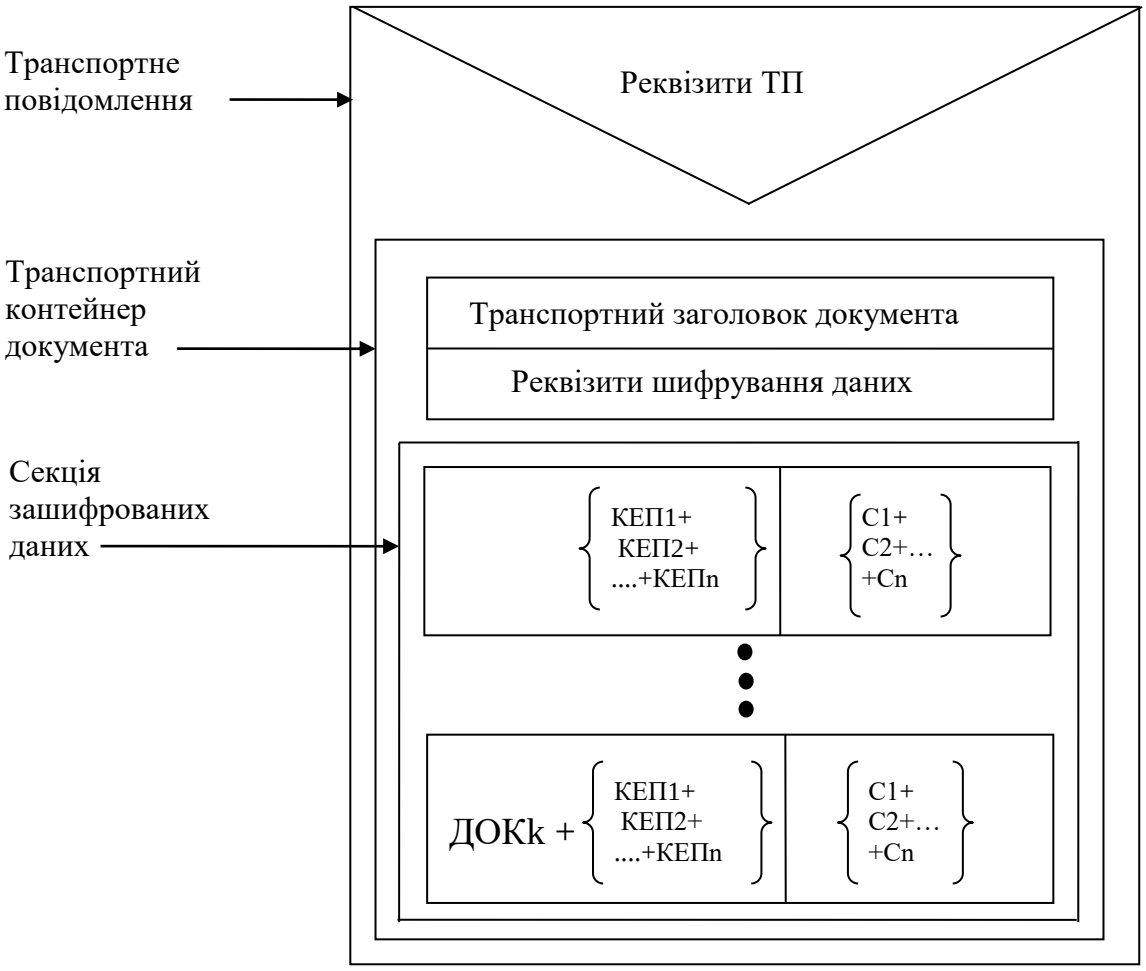

рис. 1

ДОК1, 2, …k – файл електронного документа;
КЕП1, 2, …n – один чи декілька кваліфікованих електронних підписів, якими засвідчено документ;
С1, 2, …n – один чи декілька блоків із сертифікатами ключів КЕП, якими засвідчено документ.
Сертифікати входять до складу блоку КЕП у "Секції зашифрованих даних". Розташування сертифікатів у блоці КЕП визначається постачальником криптографічної бібліотеки.
Під блоком "Реквізити шифрування даних" мається на увазі зашифрований блок, який починається із сигнатури "XXX_CRYPT", де XXX – літери, що ідентифікують відповідний КНЕДП. Структура зашифрованого блоку залежить від реалізації криптографічної бібліотеки.
У "Секції зашифрованих даних" КЕП формуються послідовно, накладаючись один на одний.

IV. Вимоги до структури транспортного повідомлення

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

Файл, який уміщує 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, передане електронними комунікаційними мережами, має містити тільки один вкладений у нього транспортний контейнер. Розмір транспортного повідомлення, переданого електронними комунікаційними мережами, не повинен перевищувати 10 Мбайт. У випадку прийняття транспортного повідомлення до обробки СЕЗ ОДС контейнер із тим самим ім'ям не може бути переданий тим самим відправником удруге.

Унікальний ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України (далі – код ЄДРПОУ), реєстраційний номер облікової картки платника податків (далі – РНОКПП) або серія (за наявності) 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 контролюючий орган і мають відмітку у паспорті).

Заголовок транспортного повідомлення має містити такі обов'язкові поля:

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

"To:" – поле, що містить ім'я одержувача в кодуванні "Quoted Printable/Windows 1251" або "Base64/Windows 1251" й електронну адресу одержувача, поміщену в 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 мають 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 має кодуватися в Quoted Printable/Windows 1251 або Base64/Windows 1251.

"Content-Disposition:", що містить ключове слово "attachment" і параметр "filename". Ім'я файла має 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 статистичної звітності, наведено в додатку 1.

Приклад файла документа статистичної звітності наведено в додатку 2.

V. Вимоги до структури транспортного контейнера для передачі документів до СЕЗ ОДС

5.1. Узагальнений формат транспортного контейнера для передачі документів до СЕЗ ОДС:

заголовок транспортного контейнера;

реквізити шифрування даних;

зашифровані дані.

5.2. Перелік блоків даних транспортного контейнера для передачі документів до СЕЗ ОДС.

5.2.1. Зашифрований блок даних

Формат зашифрованого блоку даних:

Елемент	Значення
Сигнатура	"XXX_ CRYPT", де XXX – код Кваліфікованого надавача електронних довірчих послуг*
0-символ	
4 байти	розмір зашифрованого документа
Зашифрований документ	

*Код Кваліфікованого надавача електронних довірчих послуг – послідовність із трьох прописних літер латинського алфавіту, яка однозначно ідентифікує Кваліфікованого надавача електронних довірчих послуг і яку призначає Держстат.

5.2.2. Блок сертифіката для шифрування даних

Формат блоку сертифіката для шифрування даних:

Елемент	Значення
Сигнатура	"XXX_CERTCRYPT", де XXX – код Кваліфікованого надавача електронних довірчих послуг *
0-символ	
4 байти	розмір сертифіката шифрування
Сертифікат шифрування	

* Код Кваліфікованого надавача електронних довірчих послуг – послідовність із трьох прописних літер латинського алфавіту, яка однозначно ідентифікує Кваліфікованого надавача електронних довірчих послуг СЕЗ ОДС.

Блок сертифіката для шифрування даних має розташовуватись усередині зашифрованого блоку, але перед першим підписом на документі.

Якщо в транспортному повідомленні присутня секція XXX_CERTCRYPT, вихідні документи системи (квитанції, інформаційні повідомлення тощо) шифруються за допомогою отриманого сертифіката шифрування.

Якщо в транспортному повідомленні відсутня секція XXX_CERTCRYPT, вихідні документи створюються за діючою наразі схемою – для шифрування використовується сертифікат із підпису документа.

5.3. Підпис

Формат підпису:

Елемент	Значення
Сигнатура	"XXX_SIGN", де XXX – код Кваліфікованого надавача електронних довірчих послуг *
0-символ	
4 байти	розмір буфера підпису та підписаних даних
Буфер підпису та підписаних даних	

* Код Кваліфікованого надавача електронних довірчих послуг – послідовність із трьох прописних літер латинського алфавіту, яка однозначно ідентифікує Кваліфікованого надавача електронних довірчих послуг і яку призначає Держстат.

5.4. Позначка часу

Позначка часу отримується із КНЕДП за протоколом TSP (Timestamp Protocol).

Формат позначки часу:

Елемент	Значення
Сигнатура	"XXX_STAMP", де XXX – код Кваліфікованого надавача електронних довірчих послуг
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	

* Код Кваліфікованого надавача електронних довірчих послуг – послідовність із трьох прописних літер латинського алфавіту, яка однозначно ідентифікує Кваліфікованого надавача електронних довірчих послуг і яку призначає Держстат.

5.5. Заголовок транспортного контейнера

Транспортний заголовок документа містить інформацію про документ, що передається.

Формат транспортного заголовка документа:

Елемент	Значення
Сигнатура	"TRANSPORTABLE"
0-символ	
4-байтовий розмір транспортного заголовка	без урахування довжини сигнатури й 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
EDRPOU	Код ЄДРПОУ/РНОКПП/ серія (за наявності) 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 контролюючий орган і мають відмітку у паспорті) респондента, що подає звіт (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Так
PRG_TYPE	Назва програмного забезпечення для накладання та перевірки КЕП відправника завдовжки не більше десяти символів (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Так
PRG_VER	Версія програмного забезпечення для накладання та перевірки КЕП відправника завдовжки не більше десяти символів (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Ні
SUBJECT	Назва документа статистичної звітності (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Ні
RESULT	Результат прийому повідомлення (0 – успішно, 1 – помилка, 2 – попередження)	Ні
KVTNUM	Номер квитанції (1, 2, 3, …)	Ні
FINKVT	Ознака фінальної квитанції (0/1)	Ні

5.6. Формати повідомлень, які надсилаються в транспортному контейнері

5.6.1. Формат повідомлення "Документ"

Повідомлення передається від респондента до СЕЗ ОДС.

Структура:

транспортний заголовок документа;

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

5.6.2. Формат повідомлення "Документ з позначкою часу"

Повідомлення передається від СЕЗ ОДС до респондента. Повідомлення є відповіддю СЕЗ ОДС на запит документа.

Структура:

транспортний заголовок документа;

блок даних, зашифрований на одержувача:

підпис СЕЗ ОДС;

позначка часу на момент отримання документа від респондента;

підписи респондента;

блок із документом у форматі XML.

5.6.3. Формат повідомлення "Відповідь на документ"

Повідомлення передається від СЕЗ ОДС до респондента. Повідомлення є відповіддю СЕЗ ОДС на документ, що передається.

Структура:

транспортний заголовок документа;

позначка часу;

підпис СЕЗ ОДС;

блок, зашифрований на респондента, містить підписи й текст відповіді СЕЗ ОДС.

Додаток 1

до Уніфікованого формату транспортного повідомлення при інформаційній взаємодії респондентів і органів державної статистики в електронній формі електронними комунікаційними мережами з використанням електронного цифрового підпису

Приклад транспортного повідомлення, що містить документ статистичної або фінансової звітності

From: "shevchenko@sample.com" < shevchenko@sample.com >
Subject: Zvit_to_SSCU_Report_Package:00000126
To: gate12@ukrstat.gov.ua
Content-Type: multipart/mixed;
boundary="nKL74aFLyX=_quTCo1fSXn7ExWmSEcWQKL"
MIME-Version: 1.0
Reply-To: shevchenko@sample.com
Date: Tue, 8 Apr 2008 06:55:18 +0300
X-Mailer: Unknown MailAgent (v.00.000.0001)
Message-Id: <E1Jj7og-0005FF-PO@ sample.com >

This is a multi-part message in MIME format

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

shevchenko@sample.com
00000126
ТОВ "АСТ"
Шевченко Петро Петрович

--nKL74aFLyX=_quTCo1fSXn7ExWmSEcWQKL
Content-Type: application/octet-stream;
name="01010802305001S100020610000001012009.XML"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="01010802305001S100020610000001012009.XML"
VFJBTlNQT1JUQUJMRQBsAQAARklMRU5BTUU9MjY1ODAwMDAwMDAx
MjZKMDIwMDEwNjEwMDAwMTMy
MDMyMDA4LlhNTA0KRURSUE9VPTAwMDAwMTI2DQpTTkRfTkFNRT0gx+
Dq8Ojy5SDg6vaz7u3l8O3l
IPLu4uDw6PHy4u4gIs3g4+v/5CINClNORF9FTUFJTD1jaGVwb3N0QGludGVsc2
Vydi5raWV2LnVh

DQpSQ1ZfRU1BSUw9Y2hlcG9zdEBpbnRlbHNlcnYua2lldi51YQ0KUFJHX1RZU
EU9QlpfUExVUw0K
UFJHX1ZFUj04NTQwMDANClNORF9EQVRFPTIwMDgwNDA4MTAwMDI2D
QpDRVJUWVBFPVVTQw0KRFBB
X0NEPTI2NTgNCkNSQzMyX1NJR049Qzk1QjRCMDcNCkNSQzMyX0ZJTEU9N
DFGNjgwNkQNClNVQkpF
Q1Q9x+Jp8u3gICDP7uTg8uru4uAg5OXq6+Dw4Paz/yDnIM/Ewg0KAFVTQ19DUl
lQVAAOAwAAMIID
CjCCArKgAwIBAgICIBcwDQYLKoYkAgEBAQEDAQEwTDELMAkGA1UEBh
MCVUExETAPBgNVBAcMCNCa
0LjRl9CyMSowKAYDVQQDDCHQptCh0Jog0KLQntCSICLQo9Ch0KYiICjRgtC1
0YHRgikwHhcNMDcw
NDEzMDk0MjI5WhcNMDgwNDEyMDk0MjI5WjCB9DELMAkGA1UEBhMCVU
ExQjBABgNVBAoMOdCU0J9J
INCjINCh0J7Qm9Ce0Jwn0K/QndCh0KzQmtCe0JzQoyDQoC3QnUkg0Jwu0JrQm
NCE0JLQkDERMA8G
A1UECwwIMjI2ODg4NjAxQjBABgNVBAMMOdCU0J9JINCjINCh0J7Qm9Ce0J
wn0K/QndCh0KzQmtCe
0JzQoyDQoC3QnUkg0Jwu0JrQmNCE0JLQkDE+MDwGA1UEEAw1MDMxNTEsI
NC8LtCa0LjRl9CyLCDQ
stGD0Lsu0KHQvNGW0LvRj9C90YHRjNC60LAsINCxLjYxCjAIBgNVBC4MATI
wXTAgBg0qhiQCAQEB
AQMBAQEBMA8GDSqGJAIBAQEBAwEBAgkDOQAENggKYG8dpjombuOKK
HjU8EmJs6mx7/i8jQBGRnXF
QewQfz6SWn2MACp4p10+cy9ycAdlwg8c66OB0zCB0DAfBgNVHREEGDAWgR
RyMjY1OEBreWl2c3Rh
Lmdvdi51YTApBgNVHQ4EIgQgK9puJeBtvEuvL+x8hHjhyvDkJ2UhesH2WMHG
DXFoMa0wJQYDVR0J
BB4wHDAaBgwqhiQCAQEBCwEEAgExChMIMjI2ODg4NjAwDgYDVR0PAQH/
BAQDAgTwMB4GCCsGAQUF
BwEDAQH/BA8wDTALBgkqhiQCAQEBAgEwKwYDVR0jBCQwIoAg9ZI+eWr6
Mnhv09/u27LVMD1lhQL/
rXDVIM01FUJHBvUwDQYLKoYkAgEBAQEDAQEDQwAEQEnfst10pV6MWB
XYaHozzoxTBeEu9agZgOZS
GB3cO9ES9nNMtduB0/pBT0e8sK9hH63CrgHlIB21K3vvVdCHMjUMDQoOAAM
IAgsEAQUPCQcGCgAB
DwsEDAMJAg0OBwYIBQ0FBAkOCwEABgwPCgIDCAcNAwwKAAQODwUIB
gIBCwcJBQMJDwoLDAQHDg0C
AQAGCAUGDwILDQgKBA4BAAcDDAkGAg8KCA4MCQcBBQ0DAAQLDgM
MCwkBDQUCAA8GBAgKB8a9JmfQ
ZultcgAAADBwBDZNCLod3+5SylvAYl8T4HxiXC5P493EjwKM0i1V1LCEKxNt1
42tBM+DPaIGWZoc
fh9EPcwCb+IENmf1eeElrJyJJ9/qoSOS2yVjFY4J2j54dbhLSkgi/Avpkxa6lt1VlT5kw
nRoThIW
VyMmV/UCMAUfUgYOIYoMiQqr1QTC/LrhQ0KoOk2WEBClrANuM2LzPDfYS
QYDngU+G8ou9mbSp05y

mTFYkq3n0/h+D1uQDZUAAAAABAsAABu8CngVM5kQtdMgX6Qi4jLsoMFaU
wLfkkXU1o55ZV7JiyOw
f1SQdp4xaYonmxaJXiQBbvWoMsHfZIhtkHcHTroKR+SRuT4iORQMJ4M/66wkjrI
SwunbPBwmAk73
yBWAzfev17laDETqfqDK62xp9PgI+4WVtMV5pbIM8iYTblkpioy28WYhzzL2ITJ
wwoQgtZw+915z
PWX2IwnqSbq8TnzsUlQhxm5ZNIgI5eHwk4XIiHzaPd7hxoSXSAPFwybXnysQW
HrDuNM+TtowaQ7Q
3onAPSqexqJjB+6RnEpKkQyyBT0pZ4a+FfbZ4OuWxVXsLTxSkWPZxkvZuJ3rN+
gQN92GisT+wvwX
D/U2yvg6/q7jh7BmDdfaLI1eQlVcbjO3cXT9v2v7QmBbhvID12jGP2P3PT/BwUyz
QQjBSuZXcpb9
w8J/ZdqL2S8GW16CsPAqq7Vu24ejfRa60wfMLWGsRZ9e0AKMNCBeTxDpaT/At
ye1E1NiGKhjPGUJ
FlAVVgnqPsHwxVuPo2PRPys2Mzz6vPQkR/rIyaSWZbSY6jeRlbY/EGi72PELwA
CEjsQ2smeqrqN9
np1wswtZupOWazKP4GfSTMhR/vQd10FfPAKB5ggcY826bUPsPqWOtZ7PdMJCa
ItqTsywHRphwbPu
y2VeWunrb7jsyZvEeHkP1swe3hY/JajIuhnne6V4I7W6S6O/m/0JigLPhISth4wHxl47
wwQE6cTw
2dJmrtAKxnGAN1AJxUHyiMKmwSR5MwVAqMffB8k56G+zcvfJDqY7t62IUaVr
xLv8juEN5+k6ypY1
NnNoLJNVNZ1rSUturt9WiJTAlYARkX3lzQq94azUsv9N2kLPS0r9jSd9eBbhP51fr
A==
--nKL74aFLyX=_quTCo1fSXn7ExWmSEcWQKL—

Додаток 2

до Уніфікованого формату транспортного повідомлення при інформаційній взаємодії респондентів і органів державної статистики в електронній формі електронними комунікаційними мережами з використанням електронного цифрового підпису

Приклад файла документа статистичної звітності

Ім'я файла:

05004000373590 8S0210114100000030 62011.XML

Зміст файла:

```
<?xml version="1.0" encoding="windows-1251"?>
<DECLAR xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="S0210114.XSD">
 <DECLARHEAD>
        <TIN>12345678</TIN>
         <C_DOC>S02</C_DOC>
        <C_DOC_SUB>101</C_DOC_SUB>
        <C_DOC_VER>14</C_DOC_VER>
        <C_DOC_TYPE>0</C_DOC_TYPE>
        <C_DOC_CNT>7</C_DOC_CNT>
        <C_REG>05</C_REG>
        <C_RAJ>004</C_RAJ>
        <PERIOD_MONTH>7</PERIOD_MONTH>
        <PERIOD_TYPE>1</PERIOD_TYPE>
        <PERIOD_YEAR>2021</PERIOD_YEAR>
        <D_FILL>16082021</D_FILL>
        <SOFTWARE>TEST_PZ</SOFTWARE>
 </DECLARHEAD>
 <DECLARBODY>
        <FIRM_ADR>04108, Київська область, місто Київ, Подільський район,
проспект Свободи, буд. 28</FIRM_ADR>
        <FIRM_ADR_FIZ>23700, Вінницька область, місто Гайсин, вулиця
Груднева, буд.10 </FIRM_ADR_FIZ>
        <FIRM_EDRPOU>123456789</FIRM_EDRPOU>
        <FIRM_NAME>ТОВ "Test"</FIRM_NAME>
        <REP_PERNM>Липень 2021</REP_PERNM>
        <OBL>05</OBL>
        <RAY>004</RAY>
        <VIK_TEL>287-04-22</VIK_TEL>
        <VIK_EMAIL>coez@ukrstat.gov.ua</VIK_EMAIL>
        <A003_1 xsi:nil="true" />
        <A003_2 xsi:nil="true" />
        <A003_3 xsi:nil="true" />
        <A004_1 xsi:nil="true" />
```

<A004_2 xsi:nil="true" />
<A004_3 xsi:nil="true" />
<A011_1 xsi:nil="true" />
<A011_2 xsi:nil="true" />
<A011_3 xsi:nil="true" />
<A012_1 xsi:nil="true" />
<A012_2 xsi:nil="true" />
<A012_3 xsi:nil="true" />
<A015_1 xsi:nil="true" />
<A015_2 xsi:nil="true" />
<A015_3 xsi:nil="true" />
<A040_1 xsi:nil="true" />
<A040_2 xsi:nil="true" />
<A040_3 xsi:nil="true" />
<A041_1 xsi:nil="true" />
<A041_2 xsi:nil="true" />
<A041_3 xsi:nil="true" />
<A048_1 xsi:nil="true" />
<A048_2 xsi:nil="true" />
<A048_3 xsi:nil="true" />
<A052_1 xsi:nil="true" />
<A052_2 xsi:nil="true" />
<A052_3 xsi:nil="true" />
<A075_1 xsi:nil="true" />
<A075_2 xsi:nil="true" />
<A125_1 xsi:nil="true" />
<A125_2 xsi:nil="true" />
<A132_1 xsi:nil="true" />
<A132_2 xsi:nil="true" />
<A196_1 xsi:nil="true" />
<A196_2 xsi:nil="true" />
<A377_1 xsi:nil="true" />
<A377_2 xsi:nil="true" />
<A726_1 xsi:nil="true" />
<A726_2 xsi:nil="true" />
<A753_1 xsi:nil="true" />
<A753_2 xsi:nil="true" />
<A413_1 xsi:nil="true" />
<A413_2 xsi:nil="true" />
<A443_1 xsi:nil="true" />
<A443_2 xsi:nil="true" />
<A515_1 xsi:nil="true" />
<A515_2 xsi:nil="true" />
<A757_2 xsi:nil="true" />
<A472_1 xsi:nil="true" />
<A472_2 xsi:nil="true" />
<A498_1 xsi:nil="true" />

```
        <A498_2 xsi:nil="true" />
        <A562_1 xsi:nil="true" />
        <A562_2 xsi:nil="true" />
        <A752_1 xsi:nil="true" />
        <A752_2 xsi:nil="true" />
        <A997_1 xsi:nil="true" />
        <A997_2 xsi:nil="true" />
        <A997_3 xsi:nil="true" />
        <ZERO_ZVIT>1</ZERO_ZVIT>
        <RUK>Т Тестенко</RUK>
        <KATOTTG_FACT>05040030010071792</KATOTTG_FACT>
        <REASON>Тимчасово призупинено економічну діяльність</REASON>
        <REASON_KOD>39</REASON_KOD>
        <TER_GROM1 xsi:nil="true" />
        <TER_GROM2 xsi:nil="true" />
 </DECLARBODY>
</DECLAR>
```

Додаток 3

до Уніфікованого формату транспортного повідомлення при інформаційній взаємодії респондентів і органів державної статистики в електронній формі електронними комунікаційними мережами з використанням кваліфікованого електронного підпису

Специфікація криптографічних функцій

I. Вступ

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

II. Загальні вимоги

1. Робота в середовищі Microsoft Windows 7/8/8.1/10, Linux (RadHat, Suse).
2. Багатопоточність.
3. Бібліотека має поставлятися для платформ x86 та x64.
4. Передача параметрів за угодою __stdcall.
5. Пам’ять під блоки з результатом роботи функцій виділяється стороною, що викликає.

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

IV. Функції бібліотеки

4.1. Функція накладання підпису

4.1.1. без передачі сертифіката

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

Параметр	Опис
const void* pkbuf	Буфер із секретним ключем
int pklen	Розмір буфера із секретним ключем
const char* pwd	Пароль секретного ключа має закінчуватися 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 зберігає в outbuf блок документа з підписом.
Функція повертає 0, коли успішно виконано, або код помилки.

4.1.2. з передачею сертифіката

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);

Параметр	Опис
const void* certbuf	Буфер з сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* pkbuf	Буфер із секретним ключем
int pklen	Розмір буфера із секретним ключем
const char* pwd	Пароль секретного ключа має закінчуватися 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 зберігає в outbuf блок документа з підписом.
Функція повертає 0, коли успішно виконано, або код помилки.

4.2. Функція перевірки підпису

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

Параметр	Опис
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
void* certbuf	Буфер із сертифікатом, якщо NULL – в certlen повертається розмір
int* certlen	Розмір буфера із сертифікатом

Функція зберігає в outbuf блок документа без підпису.
Функція зберігає в certbuf блок сертифіката підписувача.
Функція повертає 0, якщо підпис правильний, або код помилки.

4.3. Функція перевірки сертифіката

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

Параметр	Опис
const void* certbuf	Буфер із сертифікатом
int certlen	Розмір буфера із 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.
Функція перевірки сертифіката виконує перевірку сертифіката кореневим сертифікатом АЦСК

4.4. 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);

Параметр	Опис
const void* certbuf	Буфер із сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* pkbuf	Буфер із секретним ключем
int pklen	Довжина буфера із секретним ключем
const char* pwd	Пароль секретного ключа має закінчуватися 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 зберігає в outbuf зашифрований блок документа.
Функція повертає 0, коли успішно зашифровано, або код помилки.

4.5. 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);

Параметр	Опис
const void* pkbuf	Буфер із секретним ключем
int pklen	Довжина буфера із секретним ключем
const char* pwd	Пароль секретного ключа має закінчуватися символом "\0"
const void* certbuf	Буфер із сертифікатом
int certlen	Розмір буфера із сертифікатом
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 зберігає в outbuf розшифрований блок документа.
Функція повертає 0, коли успішно виконано, або код помилки.

4.6. Функція звірки сертифіката із секретним ключем

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

Параметр	Опис
const void* certbuf	Буфер із сертифікатом
int certlen	Розмір буфера з сертифікатом
const void* pkbuf	Буфер із секретним ключем
int pklen	Розмір буфера із секретним ключем
const char* pwd	Пароль секретного ключа має закінчуватися символом "\0"

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

4.7. Функція отримання інформації із сертифіката

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

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

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

Структура UACertInfo

Поле	Опис
char Serial[64]	Серійний номер сертифіката
char EDRPOU[11]	Код ЄДРПОУ установи
char DRFO[11]	РНОКПП фізичної особи – підприємця/ серія (за наявності) 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 контролюючий орган і мають відмітку у паспорті)
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 (4 байти)
time_t DtEnd	Дата закінчення дії сертифіката (4 байти)
char Issuer[64]	Видавець (найменування)

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

V. 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 із сертифіката
#define   CRYPT_CERT_NOT_ALLOWED    4   // Цей 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,
                                        зазначено неправильний пароль
#define   CRYPT_BAD_SIGN            11  // Неправильний 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
```