Уніфікований формат транспортного повідомлення при інформаційній взаємодії суб'єктів господарювання державного сектору економіки і органів управління державною власністю в електронному вигляді телекомунікаційними каналами зв'язку з використанням кваліфікованого електронного підпису

Зміст

Уніфікований формат транспортного повідомлення для обміну інформацією між суб'єктами господарювання державного сектору економіки та органами управління державною власністю в електронному вигляді з використанням кваліфікованого електронного підпису (далі – Уніфікований формат транспортного повідомлення) застосовується для організації обміну електронними документами між суб'єктами господарювання державного сектору економіки і органами управління державною власністю безпосередньо і телекомунікаційними каналами зв'язку з використанням кваліфікованого електронного підпису (далі – КЕП). 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 органами управління державною власністю, є електронними документами і передаються суб'єкту господарювання державного сектору економіки в уніфікованому форматі транспортного повідомлення, який регламентовано у цьому документі.

1. Шляхи обміну інформацією

Обмін інформацією між суб’єктами господарювання державного сектору економіки і органами управління державною власністю в електронному вигляді може проводитися двома шляхами:

- електронний документ передається безпосередньо до органу управління державною власністю на електронному носії інформації (дискета, флеш-накопичувач тощо);
- електронний документ передається до органу управління державною власністю 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 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 ГОСТ 28147:2009;

бути сертифікованими відповідно до законодавства України.

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

3. Уніфікований формат транспортного повідомлення

Уніфікований формат транспортного повідомлення підтримує всі діючі типи електронних документів інформаційної взаємодії, обумовлених порядком подання звітності відповідно до чинного законодавства України та інших нормативних актів Міністерства економічного розвитку і торгівлі України та Міністерства фінансів України.

Схему уніфікованого транспортного повідомлення представлено на рис.1.

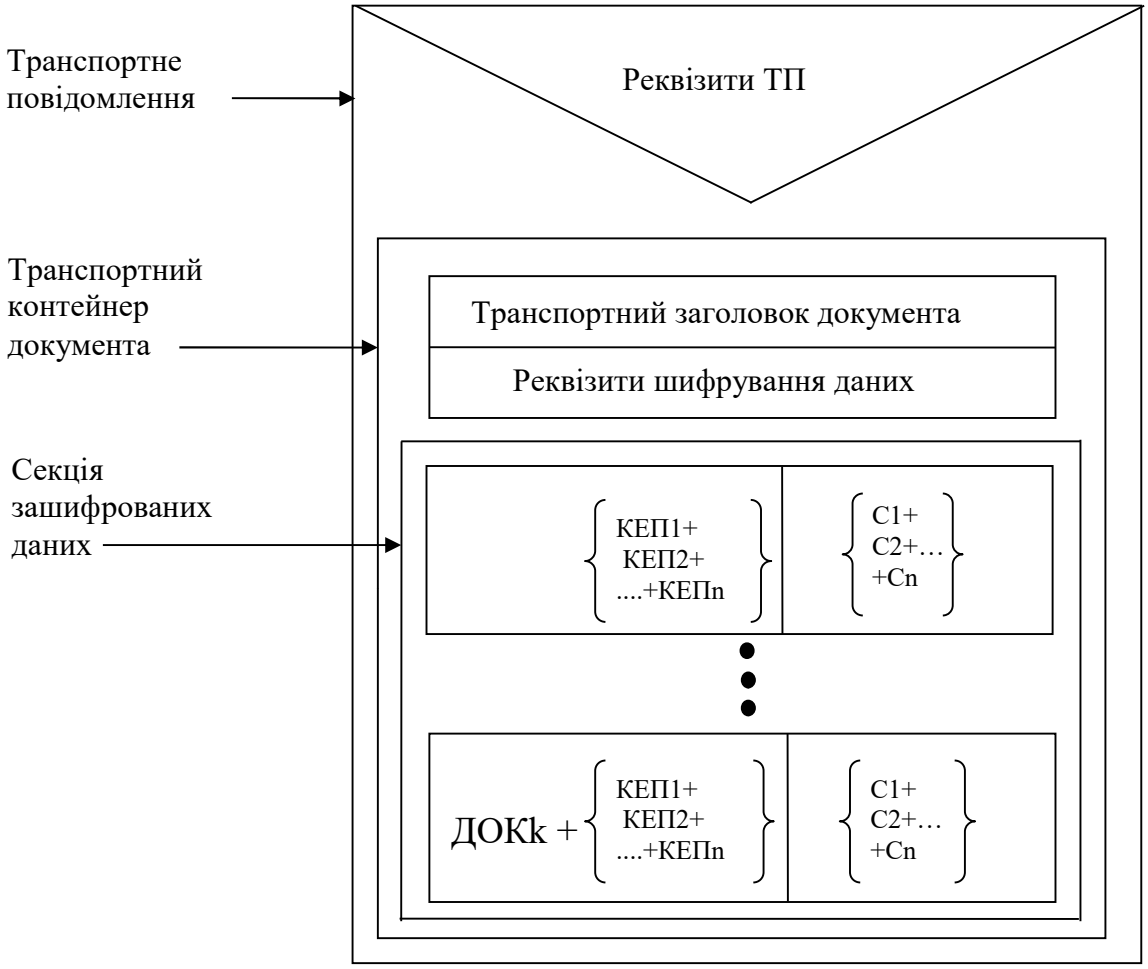

рис. 1

ДОК1, 2, …k – файл електронного документа;
КЕП1, 2, …n – один чи декілька кваліфікованих електронних підписів, якими засвідчений документ;
С1, 2, …n – один чи декілька блоків з сертифікатами ключів КЕП, якими засвідчений документ.

4. Вимоги до структури транспортного контейнера для передачі документів до органу управління державною власністю

4.1. Узагальнений формат транспортного контейнера для передачі документів до органу управління державною власністю

Заголовок транспортного контейнера
Реквізити шифрування даних
Зашифровані дані

4.2. Перелік блоків даних транспортного контейнера для передачі документів до органу управління державною власністю

Сертифікат відправника для зашифрування

Формат блоку сертифіката відправника:

Елемент	Значення
Сигнатура	"CERTCRYPT"
0-символ	
4 байти	розмір сертифіката відправника
Сертифікат відправника	

Блок сертифіката відправника повинний знаходитись перед зашифрованим блоком.

Зашифрований блок даних

Формат зашифрованого блоку даних:

Елемент	Значення
Сигнатура	"UA1_ CRYPT"
0-символ	
4 байти	розмір зашифрованого документа
Зашифрований документ	

Підпис

Формат підпису:

Елемент	Значення
Сигнатура	"UA1_SIGN"
0-символ	
4 байти	розмір буфера підпису та підписаних даних
Буфер підпису та підписаних даних	

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
PRG_TYPE	Назва програмного забезпечення для накладання та перевірки КЕП 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 КЕП 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)	Ні
SUBJECT	тип документа (у кодуванні Win1251) та закінчується символом CHR(13) + CHR(10)	Ні
RESULT	Результат прийому повідомлення (0 - успішно, 1 - помилка, 2 - попередження)	Ні

4.3. Формати повідомлень, які надсилаються в транспортному контейнері для передачі документів до органу управління державною власністю

Формат повідомлення "Документ"

Повідомлення передається від суб'єкта господарювання державного сектору економіки до органу управління державною власністю.

Структура:

1. Транспортний заголовок документа.
2. Блок даних, зашифрований на одержувача, містить і пакет ZIP з документами у форматі XML.

4 Кожен документ в пакеті засвідчено КЕП відправника.

З метою збереження цілісності пакету та контролю за його наповненням всіма обов'язковими для подання формами, відправка звіту відбувається у вигляді пакету. Пакет є zip-архівом з розширенням *.PRZ.

Найменування пакету формується згідно формату транспортного повідомлення.

Пакет містить:

- головний документ у форматі XML, найменування згідно формату імені транспортного повідомлення;
- документи, підпорядковані головному, у форматі XML, найменування згідно формату імені транспортного повідомлення.

Документи в пакеті зв'язані за допомогою тегів з секції <LINKED_DOCS></LINKED_DOCS>.

Увага! Підписи повинні накладатися у такому порядку:

1. Підписана секція (UA1_SIGN) – підписана ключем головного бухгалтера (за умови наявності посади на підприємстві).
2. Підписана секція (UA1_SIGN) – підписана ключем директора (керівника) підприємства.
3. Підписана секція (UA1_SIGN) – підписана ключем печатки підприємства (за умови її наявності).
4. Блок з документом у форматі XML.

Формат повідомлення "Відповідь на документ"

Повідомлення передається від органу управління до суб'єкта господарювання державного сектору економіки.

Повідомлення є відповіддю органу управління на переданий документ. Наприклад, квитанція про призначення реєстраційного номера.

Структура:

1. Підпис органу управління.
2. Транспортний заголовок документа.
3. Блок, зашифрований на суб'єкта господарювання, містить підписи і текст відповіді органу управління.

5. Специфікація криптографічних функцій

5.1 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).

5.2 Загальні вимоги

1. Робота в середовищі Microsoft Windows 98/2000/XP/Vista/7/10/12, 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.

5.3 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.

5.3.1 Функція накладання підпису

Без передачі сертифікату

```
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 з секретним ключем
int pklen	Розмір 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 зберігає в outbuf блок документу з підписом.
Функція повертає 0, коли успішно виконано, або код помилки.

З передачею сертифікату

```
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 з секретним ключем
int pklen	Розмір 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 зберігає в outbuf блок документу з підписом.
Функція повертає 0, коли успішно виконано, або код помилки.

5.3.2 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 з сертифікатом, якщо NULL – в certlen повертається розмір
int* certlen	Розмір буфера з сертифікатом

Функція зберігає в outbuf блок документу без підпису.
Функція зберігає в certbuf блок сертифікату підписанта.
Функція повертає 0, якщо підпис вірний, або код помилки.

5.3.3 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.

5.3.4 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);
```

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 зберігає в outbuf зашифрований блок документу.
Функція повертає 0, коли успішно зашифровано, або код помилки.

5.3.5 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);
```

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

5.3.6 Функція звірки сертифіката з секретним ключем

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

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.

5.3.7 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 (4 байта)
time_t DtEnd	Дата закінчення дії сертифіката (4 байта)
char Issuer[64]	Видавець (найменування)

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

5.4 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
```