ЗАТВЕРДЖЕНО

Наказ Державної митної служби України

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_

**Специфікація структури та формату електронних повідомлень**

**для обміну даними між Держмитслужбою та магазинами безмитної торгівлі**

**1. Загальні питання**

Інформаційний обмін здійснюється через SOAP вебсервіс, розміщений за адресою: <https://sw2.customs.gov.ua/AskCustoms.asmx>.

Назва вебметоду – AskCustoms1.

Запити (Request):

накладається кваліфікований електронний підпис запитувача;

шифруються (AES) сесійним ключем, який пропонує ініціатор запиту і який зашифрований на технологічний ключ Держмитслужби (RSA).

Відповіді (Response):

підписуються технологічним КЕП Держмитслужби (ДСТУ);

шифруються тим самим сесійним ключем.

**2. Формат запиту**

2.1. Запит містить інформацію згідно з таблицею 1.

Таблиця 1. Формат запиту

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Тег** | **Тип та розмір** | **Обов’язковість** | **Примітка** |
| 1 | MessageBody | byte[] | Так | Тіло запиту |
| 2 | MessageType | string(128) | Так | Тип запиту:  UA.SFS.REQ.39.1  (39 – код повідомлення  1 – версія ) |
| 3 | MessageID | guid | Так | Ідентифікатор запиту |
| 4 | Initiator | string(10) | Так | ЄДРПОУ ініціатора запиту |
| 5 | SignCertificate | byte[] | Ні | Сертифікат кваліфікованої електронної печатки, якою підписано запит |
| 6 | Signature | byte[] | Так | Значення КЕП запиту |
| 7 | SessionKey | byte[] | Так | Зашифрований сесійний ключ шифрування |
| 8 | CryptKeyID | guid | Так | Ідентифікатор ключа Держмитслужби, на який зашифровано повідомлення\* |

\*На сьогодні використовується такий ідентифікатор ключа Держмитслужби: 3faf09b8-5b24-4534-b382-9960dca30544.

Він відповідає такому публічному ключу:

<RSAKeyValue><Modulus>uJU/Ccqro+Tysmta1GQ2fZznfJ1bF+lgQmmNnCa1jsVbiA04bvWVyxSRCOBLLwdnpS+PESlg7c3/HqGcjjlhJ5zUPaM1yQF+qhRtaHT1uJDXiaP/ah0xpINQPfeGubst6mkXg3laae+TnbUQSnqV7+jaBV8/CE6+LsJY+0JFq4YmYsCsp8HCxqSbI/+87tY/Pesb2GfMdXx041VZB2DVQnJuUzQjWq+JxMjZSBbG2vSdTjWrIsFepZFOOYBQPTrqrC044V4VbaJVssaP9EO1I6ogI1gA6uzUMyVAEjCE0kkUpZv5wTjFOOkrn+RFovZofFQmxaCgFE6sNSwTd7MyWQ==</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>.

2.2. Тіло запиту формується таким способом:

1) формується XML, який містить дані відповідно до структури та формату, визначених нижче у додатку;

2) отримана послідовність байт підписується кваліфікованим електронним підписом ініціатора запиту. Значення КЕП передається в тезі Signature;

3) генерується випадковий сесійний ключ для алгоритму AES (довжина 256). Значення вектору ініціалізації: { 31, 207, 4, 165, 229, 33, 19, 98, 240, 133, 189, 64, 176, 145, 77, 51 };

4) ключ шифрується за допомогою алгоритму RSA, отримане значення записується в тег SessionKey;

5) стиснутий XML шифрується за допомогою алгоритму AES з використанням сесійного ключа, отримане значення записується в тег MessageBody.

**3. Формат відповіді**

3.1. Відповідь на запит містить інформацію згідно з таблицею 2.

Таблиця 2. Формат відповіді

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Тег** | **Тип та розмір** | **Обов’язковість** | **Примітка** |
| 1 | MessageBody | byte[] | Ні | Тіло відповіді. У разі помилки або якщо відповідь не потрібна – відсутнє |
| 2 | MessageType | string(128) | Так | Тип відповіді:  UA.SFS.RSP.39.1 |
| 3 | SignCertificate | byte[] | Ні | Сертифікат ключа, яким підписано відповідь. Тільки якщо підпис не містить сертифіката. У разі помилки або якщо відповідь не потрібна – відсутній |
| 4 | Signature | byte[] | Ні | Значення КЕП відповіді. У разі помилки або якщо відповідь не потрібна – відсутній |
| 5 | ErrorNumber | numeric(5) | Так | Код помилки. Якщо запит оброблено без помилки – 0 |
| 6 | ErrorMessage | string(2000) | Ні | Текст помилки – при її наявності |
| 7 | MessageID | guid | Так | Ідентифікатор запиту |

3.2. Тіло відповіді формується таким способом:

1) формується XML, який містить дані відповідно до структури та формату, визначених нижче у додатку;

2) отримана послідовність байт підписуються технологічним ключем Держмитслужби. Значення КЕП передається в тезі Signature;

3) стиснутий XML шифрується за допомогою алгоритму AES з використанням сесійного ключа, запропонованого в запиті; отримане значення записується в тег MessageBody.

1. **Формат повідомлень (MessageBody)**

4.1. Формат повідомлення запиту (UA.SFS.REQ.39.1). щодо факту перетину фізичною особою державного кордону України в певний період часу, у визначеному пункті пропуску.

4.1.1. Запит містить інформацію згідно з таблицею 3.

Таблиця 3. Формат запиту UA.SFS.REQ.39.1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Тег** | | **Опис** | | | **Примітка** |
| **UA.SFS.REQ.39.1** | | **Запит щодо факту перетину фізичною особою державного кордону України в певний період часу, у визначеному пункті пропуску** | | | **Кореневий елемент XML документа** |
| **№** | **Тег** | **Опис** | **Тип/Розмір** | **Кардина-льність[[1]](#footnote-1)** | **Примітка** |
| 1 | creation\_date | Дата та час фактичного формування запиту | DateTime | 1 | формат YYYYMMDDTHHMISS (символ «T» – роздільник) |
| 2 | cust\_code | Код місця митного оформлення | varchar(9) | 1 | Класифікатор митних установ2 |
| 3 | person\_psp | Серія та номер паспортного документа для виїзду за кордон | vatchar(20) | 1 |  |
| 4 | person\_cnt | Країна видачи паспортного документа | varchar(2) | 1 | Класифікатор країн  Формат:  ХХ – країна, яка видала закордонний паспорт |

4.2. Формат повідомлення відповіді на запит UA.SFS.REQ.39.1 (UA.SFS.RSP.39.1).

4.2.1. Відповідь містить інформацію згідно з таблицею 4.

Таблиця 4. Формат відповіді UA.SFS.RSP.39.1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Тег** | | **Опис** | | | **Примітка** |
| **UA.SFS.RSP.39.1** | | **Відомості щодо результату опрацювання запиту на перетинання фізичною особою кордону України** | | | **Кореневий елемент XML документа** |
| **№** | **Тег** | **Опис** | **Тип/Розмір** | **Кардинальність** | **Примітка** |
| 1 | creation\_date | Дата та час фактичного формування відповіді | DateTime | 1 | формат YYYYMMDDTHHMISS (символ «T» – роздільник) |
| 2 | result | Результат опрацювання запиту | numeric(1) | 1 | Приклад відповіді:  1 – Фізична особа перетинала кордон  України, за останні 12 годин через зазначений у запиті пункт пропуску.  2 – Фізична особа не перетинала кордон України.  3 – У Держмитслужбу не надходить інформація від АДПСУ |

1. **Приклади повідомлень**

**5.1. UA.SFS.REQ.39.1 (запит)**

<?xml version="1.0" encoding="windows-1251"?>

<UA.SFS.REQ.39.1>

<req\_date>20231009T111248</req\_date>

<cust\_code>UA305060</cust\_code>

<person\_psp>AB123456</person\_psp>

<person\_cnt>UA</person\_cnt>

</UA.SFS.REQ.39.1>

**5.2. UA.SFS.RSP.39.1 (відповідь)**

<?xml version="1.0" encoding="windows-1251"?>

<UA.SFS.RSP.39.1>

<creation\_date>20231016T101248 </creation\_date>

<result>1</result>

</UA.SFS.RSP.39.1>"

**Заступник директора Департаменту**

**з питань цифрового розвитку, цифрових**

**трансформацій і цифровізації Ігор СМІРНОВ**

1. Кардинальність: ? = (0,1); 1 = 1; \* = (0…n); + = (1…n).

   2 Класифікатор Державної митної служби України, її територіальних органів та їх структурних підрозділів. [↑](#footnote-ref-1)