Проверка структуры xml-ответа от СЭДО подписанная сертификатом СФР

При отправке сообщения с ответом из СЭДО к страхователю, оно проходят двухэтапную обработку: сначала на него накладывается ЭП СФР, а затем оно шифруются.

Структура подписанного сообщения описана в спецификации СЭДО в разделах 3.3 (подписание) и 4.2 (шифрование). Каркас сообщения определенный по стандартам SOAP и представляет собой следующий XML-документ:

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

<soapenv:Header>

</soapenv:Header>

<soapenv:Body>

</soapenv:Body>

</soapenv:Envelope>

, где блок Header – содержит служебную информацию, а блок Body – смысловые данные сообщения.

При наложении подписи в соответствии со стандартом OASIS Web Service Security: SOAP Message Security 1.1 внутри блока Header формируется структура данных, предназначенная для передачи информации об ЭП.

Внутри блока **Header** располагается блок **Security**, принадлежащий пространству имен http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd, содержит в себе информацию, необходимую для проверки целостности сообщения и его отправителя.

Блок **Security** состоит из следующих элементов:

**Signature** - содержит информацию об электронной подписи сообщения

**BinarySecurityToken** - содержит публичный сертификат СФР в формате X509v3.

Порядок блоков **Signature** и **BinarySecurityToken** не важен, если они не менялись после шифрования ответного сообщения, иначе вычисленное значение хэш суммы не совпадет и будет ошибка.

Порядок расположения блоков в ответе от СЭДО:

1) было в Соцстрахе:

**BinarySecurityToken** за ним **Signature**

2) стало в ЕЦП:

**Signature** за ним **BinarySecurityToken**