



101000, г. Москва,  
Армянский переулок д. 9 стр.1, оф.505  
Тел.: +7 (495) 780-52-68  
[www.afinserv.ru](http://www.afinserv.ru)

Крипто-сервис «AFS-CryptoGate»

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ (ПРОГРАММИСТА)

# **КРИПТО-СЕРВИС «AFS-CRYPTO GATE»**

## **Руководство пользователя (программиста)**

**Версия: 1.0**

**Листов: 17**

## СОДЕРЖАНИЕ

1	ОБЩИЕ СВЕДЕНИЯ.....	4
1.1	Руководящие документы.....	4
1.2	Описание электронного крипто-сервиса «AFS-CryptoGate».....	4
1.3	Операции электронного сервиса .....	4
1.4	Сценарии использования.....	5
2	ХАРАКТЕРИСТИКА ПРОГРАММЫ .....	5
2.1	Операция «Наложение электронной подписи в формате XML digital signature».....	5
2.1.1	Общие сведения .....	5
2.1.2	Описание входных параметров .....	5
2.1.3	Описание выходных параметров.....	6
2.1.4	Коды возвратов .....	6
2.1.5	Примеры.....	6
2.2	Операция «Формирование хэша xml-документа» .....	9
2.2.1	Общие сведения .....	9
2.2.2	Описание входных параметров .....	9
2.2.3	Описание выходных параметров.....	10
2.2.4	Коды возвратов .....	10
2.2.5	Примеры.....	10
2.3	Операция «Проверка электронной подписи в формате XML digital signature».....	11
2.3.1	Общие сведения .....	11
2.3.2	Описание входных параметров .....	11
2.3.3	Описание выходных параметров.....	12
2.3.4	Коды возвратов .....	12
2.3.5	Примеры.....	12
3	ПРИЛОЖЕНИЯ.....	14
3.1	Описание сервиса (WSDL).....	14
3.2	Описания справочников .....	16

## ИЗМЕНЕНИЯ

Версия	Дата	Автор	Изменения
1.01	12.10.2018	Ходырев Н.А.	Первая версия документа

## ТЕРМИНЫ/СОКРАЩЕНИЯ

Термин/сокращение	Описание
Поставщик	Организация-владелец электронного сервиса
СМЭВ	Система межведомственного электронного взаимодействия
ЭП	Электронная подпись
SOAP	Simple Object Access Protocol - протокол обмена структурированными сообщениями в распределённой вычислительной среде.
XML	eXtensible Markup Language — расширяемый язык разметки.
XSD	XML Schema definition - язык описания структуры XML документа.
WSDL	Web Services Description Language — язык описания веб-сервисов.
XMLDSIG	Цифровая подпись в формате XML

# 1 ОБЩИЕ СВЕДЕНИЯ

## 1.1 Руководящие документы

Нормативно-правовые документы:

- Приказ ФСБ России от 13 ноября 1999 г. № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

Технологические стандарты:

- Методические рекомендации по работе с Единой системой межведомственного электронного взаимодействия версия 3.4.0.3. М.: 2017, 151 с. (URL: <https://smev3.gosuslugi.ru/portal> ).
- W3C. Latest SOAP versions. URL: <https://www.w3.org/TR/soap/>.
- W3C. XML Signature WG. URL: <https://www.w3.org/Signature/>.

## 1.2 Описание электронного крипто-сервиса «AFS-CryptoGate»

<b>Наименование:</b>	Крипто-сервиса «AFS-CryptoGate» далее Сервис
<b>Назначение:</b>	Сервис предназначен для: <ul style="list-style-type: none"><li>• формирование хэша xml-документа,</li><li>• наложение электронной подписи (ЭП) на xml-документ направляемый в СМЭВ,</li><li>• проверку ЭП xml-документа, получаемого от СМЭВ.</li></ul>
<b>Условия применения</b>	Для функционирования сервиса необходимы следующие прикладное программное обеспечение: <ul style="list-style-type: none"><li>– Операционная система поддерживающая спецификации Sun Java 2™ Virtual Machine и установку КриптоПро JCP 2.0 (Linux, Microsoft Server)</li><li>– КриптоПро JCP 2.0</li><li>– Установленная JVM 1.7 и выше</li></ul>

## 1.3 Операции электронного сервиса

Крипто-сервис «AFS-CryptoGate» обеспечивает:

- проверку электронной подписи в формате XML digital signature;
- наложение электронной подписи в формате XML digital signature;
- формирование хэша xml-документа

Метод	Назначение
SignSMEV3_EPOVRequest	Принимает на вход xml сообщение, id подписываемого сообщения, имя сертификата, которым требуется подписать(или просто имя сертификата) и возвращает подпись xml элемента в виде xmldsig <Signature>..</Signature>
GenerateHash	Принимает на вход xml сообщение, id xml элемента, по которому нужно получить hash и возвращает hash элемента.
VerifySMEV3_EPOVRequest	Принимает на вход xml сообщение и возвращает результат проверки

## 1.4 Сценарии использования

Внешние системы вызывают методы данного сервиса и синхронно получают результат подписи, хэш, результат проверки сертификата и/или подписи.

## 2 ХАРАКТЕРИСТИКА ПРОГРАММЫ

### 2.1 Операция «Наложение электронной подписи в формате XML digital signature»

#### 2.1.1 Общие сведения

<b>Код операции:</b>	SignSMEV3_EPOVRequest
<b>Наименование операции:</b>	Наложение электронной подписи в формате XML digital signature
<b>Назначение операции:</b>	Наложение электронной подписи в формате XML digital signature

#### 2.1.2 Описание входных параметров

Входные данные: SignSMEV3\_EPOVRequest

№	Код параметра	Описание параметра	Обязательность	Способ заполнения/Тип	Комментарий
1	id	Идентифкатор	+	String	Xpath выражение по

		атрибута, по которому вычисляется корневой узел сообщения, которое должно быть подписано			которому вычисляется узел <code>"/*[@Id="{id}"]"</code>
2	Data	Xml сообщение в формате base64	+	Base64	Бинарные данные в кодировке base64
3	CertName	Имя сертификата с помощью которого должна быть наложена подпись	-	String	Имя сертификата латиницей (alias). Если имя сертификата не найдено, то подписание будет произведено сертификатом по умолчанию.

### 2.1.3 Описание выходных параметров

#### Выходные данные: SignSMEV3\_EPOVResponse

№	Код параметра	Описание параметра	Обязательность	Способ заполнения/Тип	Комментарий
1	DataWithSignature	Электронная подпись по формату <code>xmldsignature</code>	+	Base64	Бинарные данные в кодировке base64
2	Date	Дата формирования ЭП	+	Date	YYYY-mm-ddTНН:mm:ss.sss+utc

### 2.1.4 Коды возвратов

См. раздел 3.2

### 2.1.5 Примеры

Запрос







```

cjm0MTEiLz48ZHM6RGlnZXN0VmFsdWU+QlpMUXdFahViZCt1MEVsUTd5Zi9jWDFtQ05DQ24yZ2I1TmxuRzQvUHpKaz08L2R
z0kRpZ2VzZdFzhbHV1PjwvZHM6UmVmZXJlbnMlPjwvZHM6U2l1bnMkSv5mbz48ZHM6U2l1bnMkF0dXJlVmFsdWU+bDB5QW10Ml
hQRUNwaHRPa3B3V05PUWgxcXRIa29DMThTR0Y5V05DVUxSRStaaE90SXRNu9tccG1iMD1rYWhne1YzWUhzbtGRmdoZzF3V
FhyeklMbhc9PTwvZHM6U2l1bnMkF0dXJlVmFsdWU+PGRz0ktleUluZm8+PGRz0lg1MD1EYXRhPjxkczpYNTA5Q2VydGlmawNn
dGU+TU1JSG1EQ0NCMGVnQXdJQkFnSVFBZnBhaTY1c2Y1SG5FYUo5UGV4OWZ6QUlCZ11xaFFNQ0FnTXdnZ0dkTVJnd0ZnWUZ
Lb1VEWkFFU0RURXhNVEkyTlRFd01UYzBNREV4R2pBWUJnZ3FoUU1EZ1FNQkFSSU1NREF5TmPnMU9EQTF0VEUyTVFzd0NRWU
RWUVFHRXdKU1ZURXhNqzhQTFVRUNBd29Na1lnMEtIUmd0Q3cwTExSZ05DKzBML1F2dEM3MF16UmdkQzYwTGpRdVNEUXV0R
0EwTERRdVRFZE1Cc0dBMVVFQnd3VTBLSFJndEN3MEXmUmd0QyswTC9RdnRDnZBZd3hKVEFqQmdOVkJBa01ITkdEMExzdU1O
Q2YwTGpSZ05DKzBMUFF2dEN5MEXBc01ERTRMell4T3pBNUJnTlZCQXNNTXRdZTBZTFF0TkMxMEXzZzBZUFF0TkMrMF1IUmd
0QyswTExRdGRHQTBZL1JqdEdKMEqxUVTRFJodEMxMEwzUmd0R0FNvk3VHdZRFZRUUtERWpRaz1DYTBLTvcwS0hRbWlBaT
BKclJnTkn3MEXYUXN0QyswTgtnMF1iUXRkQzkWwUXSZ0NEUXVOQzkWwVRRdnRHQTBMe1JndEMxMF1YUXZkQyswTHZRdnRDe
jBma1F1U014VhPctkJnTlZCQU1NUnRDVDBKclFveURRb2RDYU10Q2EwWURRc05DMTBMFF2dEM1SU5HRzBMWFF2ZEEdMFLB
ZzBma1F2ZEEdMEw3Umd0QzgwUwRdGRHRjBMM1F2dEM3MEw3UXM5QzQwTgT3SGhjTk1UY3dPREV3TURjMU5ERTFXaGNOTVR
neE1URXdNRGd3TkrFMvdqQ0NBVHN4R2pBWUJnZ3FoUU1EZ1FNQkFSSU1NREF5TmPnMU9EQTF0VEUyTVJnd0ZnWUZLb1VEWk
FFU0RURXhNVEkyTlRFd01UYzBNREV4Q3pBSkJnTlZCQVlUQWxKvK1URXdMdl1EVlFRSURDZ310aURRb2RHQzBMRFFzdEdBM
Ew3UXY5QyswTHZSak5HQjBMc1F1TkM1SU5DNjBZRFzTkm1TVIwd0d3WURWUVFIREJUW9kR0MwTERRc3RHQTBMN1F2OUMr
MEX2UmpER1JNRTthQTFVRUNneEkWslBRbXRdAk10Q2gWsm9nSXRdYTBZRFzTkmxMEXMuxZ0QzVJTKdHMEXYUXZkR0MwWUF
nMEXqUXZkR0UwTddSZ05DODBZTFF0ZEEdGMEwzUXZ0QzCwTddRcZ1DNDBMa21NVkV3VHdZRFZRUURERWpRaz1DYTBLTvcwS0
hRbWlBaTBKclJnTkn3MEXYUXN0QyswTgtnMF1iUXRkQzkWwUXSZ0NEUXVOQzkWwVRRdnRHQTBMe1JndEMxMF1YUXZkQyswT
HZRdnRDejBma1F1U013WxpBY0JnWXFoUU1DQWhNd0VnUHLb1VEQWdJa0FBWUHLb1VEQWdJZUFRTkRBQVJBWnhkM0ZFQTNi
MUZCRG5DNkhPVE1kS3FTbEzVWhp4K3pPaVfHUGhRkhhMhBRdDBIRm1nd1FoSWtoA1I3d1RRZVdrb091VHJ1VH15RFcyd1p
xUjdxY0tPQ0E3MHdnZ081TUE0R0ExVWRed0VCL3dRRUF3SUU4REFkQmdOVkhRNEVGZ1FVNUdsKzJNait0dEdHdTZJChpxNE
JUyzZEcFpJd2dnRmpCZ05W5FNRRWdnRmFNSU1CVm9BVVY3bnNBsk12c0FPan1lWDFrYVg2RnN5RGRtt2hnZ0VvcE1JQkpUQ
0NBu0V4R2pBWUJnZ3FoUU1EZ1FNQkFSSU1NREEzTnpF05EYzBNemMxTVJnd0ZnWUZLb1VEWkFFU0RURXdORGMzTURJd01q
WTNNREV4SGpBY0Jna3Foa21HOXcwQkNRRVdEM1JwZEVcdGFXXpkbmXoZwk1eWRURThNRG9HQTFVRUNRd3pNVEkxTXpjMU1
OQ3pMaURRbk5DKzBZSFF1dEN5MEXBzZBZUFF1eTrNMEtMuxN0QzEwWURS2ZRDnJBMRFJqeURRdEM0M01d3dLZ11EVlFRS0
RDUFFuTKM0MEwzUXV0QyswTHpSZ2RDeTBZL1F0OUdNSU5DZzBMN1JnZEdCMEqxUXVERVZNQk1HQTFVRUJ3d00wSnpRdnRHQ
jBMc1FzdEN3TVJ3d0dnWURWUVFJREJNM055RFFzeTrNMEp6UXZ0R0IwThJRc3RDd01Rc3dDUV1EVlFRR0V3S1NWVEViTUJr
R0ExVUVBd3dTMEtQUXBPqXhJTKNZMEtFzZBKUFvOUNTz2hFRXFCNUFCYwTzWE1MbUVUL0w0eTdBClRBDUJnTlZIU1VFSnp
BbEJnZ3JCZ0VGQ1FjREFnWUHLb1VEQWdJaUJnWU1Ld11CQ1FVSEF3UudCaXFGQTJRQ0FqQWRCZ05W5FNBRUZqQVNVQWdHQM
1xRkEyUnhBVEFJQmdZcWhRTmtjUU13SFFZRFZSMFJCQ113RktBU0Jnb3JCZ0VFQV1JM0ZBSURvQV1QWdBd01JSUJDQV1GS
29VRFpIQUVnZjR3Z2ZzTUt5TFFtdEdBMEqxUXY5R0MwTddRbj1HQTBMNGdRMU5RSW1BbzBMTFF0ZEEdBMFLIUXVOR1BJRE11
T1NrTUtpTFFtdEdBMEqxUXY5R0MwTddRbj1HQTBMNGcW51BRcG1JZzBMTFF0ZEEdBMFLIUXVOQzRjRE11TUF4UDBLSFF0ZEEd
BMFLMUXVOR0UwTgPRdXRdDzBZSwcWUHRdnRDKzBZTFFzdEMxMF1MUmdkR0MwTExRdU5HUE1PS0VsaURRb2RDa0x6RX10Qz
B5T1RNNU10QyswWU1nTVRVdU1ERXVNAkF4T1F4UDBLSFF0ZEEdBMFLMUXVOR0UwTgPRdXRdDzBZSwcWUHRdnRDKzBZTFFzd
EMxMF1MUmdkR0MwTExRdU5HUE1PS0VsaURRb2RDa0x6RX1PQzB5T0RneE10QyswWU1nTVRJdU1EUXVNAkF4TmPBMkJnVXFo
UU5rYndRdERDc2kWSnJSZ05DNDBML1JndEMrMEovUmd0QytJRu5UVUNJZ0t0Q3kwtFhSZ05HQjBma1JqeUF6TGprcE1FSUd
BMVVKShdRN01Ea3dONkExb0RPR01XaDBKSEE2THk5amFYUXRjMnN1Y25VdmRYQnNiMkZrY3k5bWFXeGxjeTkwXk5amFYUX
RjMnN0TWpBeE55NwpjbxD3S3dZRFZSMFFCQ1F3SW9BUE1qQXhOekE0TVRBD056VTBNVfJhZ1E4eU1ERTRNVEV4TURBM05UU
XhORm93Q0FZR0tvVURBZ01EQTBfQVY5U1R6QnNaVmV2VG02dGttVjViZ1Zd0FqaG0zbCsvdVvAbDdWeFZLUEN0QUxKbkJw
bXA3YnM3UGQ0RzNtVU9weEtqcZlkRENvVXJEbFFyOGF2QmhBPT08L2Rz01g1MD1DZXJ0awZpY2F0ZT48L2Rz01g1MD1EYXR
hPjwvZHM6S2V5S5mbz48L2Rz01NpZ25hdHVyZT4=</DataWithSignature>
    <Date>2018-10-14T16:17:00.277+03:00</Date>
  </ns2:SignSMEV3_EPOVResponse>
</S:Body>
</S:Envelope>

```



## 2.2 Операция «Формирование хэша xml-документа»

### 2.2.1 Общие сведения

<b>Код операции:</b>	GenerateHash
<b>Наименование операции:</b>	Формирование хэша xml-документа
<b>Назначение операции:</b>	Формирование хэша xml-документа

### 2.2.2 Описание входных параметров

**Входные данные:** GenerateHashRequest

№	Код параметра	Описание параметра	Обязательность	Способ заполнения/Тип	Комментарий
1	id	Идентифкатор атрибута, по которому вычисляется корневой узел сообщения, которое должно быть подписано	+	String	Xpath выражение по которому вычисляется узел "/*[@Id="{id}"]"
2	Data	Xml сообщение в формате base64	+	Base64	Бинарные данные в кодировке base64
3	Algorithm	Алгоритм расчета хеш функции	+	Enum [3411, 3411_2012_256, 3411_2012_512]	<b>3411</b> расчет хеш по ГОСТ ГОСТ Р 34.11-94 <b>3411_2012_256</b> расчет хеш ГОСТ Р 34.11-2012 с длиной хэш кода 256 бит <b>3411_2012_512</b> расчет хеш ГОСТ Р 34.11-2012 с длиной хэш кода 512 бит



```
</eds:GenerateHash>
</soapenv:Body>
</soapenv:Envelope>
```

### Ответ на запрос в случае успешного исполнения

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns2:GenerateHashResponse xsi:type="ns2:Hash" xmlns:ns2="http://afs-eds.ru/service/eds"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <Hash>IQVvWJPBbeKEVyVdLqmUV7X1oePN1pbmbUa001fxcqt112EuKN5JoX2tdX2BADO2mZ2BFr2jNrmp0ug+I8ePGg==<
      /Hash>
    </ns2:GenerateHashResponse>
  </S:Body>
</S:Envelope>
```

## 2.3 Операция «Проверка электронной подписи в формате XML digital signature»

### 2.3.1 Общие сведения

<b>Код операции:</b>	VerifySMEV3_EPOV
<b>Наименование операции:</b>	Проверка электронной подписи в формате XML digital signature
<b>Назначение операции:</b>	Проверка электронной подписи в формате XML digital signature

### 2.3.2 Описание входных параметров

#### Входные данные: VerifySMEV3\_EPOVRequest

№	Код параметра	Описание параметра	Обязательность	Способ заполнения/Тип	Комментарий
1	DataWithSignature	Подписанное сообщение в формате XML	+	Base64	Бинарные данные в кодировке base64, поиск подписи производится по xpath выражению "//*[contains(local-name(), 'Signature')]"
2	VerifySignature	Флаг, означающий	-	boolean	true/false

		требуется ли проверять только подпись или еще и статус сертификата подписи			
3	Date	Дата на которую проверять статус сертификата	-	Date	YYYY-mm-ddTНН:mm:ss.sss+utc

### 2.3.3 Описание выходных параметров

Выходные данные: VerifySMEV3\_EPOVResponse

№	Код параметра	Описание параметра	Обязательность	Способ заполнения/Тип	Комментарий
1	Code	Результат проверки подписи и, если требовалось, сертификата	+	Int	См. раздел 3.2 коды возвратов
2	Description	Текстовое описание ошибки или причины неудачной проверки (если есть)	-	String	

### 2.3.4 Коды возвратов

См. раздел 3.2

### 2.3.5 Примеры

Запрос

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:eds="http://afs-eds.ru/service/eds">
  <soapenv:Header/>
  <soapenv:Body>
    <eds:VerifySMEV3_EPOVRequest>
      <DataWithSignature>PGRz01NpZ25hdHVyZSB4bWxuczpkcz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnIyI+PGRz01NpZ25lZEluZm8+PGRz0kNhbM9uawNhbG16YXRpb25NZXRpb2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzEwL3htbC1leGMtYzE0biMiLz48ZHM6U2lnbmF0dXJlTWV0aG9kIEFsZ29yaXR0bT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8wNC94bWxkc2lnLW1vcuUjZ29zdHIzNDEwMjAwMS1nb3N0c2Jm0MTEiLz48ZHM6UmVmZXJlbmNlIFVSST0iI0NPT1NfM2Q5NjczMzgtM2JiZS00YTk0LTg0MjItNWZiMjcyN2NkZjNhIj48ZHM6VHJhbnNmb3Jtcz48ZHM6VHJhb
```





Крипто-сервис «AFS-CryptoGate»

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ (ПРОГРАММИСТА)

```
nNmb3JtIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI2VudmVsb3B1ZC1zaWduYXR1cmUi
Lz48ZHM6VHJhbnNmb3JtIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS8xMC94bWwtZXhJLWmXNG4jiI8+PGR
z0lRyYW5zZm9ybSBbbGdvcm10aG09InVybjovL3NtZXytZ292LXJ1L3htbGRzaWcudHJhbnNmb3JtIi8+PC9kc3pUcmFuc2
ZvcmlzPjxkc3pEaWdlc3RNZXR0b2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGRzaWcudHJhbnNmb3JtIi8+PC9kc3pUcmFuc2
SNnb3N0c3pUcmFuc2ZvcmlzPjxkc3pEaWdlc3RNZXR0b2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGRzaWcudHJhbnNmb3JtIi8+PC9kc3pUcmFuc2
az08L2RzOkRpZ2VzdFZhbHVlPjwvZHM6UmVmZXJlbnNlPjwvZHM6U2lnbmVksW5mbz48ZHM6U2lnbmF0dXJlVmFsdWU+Rnh
RR0Zw083NnhTL1VwREl0WjVoUkFIYnUzVElGS3N2OT16M0k0WctialRVRTVKSm9QejNjdUdLZE9TYTlHL3RQcldwR2gwdk
9hWFJTZDZTeXJFM3c3pUcmFuc2ZvcmlzPjxkc3pEaWdlc3RNZXR0b2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxLzA0L3htbGRzaWcudHJhbnNmb3JtIi8+PC9kc3pUcmFuc2
G1maWNhdGU+TU1JSg1EQ0NCMGVnQXkJQkFnSVFBNzBhaTY1c2Y1SG5FYUo5UGV4OWZ6QUlCZ11xaFFNQ0FnTXdnZ0dkTVJn
d0ZnWUZLb1VEWkFFU0RURXhNVEkyTlRFd01UYzBNREV4R2pBUWJnZ3FoUU1EZ1FNQkFSSU1NREF5TmPnMU9EQTF0VEUyTVF
zd0NRWURWUVFHRXdKU1ZURXhNzQzhQTFVRUNBd29Na1lnMeTIUmd0Q3cwTExS05DKzBML1F2dEM3MF16UmdkQzYwTgRdV
NEUXV0R0EwTERRdVRFZE1Cc0dBmVVFQnd3VTBLSFJndEN3MEXmUmd0QyswTC9RdnRDNzBZd3hKVEFqQmd0VkJBa01ITkdEM
ExzdU1OQ2YwTgPSZ05DKzBmUff2dEN5MEXBc01ERTRMel14T3pBNUJnTlZCQXNNTXRdZTBZTFF0TkMxMEXzZBZUFF0TkMr
MFIUmd0QyswTExRdGRHQTBLZ1JqdEdKMEqxUXVTRFJodEMxMEwzUmd0R0FNVkV3VhdZRFZRuUeRwPraz1DYTB1TWCwS0h
RbW1BaTBKc1JnTkn3MEXYUXN0QyswTgtnMFIUxRkQzkwUxSZ0NEUXVOQzkwVRRdnRHQTBMel1JndEMxMF1YUXZkQyswTH
ZRdnRDejBma1F1U014VHPCtkJnTlZCQU1NunRDVDBKc1FveURRb2RDYU1OQ2EwWURRc05DMTBMtFF2dEM1SU5HRzBMWFF2Z
EdDMF1BZzBma1F2ZEEdFMEw3Umd0QzgwUxRdGRHRjBMM1F2dEM3MEw3UXM5QzQwTgt3SGhjTk1UY3dPREV3TURjMU5ERTFX
aGNOTVRneE1URXdNRGd3TkrFmVdqQ0NBVHN4R2pBUWJnZ3FoUU1EZ1FNQkFSSU1NREF5TmPnMU9EQTF0VEUyTVJnd0ZnWUZ
Lb1VEWkFFU0RURXhNVEkyTlRFd01UYzBNREV4Q3pBSk1JnTlZCQV1UQWxkV1URXdMdl1EV1FRSurdZ310aURRb2RHQzBMRF
FzdEdBMEw3UXY5QyswTHZSak5HQjBMc1F1TkM1SU5DNjBZRFfzTkM1TVIwd0d3WURWUVFIREJUuW9kR0MwTERRc3RHQTBMN
1F2OUMrMEX2UmpER1JNRTthHQTfVRUNneEkW1BRbXRdAK10Q2gW5m9nSXRdYTBZRFfzTkMxMEXMuxZ0QzVJTKdHMEYUUXZk
R0MwUUFnMEXqUXZkR0UwTdsZ05D0DBZTFF0ZEEdGMEwzUXZ0QzCWtdDrc1DNDBMa21NvkV3VhdZRFZRuURERwPraz1DYTB
LTWCwS0hRbW1BaTBKc1JnTkn3MEXYUXN0QyswTgtnMFIUxRkQzkwUxSZ0NEUXVOQzkwVRRdnRHQTBMel1JndEMxMF1YUX
ZkQyswTHZRdnRDejBma1F1U013WXPBY0JnXWFOUU1DQWhNd0VnUHLb1VEQWdJa0FBWUHLb1VEQWdJZUFRTkRBQVJBWnhkM
0ZFQTNiMUZCRG5DNkhPVE1kS3FTbEzWVhP4K3pPaVfHUGhiRkhhMHRdDBIRm1nd1FoSWtoaT13d1RRZVdrb091VHJ1VH15
RFcyd1pxUjdxY0tPQ0E3MHdnZ081TUE0R0EXVWRed0VCL3dRRUF3SUU4REFkQmd0VkhRNEVGZ1FVNUdsKzJNait0dEdHdTZ
JcHpxNEJUyZzEcFpJd2dnRmpCZ05WFSNNRwdnRmFNSU1CVm9BVVY3bnNBSk12c0FPanNlWDFrYVg2RnN5RGRTT2hnZ0VwcE
1JQkpUQ0NBu0V4R2pBUWJnZ3FoUU1EZ1FNQkFSSU1NREEzTnpF05EYzBNemMxTVJnd0ZnWUZLb1VEWkFFU0RURXdORGmZt
URJd01qWtNNREV4SGpBY0Jna3Foa21HOXcwQkNRRVdEM1JwZEVcdGFXNXpkbmxoZWk1eWRURThNRG9HQTfVRUNRd3pNVekx
TXpjMU1OQ3pMaURRbk5DKzBZSFF1dEN5MEXBZzBZUFF1eTrNMEtmUXN0QzEwWURS22RDnJBMRFJqeURRdEM0M01Td3dLZ11
EV1FRS0RDUFFuTkM0MEwzUXV0QyswThPSZ2RDeTBZL1F0UdNSU5DZzBMN1JnZEdCMEqxUXVERVZNQk1HQTFVRUJ3d00wSn
pRdnRHQjBMc1FzdEN3TVJ3d0dnWURWUVFJREJNM055RFFzeTrNMEp6UXZ0R0IwTHJRc3RDd01Rc3dDUV1EV1FRR0V3S1NWV
EV1TUJrR0EXVUVBd3dTMETQUXBPQXhJTKNZMETfZzBKUFFvOUNTz2hFRXFcNUFCYwtZWE1MbUVUL0w0eTdBc1RBdUJnTlZI
U1VFSnpBbEJnZ3JCZ0VGQ1FjREFnWUHLb1VEQWdJaUJnWU1Ld1lCQ1FVSEF3UUDCaXFGQTJRQ0FqQWRCZ05WFSNBRUZqQV
NQWdHQmlxRkEyUnhBVEFJQmdZcWhRTmtjUU13SFFZRFZSMFJCQ113RktBU0Jnb3JCZ0VFQV1JM0ZBSURvQVFLQWdBd01JSU
JDQV1GS29VRFpIQUVnZjR3Z2ZzTUt5TFFtdEdBMEqxUXY5R0MwTDdRbjlHQTBMGdRMU5RSW1BbzBMTFF0ZEEdBMF1IUXVOR
1BJRE11T1NrTUtPFFtdEdBMEqxUXY5R0MwTDdRbjlHQTBMGcW1BRcG1JZzBMTFF0ZEEdBMF1IUXV0QzRjRE11TUF4UDBL
SFF0ZEEdBMF1MuxVOR0UwTgPrdXRdDzBZSwcWUHLdRDKzBZTFFzEdEMxMF1MUMdkR0MwTExRdU5HUE1PS0VsaURRb2RDa0x
6RX1OQzB5T1RNNU1OQyswWU1nTVRVdu1ERXVnakF4T1F4UDBLSFF0ZEEdBMF1MuxVOR0UwTgPrdXRdDzBZSwcWUHLdRDKz
BZTFFzEdEMxMF1MUMdkR0MwTExRdU5HUE1PS0VsaURRb2RDa0x6RX1PQzB5T0Rne1LOQyswWU1nTVRJdU1EUXVnakF4TmPBM
k1nVXFoUU5rYndRdERdc2kwSnJSZ05DNDBML1JndEMrMEovUmd0QytJRU5UVUNJZ0tOQ3kwTfhSZ05HQjBma1JqeUF6TGpr
cE1FSudBMVVKSHdRN01Ea3dONkExb0RPR01XaDbkSEEThk5amFYUXRjMnN1Y25VdmRYQnNiMkZrY3k5bWfXEGxeTkxWkX
5amFYUXRjMnN0TwpBeE55NwpjBXd3S3dZRFZSMFQC1F3SW9BUE1qQXhOekE0TVRBd056VTBNVFJhZ1E4eU1ERTNVEV4TU
RBM05UUXhORm93Q0FZr0tVURBZ01EQTBfQVY5U1R6QnNaVm2VG02dGttVjViZFlZd0FqaG0zbCsvdVvAbDdWeFLZUEN0Q
UxKbkJwbXA3YnM3UG0RzNtVU9weEtqcZlKRENvXJEbFFyOGF2QmhBPT08L2Rz01g1MD1DZXJ0aWZpY2F0ZT48L2Rz01g1
MD1EYXRhPjwvZHM6S2V5SW5mbz48L2Rz01NpZ25hdHVyZT4=
```

</DataWithSignature>

```
<VerifySignature>true</VerifySignature>
<Date>2018-10-12T16:18:46.658+03:00</Date>
</eds:VerifySMEV3_EPOVrequest>
</soapenv:Body>
</soapenv:Envelope>
```





### Ответ на запрос в случае успешного исполнения

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns2:VerifySMEV3_EPOVResponse xsi:type="ns2:ErrorEDS" xmlns:ns2="http://afs-eds.ru/service/eds" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <Code>0</Code>
      <Description/>
    </ns2:VerifySMEV3_EPOVResponse>
  </S:Body>
</S:Envelope>
```

### Ответ на запрос с кодом возврата 3

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns2:VerifySMEV3_EPOVResponse xsi:type="ns2:ErrorEDS" xmlns:ns2="http://afs-eds.ru/service/eds" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <Code>5</Code>
      <Description>Срок действия одного из сертификатов цепочки истек, или еще не наступил</Description>
    </ns2:VerifySMEV3_EPOVResponse>
  </S:Body>
</S:Envelope>
```

## 3 ПРИЛОЖЕНИЯ

### 3.1 Описание сервиса (WSDL)

```
<?xml version="1.0" encoding="UTF-8"?><!-- Published by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is JAX-WS RI 2.2.4-b01. --><!-- Generated by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is JAX-WS RI 2.2.4-b01. -->
<definitions xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:wsp1_2="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:tns="http://afs-eds.ru/service/eds" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.xmlsoap.org/wsdl/" targetNamespace="http://afs-eds.ru/service/eds" name="EDSService">
  <wsp:Policy wsu:Id="EDSPortBinding_MTOM_Policy">
    <ns1:OptimizedMimeSerialization xmlns:ns1="http://schemas.xmlsoap.org/ws/2004/09/policy/optimizedmimeserialization" wsp:Optional="true"></ns1:OptimizedMimeSerialization>
  </wsp:Policy>
</types>
<xsd:schema>
```



```
<xsd:import namespace="http://afs-eds.ru/service/eds"
schemaLocation="http://localhost:8305/EDSService?xsd=1"></xsd:import>
</xsd:schema>
</types>
<message name="GenerateHash">
<part name="GenerateHash" element="tns:GenerateHash"></part>
</message>
<message name="GenerateHashResponse">
<part name="parameters" element="tns:GenerateHashResponse"></part>
</message>
<message name="VerifySMEV3_EPOV">
<part name="parameters" element="tns:VerifySMEV3_EPOVRequest"></part>
</message>
<message name="VerifySMEV3_EPOVResponse">
<part name="parameters" element="tns:VerifySMEV3_EPOVResponse"></part>
</message>
<message name="signSMEV3_EPOV">
<part name="parameters" element="tns:SignSMEV3_EPOVRequest"></part>
</message>
<message name="signSMEV3_EPOVResponse">
<part name="parameters" element="tns:SignSMEV3_EPOVResponse"></part>
</message>
<portType name="EDSService">
<operation name="GenerateHash">
<input wsam:Action="http://afs-eds.ru/service/eds/GenerateHash/Request"
message="tns:GenerateHash"></input>
<output wsam:Action="http://afs-eds.ru/service/eds/EDSService/GenerateHashResponse"
message="tns:GenerateHashResponse"></output>
</operation>
<operation name="VerifySMEV3_EPOV">
<input wsam:Action="http://afs-eds.ru/service/eds/VerifySMEV3_EPOV/Request"
message="tns:VerifySMEV3_EPOV"></input>
<output wsam:Action="http://afs-
eds.ru/service/eds/EDSService/VerifySMEV3_EPOVResponse"
message="tns:VerifySMEV3_EPOVResponse"></output>
</operation>
<operation name="signSMEV3_EPOV">
<input wsam:Action="http://afs-eds.ru/service/eds/signSMEV3_EPOV/Request"
message="tns:signSMEV3_EPOV"></input>
<output wsam:Action="http://afs-eds.ru/service/eds/signSMEV3_EPOV/Response"
message="tns:signSMEV3_EPOVResponse"></output>
</operation>
</portType>
<binding name="EDSPortBinding" type="tns:EDSService">
<wsp:PolicyReference URI="#EDSPortBinding_MTOM_Policy"></wsp:PolicyReference>
<soap:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document"></soap:binding>
<operation name="GenerateHash">
<soap:operation soapAction="http://afs-
eds.ru/service/eds/GenerateHash/Request"></soap:operation>
<input>
<soap:body use="literal"></soap:body>
</input>
<output>
<soap:body use="literal"></soap:body>
</output>
</operation>
```

```
<operation name="VerifySMEV3_EPOV">
<soap:operation soapAction="http://afs-
eds.ru/service/eds/VerifySMEV3_EPOV/Request"></soap:operation>
<input>
<soap:body use="literal"></soap:body>
</input>
<output>
<soap:body use="literal"></soap:body>
</output>
</operation>
<operation name="signSMEV3_EPOV">
<soap:operation soapAction="http://afs-
eds.ru/service/eds/signSMEV3_EPOV/Request"></soap:operation>
<input>
<soap:body use="literal"></soap:body>
</input>
<output>
<soap:body use="literal"></soap:body>
</output>
</operation>
</binding>
<service name="EDSService">
<port name="EDSPort" binding="tns:EDSPortBinding">
<soap:address location="http://localhost:8305/EDSService"></soap:address>
</port>
</service>
</definitions>
```

## 3.2 Описания справочников

Коды возврата методов сервиса:

Код	Описание
0	Проверка прошла успешно
1	Внутренняя ошибка
4	Не найден сертификат подписи
5	Срок действия одного из сертификатов цепочки истек, или еще не наступил
7	Один из сертификатов цепочки отозван
8	Не удалось найти подпись
9	Сообщение не подписано
10	Не удалось проверить на отзыв один или несколько сертификатов цепочки. Не доступен CRL файла с именем { имя файла }
15	Сертификат был издан не аккредитованным

	УЦ/не доверенным УЦ
18	Не найден элемент для подписи с таким Id
19	Ошибка при чтении файла списка УЦ
20	Подпись не верна. Нарушена целостность ЭП
21	Подпись не верна. Нарушена целостность данных xml сообщения