Порядок проверки электронной подписи в юрисдикциях за пределами РФ (версия на русском языке)

Настоящий порядок являются неотъемлемой частью Соглашения о использования электронного сервиса Рокет Ворк, которое размещено по ссылке https://b2b.rocketwork.ru/.

Для проверки достоверности электронной подписи используется встроенный функционал командной строки операционных систем Windows, Linux или Mac OS.

Исходные данные: после подписания документа на странице подписания sign.rocketwork.ru будет доступен файл с результатами подписания certificate.txt

Порядок действий для проверки подписи:

1. Запустите Командную строку (ОС Windows) или Терминал (ОС Linux или MacOS)
2. Укажите следующие команды:

```
echo 'Переменная 1' > signed_content.txt
echo 'Переменная 2' > base64sig.sign
echo 'Переменная 3' > pubkey.pem
base64 --decode base64sig.sign > decoded_signature.sig
openssl dgst -sha256 -verify pubkey.pem -signature decoded_signature.sig signed_content.txt
```

3. Проверьте полученный результат. Получение ответа “Verified OK” подтверждает достоверность проверяемой подписи.

Описание переменных:

Переменная 1 - данные объекта подписи (что подписываем). Скопируйте полный текст из certificate.txt между атрибутами -----ДАННЫЕ_ПОДПИСИ_1 или -----ДАННЫЕ_ПОДПИСИ_2, включая название атрибута (для проверки первой или второй подписи соответственно)

Пример 1:

```
-----ДАННЫЕ_ПОДПИСИ_1
Сумма=1.0
Наименование=Title
ЗаказчикНаименование=Demo Customer
ЗаказчикИНН=779999999999
Исполнитель=Иванов Иван Иванович
ИсполнительИНН=771533830120
Описание=desc
КонтрольнаяСумма=1929d4b4fc4b8f065f029e0ba42824e60b1b07a1c0280603f0aa8c068154e6f1
ССылкаНаДокумент=https://rocketwork.ru/api/tasks/02d3b792d7dd06cd4ec4b3bdf3e73761bfb66cf58fabd1e88cd514c5a8772117/agreement
ПубличныйКлюч=
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2aJnyesaNVe69MpM3quM
```

Zgtt9aDIg8sYwnaEdmojrwVSjpUDkSdd3Y1tJBz6vOymOTN+YiWspkVvzhZSr21i
n6fZKHG4sHIm/dg1wdRib2sodC8o6hO7eBfE2Wsd6CNpHXL1qgo0TzFFweC5pvp8
9nJVqRhalRrLpLIXqlqNqn9hnVuwQIM96/26yWFRz4Vd6AXlfPls8aNM9JTcgZTO
r95NF5++ij0Lp8dMr7196oj7P1Kp8VVqJqx1zTWIdCvSVIc8eYtyCsx1bwA/5PeV
tPEDm7kxXIG5nnM6/0emtyW2mHxIRMu+5GqmsoJFbk4oqqueBPtiOnMfVwORfibM
WQIDAQAB
-----END PUBLIC KEY-----
Подписант=ООО «Рокет Ворк»
ВремяПодписания=2021-09-14 20:52:37 +0300
НомерПодписи=13253
-----ДАННЫЕ_ПОДПИСИ_1

Переменная 2 - результат подписи. Скопируйте текст из certificate.txt между атрибутами -----ПОДПИСЬ_1 или ------ПОДПИСЬ_2, НЕ включая название самого атрибута (для проверки первой или второй подписи соответственно)

Пример 2:

r5HtObm8Xub8+mHJoopGBehdXmuXDxsjou7Zj+CBWk09c1jSIp9llodM9nZQ
nX9bRL88lO7BJUi4KRR80/1Pu65Kxnh2F1Szh/DfHjeXFg8xCqLJOjDa5jPw
VDxHVPKPH5o5Fqc0+Ga6t+Ebg9FVvnYQLAThB/BvSISI6GHTDaWRqqMlY5sA
o0dFe9Uox9MHD95P+H0N9HbjGNo8Pfz9N3BAPVVPVpNglFY0yuirWYo7w9mX
B9EFcFtT3RBwel3wuD7fyqaQNu+pQq5jnT1koa4kw+262iCHURfFMCzUC9N+
OBl5IiWxovEWMWNG6tbo+kB+r8lfr+uV5XJokf9mzw==

Переменная 3 - публичный ключ подписи. Скопируйте текст из certificate.txt между атрибутами ПубличныйКлюч=, включая заголовки -----BEGIN PUBLIC KEY----- / -----END PUBLIC KEY----- , но НЕ включая название самого атрибута (указывайте ключ соответвующий первой или второй подписи)

Пример 3:

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2aJnyesaNVe69MpM3quMZgtt9
aDIg8sYwnaEdmojrwVSjpUDkSdd3Y1tJBz6vOymOTN+YiWspkVvzhZSr21i
n6fZKHG4sHIm/dg1wdRib2sodC8o6hO7eBfE2Wsd6CNpHXL1qgo0TzFFweC5pvp8
9nJVqRhalRrLpLIXqlqNqn9hnVuwQIM96/26yWFRz4Vd6AXlfPls8aNM9JTcgZTO
r95NF5++ij0Lp8dMr7196oj7P1Kp8VVqJqx1zTWIdCvSVIc8eYtyCsx1bwA/5PeV
tPEDm7kxXIG5nnM6/0emtyW2mHxIRMu+5GqmsoJFbk4oqqueBPtiOnMfVwORfibM
WQIDAQAB
-----END PUBLIC KEY-----

Procedure for verification of electronic signature in jurisdictions outside the Russian Federation (English language version)

This procedure is an integral part of the Agreement on the use of the Rocket Work electronic service, which is available at the link https://b2b.rocketwork.ru/.

The built-in command line functionality of Windows, Linux or Mac OS operating systems is used to verify the authenticity of the electronic signature.

Initial data: after signing the document, a file with the results of signing certificate.txt will be available on the signing page of sign.rocketwork.ru.

The order of actions to verify the signature:

1. Run Command Prompt (Windows OS) or Terminal (Linux or MacOS OS).
2. Specify the following commands:

```
echo 'Variable 1' > signed_content.txt
echo 'Variable 2' > base64sig.sign
echo 'Variable 3' > pubkey.pem
base64 --decode base64sig.sign > decoded_signature.sig
openssl dgst -sha256 -verify pubkey.pem -signature decoded_signature.sig signed_content.txt
```

3. Verify the received result. Receiving a “Verified OK” response confirms that the verified signature is valid.

Variable description:

Variable 1 - signature object data (what we sign). Copy the full text from certificate.txt between the attributes -----DATA_SIGNATURE_1 or -----DATA_SIGNATURE_2, including the attribute name (to verify the first or second signature, respectively)

Example 1:

```
----- DATA_SIGNATURES_1
Amount=1.0
Name=Title
CustomerName=Demo Customer
ЗаказчикИНН=779999999999
Contractor=Ivanov Ivan Ivanovich
ИсполнительИНН=771533830120
Description=desc
КонтрольнаяСумма=1929d4b4fc4b8f065f029e0ba42824e60b1b07a1c0280603f0aa8c068154e6f1
ССылкаНаДокумент=https://rocketwork.ru/api/tasks/02d3b792d7dd06cd4ec4b3bdf3e73761bfb66cf58fa
bd1e88cd514c5a8772117/agreement
PublicKey=.
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2aJnyesaNVe69MpM3quM
Zgtt9aDIg8sYwnaEdmojrwVSjpUDkSdd3Y1tJBz6vOymOTN+YiWspkVvzhZSr21i
n6fZKHG4sHIm/dg1wdRib2sodC8o6hO6hO7eBfE2Wsd6CNpHXL1qgo0TzFFweC5pvp8
9nJVqRhalRrLpLIXqlqNqn9hnVuwQIM96/26yWFRz4Vd6AXlfPls8aNM9JTcgZTO
r95NF5++ij0Lp8dMr7196oj7P1Kp8VVVqJqx1zTWIdCvSVIc8eYtyCsx1bwA/5PeV
tPEDm7kxXIG5nnM6/0emtyW2mHxIRMu+5GqmsoJFbk4oqqueBPtiOnMfVwORfibM
WQIDAQAB
-----END PUBLIC KEY-----
Subscriber=RocketWorks LLC
```

TimeSubscribed=2021-09-14 20:52:37 +0300
Signature Number=13253
----- DATA_SIGNATURES_1

Variable 2 is the result of the signature. Copy the text from certificate.txt between the attributes ----- SIGNATURE_1 or ------SIGNATURE_2, NOT including the name of the attribute itself (to verify the first or second signature, respectively)

Example 2:

r5HtObm8Xub8+mHJoopGBehdXmuXDxsjou7Zj+CBWk09c1jSIp9llodM9nZQ
nX9bRL88lO7BJJUi4KRR80/1Pu65Kxnh2F1Szh/DfHjeXFg8xCqLJOjDa5jPw
VDxHVPKPH5o5Fqc0+Ga6t+Ebg9FVvvnYQLAThB/BvSISISI6GHTDaWRqqMlY5sA
o0dFe9Uox9MHD95P+H0N9HbjGNo8Pfz9N3BAPVVPVpNglFY0yuirWYo7w9mX
B9EFcFtT3RBBwel3wuD7fyqaQNu+pQq5jnT1koa4kw+262iCHURfFMCzUC9N+
OBl5IiWxovEWMWNG6tbo+kB+r8lfr+uV5XJokf9mzw==

Variable 3 is the public key of the signature. Copy the text from certificate.txt between the attributes PublicKey=, including the headings -----BEGIN PUBLIC KEY----- / -----END PUBLIC KEY----- , but NOT including the name of the attribute itself (specify the key corresponding to the first or second signature).

Example 3:

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2aJnyesaNVe69MpM3quMZgtt9aDIg8
sYwnaEdmojrwVSjpUDkSdd3Y1tJBz6vOymOTN+YiWspkVvzhZSr21i
n6fZKHG4sHIm/dg1wdRib2sodC8o6hO6hO7eBfE2Wsd6CNpHXL1qgo0TzFFweC5pvp8
9nJVqRhalRrLpLIXqlqNqn9hnVuwQIM96/26yWFRz4Vd6AXlfPls8aNM9JTcgZTO
r95NF5++ij0Lp8dMr7196oj7P1Kp8VVVqJqx1zTWIdCvSVIc8eYtyCsx1bwA/5PeV
tPEDm7kxXIG5nnM6/0emtyW2mHxIRMu+5GqmsoJFbk4oqqueBPtiOnMfVwORfibM
WQIDAQAB

-----END PUBLIC KEY-----