ТРЕБОВАНИЯ К ПОДДЕРЖКЕ ШИФРОВАНИЯ

Параметры участвующие в формировании seToken

ПАРАМЕТР	ОБЯЗАТЕЛЬНОСТЬ	ТИП	ОПИСАНИЕ
timestamp	да	date (YYYY-MM-DDThh:mm:ss±hh:mm)	дата запроса по стандарту ISO 8601:2004 в формате YYYY-MM-DDThh:mm:ss±hh:mm” Может отличаться не более чем на полчаса от даты/времени получения запроса в платежный шлюз (время Московское). ПРИМЕР: 2013-02-25T18:25:10+03:00 (без пробелов) РАСШИФРОВКА: 25 февраля 2013 года 18 часов 25 минут 10 секунд UTC+03 часа 00 минут
UUID	да	UUID(36)	идентификатор в стандарте UUID, формируется в соответствии https://tools.ietf.org/html/rfc4122
PAN	да	number(19)	номер карты зачисления
CVV	нет	number(3)	проверочный код карты. Этот параметр обязателен, если для мерчанта не выбрано разрешение "Может проводить оплату без подтверждения CVC".
EXPDATE	нет	number(6) YYYYMM	дата окончания срока действия карты зачисления (в формате YYYYMM, где YYYY - год, MM - месяц)
mdOrder	да	UUID(36)	идентификатор заказа который нужно исполнить криптограммой

Валидными наборами данных являются:

- timestamp/UUID/PAN/CVV/EXPDATE/mdOrder
- timestamp/UUID/PAN//EXPDATE/mdOrder
- ***timestamp/UUID/PAN///mdOrder*** ***рекомендовано***

Правила формирования строки для шифрования

timestamp/UUID/PAN///mdOrder - строка выстроена в строгой последовательности с использованием разделителей "/"

ПО НАБОРУ УКАЗЫВАЕМЫХ ДАННЫХ:

timestamp- дата запроса в формате YYYY-MM-DDThh:mm:ss±hh:mm (Может отличаться не более чем на полчаса от даты/времени получения запроса)

UUID-идентификатор заказа (в данном поле можно передавать mdOrder или номер заказа и т.д.)

mdOrder (в данном случае необходимо учитывать время жизни зарегистрированного заказа)

Пример сформированной строки

```
2019-05-09T15:18:06+03:00/550e8400-e29b-41d4-a716-446655440000/4111111111111111///5abe8400-e19b-4a14-a7c6-4466bbaacc00
```

В указанном примере используются следующие параметры:

- время по стандарту ISO 8601:2004 – в примере 2019-05-09T15:18:06+03:00
- UUID
- номер карты 4111 1111 1111 1111
- CVV2 карты – пустое поле
- срок действия карты – пустое поле
- идентификатор заказа который оплачивается (получен при выполнении метода *registerP2P*)

! ВАЖНО. Получившуюся строку необходимо зашифровать, используя алгоритм RSA шифрования "***RSA/None/PKCS1Padding***" с ключом длиной ***2048***.

Значения ключей

Боевой публичный ключ будет передаваться в рамках имплементации решения на боевую систему.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiDgvGLU1dFQ0tA0Epbpj1gbbAz9/lvZdTyspHCPQ4zTYki1xER8Dy99jzxj
83VIiamnwkHUsmcg5mxXfRI/Y7mDq9LT1mmoM5RytpfuuFELWrBE59jZzc4FgwcVdvR8oV4ol7RDPDHpSxl9ihC1h2KZ/GoKi9G6
TULRzD+hLeo9vIpC0vIlGUyxDWtOWi0yDf4MYisUKmgbYya+Z5oODANHUCiJuMMuuH7ot6hJPxZ61LE0FQP6pxo+r1cezGekwlc8
NrKq3XeeNgu4kWFXNTBSwAcNAizIvEY4wrqc4ARR3nTlwAxkye9bTNVNROMMiMtu1ERGyRFjI7wnSmRnNEwIDAQAB
-----END PUBLIC KEY-----
```

Code Block 1 Тестовый публичный ключ

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAiDgvGLU1dFQ0tA0Epbpj1gbbAz9/lvZdTyspHCPQ4zTYki1xER8Dy99jzxj83VIiamnwkHUsmcg5mxXfRI/Y7mD
q9LT1mmoM5RytpfuuFELWrBE59jZzc4FgwcVdvR8oV4ol7RDPDHpSxl9ihC1h2KZ/GoKi9G6TULRzD+hLeo9vIpC0vIlGUyxDWtOW
i0yDf4MYisUKmgbYya+Z5oODANHUCiJuMMuuH7ot6hJPxZ61LE0FQP6pxo+r1cezGekwlc8NrKq3XeeNgu4kWFXNTBSwAcNAizIv
EY4wrqc4ARR3nTlwAxkye9bTNVNROMMiMtu1ERGyRFjI7wnSmRnNEwIDAQABAoIBAF09+B71iw2BxkGo15GJsGUEdE4Y3QE8y
koyxQUaDxY3SjdlG4wYqsSWuP89n3jvi9dDhQOc8Vaik6vwoM+Rl3A0rx+p7qQwC3uY0dRYHqSHy+IkOISsaQKbgNuiebPG7Bpf2e
4YH2HvKVHYYNsRJXTjIwXGfjzKo9QOcORmoaPWHuCie1o41Sn6JTzC/mMsLRf+Ih2Rr5JuJxIR2pCIbX0gqlI7ZkqjICVPsnyCXU8aGs
paWo6PlIwYfn/r2bIBo3Uk5PkngwRwqZQy5OWzX5gZ4CT+EDsuMx/cKbahn/iUyVyxYwgGg04WqTBKjKdUsonkhh680hV+NkZk7
H0IoWECgYEA3+g3tBTk1OxwVPDwRSvphPl56LYESGkESJAkbU+IFYezNnUGzEYtoS5gZfm49IStFTF/45EzOgBboNzeatj5egpR+Wb
dIugsXfpuJ4+yJ7b1J4bjVHm84ctCWXk+KZSJk7xQr2I41xrpjPuYVIxd9jCR7zABcM39eFBR7yzcCe0CgYEAm751yXTBYGhzNdgdvGT
fjqwjSdUNA//yJHtqdcftlUvu+solpn40tn79kBTAqL3U1G67HcFb42SFv0brSCEBfJKEZPnJrPP8njEGnL+8Pxgd0dndxPtk1KuJQgs7C8
N2OJRbI1KMs43iTIJAfoXm4nhC4Re3Yx5KQ8m6Z9n2Uv8CgYB3TBzRwAgkQk2flDgQQtNK3DIN+hzSD9IOb25ZJ3TUM9cSfsu+bu
3E4RbPfnxDG6W0kwkW0LhAgQxQ6x0+RJi3o2QFw/6yqI1rDRE/1toPOvXnt4DL84jlrQyO64BpWxDqO/2pVGYAhgBF8484DQnL
MBmxHRzHY5lXT0Q4cOhUCQKBgEOWhxVTNux4x67RSC5O9Hm9GF9dNxXKSDIu4QeWKPPGjUKG4Yn8cTHVsIKLjwRrxWYfW9L
Q6+il4ikdRNP7huKhzxTnFe+ZvsKD8iOqTa5v79j3HHf0xVBJ1Po1V32GaNKrB1Yv5+GwLEoZqJV/1K/pktSOb0ZzibUbYWraOzzPAo
GBALUpcJl+wQ1V4Xkutg7JWPiT7a8f31iGOIcH39PE/Y7wt2/WBD/EgLEKtD8AcghBnpk4qMg0IHAr91QG328BFYrLLYB+UgeZjPXI
AHdCuonCh/xFqFJkLSjTapPMUOIf9vNvKf/odiQ7gMm5wrESuOpq0BWlBIe5saXW5J7cnV9D
-----END RSA PRIVATE KEY-----
```

Code Block 2 Тестовый приватный ключ

Публикация ключей

Платежный шлюз публикует набор действующих в настоящий момент открытых ключей, которые могут быть получены с общедоступного URL-адреса https://{domain_name}/payment/se/keys.do

Значение {domain_name} URL-адреса для тестовой и рабочей среды.

- Тест: https://3dsec.sberbank.ru/payment/se/keys.do
- Рабочая версия: https://securepayments.sberbank.ru/payment/se/keys.do

Ключи действительны, если это подтверждается заголовками HTTP, которые кешируются до истечения срока действия ключей. Если срок действия ключей истек, запросите новые с общедоступного URL-адреса.

Ключи, предоставленные через общедоступный URL-адрес, отображаются в следующем формате:

```
{
  "keys": [
    {
      "keyValue": "-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAij/G3JVV3TqYCFZTPmwi4JduQMsZ2HcFLBBA9fYAvApv3FtA+zKdUGgK
h/OPbtpsxe1C57gIaRclbzMoafTb0eOdj+jqSEJMlVJYSiZ8Hn6g67evhu9wXh5ZKBQ1RUpqL36LbhYnIrP+TEGR/VyjbC6QTfaktcRfa
8zRqJczHFsyWxnlfwKLfqKz5wSqXkShcrwcfRJCyDRjZX6OFUECHsWVK3WMcOV3WZREwbCkh/o5R5Vl6xoyLvSqVEKQiHupJcZu9
UEOJiP3yNCn9YPgyFs2vrCeg6qxDPFnCfetcDCLjjLenGF7VyZzBJ9G2NP3k/mNVtD8Kl7lpiurwY7EZwIDAQAB-----END PUBLIC KEY-
----",
      "protocolVersion": "RSA",
      "keyExpiration": 1598527672000
    },
    {
      "keyValue": "-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAhjH8R0jfvvEJwAHRhJi2Q4fLi1p2z10PaDMIhHbD3fp4OqypWaE7p6n6
EHig9qnwC/4U7hCiOCqY6uYtgEoDHfbNA87/X0jV8UI522WjQH7Rgkmgk35r75G5m4cYeF6OvCHmAJ9ltaFsLBdr+pK6vKz/3AzwA
c/5a6QcO/vR3PHnhE/qU2FOU3Vd8OYN2qcw4TFvitXY2H6YdTNF4YmlFtj4CqQoPL1u/uI0UpsG3/epWMOk44FBlXoZ7KNmJU29
xbuiNEm1SWRJS2URMcUxAdUfhzQ2+Z4F0eSo2/cxwlkNA+gZcXnLbEWIfYYvASKpdXBIzgncMBro424z/KUr3QIDAQAB-----END
PUBLIC KEY-----",
      "protocolVersion": "RSA",
      "keyExpiration": 1661599747000
    }
  ]
}
```


keyValue – строковое представление публичного ключа RSA 2048
keyExpiration – планируемый срок действия ключа, дата в секундах по стандарту UNIX time
protocolVersion – версия алгоритма шифрования

Обновление ключей

Обновлять ключи нужно раз в год.

Чтобы сделать это, измените открытый ключ, который используете в коде.

Примечание. После того как вы внесете в код все необходимые изменения, проверьте, правильно ли выполняется шифрование с новым публичным ключом. Получите подтверждение со стороны Службы поддержки.

ПРИМЕР

Входящая строка

```
2019-05-09T15:18:06+00:00/550e8400-e29b-41d4-a716-446655440000/4111111111111111///5abe8400-e19b-4a14-a7c6-4466bbaacc00
```

Результат шифрования

```
Dduur6hWg9dfp9aXos1QC8s/C6ZVujOc3qySy0V7UEssHQ9JE7NCK9sbJxgjsAl7l7XXOJEP1KoeNQZCoItXdOAi89rFn9AR5uuiDT0R
U3+7RC1VhbtbFPAgwd1v7GKwJ4bRc2jeyOTc5azKTqjIpeU1jVpWN+/pbLhiL+QxLI9k7oQCLYltQk50rpyIyScUavVMZGRVCnLYws
GN/sVXP+MFqqP3DUFiwjPWz2NeoFV2M5Hmb/g6Q1KkbYPZhIH6Dx0LNSy4PctzfGOr8hDe7i/f2bVKvB5z+vu1adRPmkW3TDD2
VwLv5SOB6/tK9BLu7aZkwZbWsaIr3FoTWc7eNQ==
```

ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

Работа функционала, описанного в данном документе должна соответствовать требованиям безопасности, предъявляемым к модулям платежного шлюза РБС.

Требования к криптограмме

- Криптограмму нельзя хранить после оплаты и использовать повторно

Требования к безопасности по PCI DSS

В документации PCI DSS, использование криптограммы рассматривается как "E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn’t directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant’s systems or premises.", то есть обработка платежных данных выполняется третьей стороной, но сайт влияет на безопасность карточных данных.

Для соблюдения требований стандарта, ТСП необходимо заполнять лист самооценки SAQ-EP и ежеквартально проходить ASV тестирование.

Других специальных требований не предъявлено.

ОГРАНИЧЕНИЯ

1. Шифрование необходимо реализовать на стороне клиентского приложения.
2. На стороне клиента выполнить защиту локальной сети от вредоносного ПО и регулярно обновлять антивирусное ПО или программы

В случае снятия ограничений, требования по ним должны быть сформулированы отдельно.