Техническая спецификация банковской ссылки

Запросы

В настоящем документе приводятся спецификации запросов, в которых каждой услуге соответствует свой перечень параметров. Для составления действующей услуги нельзя добавлять ни одного параметра, которого нет в списке спецификации и необходимо соблюдать указания, приведенные в документе.

- В суммах, представленных в запросах, десятичные места и сенты отделяются точкой "." Отделение тысячных не используется.
- Даты и время представлены в формате DATETIME, например, 2018-03-12T09:53:14+0200, с точностью до секунды и в соответствии с временной зоной. Получатель запроса обязан проверить значение, представленное на поле DATETIME, при этом, значение может отличаться от действующего во время проверки времени максимально ± 5 минут.
- Величина длительности поля не может превышать значения, предусмотренного в спецификации. В случае превышения допустимой величины длительности запрос не обрабатывается. Величины длительности полей указаны в символах (не в байтах). Величина поля может быть короче, по сравнению с максимально разрешенным, неиспользованные места не заполняются.
- Для замены запроса – ответа используется метод HTTP POST.
- На запросы, несоответствующие спецификации, приходит уведомление об ошибке.
- На поле VK_RETURN нельзя использовать названия полей, используемых в запросах (VK_.....).
- Для замены данных используются кодировки (VK_ENCODING), в которых банковскую ссылку Coop поддерживает UTF-8 (по умолчанию) и кодировку ISO-8859-1. Для беспроблемного действия банковской ссылки необходимо убедиться, что во всех, связанных с услугой программах, используются одинаковые кодировки.

Запросы можно разделить:
1. на базе инициатора:
   - Запрос продавца или банка.
2. на базе ответа:
   - Требующий ответа или не требующий ответа.
3. на базе назначения:
   - 1xxx – инициирование платежей или 4xxx – запросы аутентичности.

Нахождение контрольного кода VK_MAC на основании версии 008.

Контроль электронной подписи, используемой в запросах VK_MAC, осуществляется по согласованному алгоритму, на основании VK_VERSION.

Кодирование в случае VK_VERSION=008:

VK_MAC учитывается в соответствии с алгоритмом RSA и затем переносится в кодировку BASE64. Значение VK_MAC учитывается с использованием алгоритма публичного ключа RSA. Также учитывается и длительность пустых полей – “000”. Не подписываются неупорядоченные дополнительные поля запросов.

MAC(x1,x2,…,xn) := RSA(SHA-1(p(x1)|| x1|| p(x2)|| x2 || … ||p(xn)||xn),d,n)

где:

|| - выполнение строки сложения;
x1, x2, …, xn - параметры запроса;
p – длительность параметра функции. Длительность указывается в виде строки с трехзначным числом.
d – секретная компонента RSA.
n – модуль RSA.

Составление ряда данных на примере услуги „1012“:
VK_SERVICE="1012"
VK_VERSION="008"
VK_SND_ID ="testvpos"
VK_STAMP ="20011"
VK_AMOUNT="5.00"
VK_CURR ="EUR"
VK_REF ="999"
VK_MSG ="COOP test. OÜ"
VK_RETURN ="https://somehost.ee/returnurl"
VK_CANCEL ="https://somehost.ee/cancelurl"
VK_DATETIME ="2018-03-12T09:53:14+0200"

Подпись учитывается из строки данных (data string), которая состоит из следующих элементов – число символов ценности параметра и сама ценность параметра. В строке данных должны быть все поля, имеющие порядковый номер в описании услуги, поля без номеров (например, VK_LANG) сюда не относятся.

004 1012
003 008
008 testvpos
005 20011
004 5.00
003 EUR
003 999
017 COOP test. OÜ
029 https://somehost.ee/returnurl
029 https://somehost.ee/returnurl

024 2018-03-12T09:53:14+0200

В одном ряду:
0041012003008008testvpos005200110045.00003EUR003999017COOP test.
OÜ029https://somehost.ee/returnurl029https://somehost.ee/returnurl0242018-03-12T09:53:14+0200
Если, например, параметр VK_MSG был бы пустым, то его все-таки нужно добавить в строку данных, используя в качестве числа символов 000.

Спецификации запросов

Платежные услуги.

Услуга 1011.
Поставщик услуги направляет в банк данные подписанного платежного поручения, которое клиент не может изменить в интернет-банке. После успешного платежа, продавцу составляется запрос “1111”, в случае неудачного платежа – соответственно “1911”.
URL: https://i.cooppank.ee/pay

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (1011)
2	VK_VERSION	3	Используемый крипто-алгоритм (008)
3	VK_SND_ID	15	ID составителя запроса (ID магазина)
4	VK_STAMP	20	ID запроса
5	VK_AMOUNT	12	Сумма, подлежащая уплате
6	VK_CURR	3	Название валюты: EUR
7	VK_ACC	34	Номер счета получателя
8	VK_NAME	70	Имя получателя
9	VK_REF	35	Ссылочный номер платежного поручения
10	VK_MSG	95	Пояснение платежного поручения
11	VK_RETURN	255	URL, куда надо ответить в случае успешно выполненной сделке
12	VK_CANCEL	255	URL, куда надо ответить в случае неудачной сделки
13	VK_DATETIME	24	Дата и время инициирования запроса в формате DATETIME
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)

Услуга 1012
Поставщик услуги отправляет в банк заявление клиент о желании осуществить сделку. Имя и номер счета получателя платежа берутся из договора, заключенного между банком и поставщиком услуги. После успешного платежа продавцу составляется запрос“1111”, в случае неудачного платежа – соответственно“1911”.
URL: https://i.cooppank.ee/pay

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (1012)
2	VK_VERSION	3	Используемый крипто-алгоритм (008)
3	VK_SND_ID	15	ID составителя запроса (ID магазина)
4	VK_STAMP	20	ID запроса
5	VK_AMOUNT	12	Сумма, подлежащая уплате
6	VK_CURR	3	Название валюты: EUR
7	VK_REF	35	Ссылочный номер платежного поручения
8	VK_MSG	95	Пояснение платежного поручения
9	VK_RETURN	255	URL, куда надо ответить в случае успешно выполненной сделке
10	VK_CANCEL	255	URL, куда надо ответить в случае неудачной сделки
11	VK_DATETIME	24	Дата и время инициирования запроса в формате DATETIME
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)

Услуга 1111

Используется для ответа о выполнении платежного поручения внутри Эстонии.

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (1111)
2	VK_VERSION	3	Используемый крипто-алгоритм 008
3	VK_SND_ID	15	ID составителя запроса (ID банка)
4	VK_REC_ID	15	ID составителя запроса (ID магазина)
5	VK_STAMP	20	ID запроса
6	VK_T_NO	20	Номер платежного поручения
7	VK_AMOUNT	12	Уплаченная сумма
8	VK_CURR	3	Название валюты: EUR
9	VK_REC_ACC	34	Номер счета получателя
10	VK_REC_NAME	70	Имя получателя
11	VK_SND_ACC	34	Номер счета плательщика
12	VK_SND_NAME	70	Имя плательщика
13	VK_REF	35	Ссылочный номер платежного поручения
14	VK_MSG	95	Пояснение платежного поручения
15	VK_T_DATETIME	24	Дата и время инициирования запроса в формате DATETIME
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)

-	VK_AUTO	1	Y = ответ, автоматически отправляемый банком. N = ответ с движением клиента на домашней странице продавца

Услуга 1911
Используется при информировании о неудавшейся сделке.

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (1911)
2	VK_VERSION	3	Используемый крипто-алгоритм (008)
3	VK_SND_ID	15	ID составителя запроса (ID банка)
4	VK_REC_ID	15	ID принимающего запрос (ID магазина)
5	VK_STAMP	20	ID запроса
6	VK_REF	35	Ссылочный номер платежного поручения
7	VK_MSG	95	Пояснение платежного поручения
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)
-	VK_AUTO	1	Y = ответ, автоматически отправляемый банком. N = ответ с движением клиента на домашней странице продавца

В случае если поле VK_ENCODING отсутствует, то во всех текстовых полях ответа в кодовой таблице ISO-8859-1 символы, имеющие код выше 128 указываются следующим образом: заглавные буквы эстонского языка с диакритическими знаками на соответствующие аналоги без диакритических знаков (например, Ä->A и Š->S) и другие удаляются.

Сервер интернет-банка всегда старается отправить ответ со своего сервера в режиме VK_AUTO='Y', и это в случаях, если клиент прерывает сеанс или клиент не возвращается корректно на интернет-страницу продавца.

Услуги аутентичности
Услуга 4011
Пакет, отправляемый продавцом пользователю для ознакомления. Услуга открыта для продавцов, заключивших соответствующий договор. Код ответного пакета 3012.
Поля 4011 для запроса аутентичности:
URL: https://i.cooppank.ee/auth

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (4011)
2	VK_VERSION	3	Используемый крипто-алгоритм (008)
3	VK_SND_ID	15	ID составителя сообщения (партнер)

4	VK_REPLY	4	Код ожидаемого ответного пакета (3012)
5	VK_RETURN	255	URL продавца, куда ответить
6	VK_DATETIME	24	Время генерирования сообщения в формате DATETIME
7	VK_RID	30	Идентификатор, связанный с сессией
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)

Услуга 3012

При использовании услуги 4011 продавцу направляется пакет с информацией пользователя и временем аутентичности (VK_DATETIME), который продавец должен проверить из соображений безопасности.

Поля 3012 для ответа по аутентичности:

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (3012)
2	VK_VERSION	3	Используемый крипто-алгоритм (008)
3	VK_USER	16	Согласованный идентификатор пользователя
4	VK_DATETIME	24	Время генерирования сообщения в формате DATETIME
5	VK_SND_ID	15	ID составителя сообщения (ID банка)
6	VK_REC_ID	15	ID получателя сообщения (партнера)
7	VK_USER_NAME	140	Имя пользователя, в форме фамилии и имени
8	VK_USER_ID	20	Персональный код пользователя
9	VK_COUNTRY	2	Государство персонального кода (двухбуквенное ISO 3166-1)
10	VK_OTHER	150	Иная информация о пользователе
11	VK_TOKEN	2	Код идентификатора средства аутентичности: 1- ID-карточка; 2- Мобильный-ID; 5- одноразовые коды (за исключением, PIN-калькулятор); 6- PIN-калькулятор; 7- карточка многократного использования.
12	VK_RID	30	Идентификатор, связанный с сессией
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)

Пользователь обращается в банк. Банк просит пользователя идентифицироваться. После позитивного введения признаков пользователя, пользователю предлагается возможность пользоваться различными банковскими услугами, одной из которых является вход в Портал.

После того, как пользователь информирует банк, что он желает пользоваться услугами Портала, банк продуцирует сообщение 3012, которое подписывается и отправляется далее, через заголовок браузера пользователя, в Портал.

Необходимо, все таки, отметить, что проверка Временной печати по этому методу осуществляется несколько иначе: в отличии от предыдущего метода, не направляется контрольное время с запросом 4012, а это генерируется банком. Если разница между сервера времени банка и Портала будет слишком большой, то может возникнуть ситуация, что будут аннулированы все входы, которые поступили от этого предприятия. Чтобы этого избежать, Портал и Банк выбирают в интернете одну из институций, предлагающих стандартную услугу по синхронизации времени, атомные часы которой считаются обязательными при составлении сообщения временной печати (VK_TIME ja VK_DATE).

Услуга 4012
Пакет, отправляемый продавцом пользователю для ознакомления. Услуга открыта для продавцов, заключивших соответствующий договор. Код ответного пакета 3013.
URL: https://i.cooppank.ee/auth

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (4012)
2	VK_VERSION	3	Используемый крипто-алгоритм (008)
3	VK_SND_ID	15	ID составителя сообщения (партнера)
4	VK_REC_ID	15	ID получателя сообщения (банка)
5	VK_NONCE	50	Случайный одноразовый, генерированный составителем запроса
6	VK_RETURN	255	URL продавца, куда приходит ответ
7	VK_DATETIME	24	Время генерирования сообщения в формате DATETIME
8	VK_RID	30	Идентификатор, связанный с сессией
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)

Услуга 3013
Копия случайного одноразового кода, отправляемого продавцу
Поля ответа по аутентичности 3013:

№	Название поля	Длительность	Описание
1	VK_SERVICE	4	Номер услуги (3013)
2	VK_VERSION	3	Используемый крипто-алгоритм (008)
3	VK_DATETIME	24	Время генерирования сообщения в формате DATETIME
4	VK_SND_ID	15	ID составителя сообщения (ID банка)
5	VK_REC_ID	15	ID получателя сообщения (партнера)
6	VK_NONCE	50	Копия случайного одноразового кода,

			бывшего в запросе
7	VK_USER_NAME	140	Имя пользователя, в форме фамилии и имени
8	VK_USER_ID	20	Персональный код пользователя
9	VK_COUNTRY	2	Государство персонального кода (двухбуквенное ISO 3166-1)
10	VK_OTHER	150	Иная информация о пользователе
11	VK_TOKEN	2	Код идентификатора средства аутентичности: 1- ID-карточка; 2- Мобильный-ID; 5- одноразовые коды (за исключением, PIN-калькулятор); 6- PIN-калькулятор; 7- карточка многократного использования.
12	VK_RID	30	Идентификатор, связанный с сессией
-	VK_MAC	700	Контрольный код электронной подписи
-	VK_ENCODING	12	Кодировка сообщения. UTF-8 или WINDOWS-1257, или ISO-8859-13
-	VK_LANG	3	Желаемый язык общения (EST, ENG или RUS)

** В случае если поле VK_ENCODING отсутствует, то предполагается, что входом является ISO-8859-13, дополнительно к этому, во всех соответствующих текстовых полях ответа в кодовой таблице ISO-8859-1 символы, имеющие код выше 128 указываются следующим образом: заглавные буквы эстонского языка с диакритическими знаками на соответствующие аналоги без диакритических знаков (например, Ä->A и Š->S) и другие удаляются.

Портал выбранное пользователем для банка сообщение 4012 и подписывает его. Одновременно генерированное сообщение записывается и в промежуточной таблице.

Генерированное и подписанное сообщение 4012 направляется ожидающему пользователю, где отображается кнопка Autendime, которая направляет пользователя далее в интернет-банк.

Банк, после проверки подписи, просит пользователя войти. Если пользователь успешно вошел в банк, то банк составляет ответное сообщение: 3013. Аналогично сообщению 4012, оно подписывается и передается пользователю, после чего последнее направляется обратно в Портал.

Портал проверяет подпись переданного сообщения. Если подпись верная, то проверяется, был ли ответ 3013 получен в границах, предусмотренных в ранее отправленном сообщении 4012 и затем просматривается, находится ли в пользовании персональный код данного пользователя. Портал использует, в качестве идентификатора клиентов, персональный код.