

Процессинг кредитных карт через gateway Kaardikeskus

Visa, MasterCard

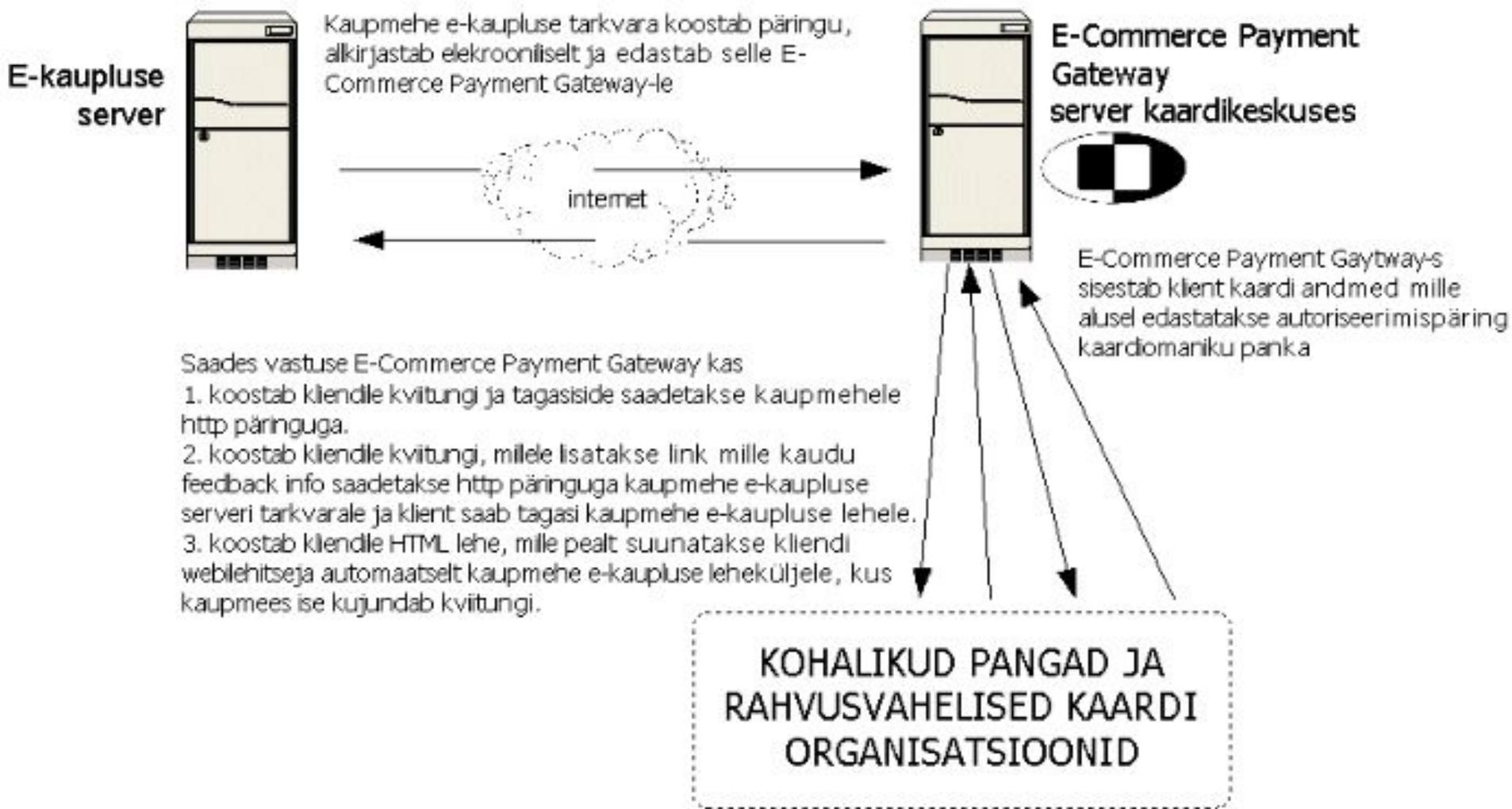
Сергей Кузнецов

work@setor.net

www.ox.ee

19.02.2009

Схема работы



Основные моменты технической реализации

- Всё аналогично с Pangalink
- Протокол передачи: HTTP GET/POST
- Безопасность: подписанная на основе публичного RSA ключа + SHA1 форма (MAC string).
- Используемая версия алгоритма 002 (устаревшая?)

Спецификация запроса

Параметр	Формат	Значение
action	String	Фиксированное значение: gaf
ver	Integer..3	Версия протокола, Фиксированное значение: 002
id	String up to 10	ID продавца (у каждого свой)
escuno	Integer ..12	Уникальный номер сделки продавца в системе мин. 100000 (должен быть уникален в течение 24 часов)
eamount	Integer ..12	Сумма сделки в центах.
cur	String 3	Наименование валюты сделки. Фиксированное значение: EEK
datetime	AAAАKKPPTTmmss	Дата время сделки (в часах и минутах)
mac	Hex String	Сигнатура сообщения (MAC)*
lang	et,en	Используемый в системе язык . et - эстонский, en - английский

Спецификация ответа

Параметр	Формат	Значение
action	String	Фиксированное значение: afb
ver	Integer..3	Версия протокола, Фиксированное значение: 002
id	String up to 10	ID продавца (у каждого свой)
ecuno	Integer ..12	Номер сделки продавца в системе из запроса
receipt_no	Integer ..6	Присвоенный Карточным центром номер сделки. У неудачной Сделки этот номер 000000
eamount	Integer ..12	Сумма сделки в центах
cur	String 3	Наименование валюты сделки из запроса
respcode	Integer 3	Ответный код Сделки 000 положительный , все иные – отрицательные. Ответный код базируется на стандарте ISO8583'97
datetime	AAAAKKPPTTmmss	Дата время сделки (в часах и минутах)
msgdata	String 40	Дополнительная информация о сделке, возможность введения на платежной форме (например имя и фамилия владельца Карточки*)
actiontext	String 40	Описание ответного кода (respcode)
mac	hex string	Сигнатура сообщения (MAC) **

Пример положительного ответа

[action] => afb

[ver] => 2

[id] => 0xEesti

[ecuno] => 542456687

[receipt_no] => 00232

[eamount] => 41000

[cur] => EEK

[respcode] => 000

[datetime] => 20081010150433

[msgdata] => Имя Фамилия владельца карточки (либо Visa Gold*)

[actiontext] => OK, tehing autoriseeritud (эст) / OK, approved (англ)

[mac] => ...

Никакой информации о кредитной карте, кроме имени владельца (для обычных Visa Classic) кардическус магазину не передаёт!

* Для карт Visa Gold имя владельца не передаётся.

Maksevormi küsimise MAC'i arvutamise RSA with SHA-1 (SHA1withRSA)

MAC=RSA(prikey, SHA1(ver+id+ecuno+eamount+cur+datetime))

```
3 // Define variables
4 $action = 'gaf';
5 $ver = '002';
6 $id = 'IDFirmName';
7
8 // Ecuno must be unique at least 24 hours
9 $ecuno = '123456';
10 $eamount = '1000'; // 10 EEK
11 $cur = 'EEK';
12 $datetime = date("YmdHis");
13 $lang = 'en';
14
15 // Number fields must be filled from left with "0"
16 // (null) & string values from right with spaces (ASCII code 20H)
17 $id = sprintf("%-10s", "$id");
18 $ecuno = sprintf("%012s", "$ecuno");
19 $eamount = sprintf("%012s", "$eamount");
20
21 // Lets prepare data for sha1
22 $data = $ver . $id . $ecuno . $eamount . $cur . $datetime;
23
24 // Now compute sha1
25 $signature = sha1($data);
26
27 openssl_sign($data, $signature, "...");
28
29 // MAC to HEX
30 $mac = bin2hex($signature);
```

Kaupmehe tagasiside MAC'i arvutamine RSA with SHA-1 (SHA1withRSA)

MAC=RSA(prikey,SHA1(ver+id+ecuno+receipt_no+eamount+cur+respcode+datetime+msgdata+actiontext))

```
3 function hex2str($hex) {
4   for($i=0;$i<strlen($hex);$i+=2) $str.=chr(hexdec(substr($hex,$i,2)));
5   return $str;
6 }
7
8 $data = sprintf("%03s", $ver)
9         . sprintf("%-10s", $id)
10        . sprintf("%012s", $ecuno)
11        . sprintf("%06s", $receipt_no)
12        . sprintf("%012s", $eamount)
13        . sprintf("%3s", $cur)
14        . $respcode
15        . $datetime
16        . sprintf("%-40s", $msgdata)
17        . sprintf("%-40s", $actiontext);
18
19 $mac = hex2str($mac);
20 $signature = sha1($data);
21
22 if (1 === openssl_verify($data, $signature, $pubkeyid))
23 {
24   // ok
25 }
```

Пара слов об интеграции...

- На главной странице сайта должен быть логотип Visa/MasterCard
- На чекауте так же должен быть логотип
- Переход на биллинг кардического куска должен осуществляться в том же окне, где была нажата ссылка/кнопка отправки формы
- Графика должна соответствовать брендингу Visa/MasterCard

Проблемы кардинга

- От кардинга ни кто не защищён
- Уголовное расследование можно начать только после реальной отгрузки товара/услуги
- Банкам и кардикескусу нет дела до кардеров
- Мы разрешаем платить кредитками только с эстонских IP

- <http://www.estcard.ee/publicweb/html/est/e-commerce.html> Тех. спецификация
- Так выглядит страница оплаты (на сервере кардикескуса):

Merchant Ox Eesti OÜ
Transaction authorization:

Card no.:	<input type="text"/>
Expiration (MMYY):	<input type="text"/>
CW2:	<input type="text"/> (three-digit number on the back of the card)
Name:	<input type="text"/>
Amount:	680.00 EEK
	<input type="button" value="Authorize"/> <input type="button" value="Reset fields"/>

Интерфейс немного педальный, кастомизить под дизайн своего сайта нельзя