Процессинг кредитных карт через gateway Kaardikeskus

Visa, MasterCard

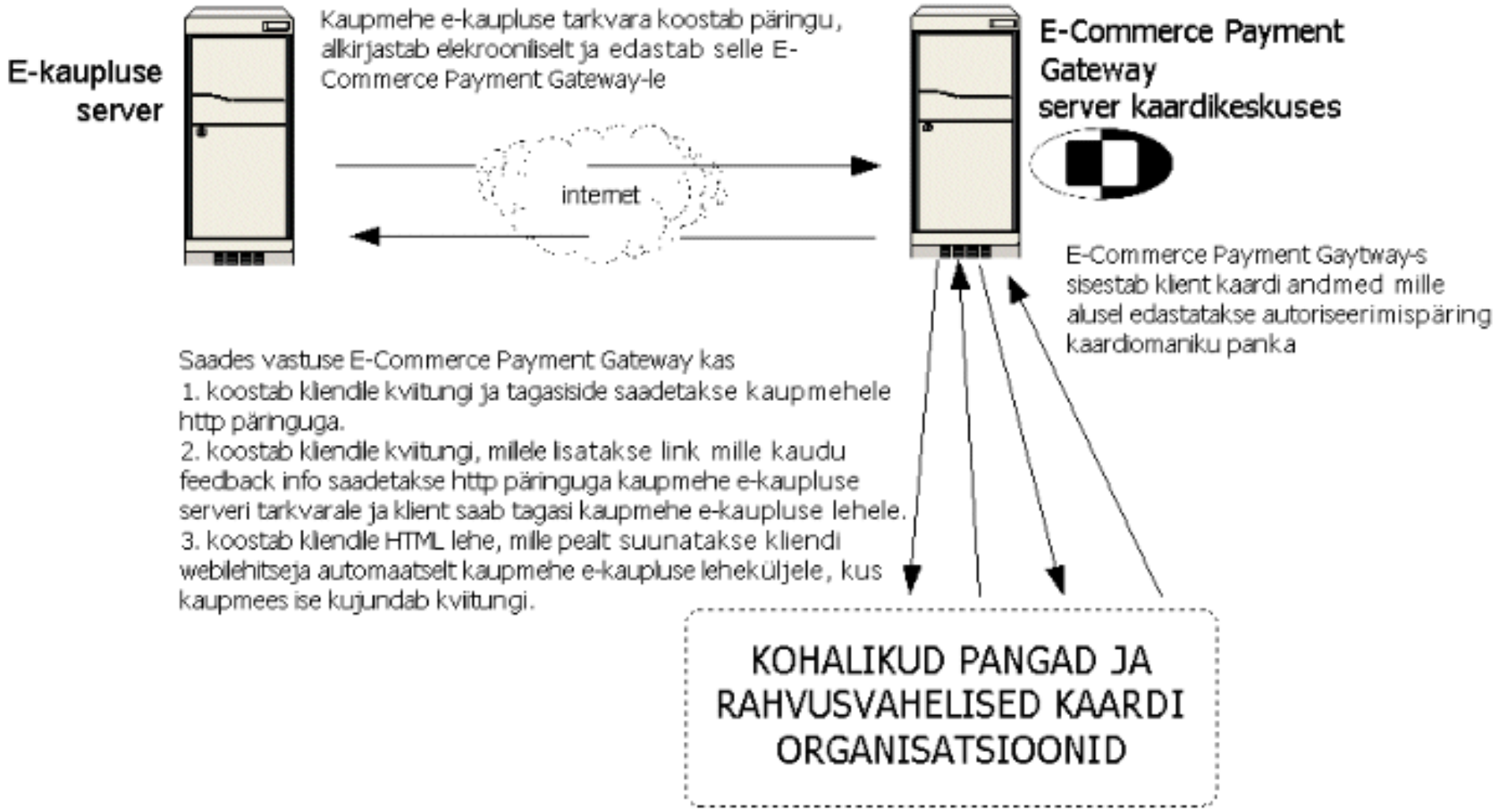
Сергей Кузнецов

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)
ecuno	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	AAAAKKPPTTmmss	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] => OxEesti
[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) кардикескус магазину не передаёт!

* Для карт Visa Gold имя владельца не передаётся.

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

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

```
// Define variables
$action = 'gaf';
$ver    = '002';
$id     = 'IDFirmName';

// Ecuno must be unique at least 24 hours
$ecuno    = '123456';
$eamount  = '1000'; // 10 EEK
$cur      = 'EEK';
$datetime = date("YmdHis");
$lang     = 'en';

// Number fields must be filled from left with "0"
// (null) & string values from right with spaces (ASCII code 20H)
$id     = sprintf("%-10s", "$id");
$ecuno  = sprintf("%012s", "$ecuno");
$eamount = sprintf("%012s", "$eamount");

// Lets prepare data for sha1
$data = $ver . $id . $ecuno . $eamount . $cur . $datetime;

// Now coumpute sha1
$signature = sha1($data);

openssl_sign( $data, $signature, … );

//  MAC to HEX
$mac=bin2hex($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))

```
function hex2str($hex) {
  for($i=0;$i<strlen($hex);$i+=2) $str.=chr(hexdec(substr($hex,$i,2)));
  return $str;
}

$data = sprintf( "%03s",  $ver)
      . sprintf( "%-10s", "$id")
      . sprintf( "%012s", $ecuno)
      . sprintf( "%06s",  $receipt_no)
      . sprintf( "%012s", $eamount)
      . sprintf( "%3s",   $cur)
      . $respcode
      . $datetime
      . sprintf( "%-40s", $msgdata)
      . sprintf( "%-40s", $actiontext);

$mac       = hex2str($mac);
$signature = sha1($data);

if ( 1 === openssl_verify($data, $mac, $pubkeyid) )
{
    // ok
}
```

Пара слов об интеграции...

- На главной странице сайта должен быть логотип Visa/MasterCard
- На чекауте так же должен быть логотип
- Переход на биллинг кардикескуса 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-
  Тех. спецификация

- Так выглядит страница оплаты (на сервере кардикескуса):