iPAYServlet technical Specification

iPAYServlet's input/output parameters for e-commerce protocol:
iPAYServlet's input parameters can be given using HTTP(s) POST requests in x-www urlencoded format (parameter1=value1&parameter2=value2 etc).
Note: parameter character encoding must be ISO-8859-1 in version 1,2

To get authorization form for E-transaction:	Value(s)	
action	gaf	Get authorization form. User will be provided with transaction authorization form.
ver	Integer 3	The protocol version (use 002 or 004)
id	String up to 10	Merchant/user id in system, must be present with all operations. Length max 10
ecuno	Number integer 12	Merchant electronic order system unique transaction id for e-commerce transaction. Length max 12
eamount	Number integer 12	Transaction amount provided by merchant in minor currency units without decimals. Length max 12
cur	String 3	Transaction currency name (USD, EUR, EEK etc)
datetime	YYYYMMDDHHmmss	The transaction date and time (timestamp)
mac	Hex String	the message mac signature
lang	et,en	Optional. Specifies the interface language et – estonian, en - english
charEncoding	String up to ..16 UTF-8, ISO-8859-1	Applicable for version 004. The character encoding used to encode parameters
feedBackUrl	URL, String up to ..128	The URL to send (POST) the payment confirmation at merchant shop. Applicable for version 004
delivery	String 1	Delivery method. Applicable for version 004 Values S – Electronic delivery T – Physical delivery

Calculation of MAC

```
version=2: RSA with SHA-1 (SHA1withRSA)
MAC=RSA(prikey, SHA1(ver+id+ecuno+eamount+cur+datetime))


version=4: RSA with SHA-1 (SHA1withRSA)
MAC=RSA(prikey, SHA1(ver+id+ecuno+eamount+cur+datetime+feedBackUrl+delivery))
```

NB! The length parameters used in signature must be padded up to their maximum length before generating or verifying the signature. Numbers must be padded from left with "0"-s and Strings must be padded from right with space " " (char(32)). After user payment E-shop receives following request with payment confirmation.

E-commerce feedback parameters:	Value(s)	
action	afb	E-commerce authorization feedback message from iPAYServlet to merchant/user system
ver	Integer 3	The protocol version (use 002 or 004)
id	String up to 10	Merchant/user id
ecuno	Number integer 12	the same unique transaction number that was generated by merchant system
receipt_no	Number 6 or "000000"	The receipt number assigned with transaction by iPAYServlet server if tranaction was successful and "000000" if tranaction was unsuccessful
eamount	Integer 12	Tranaction amount approved in minor units without decimals
cur	String 3	Transaction currency name
Respcode	Integer 3	Tranaction action code (000 is OK)
datetime	YYYYMMDDHHmmss	The transaction date and time (timestamp)
msgdata	String 40	Additional tranaction data (cardholders name etc)
Actiontext	String 40	Respcode description text
mac	Hex String	message signature (MAC)
charEncoding	String up to ..16 UTF-8, ISO-8859-1	Applicable for version 004. The character encoding used to encode parameters. Server will reply in same encoding as request received if received encoding was supported.
auto	String 1	Optional. Applicable all versions. Indicating whether the feedback was posted by user or server Y-server N-user

Calculation of MAC for feedback

```
version=2: RSA with SHA-1 (SHA1withRSA)
MAC=RSA( prikey,SHA1(ver+id+ecuno+receipt_no+eamount+cur+respcode+datetime+msgdata+
actiontext))

version=4: RSA with SHA-1 (SHA1withRSA)
MAC=RSA( prikey,SHA1(ver+id+ecuno+receipt_no+eamount+cur+respcode+datetime+msgdata+
actiontext))
```