БОРИКА
БАНКОВИ УСЛУГИ

Сигурни плащания чрез интернет

(протокол EMV 3DS)

Инструкция за виртуални търговци

Интеграция чрез CGI/WWW Forms

Secure payments via Internet

(EMV 3DS protocol)

Instructions for virtual merchants

Integration via CGI / WWW Forms

Идентификатор: **P-OM-41**
Версия: **2.3 / 16.11.2020**
Гриф: **С3 / ЗА ОГРАНИЧЕНО ПОЛЗВАНЕ**

Съдържание

Фигури

Таблици

1. Въведение

1.1 Цел и предназначение на документа

Този документ има за цел да даде насоки за включване на е-търговец към APGW акцептиращ и платежен сървър на БОРИКА, в съответствие с изискванията на EMV 3-D Secure. В него са описани формата и начина на обмен на съобщенията между БОРИКА и е-търговеца, при ползване на протокола, въведен от EMV Co.

Документът е предназначен за разработчиците на търговските сайтове и съдържа необходимите изисквания и указания, за да се реализира връзка с APGW акцептиращия и платежен сървър на БОРИКА за извършване на плащания чрез схемата 3-D Secure.

Ръководството може да се ползва и при миграция към APGW MPI на е-търговци, текущо обслужвани от БОРИКА, като за целта са посочени разликите със системата на Netcetera и особеностите при преминаване към APGW.

Към Ръководството има отделни приложения, които описват специфични операции. Тези приложения се предоставят при поискване от институциите, които предлагат съответните услуги (използване на токъни, P2P и др.)

1.2 Определения и акроними

1.2.1 Определения

Плащане (Authorization)
Процес, при който издател или процесор, от името на издателя, одобрява платежна трансакция.

Акцептираща Институция (Acquirer)
Финансова институция, член на местна и/или международна картова организация, която има договорни отношения с търговец за приемане (акцептиране) на плащания с картови продукти на съответната схема. В схемата EMV 3DS акцептиращата институция, или упълномощеният от нея агент (процесор), определят дали съответният търговец да участва в схема за извършване на плащания през отворената мрежа Internet.

EMV® Three-Domain Secure (3DS)
Протокол на съобщения, разработен от EMVCo., който позволява автентикация на картодържателите пред издателите на карти при извършване на трансакции през интернет.

Домейн на издателя (Issuer Domain)
Съдържа системите и извършва функциите, свързани с издателя и обслужваните от него клиенти (картодържатели).

Е-Търговец (e-merchant)
Субект (юридическо лице), който е в договорни отношения с акцептираща институция да приема плащания с платежни карти през интернет.

Отмяна на плащане (Reversal)
Процес, при който издател или процесор от името на издателя, отменя платежна трансакция.

Издател (Issuer)
Финансова институция, член на местни и/или международна картова организация, която издава картови продукти, има договорни отношения с картодържатели за доставяне на услуги, свързани с платежни карти, определя дали даден картодържател да участва в схемата 3-D Secure и идентифицира обхвата на номерата на картите, които да участват в схемата EMV 3DS.

Първоначална авторизация (Deferred Authorization)
Тази трансакция се изпълнява на две стъпки. При първата стъпка акцентиращият и платежен сървър регистрира заявката за първоначална авторизация. Тази заявка потвърждава наличието и блокира изискуемата, в заявката, сума по картовата сметка или картата на картодържателя. Втората стъпка, завършване на първоначална авторизация, се инициира от търговеца. Чрез нея се извършва плащането на посочената от търговеца сума, която трябва да бъде равна на посочената в първоначалната заявка. По този начин се завършва отложеното плащане.

1.2.2 Акроними

ACS	Access Control Server (Сървър за контрол на автентикацията)
APGW	Acquiring and Payment Gateway, *e-Commerce CGI сървър* (Акцептиращ и платежен сървър на БОРИКА)
API	Application Programming Interface (Приложен програмен интерфейс)
BIN	Банков идентификационен номер. При платежните карти това са първите шест/осем цифри, които еднозначно определят финансовата институция, издател на картата
CGI	Common Gateway Interface
DS	Directory Server (Справочен сървър [на регистрациите в схемата 3-D Secure])
HTML	Hypertext Markup Language - стандартен език за документи, предназначени да се визуализират в интернет
HTTP	Hypertext Transfer Protocol – апликационен протокол за предаване на hypermedia документи, например HTML
PAN	Primary Account Number - номер на карта
URL	Адресна схема за страниците в отворената световна мрежа за обмен на информация Internet
JRE	Java Runtime Environment
SSL	Secure Socket Layer
OpenSSL	Свободна софтуерна библиотека, предоставяща набор от криптографски от функции и дефиниции. https://www.openssl.org.
UTF-8	8-bit Unicode Transformation Format – стандарт за символно кодиране с променлива дължина
Keystore	Хранилище на сертификати и частни ключове

2. Спецификация на интерфейса с е-търговец

2.1 Интерфейс на е-търговеца с Акцептиращ и платежен сървър на БОРИКА

Комуникацията и предаването на параметри става посредством HTML Forms и HTTP Post към e-Commerce CGI сървъра на БОРИКА.

Комуникацията между търговеца и e-Commerce CGI сървъра включва:

- **Изпращане на данни за „Плащане“ или „Първоначална авторизация“ към APGW**

  Данните описват частта от трансакцията, свързана с търговеца (номер на поръчка, сума, и т.н.). Те се изпращат към акцептиращия и платежен сървър (APGW) като първа стъпка от процеса, преди клиентът да въведе своята картова информация (PAN, валидност и др.) на сайта на БОРИКА. Данните се предават чрез HTTP Post през браузъра на картодържателя към сайта на БОРИКА.

  Терминалът работи в една валута. Необходимо е валутата в заявката да съвпада с валутата на терминала.

- **Получаване на резултат от „Плащане” или „Първоначална авторизация“ от APGW**

  Търговецът получава резултат от „Плащане” или „Първоначална авторизация“ (независимо дали е положителен или отрицателен), след като са преминати всички стъпки по автентициране на картодържателя и авторизиране на трансакцията от авторизационната система на издателя на картата.

  Данните се предават чрез препращане от браузъра на картодържателя към сайта на Търговеца посредством HTTP Post. Търговецът отговаря за проверката на цифровия подпис на данните, за да удостовери, че резултатът е подписан от БОРИКА. Входната точка в сайта на търговеца (BACKREF) предварително се задава в APGW за всеки терминал.

  Търговецът отговаря за визуализиране на резултата към картодържателя след получаване на отговора.

- **Получаване на информация за състояние на трансакция**

  Възможно е (поради същността на Интернет) търговецът никога да не получи резултат от „Плащане“ или резултат от „Първоначална авторизация” на успешно или неуспешно авторизирана трансакция. Това може да се получи, ако картодържателят затвори браузъра си по невнимание, след като APGW е изпратил резултата, или поради прекъсване на връзката му с Интернет в този момент.

  Чрез изпращане на заявка за „Проверка на статус на трансакция“ може да се получи резултат от приключването на всички останали типове трансакции, поддържани от APGW.

  В интерфейса към APGW има заложена възможност за изпращане на резултата от трансакцията към търговеца чрез емайл.

- **Завършване на първоначална авторизация**

  При „Първоначална авторизация“ APGW връща на търговеца резултата, с което се инициира отложено плащане. При успешна „първоначална авторизация“ е необходимо търговецът да инициира „Завършване на първоначална авторизация“.

В настоящата версия на интерфейса се изисква сумата на завършващата операция да е равна на тази от първоначалната авторизация.

- **Отмяна на „Плащане“ или „Първоначална авторизация“**

  На търговеца се предоставя възможност за отмяна на „Плащане“ или „Първоначална авторизация“ (Reversal) на успешно завършила трансакция. Отмяната може да се извърши най-късно до 30 дни след извършване на успешната трансакция. Механизмът, по който това става, е описан в Раздел 5 „Поддържани типове трансакции“.

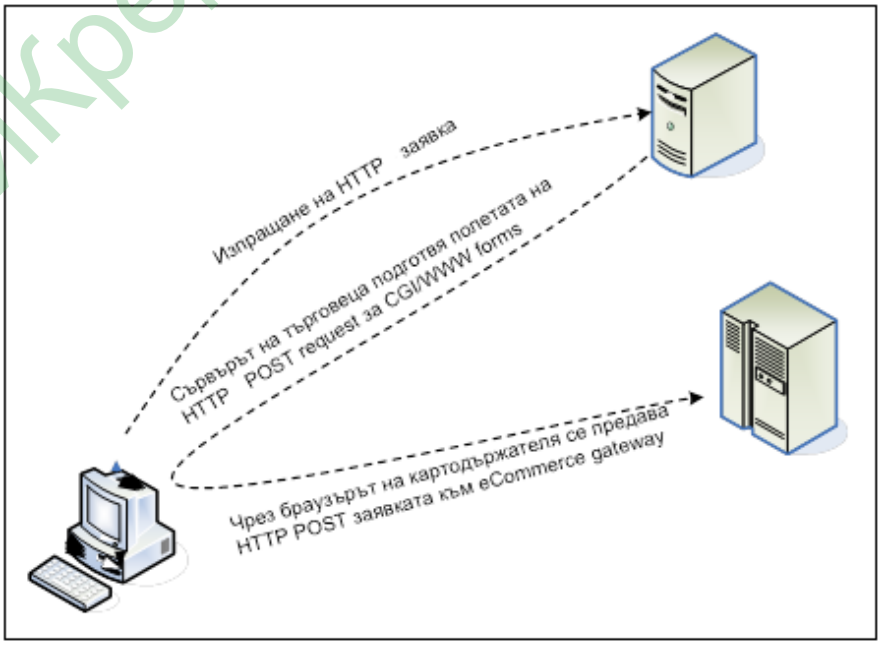
  Акцептиращата институция на търговеца може да има допълнителни изисквания за изпълнение на този тип трансакция.

- **Повторна трансакция при Soft Decline (RC 65/1A)**

  При получаване на отговор от авторизационната система с отказ на трансакция „Плащане“ или „Първоначална авторизация“ с код RC 65 за Mastecard или 1A за VISA, терминалът следва да направи повторна заявка за същата трансакция. Тъй като се налага картодържателят да въведе повторно данните за картата - препоръчително е търговецът да му предостави информация, че системата изисква неговата автентикация. Пример: „Издателят на Вашата карта изисква автентикация за извършване на плащането. Моля, въведете отново картовите данни и изпълнете следващите стъпки“.
  Данните за повторната заявка са като при началната, с допълнително въведена стойност 04 в поле M_INFO, подполе 3DS Requestor Challenge Indicator Field Name: threeDSRequestorChallengeInd.
  Повторната трансакция се генерира с различен номер на поръчка (ORDER).

2.2 Обмен на съобщения

Обменът на съобщения между сайта на търговеца и акцептиращия и платежен сървър на БОРИКА става посредством браузъра на картодържателя с помощта на метода HTTP POST. На Фигура 2-1 е показана схемата на изпращане на съобщение от сървъра на търговеца към сървъра на БОРИКА.



Фигура 2-1 Схема на предаването на съобщение чрез HTTP POST

В интерфейса към Netcetera се предава само един параметър **eBorica,** който съдържа структурирано поле.

В интерфейса към APGW предаването на данни от търговеца към БОРИКА става посредством HTML Forms полета с помощта на HTTP Post.

Форматът и имената на параметрите са подробно описани в Раздел 3 „Полета в съобщението при комуникация между е-Търговец и APGW“.

Когато картодържателят заяви плащане в сайта на търговеца (например чрез натискане на бутона „Плащане”), сървърът на търговеца създава HTML форма с параметри за „Плащане” или „Първоначална авторизация” и ги изпраща чрез браузъра на картодържателя към сайта на БОРИКА посредством HTTP POST.

Браузърът на картодържателя установява SSL/TLS връзка със сайта на БОРИКА посредством сървърния сертификат на БОРИКА, предава изготвените от търговеца параметри и инициира началото на диалог за автентикация и авторизация на плащане с картодържателя.

Адресите, на които се препращат заявките, са:

Девелопмент среда: https://3dsgate-dev.borica.bg/cgi-bin/cgi_link

Продукционна среда: https://3dsgate.borica.bg/cgi-bin/cgi_link

На тези адреси се обработват заявките за всички типове трансакции. При комуникация с картодържателя, на сайта на търговеца не се въвеждат данни за картата.

3. Полета в съобщението при комуникация е-Търговец - APGW

3.1 Полета в заявката от търговец към APGW

Параметрите, които се предават посредством полета в HTML Form са:

Поле	Описание	Размер	M/O/C	Съдържание
TERMINAL	Идентификатор на терминала	8	M	Terminal ID
TRTYPE	Тип на трансакцията	1-2	M	Възможни стойности 1, 12, 21, 22, 24, 90
AMOUNT	Сума	1-12	C	Обща стойност на поръчката по стандарт ISO_4217 с десетичен разделител точка (напр. 12.00)
CURRENCY	Валута	3	C	Валута на поръчката: три буквен код на валута по стандарт ISO 4217
ORDER	Номер на поръчка	6	M	Номер на поръчката за търговеца. Съдържа 6 цифри, дясно изравнено и допълнено с водещи нули. **ВНИМАНИЕ! Трябва да бъде уникален за терминала в рамките на последните 24 часа (напр. „000123“).**
DESC	Описание	1-50	C	Описание на поръчката*
MERCHANT	Идентификатор на търговеца	10-15	C	Merchant ID
MERCH_NAME	Име на търговеца	1-80	C	Име на търговеца*
MERCH_URL	URL на търговеца	1-250	O	URL на web сайта на търговеца

EMAIL		80	O	E-mail адрес за уведомления. Ако това поле е попълнено, платежният сървър може да изпраща резултата от трансакцията на посочения e-mail адрес.
COUNTRY	Държава	02	C	Двубуквен код на държавата, където се намира магазинът на търговеца, по стандарт ISO 3166-1.
MERCH_GMT	Часова зона на търговеца	3	C	Отстояние на часовата зона на търговеца от UTC/GMT (напр. +03).
LANG	Език	2	O	Език на транзакцията BG или EN. По подразбиране е избран език BG.
ADDENDUM	Допълнение	5	C	Служебно поле със стойност “AD,TD”. Подава се задължително, ако присъства поле „AD.CUST_BOR_ORDER_ID”.
AD.CUST_BOR_ORDER_ID	Идентификатор на поръчка	22	C	ORDER + 16 символа** **ВНИМАНИЕ, полето не трябва да съдържа символ “;”.**
TIMESTAMP	Дата/час	14	C	Време на трансакцията по **UTC**: YYYYMMDDHHMMSS. Разлика между времето на сървъра на търговеца и e-Gateway сървъра не трябва да надвишава 1 час. В противен случай e-Gateway ще отхвърли трансакцията.
TRAN_TRTYPE	Тип на оригиналната трансакция	1-2	C	Тип на оригиналната трансакция в заявка „Проверка на статус“
RRN	Референция на трансакцията	12	C	Референция на трансакцията (ISO-8583 -1987, поле 37).
INT_REF	Вътрешна референция	16	C	Вътрешна референция за e-Commerce gateway
M_INFO		0-35000	C	Опционален набор от данни по протокола EMV 3DS v.2 Трябва да бъде Base64-encoded string of JSON-formatted “parameter”:”value” data. Пример: { "threeDSRequestorChallengeInd":"04" }
NONCE		32	M	Съдържа 16 непредсказуеми случайни байтове, представени в шестнадесетичен формат. Може да съдържа главни латински букви A..F и цифри 0..9. **ВНИМАНИЕ! Трябва да бъде уникален за терминала в рамките на последните 24 часа.**
P_SIGN	Подпис	512	M	Код за автентициране на съобщението от APGW. Съдържа 256 байта в шестнадесетичен формат. Може да съдържа главни латински букви A..F и цифри 0..9.

Таблица 1 Полета, използвани за заявка към APGW

∗ Използва са за предоставяне на информация на платежната страница от страна на търговеца за картодържателя. Възможно е използване на кирилица.

** Използва се за информация, с която търговецът и картодържателят да разпознават плащането. Предава се през финансовите файлове. Въведената информация следва да се състои от цифри и латински букви.

M/O/C:
M – Mandatory / Задължително поле
C – Conditional / Полето е задължително според типа на трансакцията
O – Optional / Опционално поле

В таблицата са описани всички допустими полета. В зависимост от типа трансакция, някои полета не се задават.

Параметрите от Таблица 1 се предават чрез HTML Form посредством HTTP/POST.

ВАЖНО! В Раздел 5 са указани участващите полета за всеки тип трансакция. Полетата участващи във формиране на подписа задължително участват в заявката.

Примерна POST заявка за тип на трансакция 1 (Плащане):

```
<form name="pay" action="https://3dsgate-dev.borica.bg/cgi-bin/cgi_link" method="POST">
AMOUNT: <input type="text" name="AMOUNT" size="4" value="1.00" readonly="readonly"/><br>
CURRENCY: <input type="text" name="CURRENCY" size="3" value="BGN" readonly="readonly"/><br>
DESC: <input type="text" name="DESC" size="16" value="Детайли плащане." readonly="readonly"/><br>
TERMINAL: <input type="text" name="TERMINAL" size="8" value="V1800001" readonly="readonly"/><br>
MERCH_NAME: <input type="text" name="MERCH_NAME" size="12" value="Мол България" readonly="readonly" /><br>
MERCH_URL: <input type="text" name="MERCH_URL" size="20" value="http://www.borica.bg" readonly="readonly" /><br>
MERCHANT: <input type="text" name="MERCHANT" size="10" value="1600000001" readonly="readonly" /><br>
EMAIL: <input type="text" name="EMAIL" size="18" value="merchant@borica.bg" readonly="readonly" /><br>
TRTYPE: <input type="text" name="TRTYPE" size="1" value="1" readonly="readonly" /><br>
ORDER: <input type="text" name="ORDER" size="6" value="113920" readonly="readonly" /><br>
AD.CUST_BOR_ORDER_ID: <input type="text" name="AD.CUST_BOR_ORDER_ID" size="13" value="113920ORD@<n>"
readonly="readonly" /><br>
COUNTRY: <input type="text" name="COUNTRY" size="2" value="BG" readonly="readonly" /><br>
TIMESTAMP: <input type="text" name="TIMESTAMP" size="14" value="20201013083932" readonly="readonly" /><br>
MERCH_GMT: <input type="text" name="MERCH_GMT" size="3" value="+03" readonly="readonly" /><br>
NONCE: <input type="text" name="NONCE" size="32" value="D41AAAFC7F8119A3BB7C4868E0B256F9" readonly="readonly" /><br>
ADDENDUM: <input type="text" name="ADDENDUM" size="5" value="AD,TD" readonly="readonly" /><br>
P_SIGN: <input type="text" name="P_SIGN" size="512"
value="402C0EFAD1114AA3523C65C2ABF58008180DC8231EAEC84D3731A06437D39750B7516706E45E84F4FA120210F0402B0BDF65E
803EB9844D37D3DF4797B0D75600E8DBD7AB46DC4A6FA82C9FE7C27B218C18AC786C12BB70BF58BEF1CBEDBCC80621C9CCCA260
4F2D76E8ED77AB0702CE78DB2C5A5A61F32F85021DCE93D90CBC0CB55591D6188214BCFB76C94E5EDFBDD1BFB645AD3DC660F66
20ABB543B4C9253D697D8506830F18F6C1B7C93C3B2ECB871225ECAC2B3EB705DF8E778155F7748296B13F4F4B5EA40066694DD9D2
B8DFB3FF03F02739568768E33322E2F2C647B284DB010827B64C7FEB1D389E46D81CDCA9BE07FE8E69118FCD478E294743B"
readonly="readonly" /><br>
<INPUT type="submit" name="Submit" value="Approve"></br>
</form>
```

Търговецът има свободата да реализира на своята страница допълнителни валидации и логика на изпращане на данните на Java Script.

3.2 Полета в отговора от APGW към е-търговеца

На сайта на търговеца се получава резултат от заявка за трансакция от APGW чрез браузера на картодържателя посредством HTML Form и HTTPS/POST метода.

Полетата, които се ползват са следните:

Поле	Описание	Размер	M/O/C	Съдържание
ACTION	Действие	1-2	M	E-Gateway код на действие: 0 – успешно приключена трансакция; 1 – дублирана трансакция; 2 – отказана трансакция; 3 – грешка при обработка на трансакцията
RC	Код на завършване	2	O	Отговор при обработка на трансакция (ISO-8583, поле 39)
STATUSMSG	Текстово описание на код на завършване	1-255	C	Текстово описание на код на завършване
TERMINAL	Терминал	8	M	Ехо от заявката
TRTYPE	Тип на трансакция	1-2	M	Ехо от заявката
AMOUNT	Сума	12	C	Сума на поръчката
CURRENCY	Валута	3	C	Ехо от заявката
ORDER	Поръчка	6	M	Ехо от заявката
LANG	Език	2	O	Ехо от заявката
TIMESTAMP	Дата/час	14	M	Дата/час на отговора по UTC: YYYYMMDDHHMMSS
TRAN_DATE	Дата/час	19	C	Дата/час на трансакцията: YYYYMMDDHHMMSS
TRAN_TRTYPE	Тип на оригинална трансакция	1-2	O	Тип на оригинална трансакция в отговор на „Проверка на статус“
APPROVAL	Одобрение	6	O	Код за одобрение (ISO-8583, поле 38). Може да бъде празно, ако не е подадено от издателя на картата.
RRN	Референция на трансакцията	12	O	Референция на трансакцията (ISO-8583 -1987, поле 37)
INT_REF	Вътрешна референция	16	M	Вътрешна референция за e-Commerce gateway
PARES_STATUS	Статус на автентикация	1	C	Статус на автентикация, използван в схемата 3-D Secure
ECI		2	C	e-commerce индикатор (ECI)
CARD	Маскиран номер карта	16-19	C	Маскиран номер карта (напр. „5100XXXXXXXX0022“)
NONCE		32	M	Съдържа 16 непредсказуеми случайни байтове, представени в шестнадесетичен формат. Може да съдържа

				главни латински букви A..F и цифри 0..9.
P_SIGN	Подпис	512	M	Код за автентициране на съобщението от APGW. Съдържа 256 байта в шестнадесетичен формат. Може да съдържа главни латински букви A..F и цифри 0..9.

Таблица 2 Полета, използвани в отговора от APGW

Значението на поле **ACTION** „Действие ” съдържа код от изпълнението на трансакцията. При код, различен от „**0**” - трансакцията не е завършила успешно.

Значението на поле **RC** „Код на завършване” съдържа код от изпълнението на трансакцията. При код, различен от „**00**” - трансакцията не е завършила успешно.

Отговорите за трансакции, които не са свързани с браузера на картодържателя, а се предават директно от сайта на е-търговеца към APGW с методи GET или POST, са в json формат.

3.3 Особености на полета при миграция към CGI интерфейс

Когато се мигрира сайт към APGW CGI/WWW Forms интерфейс, трябва да се имат предвид някои особености за сходните полета в двата протокола.

1) Поле AMOUNT (Сума) - съдържа сумата на поръчката **заедно с десетичната точка,** например „10.20“. Ако не се въведат цифри след десетичния разделител, сумата се възприема като цяло число, например „200“ = 200 BGN.
2) Поле ORDER (Номер на поръчка) - съдържа само цифри
3) Времето в поле TIMESTAMP (Дата/час) се задава по UTC
4) Поле AD.CUST_BOR_ORDER_ID (Идентификатор на поръчка) се използва за предаване на номера на поръчката към Банката на търговеца във финансовите файлове. Полето трябва да съдържа значението на поле ORDER (Номер на поръчка) - 6 цифри, конкатенирано със символен низ с дължина до 16 символа. Същият низ може да се използва като символен номер на поръчка с размер до 16 символа.

   ВАЖНО! Полето не трябва да съдържа символ “;”.
5) APGW интерфейсът поддържа възможност за e-mail нотификация, която да информира търговеца за статуса на всяко плащане.

4. Цифров подпис

Цифровият подпис осигурява достоверност и цялостност на разменяните данни между е-търговеца и APGW. Полето, в което се предава е P_SIGN.

В зависимост от типа съобщение - заявка или отговор, подписът се формира върху част от полетата в Таблица 1 или Таблица 2. В зависимост от типа трансакция (TRTYPE), могат да се включват различни полета от посочените в тези таблици. При описанието на трансакциите в Раздел 5 за всеки тип са указани полетата, върху които се прави цифров подпис в заявката и отговора от APGW.

ВАЖНО! Стойностите на всички полета, участващи в подписа на заявката, трябва да са налични в заявката.

За цифровия подпис в заявките към APGW всеки е-търговец използва собствена двойка RSA ключове. Алгоритъмът, който се използва, е SHA256withRSA.

Символният низ за подпис се формира от дължината на значението в байтове и самото значение на полетата. Последователността на полетата задължителна.

Кодовата таблица, която се ползва по подразбиране, е UTF-8.

Алгоритъмът за подписване се прилага върху символния низ. Подписването става с частния ключ на търговеца.

Проверката на подписа в отговорите от APGW се извършва от всеки е-търговец посредством публичния ключ на APGW по същия начин.

Липсващо поле в отговора от APGW, участващо в проверката на подписа, се замества с един байт 0x2D (знак минус "-").

APGW поддържа две схеми на подпис – MAC_COMMON и MAC_EXTENDED.

Терминалът работи по една от двете схеми за подпис. Превключването на схемата за подпис се осъществява по искане на търговеца.

По подразбиране се ползва схема MAC_EXTENDED, която осигурява по-висока степен на защита на данните.

Схема за подписване MAC_COMMON може да бъде ползвана от е-търговец, по негово искане, не по-късно от 31 март 2021 г.

Полета за сформиране на символен низ за подпис по схема MAC_EXTENDED.

N	TRTYPE	P_SIGN_FIELDS_REQUEST	P_SIGN_FIELDS_RESPONCE
1	1	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE
2	12	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE
3	21	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE
4	22	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

5	24	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE
6	90	TERMINAL, TRTYPE, ORDER, NONCE	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

Таблица 3 Полета, участващи във формиране на подписа, според вида на съобщението, по схема MAC_EXTENDED

Полета за сформиране на символен низ за подпис по схема MAC_COMMON.

N	TRTYPE	P_SIGN_FIELDS_REQUEST	P_SIGN_FIELDS_RESPONCE
1	1	TERMINAL, TRTYPE, AMOUNT, CURRENCY, TIMESTAMP	TERMINAL, TRTYPE, AMOUNT, TIMESTAMP
2	12	TERMINAL, TRTYPE, AMOUNT, TIMESTAMP, DESC	TERMINAL, TRTYPE, AMOUNT, ORDER, TIMESTAMP
3	21	TERMINAL, TRTYPE, AMOUNT, TIMESTAMP, DESC	TERMINAL, TRTYPE, AMOUNT, ORDER, TIMESTAMP
4	22	TERMINAL, TRTYPE, AMOUNT, TIMESTAMP, DESC	TERMINAL, TRTYPE, AMOUNT, ORDER, TIMESTAMP
5	24	TERMINAL, TRTYPE, AMOUNT, TIMESTAMP, DESC	TERMINAL, TRTYPE, AMOUNT, ORDER, TIMESTAMP
6	90	TERMINAL, TRTYPE, ORDER	TERMINAL, TRTYPE, AMOUNT, TIMESTAMP

Таблица 4 Полета, участващи във формиране на подписа, според вида на съобщението, по схема MAC_COMMON, в сила до 31 март 2021 г.

Примери за подписване на заявка и валидация на отговор от APGW на PHP– в Приложение 1.

Примерни разработки на интерфейса могат да бъдат намерени на:
https://3dsgate-dev.borica.bg/

ВАЖНО! Поле TIMESTAMP е в часова зона UTC. Не се допуска разлика между TIMESTAMP в заявката и времето на APGW, в UTC, по-голяма от 1 час. За България отместването е “+03” лятно време и “+02” зимно време.

Пример Java:
```
DateFormat df = new SimpleDateFormat("yyyyMMddHHmmss");
df.setTimeZone(TimeZone.getTimeZone("UTC"));
String fldTimeStamp = df.format(new Date());
```

Пример PHP:
```
$fldTimeStamp = gmdate('YmdHis');
```

4.1 Формиране на подписа в заявка към APGW

При изпращане на заявка към APGW, търговецът задължително подписва съобщението с частния си ключ.

В Таблица 5 са изброени полетата от HTML формата, които участват в подписа, за трансакция тип 1 (Плащане), заедно с техните дължини и значения.

Поле	Описание	Брой байтове в UTF-8	Значение
TERMINAL	Терминал	8	V1800001
TRTYPE	Тип на трансакция	1	1
AMOUNT	Сума	4	9.00
CURRENCY	Валута	3	BGN
ORDER	Поръчка	6	154744
MERCHANT	Идентификатор на търговеца	10	1600000001
TIMESTAMP	Дата/час	14	20201012124757
NONCE		32	9EADBD70C0A5AFBAD3DF405902602F79

Таблица 5 Пример за формиране на низ за подписване при плащане

Третата колона съдържа броя байтове, които заема значението на съответното поле.

Низът за подпис изглежда така:

8V1800001**1**1**4**9.00**3**BGN**6**154744**10**1600000001**14**20201012124757**32**9EADBD70C0A5AFBAD3DF405902602F79

В зелен цвят са отбелязани дължините.

Общата дължина на полето за подпис в случая е 89 символа.

Горният символен низ, ако бъде представен като последователност от байтове в шестнадесетичен вид, само с илюстративна цел, е:

385631383030303031**31**31**34**392E3030**33**42474E**36**313534373434**3130**313630303030303030303031**3134**32303230313031323132343735373**3332**3945414442443730433041354146424144334446343035393032363032463739

ВАЖНО! При сформиране на символния низ за подписване е необходимо да се спазва поредността на полетата.

4.2 Проверка на подписа в отговор от APGW

При получаване на отговор от APGW, търговецът е длъжен да провери валидността на подписа от APGW, като използва сертификата на CGI e-Commerce сървъра. Ако в отговора липсва поле, участващо в проверката на подписа, то се замества с един байт 0x2D (знак минус "-").

В Таблица 6 са изброени полетата от отговора на APGW, които участват в подписа, за трансакция тип 1 (Плащане), заедно с техните дължини и значения.

Поле	Описание	Брой байтове в UTF-8	Значение
ACTION	Действие	1	1
RC	Код на завършване	2	00
APPROVAL	Одобрение	6	S97539
TERMINAL	Терминал	8	V1800001
TRTYPE	Тип на трансакция	1	1
AMOUNT	Сума	4	9.00
CURRENCY	Валута	3	BGN
ORDER	Поръчка	6	154744
RRN	Референция на трансакцията	12	028601253152
INT_REF	Вътрешна референция	16	97E2F39EFCA1CAF1
PARES_STATUS	Статус на идентификация	0	-
ECI		0	-
TIMESTAMP	Дата/час	14	20201012160009
NONCE		32	9EADBD70C0A5AFBAD3DF405902602F79

Таблица 6 Пример за формиране на низ за проверка на отговор при плащане

Третата колона съдържа броя байтове, които заема значението на съответното поле.

112006S97539 8V1800001 1149.00 3BGN 6154744 12028601253152 16 97E2F39EFCA1CAF1--14 20201012160009 32 9EADBD70C0A5AFBAD3DF405902602F79

В зелен цвят са отбелязани дължините.

Общата дължина на полето за подпис в случая е 123 символа.

Горният символен низ, ако бъде представен като последователност от байтове в шестнадесетичен вид, само с илюстративна цел, е:

313132303036533937353339385631383030303031313134392E30303342474E3631353437343431323032383630313235333135323136393745324633394546434131434146312D2D313432303230313031303132313630303039333239454144424437304330413541464241443344463430353930323630324639

ВАЖНО! При сформиране на символния низ за подписване е необходимо да се спазва поредността на полетата.

5. Поддържани типове трансакции

Всеки търговец следва да поддържа Soft Decline при трансакция "Плащане" (TRTYPE=1) и трансакция "Първоначална авторизация" (TRTYPE=12), съгласно изискванията на местните и/или международните картови организации.

APGW обработва заявки за трансакции в рамките на времеви интервал GUARDTIME. Ако TIMESTAMP в заявката е по-стар от GUARDTIME, заявката се отхвърля. Стойността по подразбиране на GUARDTIME е 15 мин. (900 сек.).

5.1 Плащане

TRTYPE=1

Трансакцията „Плащане“ се използва за плащане на стоки и услуги.

Участващи полета: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, DESC, MERCHANT, MERCH_NAME, MERCH_URL, EMAIL, COUNTRY, MERCH_GMT, LANG, ADDENDUM, AD.CUST_BOR_ORDER_ID, TIMESTAMP, NONCE, P_SIGN

Полета за подпис на заявка: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE

Полета за подпис на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

5.2 Проверка за статус на трансакция

TRTYPE=90

Заявката може да е HTTP GET или POST. Обичайно заявката се генерира от сървъра на търговеца и се изпраща директно към APGW.

APGW съхранява данни за трансакции за последните 24 часа. В случай, че APGW намери резултат за трансакция, отговора съдържа данни за намерената трансакция в json формат. Ако транзакцията не бъде намерена, валутата по подразбиране в отговора е USD.

При отговор на заявка за проверка на статус RC=-40 (Client side transaction form in progress), чиято оригинална трансакция е по-стара от GUARDTIME, можем да считаме че оригиналната транзакция не е успешна (timeout).

ВАЖНО! Поле ORDER съдържа номер поръчка на оригиналната трансакция а поле TRAN_TRTYPE съдържа типа на оригиналната трансакция. Останалите полета се подават според изискванията в таблица 1.

ВАЖНО! При отменена трансакция следва да се направи проверка за тип на оригинална трансакция 22 или 24. Отговора съдържа информация за съответния тип трансакция, указана в параметър TRAN_TRTYPE.

Значенията на полета “Действие“ (ACTION) и „Код на завършване“ (RC) в отговора са описани в таблицата по-долу:

<table>
<tr><th>ACTION</th><th>RC</th><th colspan="2">Описание</th></tr>
<tr><td>0</td><td>0</td><td colspan="2">Трансакцията е успешно обработена. В отговора се връща оригиналната информация за трансакцията</td></tr>
<tr><td>2</td><td>Код на завършване от издателя</td><td colspan="2">Трансакцията е отказана от издателя. В отговора се връща оригиналната информация за трансакцията</td></tr>
<tr><td rowspan="4">3</td><td rowspan="4">-19</td><td colspan="2">Неуспешна автентикация. Поле statusMsg може да бъде анализирано за повече информация за неуспешната автентикация:</td></tr>
<tr><td>Код</td><td>Описание</td></tr>
<tr><td>AS_FAIL</td><td>Трансакцията е отхвърлена по време на 3DS автентикация</td></tr>
<tr><td>AS_OTP_ERROR</td><td>Неуспешна автентикация с еднократна парола</td></tr>
<tr><td>AS_RND_ERROR</td><td>Неуспешна автентикация със случайна сума</td></tr>
<tr><td>3</td><td>-25</td><td colspan="2">Потвърждаването на трансакцията е прекъснато от клиента</td></tr>
<tr><td>3</td><td>-31</td><td colspan="2">Трансакцията се обработва от издателя</td></tr>
<tr><td>3</td><td>-33</td><td colspan="2">Извършва се автентикация на клиента</td></tr>
<tr><td>3</td><td>-39</td><td colspan="2">Искане за потвърждаване на клиента / User confirmation request</td></tr>
<tr><td>3</td><td>-40</td><td colspan="2">Искане за потвърждаване на трансакцията /User transaction form request</td></tr>
</table>

Таблица 7 Статус на трансакция

Участващи полета: TERMINAL, TRTYPE, ORDER, TRAN_TRTYPE, NONCE, P_SIGN

Полета за подпис на заявка: TERMINAL, TRTYPE, ORDER, NONCE

Полета за подпис на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

5.3 Отмяна на плащане

TRTYPE=24

Заявката може да е HTTP GET или POST. Обичайно заявката се генерира от сървъра на търговеца и се изпраща директно към APGW.

Трансакцията от тип “Отмяна на плащане” (Reversal) представлява отмяна на предходно плащане (трансакция тип 1) или отмяна на “Завършване на първоначална авторизация“ (трансакция тип 21).
Полетата на заявката са същите като тези при „Отмяна на първоначална авторизация“ (трансакция тип 22).

Участващи полета: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, DESC, MERCHANT, MERCH_NAME, MERCH_URL, EMAIL, COUNTRY, MERCH_GMT,

LANG, ADDENDUM, AD.CUST_BOR_ORDER_ID, TIMESTAMP, RRN, INT_REF, NONCE, P_SIGN

Полета за подпис на заявка: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE

Полета за подпис на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

5.4 Първоначална авторизация

TRTYPE=12

За приключване на трансакцията „Първоначална авторизация“ е необходимо последващо пускане на трансакция „Завършване на авторизация.

Участващи полета: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, DESC, MERCHANT, MERCH_NAME, MERCH_URL, EMAIL, COUNTRY, MERCH_GMT, LANG, ADDENDUM, AD.CUST_BOR_ORDER_ID, TIMESTAMP, NONCE, P_SIGN

Полета за подпис на заявка: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE

Полета за подпис на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

5.5 Завършване на първоначална авторизация

TRTYPE=21

Заявката може да е HTTP GET или POST. Обичайно заявката се генерира от сървъра на търговеца и се изпраща директно към APGW.

Трансакцията „Завършване на първоначална авторизация“ се използва за приключване на трансакция от тип „Първоначална авторизация“. Необходимо е сумата да съвпада със сумата на първоначалната авторизация.

Участващи полета: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, DESC, MERCHANT, MERCH_NAME, MERCH_URL, EMAIL, COUNTRY, MERCH_GMT, LANG, ADDENDUM, AD.CUST_BOR_ORDER_ID, TIMESTAMP, RRN, INT_REF, NONCE, P_SIGN

Полета за подпис на заявка: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE

Полета за подпис на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

5.6 Отмяна на първоначална авторизация

TRTYPE=22

Заявката може да е HTTP GET или POST. Обичайно заявката се генерира от сървъра на търговеца и се изпраща директно към APGW.

Трансакцията от тип „Отмяна на първоначална авторизация“ (Reversal) представлява отмяна на предходна авторизация (трансакция тип 12), която не е завършена.

Полетата на заявката са като при „Завършване на първоначална авторизация“, с изключение на TRTYPE/Тип на трансакция, чиято стойност трябва да е 22.

Участващи полета: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, DESC, MERCHANT, MERCH_NAME, MERCH_URL, EMAIL, COUNTRY, MERCH_GMT, LANG, ADDENDUM, AD.CUST_BOR_ORDER_ID, TIMESTAMP, RRN, INT_REF, NONCE, P_SIGN

Полета за подпис на заявка: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE

Полета за подпис на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

5.7 Повторна трансакция при Soft Decline

TRTYPE=1,12

При получаване на отговор от авторизационната система с отказ на трансакцията с код RC 65 за Mastecard или 1A за VISA, терминалът следва да направи повторна заявка за същата трансакция.
Тъй като се налага картодържателят да въведе повторно данните за картата - препоръчително е търговецът да му предостави информация, че системата изисква неговата автентикация. Пример: „Издателят на Вашата карта изисква автентикация за извършване на плащането. Моля, въведете отново картовите данни и изпълнете следващите стъпки“.
Данните за повторната заявка са като при началната, с допълнително въведена стойност 04 в поле M_INFO, подполе 3DS Requestor Challenge Indicator Field Name: threeDSRequestorChallengeInd.

ВАЖНО! Повторната трансакция се генерира с различен номер на поръчка (ORDER).

Участващи полета: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, DESC, MERCHANT, MERCH_NAME, MERCH_URL, EMAIL, COUNTRY, MERCH_GMT, LANG, ADDENDUM, AD.CUST_BOR_ORDER_ID, TIMESTAMP, M_INFO, NONCE, P_SIGN

Полета за подпис на заявка: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE

Полета за подпис на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE

6. Криптографски операции

Приложният протокол за връзка с платежния сървър на БОРИКА (APGW) изисква обменяните съобщения да бъдат подписани с цифров подпис.

Тази особеност определя необходимостта от познаване на някои криптографски операции.

Всеки е-търговец подписва заявките със своя частен ключ и проверява подписа в отговорите с публичния ключ на APGW. Публичния ключ на APGW се предоставя в .pem формат или със сертификат .cer.

По-долу са показани примери за изпълнение на характерните криптографски операции чрез използване на OpenSSL.

6.1 Генериране на RSA ключ за подписване на съобщенията

openssl genrsa -out *privatekeyname.key* [-aes256] 2048

Забележки:

- параметър -aes256, се използва, при желание да се защити с парола генерирания частен ключ;
- 2048 е размерът на ключа в битове.

Чрез командата е необходимо да се създадат два ключа: за тестовия и за реалния терминал. Те се използват за подписване на съобщенията, изпращани към платежния сървър на БОРИКА. Частните ключове се генерират от търговеца и трябва да бъдат съхранявани от него по сигурен начин.

6.2 Генериране на заявка за сертификат с OpenSSL

openssl req -new -key *privatekeyname.key* -out *name.csr*

Търговецът трябва да генерира две заявки за сертификати, които се изпращат за подписване в БОРИКА:

- заявка за сертификат за тестовия терминал;
- заявка за сертификат за реалния терминал;
- имената на файловете се създават по следната конвенция:

VNNNNNNN_YYYYMMDD_T, където:
VNNNNNNN – TID на терминала, предоставен от Финансовата Институция
YYYYMMDD – дата на заявка
T – тип на искания сертификат, значения – D – за development среда, P – за продукционна среда

ВАЖНО! TID на терминала в тестова и продукционна среди може да бъде различен.

6.3 Задължителни полета на сертификата

(изписани на латиница, без специални символи):

- Common name – име на домейна
- Organization utility – TID на терминала

- Organization – име на фирма,
- Location –населено място
- State or Province name – област/район
- Country = BG

6.4 Преобразуване сертификат в PKCS12 формат

openssl pkcs12 -export -inkey privatekeyname.key -in certificate_name.cer -out keystore_name.p12

openssl pkcs12 -export -inkey privatekeyname.key -in certificate_name.cer -out keystore_name.pfx

7. Примери за трансакции

Данните по-долу са изведени от различни тестови операции.

Примерни разработки на интерфейса могат да бъдат намерени на:
https://3dsgate-dev.borica.bg/

ВАЖНО! Показаните екрани са примерни и имат за цел само да илюстрират представянето на информацията по време на трансакция. При разработката на всеки реален сайт е възможно той да изглежда по различен начин.

7.1 Пример за плащане

Информация от търговеца към e-Commerce CGI:

TERMINAL	V1800001
TRTYPE	1
AMOUNT	1.00
CURRENCY	BGN
ORDER	145659
DESC	Детайли плащане.
MERCHANT	1600000001
MERCH_NAME	Мол България
MERCH_URL	http://www.borica.bg
EMAIL	merchant@borica.bg
COUNTRY	BG
MERCH_GMT	+03
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	145659ORD@<n>
TIMESTAMP	20201013115715
NONCE	FC8AC36A9FDADCB6127D273CD15DAEC3
P_SIGN	8125E0E604B8BC6430B03B1365B63D91ACB7210F2777776D7587A633D222368CB36936855090C810203185039984995035 95EBB32092014A2843C7E6DB75C1AD7FCB018BB4CDA98B379B411E74C62881529A7787B73D8D0E00D1406E1D2A64ADD1A298CCDF3B5A13C14825990010541444122F4A8FBB23BB3747B962BEFB5C57C5737FCF8DC9E61F377777B661B04FFE604EE5E49EB87CA49737FD39AA27639DE0CEF11B527B630070BE97ECC81F0D14D355F37C5C684A040C615563C962CE137A0B7C7F0B3567DEB0A05C4D79F373D7938D4CBFCE86CA6AA5DBAC99081F3AB4C52E0A3B35748A7600ECE4278060B14F5D3ACE5D964A73F49CF8844B6C86E10E

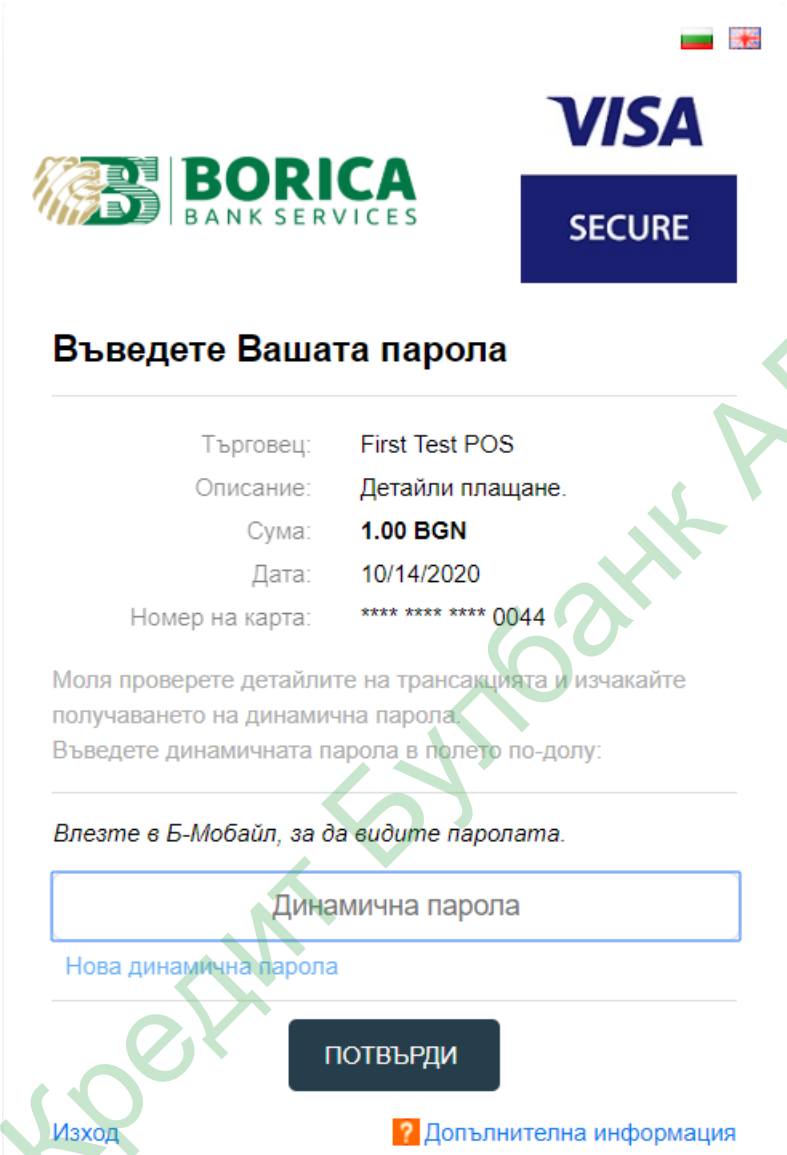
MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE]
macSourceValue	8V18000011141.003BGN617040310160000000114202010131404173222EA51788AFE61A9D814B771A8FA6379

Таблица 8 Данни на съобщението при плащане

След натискане на бутона Approve се извежда страницата за въвеждане на детайли за карта.

Ако въведената карта е регистрирана в ACS, се извежда екран за автентикация на картодържателя през ACS-а на институцията, която му е издала картата:



След завършване на трансакцията, управлението се предава на url, предварително зададено за търговеца.

Полето RC=00 показва успешна трансакция.

В следващата таблица са изброени всички променливи и техните значения за резултата от трансакцията.

Отговор от e-Commerce CGI:

Parameter	Length	Value
ACTION	1	0
RC	3	00
STATUSMSG	8	Approved
TERMINAL	8	V1800001
TRTYPE	1	1
AMOUNT	4	1.00
CURRENCY	3	BGN
ORDER	6	170403
TIMESTAMP	14	20201013140707
TRAN_DATE	14	20201013170707
APPROVAL	0	S19527
RRN	12	028701253242
INT_REF	16	B7A68A9F37E8586E
PARES_STATUS	0	
ECI	0	
CARD	16	5100XXXXXXX0022
NONCE	32	22EA51788AFE61A9D814B771A8FA6379
P_SIGN	512	31C6507191249D361086E1CA70A2A0374ACF9191D765055E10ACB93D720E934FEBE44E59D41D19C7B976CF358FA572B12EB08556EA602141E983F6FC93F106B0249780C192FAD7BC6411C33E966317804681D692CCDAF42F7494B1B7A7ED8AB23CB8DE5F0621E0C3582671BD222A3E5409538D9BD93F11B150B75D0C59AAC5E77D439FE14A6B494C8FECB1C23867A77D291E34425B5F1A6E9CBA9B92E3BC344E2C9AFAD45E2AE2D1313200A80DE26C2DD870E63AFEADA9EDAEF4DF5B32AD533D68665CB8F7F6E42D8ED7FFE31415FFAED25B3BA159063A9FC542FA958719016697CE9760954A58A2AF077BA049D1DD2216242D80572AA0EA98A39CD7C8DDB5BE

==== Response signature from ====

macFields = [ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,NONCE]

macSourceValue = [102006S195278V18000011141.003BGN617040312028701253242 16B7A68A9F37E8586E--142020101314070732 22EA51788AFE61A9D814B771A8FA6379]

Signature = [true]

Таблица 9 Данни на отговор на съобщението при плащане

7.2 Пример за проверка статус на трансакция

Полетата, с данни от оригиналната трансакция, са удебелени.

Информация от търговеца към e-Commerce CGI:

TERMINAL	V1800001
TRTYPE	90
ORDER	**114233**
TRAN_TRTYPE	**1**
NONCE	622CAAA8BF20C5A21A917DCB8401C336
P_SIGN	5FD6E5A6A0121A599594DB1F0FC96F2CEB4CCC7B3B829E9DBA74E1DC4AF115B774A5460AAA268DB65E04B71C6E9EB6A3F7A820C27D4EA1BC648A19BC97D2577F510F4CDF4BFD6EDA4B8D2B85564791ED6287A08282027099F07166FA8416F123FEEBBC920A33A0ED5964CA02C49A7ED7D5E61F4B5D53CC14DF542BDF4221DCDA22C5864F9F722BF989CB7A2BF2ABE0B76F823561A33F2152772312429204AAB94B58C7AFC82F64D5C20069D4A5B1DF406041CAB77BCCE88C6F84704B2B33AFC82216C2F41B92129D68933CE1C59F87CEAE6B1E8CFBE6DD4CE5898F8FE6453CC7DB7519801FB05BBDE7973E18A86AFF020121B74A65EAD2741BC1D6E39DD42564

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, ORDER, NONCE]
macSourceValue	8V1800001290611423332622CAAA8BF20C5A21A917DCB8401C336

Таблица 10 Данни за проверка на статус на трансакция

Резултатът от проверка на статус на трансакция е в json формат. Ако липсва поле, използвано за проверка на P_SIGN, то се замества с един байт 0x2D знак минус "-". Например “102006S449738V180000129041.003BGN6120353120287012531951 66AF46A8970774DBB—1420201013152429325E7EFC5D43E684642F0FB8B7F22167B9”).

Отговор от e-Commerce CGI (Трансакция от тип 1 е успешна):

{
"ACTION":"0",
"RC":"00",
"STATUSMSG":"Approved",
"TERMINAL":"V1800001",
"TRTYPE":"90",
"AMOUNT":"1.00",
"CURRENCY":"BGN",
"ORDER":"114233",
"TIMESTAMP":"20201016084515",
"TRAN_DATE":"20201016114310",
"TRAN_TRTYPE":"1",
"APPROVAL":" S78952",
"RRN":"029001254078",
"INT_REF":"4C9B34468610CF9F ",
"PARES_STATUS":"Y",
"ECI":"05",
"CARD":"4341XXXXXXXX0044",
"NONCE":"7A9A2E5CD173AF3F69A87F06E1F602ED",
"P_SIGN":"A20DE81C5723E3A92D8D1B73C7C2B8848A42D3380E9DF9951127E5878AF989E6951F595A52C16CC9B9F690BDC0165DE8E4CF2FA5892A17C5F8026011D604AF5723DF4C35486AA0094C1C23AE9617F8BE2C11F448EA40CDB332EBAB73DE2D33A01AC1BEE83108B788D22D8653F86DFAE8BAEB17048869156D2876FD7F8E232BDB1311D5D4EB63C630EC4941EDBFC70802508F86147714CD7E671014EC8D56882070B6B203FFECE07A67FED6D20C9F4E4637E8EA5B0FE274AD4D8965CB7025BD205F259E41EAF2E48E5566099842B02FB89E7534081CFD4289F6F5F7727DAAB7EBB472FDFD9D091F57616120190732BF635D49EF9519B4CEE26D8DFBB34C2D033B"
}

==== Response signature ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,NONCE]
macSourceValue =
[102006S789528V180000129041.003BGN611423312029001254078164C9B34468610CF9F1Y2051420201016084515327A9A2E5CD173AF3F69A87F06E1F602ED]
Signature = [true]

Информация от търговеца към e-Commerce CGI

TERMINAL	V1800001
TRTYPE	90
ORDER	**114233**
TRAN_TRTYPE	**24**
NONCE	B1A1B57F8D66EF6B604690BF7141B53C
P_SIGN	AEC96B3551F4B951E91A5BE6DFD91AD6AF859D4358B7A5D7CD5E8E5B7B4C32E995A6B5FFDBC4265F535D16ED8D591E06DA57E7A05357C93153A13807E2FBA6BB7C9A94AE6B2F2253F9DB8A7D0273AB68B8B9A427814B2646C6585E51396A531BABB3A8EF034496EA0ECEB29379A3E97195FB65DF85B571537620C27FF33483FDD09E8E106EE02FC59B15E70C4D692BD8A3A269DAF24DCBF300B3AB9DA623F789855828AE876CB6304D43027F212EFDB3CD1271A809920725BB3A8A247C84824B468EBF55DDD0540B5E7B6E844BBE28FBA49B62A91BB623A05158DC0D8CD4E6B1FF6BEE0D0EA1012EB04E44E930A3D728F0178BC4458734A3E1D462EB5BEA259E

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, ORDER, NONCE]
macSourceValue	8V1800001290611423332B1A1B57F8D66EF6B604690BF7141B53C

Таблица 11 Данни за проверка на статус на трансакция

Отговор от e-Commerce CGI (Трансакцията от тип 1 не е отменена):

{
"ACTION":"3",
"RC":"-24",
"STATUSMSG":"Transaction context mismatch",
"TERMINAL":"V1800001",
"TRTYPE":"90",
"AMOUNT":"",
"CURRENCY":"USD",
"ORDER":"114233",
"TIMESTAMP":"20201016084907",
"TRAN_DATE":"",
"TRAN_TRTYPE":"24",
"APPROVAL":"",
"RRN":"",
"INT_REF":"",
"PARES_STATUS":"",
"ECI":"",
"CARD":"",
"NONCE":"B1A1B57F8D66EF6B604690BF7141B53C",

"P_SIGN":"774F0E62105F5AEED1AED347D81AC12E122423F3E5F0DFBA2DEA3E93D9FC30EFBA9067E6F8A26DA4F44A9CB1B1824A942DA759B051C14CD5D303AA2A11285382C2CFD6B1188ED0DA2E4D1B5E33143DF8A27F0D785749597F7269A40A44113FE5EEF7ACD6D4B0A924053538462BF9F7C58FBD0CB3AC47E61EA039F6A0693B992E1AD0CA278D6B9BC2BA0F3BB1FFDCBCA68D631D7B00B8877004E8C758E335EF3C46E468D9A06C2F94FBF0753FF95A33404FBD8F9BFCB4D60AAA593C5C37AF9BEC3FFCA234B419528A635FCBAA8ED498D1A68834FF71C62286EF5DCC6992EAED703B6AAC262225A655874E8B7277138E68DD8886C44930E7814661B5F9006C0013"
}

==== Response signature ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,NONCE]
macSourceValue = [133-24-8V1800001290-3USD6114233----142020101608490732B1A1B57F8D66EF6B604690BF7141B53C]
Signature = [true]

Отговор от e-Commerce CGI (Трансакцията от тип 1 е отменена успешно):

{
"ACTION":"0",
"RC":"00",
"STATUSMSG":"Approved",
"TERMINAL":"V1800001",
"TRTYPE":"90",
"AMOUNT":"1.00",
"CURRENCY":"BGN",
"ORDER":"114233",
"TIMESTAMP":"20201016085138"
"TRAN_DATE":"20201016115039",
"TRAN_TRTYPE":"24",
"APPROVAL":"S78952",
"RRN":"029001254078",
"INT_REF":"4C9B34468610CF9F",
"PARES_STATUS":"",
"ECI":"",
"CARD":"",
"NONCE":"E8CAC1D2FBE11A899204AED74C02BDEC",
"P_SIGN":"9C22C8E340976C8360B7CB53C5EC90B99BA9A67EE86FE703715766ED3BF8490366C43B579DD1454C0C38B4D31CCD94515EA63AF97FFEB9884234B907B92E4FDF5CF7E806C114C2211BD800E0A659EC35CFD45F0027F05FA66C6F5468982743581416DA42EDC33EDC83537CB57598D527DE193C7BAA360E383CA7172AC0720A50BE2A3530008E8C867427B69CEC9A281907ECE7584BAA49D287BA33F80B49E7857E57509E69CF1F54D83555BF2258F45D36CC4764F9F5803F3D6710FF2F1A82AE4CD345BBB40102563FCA605479759D9E6C1CACBF3A9B1D48BFEC17388261782745CECEE27E3B75A106E0560A2D2403A5EE9DB38932E995D920F38875ABA2D3AF",
}

==== Response signature ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,NONCE]
macSourceValue = [102006S789528V180000129041.003BGN611423312029001254078164C9B34468610CF9F--142020101608513832E8CAC1D2FBE11A899204AED74C02BDEC]
Signature = [true]

7.3 Пример за отмяна на плащане

Полетата, с данни от оригиналната трансакция, са удебелени.

Информация от търговеца към e-Commerce CGI:

TERMINAL	V1800001
TRTYPE	24
AMOUNT	1.00
CURRENCY	BGN
ORDER	**145659**
DESC	Детайли плащане.
MERCHANT	1600000001
MERCH_NAME	Мол България
MERCH_URL	http://www.borica.bg
EMAIL	merchant@borica.bg
COUNTRY	BG
MERCH_GMT	+03
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	125353ORD@<n>
TIMESTAMP	20201014095541
RRN	**028701253242**
INT_REF	**B7A68A9F37E8586E**
NONCE	7D51498A3C22B86DD57EFB699A175714
P_SIGN	35917C0FF8B74F5537F871028E1B21391945C54DB837770192FAFA1523DA236500DCE232C598B50E0275236299FF6CAD3F730325F90BFC2BA3865D3594C6E9896FF50C086E722410DEBDB44F87114A56BA3228F29BB4CC2CA3D1960033DF49811B80624D8978619E2C77DBE4BBDA72F64C677A781184B70BC4B8C7AC8423A754C6E50E2E4AB5E165FBE5153D17108B79ABBC2DC9164ABE3A6178BF3379725A28C0B6F65706CC344AA087578FD56B0C24E600352710E54123D457EE2EBC0854108618D7147877F34650F0D6D13E22A7D6E1E9B8B3F10873D031A0DB7D6340B9DAE2FE2262852C90B943BEB5B44D1EFB95DEBC67A29643596D3DA415AC11E7C1DC

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, ORDER, NONCE]
macSourceValue	8V18000012906120353 32DB06A1A6494937428EEDEEDA5B3908E8

Отговор от e-Commerce CGI:

{
"ACTION": "0",
"RC": "00",
"STATUSMSG":"Approved",
"TERMINAL": "V1800001",
"TRTYPE": "24",
"AMOUNT": "1.00",
"CURRENCY": "BGN",
"ORDER": "145659",
"TIMESTAMP": "20201014100040",
"TRAN_DATE": "20201014125901",
"APPROVAL": "S19527",
"RRN": "028701253242",
"INT_REF": "B7A68A9F37E8586E",
"PARES_STATUS": "",
"ECI": "",
"CARD":"",
"NONCE": "7D51498A3C22B86DD57EFB699A175714",
"P_SIGN":
"4B2C8E02632CA1A753CF9904DF782A2015C8C70546D154842451F5C97ED348D242FBC367CFB91FAAFA53ED2537BF7747CFC2680E3689AD08AC0D0D97C5FE29B2ED2CF8AA8A12E709021FC9C2A179C993A4D673A80F4C27A76D4141DC85D394BBCCA1977196042D81AEA907B77B507F95FA4210B13E65D68965294110E483B42D3E1E27FFC06F566A2741BA48FD97092B20896CF8C66523E92AA1AD2D43CDEDFB21DA875E06581D94B51375FCBC772B93EA91C191DF9BE4C531D5D5FD9E9FE5F8E840B464BDA150D1AC00D28F58750E0C45F4C62BB8D13A5311E59F8201CCDA601AD47526ED542535E428ED77DBD194E4E87876A270A7E743873F191639D2DDD7"
}

==== Response signature ====

macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,NONCE]

macSourceValue = [102006S195278V180000122441.003BGN614565912028701253242 16B7A68A9F37E8586E--142020101410004032 7D51498A3C22B86DD57EFB699A175714]

Signature = [true]

Резултатът RC=00 показва, че трансакцията е отменена успешно.

7.4 Пример за първоначална авторизация

Информация от търговеца към e-Commerce CGI:

TERMINAL	V1800001
TRTYPE	12
AMOUNT	3.00
CURRENCY	BGN
ORDER	170000
DESC	Детайли плащане.
MERCHANT	1600000001
MERCH_NAME	Мол България
MERCH_URL	http://www.borica.bg
EMAIL	merchant@borica.bg
COUNTRY	BG
MERCH_GMT	+03
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	170000ORD@<n>
TIMESTAMP	20201012140015
NONCE	C3ACF912658C0A2310EA5AAAF739E627
P_SIGN	7F680909B85924364567937EA4500812022980A0CE047C39B5972123558BBD5B74FF8A1BE4C24C88C691E8B5815858958A9BA979A83D9884EAC807214100399665FAAAFBAF8F4BBB8FB0210FC70A907415899600640D00E87F052B4DA4CF322BBAA126C98033235E8BE3CFA1EF4079B0AD1EC5E490496D2CFA6D0A6CED1ACE747E54D4BCA0F494C530E413F23E2C7C2C9765AFA700F43C537547AC41F484C12B3BD2D006070A65EF634136744981722FE9D2173AC60015B43D243E32552FDE2ED13CC028B697F7498A6CAEBDC406B5A7B5F04920061ED5D6DDCAFF87AD284351E1E44AFD73C03D767B5E4B6D908AA9CDD88F1E65CE118D7938D01DAC06D65B8B

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE]
macSourceValue	8V180000121243.003BGN617000010160000000114202010121400153 2C3ACF912658C0A2310EA5AAAF739E627

Таблица 12 Данни за първоначална авторизация

Отговор от e-Commerce CGI:

Parameter	Length	Value
ACTION	1	2
RC	2	05
STATUSMSG	8	Approved
TERMINAL	8	V1800001
TRTYPE	2	12
AMOUNT	4	3.00
CURRENCY	3	BGN
ORDER	6	170000
TIMESTAMP	14	20201012140349
TRAN_DATE	14	20201012170349
APPROVAL	0	
RRN	12	028601253175
INT_REF	16	04F45801DAF13E22
PARES_STATUS	1	Y
ECI	2	05
CARD	16	4341XXXXXXXX0044
NONCE	32	C3ACF912658C0A2310EA5AAAF739E627
P_SIGN	512	95F5FFF8779932EC04CFE19CC1F75AF01CA5050E8AED8222DA9B5E16ADDBABB6FC51B0FB5501C82FAE2919345F92961E8631CD5A8807DD907E4A32B34B47B4F783EF99C3A4F37B7AB6726DE79FEF0E6E55A5F467ABA82DB3E3C0A8AC09A1E1D7F0D67A83418DC1DF5D362C94774467FA5656F7827C469C307743E93C73DB434940B002E02B0EE2FBC8A8ADB33CC69F3DF6C6D0E69F5042D5C171C840CA296928BEBD79DB9F3D3D2428730C1BEA2261C80DB1A0511687A5D77F242CBE42B204B57B6BDC7F31DDF6027D55E9CE584B101DF5520DD26A399C6D05759C1651B320C176CA206AA775DAA1D7288C60DEB12508DE2DF49A2F308BB28059EEA8FEC3BE0C

==== Response signature from ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,NONCE]
macSourceValue = [12205-3BGN43.008V18000012126170000120286012531751420201012140349 1604F45801DAF13E221Y20532C3ACF912658C0A2310EA5AAAF739E627]
Signature = [true]

Таблица 13 Данни за отговор за първоначална авторизация

7.5 Пример за завършване на първоначална авторизация

Полетата, с данни от оригиналната трансакция, са удебелени.

Информация от търговеца към e-Commerce CGI:

TERMINAL	V1800001
TRTYPE	21
AMOUNT	3.00
CURRENCY	BGN
ORDER	**162021**
DESC	Детайли плащане.
MERCHANT	1600000001
MERCH_NAME	Мол България
MERCH_URL	http://www.borica.bg
EMAIL	merchant@borica.bg
COUNTRY	BG
MERCH_GMT	+03
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	170075ORD@<n>
TIMESTAMP	20201012141516
RRN	**028601253167**
INT_REF	**92339532D5866339**
NONCE	CCF64A57E0B9E35D2E01DF4A3805DC58
P_SIGN	30C6A7AF32710144583C62F1E3B5A21660C0BF952673FBC85AE044D3D84BF516086B90D0F5BCCCF78B8210CFC63BB5F5BE74C9DE1EEB671FCC311C96A8AD0C5B31DBE15272B0CC6C561CBA2EADD31DD0198D0B1D9490A96E649179AC6FCC7DAABCFF44F886AA3C43FE707E34AAC291CC2561AB267C9A7C20B926F145655A83801CEAA9A8F934F872BFD9EE808C1A8D0C015215ADEB3B98E028550451FEBF4AAB80E4909E1247A5B9E84B7B78E7135D358424A683D8297DC6C1027F1A91A4B3B14B870A0AD958B6D1F944AA26EFC9A54832469E110AA5CE738738936433F9B0CDD001617FE628E9512B06541B46652B929DCB196A4FF414B72058FAAE93913A0E

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE]
macSourceValue	8V180000122141.003BGN6162021101600000001142020101214151632CCF64A57E0B9E35D2E01DF4A3805DC58

Таблица 14 Данни за завършване на първоначална авторизация

Отговор от e-Commerce CGI:

{
"ACTION": "3",
"RC": "-20",
"STATUSMSG":"Invalid amount",
"TERMINAL": "V1800001",
"TRTYPE": "21",
"AMOUNT": "1.00",
"CURRENCY": "BGN",
"ORDER": "162021",
"TIMESTAMP": "20201013174253",
"TRAN_DATE": "20201013204253",
"APPROVAL": "",
"RRN": "028601253167",
"INT_REF": "92339532D5866339",
"PARES_STATUS": "",
"ECI": "",
"CARD":"",
"NONCE": "CCF64A57E0B9E35D2E01DF4A3805DC58",
"P_SIGN":
"B2F33F1BE13EDAD498E67A01720AFABD93454C1506038F374EA7B771039C15B6A7C24B2FB9EBA7FEFDE49052118561A09D3D9CFEC98D3A17A8058725EF2E9909C8EF5DDD499B8CBCF5606770588B110B18A1014636F8B6A7CE9F17A3023B6499602A8BE53D3E83FC0FAD97D61B0DCD0DC2C3FBE6600B4B91A8576C34F058FEF80254F4E089567C154EDA67DD6CB997425251C6E4EA4A8531EC1724CA7AC8C9BE11438EBF86CE2B486326EAC03AF8005C443F1B32690B8031774903F847499C1F6080F626EDD5568A41341F70546F90DF67F8980BD3F391D33928554B62A4744A2B331C3350AAE64D0DE3801FE40B73DD89A772D5093D502035AE90D081A85CE8"
}

==== Response signature ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,NONCE]
macSourceValue = [133-20-8V180000122141.003BGN61620211202860125316716923395 32D5866339--142020101317425332CCF64A57E0B9E35D2E01DF4A3805DC58]
Signature = [true]

7.6 Пример за отмяна на първоначална авторизация

Полетата, с данни от оригиналната трансакция, са удебелени.

Информация от търговеца към e-Commerce CGI:

TERMINAL	V1800001
TRTYPE	22
AMOUNT	1.00
CURRENCY	BGN
ORDER	**170000**
DESC	Детайли плащане.
MERCHANT	1600000001
MERCH_NAME	Мол България
MERCH_URL	http://www.borica.bg
EMAIL	merchant@borica.bg
COUNTRY	BG
MERCH_GMT	+03
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	095949ORDnnn
TIMESTAMP	20201014070415
RRN	**028601253175**
INT_REF	**04F45801DAF13E22**
NONCE	D1AA7234EF80331750C61FCCDCE7C5C7
P_SIGN	41D458281E2E682B70F233457C0887F08838398FB8196A059BD4A7C1CCAAF6E880874E233F65A04778B242F57D4C4EBE0A4E407AF7B0FCA0B7AB53E6FDE19B03591475FE9F6D6FDE60B5DE02E9006A8A7F546B140454F9F07A7E7217B4213E7F09B9DC4ABAE6D8322615D12BF5DEE5E52B5CABF939A9F4DD93D0A6325AC167A0FE77EE033A1CEE5C8A842B6D92040B30A6661F84E7DC150755689259CB9D6787C9E28A9C175B5162DF139A19AC3D752CA80F3EE2FE87874FEE891DF8872E0D2AAADEB290726E212D9C440E558463B1D48AFB5276B30F0609DA32AD5129D1C7D3C6200E5B008C42481E3018927602E99129F73EFCE16ECA4A6D7C41C94297DC30

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE]
macSourceValue	8V180000122241.003BGN6170000101600000001142020101407041532D1AA7234EF80331750C61FCCDCE7C5C7

Таблица 15 Данни за отмяна на първоначална авторизация

Отговор от e-Commerce CGI:

{
"ACTION": "2",
"RC": "95",
"STATUSMSG":"Invalid amount",
"TERMINAL": "V1800001",
"TRTYPE": "22",
"AMOUNT": "1.00",
"CURRENCY": "BGN",
"ORDER": "170000",
"TIMESTAMP": "20201014070617",
"TRAN_DATE": "20201014100617",
"APPROVAL": "",
"RRN": "028601253175",
"INT_REF": "04F45801DAF13E22",
"PARES_STATUS": "",
"ECI": "",
"CARD":"",
"NONCE": "D1AA7234EF80331750C61FCCDCE7C5C7",
"P_SIGN":
"885457783119E64E93D346C38D1050D5A848B97FB8319874CAE1BAB898D6E53B818E2FC83C96C754983B9B0C727FC25BB30A
67455DAA8CF67A5DE9086DE0A96F10FAEE8F7A8D27A9B9FEC69F956DC95E250D970FE380D65F8A99B1115B9B289E2C633D6
CB993246B383A6CC133233F9A14C9EEA554832AD58368893212CCFECDD8268498BF0B307BD414805DA7D23D1B297250B3AE3
CF9164256387E4BF4C386424886BC18B33B43808CECC436F2EE2C4A4114B8609D2D60E836DDA6B82D0BB5CFED1FC8581418
EE4FFAA34828B94B384CF2F22B043894666E13B3BA429FEFD9FAC1D67614927AB11B86141F69DBD2365E868F1B3BA250199C
1CE4D016EF59F0"
}

==== Response signature ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,N
ONCE]
macSourceValue = [12295-8V180000122241.003BGN617000012028601253175160 4F45801DAF13E22--
142020101407061732D1AA7234EF80331750C61FCCDCE7C5C7]
Signature = [true]

7.7 Пример за повторна трансакция при Soft Decline

В поле M_INFO е попълнена стойност "threeDSRequestorChallengeInd":"04", Base64 кодирана, което инструктира ACS на издателя да бъде извършена пълна автентикация.

Информация от търговеца към e-Commerce CGI:

TERMINAL	V1800001
TRTYPE	1
AMOUNT	1.00
CURRENCY	BGN
ORDER	099001
DESC	Детайли плащане.
MERCHANT	1600000001
MERCH_NAME	Мол България
MERCH_URL	http://www.borica.bg
EMAIL	merchant@borica.bg
COUNTRY	BG
MERCH_GMT	+03
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	099001ORD@<n>
TIMESTAMP	20201014070418
M_INFO	eyAidGhyZWVEU1JlcXVlc3RvckNoYWxsZW5nZUluZCI6IjA0IiB9
NONCE	D664F6A61A6F4B2CE72A43A3B5165A44
P_SIGN	3D89692A3C2C02B94DF0B5A96565AF25B7EA38FD3413B506611E0EDDEF1C9C7A62D3C4005F8A7D0404ECAE0B945E3E1CB215C65ADBC592D37A6C2D7F6E936D877099BB5446AEFBA1C95AEA7E3D8263CFDEF7FEBE1D990CCCFF7E1A6B3FF889673DAC69A9107FDA24C19675896C316A44EC857C23E897278B6420A9188EDF60ADC0691B9AD26E982624A4C1F8CC2E1DD3786BDC65130172302509B23920DE0458CEDC79DF99B32A349563900F1153E78BAAAAB10ECD5870DDF21FF3EECA6B47F9004395B639E4E81F72E4D6A72C52D7486F8724E000E128350F02E12AE9CFDC6C78303106282BB79972E1D46B5C97FCA9833A4208769D50946DE278862485C1D1

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE]
macSourceValue	8V18000011111.003BGN990011016000000011420201014070418D664F6A61A6F4B2CE72A43A3B5165A44

Таблица 16 Данни на съобщението при плащане

8. Тестови карти

При извършване на тестове се ползват следните тестови карти:

8.1 Карти, за които се получава съответен резултат според PAN

Тип на карта	Номер на карта (PAN)	Реакция на APGW / Reponse code	Response Code Описание	Изисква тестов ACS
Mastecard	5100770000000022	Response code = 00	Successfully completed	Не
Mastecard	5555000000070019	Response code = 04	Pick Up	Не
Mastecard	5555000000070027	Системата се забавя 10 сек. за авторизация, Response code = 13	Invalid amount	Не
Mastecard	5555000000070035	Timeout, Response code = 91	Issuer or switch is inoperative	Не
Visa	4341792000000044	Response code = 00 Това е пълен тест с автентикация от тестов Visa ACS и авторизация. Може да бъде използвана за тестване на Soft Decline.	Successfully Completed	Да, паролата е 111111 за сума над 30.00 лв.

Таблица 17 Тестови карти, за които резултат се получава според PAN

8.2 Карти, за които се получава съответен резултат според сумата

Тип на карта	Номер на карта (PAN)	Реакция на APGW / RC	Изисква тестов ACS
Visa	4010119999999897	Зависи от сумата. Виж таблица 23	Не
Mastecard	5100789999999895		Да, паролата е 111111

Таблица 18 Тестови карти, за които резултатът е според сумата

Сума от	Сума до	Реакция на APGW / Reponse code	RC Описание	Коментар
1.00	1.99	01	Refer to card issuer	Код 01 може да бъде заменен с код 05 при обработка на трансакцията в National Switch
2.00	2.99	04	Pick Up	
3.00	3.99	05	Do not Honour	
4.00	4.99	13	Invalid amount	Response after 10 sec
5.00	5.99	30	Format error	
6.00	6.99	91	Issuer or switch is inoperative	

7.00	7.99	96	System Malfunction	
8.00	8.99	82	Timeout	
30.00	40.00	01	Refer to card issuer	
50.00	70.00	04	Pick Up	
80.00	90.00	05	Do not Honour	
100.00	110.00	13	Invalid amount	Response after 10 sec
120.00	130.00	30	Format error	
140.00	150.00	91	Issuer or switch is inoperative	
160.00	170.00	96	System Malfunction	
180.00	190.00	82	Timeout	
10000.65	10000.65	65/1A	Soft Decline	

Таблица 19 Очакван резултат според сумата на трансакцията

За целите на тестовете се въвеждат произволни стойности за валидност на карта и CVV/CVC, съобразени с формата на полетата – дата MMYY (MM – 01…12, YY- 00…99), CVV/CVC – три цифри.

9. Кодове за грешка, използвани от CGI e-Gateway

В следващата таблица са изброени най-често използваните кодове за грешка при обработка в APGW (поле RC)

RC	Description	Описание
-1	A mandatory request field is not filled in	В заявката не е попълнено задължително поле
-2	CGI request validation failed	Заявката съдържа поле с некоректно име
-3	Acquirer host (TS) does not respond or wrong format of e-gateway response template file	Авторизационният хост не отговаря или форматът на отговора е неправилен
-4	No connection to the acquirer host (TS)	Няма връзка с авторизационния хост
-5	The acquirer host (TS) connection failed during transaction processing	Грешка във връзката с авторизационния хост
-6	e-Gateway configuration error	Грешка в конфигурацията на APGW
-7	The acquirer host (TS) response is invalid, e.g. mandatory fields missing	Форматът на отговора от авторизационния хост е неправилен
-10	Error in the "Amount" request field	Грешка в поле "Сума" в заявката
-11	Error in the "Currency" request field	Грешка в поле "Валута" в заявката
-12	Error in the "Merchant ID" request field	Грешка в поле “Идентификатор на търговеца” в заявката
-13	The referrer IP address (usually the merchant's IP) is not the one expected	Неправилен IP адрес на търговеца
-15	Error in the "RRN" request field	Грешка в поле "RRN" в заявката
-16	Another transaction is being performed on the terminal	В момента се изпълнява друга трансакция на терминала
-17	The terminal is denied access to e-Gateway	Отказан достъп до платежния сървър (напр. грешка при проверка на P_SIGN)
-19	Error in the authentication information request or authentication failed.	Грешка в искането за автентикация или неуспешна автентикация
-20	The permitted time interval (1 hour by default) between the transaction timestamp request field and the e-Gateway time was exceeded	Разрешената разлика между времето на сървъра на търговеца и e-Gateway сървъра е надвишена
-21	The transaction has already been executed	Трансакцията вече е била изпълнена
-22	Transaction contains invalid authentication information	Транзакцията съдържа невалидни данни за автентикация
-23	Invalid transaction context	
-24	Transaction context data mismatch	Заявката съдържа стойности за полета, които не могат да бъдат обработени. Например валутата е различна от валутата на терминала или транзакцията е по-стара от 24 часа.
-25	Transaction canceled (e.g. by user)	Трансакцията е отказана (напр. от картодържателя)
-26	Invalid action BIN	Невалиден BIN на картата
-27	Invalid merchant name	Невалидно име на търговеца
-28	Invalid incoming addendum(s)	Невалидно допълнително поле (например AD.CUST_BOR_ORDER_ID)
-29	Invalid/duplicate authentication reference	Невалиден отговор от ACS на издателя на картата
-30	Transaction was declined as fraud	Трансакцията е отказана
-31	Transaction already in progress	Трансакцията е в процес на обработка
-32	Duplicate declined transaction	Дублирана отказана трансакция
-33	Customer authentication by random amount or verify one-time code in progress	Трансакцията е в процес на аутентикация на картодържателя
-40	Client side transaction form in progress	Трансакцията е в процес на обработка

Таблица 20 Допълнителни кодове за грешка, ползвани от CGI протокола

В следващата таблица са изброени най-често използваните кодове за грешка при обработка на трансакцията от издателя по протокол ISO-8583 (поле RC)

Код	Описание
00	Successfully completed
01	Refer to card issuer
04	PICK UP
05	Do not Honour
06	Error
12	Invalid transaction
13	Invalid amount
14	No such card
15	No such issuer
17	Customer cancellation
30	Format error
35	Pick-up, card acceptor contact acquirer
36	Pick up, card restricted
37	Pick up, call acquirer security
38	Pick up, Allowable PIN tries exceeded
39	No credit account
40	Requested function not supported
41	Pick up, lost card
42	No universal account
43	Pick up, stolen card
54	Expired card / target
55	Incorrect PIN
56	No card record
57	Transaction not permitted to cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
85	No reason to decline
88	Cryptographic failure
89	Authentication failure
91	Issuer or switch is inoperative
95	Reconcile error / Auth Not found
96	System Malfunction

Таблица 21 Кодове за грешка при обработка от издателя на картата

10. Приложение 1:

10.1 Пример за цифров подпис на PHP:

```
<?php
//Borica Sign Data, private key without password
//execute in https://wtools.io/php-sandbox

//Private key (privatekeyname.key)
$priv_key = '-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQC5z1/LHY1GcX9f
vMOBZPx3edgmqFkPd7eV136Nog9+VeM4UMfg22d64LAwpRHdfFigTPkc9leR68xT
JXGeiiGJSaG+Vb9oUK3yb9W7YMhk1vJy4p2oyo77Sirki4bhh8RPIVWAqeVUgEL/
f5ZuZSNzB2cFkUOknbRwM/j98fft4lgZN/nYkYjW22UaPA7ULEBMxmQUKrJKi04S
PVIG1iKzLh3jVyRsxi+giFrlQ+/jVWA0wJm8B25jsRcwObjL6+MczutVKmaNjaVy
FNkBtLOWSCf4A6i4xOfafWoEx4tEa4Dl5PTqQI4PBvH6SW3lKulfNpa5m1wvnlA3
hFy9IfUPAgMBAAECggEBAJz/stl9yxQ9bEGpjovzlzsgcdngHzhpkG6EocLsryix
S4dXAjxlRp9V4KmJoHnDymLQByFIqJ98XK3YkpNB5apJ0+euLkfm+8NAaZik404J
LNyTzGFFneCIP4vStQo1HFM8ODG53DM1GOcnmCT5QiW8mHjk0AH02vR/haCU5kdR
qQeMBnGAuqOcO3T7QcuK2AMO7BoGrkq0+V58DyCdf1UpeLoi71HCdBpj8FPHcU0H
ScsPUrWXSkJSVj7R68AUtI4Sss3CEk7DbbSLcW1DfmX6esujM/fx1SLc9Bue4Ipa
0ec7wKvvMbLap0gWOOxZGRtxS9ALJ3T75AOjDx38q6ECgYEA86cPMYUePy/l9CEu
F2fsr0LnpB3clwEhhMeIIjKMCTVnPlHMy8Sm9WrRdErKMpsIbOWgeIqUaPPCt3NZ
FTgJnIJnFR4KI5qPOb3ZRA9OI6eliVvdgxe7e/bHe74b/v/uE6378ddtniHCIvgk
6Oi9/luImv3kYzX1pmJr/8VZQdECgYEAwznqU1QiPaUFtZwkb3hIoTcIYlKwIbmP
3HYdsS2p20WHh3XJC9nojABIBgJJYKdACzQyIy1FJJ3ga0fgkSZ5KL1LXmclXXL6
lzdQNIyF/boRP+XC7fB9MNwIClqJCnmciKWE4xCt9GgEiLnJDYnOhGiQ50BuxJFn
RU6RxjAPoN8CgYEA3LmYr/mx/vf7T3/Ha3jAF716b1iF/14M6WaA0soLxkPUtcYQ
yv/paCZOfRVLuzBrH4ueJdUUwUciPGKIbwqG2nvfumeuM7bOzTZJXrimxvlWqirl
rvuO4qwa5uTAI+/h034n4VyRd1GJt3gop75Ab+6oABDFF4NIeGRtBhXX2CECgYB9
/QRCHouyaKsUlt3UqjWFBPT+LwrH2O8EgZ2L2EJD5c0fGF5UrZ4rq4rPhe5A1+62
zEqG9RIoHVLVKR+9zKxoJDFdjQdKFYeuyt2R7BYUtl2ndOmlkIvaWkU+GUtTXUQt
01O9DeiVUAONEQi1GfgS70CEXMqfRI725UuiMSYE1QJ/EkPO8VPbWf+BgKovYFf1
AsStOfMMvrgVn8e/vZmWluaGb40L34Dxuvv3YRk1EsQFirGZ5XDDCm5r8H1IY8Ne
PXnxLP2opIuch1JHQdebFZqN1C68pX6hopEixOmwShhaNXNJ5RN8c9q+4NXIu73n
lKFJBDsxoMVB/VEoVeQEMg==
-----END PRIVATE KEY-----';
//Private key password. Leave empty if there is no password.
$priv_key_password = '';

//Data you want to sign
//MAC_EXTENDED = TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, MERCHANT, TIMESTAMP, NONCE
$data = '8V18000011141.003BGN611392010160000000114202010130839323 2D41AAAFC7F8119A3BB7C4868E0B256F9';

$pkeyid = openssl_get_privatekey($priv_key,$priv_key_password);
echo 'Private Key Result: '.$pkeyid.PHP_EOL;
echo 'Data: '.$data.PHP_EOL;

openssl_sign($data,$signature,$pkeyid,OPENSSL_ALGO_SHA256);
openssl_free_key($pkeyid);

echo PHP_EOL;
echo 'P_SIGN = '.strtoupper(bin2hex($signature));
?>
```

10.2 Пример за проверка на цифров подпис на PHP:

```
<?php
//Borica Verify Signature in Response
//execute in https://wtools.io/php-sandbox

//Certificate containing the public key (MPI_OW_APGW_B-Trust.cer)
$pub_key = '-----BEGIN CERTIFICATE-----
MIIGWjCCBEKgAwIBAgIIQSHpHDZ7ASAwDQYJKoZIhvcNAQELBQAwgYoxCzAJBgNVBAYTAkJHMRgw
FgYDVQRhDA9OVFJCRy0yMDEyMzA0MjYxIDAeBgNVBAoMF0JPUklDQSAtIEJBTktTRVJWSUNFIEFE
MRAwDgYDVQQLDAdCLVRydXN0MS0wKwYDVQQDDCRCLVRydXN0IFRFU1QgT3BlcmF0aW9uYWwgQWR2
YW5jZWQgQ0EwHhcNMjAwOTEwMDg0NzU5WhcNMjMwOTEwMDg0NzU5WjBkMRQwEgYDVQQDDAtNUEkg
T1cgQVBHVzELMAkGA1UECwwCSVMxEjAQBgNVBAoMCUJvcmljYSBBRDEOMAwGA1UECAwFU29maWEx
DjAMBgNVBAcMBVNvZmlhMQswCQYDVQQGEwJCRzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAMmtJ1gcFkdfY/wfEk3IbqAA1dveXj9J3dCNyliHoooj1ePsX86jlYLijrdPOgayESwH01OO
nVEbcF9z2qoicH12vJaa9ZEFgqkB+qv55erfQOTjgVhd+KRb8YES+uEGkIFE8D/peLMeKeiRSleN
corRa4J1ms/V/2Oklxg0xSnEXw8tRa0U2OoPlEwCbT01DgPMoud5EitpTvD9/gc69aWgVS477Erf
ro+CW89bLGNiHh6mmZt71uIXugNtGf2RhP59fmEKBKj+DSF1QI65SVvv2eYb6JBlhHX+hZss/oAN
xvqYFSG4k6L1tkoDwctB+q7p1EbWEuqDNxYT0RidkLkCAwEAAaOCAecwggHjMB0GA1UdDgQWBBTT
nQwEEjMqWryNqt8onGmGk6nm4DAfBgNVHSMEGDAWgBT1J8z325solCubZvApcg6KPWLcmDAgBgNV
HRIEGTAXhhVodHRwOi8vd3d3LmItdHJ1c3QuYmcwCQYDVR0TBAIwADBNBgNVHSAERjBEMEIGDCsG
AQQB+3YBBwEEAjAyMDAGCCsGAQUFBwIBFiRodHRwOi8vd3d3LmItdHJ1c3Qub3JnL2RvY3VtZW50
cy9jcHMwDgYDVR0PAQH/BAQDAgOoMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBUBgNV
HR8ETTBLMEmgR6BFhkNodHRwOi8vY3JsdGVzdC5iLXRydXN0Lm9yZy9yZXBvc2l0b3J5L0ItVHJ1
c3RUZXN0T3BlcmF0aW9uYWxBQ0EuY3JsMIGHBggrBgEFBQcBAQR7MHkwJwYIKwYBBQUHMAGGG2h0
dHA6Ly9vY3NwdGVzdC5iLXRydXN0Lm9yZzBOBggrBgEFBQcwAoZCaHR0cDovL2NhdGVzdC5iLXRy
dXN0Lm9yZy9yZXBvc2l0b3J5L0ItVHJ1c3RUZXN0T3BlcmF0aW9uYWxBQ0EuY2VyMBYGA1UdEQQP
MA2CC01QSSBPVyBBUEdXMA0GCSqGSIb3DQEBCwUAA4ICAQAUJfDjTROuVORLojCzVQdppoiPs3hX
Ra/9MaNIUP5xII0AamWmN7bTDQpnNfw5tlo8DPSBIMfP+5xJyfMTHAi43i+7vf1t1ZucEbVJ73FF
zdzZQaxw9NY0n0IBBz8WEnkaGewh45aQ6XMgNe5xcKbtP2vqq+qZiy0eyIHJwaQORKyZ9+jBlnVo
ZdzUbDrrSEMka98IQ52XO8EPbCmB/GhJlZ991yNo5/PVsFxT9sjG3VGm+sStD3G7+pjX+HsHLn65
gwWq2oRiQqe62W/HSNb5dnIWqIJldT4Zd0Ar97hQwU1ZQVnmL5ZjswsjafI7B/0N4U5QzbOvWX1W
oDXCCqmXAoTP1DDEWJ0vmvVDHGrrC0rIbluBdzQEK/D1f3A1jlCzQPyKOwUuafLlpCX17b09Zwxi
45prDk/LBqE6CI6CM+8nF0QyN3Th+r2IqUuhGpfLApGlp6sJvJdAhnqX1VCGJCdozIhzrEJ4oha3
/+HijQl+vUaYevk1d/EipZNHU1gkcocrj2qmTMOKzEw9zDs5jVSgtBZTUF5ORwUNiTXj7EZUnQUC
wANFl8k0EcWPhkU5L7v9/9rcGkMcm0S3bM5rbKksabvq01cvxkepS5qqvbxgugci/8sPCXMAThCK
eiJHilEt1uns+tFA+7RSVFKOpf07g3DBGYf5P8qKLQCFMg==
-----END CERTIFICATE-----';

//Public key (MPI_OW_APGW_B-Trust_pubkey.pem)
/*$pub_key = '-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAya0nWBwWR19j/B8STchu
oADV295eP0nd0I3KWIeiiiPV4+xfzqOVguKOt086BrIRLAfTU46dURtwX3PaqiJw
fXa8lpr1kQWCqQH6q/nl6t9A5OOBWF34pFvxgRL64QaQgUTwP+I4sx4p6JFKV41y
itFrgnWaz9X/Y6SXGDTFKcRfDy1FrRTY6g+UTAJtPTUOA8yi53kSK2lO8P3+Bzr1
paBVLjvsSt+uj4Jbz1ssY2IeHqaZm3vW4he6A20Z/ZGE/n1+YQoEqP4NIXVAjrlJ
W+/Z5hvokGWEdf6Fmyz+gA3G+pgVIbiTovW2SgPBy0H6runURtYS6oM3FhPRGJ2Q
uQIDAQAB
-----END PUBLIC KEY-----';*/

//Data you want to verify (signed message)
//MAC_EXTENDED =
ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTA
MP,NONCE
$data = '112006S975398V18000011149.003BGN615474412028601253152169 7E2F39EFCA1CAF1--
14202010121600093 29EADBD70C0A5AFBAD3DF405902602F79';

//P_SIGN in hex from mpi_sign.php
$p_sign =
hex2bin('6FF21243639A23946393023839C0B549C6794C516E4C077F65DD476B700C0A53A9A23F1517B9F8F955C4E8E519
CFF1C9428B32F0259E8EA2284B244B39AA8E4E4A251D840479CB3DDB988F25674D1BEB97A814DB04E846FC9795058E2
BDC3A511CA503F15C71BD3F1687FF15FE9F8CA393555286CEB4A3B722683E1FFD7C30A6ED19C6EDB7D40A6356B12BD
4C010DD43D596753CC6BA52523EC5DB4E0BC48B8A99DDE2D1B946D504EA3A692C3E56DA3941E83F226EEEC109DAB3
6C3FEE70C89E2E54000E62AC53DB43B72E75597DA735CF513BFFD8D4A61F5468C8A77C9704E9B9BD8AB5167BA1DAD0
898CAF7BED831C7786F8E75100FB179657B05CC4EDA87E');


if (strpos($pub_key, 'CERTIFICATE') !== false) {
    $pkeyid = openssl_get_publickey($pub_key);
} else {
    $pkeyid = $pub_key;
}
echo 'Public Key Result: '.$pkeyid.PHP_EOL;
echo 'Data: '.$data.PHP_EOL;

//verify signature
```

```
$result = openssl_verify($data,$p_sign,$pkeyid,OPENSSL_ALGO_SHA256);
if (strpos($pub_key, 'CERTIFICATE') !== false) {
openssl_free_key($pkeyid);
}

echo PHP_EOL;
echo 'Result = '.$result.' ';
// 1- OK, 0 - Error
if ($result == 1) {
    echo 'Valid';
} elseif ($result == 0) {
    echo 'Invalid';
} else {
    echo 'Error: '.openssl_error_string();
}
?>
```