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: **4.0 / 15.07.2022**
Гриф: **C1 / ОБЩОДОСТЪПЕН ДОКУМЕНТ**

Хронология на измененията на документа				
Версия	**Автор (и)**	**Дата**	**Състояние**	**Коментар**
1.0	Сиана Кръстева	21.05.2020	Отменен	Първо издание на документа. Изменения, свързани с миграция към БОРИКА – Нова генерация
2.0	Сиана Кръстева	09.09.2020	Отменен	Второ издание на документа. Добавен списък с тестови карти и допълнителни уточнения
2.1	Сиана Кръстева	06.10.2020	Отменен	Добавени корекции
2.2	Емил Георгиев/ Сиана Кръстева	13.10.2020	Отменен	Въведен е метод на подписване MAC_EXTENDED
2.3	Емил Георгиев/ Сиана Кръстева	16.11.2020	Отменен	Унифициране имената на полетата в отговора за TRTYPE=90. Отговор в json формат за TRTYPE=21,22 и 24
3.0	Емил Георгиев	13.03.2021	Отменен	Добавени полета в отговора: AUTH_STEP_RES, CARHOLDERINFO, CARD_BRAND.
4.0	Емил Георгиев	15.07.2021	Утвърден	Въведен е метод на подписване MAC_GENERAL

Съдържание

1. Въведение 6
1.1 Цел и предназначение на документа 6
1.2 Определения и акроними 6
1.2.1 Определения 6
1.2.2 Акроними 8
2. Спецификация на интерфейса с е-търговец 8
2.1 Интерфейс на е-търговеца с Акцептиращ и платежен сървър на БОРИКА 8
2.2 Обмен на съобщения 10
3. Полета в съобщението при комуникация е-търговец - APGW 12
3.1 Полета в заявката от е-търговец към APGW 12
3.2 Полета в отговора от APGW към е-търговеца 14
3.3 Особености на полета на APGW интерфейс 17
4. Поддържани типове трансакции 18
4.1 Плащане 18
4.2 Проверка за статус на трансакция 19
4.3 Отмяна на плащане 21
4.4 Първоначална авторизация 22
4.5 Завършване на първоначална авторизация 24
4.6 Отмяна на първоначална авторизация 25
4.7 Повторна трансакция при Soft Decline 27
5. Криптографски операции 28
5.1. Цифров подпис за подписване на съобщение 28
5.2 Генериране на частен ключ за подписване на съобщенията с OpenSSL 30
5.3 Генериране на заявка за сертификат с OpenSSL 30
5.4 Задължителни полета на сертификата 31
5.5 Преобразуване на частен ключ и сертификат в PKCS12 формат с OpenSSL 31
5.6 Проверка на частен ключ / сертификат с OpenSSL 31
5.7 Сформиране на подписа в заявка към APGW 32
5.8 Проверка на подписа в отговор от APGW 33
6. Примери за трансакции 33
6.1 Пример за „Плащане“ 34
6.2 Пример за „Проверка статус на трансакция“ 38
6.3 Пример за „Отмяна на плащане“ 41

6.4 Пример за „Първоначална авторизация“ 43
6.5 Пример за „Завършване на първоначална авторизация“ 45
6.6 Пример за „Отмяна на първоначална авторизация“ 47
7. Тестови карти 49
7.1 Карти, за които се получава съответен резултат според PAN 49
7.2 Карти, за които се получава съответен резултат според сумата 49
8. Кодове за грешка, използвани от APGW 51
9. Приложение 1: 53
9.1 Пример за цифров подпис на PHP: 53
9.2 Пример за проверка на цифров подпис на PHP: 54
10. Приложение 2: 56
10.1 Стойности на AUTH_STEP_RES: 56
10.2 Стойности на ECI (Electronic Commerce Indicator) 57
10.3 Често задавани въпроси: 59

Фигури

Фигура 2-1 Схема на предаването на съобщение чрез HTTP POST 11

Таблици

Таблица 1 Полета, използвани за заявка към APGW 13
Таблица 2 Полета, използвани в отговора от APGW.....15
Таблица 3 Полета в заявка за трансакция „Плащане“.....18
Таблица 4 Статус на трансакция.....20
Таблица 5 Полета в заявка за трансакция „Проверка за статус на трансакция“.....21
Таблица 6 Полета в заявка за трансакция „Отмяна на плащане“.....22
Таблица 7 Полета в заявка за трансакция „Първоначална авторизация“ 22
Таблица 8 Полета в заявка за трансакция „Завършване на първоначална авторизация“ .24
Таблица 9 Полета в заявка за трансакция „Отмяна на първоначална авторизация“ 25
Таблица 10 Полета, участващи в сформиране на подписа, според вида на съобщението, по схема MAC_GENERAL 29
Таблица 11 Пример за сформиране на символен низ за подписване при плащане 32
Таблица 12 Пример за сформиране на символен низ за проверка на отговор при плащане 33
Таблица 13 Пример за заявка „Плащане“ 34
Таблица 14 Пример за отговор „Плащане“.....37
Таблица 15 Пример за заявка „Проверка статус на трансакция“ 38
Таблица 16 Пример за заявка „Проверка статус на трансакция“ 39
Таблица 17 Пример за заявка „Отмяна на плащане“.....41
Таблица 18 Пример за заявка „Първоначална авторизация“.....43
Таблица 19 Пример за отговор „Първоначална авторизация“ 44
Таблица 20 Пример за заявка „Завършване на първоначална авторизация“.....45
Таблица 21 Пример за заявка „Отмяна на първоначална авторизация“.....47
Таблица 22 Тестови карти, за които резултат се получава според PAN 49
Таблица 23 Тестови карти, за които резултатът е според сумата 49
Таблица 24 Очакван резултат според сумата на трансакцията.....50
Таблица 25 Допълнителни кодове за грешка, ползвани APGW.....51
Таблица 26 Кодове за грешка при обработка от издателя на картата 52
Таблица 27 Ниво на автентикация на картодържателя.....57
Таблица 28 Резултат от автентикация на картодържателя (Visa) 58
Таблица 29 Резултат от автентикация на картодържателя (Mastercard).....58

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 съобщения 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.

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

1.2 Определения и акроними

1.2.1 Определения

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

Първоначална авторизация (Pre-Authorization)
Тази трансакция се изпълнява на две стъпки. При първата стъпка акцептиращия 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 по-малка или равна на тази от първоначалната заявка. По този начин се завършва отложеното плащане.

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

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.

Виртуален търговец (е-търговец)
Субект (юридическо лице), който е в договорни отношения с акцептираща институция да приема плащания с платежни карти през интернет.

Merchant ID (MID)
Идентификационен номер на търговец. Предоставя се от обслужващата финансова институция.

Terminal ID (TID)
Идентификационен номер на терминал. Предоставя се от обслужващата финансова институция.

ВАЖНО! TID на терминала в среда за тестове и продукционна среда може да бъде различен.

EMV® Three-Domain Secure (3DS)
Протокол на съобщения, разработен от EMVCo., който позволява автентикация на картодържателите пред издателите на карти при извършване на трансакции в интернет, чрез разработените от картовите схеми системи за сигурни плащания Visa Secure, Mastercard ID Check, B-Secured, ProtectBuy. С използването им се осигурява възможността за обмен на по-голямо количество данни между участниците в процеса.

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

GUARDTIME
Максималното време за осъществяване на трансакция. В настоящата версия на интерфейса максималното време за осъществяване на трансакция е 15 минути (900 секунди).

Return URL (BackRef)
Адрес на търговеца, където се получават отговорите от платежния сървър на БОРИКА.

Merchant Portal
Приложение, през което търговците могат да наблюдават трансакциите, извършени на техните терминали. Намира се на адрес

Среда на разработчика за провеждане на тестове:

https://3dsgate-dev.borica.bg/mwp_cert

Продукционна среда:

https://3dsgate.borica.bg/mwp/static/

Ръководство за работа с приложението се получава от обслужващата финансова институция.

1.2.2 Акроними

ACS	Access Control Server (Сървър за контрол на автентикацията), който дава възможност на издателя на картата да участва в 3-D Secure
APGW	Acquiring and Payment Gateway, (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 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 APGW сървъра на БОРИКА.

Комуникацията между е-търговеца и APGW сървъра включва:

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

  Данните описват частта от трансакцията, свързана с е-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.

Всеки виртуален терминал може да роботи само в една валута. Необходимо е валутата в заявката да съвпада с валутата на терминала.

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

  Е-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 е-търговеца посредством HTTP Post.

  Е-търговецът отговаря за проверката на цифровия подпис на данните, за да удостовери, че резултатът е подписан от БОРИКА. Тестовият и продукционният публични ключове на БОРИКА са публикувани на https://3dsgate-dev.borica.bg/ Предоставени са в .pem формат или със сертификат (.cer).

  Всеки търговец трябва да предвиди процедура за подмяна на публичния ключ на БОРИКА.

  Адресът, на който е-търговецът получава отговорите от APGW (BACKREF) предварително се задава в системата за всеки терминал.

  Е-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) е-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.

  За да се провери резултата от трансакцията може да се използва операция TRTYPE=90 „Проверка на статус на трансакция". По този начин се получава информация за операции, извършени в рамките на предходните 24 часа.

- **Завършване на първоначална авторизация**

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

  Сумата на завършващата операция следва да е по-малка или равна на първоначалната авторизация.

  За всяка първоначална авторизация може да се направи само една завършваща операция, без значение дали е успешна или не.

При неуспешно завършване на авторизация следва да се направи нова Първоначална авторизация.

- **Отмяна на „Първоначална авторизация“**

  На е-търговеца се предоставя възможност за отмяна на „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 4 „Поддържани типове трансакции“.

  Отмяна на „Първоначална авторизация“ може да се направи само за сума, равна на тази на първоначалната авторизация.

  За всяка осъществена операция може да се направи само една отмяна (успешна или неуспешна). При неуспешна отмяна на първоначална авторизация търговецът следва да се обърне към акцептиращата институция.

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

- **Отмяна на „Плащане“**

  На е-търговеца се предоставя възможност за отмяна на „Плащане“ (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 4 „Поддържани типове трансакции“.

  Отмяна на плащане може да се направи за сума, равна или по-малка от тази на плащането.

  За всяка осъществена операция може да се направи само една отмяна (успешна или неуспешна).

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

  При неуспешна отмяна, сумата може да се възстанови на картодържателя през обслужващата финансова институция.

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

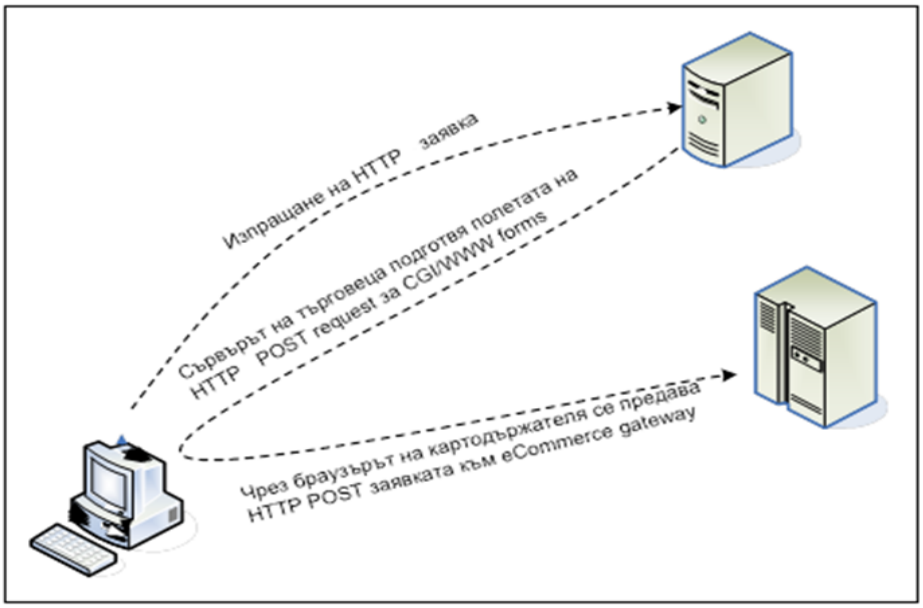
  При получаване на отговор от авторизационната система с отказ на трансакция „Плащане“ или „Първоначална авторизация“ с код RC 65 за Mastecard или 1A за VISA, терминалът следва да направи повторна заявка за същата трансакция.

  Това се осъществява автоматично от терминала, като за търговеца са видими двете трансакции – първата – неуспешна и, втората – с резултат според отговора на хоста на издателя.

  Когато повторната операция е неуспешна, трансакцията завършва с код на отговор 1A.

2.2 Обмен на съобщения

Обменът на съобщения между сайта на е-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 е-търговеца към сървъра на БОРИКА.



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

В интерфейса към APGW предаването на данни от е-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 е-търговеца (например чрез натискане на бутона „Плащане”), сървърът на е-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 е-търговеца параметри и инициира началото на диалог за автентикация и авторизация на плащане с картодържателя.

Адресите, на които се препращат заявките, са:

Среда на разработчика за провеждане на тестове:
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 е-търговеца не се въвеждат данни за картата.

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

3.1 Полета в заявката от е-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 Предоставя се от Акцептиращата институция
TRTYPE	Тип на трансакцията	1-2	M	Възможни стойности 1, 12, 21, 22, 24, 90
AMOUNT	Сума	4-12	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 в заявката. 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 е-търговеца	10	C	Merchant ID Предоставя се от Акцептиращата институция
MERCH_NAME	Име на е-търговеца	1-80	C	Име на е-търговеца*
MERCH_URL	URL на е-търговеца	1-250	O	URL на web сайта на е-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	2	C	Двубуквен код на държавата, където се намира магазинът на е-търговеца, по стандарт ISO 3166-1.
MERCH_GMT	Часова зона на е-търговеца	3	C	Отстояние на часовата зона на е-търговеца от UTC/GMT (напр. +03).
LANG	Език	2	O	Език на трансакцията 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	6-22	C	ORDER + до 16 символа за номер на поръчката при е-търговеца** **ВНИМАНИЕ, полето не трябва да съдържа символ “;”.**
TIMESTAMP	Дата/час	14	C	Време на трансакцията по **UTC**: YYYYMMDDHHMMSS. Разлика между стойността на TIMESTAMP и текущото време в e-Gateway сървъра не трябва да надвишава GUARDTIME. 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 е-търговеца за картодържателя. Възможно е използване на кирилица.

** Използва се за информация, с която е-търговецът и картодържателят да разпознават плащането. Предава се през **финансовите файлове**. Въведената информация следва да се състои от цифри, латински букви и символи, без “;”.

ВАЖНО! При използване на кирилица трябва да се ползва само **encoding UTF-8**.

M/O/C:
M – Mandatory / Задължително поле
C – Conditional / 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 4 са указани участващите полета за всеки тип трансакция.

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="+02" 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="
22EBD7271192B4A706DC10A5BB7EDB11B95A6ABB58F88DC4E478CDBCD36BDE23844E2799FE6798DB3E0EB99AF7B913607C1903A
0F9D46DC6210155124823FC8598CECB238D1829F5E53FD9DFDA88E5676E470568C12F06DFD43677861799045C455C1E8C446ABE1B
D383289FBFD13612D2D8F677ABB3F45CB1A9A9D45B2102F468CA0C8513FCF02F0418EB72DB375A2280BBEB01797692382EA399849
DFD0E805DFDF9C80A07A2BA1D2027C943FDBC6FBAD36AFC19A63EC188A0DD486CBE57CAAFC3BE453E82FC7E1126B209DFFC9B
6CA73DD222DBB11FCEF790DF0F2379341900E284DD92D1D72B377EE756594B707D9BD1859CEF70CC6845455AF1FA681651"
readonly="readonly" /><br>
<INPUT type="submit" name="Submit" value="Approve"></br>
</form>
```

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

Важно: При използване на бисквитки на сайта, търговецът е длъжен да осигури съответствие на тяхното съдържание и прилагане с RFC 6265.

3.2 Полета в отговора от APGW към е-търговеца

На сайта на е-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 7 – дублирна трансакция при неуспешна автентикация 21 – Soft Decline
RC	Код на завършване	2	O	Отговор при обработка на трансакция от APGW или издателя на картата по 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	4-12	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	14	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 (авторизационен код)	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
AUTH_STEP_RES	Статус на автентикация	1-32	C	Статус на автентикация, използван в схемата 3-D Secure
CARDHOLDERINFO	Информация за картодъжателя	1-128	C	Информация за картодъжателя от ACS на издателя. **ВНИМАНИЕ, е-търговецът е длъжен да визуализира стойността на това поле пред картодъжателя.**
ECI		2	C	e-commerce индикатор (ECI)
CARD	Маскиран номер карта	16-19	C	Маскиран номер карта (напр. „5100XXXXXXX0022“)
CARD_BRAND	Бранд на картата	1-4	C	Бранд на картата
NONCE		32	M	Ехо от заявката
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. За отхвърлени от APGW заявки се използват отрицателни стойности (напр. -17 при грешен подпис). Възможно е в последващ момент да се получи същата заявка, но с правилен подпис, при което APGW ще обработи заявката. Когато операцията е отхвърлена от хоста на издателя – кодът е положителен, различен от 0.

Ако трансакцията е автентицирана и одобрена от издателя, кодът за завършване е „00".

ВНИМАНИЕ: Успешна трансакция е само тази, която завършва с RC „**00**" и Action "**0**".

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.

За съпоставянето на отговора със заявката може да се използват полета TERMINAL, ORDER и NONCE.

3.3 Особености на полета на APGW интерфейс

1) Поле AMOUNT (Сума) **-** съдържа сумата на поръчката **заедно с десетичната точка,** например „10.20“ или „0.29“.
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 е-търговеца във финансовите файлове. Полето трябва да съдържа значението на поле ORDER, конкатенирано със символен низ с дължина до 16 символа. Същият символен низ може да се използва като буквено-цифров номер на поръчка с размер до 16 символа.

   ВАЖНО! Полето не трябва да съдържа символ “;”.

4. Поддържани типове трансакции

APGW обработва заявки за трансакции в рамките на времеви интервал GUARDTIME. Стойността на GUARDTIME по подразбиране е 15 мин. (900 сек.).

ВАЖНО: Валидно за всички типове трансакции - поле RFU не участва в заявката или отговора към/от APGW, но се включва в символния низ за подписване с дължина един байт 0x2D (знак минус "-").

4.1 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, M_INFO, NONCE, P_SIGN

Поле	M/O	Условие
TERMINAL	M	
TRTYPE	M	
AMOUNT	M	
CURRENCY	M	
ORDER	M	
DESC	M	
MERCHANT	M	
MERCH_NAME	M	
MERCH_URL	O	
EMAIL	O	
COUNTRY	O	
MERCH_GMT	O	
LANG	O	
ADDENDUM	M	
AD.CUST_BOR_ORDER_ID	M	
TIMESTAMP	M	
M_INFO	C	За изискване на пълна автентикация от страна на издателя (SCA) се подава стойност “eyAidGhyZWVEU1JlcXVlc3RvckNoYWxsZW5nZUluZCI6IjA0IiB9”
NONCE	M	
P_SIGN	M	

Таблица 3 Полета в заявка за трансакция „Плащане“

Полета, участващи в подписа на заявката: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU

Полета участващи в подписа на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU

4.2 Проверка за статус на трансакция

TRTYPE=90

Заявката може да е HTTP GET или POST. Обичайно заявката се генерира от сървъра на е-търговеца и се изпраща директно към APGW, в случай че не е получен отговор за трансакция.

APGW съхранява данни за трансакции за последните 24 часа. В случай, че APGW намери резултат за трансакция, отговорът съдържа данни за намерената трансакция в json формат. Ако трансакцията не бъде намерена, валутата в отговора, по подразбиране, 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 трансакция не е успешна (timeout).

ВАЖНО! Поле ORDER съдържа номер поръчка на оригиналната трансакция, а поле TRAN_TRTYPE показва 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. Отговорът съдържа информация за съответния тип трансакция, указана в параметър TRAN_TRTYPE.

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

ACTION	RC	Описание
0	00	Трансакцията е успешно обработена. В отговора се връща оригиналната информация за трансакцията
2	Код на завършване от издателя	Трансакцията е отказана от издателя. В отговора се връща оригиналната информация за трансакцията
3	-19	Неуспешна автентикация. Поле statusMsg съдържа повече информация за неуспешната автентикация:
3	-31	Трансакцията се обработва от издателя
3	-33	Извършва се автентикация на клиента
3	-39	Искане за потвърждаване на клиента
3	-40	Искане за потвърждаване на трансакцията

Таблица 4 Статус на трансакция

Значенията на полета ACTION и RC са описани в точка 3.2

ВАЖНО! Отрицателните стойности на поле RC може да се променят в хода на завършване на трансакцията.

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

Поле	M/O	Условие
TERMINAL	M	
TRTYPE	M	
ORDER	M	
TRAN_TRTYPE	M	
NONCE	M	
P_SIGN	M	

Таблица 5 Полета в заявка за трансакция „Проверка за статус на трансакция“

Полета участващи в подписа на заявката: TERMINAL, TRTYPE, ORDER, NONCE

Полета участващи в подписа на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU

4.3 Отмяна на плащане

TRTYPE=24

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

Трансакцията от тип “Отмяна на плащане” (Reversal) представлява отмяна на предходно “Плащане“. Сумата на отмяната може да е по-малка или равна на тази от първоначалната трансакция. За всяка осъществена операция може да се направи само една отмяна (успешна или неуспешна) в рамките на 30 дни от първоначалната операция.

При неуспешна отмяна търговецът може да е обърне към обслужващата финансова институция.

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

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

Поле	M/O	Условие
TERMINAL	M	
TRTYPE	M	
AMOUNT	M	
CURRENCY	M	
ORDER	**M**	
DESC	M	
MERCHANT	M	
MERCH_NAME	M	
MERCH_URL	O	
EMAIL	O	
COUNTRY	O	
MERCH_GMT	O	
LANG	O	
ADDENDUM	M	
AD.CUST_BOR_ORDER_ID	M	
RRN	**M**	
INT_REF	**M**	

TIMESTAMP	M	
NONCE	M	
P_SIGN	M	

Таблица 6 Полета в заявка за трансакция „Отмяна на плащане“

ВАЖНО! Полета ORDER, RRN и INT_REF съдържат стойностите от оригиналната трансакция „Плащане“.

Полета участващи в подписа на заявката: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU

Полета участващи в подписа на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU

4.4 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, M_INFO, NONCE, P_SIGN

Поле	M/O	Условие
TERMINAL	M	
TRTYPE	M	
AMOUNT	M	
CURRENCY	M	
ORDER	M	
DESC	M	
MERCHANT	M	
MERCH_NAME	M	
MERCH_URL	O	
EMAIL	O	
COUNTRY	O	
MERCH_GMT	O	
LANG	O	
ADDENDUM	M	
AD.CUST_BOR_ORDER_ID	M	
TIMESTAMP	M	
M_INFO	C	За изискване на пълна автентикация от страна на издателя (SCA) се подава стойност “eyAidGhyZWVEU1JlcXVlc3RvckNoYWxsZW5nZUluZCI6IjA0IiB9”
NONCE	M	
P_SIGN	M	

Таблица 7 Полета в заявка за трансакция „Първоначална авторизация“

Полета участващи в подписа на заявката: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU

Полета участващи в подписа на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU

4.5 Завършване на първоначална авторизация

TRTYPE=21

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

Трансакцията „Завършване на първоначална авторизация“ се използва за приключване на трансакция от тип „Първоначална авторизация“. Сумата на трансакцията може да е по-малка или равна на сумата на първоначалната авторизация. За всяка осъществена първоначална авторизация може да се направи само едно завършване (успешно или неуспешно) в рамките на 30 дни.
Акцептиращата институция на е-търговеца може да има допълнителни изисквания за изпълнение на този тип трансакция.
При неуспешно завършване търговецът следва да направи нова 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

Поле	M/O	Условие
TERMINAL	M	
TRTYPE	M	
AMOUNT	M	
CURRENCY	M	
ORDER	**M**	
DESC	M	
MERCHANT	M	
MERCH_NAME	M	
MERCH_URL	O	
EMAIL	O	
COUNTRY	O	
MERCH_GMT	O	
LANG	O	
ADDENDUM	M	
AD.CUST_BOR_ORDER_ID	M	
RRN	**M**	
INT_REF	**M**	
TIMESTAMP	M	
NONCE	M	
P_SIGN	M	

Таблица 8 Полета в заявка за трансакция „Завършване на първоначална авторизация“

ВАЖНО! Полета ORDER, RRN и INT_REF съдържат стойностите от оригиналната трансакция „Първоначална авторизация“.

Полета участващи в подписа на заявката: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU

Полета участващи в подписа на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU

4.6 Отмяна на първоначална авторизация

TRTYPE=22

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

Трансакцията от тип „Отмяна на първоначална авторизация“ (Reversal) представлява отмяна на предходна авторизация.

Необходимо е сумата на отмяна на първоначална авторизация да равна на тази от първоначалната трансакция. За всяка осъществена операция може да се направи само една отмяна (успешна или неуспешна) в рамките на 30 дни от първоначалната операция.

При неуспешна отмяна търговецът следва да се обърне към обслужващата финансова институция.

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

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

Поле	M/O	Условие
TERMINAL	M	
TRTYPE	M	
AMOUNT	M	
CURRENCY	M	
ORDER	**M**	
DESC	M	
MERCHANT	M	
MERCH_NAME	M	
MERCH_URL	O	
EMAIL	O	
COUNTRY	O	
MERCH_GMT	O	
LANG	O	
ADDENDUM	M	
AD.CUST_BOR_ORDER_ID	M	
RRN	**M**	
INT_REF	**M**	
TIMESTAMP	M	
NONCE	M	
P_SIGN	M	

Таблица 9 Полета в заявка за трансакция „Отмяна на първоначална авторизация“

ВАЖНО! Полета ORDER, RRN и INT_REF съдържат стойностите от оригиналната трансакция „Първоначална авторизация“.

Полета участващи в подписа на заявката: TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU

Полета участващи в подписа на отговора: ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU

4.7 Повторна трансакция при Soft Decline

TRTYPE=1,12

При получаване на отговор от авторизационната система за отказ на трансакцията с код RC 65 за Mastecard или 1A за VISA, APGW генерира автоматично повторна заявка към ACS на издателя за пълна автентикация и повторна заявка за авторизация към издателя.

Когато повторната операция е неуспешна, трансакцията завършва с код на отговор 1A.

5. 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.

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

5.1. Цифров подпис за подписване на съобщение

Цифровият подпис осигурява постигането на три основни цели в информационната сигурност – цялост на съобщението, автентикация на страните и невъзможност от отричане при 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 сформира 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 4 за всеки тип са указани полетата, върху които се прави цифров подпис в заявката и отговора от APGW.

За цифровия подпис в заявките към APGW всеки е-търговец използва собствени двойки RSA ключове, различни за тестова и продукционна среда. Алгоритъмът, който се използва за генериране на двойка ключове е RSA PKCS#1.

Съхранението и подмяната на частния ключ на търговеца е негова отговорност.. Частните ключове на търговеца трябва да се съхраняват от търговеца по сигурен начин, така че да не стават достояние на трети лица. Не трябва да се изпращат при никакви обстоятелства по електронна поща или друг канал, т.к. това е предпоставка за компрометиране и следва да бъдат деактивирани и да се издадат нови.

Препоръчително е генерирането на нов частен ключ при всяка подмяна на изтекъл сертификат или публичен ключ.

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

Алгоритъмът за подписване се прилага върху символния низ. Подписването става с частния ключ на е-търговеца, съответно за тестова и продукционна среда.

Проверката на подписа в отговорите от APGW се извършва от всеки е-търговец посредством публичния ключ на APGW, съответно за тестова и продукционна среда.

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

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

APGW поддържа схема на подпис MAC_GENERAL. По-старите схеми за подпис от предходни версии на интерфейса (MAC_EXTENDED и MAC_ADVANCED) ще бъдат поддържани до 31 юли 2023 г.

Прилагането на MAC_GENERAL осигурява допълнителна сигурност при извършване на трансакции, при които се извършва запазване на карта, както и последващото използване на токенизираните карти.

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

По подразбиране се ползва схема MAC_GENERAL.

Полета за сформиране на символен низ за подпис по схема MAC_GENERAL:

N	TRTYPE	P_SIGN_FIELDS_REQUEST	P_SIGN_FIELDS_RESPONSE
1	1	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU
2	12	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU
3	21	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU
4	22	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU
5	24	TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU
6	90	TERMINAL, TRTYPE, ORDER, NONCE	ACTION, RC, APPROVAL, TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, RRN, INT_REF, PARES_STATUS, ECI, TIMESTAMP, NONCE, RFU

Таблица 10 Полета, участващи в сформиране на подписа, според вида на съобщението, по схема MAC_GENERAL

ВАЖНО: В настоящата версия на интерфейса значението на поле RFU (Reserved for Future Use) в символния низ за подписване е един байт 0x2D (знак минус "-"). Поле RFU е запазено за бъдещо ползване в символния низ за подпис и не участва в заявката или отговора към/от APGW.

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

Примерни разработки на интерфейса както и допълнителна информация 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 текущото време на APGW, в UTC, по-голяма от 15 минути. За България отместването е “+03” лятно време и “+02” зимно време.

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

5.2 Генериране на частен ключ за подписване на съобщенията с OpenSSL

Тестови терминал:

openssl genrsa -out privatekeyname_T.key [-aes256] 2048

Продукционен терминал:

openssl genrsa -out privatekeyname_P.key [-aes256] 2048

Забележки:

- privatekeyname_T – име на генерирания частен ключ за тестови терминал;
- privatekeyname_P – име на генерирания частен ключ за реален терминал;
- опционален параметър -aes256 – използва се при желание да се защити с парола генерирания частен ключ;
- 2048 е размерът на ключа в битове.

Чрез командата е задължително да се създадат два различни 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 е-търговеца и трябва да бъдат съхранявани от него по сигурен начин.

ВАЖНО! Препоръчително е частният ключ за реалния терминал да е защитен с парола.

5.3 Генериране на заявка за сертификат с OpenSSL

Имената на вече генерираните частни ключове от предходната стъпка се използват в командите за генериране на заявките за сертификати в частта [privatekeyname_T.key и privatekeyname_P.key].

Тестови терминал:

openssl req -new -key privatekeyname_T.key -out VNNNNNNN_YYYYMMDD_T.csr

Реален терминал:

openssl req -new -key privatekeyname_P.key -out VNNNNNNN_YYYYMMDD_P.csr

Е-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_Z, където:
VNNNNNNN – TID на терминала, предоставен от Финансовата Институция
YYYYMMDD – дата на заявка във формат ГодинаМесецДен
Z – тип на искания сертификат, значения – T – за среда за тестове, P – за продукционна среда

Всеки от генерираните .csr файлове се поместват в .zip архив с име VNNNNNNN_YYYYMMDD_Z.zip или VNNNNNNN_YYYYMMDD_Z_YYYYMMDDHHMMSS.zip, където:
VNNNNNNN – TID на терминала, предоставен от Финансовата Институция
YYYYMMDD – дата на заявка във формат ГодинаМесецДен
Z – тип на искания сертификат, значения – T – за среда за тестове, P – за продукционна среда
YYYMMDDHHMMSS - опционално поле указващо дата и час на влизане в сила на сертификата (Valid from). Ако не бъде указано следва да се уточни допълнително между банката и търговеца. Валидни стойности за часа HH са 00 - 23. Валидни стойности за минутите MM са 00 – 59. Валидни стойности за секундите SS са 00 – 59. Времето е в часова зона EET (Eastern European Time).

5.4 Задължителни полета на сертификата

(изписани на латиница, без специални символи):

- Common name (CN) – име на домейна (например: merchantdomain.bg)
- Organization Unit Name (OU) – TID на терминала
- Organization Name (O) – име на фирма,
- Locality Name (L) – населено място
- State or Province Name (ST) – област/район
- Country Name (C) = BG
- Email Address

5.5 Преобразуване на частен ключ и сертификат в PKCS12 формат с OpenSSL

openssl pkcs12 -export -inkey privatekeyname_Z.key -in VNNNNNNN_YYYYMMDD_Z.cer -out keystore_name.p12

openssl pkcs12 -export -inkey privatekeyname_Z.key -in VNNNNNNN_YYYYMMDD_Z.cer -out keystore_name.pfx

privatekeyname_Z.key е името на съответния частен ключ (генериран в т.5.2), със следните значения: T – за среда за тестове, P – за продукционна среда;
VNNNNNNN_YYYYMMDD_Z е името на съответния сертификат (получен от Борика в резултат на изпратени заявки от т.5.3), със следните значения: T – за среда за тестове, P – за продукционна среда

5.6 Проверка на частен ключ / сертификат с OpenSSL

Търговецът може да провери дали използвания частен ключ за подпис на заявката и публичния ключ (полученият от Борика сертификат) в терминала са валидна двойка RSA ключове чрез пресмятане на md5 (контролна) сума. Ако пресметнатите суми съвпадат, то частният и публичният ключ са RSA двойка ключове.

openssl rsa –noout –modulus –in privatekeyname_Z.key | openssl md5

openssl x509 –noout –modulus –in VNNNNNNN_YYYYMMDD_Z.cer | openssl md5

Където:
- **privatekeyname_Z.key** е името на частния ключ на терминала,
- **VNNNNNNN_YYYYMMDD_Z.cer** е името на подписания сертификат на терминала,
- **Z** – тип на искания сертификат, значения – T – за среда за тестове, P – за продукционна среда

5.7 Сформиране на подписа в заявка към APGW

При изпращане на заявка към APGW, е-търговецът задължително подписва съобщението с частния си ключ, съответно за среда за тестове или продукционна среда.

В следващата таблица са изброени полетата от заявката, които участват в подписа, за трансакция тип „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
TIMESTAMP	Дата/час	14	20201012124757
NONCE		32	9EADBD70C0A5AFBAD3DF405902602F79
RFU (Reserved for Future use)		0	-

Таблица 11 Пример за сформиране на символен низ за подписване при плащане

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

Символният низ за подпис е:

8V1800001149.003BGN6154744142020101212475732 9EADBD70C0A5AFBAD3DF405902602F79-

В зелен цвят са отбелязани дължините.

Общата дължина на полето за подпис в случая е 78 символа.

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

385631383030303031313134392E303033424 74E36313534373434313432303230313031323132343735373332394541444244373043304135414642414433444634303539303236303246373 92D

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

5.8 Проверка на подписа в отговор от APGW

При получаване на отговор от APGW, е-търговецът е длъжен да провери валидността на подписа, като използва публичния ключ на APGW, съответно за среда за тестове или продукционна среда. Ако в отговора липсва поле, участващо в проверката на подписа, то се замества с един байт 0x2D (знак минус "-").

В следващата таблица са изброени полетата от отговора на APGW, които участват в подписа, за трансакция тип „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
RFU (Reserved for Future use)		0	-

Таблица 12 Пример за сформиране на символен низ за проверка на отговор при плащане

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

112006S975398V18000011149.003BGN6154744120286012531521697E2F39EFCA1CAF1--1420201012160009329EADBD70C0A5AFBAD3DF405902602F79-
В зелен цвят са отбелязани дължините.

Общата дължина на полето за подпис в случая е 124 символа.

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

3131323030365339373533393856313830303030313131343932E3030334247 4E3631353437343434313230323836303132353331353231363937453246333945464341314341463 12D2D313432303230313031323136303030393332394541444244373043304135414642414433444634303539303236303246373 92D

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

6. Примери за трансакции

6.1 Пример за „Плащане“

Информация от е-търговеца към APGW:

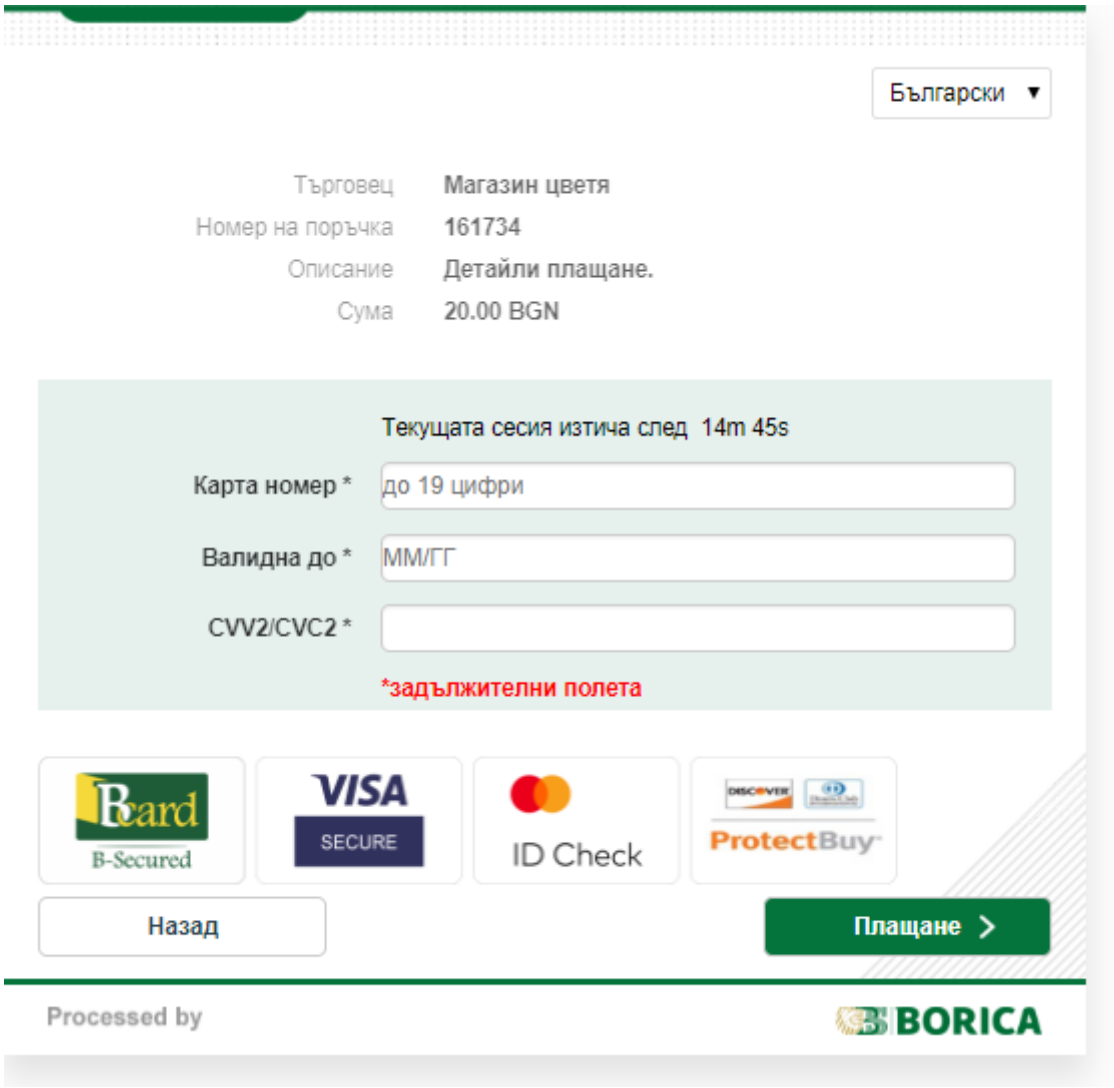
TERMINAL	V1800001
TRTYPE	1
AMOUNT	1.00
CURRENCY	BGN
ORDER	145659
DESC	Детайли плащане.
MERCHANT	1600000001
MERCH_NAME	Мол България
MERCH_URL	http://www.borica.bg
EMAIL	merchant@borica.bg
COUNTRY	BG
MERCH_GMT	+02
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	145659ORD@<n>
TIMESTAMP	20201013115715
NONCE	FC8AC36A9FDADCB6127D273CD15DAEC3
P_SIGN	95B299B9706ED8D9FDA2F3EC3ADCBF0346A1299C512CFB498321DB8AFAE853F6A96BE472B54A75231F894D19F488E2BD3803D893E0924B678BD9777DDF922BCB0BD8F38E887E2FDEF675C428E7C023C420679D93E72A90A51B9B21E2209C5751813754F3ACC30F35BA3E61298D43BFBB2902B59B3B226F71BFA2DB8A17488B42FB60466983B421442DD4C9799C612579DECC32192153B62EF2AF02C24BD3433BE02AE7AB5976C7B769666DE5984293AE1CA814C9FB2E0D2B45FA098F0B08591832AEC8A334C6783A274F4C2D25E1B0296139439D41B313E1CDB4C730DBC2E32812135FE7E7F0CB97E535D1742EBA848B5F6D20259D364B46D9449955CE46B335

MAC (P_SIGN) - Calculation info

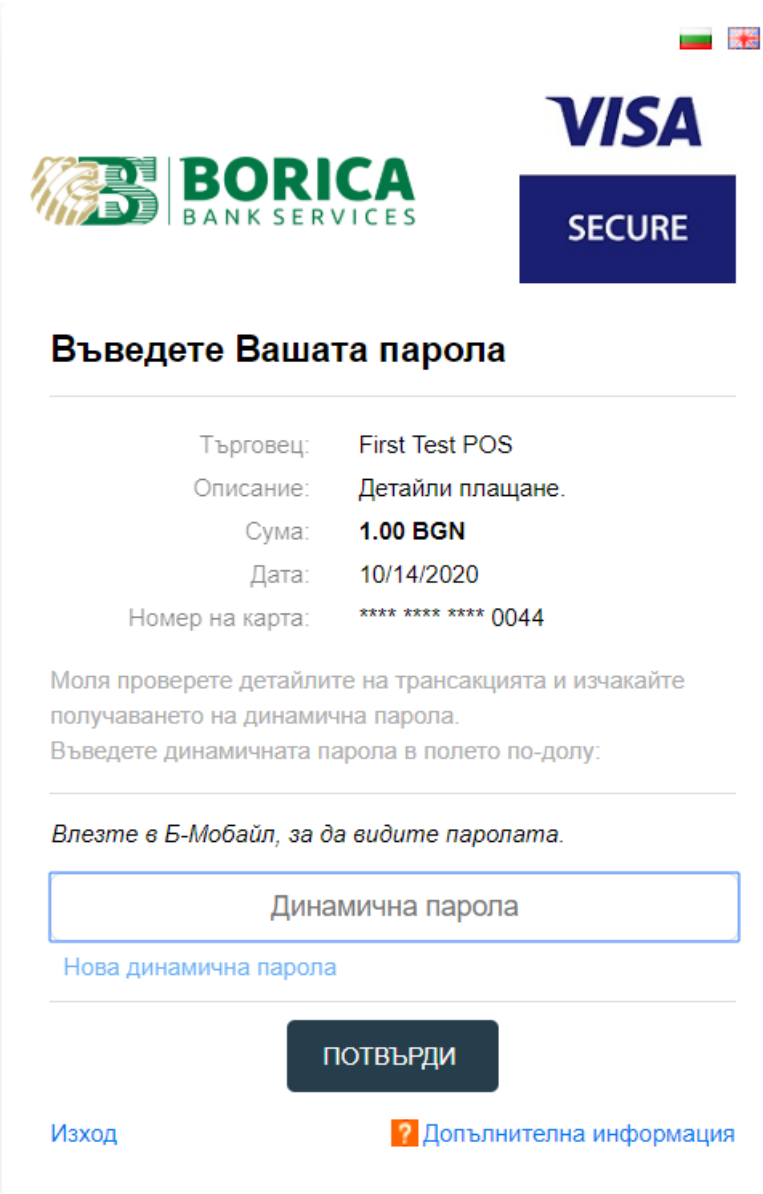
macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU]
macSourceValue	8V18000011141.003BGN6145659142020101311571532FC8AC36A9FDADCB6127D273CD15DAEC3-

Таблица 13 Пример за заявка „Плащане“

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



Ако въведената карта е регистрирана в ACS за 3-D Secure, 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 е-търговеца.

Полето RC=00 показва успешна трансакция.

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

Отговор от APGW:

Parameter	Length	Value
ACTION	1	0
RC	2	00
STATUSMSG	8	Approved. No errors
TERMINAL	8	V1800001
TRTYPE	1	1
AMOUNT	4	1.00
CURRENCY	3	BGN
ORDER	6	170403
TIMESTAMP	14	20201013140707
TRAN_DATE	14	20201013170707
APPROVAL	6	S19527
RRN	12	028701253242
INT_REF	16	B7A68A9F37E8586E
LANG	0	
PARES_STATUS	0	
AUTH_STEP_RES	7	VERES_N
CARDHOLDERINFO	0	
ECI	2	
CARD	16	5100XXXXXXXX0022
CARD_BRAND	3	MCC
NONCE	32	22EA51788AFE61A9D814B771A8FA6379
P_SIGN	512	31C6507191249D361086E1CA70A2A0374ACF9191D765055E10ACB93D720E934FEBE44E59D41D19C7B976CF358FA572B12EB08556EA602141E983F6FC93F106B0249780C192FAD7BC6411C33E966317804681D692CCDAF42F7494B1B7A7ED8AB23CB8DE5F0621E0C3582671BD222A3E5409538D9BD93F11B150B75D0C59AAC5E77D439FE14A6B494C8FECB1C23867A77D291E34425B5F1A6E9CBA9B92E3BC344E2C9AFAD45E2AE2D1313200A80DE26C2DD870E63AFEADA9EDAEF4DF5B32AD533D68665CB8F7F6E42D8ED7FFE31415FFAED25B3BA159063A9FC542FA958719016697CE9760954A58A2AF077BA049D1DD2216242D80572AA0EA98A39CD7C8DDB5BE

Таблица 14 Пример за отговор „Плащане“

==== Response signature from ====

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

macSourceValue = [102006S195278V18000011141.003BGN6170403120287012532421 6B7A68A9F37E8586E--142020101314070732 22EA51788AFE61A9D814B771A8FA6379-]

Signature = [true]

6.2 Пример за „Проверка статус на трансакция“

Полетата, с данни от оригиналната трансакция, са удебелени.

Информация от е-търговеца към APGW (за операция тип Плащане) **:**

TERMINAL	V1800001
TRTYPE	90
ORDER	**114233**
TRAN_TRTYPE	**1**
NONCE	622CAAA8BF20C5A21A917DCB8401C336
P_SIGN	5FD6E5A6A0121A599594DB1F0FC96F2CEB4CCC7B3B829E9DBA74 E1DC4AF115B774A5460AAA268DB65E04B71C6E9EB6A3F7A820C27 D4EA1BC648A19BC97D2577F510F4CDF4BFD6EDA4B8D2B8556479 1ED6287A08282027099F07166FA8416F123FEEBBC920A33A0ED596 4CA02C49A7ED7D5E61F4B5D53CC14DF542BDF4221DCDA22C5864 F9F722BF989CB7A2BF2ABE0B76F823561A33F2152772312429204A AB94B58C7AFC82F64D5C20069D4A5B1DF406041CAB77BCCE88C6 F84704B2B33AFC82216C2F41B92129D68933CE1C59F87CEAE6B1E 8CFBE6DD4CE5898F8FE6453CC7DB7519801FB05BBDE7973E18A8 6AFF020121B74A65EAD2741BC1D6E39DD42564

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, ORDER, NONCE]
macSourceValue	8V18000012906114233326 22CAAA8BF20C5A21A917DCB8401C336

Таблица 15 Пример за заявка „Проверка статус на трансакция“

Резултатът от „Проверка за статус на трансакция“ е в json формат. Ако липсва поле, използвано за проверка на P_SIGN, то се замества в с един байт 0x2D знак минус "-". Например
“102006S449738V180000129041.003BGN612035312028701253195166AF46A8970774DBB--142020101315242932 5E7EFC5D43E684642F0FB8B7F22167B9-”.

Отговор от APGW (Трансакция „Плащане“ 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",
"AUTH_STEP_RES":"ARES_Y",
"CARDHOLDERINFO":"",
"ECI":"05",
"CARD":"4341XXXXXXXX0044",
"CARD_BRAND":"",
"NONCE":"7A9A2E5CD173AF3F69A87F06E1F602ED",
"P_SIGN":"A20DE81C5723E3A92D8D1B73C7C2B8848A42D3380E9DF9951127E5878AF989E6951F595A52C16CC9B9F690BDC0
165DE8E4CF2FA5892A17C5F8026011D604AF5723DF4C35486AA0094C1C23AE9617F8BE2C11F448EA40CDB332EBAB73DE2D
33A01AC1BEE83108B788D22D8653F86DFAE8BAEB17048869156D2876FD7F8E232BDB1311D5D4EB63C630EC4941EDBFC708
02508F86147714CD7E671014EC8D56882070B6B203FFECE07A67FED6D20C9F4E4637E8EA5B0FE274AD4D8965CB7025BD205
F259E41EAF2E48E5566099842B02FB89E7534081CFD4289F6F5F7727DAAB7EBB472FDFD9D091F57616120190732BF635D49E
F9519B4CEE26D8DFBB34C2D033B"
}

==== Response signature ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,
NONCE, RFU]
macSourceValue =
[102006S789528V180000129041.003BGN611423312029001254078164C9B34468610CF9F1Y205142020101608451532 7A9A2E5C
D173AF3F69A87F06E1F602ED-]
Signature = [true]

Информация от е-търговеца към APGW (за операция тип Отмяна на плащане)

TERMINAL	V1800001
TRTYPE	90
ORDER	**114233**
TRAN_TRTYPE	**24**
NONCE	B1A1B57F8D66EF6B604690BF7141B53C
P_SIGN	AEC96B3551F4B951E91A5BE6DFD91AD6AF859D4358B7A5D7CD5E8E5B7 B4C32E995A6B5FFDBC4265F535D16ED8D591E06DA57E7A05357C93153A 13807E2FBA6BB7C9A94AE6B2F2253F9DB8A7D0273AB68B8B9A427814B2 646C6585E51396A531BABB3A8EF034496EA0ECEB29379A3E97195FB65DF 85B571537620C27FF33483FDD09E8E106EE02FC59B15E70C4D692BD8A3 A269DAF24DCBF300B3AB9DA623F789855828AE876CB6304D43027F212E FDB3CD1271A809920725BB3A8A247C84824B468EBF55DDD0540B5E7B6E 844BBE28FBA49B62A91BB623A05158DC0D8CD4E6B1FF6BEE0D0EA1012 EB04E44E930A3D728F0178BC4458734A3E1D462EB5BEA259E

MAC (P_SIGN) - Calculation info

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

Таблица 16 Пример за заявка „Проверка статус на трансакция“

Отговор от APGW (Трансакцията „Отмяна на плащане“ не е успешна):

{
"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":"",
"AUTH_STEP_RES":"",
"CARDHOLDERINFO":"",
"ECI":"",
"CARD":"",
"CARD_BRAND":"",
"NONCE":"B1A1B57F8D66EF6B604690BF7141B53C",

"P_SIGN":"774F0E62105F5AEED1AED347D81AC12E122423F3E5F0DFBA2DEA3E93D9FC30EFBA9067E6F8A26DA4F44A9CB1B1824A942DA759B051C14CD5D303AA2A11285382C2CFD6B1188ED0DA2E4D1B5E33143DF8A27F0D785749597F7269A40A44113FE5EEF7ACD6D4B0A924053538462BF9F7C58FBD0CB3AC47E61EA039F6A0693B992E1AD0CA278D6B9BC2BA0F3BB1FFDCBCA68D631D7B00B8877004E8C758E335EF3C46E468D9A06C2F94FBF0753FF95A33404FBD8F9BFCB4D60AAA593C5C37AF9BEC3FFCA234B419528A635FCBAA8ED498D1A68834FF71C62286EF5DCC6992EAED703B6AAC262225A655874E8B7277138E68DD8886C44930E7814661B5F9006C0013"
}

==== Response signature ====

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

Отговор от APGW (Трансакцията „Отмяна на плащане“ е успешна):

{
"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":"",
"AUTH_STEP_RES":"",
"CARDHOLDERINFO":"",
"ECI":"",
"CARD":"",
"CARD_BRAND":"",
"NONCE":"E8CAC1D2FBE11A899204AED74C02BDEC",
"P_SIGN":"9C22C8E340976C8360B7CB53C5EC90B99BA9A67EE86FE703715766ED3BF8490366C43B579DD1454C0C38B4D31CCD94515EA63AF97FFEB9884234B907B92E4FDF5CF7E806C114C2211BD800E0A659EC35CFD45F0027F05FA66C6F5468982743581416DA42EDC33EDC83537CB57598D527DE193C7BAA360E383CA7172AC0720A50BE2A3530008E8C867427B69CEC9A281907ECE7584BAA49D287BA33F80B49E7857E57509E69CF1F54D83555BF2258F45D36CC4764F9F5803F3D6710FF2F1A82AE4CD345BBB40102563FCA605479759D9E6C1CACBF3A9B1D48BFEC17388261782745CECEE27E3B75A106E0560A2D2403A5EE9DB38932E995D920F38875ABA2D3AF",
}

==== Response signature ====

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

6.3 Пример за „Отмяна на плащане“

Полетата с данни от оригиналната трансакция, са удебелени.

Информация от е-търговеца към APGW:

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	+02
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	125353ORD@<n>
TIMESTAMP	20201014095541
RRN	**028701253242**
INT_REF	**B7A68A9F37E8586E**
NONCE	7D51498A3C22B86DD57EFB699A175714
P_SIGN	277DC35B76CD5CAA9BB025A7A5B39EEBF1B3005EA5214F6EB781995FE65418378C5AFA60925977E9A3376D937292C7D57928E3F6B635C78C67411683FB38ABDB876A8EB122196D8534B355A9940934BAD88D2B7FBC25B43CD294059FA6BBB7FDFDC5DBDA0D9306D30F4E387EA879FBC59ED50E64569E3D36A068D6BC6CA57F1FC22F8B0373AF7B1612880648C68E428AF74374AE96A8043C99C99ED21C72B7FFB64EDFCD67BDFCC71B1220FF8CD7A2DFA106EDDD8F5D9B92E4AA8B46FA65F1C3849CE31635FEE43B950240FDE0EB3D638644B9066AE83051F96A34D64C8BF94E92A868C33684DD6A56BD2D26D104EDF8462E2585491BA8B65B8C2B9176C80FC8

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU]
macSourceValue	8V180000122441.003BGN6145659142020101409554132 7D51498A3C22B86DD57EFB699A175714-

Таблица 17 Пример за заявка „Отмяна на плащане“

Отговор от APGW:

{
"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": "",
"AUTH_STEP_RES":"",
"CARDHOLDERINFO":"",
"ECI": "",
"CARD":"",
"CARD_BRAND":"",
"NONCE": "7D51498A3C22B86DD57EFB699A175714",
"P_SIGN":
"4B2C8E02632CA1A753CF9904DF782A2015C8C70546D154842451F5C97ED348D242FBC367CFB91FAAFA53ED2537BF7747CF
C2680E3689AD08AC0D0D97C5FE29B2ED2CF8AA8A12E709021FC9C2A179C993A4D673A80F4C27A76D4141DC85D394BBCCA
1977196042D81AEA907B77B507F95FA4210B13E65D68965294110E483B42D3E1E27FFC06F566A2741BA48FD97092B20896CF8
C66523E92AA1AD2D43CDEDFB21DA875E06581D94B51375FCBC772B93EA91C191DF9BE4C531D5D5FD9E9FE5F8E840B464B
DA150D1AC00D28F58750E0C45F4C62BB8D13A5311E59F8201CCDA601AD47526ED542535E428ED77DBD194E4E87876A270A
7E743873F191639D2DDD7"
}

==== Response signature ====

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

macSourceValue = [102006S195278V180000122441.003BGN6145659120287012532421 6B7A68A9F37E8586E--
142020101410004032 7D51498A3C22B86DD57EFB699A175714-]

Signature = [true]

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

6.4 Пример за „Първоначална авторизация“

Информация от е-търговеца към APGW:

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	+02
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	170000ORD@<n>
TIMESTAMP	20201012140015
NONCE	C3ACF912658C0A2310EA5AAAF739E627
P_SIGN	A76449365B63104B514683D2C02F47C6EBA202394C60732821A4A7E A43E7B73204C60023B8739B7B91E27F1E0E5CE18B8C1C116408A41D 90AC70A392CEF58990DD505AF87E71370D345C295C92F9E03F9F379 984BFDE292131B0BAADF19F86398DE18673989F65A2D035B67A05F3 114B0D0E8FCA527F513FE27AEBE63F66A8C4C1A5C36F16F4CA0B8B 82C0F0E75FFEE2DD6C7139E430F08AD847145AF282B8970CDBC7D3 CB8AC22CF7D730C6486C9E10E3925FB4CF9353750907FEE94894019 4FB702D075DA222F1C7C52C4CDCD86D8893B937B3CAA68372CAD0 706A1F20F2E8AD7A4A0C3E8E54815CF6E45AE155A21AECCE773827 43E9241E36B76145B7AABC

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU]
macSourceValue	8V180000121243.003BGN6170000142020101214001532C3ACF912658 C0A2310EA5AAAF739E627-

Таблица 18 Пример за заявка „Първоначална авторизация“

Отговор от APGW:

Parameter	Length	Value
ACTION	1	2
RC	2	05
STATUSMSG	8	Transaction declined
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
LANG	0	
PARES_STATUS	1	Y
AUTH_STEP_RES	7	PARES_Y
CARDHOLDERINFO	0	
ECI	2	05
CARD	16	4341XXXXXXXX0044
CARD_BRAND	4	VISA
NONCE	32	C3ACF912658C0A2310EA5AAAF739E627
P_SIGN	512	95F5FFF8779932EC04CFE19CC1F75AF01CA5050E8AED8222 DA9B5E16ADDBABB6FC51B0FB5501C82FAE2919345F92961E 8631CD5A8807DD907E4A32B34B47B4F783EF99C3A4F37B7A B6726DE79FEF0E6E55A5F467ABA82DB3E3C0A8AC09A1E1D 7F0D67A83418DC1DF5D362C94774467FA5656F7827C469C30 7743E93C73DB434940B002E02B0EE2FBC8A8ADB33CC69F3D F6C6D0E69F5042D5C171C840CA296928BEBD79DB9F3D3D24 28730C1BEA2261C80DB1A0511687A5D77F242CBE42B204B57 B6BDC7F31DDF6027D55E9CE584B101DF5520DD26A399C6D 05759C1651B320C176CA206AA775DAA1D7288C60DEB12508 DE2DF49A2F308BB28059EEA8FEC3BE0C

Таблица 19 Пример за отговор „Първоначална авторизация“

==== Response signature from ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,
PARES_STATUS,ECI,TIMESTAMP,NONCE, RFU]
macSourceValue = [12205-
3BGN43.008V18000012126170000120286012531751420201012140349 1604F45801DAF13E22
1Y20532C3ACF912658C0A2310EA5AAAF739E627-]
Signature = [true]

6.5 Пример за „Завършване на първоначална авторизация“

Полетата, с данни от оригиналната трансакция, са удебелени.

Информация от е-търговеца към APGW:

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	+02
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	170075ORD@<n>
TIMESTAMP	20201012141516
RRN	**028601253167**
INT_REF	**92339532D5866339**
NONCE	CCF64A57E0B9E35D2E01DF4A3805DC58
P_SIGN	724DEA99E6AD3D1E1692FBE24A44F805581F176F14A8853BA9F7A8389DFFF7C10CF01C0E11FFF755503C1716552BE47B9DB383CCDFBD2B087A0D4C23DE70C4D9A2B7FF8FFA16BFE26ACF335472B2208EE6BD82DEC94DE854D141F9B30B697801629F676F0433D656E93A6450FA2435C57C1FA572BF6C84F079D3D1DC842D6E8CF7F55F9A3DDB03E07218CF986D16B08DEFCA8687142B625A714D1223B7613CA48C615DF70E56D6CC26B2EF50E07223FE246E9A21D1ED88CD746B760DEA17EF0ED10F18E7BA5F31F886917E08909AD347828F6D8C7FB957DE211E888C3A43F013391A82FC66025633E68C4BD59AF1BEF2C18651BD25FD14DC769DDB2DD3A854E7

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU]
macSourceValue	8V180000122141.003BGN6162021142020101214151632CCF64A57E0B9E35D2E01DF4A3805DC58-

Таблица 20 Пример за заявка „Завършване на първоначална авторизация“

Отговор от APGW:

{
"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": "",
"AUTH_STEP_RES":"",
"CARDHOLDERINFO":"",
"ECI": "",
"CARD":"",
"CARD_BRAND":"",
"NONCE": "CCF64A57E0B9E35D2E01DF4A3805DC58",
"P_SIGN":
"B2F33F1BE13EDAD498E67A01720AFABD93454C1506038F374EA7B771039C15B6A7C24B2FB9EBA7FEFDE49052118561A09D
3D9CFEC98D3A17A8058725EF2E9909C8EF5DDD499B8CBCF5606770588B110B18A1014636F8B6A7CE9F17A3023B6499602A8
BE53D3E83FC0FAD97D61B0DCD0DC2C3FBE6600B4B91A8576C34F058FEF80254F4E089567C154EDA67DD6CB997425251C6
E4EA4A8531EC1724CA7AC8C9BE11438EBF86CE2B486326EAC03AF8005C443F1B32690B8031774903F847499C1F6080F626E
DD5568A41341F70546F90DF67F8980BD3F391D33928554B62A4744A2B331C3350AAE64D0DE3801FE40B73DD89A772D5093D
502035AE90D081A85CE8"
}

==== Response signature ====
macFields =
[ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMESTAMP,
NONCE, RFU]
macSourceValue = [133-20-8V180000122141.003BGN6162021120286012531671692339532D5866339--
142020101317425332CCF64A57E0B9E35D2E01DF4A3805DC58-]
Signature = [true]

6.6 Пример за „Отмяна на първоначална авторизация“

Полетата, с данни от оригиналната трансакция, са удебелени.

Информация от е-търговеца към APGW:

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	+02
ADDENDUM	AD,TD
AD.CUST_BOR_ORDER_ID	095949ORDnnn
TIMESTAMP	20201014070415
RRN	**028601253175**
INT_REF	**04F45801DAF13E22**
NONCE	D1AA7234EF80331750C61FCCDCE7C5C7
P_SIGN	4C25AC3904F371D1767AD8D75A66A0A997C8EA70C5B0524611484ECB766583F55EBB1C65306348B6FCA16E75A99815DFC32A87FB5383264C780D30E3507C26E4ECF07B50636141E6AB205338BBE340301233F116C6A4947BA565C8C1C754FC81AFEFF68ADF4B30BD7FA3CA2D0114762AE796C6F6C55EB9862AC159079D3ADFDFD262201BE74C416633A19272146A0B13D78CA6E55D6AEAA62F22AACAA617C85192AE417E445D01DFE1F06C713B35D58DF09B5ABA08CBAFA8F3D106E3699D1356A82FEFA400981A055196F906F27AD400BB34C3CA5C648A0F1A8DC47D642295736A39418B37C8FBB4596939376D170D89016D4DC97D8FD6607B2B6E68158C4438

MAC (P_SIGN) - Calculation info

macFields	[TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU]
macSourceValue	8V180000122241.003BGN6170000142020101407041532D1AA7234EF80331750C61FCCDCE7C5C7-

Таблица 21 Пример за заявка „Отмяна на първоначална авторизация“

Отговор от APGW:

{
"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": "",
"AUTH_STEP_RES":"",
"CARDHOLDERINFO":"",
"ECI": "",
"CARD":"",
"CARD_BRAND":"",
"NONCE": "D1AA7234EF80331750C61FCCDCE7C5C7",
"P_SIGN":
"885457783119E64E93D346C38D1050D5A848B97FB8319874CAE1BAB898D6E53B818E2FC83C96C754983B9B0C727FC25BB30
A67455DAA8CF67A5DE9086DE0A96F10FAEE8F7A8D27A9B9FEC69F956DC95E250D970FE380D65F8A99B1115B9B289E2C633
D6CB993246B383A6CC133233F9A14C9EEA554832AD58368893212CCFECDD8268498BF0B307BD414805DA7D23D1B297250B
3AE3CF9164256387E4BF4C386424886BC18B33B43808CECC436F2EE2C4A4114B8609D2D60E836DDA6B82D0BB5CFED1FC85
81418EE4FFAA34828B94B384CF2F22B043894666E13B3BA429FEFD9FAC1D67614927AB11B86141F69DBD2365E868F1B3BA2
50199C1CE4D016EF59F0"
}

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

7 Тестови карти

При извършване на тестове се ползват следните тестови карти:

7.1 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.	Successfully Completed	Да, паролата е 111111 за сума над 30.00 лв.

Таблица 22 Тестови карти, за които резултат се получава според PAN

7.2 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 24	Не
Mastecard	5100789999999895		Да, паролата е 111111

Таблица 23 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	

Таблица 24 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.

8 Кодове за грешка, използвани от APGW

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 некоректни име или стойност
-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 авторизационният 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 е-търговеца” в заявката
-13	The referrer IP address (usually the merchant's IP) is not the one expected	Неправилен IP адрес на е-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 (15 min by default) between the transaction timestamp request field and the e-Gateway time was exceeded	Разрешената разлика между TIMESTAMP в заявката от е-търговеца и текущото време в e-Gateway сървъра е надвишена
-21	The transaction has already been executed	Трансакцията вече е била изпълнена
-22	Transaction contains invalid authentication information	Трансакцията 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 трансакцията е по-стара от 24 часа.
-25	Transaction confirmation state was canceled by user	Допълнителното потвърждение на трансакцията е отказано от картодържателя
-26	Invalid action BIN	Невалиден BIN на картата
-27	Invalid merchant name	Невалидно име на е-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 автентикация на картодържателя
-40	Client side transaction form in progress	Трансакцията е в процес на обработка

Таблица 25 Допълнителни кодове за грешка, ползвани APGW

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 26 Кодове за грешка при обработка от издателя на картата

9 Приложение 1:

9.1 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+Vb9oUK3yb9W7YMhk1vJy4p2oyo77Sirki4bhh8RPlVWAqeVUgEL/
f5ZuZSNzB2cFkUOknbRwM/j98fft4lgZN/nYkYjW22UaPA7ULEBMxmQUKrJKi04S
PVIG1iKzLh3jVyRsxi+giFrlQ+/jVWA0wJm8B25jsRcwObjL6+MczutVKmaNjaVy
FNkBtLOWSCf4A6i4xOfafWoEx4tEa4Dl5PTqQl4PBvH6SW3lKulfNpa5m1wvnlA3
hFy9lfUPAgMBAAECggEBAJz/stl9yxQ9bEGpjovzlzsgcdngHzhpkG6EocLsryix
S4dXAjxlRp9V4KmJoHnDymLQByFIqJ98XK3YkpNB5apJ0+euLkfm+8NAaZik404J
LNyTzGFFneCIP4vStQo1HFM8ODG53DM1GOcnmCT5QiW8mHjk0AH02vR/haCU5kdR
qQeMBnGAuqOcO3T7QcuK2AMO7BoGrkq0+V58DyCdf1UpeLoi71HCdBpj8FPHcU0H
ScsPUrWXSkJSVj7R68AUtl4Sss3CEk7DbbSLcW1DfmX6esujM/fx1SLc9Bue4Ipa
0ec7wKvvMbLap0gWOOxZGRtxS9ALJ3T75AOjDx38q6ECgYEA86cPMYUePy/l9CEu
F2fsr0LnpB3clwEhhMeIIjKMCTVnPlHMy8Sm9WrRdErKMpsIbOWgeIqUaPPCt3NZ
FTgJnlJnFR4KI5qPOb3ZRA9OI6eliVvdgxe7e/bHe74b/v/uE6378ddtniHCIvgk
6Oi9/luImv3kYzX1pmJr/8VZQdECgYEAwznqU1QiPaUFtZwkb3hIoTcIYlKwIbmP
3HYdsS2p20WHh3XJC9nojABIBgJJYKdACzQyIy1FJJ3ga0fgkSZ5KL1LXmclXXL6
lzdQNIyF/boRP+XC7fB9MNwIClqJCnmciKWE4xCt9GgEiLnJDYnOhGiQ50BuxJFn
RU6RxjAPoN8CgYEA3LmYr/mx/vf7T3/Ha3jAF716b1iF/14M6WaA0soLxkPUtcYQ
yv/paCZOfRVLuzBrH4ueJdUUwUciPGKIbwqG2nvfumeuM7bOzTZJXrimxvIWqirl
rvuO4qwa5uTAI+/h034n4VyRd1GJt3gop75Ab+6oABDFF4NIeGRtBhXX2CECgYB9
/QRCHouyaKsUlt3UqjWFBPT+LwrH2O8EgZ2L2EJD5c0fGF5UrZ4rq4rPhe5A1+62
zEqG9RIoHVLVKR+9zKxoJDFdjQdKFYeuyt2R7BYUtl2ndOmlkIvaWkU+GUtTXUQt
01O9DeiVUAONEQi1GfgS70CEXMqfRI725UuiMSYE1QJ/EkPO8VPbWf+BgKovYFf1
AsStOfMMvrgVn8e/vZmWIuaGb40L34Dxuvv3YRk1EsQFirGZ5XDDCm5r8H1IY8Ne
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_GENERAL = TERMINAL, TRTYPE, AMOUNT, CURRENCY, ORDER, TIMESTAMP, NONCE, RFU
$data = '8V18000011141.003BGN611392014202010130839232D41AAAFC7F8119A3BB7C4868E0B256F9-';

$pkeyid = openssl_get_privatekey($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));
?>
```

9.2 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+CW89bLGNiHh6mmZt71ulXugNtGf2RhP59fmEKBKj+DSF1Ql65SVvv2eYb6JBlhHX+hZss/oAN
xvqYFSG4k6L1tkoDwctB+q7p1EbWEuqDNxYT0RidkLkCAwEAAaOCAecwggHjMB0GA1UdDgQWBBTT
nQwEEjMqWryNqt8onGmGk6nm4DAfBgNVHSMEGDAWgBT1J8z325solCubZvApcg6KPWLcmDAgBgNV
HRIEGTAXhhVodHRwOi8vd3d3LmItdHJ1c3QuYmcwCQYDVR0TBAIwADBNBgNVHSAERjBEMEIGDCsG
AQQB+3YBBwEEAjAyMDAGCCsGAQUFBwIBFiRodHRwOi8vd3d3LmItdHJ1c3Qub3JnL2RvY3VtZW50
cy9jcHMwDgYDVR0PAQH/BAQDAgOoMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjBUBgNV
HR8ETTBLMEmgR6BFhkNodHRwOi8vY3JsdGVzdC5iLXRydXN0Lm9yZy9yZXBvc2l0b3J5L0ltVHJ1
c3RUZXN0T3BlcmF0aW9uYWxBQ0EuY3JsMIGHBggrBgEFBQcBAQR7MHkwJwYIKwYBBQUHMAGGG2h0
dHA6Ly9vY3NwdGVzdC5iLXRydXN0Lm9yZzBOBggrBgEFBQcwAoZCaHR0cDovL2NhdGVzdC5iLXRy
dXN0Lm9yZy9yZXBvc2l0b3J5L0ltVHJ1c3RUZXN0T3BlcmF0aW9uYWxBQ0EuY2VyMBYGA1UdEQQP
MA2CC01QSSBPVyBBUEdXMA0GCSqGSIb3DQEBCwUAA4ICAQAUJfDjTROuVORLojCzVQdppoiPs3hX
Ra/9MaNIUP5xlI0AamWmN7bTDQpnNfw5tlo8DPSBIMfP+5xJyfMTHAi43i+7vf1t1ZucEbVJ73FF
zdzZQaxw9NY0n0IBBz8WEnkaGewh45aQ6XMgNe5xcKbtP2vqq+qZiy0eyIHJwaQORKyZ9+jBlnVo
ZdzUbDrrSEMka98IQ52XO8EPbCmB/GhJlZ991yNo5/PVsFxT9sjG3VGm+sStD3G7+pjX+HsHLn65
gwWq2oRiQqe62W/HSNb5dnIWqIJldT4Zd0Ar97hQwU1ZQVnmL5ZjswsjafI7B/0N4U5QzbOvWX1W
oDXCCqmXAoTP1DDEWJ0vmvVDHGrrC0rIbluBdzQEK/D1f3A1jlCzQPyKOwUuafLlpCX17b09Zwxi
45prDk/LBqE6CI6CM+8nF0QyN3Th+r2IqUuhGpfLApGlp6sJvJdAhnqX1VCGJCdozIhzrEJ4oha3
/+HijQI+vUaYevk1d/EipZNHU1gkcocrj2qmTMOKzEw9zDs5jVSgtBZTUF5ORwUNiTXj7EZUnQUC
wANFI8k0EcWPhkU5L7v9/9rcGkMcm0S3bM5rbKksabvq01cvxkepS5qqvbxgugci/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+l4sx4p6JFKV41y
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_GENERAL =
ACTION,RC,APPROVAL,TERMINAL,TRTYPE,AMOUNT,CURRENCY,ORDER,RRN,INT_REF,PARES_STATUS,ECI,TIMEST
AMP,NONCE
$data = '112006S975398V18000011149.003BGN615474412028601253152169 7E2F39EFCA1CAF1--
14202010121600093 29EADBD70C0A5AFBAD3DF405902602F79';

//P_SIGN in hex from mpi_sign.php
$p_sign =
hex2bin('6FF21243639A23946393023839C0B549C6794C516E4C077F65DD476B700C0A53A9A23F1517B9F8F955C4E8E51
9CFF1C9428B32F0259E8EA2284B244B39AA8E4E4A251D840479CB3DDB988F25674D1BEB97A814DB04E846FC9795058
E2BDC3A511CA503F15C71BD3F1687FF15FE9F8CA393555286CEB4A3B722683E1FFD7C30A6ED19C6EDB7D40A6356B1
2BD4C010DD43D596753CC6BA52523EC5DB4E0BC48B8A99DDE2D1B946D504EA3A692C3E56DA3941E83F226EEEC109
DAB36C3FEE70C89E2E54000E62AC53DB43B72E75597DA735CF513BFFD8D4A61F5468C8A77C9704E9B9BD8AB5167BA
1DAD0898CAF7BED831C7786F8E75100FB179657B05CC4EDA87E');


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

```php
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();
}
?>
```

10 Приложение 2:

10.1 Стойности на AUTH_STEP_RES:

Поле AUTH_STEP_RES съдържа стойност получена от Directory Server (Visa, MasterCard), показваща нивото на автентикация на картодържателя.

N	AUTH_STEP_RES	CARD 3DS VERSION	AUTHENTICATION RESULT	DESCRIPTION
1	VERES_N	1	Cardholder Not Participating	Cardholder Not Participating – Cardholder is not enrolled.
2	VERES_U	1	Unable to Authenticate or Card Not Eligible for Attempts	Unable to Authenticate or Card Not Eligible for Attempts (such as a Commercial or anonymous Prepaid card).
3	PARES_Y	1	Authentication Successful	The issuer has authenticated the cardholder by verifying the password or other identity information.
4	PARES_A	1	Attempts Processing Performed	Authentication was not available, but functionality was available (through the issueror a third party) to generate a proof the merchant attempted VbV authentication.
5	PARES_N	1	Authentication Failed	The cardholder's password (or other authentication information) failed validation, thus, the issuer is not able to authenticate the cardholder. The following are reasons to fail an authentication: Cardholder fails to correctly enter the authentication information within the issuer-defined number of entries (possible indication of fraudulent user). Cardholder "cancels" authentication page (possible indication of a fraudulent user).
6	PARES_U	1	Authentication Could Not Be Performed	The issuer ACS is not able to complete the authentication request – possible reasons include: Card type is excluded from attempts (such as a Commercial Card or an anonymous Prepaid Card) ACS not able to handle authentication request message ACS is not able to establish an SSL session with cardholder browser System failure that prevents proper processing of the authentication request
7	ARES_Y	2	Authentication Successful (Frictionless)	Successful frictionless transaction without SCA authentication.
8	ARES_N	2	Authentication Declined (Frictionless)	Cardholder is not enrolled / Frictionless authentication declined.

9	ARES_R	2	Authentication Rejected (Frictionless)	The issuer rejects authentication (e.g. Cardholder is blocked/closed).
10	RREQ_Y	2	Authentication Successful (SCA)	The issuer has authenticated the cardholder using SCA (e.g. verification of password or other identity information).
11	RREQ_N	2	Authentication Failed (SCA)	The cardholder's password (or other authentication information) failed validation, thus, the issuer is not able to authenticate the cardholder. The following are reasons to fail an authentication: Cardholder fails to correctly enter the authentication information within the issuer-defined number of entries (possible indication of fraudulent user). Cardholder "cancels" authentication page (possible indication of a fraudulent user).
12	RREQ_U	2	Authentication Could Not Be Performed (SCA)	The issuer ACS is not able to complete the authentication request – possible reasons include: ACS not able to handle authentication request message ACS is not able to establish an SSL session with cardholder browser System failure that prevents proper processing of the authentication request

Таблица 27 Ниво на автентикация на картодържателя

10.2 Стойности на ECI (Electronic Commerce Indicator)

Поле ECI (Electronic Commerce Indicator) съдържа стойност получена от Directory Server (Visa, MasterCard), показваща резултата от автентикацията на картодържателя.

VISA	
ECI Value	**Definition**
05	Both cardholder and card issuing bank are 3D enabled. 3D card authentication is successful
06	Either cardholder or card issuing bank is not 3D enrolled. 3D card authentication is unsuccessful, in sample situations as: 1. 3D cardholder not enrolled 2. Card issuing bank is not 3D Secure ready

07	Authentication is unsuccessful or not attempted. The credit card is either a non-3D card or card issuing bank does not handle it as a 3D transaction

Таблица 28 Резултат от автентикация на картодържателя (Visa)

MasterCard	
ECI Value	**Definition**
00	Authentication is unsuccessful or not attempted. The credit card is either a non-3D card or card issuing bank does not handle it as a 3D transaction
01	Either cardholder or card issuing bank is not 3D enrolled. 3D card authentication is unsuccessful, in sample situations as: 1. 3D Cardholder not enrolled 2. Card issuing bank is not 3D Secure ready
02	Both cardholder and card issuing bank are 3D enabled. 3D card authentication is successful

Таблица 29 Резултат от автентикация на картодържателя (Mastercard)

10.3 Често задавани въпроси:

10.3.1 Какво е значението на кодовете за грешка? Кои кодове са финални и кои – не?

Кодовете за грешки, използвани от APGW, са описани в Раздел 9, като е необходимо да се имат предвид следните особености:

- **RC=00** – успешна трансакция, като е необходимо да са покрити едновременно два критерия - RC=00 и Action=0, при което резултатът е **окончателен**. Възможните стойности за Action са описани в Таблица 2.
- **Отрицателни кодове** – те са базирани на обработката на автентикационното съобщение и е възможно да бъдат променени в рамките на определен период от време - GUARDTIME, който съгласно текущите настройки е 15 минути. Типичен пример за такава промяна е ситуацията, в която картодържателят натиска бутон “Back” на своя браузър, в резултат на което се сформира съобщение за грешка; ако впоследствие картодържателят продължи с потвърждението на трансакцията, тя може да е успешна. При отрицателни кодове е препоръчително да се ползва „Проверка за статус на трансакция“ (TRTYPE=90). **Резултатът, получен след повече от 16 минути (след изтичане на GUARDTIME, който е 15 минути плюс 1 минута буфер) при „Проверка за статус на трансакция“ е окончателен.**
- **Положителни кодове, различни от 00** – те са **окончателни** и са базирани на обработката на авторизационното съобщение, респективно на отговора от страна на хоста на издателя на картата.
- Не следва да се правят допълнителни проверки за трансакция, за която е получен окончателен отговор. Дори и по някаква причина да се получи такъв, той не следва да се взима предвид.

10.3.2 Кои са най-често срещаните грешки в отговорите на заявките от APGW:

- -17 – грешка при сформиране на POST заявката. Възможни причини:
  - Неправилно сформиране на подписа от страна на е-търговеца поради некоректно съставен символен низ за подписване. Търговеца следва да провери коректността на символния низ за подписване.
  - Неправилно сформиране на подписа от страна на търговеца поради ползване на неправилен частен ключ. Търговеца следва да провери съответствието на частния и публичния ключове според точка 6.5.
  - Некоректно конфигурирана схема за подпис на терминала. Обслужващата ФИ следва да конфигурира схемата за подпис на терминала.
  - TIMESTAMP на заявката е по-стар от 15 мин. (UTC), в този случай поле STATUSMSG съдържа текст "Expired transaction".
  - В момента APGW обработва трансакция със същия номер поръчка (ORDER) за този терминал .
- -19 – грешка при автентикацията на картодържателя:
  - Картата не е регистрирана за 3D Сигурни плащания.
  - Изтекла/не сменена статична парола.
  - Грешно въведена статична или динамична парола.
  - Картодържателят сам е отказал плащането при показване на страницата за автентикация.

- 58 – терминалът не е активиран. Обслужващата ФИ следва да премине през стъпки Initialize & Enable.

10.3.3 Получавам съобщение “Missing BACKREF parameter, using default. “. Каква може да е причината?

APGW връща данните за отговор към URL, дефиниран за терминала в APGW база данни. Проверете в банката дали този URL е правилно зададен за терминала.

10.3.4 Не получавам никакъв отговор. Каква може да е причината?

В случай, че картодържателят затвори браузъра на екрана за въвеждане на данни за картата, трансакцията остава в състояние „Transaction form in progress’“ за следващите 24 часа и отговор няма да бъде изпратен. Също така проверете в банката дали BACKREF URL адресът е правилно зададен за терминала.

10.3.5 Как се отразяват трансакциите в приложението Merchant Portal?

Трансакциите се отразяват по следния начин:

- Authentications – всички операции, за които POST заявката е обработена от APGW.
- Pending – трансакциите, при които статусът все още не е финализиран, но са стигнали до авторизация.
- Rejected – операции, отказани от авторизационния хост (положителен код за грешка).
- Transactions – всички успешни трансакции.

10.3.6 Как може да се идентифицира поръчката, за която е направено плащане в приложението Merchant Portal?

- В меню Authentications за всяка трансакция се показва стойността на поле ORDER, като стойността в колона Order ID може да се ползва за връзка между изпратената заявка за плащане и данните в системата на търговеца.
- В tab Tagged Data за всяка трансакция могат да се видят стойностите на AD.CUST_BOR_ORDER ID и DESC.
- Важно! Стойността на поле AD.CUST_BOR_ORDER_ID (която съдържа и ORDER) се предава и във финансовите файлове, съответно в информацията, която се визуализира в банковото извлечение, и може да се ползва и за счетоводно засичане на направените плащания.