
ПРОЕКТ: Надграждане на информационна система „Е-плащане“ по проект BG05SFOP001-1.004 „Надграждане на хоризонталните и централни системи на електронното управление във връзка с прилагане на Единния модел за заявяване, заплащане и предоставяне на електронни административни услуги“ финансиран със средствата на оперативна програма „Добро управление“.

ДЕТАЙЛНА ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ ЗА ИНТЕГРАЦИЯ НА ЕЛЕКТРОННИ РАЗПЛАЩАНИЯ СЪС ЦЕНТРАЛЕН ВПОС ТЕРМИНАЛ

Изготвена от „Булпрос Консултинг АД“

История на промените:

Версия	Дата	Автор	Описание	Стр.
1.0	27.11.2020	Емилиан Евгениев	Първа версия на документа	11

Преглед и одобрение на документа:

Версия	Дата	Отговорник	Описание	Стр.
1.0	17.12.2020	Симеон Александров	Първа версия на документа	11



Европейски съюз



ОПАК. Експерти в действие



Европейски социален фонд
Инвестиции в хората

Подписи:

1	Изготвил документа - Програмист	Емилиан Евгениев подпис
4	Одобрил документа – ръководител проекти	Симеон Александров подпис



СЪДЪРЖАНИЕ:

1. Въведение	3
2. Определения.....	3
3. Акроними	4
4. Интерфейс на е-търговеца с Акцептиращ и платежен сървър на БОРИКА	5
4.1. Полета в заявката към APGW	6
4.2. Полета в отговора от APGW	7
4.3. Извличане на данни за трансакции	9
4.4. Бизнес процес по съхранение на такси и комисионни по трансакции за плащания	9
4.5. Алгоритъм за разпределение на сумите	11
4.6. Бизнес процес по разпределение на средствата	12

1. Въведение

Интеграцията между системата еПлащане със централния виртуален пос терминал (ЦВПОС), ще бъде извършена посредством предоставяне от Борика АД услуги за комуникация – APGW акцептиращ и платежен сървър на Борика, в съответствие с изискванията на EMV 3-D Secure.

2. Определения

Авторизация (Authorization) Процес, при който издател или процесор, от името на издателя, одобрява платежна трансакция.
Акцептираща Институция (Acquirer) Финансова институция, член на местна и/или международна картова организация, която има договорни отношения с търговец за приемане (акцептиране) на плащания с картови продукти на съответната схема. В схемата EMV 3DS акцептиращата институция, или упълномощеният от нея агент (процесор), определят дали съответният търговец да участва в схема за извършване на плащания през отворената мрежа Internet.
EMV® Three-Domain Secure (3DS) Протокол на съобщения, разработен от EMVCo., който позволява автентикация на картодържателите пред издателите на карти при извършване на трансакции през интернет.
Домейн на издателя (Issuer Domain) Съдържа системите и извършва функциите, свързани с издателя и обслужваните от него клиенти (картодържатели).

Е-Търговец (e-merchant) Субект (юридическо лице), който е в договорни отношения с акцептираща институция да приема плащания с платежни карти през интернет.
Отмяна на плащане (Reversal) Процес, при който издател или процесор от името на издателя, отменя платежна трансакция.
Издател (Issuer) Финансова институция, член на местни и/или международна картова организация, която издава картови продукти, има договорни отношения с картодържатели за предоставяне 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.БОРИКА
Първоначална авторизация (Deferred Authorization) Тази трансакция се изпълнява на две стъпки. При първата стъпка акцентиращият и платежен сървър регистрира заявката за първоначална авторизация. Тази заявка потвърждава наличието и блокира изискуемата, в заявката, сума по картовата сметка или картата на картодържателя. Втората стъпка, завършване на първоначална авторизация, се инициира от търговеца. Чрез нея се извършва плащането на посочената от търговеца сума, която трябва да бъде равна на посочената в първоначалната заявка. По този начин се завършва отложеното плащане.

3. Акроними

ACS - Access Control Server (Сървър за контрол на автентикацията)
APGW - Acquiring and Payment Gateway, e-Commerce CGI сървър (Акцептиращ и платежен сървър на БОРИКА)
API - Application Programming Interface (Приложен програмен интерфейс)
BIN - Банков идентификационен номер. При платежните карти това са първите шест/осем цифри, които еднозначно определят финансовата институция, издател на картата
CGI - Common Gateway Interface
DS - Directory Server (Справочен сървър [на регистрациите в схемата 3-D Secure])
HTML - Hypertext Markup Language - стандартен език за документи, предназначени да се визуализират в интернет
HTTP - Hypertext Transfer Protocol – апликационен протокол за предаване на hypermedia документи, например HTML
PAN - Primary Account Number-номер на карта
URL - Адресна схема за страниците в отворената световна мрежа за обменна информация Internet
JRE - Java Runtime Environment
SSL - Secure Socket Layer

OpenSSL - Свободна софтуерна библиотека, предоставяща набор от криптографски от функции и дефиниции. https://www.openssl.org .
UTF-8 - 8- bit Unicode Transformation Format – стандарт за символно кодиране с поменлива дължина
Keystore - Хранилище на сертификати и частни ключове

4. Интерфейс на е-търговеца с Акцептирац и платежен сървър на БОРИКА

Комуникацията и предаването на параметри ще бъде осъществено посредством HTML Forms и HTTP Post към е-Commerce CGI сървъра на БОРИКА. Комуникацията между търговеца и е-Commerce CGI сървъра включва:

- Изпращане на данни за „Плащане“ или „Първоначална авторизация“ към APGW - данните описват частта от трансакцията, свързана с еПлащае (номер на по-ръчка, сума, и т.н.). Те ще 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 брауъра на картодържателя към сайта на БОРИКА. Терминалът работи в една валута. Необходимо е валутата в заявката да съв-пада с валутата на терминала.
- Получаване на резултат от „Плащане“ или „Първоначална авторизация“ от APGW – системата получава резултат от „Плащане“ или „Първоначална авторизация“ (независимо дали е положителен или отрицателен), след като са преминати всички стъпки по автентизиране на картодържателя и авторизиране на трансакцията от авторизационната система на издателя на картата. Данните се предават чрез препращане от брауъра на картодържателя към сайта на Търговеца посредством HTTP Post.
- Получаване на информация за състояние на трансакция - възможно е (поради същността на Интернет) системата 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 брауъра си по невнимание, след като APGW е изпратил резултата, или поради прекъсване на връзката му с Интернет в този момент. Чрез изпращане на заявка за „Проверка на статус на трансакция“ може да се получи резултат от приключването на всички останали типове трансакции, поддържани от APGW.

При заплащане на едно или повече задължения, задълженото лице ще бъде пренасочвано към формата на Борика, в която да попълни необходимите данни за картата, с която ще заплати избраните задължения. След подаване на данните и извикване на съответния сървиз, Борика ще верифицира данните и ще върне резултат на плащането в зависимост от наличността на картата, верността на данните и т.н. Всяко едно плащане на едно или повече задължение, ще бъде обединявано в така наречената „трансакция“, която ще съдържа необходимата информация за направеното плащане – дата, сума, такса, комисионна и други.

Обменът на съобщения между сайта на търговеца и акцептиращия и платежен сървър на БОРИКА става посредством браузъра на картодържателя с помощта на метода HTTP POST. Браузърът на картодържателя установява SSL/TLS връзка със сайта на БОРИКА посредством сървърния сертификат на БОРИКА, предава изготвените параметри и инициира началото на диалог за автентикация и авторизация на плащане с картодържателя.

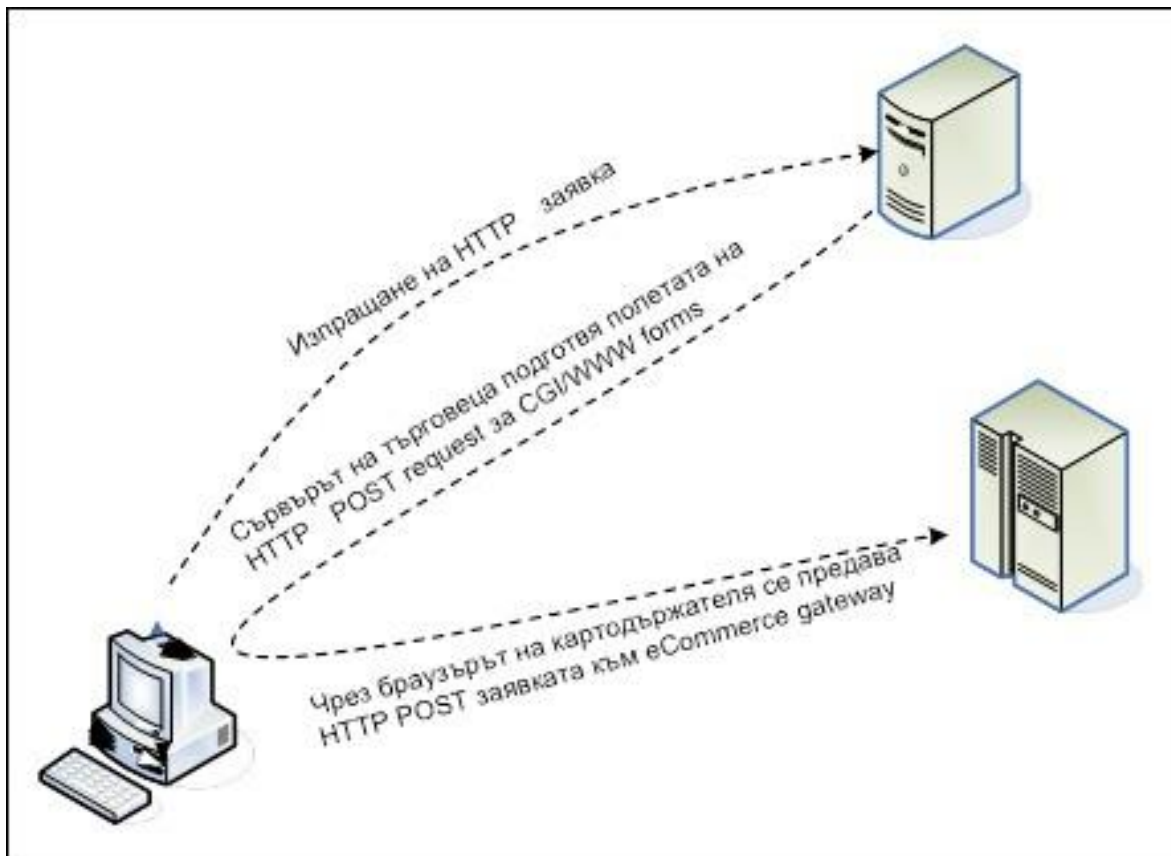


Схема на предаването на съобщение чрез HTTP POST

4.1. Полета в заявката към APGW

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

Поле	Описание	Размер	М/О/С	Съдържание
TRTYPE	Тип на транзакцията	1-2	M	Възможни стойности 1, 12, 21, 22, 24, 90
AMOUNT	Сума	1-12	C	Обща стойност на поръчката по стандарт ISO 4217 с десетичен разделител точка (напр. 12.00)
CURRENCY	Валута	3	C	Валута на поръчката: три буквен код на валута по стандарт ISO 4217
ORDER	Номер на поръчка	6	M	Номер на поръчката за търговеца. Съдържа 6 цифри, дясно изравнено и допълнено с водещи нули. ВНИМАНИЕ! Трябва да бъде уникален за терминала в рамките на деня (напр. „000123“).
DESC	Описание	1-50	C	Описание на поръчката*

MERCH_URL	URL на търговеца	1-250	O	URL на web сайта на търговеца
MERCHANT_NAME	Име на търговеца	1-80	C	Име на търговеца*
MERCHANT	Идентификатор на търговеца	10-15	C	Merchant ID
TERMINAL	Идентификатор на терминала	8	M	Terminal ID
EMAIL		80	O	Е-mail адрес за уведомления. Ако това поле е попълнено, платежният сървър може да изпраща резултата от трансакцията на посочения е-mail адрес.
COUNTRY	Държава	02	C	Двубуквен код на държавата, където се намира магазинът на търговеца, по стандарт ISO 3166-1.
MERCH_GMT	Часова зона на търговеца	3	C	Отстояние на часовата зона на търговеца от UTC/GMT (напр. +03).
TRAN_TRTYPE	Тип на оригиналната трансакция	1-2	C	Тип на оригиналната трансакция в заявка „Проверка на статус“
TIMESTAMP	Дата/час	14	C	Време на трансакцията по UTC/GMT : YYYYMMDDHHMMSS. Разлика между времето на сървъра на търговеца и е-Gateway сървъра не трябва да надвишава 1 час. В противен случай е-Gateway ще отхвърли трансакцията.
NONCE		32	M	Съдържа 16 непредсказуеми случайни байтове, представени в шестнадесетичен формат. Може да съдържа главни латински букви A..Z и цифри 0..9.
P_SIGN	Подпис	512	M	Код за автентичиране на съобщението от APGW. Съдържа 256 байта в шестнадесетичен формат.

M/O/C:

M – Mandatory / Задължително поле

C – Conditional / Полето е задължително според типа на трансакцията

O – Optional / Опционално поле

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

4.2. Полета в отговора от APGW

На сайта 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
TERMINAL	Терминал	8	M	Ехо от заявката
TRTYPE	Тип на трансакция	1-2	M	Ехо от заявката
ORDER	Поръчка	6	M	Ехо от заявката



Европейски съюз



ОПАК. Експерти в действие



Европейски социален фонд
Инвестиции в хората

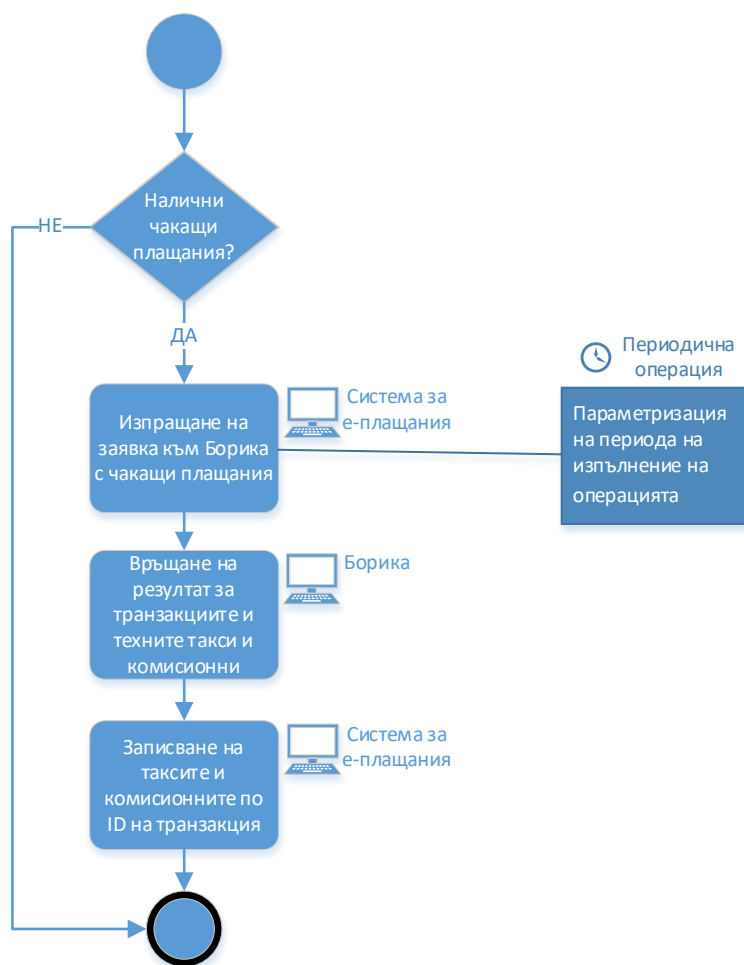
AMOUNT	Сума	12	C	Сума на поръчката
CURRENCY	Валута	3	C	Ехо от заявката
ACTION	Действие	1	M	E-Gateway код на действие: 0 – успешно приключена трансакция; 1 – дублирана трансакция; 2 – отказана трансакция; 3 – грешка при обработка на трансакцията
RC	Код на завършване	2	O	Отговор при обработка на трансакция (ISO-8583, поле 39)
APPROVAL	Одобрение	6	O	Код за одобрение (ISO-8583, поле 38). Може да бъде празно, ако не е подадено от картовата система.
RRN	Референция на трансакцията	12	O	Референция на трансакцията (ISO-8583 -1987, поле 37).
INT_REF	Вътрешна референция	1-32	M	Вътрешна референция за e-Commerce gateway
Tran_trtype	Тип на оригинална трансакция	1-2	O	Тип на оригинална трансакция в отговор на „Проверка на статус“
StatusMsg	Допълнителен код на завършване	1-255	C	Допълнителен код за грешка при автентикация в отговор на „Проверка на статус“
Card	Маскиран номер карта	16-19	C	Маскиран номер карта в в отговор на „Проверка на статус“ (напр. „5100XXXXXXXXX0022“)
TranDate	Дата/час	19	C	Дата/час на оригиналната трансакция в отговор на „Проверка на статус“
TIMESTAMP	Дата/час	14	M	Дата/час на отговора по UTC/GMT: YYYYMMDDHHMMSS
PARES_STATUS	Статус на автентикация	1	C	Статус на автентикация, използван в схемата 3-D Secure
ECI		2	C	e-commerce индикатор (ECI)
NONCE		32	M	Съдържа 16 непредсказуеми случайни байтове, представени в шестнадесетичен формат. Може да съдържа главни латински букви A..Z и цифри 0..9.

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

4.3. Извличане на данни за трансакции

Заради процеса на осчетоводяване на плащанията, таксата и комисионната не могат да върнати веднага от Борика. За да се извлекът тези данни, трябва да е минал съответния сетълмент (за международни плащания, това може да отнеме дори 2-3 дни). За необходимостта от извличане на данните за таксата и комисионната, ще бъде реализиран т.нар. Job, който ще се изпълнява през определен период от време, който ще бъде параметризиран и ще може да бъде променян. Неговата функция ще бъде да извлече всички трансакции, за които не са попълнени необходимите данни, и ще извиква съответния метод от сервиза на Борика. При получаване на съответните данни, те ще бъдат съхранени в съответните таблици в системата на еПлащане.

4.4. Бизнес процес по съхранение на такси и комисионни по трансакции за плащания



Кратко описание:

Системата трябва да съхранява таксите и комисионните за всяка транзакция идваща от централния ВПОС

Предпоставки:

Интеграцията с централния ВПОС на Борика е изпълнена успешно

Основен сценарий:

1. След успешно плащане на задължения с карта към централния ВПОС в системата за е-плащания все още липсва информация за settlement-а на транзакциите, към които са присъединени задълженията.
2. На определен период от време, който е параметризиран (например веднъж дневно) системата за е-плащания изпраща заявка към Борика при наличие на транзакции, за които няма информация за такси и комисионни. В заявката се изпраща ID на транзакцията, по което се идентифицират задълженията.

3. Борика връща информация при налични транзакции, за които е settlement-a е минал успешно. В заявката се получава ID на транзакцията и таксата и комисионната на тази транзакция.
4. В системата за е-плащания таксата и комисионната се съхраняват в нова таблица и се реферират с номер на транзакция – всяко уникално задължение се отнася към номер на транзакция, с която е заплатено.

Успешен край

Налична е информация в базата данни за таксата и комисионната, която ДАЕУ дължи за всяка транзакция, минала през централния ВПОС.

Методът за извличане данни за транзакциите е TransactionsForDate, а параметрите са следните:

Option	Име	Тип	Коментар
M	agency	String	Приходна агенция („NAP“, „BNB“, „API“)
M	event	String	Събитие
M	dateEvent	Date	Дата на събитието(yyyyMMdd) – сетълмент или авторизация (при Event=„A“ трябва да е по-стара от текущата)
O	tid	String	TID

Като резултат ще се върне списък с транзакции от тип RecEventTransaction.

Картови транзакции сетлирани на дата – { RecEventTransaction }

Mandatory	№	Field	Name	Type
M	1	transactionDate	Дата на авторизацията (yyyyMMdd)	Date
M	2	authorizationCode	Авторизационен код (6C)	String
M	3	tid	ТИД (8N)	String
M	4	sum	Сума на картовата транзакция	BigDecimal
M	5	tax	Междубанкова такса	BigDecimal
O	6	settlementDate	Дата на сетълмент(yyyyMMdd)	Date
O	7	distributionDate	Дата на разпределение(yyyyMMdd)	Date
O	8	Tax_Borica	Комисионна за Борика	BigDecimal
O	9	RRN	RRN (за физ.ПОС (12C))	String
O	10	orderId	OrderId (за виртуален ПОС, източник НАП)	String
M	11	productCategory	Тип карта	String
M	12	areaOfIssue	Произход на картата	String
M	13	cardBrand	Бранд на картата	String

4.5. Алгоритъм за разпределение на сумите

За разпределение на суми, ще се използва метод DistributionRevenueAgencies със следните параметри:

Option	Име	Тип	Коментар
M	agency	String	Приходна агенция („NAP“, „BNB“, „API“)

M	distributedDate	Date	Дата на разпределението (yyyymmdd)
M	num	Integer	Пореден номер на разпределението за деня
M	transactions	List<RecTransaction>	Списък на транзакциите за разпределение
M	totalSum	BigDecimal	Обща сума за разпределение
M	distributedAmounts	List< RecDistributedAmount >	Разпределени суми

Картови транзакции, включени в разпределението – { RecTransaction }

Mandatory	№	Field	Name	Type
M	1	transactionDate	Дата на авторизацията (yyyymmdd)	Date
M	2	authorizationCode	Авторизационен код (6C)	String
M	3	tid	ТИД (8N)	String
O	4	RRN	RRN (за физ. ПОС (12C))	String
O	5	orderId	OrderId (за виртуален ПОС, източник НАП)	String
M	6	sum	Сума на картовата транзакция	BigDecimal

Разпределение на суми – { RecDistributedAmount }

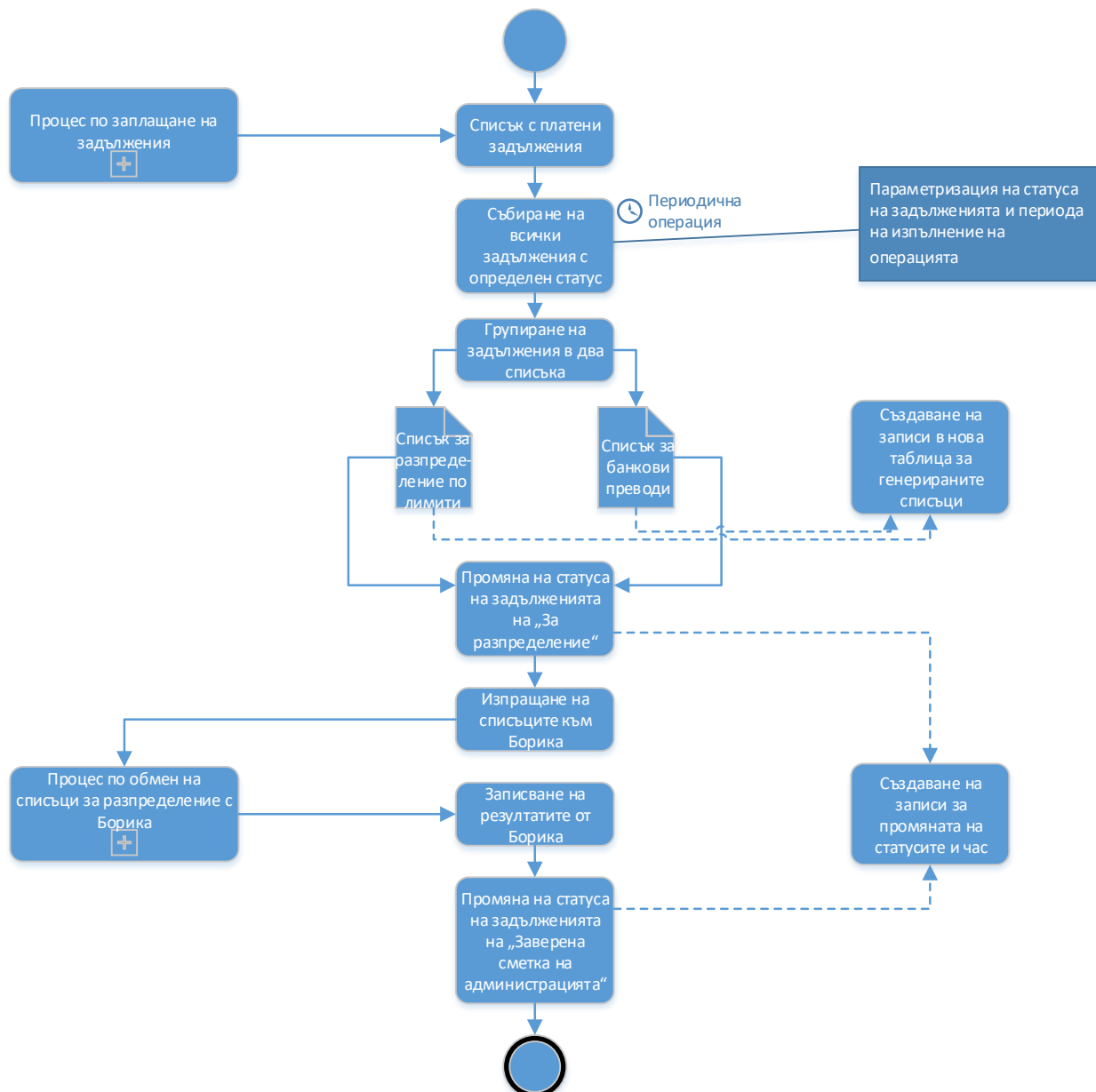
Mandatory	№	Field	Name	Type
M	1	code	Код на разпределение (2C)	String
M	2	sum	Сума на разпределението	BigDecimal

Код на разпределение (2C)

Код за разпределение	Значение
31	приходи от ДОО
32	приходи от ЗО
35	приходи от ДЗПО
37	приходи от данъци

Получените данни ще бъдат съхранявани в базата на системата, така че данните да бъдат налични за бъдещи справки.

4.6. Бизнес процес по разпределение на средствата



Кратко описание:

Системата трябва да поддържа автоматизиран процес на изчисляване и изпращане на информация за разпределение на средствата, които представляват всички плащания с дебитна или кредитна карта ще постъпват чрез централния виртуален ПОС терминал в централна сметка на ДАЕУ. Функционалността има за цел да генерира 2 списъка в дефиниран от Борика изходящ файлов формат.

Предпоставки:

Процесът по заплащане на задължения от страна на задълженото лице е минал успешно. Статусите на задълженията са се променили спрямо процеса и парите от плащанията са налични по централната сметка на ДАЕУ.

Основен сценарий:

1. Всички платени задължения по сметката на ДАЕУ се обработват автоматично на периодична база – статусът на задълженията, които трябва да се обработват е параметър, както и периодът за обработка на задълженията в списъци са параметри.
2. Плащанията се агрегират в различни нива, спрямо бюджетните разпоредители (заявители на задължения) на които принадлежат.
3. Ако е зададено агрегиране на първо ниво, първостепенния разпоредител ще получи всички приходи от второстепенните разпоредители и разпоредителите на по-ниски нива.
4. Агрегираните задължения се разпределят в два списъка, спрямо типа на разпределение, идващ от бюджетния разпоредител.
5. В списък „Списък за разпределение по лимити“ се разпределят всички задължения към определен разпоредител с тип на разпределение „по лимити“. Статусът на тези задължения автоматично се сменя на „За разпределение“.
6. В таблицата за записване на дата и час на смяна на статуса на задължение автоматично се създава запис.
7. В списък „Списък за банкови преводи“ се разпределят всички задължения към определен разпоредител с тип на разпределение „с банков превод“. Статусът на тези задължения автоматично се сменя на „За разпределение“.
8. В таблицата за записване на дата и час на смяна на статуса на задължение автоматично се създава запис.
9. Двата генерирани списъка се съхраняват в нова таблица, с дата и час на създаване, статус и участващи в списъка задължения.
10. Двата списъка се изпращат на БОРИКА чрез предварително дефиниран service. Предварително е определена и честотата на тази операция.
11. БОРИКА връща обратно потвърждение за разпределението на задълженията.
12. След връщането на потвърждение от БОРИКА статусът на задълженията автоматично се сменя на „Заверена сметка на администрацията“.
13. В таблицата за записване на дата и час на смяна на статуса на задължение автоматично се създава запис.

Успешен край:

Постъпилите задължения в централната банкова сметка на ДАЕУ се преразпределят към сметките на заявители на задължения или техни структури на по-високо ниво, по предварително зададения алгоритъм в т.4.5.