

Protokół FROB w aplikacji ITCARD

Podręcznik Integratora

|  |  |
| --- | --- |
| Autorka | Maria Siewierska |
| Wersja | 1.4 |
| Data | 2019.05.16 |
|  |  |
|  |  |

Spis treści

[1. Jaki zakres implementacji protokołu jest niezbędny do wykonania integracji? 4](#_Toc8931558)

[2. Jakie typy transakcji można wywołać? 5](#_Toc8931559)

[3. Które pola z komunikatu S1 są obowiązkowe? 6](#_Toc8931560)

[4. W jaki sposób przesyłane są informacje o etapie transakcji? 6](#_Toc8931561)

[5. Jakie rezultaty transakcji mogą pojawić się w pakiecie S2? 7](#_Toc8931562)

[6. Kiedy transakcja może być unieważniona i jak jest dosyłana? 9](#_Toc8931563)

[7. Które interakcje ze sprzedawcą odbywają się na kasie, a które na terminalu? 10](#_Toc8931564)

[8. Jak wykonywane są wydruki? 10](#_Toc8931565)

[9. Czy wydruk potwierdzenia transakcji dla Akceptanta jest obowiązkowy? 11](#_Toc8931566)

[10. Czy wydruk potwierdzenia transakcji dla Klienta jest obowiązkowy? 12](#_Toc8931567)

[11. Jakie dane prezentowane są na wydrukach? 12](#_Toc8931568)

[12. Jak wywołać opcję wydruku kopii ostatniej transakcji? 13](#_Toc8931569)

[13. Na jakim etapie można anulować transakcję? 13](#_Toc8931570)

[14. Jak przebiega transakcja z dynamiczną wymianą walut (DCC)? 14](#_Toc8931571)

[15. Z jakich narzędzi korzystać do testów autoryzacji? 15](#_Toc8931572)

[16. Jak konfigurować port szeregowy terminala? 16](#_Toc8931573)

[17. Bibliografia 18](#_Toc8931574)

[18. Changelog 18](#_Toc8931575)

# Jaki zakres implementacji protokołu jest niezbędny do wykonania integracji?

Aplikacja sprzedażowa musi wspierać warstwę komunikacyjną protokołu (rozdział 2 specyfikacji *Protokół ECR-EFT*). Do wyzwolenia transakcji niezbędne jest obsłużenie pakietów S1/S2 (rozdział 4), zakres (typy transakcji, przekazywane dane) zależy od integratora.

Jeśli w integracji planowane jest informowanie aplikacji sprzedażowej o postępie transakcji, to musi ona wspierać obsługę pakietów I1.

Jeśli w integracji planowane jest przekazywanie (forwardowanie) komunikacji aplikacji płatniczej przez aplikację sprzedażową, to konieczna jest obsługa pakietów C1/C2. Aplikacja płatnicza pozwala na skonfigurowanie czy forwardowanie ma być wykonywane (potrzebne w przypadku pinpadów programowalnych) czy nie (w wypadku urządzeń z własnymi mediami komunikacyjnymi).

Jeśli w integracji planowane jest wykonywanie wydruków przez aplikację sprzedażową to musi ona wspierać pakiety DD/D0. Wsparcie dla wydruków jest niezbędne w wypadku użycia pinpada programowalnego i opcjonalne w wypadku urządzeń płatniczych posiadających własną drukarkę. Aplikacja płatnicza pozwala na skonfigurowanie tego ustawienia.

Jeśli w integracji planowane jest wykonywanie interakcji z operatorem w aplikacji sprzedażowej to niezbędne jest wspieranie pakietów K0, K3, K4. Opcjonalnie aplikacja sprzedażowa może wspierać również pakiet P1 anulowania transakcji. Wykorzystanie konsoli aplikacji sprzedażowej jest konfigurowalne w aplikacji płatniczej. Jeśli nie zostanie ono włączone to wszystkie interakcje będzie można wykonać na urządzeniu płatniczym.

Jeśli w integracji planowane jest nieudostępnianie aplikacji możliwości wysyłania komunikatów C1/C2 poza przeprowadzanymi transakcjami, to konieczne jest wsparcie dla pakietów SA/SB. Pakiety SA/SB pozwalają wyzwalać rozliczenia transakcji i odpytania o konfigurację (połączenie do TMS – Terminal Management System).

Aplikacja sprzedażowa może korzystać z odpytywania o parametry aplikacji płatniczej D4/D5.

Aplikacja sprzedażowa może wspierać wysyłanie komunikatu M1 – w reakcji na niego aplikacja płatnicza podejmie próbę wykonania rozliczenia.

Aplikacja sprzedażowa może wspierać obsługę pakietu L1 – aplikacja płatnicza wysyła go w momencie rozpoczęcia procesu aktualizacji. Jeśli aplikacja sprzedażowa wykona próbę przeprowadzenia jakiejkolwiek operacji w czasie niedostępności, to aplikacja płatnicza odpowie kodem błędu 255 – zajęty.

Zgodnie z protokołem aplikacja płatnicza obsługuje pakiety T1/T2, jednak nie buduje wokół nich żadnej logiki – jest wystarczające, jeśli aplikacja sprzedażowa odeśle ACK w odpowiedzi na T1.

Poza zakresem integracji są wydruki w trybie linia po linii, interakcje inne niż wymienione powyżej i szyfrowanie komunikacji.

# Jakie typy transakcji można wywołać?

Aplikacja płatnicza wspiera następujące typy transakcji:

* „S” – sprzedaż z możliwością cashback
* „C” – sprawdzenie statusu ostatniej transakcji sprzedaży
* „U” – unieważnienie transakcji
* „K” – kopia wydruku
* „Z” – zwrot
* „P” – preautoryzacja
* „D” – dopełnienie preautoryzacji
* „N” – sprzedaż z możliwością napiwku
* „R” – płatność za rachunki

Aplikacja sprzedażowa wspierać może jedynie wybrane typy transakcji, zależnie od potrzeb integracyjnych.

# Które pola z komunikatu S1 są obowiązkowe?

Aplikacja sprzedażowa musi uzupełnić wszystkie pola przewidziane w protokole FROB jako obowiązkowe. Aplikacja płatnicza nie analizuje danych przesłanych w polach ‘kwota netto’ oraz ‘VAT’ – mogą być one uzupełnione zerami, jeśli te wartości nie są dostępne.

# W jaki sposób przesyłane są informacje o etapie transakcji?

Aplikacja płatnicza wysyła do aplikacji sprzedażowej komunikaty I1. Zawierają one kody statusów zgodne ze specyfikacją (rozdział 16). Aplikacja płatnicza nie przesyła tekstów komunikatów, które mają się wyświetlić w aplikacji sprzedażowej. Jest to działanie celowe, wynikające z potrzeby ograniczenia ilości wymienianych danych (szczególnie istotne przy połączeniu szeregowym, w ciągu transakcji komunikatów może być sporo), a także z założenia, że dostawca aplikacji sprzedażowej będzie lepiej w stanie dopasować komunikaty do rozmiarów ekranu i ew. przyzwyczajeń użytkowników.

Aplikacja płatnicza w swoim buforze pakietów do wysyłki usuwa wszystkie komunikaty przeterminowane, tj. nie wyśle danego pakietu I1, jeśli w buforze jest już dostępny komunikat o późniejszym stanie transakcji. Oznacza to, że nie można zakładać, że dla każdej transakcji zestaw komunikatów będzie identyczny. Jest to działanie celowe, aplikacja płatnicza nie spowalnia przebiegu transakcji jedynie w celu poinformowania użytkownika, że wykonany został standardowy krok przebiegu.

Aplikacja płatnicza oczekuje odpowiedzi ACK na wysłane ramki I1, jednak ich brak nie powoduje przerwania transakcji (rozluźnienie względem wymagań protokołu). Zakłada się, że część urządzeń sprzedażowych może mieć trudność z wysoko asynchroniczną komunikacją podczas transakcji, a informowanie o etapie transakcji jest procesem pomocniczym względem jej przetwarzania.

UWAGA: w specyfikacji Protokół ECR-EFT w rozdziale 16 znajduje się niespójność – token pakietu I1 nie może być echem S1 (sprzeczność z rozdziałem 2.3). Niespójność aplikacja płatnicza rozstrzyga na korzyść ujednolicenia warstwy liniowej.

# Jakie rezultaty transakcji mogą pojawić się w pakiecie S2?

Terminal przesyła do kasy rezultat transakcji w trzecim polu pakietu S2, oprócz tego dokładny komunikat z hosta autoryzacyjnego (jeśli dostępny) jest prezentowany na wydruku dla Merchanta i klienta. Rezultat ‘0’, zgodnie ze specyfikacją, oznacza transakcję zaakceptowaną, wszystkie pozostałe kodują przyczynę odmowy. Tabela możliwych kodów błędów poniżej, może być ona rozszerzana w ramach potrzeb i rozwoju aplikacji płatniczej.

|  |  |  |
| --- | --- | --- |
| Kod | Znaczenie | Przykład |
| 0 | Transakcja zaakceptowana | Poprawna autoryzacja środka płatniczego |
| 1 | Błędne dane karty | Karta niemożliwa do odczytu |
| 2 | Odmowa z karty | Karta do użycia tylko w bankomatach |
| 3 | Brak karty | Karta wyjęta z czytnika przed końcem transakcji |
| 4 | Anulowano | Transakcja przerwana przez użytkownika |
| 5 | Błąd terminala/pinpada | Błąd komponentu szyfrującego podczas wprowadzania PIN |
| 6 | Rozliczenie nieudane | Nie udało się wykonać transakcji rozliczenia |
| 7 | Odmowa online | Host autoryzacyjny przysłał odmowę dla transakcji, szczegóły na wydruku |
| 8 | Błąd otwarcia połączenia | Medium komunikacyjne niedostępne |
| 9 | Błąd parsowania odpowiedzi | Host autoryzacyjny przysłał niezrozumiałą dla terminala odpowiedź na transakcję |
| 10 | Wyczerpane próby połączenia | Wszystkie próby połączenia do hosta autoryzacyjnego zakończyły się błędem |
| 11 | Automatyczne unieważnienie | Transakcja unieważniona z powodu błędnego podpisu posiadacza karty |
| 12 | Ręczne unieważnienie | Transakcja unieważniona przez Merchanta |
| 13 | Restart | Terminal zrestartowany podczas trwania transakcji |
| 14 | Błąd dosyłania | Nie udało się dosłać do hosta poprzedniej unieważnionej transakcji |
| 15 | Karta odrzucona | Analiza karty zakończona rezultatem odmowy |
| 16 | Nierozliczone transakcje | Wykonano więcej niż 200 transakcji bez rozliczenia |
| 17 | Transakcja niedozwolona | Transakcja niedozwolona na danym terminalu |
| …. |  |  |
| …. |  |  |
| 255 | Terminal zajęty | Na terminalu ktoś przeszedł do podmenu (wyzwolenie transakcji możliwe tylko, jeśli aplikacja jest w trybie idle i nie przetwarza innych transakcji) |

# Kiedy transakcja może być unieważniona i jak jest dosyłana?

Transakcja może być unieważniona przez aplikację płatniczą w kilku przypadkach: odmowa z karty bądź niezgodny podpis, brak odpowiedzi z hosta autoryzacyjnego po wysłaniu ramki oraz unieważnienie wyzwolone ręcznie/z terminala. W każdym z tych przypadków aplikacja będzie próbowała dosłać takie unieważnienie (jako offline): tuż po unieważnieniu, co 10 sekund w okresie bezczynności, tuż po rozpoczęciu kolejnej transakcji.

Aplikacja terminalowa może się spodziewać przyjścia komunikatów C1 poza transakcjami. Optymalnym rozwiązaniem jest obsłużenie takiej komunikacji (wtedy kolejne transakcje przebiegną szybciej), ale jeśli aplikacja pinpadowa nie otrzyma odpowiedzi na C1, to nie będzie to dla niej błędem – ponowi próbę dosyłki zgodnie z powyższym schematem.

Aplikacja APDU nie blokuje możliwości rozpoczęcia kolejnej transakcji w wypadku niedosłania offline – kolejna transakcja z punktu widzenia użytkownika wygląda normalnie, próby dosyłki odbywają się w tle. Jeśli dosyłka uda się, to nowa transakcja będzie rozpatrzona zwykłym trybem i może być zaakceptowana. Jeśli dosłanie nie uda się, to nowa transakcja będzie odrzucona z komunikatem ‘brak połączenia [1]’.

Jeśli istnieje taka konieczność, to w aplikacji płatniczej można konfiguracyjnie wyłączyć dosyłanie transakcji w tle – będą one wtedy dosyłane na początku kolejnych transakcji albo tuż przed rozliczeniem.

# Które interakcje ze sprzedawcą odbywają się na kasie, a które na terminalu?

W protokole przewidziane są komunikaty K, umożliwiające zadawanie pytań do Merchanta na terminalu. Podział odpowiedzialności:

1. Pinpad: wybór aplikacji na karcie, pytanie o PIN/kod BLIK
2. Automatyczne: potwierdzenie wydruku kopii dla klienta (pinpad uzna odpowiedź za twierdzącą)
3. Terminal: wszystkie pozostałe pytania (w tym pytanie o podpis i DCC)

Komunikaty K\* niwelują konieczność wysłania dedykowanego I1. Przykład: jeśli pinpad wyśle pakiet K3 z pytaniem o DCC to nie zostanie wysłany pakiet I1 z informacją odnośnie oczekiwania na decyzję DCC.

# Jak wykonywane są wydruki?

Aplikacja płatnicza oczekuje, że wykonane zostaną wydruki transakcyjne, wszystkie pozostałe (informacja o rozliczeniu, aktualizacji, rezultacie diagnostyki) są nieobowiązkowe i nieblokujące.

Aplikacja płatnicza wysyła dane do wydruku potwierdzenia w pakiecie DD.

Przykładowe dane do wydruku wyglądają następująco:

Layout#Transaction;TID#000000123;MID#200002000005;TrDate#06-04-2018 19:07:28;DemoTxt#;Name#APDU SP. Z O.O.;Addr1#UL. Rï¿½WNOLEGï¿½A 2;Addr2#02-231 WARSZAWA;ExgProvider#;DccDisclamer#;DccFlag#;FooterLogoFlag#;CardName#VISA CREDIT;EntryPAN#07;EntryPin#1;CtlsMark#CONTACTLESS;PAN#476173\*\*\*\*\*\*0010;AID#A0000000031010;AOSA#;BLIK#;RefCode#;RRN#809617460178;AuthNo#171691;HostResText#;TrResText#TRANSAKCJA ZAAKCEPTOWANA;TrResFailFlag#;AuthSig#;AuthPin#;InvNo#000198;InvAddText#KOPIA KLIENTA;TrTotalAmt#9.28 PLN;TrTotalName#SPRZEDA¯;

Przykładowe wydruki aplikacji płatniczej można znaleźć w dokumencie „INSTRUKCJA\_OBSŁUGI\_APLIKACJI\_PŁATNICZEJ\_Vx675”.

Uwaga 1: wydruki odcinka dla Akceptanta i Klienta mogą się od siebie różnić, co wynika z wymagań certyfikacyjnych aplikacji płatniczej. W aplikacji sprzedażowej należy bezwzględnie korzystać z danych wysyłanych w obydwu komunikatach i nie należy stosować ich wymiennie.

Uwaga 2: aplikacja płatnicza wspiera przekazywanie danych do wydruków w cp-1250 oraz ISO 8859-2; jest to opcja konfiguracyjna.

# Czy wydruk potwierdzenia transakcji dla Akceptanta jest obowiązkowy?

W ITCARD warunkiem koniecznym, aby uznać transakcję za zaakceptowaną jest wydruk całości potwierdzenia dla Akceptanta. Aplikacja płatnicza wysyła dane potrzebne do wydruku w pakiecie DD i oczekuje na rezultat przez 10 sekund. Nie otrzymanie komunikatu z odpowiedzią będzie równe uznaniu wydruku za wykonany – to aplikacja terminalowa musi zatroszczyć się o unieważnienie transakcji, jeśli zajdzie potrzeba. Aplikacja płatnicza sama unieważni transakcję, jeśli w odpowiedzi na DD otrzyma informację o błędzie logicznym.

# Czy wydruk potwierdzenia transakcji dla Klienta jest obowiązkowy?

Wydruk potwierdzenia dla Klienta nie jest wydrukiem obowiązkowym, jednak silnie zaleca się, aby w wypadku transakcji zaakceptowanych pytać użytkownika o wydruk, ale dla transakcji odrzuconych wykonywać go zawsze.

Aplikacja płatnicza wysyła oddzielne wydruki dla klienta i Merchanta – ogranicza to konieczność kontroli po stronie kasy/terminala, które pola mogą pojawić się na których odcinkach. Wydruki będą wysyłane jeden po drugim w osobnych komunikatach, aplikacja kasowa obsłuży logikę decydowania czy kopia dla klienta jest obowiązkowa oraz przerwę pomiędzy wydrukami. Aplikacja płatnicza nie będzie wysyłała pytania o wydruk kopii klienta – tę logikę powinien obsłużyć terminal.

# Jakie dane prezentowane są na wydrukach?

Wszystkie dane, które zostaną przekazane przez aplikację płatniczą muszą być umieszczone na wydruku dla klienta. W tabeli wyszczególniono, które dane dostępne są zawsze (mandatory), które zależnie od przebiegu transakcji (optional).

|  |  |  |
| --- | --- | --- |
| Stałe informacje dotyczące terminala płatniczego | | |
| Logo Merchanta | marketingowe, nie wysłane przez FROB |  |
| Nazwa i adres Merchanta, | identyfikują merchanta | Mandatory |
| POS ID (TID) i MID | identyfikują terminal w systemie, | Mandatory |
| „Prosimy zachować dowód sprzedaży” | wymaganie Visa/MasterCard | Mandatory |
| Dane o transakcji na terminalu | | |
| Numer rachunku | pozwala zarządzać unieważnieniami i rozliczeniami | Mandatory |
| Typ transakcji, kwota, waluta | wymaganie Visa/MasterCard/BLIK | Mandatory |
| Data i godzina transakcji | wymaganie Visa/MasterCard | Mandatory |
| Dane o karcie/środku płatniczym | | |
| Nazwa karty | wymaganie Visa/MasterCard/BLIK | Optional |
| Skrócony numer karty | wymaganie Visa/MasterCard | Optional |
| Tryb wprowadzania karty | wymaganie Visa/MasterCard/BLIK | Optional |
| AID | numer aplikacji na karcie, wymaganie Visa/MasterCard, | Optional |
| Kod referencyjny | wymaganie BLIK | Optional |
| Skrócony kod BLIK | wymaganie BLIK | Optional |
| Dane o transakcji w systemie autoryzacyjnym | | |
| Rezultat | wymaganie Visa/MasterCard/BLIK | Mandatory |
| Kod odmowy | wymaganie Visa/MasterCard/BLIK | Optional |
| Opis przyczyny odmowy | wymaganie ITCARD | Optional |
| AOSA | wymaganie Visa | Optional |

# Jak wywołać opcję wydruku kopii ostatniej transakcji?

Funkcja ta jest wspierana, kasa powinna wysłać do terminala pustą wartość numeru transakcji (nie wartość zero, która jest w szczególności poprawnym ID transakcji).

Przykład:

[STX]2809[FS]S1[FS]K[FS]ABC1234567890[FS][FS]0[FS]0[FS]0[FS]PLN[FS][ETX][0x16] – wydruk kopii ostatniej transakcji

[STX]2816[FS]S1[FS]K[FS]ABC1234567890[FS]einv1016[FS]0[FS]0[FS]0[FS]PLN[FS][ETX][0xa] – wydruk kopii transakcji einv1016

Po stronie terminala istnieje możliwość sparametryzowania czy ID transakcji (tu: einv1016) pochodzić ma z kasy czy z terminala.

# Na jakim etapie można anulować transakcję?

Aplikacja płatnicza pozwala na anulowanie transakcji od momentu jej rozpoczęcia aż do wysłania komunikatu do centrum autoryzacyjnego. Wysyłka odbywa się:

* po odczycie karty dla transakcji CTLS bez uwierzytelniania albo dla transakcji weryfikowanych podpisem, albo
* po wpisaniu PIN

Jeśli transakcja jest na etapie, w którym można ją anulować, to po odebraniu pakietu P1 aplikacja odeśle ACK, a następnie wyśle komunikat kończący S2 z kodem 4 – anulowano.

Jeśli transakcja jest za punktem, do którego możliwe było anulowanie, to zgodnie z protokołem będzie kontynuowała transakcję aż do S2 z rezultatem uzyskanym w uzgodnieniu pomiędzy kartą a centrum autoryzacyjnym. Wycofanie transakcji możliwe jest przez wykonanie transakcji unieważnienia (S2 ‘U’).

# Jak przebiega transakcja z dynamiczną wymianą walut (DCC)?

Wsparcie dla dynamicznej wymiany walut nie jest obowiązkowym elementem integracji. Dostępność tej funkcji dla Akceptantów zależy od ustaleń umownych z ITCARD, a w aplikacji płatniczej jest konfigurowalna.

Jeśli DCC jest wspierane, to po odczycie danych karty (zbliżenie, wprowadzenie, przeciągnięcie), aplikacja płatnicza weryfikuje najpierw offline a następnie online (dodatkowe zapytanie do centrum autoryzacyjnego) dostępność oferty DCC. Jeśli oferta jest dostępna, to aplikacja płatnicza generuje wydruk z warunkami (obowiązkowy do obsługi przez aplikację sprzedażową).

Przykładowe dane do wydruku:

Layout#DccQuote;TrDate#06-04-2018 19:14:48;ExgHeader#DCC Quote;ExgRateTxt#Exchange rate;ExgCommTxt#Commission;ExgFeeTxt#Fee/Mark-up;ExgTotalAmtName#TOTAL;ExgOrigAmt#9.28 PLN;ExgOrigCurr#PLN;ExgTotalAmt#2.12 GBP;ExgTotalAmtCurr#GBP;ExgCommAmt#0.00 GBP;ExgRateAmt#0.2288082;ExgFeeAmt#0.00 GBP;ExgProvider#MBANK;

Po wykonaniu wydruku aplikacja płatnicza pyta o wybór waluty (do wyboru waluta transakcji albo waluta karty). Pytanie może zostać zadane w aplikacji płatniczej albo sprzedażowej.

Uwaga: w żadnym wypadku aplikacja sprzedażowa nie może podjąć decyzji o zmianie waluty transakcji na walutę karty bez aktywnej zgody Klienta. Jeśli użytkownik nie udzieli odpowiedzi, to użytą walutą musi być PLN. Jest to zachowanie bardzo silnie regulowane i nadzorowane przez Organizacje Płatnicze.

Po dokonaniu wyboru waluty transakcja kontynuowana jest w standardowym przebiegu. Wydruk odcinka dla klienta przygotowany jest w języku angielskim.

# Z jakich narzędzi korzystać do testów autoryzacji?

Testy poprawnych autoryzacji transakcji płatniczych można wykonywać za pomocą:

* fizycznych kart testowych
* aplikacji Visa CDET (Contactless Device Evaluation Toolkit)
* kodów BLIK z zakresu 777000 – 777777

Narzędzie do emulacji kart CTLS Visa można pobrać ze sklepu Google (aplikacja dostępna w wersji na Android). Aplikacja wymaga aby ustawić ją jako domyślną do obsługi czytnika NFC. Osoby, które nie korzystają na co dzień z płatności komórką muszą pamiętać również o aktywowaniu NFC w telefonie. Po skończonych testach warto pamiętać o przywróceniu domyślnej aplikacji do obsługi NFC (np. Google Pay).

Kody BLIK z zakresu 777000 – 777777 według PSP powinny być akceptowane bezwarunkowo na środowisku testowym. Praktyka pokazuje, że jest w tym procesie pewna losowość, natomiast faktycznie większość kodów jest akceptowanych.

Używanie produkcyjnych kart do wykonywania transakcji na środowisku testowym nie jest zalecane. Oczywiście w ślad za takimi transakcjami nie pójdą żadne obciążenia, ale aplikacje na karcie będą podbijały sobie liczniki, co może skutkować innym niż standardowe zachowanie przy wykonywaniu transakcji produkcyjnych. Jeśli istnieje konieczność korzystania z takich kart do wykonywania testów, to zaleca się wyzwalanie transakcji na możliwie najniższą kwotę (1,00 PLN).

# Jak konfigurować port szeregowy terminala?

Ustalenie sposobu komunikowania się urządzenia płatniczego z systemem kasowym powinno odbyć się na samym początku projektu, a informacja o produkcyjnych ustawieniach powinna zostać przekazana do zespołu operacyjnego ITCARD.

W integracjach z wykorzystaniem kabla szeregowego dostępne są następujące ustawienia:

* Numer portu – poprawne wartości to:
  + 1 - port szeregowy RS-232 terminala
  + 6 – port USB host (USB A) w terminalu, do którego podpięta będzie przejściówka z końcówką RS-232
  + 16 - port client USB, w praktyce wejście mini bądź mikro w terminalu płatniczym albo kabel do Vx820 kończący się USB A wpinanym do komputera systemu kasowego
* Baudrate – prędkość komunikacji – zalecana wartość to 115200
* Desc (format słowa) – zalecana wartość to 8n1
* Hardware Flow Control – zalecana wartość to 0 (wyłączony)

# Bibliografia

1. Protokół komunikacyjny ECR-EFT. Wersja 1.6. APDU 0.6 2019.03.14
2. INSTRUKCJA\_OBSŁUGI\_APLIKACJI\_PŁATNICZEJ\_Vx675\_ver. 1.0.0

# Changelog

|  |  |  |  |
| --- | --- | --- | --- |
| Wersja | Data | Autor/ka | Zmiana |
| 1.0 | 2018.12.13 | Maria Siewierska | Wersja początkowa |
| 1.1 | 2019.01.31 | Maria Siewierska | Opis danych na wydrukach |
| 1.2 | 2019.04.01 | Maria Siewierska | Jak wywołać opcję wydruku kopii ostatniej transakcji?  Dodano zapis o możliwości kodowania komunikatów w cp-1250 albo iso-2 |
| 1.3 | 2019.04.05 | Maria Siewierska | Jak konfigurować port szeregowy terminala? Aktualizacja referencyjnej specyfikacji ECR-EFT do wersji 1.6\_0.6 |
| 1.4 | 2019.05.16 | Maria Siewierska | Jakie rezultaty transakcji mogą pojawić się w pakiecie S2? |