

Sprawozdanie - Skrypt LDR do odczytu NTAG przez czytnik PC/S.C.

Aleksander Kwaśnioch 151887

Temat

Odczyt zawartości pamięci układu **NXP NTAG21x** (NTAG213/215/216, NFC Type 2 Tag) przy pomocy czytnika zbliżeniowego w standardzie **PC/SC**, zrealizowany jako skrypt w formacie **EasyReader LDR**.

Cel i zakres

Celem jest przygotowanie skryptu, który po przyłożeniu karty do czytnika sekwencyjnie odczytuje i prezentuje: identyfikator karty (UID), typ układu, Capability Container oraz pamięć użytkownika (komunikat NDEF). Pełny przebieg sesji jest zapisywany do logu na dysku.

Środowisko

- Czytnik PC/SC dla kart 13,56 MHz (ISO/IEC 14443A), np. ACR122U (kontroler PN532).
- Usługa PC/SC (pcscd w systemie Linux lub *Smart Card* w Windows).
- Tester skryptów EasyReader (format .ldr - ten sam, co dołączony przykład EMV).
- Karta z układem NTAG213, NTAG215 lub NTAG216.

Budowa pamięci NTAG21x (na podstawie dokumentacji)

Pamięć jest podzielona na **strony po 4 bajty**:

Strony	Zawartość
0–1	UID (7 B) + bajt kontrolny BCC0
2	BCC1, bajt wewnętrzny, bajty blokad (lock)
3	Capability Container (CC) - informacja o pojemności NDEF
4 ...	Pamięć użytkownika / komunikat NDEF
końcowe	Strony konfiguracyjne (CFG0/CFG1, hasło PWD/PACK)

Pojemność obszaru użytkownika zależy od wariantu: NTAG213 $\approx$ 144 B (strony 0x04–0x27), NTAG215 $\approx$ 504 B, NTAG216 $\approx$ 888 B.

Realizacja - opis kroków skryptu read_ntag.ldr

Skrypt napisano w konwencji dołączonego przykładu EMV: dyrektywy PWRON/ PWROFF, polecenia CMD <APDU> \ z oczekiwanym słowem statusu (90 00) oraz komentarze REM/;. Wykorzystano dwa rodzaje poleceń: **pseudo-APDU PC/SC** (warstwa czytnika) oraz **polecenia natywne NTAG** opakowane w *InCommunicateThru* (D4 42) i wysyłane przez FF 00 00 00 <Lc> D4 42

Krok 0 - Aktywacja karty (PWRON)

Aktywuje pole RF czytnika i nawiązuje połączenie z kartą zbliżeniową (odpowiednik zasilenia karty stykowej w przykładzie EMV). Bez tego kroku żadne CMD nie zostanie wykonane.

Krok 1 - Odczyt UID (FF CA 00 00 00)

Standardowe pseudo-APDU PC/SC *Get Data*. Zwraca 7-bajtowy unikatowy identyfikator układu zakończony statusem 90 00. Pierwszy bajt UID to 04 (kod producenta NXP).

Krok 2 - Identyfikacja typu (GET_VERSION, D4 42 60)

Natywne polecenie 0x60 opakowane w *InCommunicateThru*. W odpowiedzi otrzymujemy 8 bajtów; **bajt rozmiaru pamięci** rozróżnia wariant układu: 0F → NTAG213, 11 → NTAG215, 13 → NTAG216. Dzięki temu wiadomo, do której strony należy czytać pamięć w kroku 4.

Krok 3 - Capability Container (FF B0 00 03 04)

Pseudo-APDU PC/SC *Read Binary* odczytujące stronę 3 (4 bajty). CC potwierdza typ formatu NDEF i deklarowaną pojemność: E1 10 12 00 (NTAG213), E1 10 3E 00 (NTAG215) lub E1 10 6D 00 (NTAG216).

Krok 4 - Pamięć użytkownika / NDEF (FF B0 00 <strona> 10)

Seria odczytów *Read Binary* po 16 bajtów (4 strony naraz), począwszy od strony 0x04. W skrypcie pokryto pełny obszar użytkownika NTAG213 (strony 0x04-0x27). Tu znajduje się właściwa zawartość zapisana na karcie - np. komunikat NDEF (URL, tekst). Dla NTAG215/216 zakres pętli należy rozszerzyć zgodnie z wynikiem kroku 2.

Krok 5 - Zakończenie (PWROFF)

Wyłącza pole RF / kończy sesję z kartą. Cały dialog (wysłane APDU oraz odpowiedzi karty wraz ze słowami statusu) jest na bieżąco zapisywany przez EasyReader do **pliku logu** na dysku - to realizuje wymaganie zapisania wyników. Końcowy WARN zostawia w logu czytelny znacznik zakończenia.

Rezultaty

Po uruchomieniu skryptu w EasyReaderze w logu pojawiają się kolejne pary „polecenie → odpowiedź”. Poniżej **przykładowy** układ wyników:

[KROK 1] UID : 04 A1 B2 C3 D4 E5 F6 SW=90 00
[KROK 2] GET_VERSION : 00 04 04 02 01 00 0F 03 -> NTAG213
[KROK 3] CC (strona 3) : E1 10 12 00 -> NDEF, ~144 B
[KROK 4] Pamięć 04..27 : <zrzut stron użytkownika / komunikat NDEF>

Podsumowanie realizacji kroków

Krok	Polecenie	Efekt
0	PWRON	aktywacja karty / pola RF
1	FF CA 00 00 00	odczyt UID
2	D4 42 60 (GET_VERSION)	identyfikacja typu układu
3	FF B0 00 03 04	odczyt Capability Container
4	FF B0 00 <str> 10	odczyt pamięci użytkownika / NDEF
5	PWROFF + log	zakończenie i zapis wyników na dysku

Uwagi

- Dokładne pseudo-APDU (*InCommunicateThru*, *Read Binary*) zależą od modelu czytnika; przy czytniku innym niż ACR122U należy je dostosować do jego dokumentacji.
- Skrypt można rozszerzyć o odczyt podpisu oryginalności (READ_SIG, D4 42 3C 00) oraz stron konfiguracyjnych, jeśli zakres projektu ma objąć także autentykację układu.

Zawartość

- read_ntag.ldr - skrypt odczytu NTAG (format EasyReader LDR);
- SPRAWOZDANIE.pdf - dokumentacja opisująca kroki skryptu.