



Systemy Automatycznej Identyfikacji

AI - Odczyt i interpretacja EF.CERT i EF.ELS

Rafał Szygenda 151152

9 czerwca 2026

Spis treści

1	Temat projektu i punkty do realizacji	3
2	Projekt	3
2.1	Zadanie 1 - Odczytanie pliku EF.CERT	4
2.2	Zadanie 2 - Interpretacja pliku EF.CERT	5
2.3	Zadanie 3 - Odczytanie pliku EF.ELS	6
2.4	Zadanie 4 - Interpretacja pliku EF.ELS	6

1 Temat projektu i punkty do realizacji

Tematem projektu jest odczyt i interpretacja plików EF.CERT, EF.ELS z wykorzystaniem narzędzi AI. Do realizacji zadań wykorzystano **Google Gemini 3.1 Pro** z Rozszerzonym poziomem myślenia, oraz **Claude Opus 4.8** z opcją Effort high. Pełna historia promptów oraz odpowiedzi znajdują się w załączniku [1]. W ramach projektu wyznaczone zostały następujące punkty do realizacji:

- Wykonanie następujących zadań, polecenia których, znajdują się na eKursie w sekcji Elektroniczna Legitymacja Studencka
 1. Odczytanie pliku EF.CERT
 2. Interpretacja pliku EF.CERT
 3. Odczytanie pliku EF.ELS
 4. Interpretacja pliku EF.ELS
- Przygotowanie promptów, zapisanie odpowiedzi modelu
- Analiza poprawności wykonanych zadań przez AI

2 Projekt

W tej sekcji przedstawione zostaną zrealizowane zadania, w następującym formacie: AI Prompt → Odpowiedź AI → wykonanie poleceń i analiza poprawności. Przed wysłaniem poleceń do AI przygotowano następujący prompt, do którego załączono pliki ISO_7816-4.2005, ISO_7816-3.2006, LabPKE_03 - ELS do konwersacji z modelem **Google Gemini 3.1 Pro**. Odpowiedzi dla modelu **Claude Opus 4.8** nie posiadają żadnych plików w kontekście. Wewnątrz promptów umieściłem także informację o wersji platformo-sprzętowej własnej legitymacji studenckiej (OberthurCS IAS).

```

1  Cześć, będę przygotowywać projekt związany z realizacją zadań na kartach
    elektronicznych z wykorzystaniem narzędzi AI. Zanim rozpoczniemy pracę pokażę ci
    co konkretnie będziemy robić, oraz dorzucę ci w kontekst pliki/normy/prezentacje
    które pomogą ci w realizacji zadań. Warto napomknąć iż do zadań potrzebna jest
    informacja, że moja karta jest typu OberthurCS IAS.
2
3  Tematem projektu jest odczyt i interpretacja plików \texttt{EF.CERT}, \texttt{EF.ELS}
    z wykorzystaniem narzędzi AI.
4  W ramach projektu wyznaczone zostały następujące punkty do realizacji:
5  \begin{itemize}
6    \item Wykonanie następujących zadań, polecenia których, znajdują się na eKursie w
      sekcji \texttt{Elektroniczna Legitymacja Studencka}
7    \begin{enumerate}
8      \item Odczytanie pliku \texttt{EF.CERT}
9      \item Interpretacja pliku \texttt{EF.CERT}
10     \item Odczytanie pliku \texttt{EF.ELS}
11     \item Interpretacja pliku \texttt{EF.ELS}
12   \end{enumerate}
13   \item Przygotowanie promptów, zapisanie odpowiedzi modelu
14   \item Analiza poprawności wykonanych zadań przez AI
15 \end{itemize}

```

2.1 Zadanie 1 - Odczytanie pliku EF.CERT

Przygotowany prompt:

```

1 Dobrze, to idziemy z zadaniem 1, odczytanie pliku EF.CERT, Wykonaj zadanie według
  następujących poleceń
2 Uruchom oprogramowanie EDSI Easy Reader
3 Przygotuj polecenia APDU pozwalające na wybranie pliku EF.CERT
4
5 Wyślij polecenia APDU do karty
6 Odczytaj i zinterpretuj odpowiedzi
7 Odczytaj zawartość pliku
8 Zapisz plik w postaci binarnej (możesz użyć oprogramowania HxD),
9 jako nazwę podaj numer albumu uzupełnione o _"EF_CERT" z rozszerzeniem
10 ".bin"
11 Odczytaj plik w oprogramowaniu ASN.1 Edytor, w razie
12 konieczności dostosuj długość pliku, w wyniku otrzymasz "drzewko" tagów i
13 ich wartości
14 Plik binarny dołącz w odpowiedzi zwrotnej

```

Odpowiedź **Google Gemini 3.1 Pro** w tym przypadku starało się wykonać wszystkie dane zadania. Poza przygotowaniem komend do wysłania przygotowało także analizę i strukturę w ASN1.Editor i skrypt python do generowania pliku binarnego. Przedstawiono poniżej wyłącznie odpowiedź dotyczącą przygotowanych poleceń.

```

1 ### 1. Przygotowanie i wysłanie poleceń APDU
2 W celu odczytania certyfikatu, należy najpierw wybrać odpowiednią aplikację (ELS),
  następnie plik 'EF.CERT', a na końcu odczytać jego zawartość w blokach.
3 **Wybór aplikacji ELS (SELECT FILE)**
4 *
5 **APDU:** '00 A4 04 04 07 D6 16 00 00 30 01 01'
6 * **Oczekiwana odpowiedź:** '90 00' (Sukces)
7 **Wybór pliku EF.CERT (SELECT FILE)**
8 *
9 **APDU:** '00 A4 02 04 02 00 01'
10 * **Oczekiwana odpowiedź:** '90 00'
11
12 **Odczyt zawartości pliku (READ BINARY)**
13 Z uwagi na rozmiar certyfikatu, dane odczytywane są partiami poprzez inkrementację
  parametru offsetu.
14 * Blok 0: '00 B0 00 00 80'
15 * Blok 1: '00 B0 00 80 80'
16 * Blok 2: '00 B0 01 00 80'
17 * ... (proces powtarzany do momentu otrzymania błędu braku danych, np. '6B 00' lub
  '62 82').

```

Claude Opus 4.8 sam rozpoczął wyszukiwanie odpowiednich norm oraz standardów ISO do realizacji zadania, mimo braku posiadania ich w kontekście. Odpowiedź:

```

1 00 A4 00 00 02 3F 00 ; SELECT MF (3F 00)
2 00 A4 04 04 07 D6 16 00 00 30 01 01 00 ; SELECT DF.SELS po AID
3 00 A4 00 00 02 00 01 00 ; SELECT EF.CERT (id 00 01)
4 00 B0 00 00 80 ; READ BINARY, offset 0x0000, 128 B
5 00 B0 00 80 80 ; offset 0x0080
6 00 B0 01 00 80 ; offset 0x0100
7 ... ; kolejne offsety co 0x80, aż do końca
  pliku

```

Przygotowane polecenia od **Google Gemini 3.1 Pro** były prawidłowe, jednakże te przygotowane przez **Claude Opus 4.8** nie były w pełni poprawne. W odróżnieniu do przygotowanych poleceń przez Gemini, Claude dodaje dodatkowe 00 dla poleceń SELECT. Możliwą przyczyną jest to, iż Claude automatycznie przeszukał internet w poszukiwaniu standardu, który dodał do kontekstu, aby utworzyć polecenia.

2.2 Zadanie 2 - Interpretacja pliku EF.CERT

Przygotowany prompt załącza plik EF_CERT.BIN.

```
1 Przechodzimy do realizacji zadania nr 2, interpretacja EF_CERT. Wykorzystując twoje
   polecenia, przygotowałem plik binarny zawartości EF.CERT.
2 Chciałbym zobaczyć czy masz możliwość analizy własnoręcznej analizy, bez
   wykorzystania oprogramowania, jeżeli nie, sam otworzę ten plik i przestawię ci
   zawartość w następnym promptcie.
3
4 Uruchom oprogramowanie ASN.1 Edytor
5 Wczytaj zapisany w zadaniu 1 plik EF.CERT
6 Znajdź element struktury wskazujący na osobę przedłużającą ELS
7 W odpowiedzi podaj imię i nazwisko oraz PESEL osoby przedłużającej
8
9 Poniżej wrzucam ci otwarty plik bin w ASN1 Editor w formie tekstowej
10 (Zawartość pliku w formie tekstowej, View node as text w asn1 editor)
```

Poniżej przedstawiono odpowiedź **Google Gemini 3.1 Pro**. Model **Claude Opus 4.8** także znalazł prawidłowo dane. AI poprawnie odczytało imię nazwisko oraz pesel osoby przedłużającej.

```
1 Na podstawie przesłanej struktury ASN.1 pliku 'EF.CERT', odpowiednie dane podmiotu (
   osoby przedłużającej) znajdują się w sekcji 'Subject' certyfikatu.
2 Oto wyodrębnione informacje:
3 * **Imię:** Arleta (odczytane z atrybutu 'G' - Given Name, OID '2.5.4.42', offset '01
   e0')
4 * **Nazwisko:** Pieńkowska (odczytane z atrybutu 'SN' - Surname, OID '2.5.4.4',
   offset '01f1')
5 * **PESEL:** 73071706784 (odczytane z atrybutu 'SERIALNUMBER', OID '2.5.4.5', offset
   '012d' z wartości 'PNOPL-73071706784')
```

2.3 Zadanie 3 - Odczytanie pliku EF.ELS

Prompt:

```

1 Przechodzimy do następnego zadania, odczytanie EF.ELS
2 Przygotuj wyłącznie polecenia do odczytu pliku, pozostałe polecenia możesz pominąć.
3 Uruchom oprogramowanie EDSI Easy Reader
4 Przygotuj polecenia APDU pozwalające na wybranie pliku EF.ELS
5 Wyślij polecenia APDU do karty
6 Odczytaj i zinterpretuj odpowiedzi
7 Odczytaj zawartość pliku
8 Zapisz plik w postaci binarnej (możesz użyć oprogramowania HxD), jako nazwę
9 podaj numer albumu uzupełnione o "_EF.ELS" z rozszerzeniem ".bin"
10 Odczytaj plik w oprogramowaniu ASN.1 Edytor, w razie konieczności dostosuj
11 długość pliku, w wyniku otrzymasz "drzewko" tagów i ich wartości
12 Plik binarny dołącz w odpowiedzi zwrotnej

```

Odpowiedź Google Gemini 3.1 Pro:

```

1 Poniżej znajduje się sekwencja komend APDU niezbędna wyłącznie do odczytu pliku 'EF.
  ELS':
2 **1. Wybór aplikacji ELS (DF.SELS)**
3 '00 A4 04 04 07 D6 16 00 00 30 01 01'
4
5 **2. Wybór pliku (EF.ELS)**
6 '00 A4 02 04 02 00 02'
7
8 **3. Odczyt zawartości pliku (READ BINARY)**
9 Odczyt należy realizować sekwencyjnie w blokach po 128 bajtów (0x80), inkrementując
10 offset (parametry P1 i P2), aż do momentu, gdy karta zwróci błąd braku danych:
11 * '00 B0 00 00 80'
12 * '00 B0 00 80 80'
13 * '00 B0 01 00 80'
14 * '00 B0 01 80 80'
15 * ...

```

Odpowiedź Claude Opus 4.8:

```

1 00 A4 00 00 02 3F 00 ; SELECT MF (3F 00)
2 00 A4 04 04 07 D6 16 00 00 30 01 01 00 ; SELECT DF.SELS po AID
3 00 A4 00 00 02 00 02 00 ; SELECT EF.ELS (id 00 02)
4 00 B0 00 00 80 ; READ BINARY, offset 0x0000, 128 B
5 00 B0 00 80 80 ; offset 0x0080
6 00 B0 01 00 80 ; offset 0x0100
7 ... ; offsety co 0x80, aż do końca pliku

```

Podobnie jak w punkcie 2.1 przygotowane polecenia od Google Gemini 3.1 Pro były prawidłowe, jednakże te przygotowane przez Claude Opus 4.8 nie były w pełni poprawne. Prawdopodobnym jest, iż ten sam problem automatycznego zaciągnięcia kontekstu, mógł spowodować błąd przy tworzeniu poleceń.

2.4 Zadanie 4 - Interpretacja pliku EF.ELS

Prompt:

```

1 Przechodzimy do ostatniego zadania, interpretacja zawartosci ef.els
2 Polecenia:
3 Uruchom oprogramowanie ASN.1 Edytor
4 Wczytaj zapisany w zadaniu 2 plik EF.ELS
5 Znajdź element struktury wskazujący na numer układu ELS
6 W odpowiedzi podaj ten numer
7
8 Zawartość pliku z asn1 editor w formie tekstowej:
9 (Zawartość pliku w formie tekstowej, View node as text w asn1 editor)

```

Przedstawiono poniżej krótką odpowiedź **Google Gemini 3.1 Pro**. Odpowiedź **Claude Opus 4.8** także znalazła ten sam numer układu ELS, jednakże dołączyła w także inne dane jak imię, nazwisko, nr pesel, data ważności.

```
1 Numer układu ELS to 01314865B7A63300.
2 W strukturze ASN.1 znajduje się on pod offsetem 0044 jako wartość elementu
  PrintableString (deklaracja pod offsetem 0042)
```

Sztuczna inteligencja poprawnie znalazła numer układu ELS.

Literatura

- [1] Google. (2026). *Gemini [Large language model]*. Historia promptów do wykonania projektu. Dostępne pod adresem: <https://gemini.google.com/share/0509f8c0e773> (dostęp: 4 czerwca 2026).
- [2] Claude. (2026). *Claude [Large language model]*. Historia promptów do wykonania projektu. Dostępne pod adresem: <https://claude.ai/share/befb477c-a193-418f-b2f6-4e5dd717d707> (dostęp: 4 czerwca 2026).