

Temat projektu: AI – wykonanie zadania (Zinterpretuj ATR)

Filip Witkowski 151459

1. Wybrane modele językowe

Wybrane modele językowe: GPT-4.1, Claude Haiku 4.5, Gemini 3.5 Thinkings.

2. Prompt

Wykonaj następujące zadania dotyczące elektronicznej legitymacji studenckiej (ELS):

- Wyjaśnij, czym jest ATR (Answer To Reset) w kontekście ELS.
- Podaj, jakim programem i przy użyciu jakiego sprzętu można odczytać ATR z elektronicznej legitymacji studenckiej.
- Opisz, jak skonstruować zapytanie do karty ELS oraz jak je poprawnie wysłać.
- Wyjaśnij, jak interpretować odpowiedź otrzymaną z karty.

3. Porównanie odpowiedzi poszczególnych modeli językowych

Cecha	GPT	Haiku	Gemini
Pokrycie pytań	Odpowiada na wszystkie pytania, ale skrótowo.	Odpowiedzi pełniejsze, z przykładami.	Odpowiedzi pełne (często rozbudowane).
Kluczowy błąd / ryzyko merytoryczne	Mieszanie kontekstów (np. sugestie o „MIFARE” w ATR) oraz nieścisłość „EF” vs SELECT AID.	Podaje bardzo konkretny ATR jako „dla polskiej ELS PWPW” i dekoduje „JCOP...” bez źródeł — wysokie ryzyko konfabulacji.	Miesza ATR z NFC (powinno być ATR vs ATS) oraz kategoryczne twierdzenia o DF.SELS i „oficjalnym AID” bez źródeł.

Kontynuacja na następnej stronie

Cecha	GPT	Haiku	Gemini
ATR: poprawność definicji (ISO 7816)	Definicja poprawna.	Definicja poprawna.	Definicja poprawna.
ATR: przykłady i wiarygodność	Brak przykładów (mniej ryzyka, ale mniej konkretnie).	Jest przykład, ale trudno ocenić wiarygodność bez źródeł (ryzyko konfabulacji).	Brak przykładu.
Sprzęt (czytniki) i dopasowanie do styk/NFC	Lista sensowna, ale bez jasnego rozdziału: stykowe vs NFC.	Sensownie, ale missing modele bez wyjaśnienia trybu (styk/NFC).	Dobrze sygnalizuje ISO 7816 vs ISO 14443, ale nadal brakuje mapowania „który model do czego”.
Oprogramowanie (pcsc_scan, CardPeek, itd.)	Propozycje ogólnie trafne; lista dla Windows wygląda trochę przypadkowo.	Lista dłuższa, ale część narzędzi/nazw jest mało precyzyjna lub niepewna.	Sensowne propozycje, ale stwierdzenie „pcsc_scan odpytuje publiczną bazę” jest mylące.
APDU: opis struktury (CLA/INS/P1/P2/Lc/Le)	Jest, ale z nieprecyzyjnym formatem i „Case 1”.	Bardzo klarownie: pole po polu + sensowne przykłady.	Bardzo czytelnie, ale upraszcza Lc/Le do 1 bajtu bez zastrzeżeń (brak uwagi o extended length).
APDU: przykłady (SELECT/READ) i spójność	Przykład SELECT AID opisany jako „EF” — niespójność.	SELECT MF, READ BINARY, SELECT AID — opis raczej spójny.	SELECT AID poprawny składniowo, ale oparty o niepewne założenia (DF.SELS, „oficjalny AID”).
Interpretacja odpowiedzi (SW1/SW2)	Dobre klasyczne kody (np. 90 00, 6A 82).	Szeroka tabela kodów — praktycznie użyteczna.	Dobre omówienie m.in. 90 00, 61xx, 6A82, 6D00, 6E00, 6700.
Bezpieczeństwo / legalność / prywatność	Neutralnie, ale brakuje wyraźnych zastrzeżeń/ostrzeżeń.	Brak ostrzeżeń; sugerowanie parsera online może ujawniać fingerprint karty.	Brak ostrzeżeń; dużo spekulacji o danych/strukturach.

Kontynuacja na następnej stronie

Cecha	GPT	Haiku	Gemini
Ton i styl (klarowność)	Zwięzłe i czytelne.	Uporządkowane i in- struktażowe, ale for- matowanie momen- tami chaotyczne.	Bardzo dydak- tyczne, ale zbyt pewne tam, gdzie powinny być za- strzeżenia.
Ogólna rzetelność (bez źró- deł)	Mniej konkretów → mniejsze ryzyko konfabulacji, ale też mniejsza precyzja.	Dużo konkretów.	Dużo konkretów o „polskiej ELS”.

4. Podsumowanie

Najbezpieczniejsza pod względem niekonfabulowania szczegółów jest odpowiedź GPT, ale jest też najmniej precyzyjna i ma kilka nieścisłości. Najbardziej „praktyczna warsztatowo” jest odpowiedź Haiku, tylko że zawiera najbardziej ryzykowny, niezweryfikowany konkret (ATR rzekomo dla ELS PWPW). Odpowiedź Gemini jest najlepiej napisana dydaktycznie, ale ma istotny błąd koncepcyjny (ATR vs NFC/ATS) i zbyt kategoryczne twierdzenia o specyficznych elementach polskiej ELS bez podania źródeł.