# Metoda ochrony informacji w systemach mobilnych wykorzystująca zewnętrzny komponent sprzętowy

mgr inż. Marcin Nowacki

opiekun naukowy: prof. dr hab. inż. Zbigniew Suszyński



Politechnika Koszalińska
Zakład Systemów Multimedialnych i Sztucznej Inteligencji

Koszalin, 16.04.2019 r.

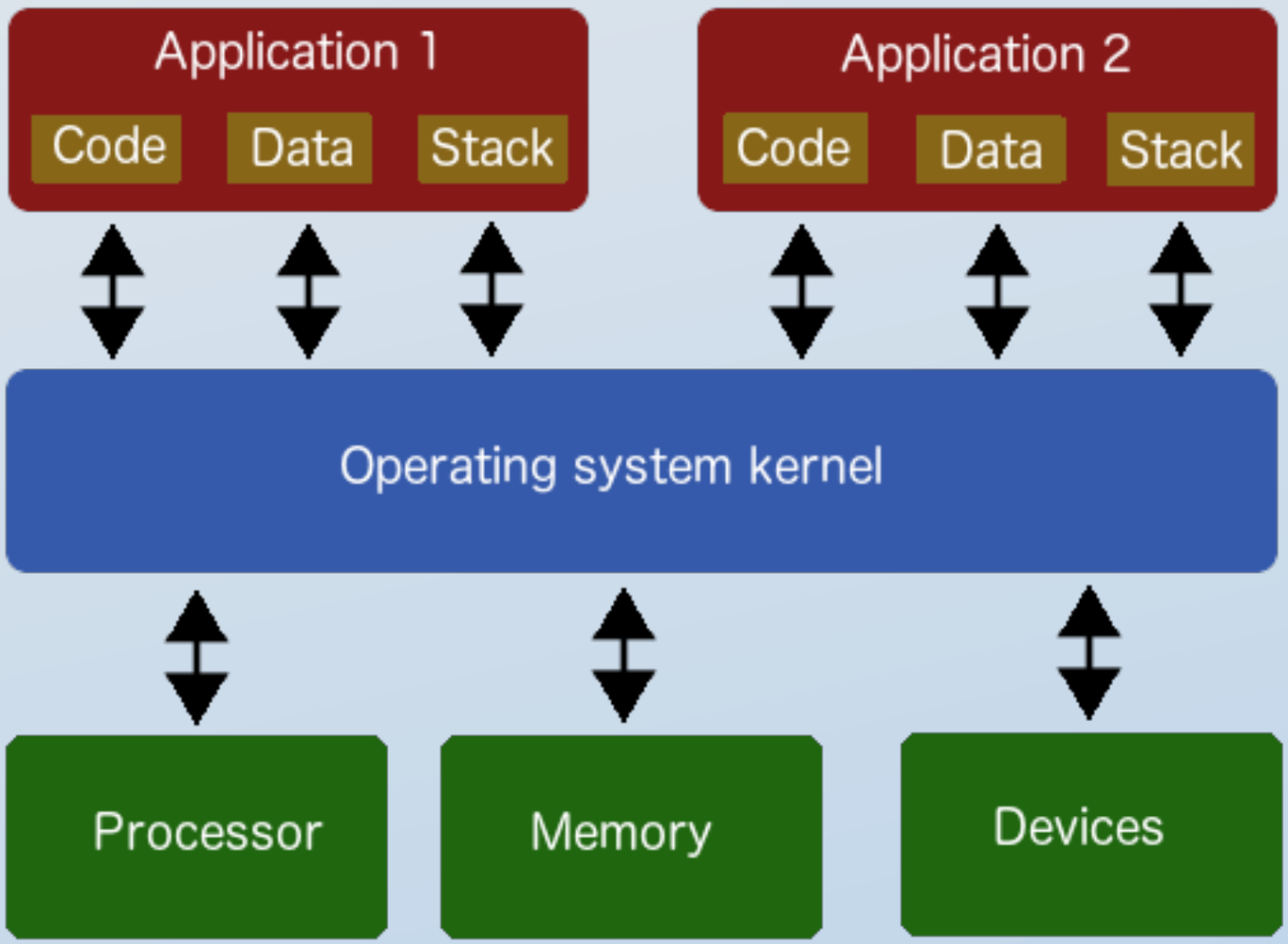
# GŁÓWNE ZAGROŻENIA W SYSTEMACH MOBILNYCH

- błędy w systemach operacyjnych
- korzystanie z sieci internetowej poprzez niezabezpieczone punkty dostępu Wi-Fi, m. in. w miejscach publicznych
- instalowanie aplikacji mobilnych z niezaufanych źródeł
- niedostateczna weryfikacja aplikacji przez tzw. „Sklepy aplikacji”
- brak świadomości użytkowników wobec zagrożeń, które mogą wystąpić w skutek niewłaściwego korzystania z urządzeń mobilnych

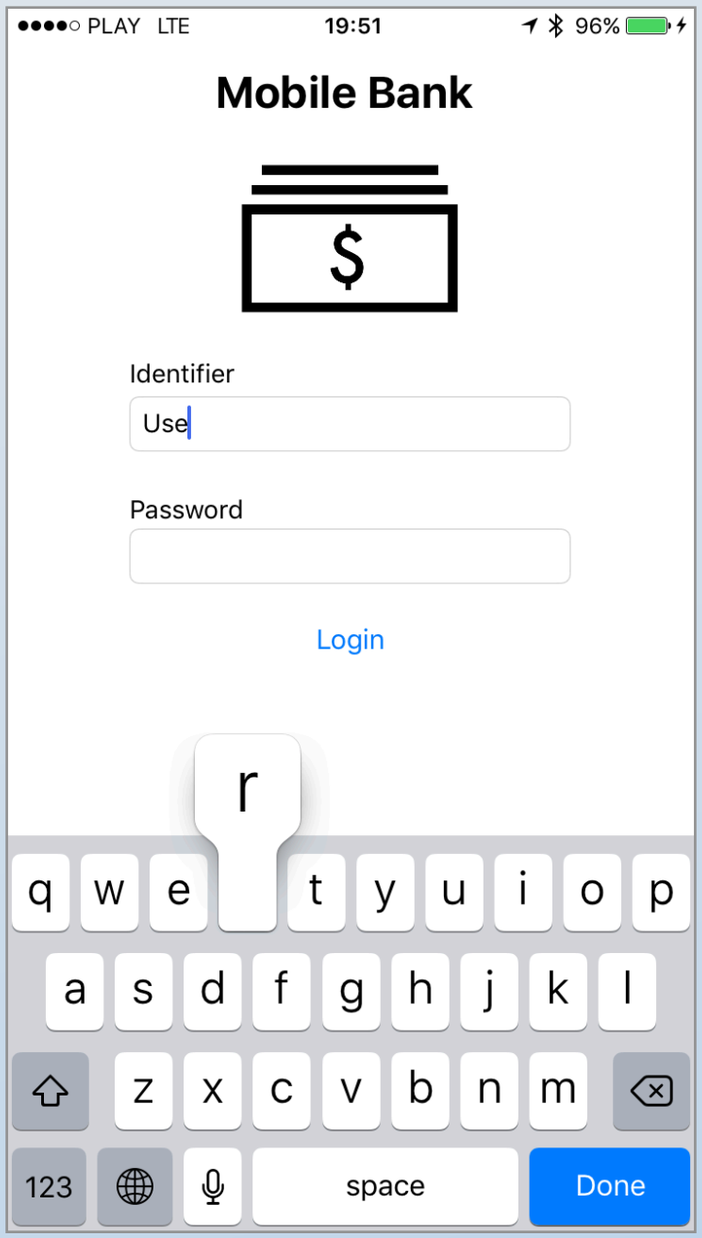
# KLASY ATAKÓW

- atak od środka
- atak wykonany przez inną aplikację
- atak z wykorzystaniem warstwy sprzętowej

# ATAK OD ŚRODKA



# ATAK WYKONANY PRZEZ INNĄ APLIKACJĘ



# ATAK Z WYKORZYSTANIEM WARSTWY SPRZĘTOWEJ


Źródło: https://www.purepc.pl/image/felieton/2018/01/10_meltdown_i_spectre_wszystko_o_lukach_w_procesorach_intel_amd_0_b.png

# PRZEGLĄD LITERATURY - KIERUNKI PROWADZONYCH BADAŃ

## Ochrona informacji z wykorzystaniem zewnętrznych komponentów

- Jongwon Choi, Geonbae Na, Jeong Hyun Yi, *„Hardware-assisted credential management scheme for preventing private data analysis from cloning attacks”*, Multimed Tools Appl (2016) 75:14833–14848

- Bhoraskar R, Han S, Jeon J, Azim T, Chen S, Jung J, Nath S, Wang R, Wetherall D (2014) *„Brahmas- tra: driving apps to test the security of third-party components”*. In: Proceedings of the 23rd USENIX conference on Security Symposium, pp 1021–1036. USENIX Association

## Ochrona informacji z wykorzystaniem dodatkowego komponentu wbudowanego w urządzenie mobilne

- Mohamed Amine Bouazzouni, Emmanuel Conchon, Fabrice Peyrard, „*Trusted mobile computing: An overview of existing solutions*”, Future Generation Computer Systems 80 (2018) 596–612

- Q Zhang, JZ Qiao, QY Meng, *„Build a trusted storage system on a mobile phone”*, IET Information Security, 2018

## Ochrona informacji z wykorzystaniem mechanizmów systemu operacyjnego, dedykowanych aplikacji

- Jalaluddin Khan, Haider Abbas, Jalal Al-Muhtadi, *„Survey on Mobile User's Data Privacy Threats and Defense Mechanisms”*, Procedia Computer Science 56 (2015)

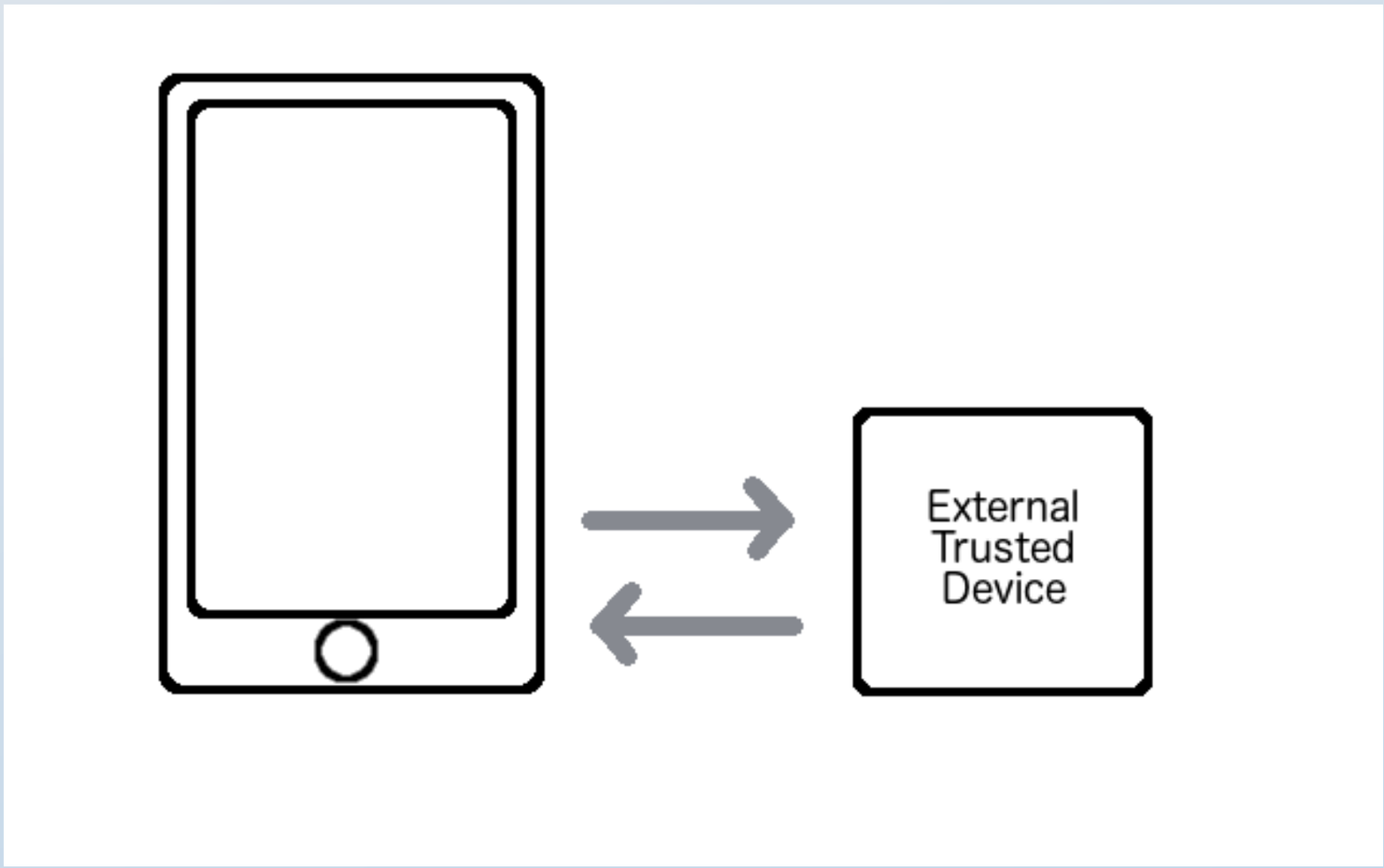
- Syed Farhan Alam Zaidi, Munam Ali Shah, Muhammad Kamran, Qaisar Javaid, Sijing Zhang *„A Survey on Security for Smartphone Device”*, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4 (2016)

# CELE ROZPRAWY DOKTORSKIEJ

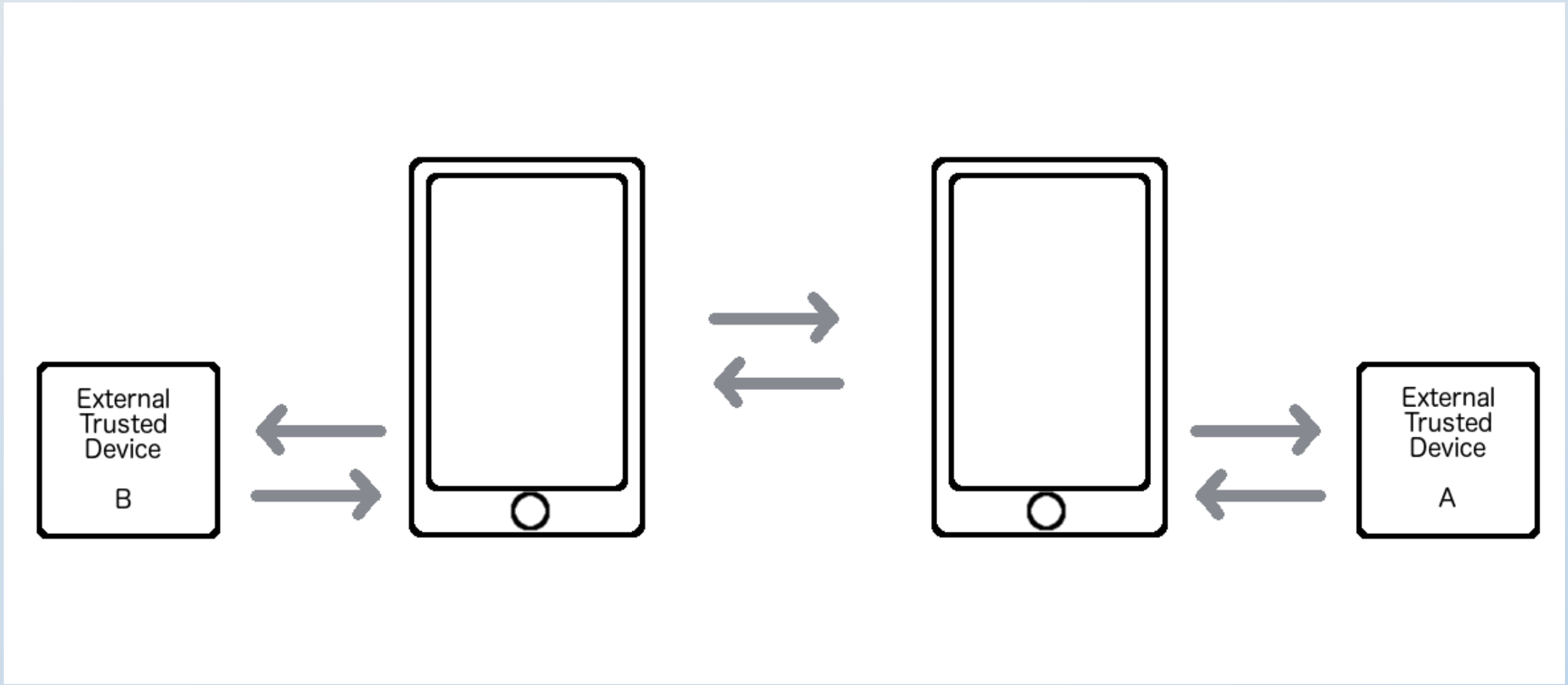
Opracowanie i weryfikacja skuteczności metody ochrony informacji dla platform mobilnych charakteryzującej się:

- brakiem podatności na ataki związane ze współdzielonymi komponentami sprzętowymi (klawiatura, ekran),
- brakiem podatności na ataki od środka oraz przez inną aplikację mobilną,
- brakiem ograniczeń funkcjonalnych dla użytkowników współczesnych platform mobilnych,
- selektywnym zastosowaniem dla wybranych sesji komunikacyjnych,
- neutralnością technologiczną z punktu widzenia systemu operacyjnego, modelu telefonu, stosowanej technologii sieci komórkowej.

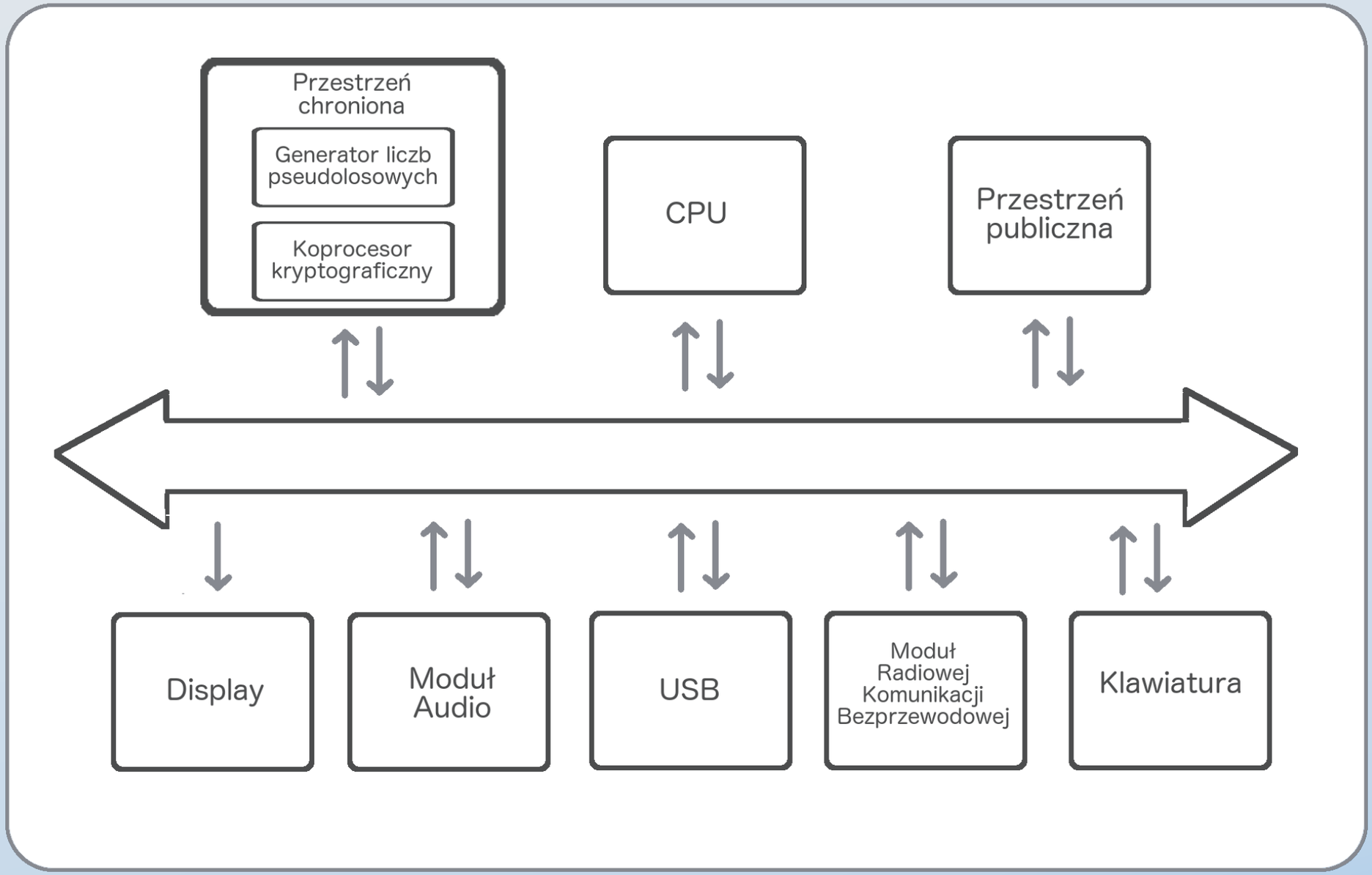
# ZEWNĘTRZNY KOMPONENT SPRZĘTOWY - EXTERNAL TRUSTED DEVICE (ETD)



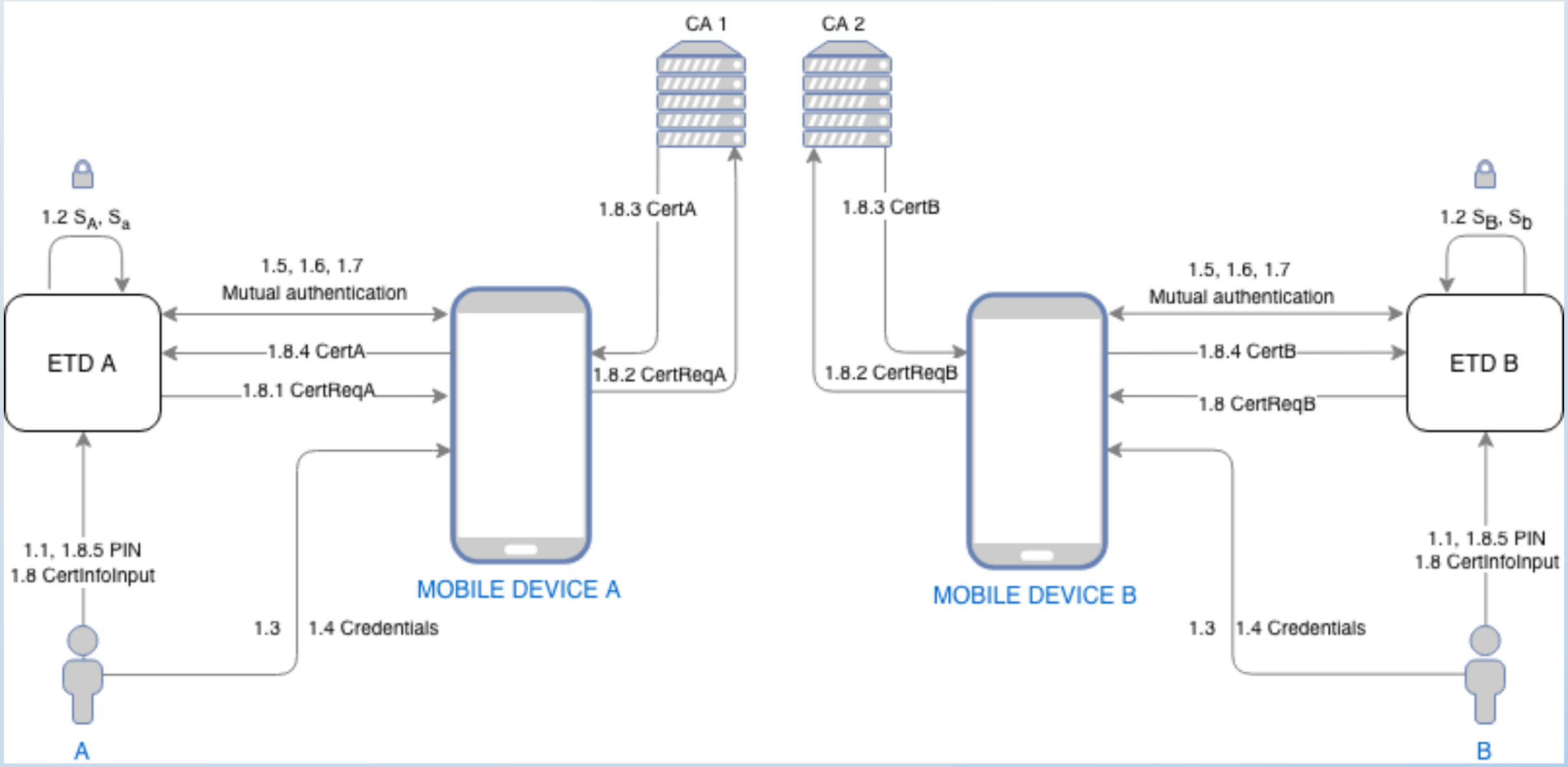
# IDEA METODY OCHRONY INFORMACJI WYKORZYSTUJĄCA MODUŁY ETD



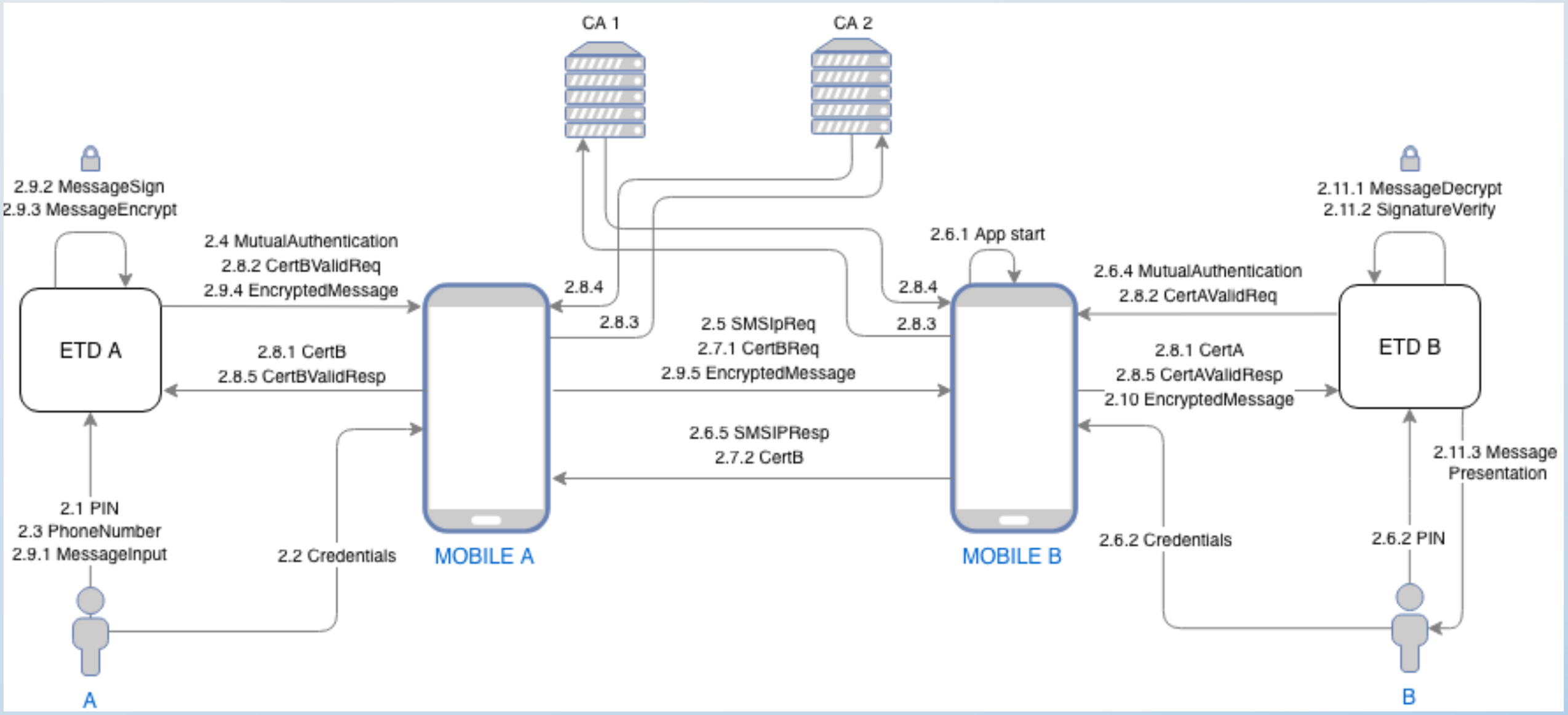
# SPECYFIKACJA TECHNOLOGICZNA – BUDOWA MODUŁU



# SEKWENCJA OPERACJI INICJALIZACJI MODUŁÓW ETD



# SEKWENCJA OPERACJI DO PRZESŁANIA ZAKODOWANEJ WIADOMOŚCI SMS



# WYKONANE PRACE BADAWCZE

- analiza zagrożeń oraz stosowanych metod ochrony we współczesnych systemach mobilnych

- opracowanie koncepcji metody ochrony informacji wykorzystująca zewnętrzny moduł sprzętowy ETD (klasy Embedded System)

- opracowanie architektury, przegląd oraz wybór komponentów do budowy prototypu modułu ETD

- szczegółowa specyfikacja protokołów inicjalizacji oraz komunikacji

# PUBLIKACJE

- G. Górski, M. Nowacki, *„Analiza zagrożeń bezpieczeństwa dla współczesnych platform mobilnych”*, Zeszyty Naukowe Wydziału Elektroniki i Informatyki Politechniki Koszalińskiej, Zeszyt: 13 str. 47-54, Koszalin 2018

- G. Górski, M. Nowacki, *„External Trusted Device (ETD) – zewnętrzny, mobilny moduł sprzętowy do uwierzytelniania i szyfrowania informacji w sieciach telefonii komórkowej*”, w przygotowaniu zgłoszenie do Urzędu Patentowego RP

# ZADANIA PLANOWANE DO WYKONANIA W TRAKCIE DALSZYCH BADAŃ

- symulacja programowa prototypu ETD z wykorzystaniem dwóch telefonów komórkowych
- budowa warstwy sprzętowej oraz napisanie oprogramowania wbudowanego dla zaprojektowanej architektury ETD
- opracowanie dedykowanych aplikacji mobilnych
- przygotowanie i przeprowadzenie testów penetracyjnych, ocena systemu pod kątem poziomu bezpieczeństwa (według zaleceń OWASP Top10) i wydajności w odniesieniu do wymagań stawianych przez usługi telekomunikacyjne (rozmowy telefoniczne, wideo-rozmowy, wiadomości SMS)
- publikacja wyników

# STRUKTURA PLANOWANEJ ROZPRAWY DOKTORSKIEJ

- analiza zagrożeń i podatności we współczesnych systemach mobilnych
- przegląd stosowanych metod ochrony
- charakterystyka proponowanej metody ochrony informacji wykorzystującej zewnętrzny moduł sprzętowy ETD
- opis architektury opracowanego modułu ETD, charakterystyka wybranych komponentów, budowa prototypu urządzenia
- prezentacja protokołów inicjalizacji oraz kodowanej sesji komunikacyjnej z wykorzystaniem modułu ETD
- przeprowadzenie testów penetracyjnych i testów wydajności
- analiza skuteczności opracowanej metody ochrony informacji dla platform mobilnych

Dziękuję za uwagę