ZAŁĄCZNIK NR 1

SZCZEGÓŁOWA SPECYFIKACJA TECHNICZNA I FUNKCJONALNA (STiF)
Prace przedwdrożeniowe w ramach projektu pn.: SCIENCE4BUSINESS – Zadanie nr 1 Inkubator Rozwoju

I. INFORMACJE OGÓLNE O PRZEDSIĘWZIĘCIU

1. Tytuł projektu / przedsięwzięcia: Prototyp terminala do rejestracji czasu pracy z wykorzystaniem biometrii i kart zbliżeniowych.

2. Zamawiający: Wyższa Szkoła Gospodarki w Bydgoszczy.

3. Cel prac przedwdrożeniowych: Opracowanie, wykonanie i przetestowanie działającego prototypu oprogramowania stacjonarnego terminala rejestracji czasu pracy (poziom gotowości technologicznej TRL 5). Celem prac jest stworzenie stabilnego rozwiązania integrującego bezdotykową identyfikację zbliżeniową (NFC/MIFARE 13,56 MHz) oraz identyfikację biometryczną (czytnik linii papilarnych) z zewnętrznym systemem RCP za pośrednictwem szyfrowanego interfejsu REST API.

II. SZCZEGÓŁOWY ZAKRES PRAC PRZEDWDROŻENIOWYCH

1. Opracowanie i modyfikacja rozwiązania:

Wykonanie natywnej aplikacji terminalowej dla systemu Android w języku Java (minimalna obsługiwana wersja: Android 10), przeznaczonej do uruchomienia na tablecie 10,1" o rozdzielczości 1200 × 1920 px zintegrowanym z modułem NFC oraz czytnikiem odcisku palca.

2. Wykonanie testów i prób laboratoryjnych:

Przeprowadzenie kompleksowej serii testów funkcjonalnych, wydajnościowych, bezpieczeństwa oraz użytkownika w siedzibie Zamawiającego (minimum 10 sesji po 8 godzin dydaktycznych/ zegarowych z udziałem Wykonawcy i Badacza wiodącego).

3. Dostosowanie rozwiązania do potrzeb Zamawiającego:

Zapewnienie pełnej komunikacji online z zewnętrznym systemem rejestracji czasu pracy, w tym realizacja dwuskładnikowej/hybrydowej autoryzacji, rejestracji zdarzeń pracowniczych oraz dedykowanego trybu administracyjnego chronionego PIN-em.

III. SPECYFIKACJA FUNKCJONALNA

1. Identyfikacja i autoryzacja użytkownika:

Terminal umożliwia identyfikację pracownika na dwa sposoby: za pomocą karty zbliżeniowej NFC/MIFARE 13,56 MHz lub za pomocą czytnika linii papilarnych. W przypadku identyfikacji

biometrycznej terminal pobiera dane ze skanera, generuje hash odcisku palca i przesyła go do zewnętrznego systemu RCP w celu porównania z hashem przypisanym do użytkownika. W przypadku karty zbliżeniowej do systemu przekazywany jest identyfikator karty. Wynikiem procesu jest jednoznaczna identyfikacja użytkownika albo informacja o braku autoryzacji.

2. Rejestracja zdarzeń czasu pracy:

Po prawidłowej identyfikacji użytkownika terminal umożliwia rejestrację czterech rodzajów zdarzeń: rozpoczęcie pracy, zakończenie pracy, rozpoczęcie przerwy i zakończenie przerwy. Zdarzenie wraz z identyfikatorem użytkownika i wymaganymi danymi jest przesyłane online do zewnętrznego systemu RCP przez REST API. Terminal prezentuje użytkownikowi czytelną informację o poprawnym zapisaniu albo błędzie operacji.

3. Tryb administracyjny i zarządzanie metodami identyfikacji:

Terminal posiada odrębny tryb administracyjny zabezpieczony kodem PIN. Po zalogowaniu administrator może pobrać z zewnętrznego systemu RCP listę użytkowników, wskazać wybranego użytkownika oraz przypisać mu kartę NFC/MIFARE lub zarejestrować odcisk palca. Dane identyfikacyjne są przekazywane do zewnętrznego systemu RCP za pośrednictwem REST API.

4. Komunikacja z zewnętrznym systemem RCP:

Terminal współpracuje z niezależnym zewnętrznym systemem rejestracji czasu pracy poprzez interfejs REST API. Komunikacja obejmuje co najmniej pobieranie użytkowników, rejestrację metod identyfikacji, identyfikację/autoryzację użytkownika oraz przesyłanie zdarzeń czasu pracy. Terminal działa w trybie online i wymaga aktywnego połączenia sieciowego przez Wi-Fi lub LTE. W przypadku braku komunikacji użytkownik otrzymuje informację o braku możliwości wykonania operacji.

IV. WYMAGANIA TECHNICZNE I PARAMETRY KONSTRUKCYJNE

Poniżej przedstawiono szczegółowe zestawienie wszystkich parametrów technicznych i gabarytowych. W myśl wytycznych specyfikacji, dla każdego parametru określono osobno wartość wymaganą, wartość docelową oraz przyjętą metodę weryfikacji:

1. Wydajność:

- **Wartość wymagana:** Identyfikacja użytkownika ≤ 2 s; reakcja interfejsu po wykonaniu operacji ≤ 1 s; obsługa odpowiedzi API w typowych warunkach sieciowych ≤ 3 s.
- **Wartość docelowa:** Spełnienie lub poprawa wartości wymaganych.
- **Metoda weryfikacji:** Testy pomiarowe w środowisku WSG.

2. Dokładność:

- **Wartość wymagana:** Poprawne przypisanie i przetwarzanie zdarzeń: 100% w scenariuszach testowych; skuteczność odczytu poprawnie zarejestrowanej karty NFC/MIFARE ≥ 99% w warunkach testowych.
- **Wartość docelowa:** ≥ wartości wymaganych.
- **Metoda weryfikacji:** Seria powtarzalnych testów funkcjonalnych.

3. Rozdzielczość:

- **Wartość wymagana:** Obsługa rozdzielczości urządzenia dostarczonego przez Zamawiającego.
- **Wartość docelowa:** 1200 × 1920 px FHD, ekran 10,1".
- **Metoda weryfikacji:** Uruchomienie aplikacji i ocena poprawności interfejsu.

4. Trwałość:

- **Wartość wymagana:** Nie dotyczy w zakresie mechanicznym; oprogramowanie powinno umożliwiać wielogodzinną pracę ciągłą.
- **Wartość docelowa:** Stabilna praca podczas min. 8-godzinnej sesji testowej.
- **Metoda weryfikacji:** Test ciągłej pracy.

5. Kompatybilność:

- **Wartość wymagana:** Nie dotyczy dla sprzętu; aplikacja powinna działać na Android 10 i nowszym.
- **Wartość docelowa:** Android ≥ 10.
- **Metoda weryfikacji:** Instalacja i test na urządzeniu docelowym.

6. Zużycie energii:

- **Wartość wymagana:** Brak dodatkowych wymagań poza możliwościami dostarczonego urządzenia.
- **Wartość docelowa:** Brak nieuzasadnionego ciągłego obciążenia CPU / wybudzania urządzenia.
- **Metoda weryfikacji:** Obserwacja działania podczas testów.

7. Odporność środowiskowa:

- **Wartość wymagana:** Przeznaczenie do użytkowania w pomieszczeniach wewnętrznych.
- **Wartość docelowa:** Stabilna praca w typowych warunkach biurowych.
- **Metoda weryfikacji:** Testy w siedzibie Wyższej Szkole Gospodarki w Bydgoszczy.

8. Niezawodność:

- **Wartość wymagana:** Brak awarii krytycznej aplikacji oraz brak niekontrolowanej utraty poprawnie potwierdzonych przez API zdarzeń podczas testów.
- **Wartość docelowa:** Stabilna praca w trakcie całego cyklu testowego.
- **Metoda weryfikacji:** Testy funkcjonalne i wielogodzinne sesje walidacyjne.

V. WYMAGANIA MATERIAŁOWE

1. Materiały konstrukcyjne: Nie dotyczy – prototyp wykorzystuje gotowe urządzenie dostarczone przez Zamawiającego. Przedmiotem prac wykonawcy nie jest projektowanie ani wykonanie obudowy lub elementów konstrukcyjnych terminala.

VI. WYMAGANIA DLA OPROGRAMOWANIA

1. Architektura systemu: Natywna aplikacja terminalowa dla systemu Android, działająca na urządzeniu dostarczonym przez Zamawiającego. Oprogramowanie powinno posiadać modularną strukturę rozdzielającą co najmniej warstwę interfejsu użytkownika, logikę obsługi zdarzeń, obsługę urządzeń identyfikacyjnych oraz komunikację z zewnętrznym REST API. System zewnętrzny pozostaje niezależny od terminala i stanowi źródło danych o użytkownikach oraz miejsce rejestracji zdarzeń i danych identyfikacyjnych.

2. Język programowania: Java. Minimalna obsługiwana wersja systemu: Android 10. Niedopuszczalne jest wykonanie podstawowej części aplikacji w języku Kotlin.

3. Baza danych: Terminal nie powinien posiadać niezależnej, nadrzędnej bazy użytkowników ani zdarzeń RCP. Dane użytkowników pobierane są z zewnętrznego systemu przez REST API. Dane identyfikacyjne użytkowników, w tym identyfikatory kart oraz hashe danych biometrycznych, są przechowywane w systemie zewnętrznym. Dopuszcza się lokalne przechowywanie wyłącznie danych konfiguracyjnych niezbędnych do działania aplikacji.

4. Interfejs użytkownika: Interfejs dotykowy przeznaczony do pracy na ekranie 10,1" o rozdzielczości 1200 × 1920 px. Interfejs powinien być czytelny, uproszczony i dostosowany do szybkiej obsługi terminala stacjonarnego. Podstawowe akcje użytkownika: rozpoczęcie pracy, zakończenie pracy, rozpoczęcie przerwy i zakończenie przerwy. System powinien jednoznacznie prezentować potwierdzenie wykonania operacji, błąd identyfikacji, błąd komunikacji oraz inne komunikaty wymagające reakcji użytkownika.

5. Integracje: Integracja z czytnikiem NFC/MIFARE 13,56 MHz, czytnikiem linii papilarnych oraz zewnętrznym systemem RCP. Integracja sprzętowa powinna wykorzystywać interfejsy i biblioteki/SDK udostępnione dla dostarczonego urządzenia.

6. API oraz protokoły: Komunikacja z systemem zewnętrznym przez REST API z wykorzystaniem HTTP/HTTPS oraz danych w formacie JSON. Zakres integracji powinien obejmować co najmniej:

pobieranie listy użytkowników, przypisywanie karty użytkownikowi, rejestrację danych biometrycznych użytkownika, identyfikację/autoryzację użytkownika oraz rejestrację zdarzeń czasu pracy. Konkretne adresy endpointów i struktury danych zostaną dostosowane do dokumentacji API systemu integracyjnego przekazanej wykonawcy.

7. Cyberbezpieczeństwo: Komunikacja z systemem zewnętrznym powinna być realizowana z wykorzystaniem szyfrowanego połączenia HTTPS, o ile jest ono dostępne po stronie systemu integracyjnego. Aplikacja nie może zapisywać obrazu odcisku palca ani umieszczać danych uwierzytelniających i biometrycznych w logach diagnostycznych. Dostęp do funkcji administracyjnych musi być zabezpieczony kodem PIN. Konfiguracja aplikacji nie może być dostępna dla zwykłego użytkownika terminala.

8. Mechanizmy autoryzacji: Użytkownik terminala identyfikowany jest za pomocą karty NFC/MIFARE lub odcisku palca. W przypadku odcisku terminal generuje hash danych biometrycznych i przesyła go do zewnętrznego systemu w celu porównania. Administrator uzyskuje dostęp do oddzielnego trybu administracyjnego po podaniu poprawnego kodu PIN.

9. Kopie zapasowe: Nie dotyczy dla danych biznesowych – terminal nie stanowi nadrzędnego repozytorium danych użytkowników ani ewidencji czasu pracy. Dane te są przechowywane w systemie zewnętrznym. Kod źródłowy i finalna wersja oprogramowania są przekazywane Zamawiającemu.

10. Wymogi wydajnościowe: Czas identyfikacji użytkownika w typowych warunkach: do 2 sekund. Reakcja lokalnego interfejsu: do 1 sekundy. Zakończenie operacji wymagającej komunikacji z REST API: docelowo do 3 sekund przy prawidłowo działającym połączeniu sieciowym i prawidłowo odpowiadającym systemie zewnętrznym.

11. Wymogi skalowalności: Oprogramowanie powinno umożliwiać współpracę z zewnętrznym systemem zawierającym minimum 1000 użytkowników. Architektura aplikacji powinna umożliwiać rozszerzenie w przyszłości o kolejne typy zdarzeń i sposoby identyfikacji bez konieczności przebudowy podstawowych mechanizmów komunikacyjnych.

VII. INTEGRACJE I INTEROPERACYJNOŚĆ

1. Systemy współpracujące: Niezależny zewnętrzny system rejestracji czasu pracy udostępniający REST API. Prototyp nie może być na stałe powiązany z nazwą ani produktem jednego dostawcy systemu RCP.

2. Standardy wymiany danych: REST, JSON.

3. Protokoły komunikacyjne: HTTP/HTTPS; połączenie z Internetem przez Wi-Fi lub LTE.

4. Integracja sprzętowa: Czytnik linii papilarnych oraz czytnik NFC/MIFARE 13,56 MHz w urządzeniu dostarczonym przez Zamawiającego. Integracja za pomocą dostępnych interfejsów systemowych lub SDK producenta urządzenia.

5. Integracja programowa: Integracja aplikacji Android z zewnętrznym REST API oraz bibliotekami/SDK modułów identyfikacyjnych.

6. Wymagane interfejsy: Interfejs REST API systemu RCP, interfejs czytnika NFC/MIFARE, interfejs/SDK czytnika linii papilarnych, połączenie Wi-Fi i LTE.

VIII. WYMAGANIA DOTYCZĄCE PROTOTYPU

1. Liczba prototypów: 1 funkcjonalny prototyp oprogramowania terminala uruchomiony na urządzeniu dostarczonym przez Zamawiającego.

2. Technologia wykonania: Natywna aplikacja Android wykonana w języku Java, minimalna wersja Android 10, uruchomiona na dostarczonym tablecie 10,1", 1200 × 1920 px, wyposażonym w czytnik NFC/MIFARE oraz linii papilarnych.

3. Oczekiwane wyniki: Działający prototyp terminala umożliwiający identyfikację użytkownika kartą lub odciskiem palca, komunikację z zewnętrznym REST API oraz rejestrację przewidzianych zdarzeń czasu pracy.

4. Zakres funkcjonalny: Identyfikacja kartą NFC/MIFARE; identyfikacja biometryczna; tryb administracyjny PIN; pobieranie użytkowników z API; przypisywanie metod identyfikacji; rozpoczęcie i zakończenie pracy; rozpoczęcie i zakończenie przerwy; komunikacja online z zewnętrznym systemem RCP.

5. Stopień odwzorowania produktu końcowego (TRL): TRL 5 – działający prototyp poddany walidacji w środowisku zbliżonym do rzeczywistych.

6. Możliwość dalszej rozbudowy: Architektura powinna umożliwiać dalszą rozbudowę m.in. o kolejne rodzaje zdarzeń, dodatkowe systemy RCP, inne sposoby identyfikacji oraz dodatkowe funkcje terminala bez konieczności całkowitej przebudowy aplikacji.

IX. TESTY, WALIDACJA I KRYTERIA AKCEPTACJI

Poniżej przedstawiono opis wymagań testowych i walidacyjnych w pełnej formie opisowej bez ujęcia tabelarycznego:

1. Testy funkcjonalne (Wymagane):

Test wszystkich funkcji identyfikacji, administracji i ewidencji zdarzeń. Kryteria akceptacji: poprawne wykonanie wszystkich zatwierdzonych scenariuszy testowych, brak błędów krytycznych.

2. Testy wydajnościowe (Wymagane):

Pomiar czasu identyfikacji, reakcji interfejsu i wykonania operacji przez API. Kryteria akceptacji: identyfikacja ≤ 2 s, reakcja interfejsu ≤ 1 s, wykonanie operacji online docelowo ≤ 3 s przy prawidłowym działaniu API i sieci.

3. Testy bezpieczeństwa (Wymagane):

Podstawowa weryfikacja zabezpieczenia trybu administracyjnego, komunikacji sieciowej oraz sposobu obsługi danych identyfikacyjnych. Kryteria akceptacji: brak dostępu do trybu administracyjnego bez PIN; brak zapisywania obrazu odcisku; brak danych biometrycznych lub uwierzytelniających w logach aplikacji.

5. Testy użytkownika (Wymagane):

Testy wykonywane w siedzibie Wyższej Szkoły Gospodarki w Bydgoszczy w warunkach odpowiadających przewidywanemu sposobowi użytkowania terminala. Wykonawca aktywnie uczestniczy w procesie prototypowania i testowania – minimum 10 spotkań po 8 godzin w siedzibie Zamawiającego. Kryteria akceptacji: zrealizowanie min. 10 sesji × 8 h, usunięcie błędów krytycznych ujawnionych podczas testów i akceptacja końcowej wersji przez Badacza wiodącego.

6. Testy inne (Wymagane):

Testy integracyjne czytnika linii papilarnych, NFC/MIFARE i REST API oraz testy obsługi błędów systemu zewnętrznego i braku połączenia sieciowego. Kryteria akceptacji: poprawne działanie integracji i prawidłowa prezentacja komunikatów błędów.

7. Walidacja (Wymagane):

Walidacja prototypu w siedzibie Wyższej Szkoły Gospodarki w Bydgoszczy w środowisku zbliżonym do rzeczywistych. Kryteria akceptacji: potwierdzenie działania kluczowych funkcji i osiągnięcia poziomu TRL 5.

X. ODBIÓR PROTOTYPU I KRYTERIA AKCEPTACJI

1. Realizacja wymaganego zakresu funkcjonalnego:

- Sposób weryfikacji: przeprowadzenie scenariuszy testowych przez badacza wiodącego na dostarczonym prototypie.
- Kryteria akceptacji: poprawna identyfikacja kartą i odciskiem palca, obsługa trybu administracyjnego oraz rejestracja rozpoczęcia/zakończenia pracy i rozpoczęcia/zakończenia przerwy.

2. Poprawność integracji sprzętowej i programowej:

- Sposób weryfikacji: test czytnika NFC/MIFARE, czytnika linii papilarnych, Wi-Fi/LTE i komunikacji z zewnętrznym REST API.
- Kryteria akceptacji: wszystkie wymagane komponenty współpracują z aplikacją; terminal prawidłowo pobiera użytkowników, przekazuje dane identyfikacyjne i rejestruje zdarzenia w systemie zewnętrznym.

3. Kompletność i stabilność prototypu: Sposób weryfikacji: Testy w siedzibie WSG, kontrola dostarczonego kodu źródłowego i dokumentacji. Kryteria akceptacji: Brak błędów krytycznych uniemożliwiających korzystanie z podstawowych funkcji, przeprowadzenie min. 10 × 8 h sesji prototypowania/testów oraz przekazanie kompletnego kodu źródłowego i wymaganej dokumentacji.

XI. DOKUMENTACJA WYMAGANA OD WYKONAWCY

1. Dokumentacja techniczna: zwięzły opis architektury wykonanej aplikacji, sposobu konfiguracji, kompilacji i uruchomienia oraz integracji z czytnikiem NFC, czytnikiem linii papilarnych i systemem zewnętrznym.

2. Instrukcja użytkowania: NIE jako osobny dokument. Podstawowy opis obsługi użytkownika i trybu administracyjnego należy umieścić w dokumentacji technicznej.

3. Kod źródłowy: kompletny kod źródłowy aplikacji wraz z plikami projektu, konfiguracją procesu budowania oraz wszystkimi elementami niezbędnymi do samodzielnego skompilowania i dalszego rozwijania oprogramowania przez Wyższą Szkołę Gospodarki w Bydgoszczy.

4. Dokumentacja API: dokumentacja zakresu komunikacji aplikacji terminalowej z zewnętrznym REST API: wykorzystywane operacje, struktury żądań i odpowiedzi, sposób uwierzytelnienia oraz obsługa błędów. Nie jest wymagane dokumentowanie całego zewnętrznego systemu RCP.

XII. OCZEKIWANE ZASADY 6R

Przedstawienie opisowe wymagań środowiskowych i ekologicznych zgodnych z koncepcją 6R:

1. Rethink (Przemyśl na nowo): Projektowanie rozwiązania jako jednego zintegrowanego terminala łączącego identyfikację NFC, biometrię i komunikację cyfrową z systemem zewnętrznym, przy ograniczeniu zbędnych funkcji na etapie prototypowania. Wykorzystanie istniejącego urządzenia dostarczonego przez Zamawiającego zamiast projektowania i wytwarzania nowej platformy sprzętowej. Architektura oprogramowania powinna umożliwiać dalszy rozwój bez konieczności wymiany urządzenia.

2. Reduce (Ogranicz): Minimalizacja zużycia materiałów i energii. Rozwiązanie wspiera cyfrową ewidencję czasu pracy i ograniczenie papierowych list obecności oraz ręcznego obiegu. Brak dodatkowych urządzeń pomocniczych – wykorzystanie jednego istniejącego terminala.