



POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

Wydział Informatyki

Filia w Gdańsku

Bartosz Bohatyrewicz

Nr albumu s26860

Nazwa specjalizacji: Sztuczna Inteligencja

Łukasz Korycki

Nr albumu s26972

Nazwa specjalizacji: Cyberbezpieczeństwo

Kamil Maliński

Nr albumu s26984

Nazwa specjalizacji: Cyberbezpieczeństwo

Jan Szydłowski

Nr albumu s26978

Nazwa specjalizacji: Cyberbezpieczeństwo

Igor Wojciechowski

Nr albumu s27106

Nazwa specjalizacji: Aplikacje Internetowe

Wdrożenie systemu cyfrowych kluczy do budynku uczelni

Rodzaj pracy

inżynierska

Imię i nazwisko promotora

dr hab. Marek Bednarczyk

Gdańsk, Marzec, 2026

Streszczenie: Celem projektu inżynierskiego jest stworzenie modułu integrującego system zarządzania dostępem "Cyfrowe Klucze" z systemem uczelnianym PJATK. Moduł ten będzie odpowiedzialny za pobieranie danych z planu zajęć oraz wspomaganie zarządzania dostępem do pomieszczeń na podstawie tych danych. Projekt obejmuje również stworzenie aplikacji webowej dla administracji, dziekanatu oraz ochrony, umożliwiającej łatwe zarządzanie uprawnieniami dostępu oraz generowanie raportów na podstawie danych z systemu "Cyfrowe Klucze". Ostatecznym celem jest zwiększenie efektywności zarządzania dostępem do pomieszczeń uczelnianych oraz poprawa bezpieczeństwa poprzez automatyzację procesu przydzielania uprawnień.

Słowa kluczowe: czytniki, systemy kontroli dostępu, bezpieczeństwo, karty [RFID](#), integracja systemów



POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

Karta projektu

Temat projektu: Wdrożenie systemu cyfrowych kluczy do budynku uczelni Temat projektu po angielsku: Implementation of a digital key system in a university building	Akronim: EkeyPJATK Data ustalenia tematu 2025-04-01
Promotor: dr hab. Marek Bednarczyk	Konsultanci: 1. Antoni Ulenberg
Cele projektu: Integracja oryginalnego systemu: "Cyfrowe Klucze" z systemem uczelnianym PJATK, wraz z ulepszeniem stworzonych wcześniej rozwiązań.	
Rezultaty projektu: Moduł pobierający i przekazujący dane z systemu uczelnianego PJATK do systemu "Cyfrowe Klucze", wraz z dokumentacją techniczną i użytkową. Aplikacja webowa dla administracji, dziekanatu oraz ochrony. Przekazywanie danych z planu zajęć, wspomaganie zarządzania dostępem do pomieszczeń uczelnianych, dla systemu "Cyfrowe Klucze" na podstawie planu zajęć.	
Miary sukcesu: Integracja systemu "Cyfrowe Klucze" z systemem uczelnianym PJATK, umożliwiającą automatyczne zarządzanie dostępem do pomieszczeń na podstawie planu zajęć.	
Ograniczenia: Współpraca z istniejącym systemem uczelnianym PJATK. Wiele osób pośrednich wymaganych do realizacji projektu.	

Wykonawcy	Numer albumu	Specjalizacja	Tryb studiów
Bartosz Bohatyrewicz	s26860	Sztuczna Inteligencja	Stacjonarny
Łukasz Korycki	s26972	Cyberbezpieczeństwo	Stacjonarny
Kamil Maliński	s26984	Cyberbezpieczeństwo	Stacjonarny
Jan Szydłowski	s26978	Cyberbezpieczeństwo	Stacjonarny
Igor Wojciechowski	s27106	Aplikacje Internetowe	Stacjonarny

Data ukończenia projektu: 20 października 2025	Recenzent: —TBA—
--	----------------------------

Spis treści

1	Wstęp	3
2	Słownik pojęć	4
3	Opis problemu	6
3.1	Analiza aktualnych rozwiązań	6
3.2	Analiza oryginalnego projektu "Cyfrowe Klucze"	6
3.3	Analiza konkurencji	7

Rozdział 1

Wstęp

Dokument opisuje stworzenie system weryfikacji uprawnień według rezerwacji z planu zajęć gotowego do wdrożenia. EkeyPJATK nie jest bezpośrednią kontynuacją projektu "Cyfrowe Klucze". System został zaprojektowany z myślą o bezpośredniej współpracy z działającym już systemem na terenie uczelni.

System EkeyPJATK jako uzupełnienie istniejącego już systemu wprowadza weryfikację uprawnień według rezerwacji z planu zajęć. Ze względu na prototypowy charakter oryginalnego projektu, nasz zespół był również odpowiedzialny za odświeżenie paneli zarządzania dla Ochrony, Dziekanatu i Administracji oraz stworzenia nowej wersji modułu zamka.

Rozdział 2

Słownik pojęć

Pojęcia

API Interfejs programistyczny aplikacji; umożliwia komunikację pomiędzy modulem raportowym a panelami użytkowników oraz systemem kontroli dostępu.

Cyfrowe Klucze System kontroli dostępu do sal na kampusie uniwersyteckim zbudowany przez zespół Antoniego Ulenberga, Marka Kudły i Kingi Marszałkowskiej.

Czytnik RFID Urządzenie służące do odczytu kart identyfikacyjnych na podstawie fal radiowych, wykorzystywane w systemie EkeyPJATK do kontroli dostępu.

EkeyPJATK System zarządzania dostępem oparty na cyfrowych kluczach, zintegrowany z systemem uczelnianym PJATK.

Elektrozawora Urządzenie służące do mechanicznego blokowania i odblokowywania drzwi w systemie kontroli dostępu.

GAKKO System zarządzania uczelnią, z którego pobierane są dane dotyczące planu zajęć i uprawnień dostępu.

Karta magnetyczna Nośnik identyfikacyjny wykorzystywany przez studentów, wykładowców i gości do autoryzacji dostępu do pomieszczeń uczelni.

MamaJana czy ktoś to w ogóle czyta?

Moduł zamka Element systemu kontroli dostępu odpowiedzialny za fizyczne odblokowywanie drzwi na podstawie weryfikacji uprawnień.

REST API Interfejs programistyczny oparty na architekturze REST, umożliwiający komunikację między modulem integracyjnym a systemem GAKKO.

TataBartka też się nad tym zastaniawiam

UI Interfejs użytkownika; graficzne środowisko umożliwiające interakcję z aplikacją webową.

WebSocket Protokół komunikacyjny umożliwiający dwukierunkową komunikację w czasie rzeczywistym między klientem a serwerem.

Akronimy

BSS Baza Sprzętowo-Systemowa

POE Power over Ethernet

RFID Radio-Frequency Identification

Rozdział 3

Opis problemu

3.1 Analiza aktualnych rozwiązań

Aktualnie uczelnia powierza wydawanie odpowiednich kluczy do sal ochronie. Osoba chcąc dostęp do danej sali musi się wpisać do dziennika. Jeżeli następna osoba chce mieć dostęp do tej sali, to klucz zwykle jest przekazywany, co nie jest oczywiście zapisywane w dzienniku. Przez co dziennik nie jest realnym odwzorowaniem kto jest w jakiej sali.

Dziennik przez to nie może stanowić podstawy dla Dziekanatu, który musi wiedzieć czy dane zajęcia zostały odbyte.

Administracja budynku pomimo swoich ogólnych uprawnień, nie ma ułatwionego sposobu do sal. Muszą jak reszta brać klucze od ochrony lub wziąć go od osoby która ostanio go miała.

3.2 Analiza oryginalnego projektu "Cyfrowe Klucze"

Przez istniejące problemy aktualnego rozwiązania, zespół Antoniego Ulenberga, Marka Kudły i Kingi Marszałkowskiej zwanego "Cyfrowe Klucze" zdecydował o stworzeniu prototypu systemu weryfikacji uprawnień przy pomocy czytników zamontowanych na ścianach przy salach oraz kart identyfikacyjnych. Po wielu konsultacjach z głównymi grupami użytkowników potencjalnego nowego systemu, zdecydowali o stworzeniu modularnego systemu.

System został podzielony na parę submodułów, system zarządzania dla administracji i ochrony, moduł sprzętowy, bazę danych, [API](#) autoryzacji użytkowników i

[API GAKKO](#). Podczas ich pracy zdecydowali o porzuceniu planu z integracją z [GAKKO](#), na rzecz przedstawienia całokształtu prototypu ówego systemu.

3.3 Analiza konkurencji

Ze względu na specyfikę systemu, nie ma bezpośredniej konkurencji dla naszego projektu, natomiast istnieją firmy oferujące usługi wprowadzenia systemów rezerwacji sal konferencyjnych.