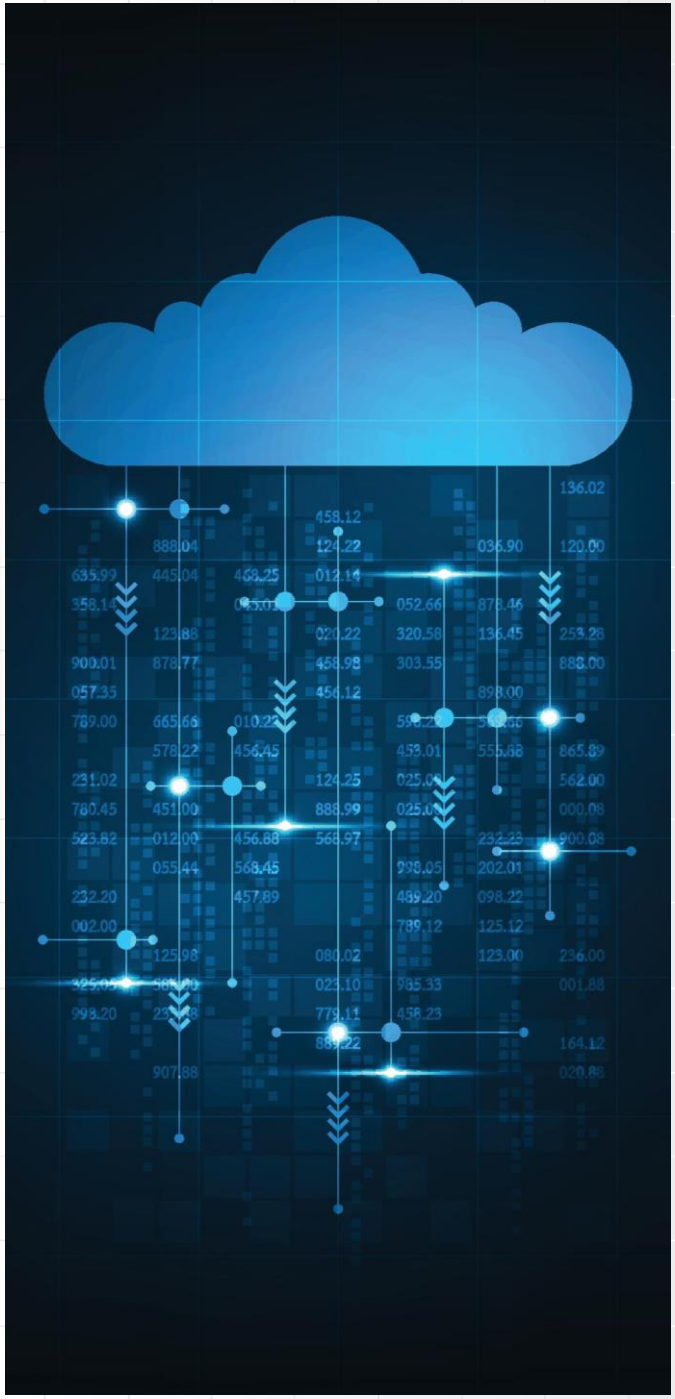


Programowanie w chmurze

Rafał Palak

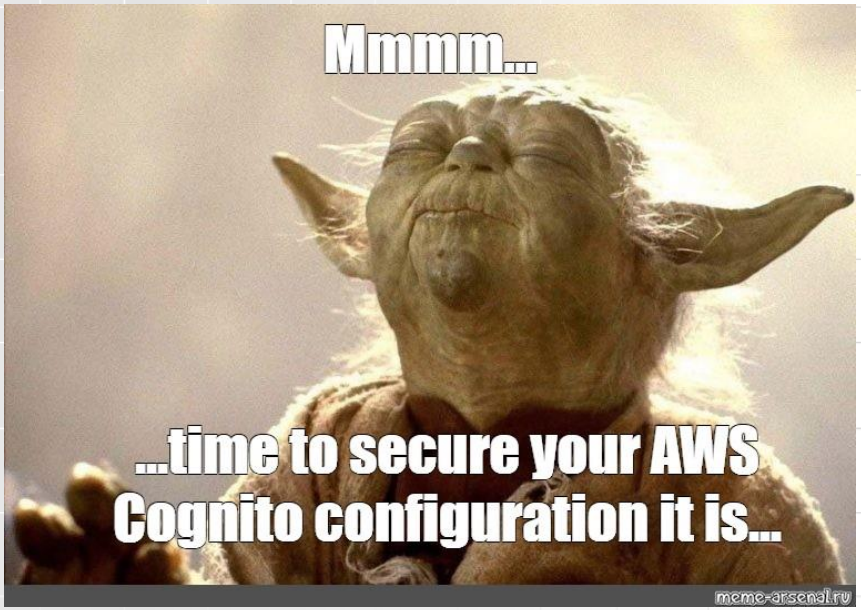
Politechnika Wrocławska

Wrocław
University
of Science
and Technology

AWS Cognito

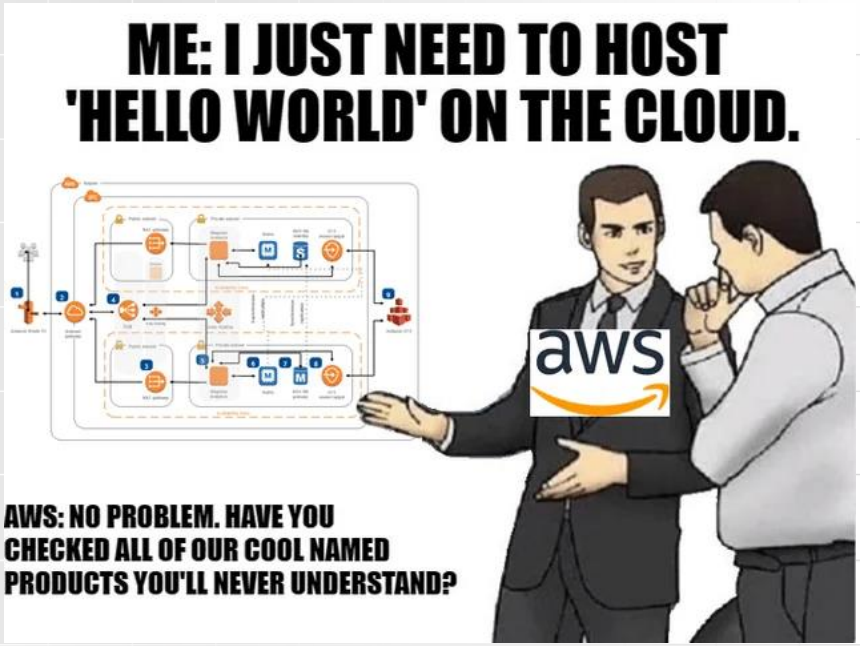
AWS Cognito [1]

- Usługa **zarządzania tożsamościami i dostępem do danych użytkowników**
- Zapewnia **rozwiązania** dla **aplikacji webowych** i **mobilnych**, umożliwiając bezpieczne dodawanie **funkcji logowania**, **rejestracji** oraz **zarządzania tożsamościami** użytkowników.
- **Umożliwia dostosowywanie procesów logowania i rejestracji**, w tym dodawanie własnych walidacji i logiki.
- Pozwala na **autentykację użytkowników poprzez zewnętrznych dostawców tożsamości**, takich jak Google, Facebook, Amazon oraz przez dostawców korzystających z protokołów OpenID Connect i SAML.
- Obsługuje **logowanie za pomocą nazwy użytkownika i hasła**, **logowanie przez zewnętrznych dostawców tożsamości** oraz inne opcje.



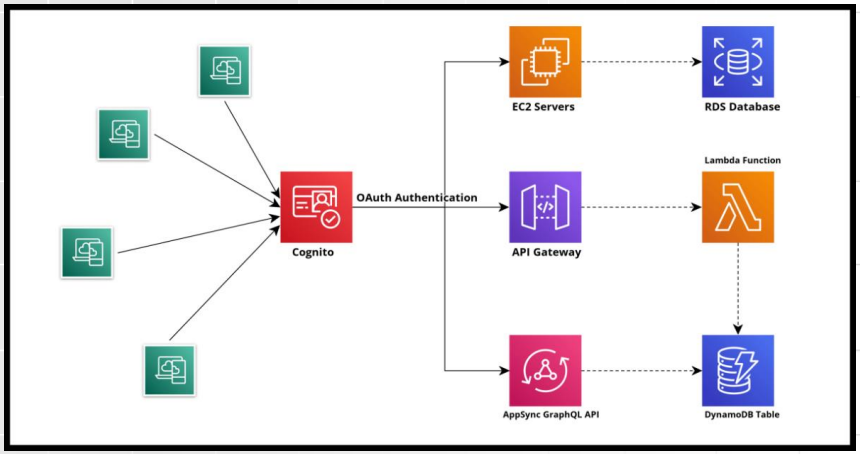
AWS Cognito [2]

- **Wspiera MFA** (Wieloskładnikowe uwierzytelnianie), co zwiększa bezpieczeństwo poprzez wymaganie dodatkowej formy weryfikacji użytkownika podczas logowania.
- Jest zaprojektowane tak, aby **łatwo skalować się w miarę rosnącej liczby użytkowników** aplikacji, co jest istotne dla rosnących firm i aplikacji.
- Oferuje **bogaty zestaw SDK i API**, które ułatwiają integrację z różnymi platformami programistycznymi i aplikacjami.



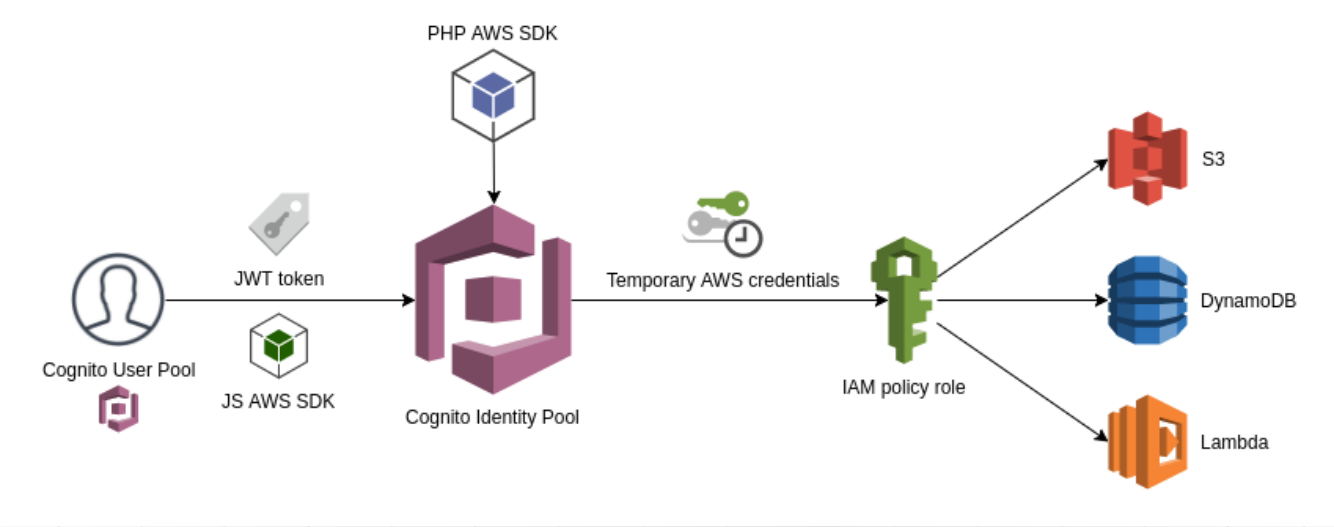
AWS Cognito – dlaczego?

- **Uproszczenie procesu tworzenia, zarządzania i personalizacji profili użytkowników** z automatycznymi funkcjami zarządzania cyklem życia użytkownika.
- **Elastyczne i skalowalne rozwiązania uwierzytelniające**, które mogą obsługiwać od kilku do milionów użytkowników bez konieczności ręcznego zwiększania zasobów.
- **Wsparcie dla wielu dostawców tożsamości** przy **minimalnym nakładzie** kodowania i konfiguracji.
- Oferuje wysokie bezpieczeństwo danych użytownika poprzez **szyfrowanie danych w spoczynku** i **w tranzycie**, **opcje wieloskładnikowego uwierzytelniania** (MFA), i zgodność z międzynarodowymi standardami bezpieczeństwa.



AWS Cognito – dlaczego?

- Pomaga w **utrzymaniu zgodności z przepisami dotyczącymi danych**, dzięki wbudowanym funkcjom bezpieczeństwa i prywatności.
- Umożliwia **tworzenie zaawansowanych profili użytkowników**, które umożliwiają personalizację i lepszą interakcję z aplikacją.

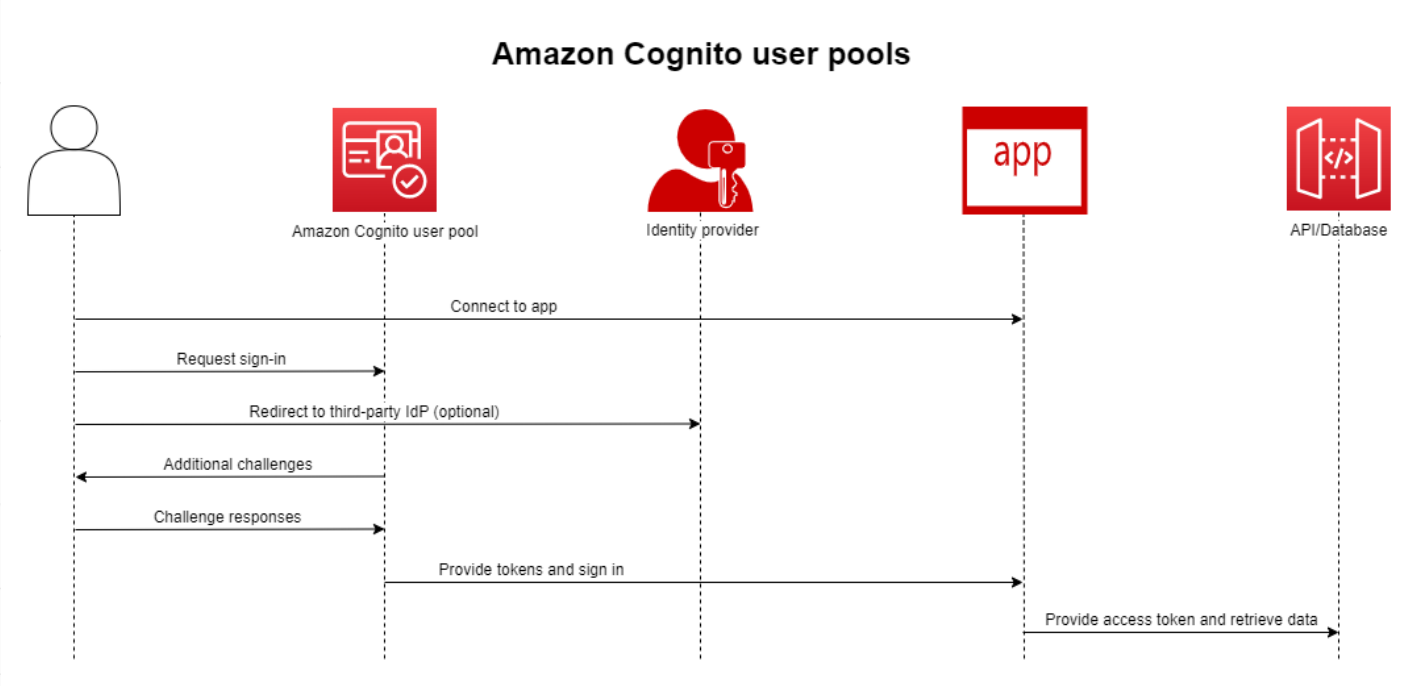


Wrocław
University
of Science
and Technology

AWS Cognito - Główne komponenty

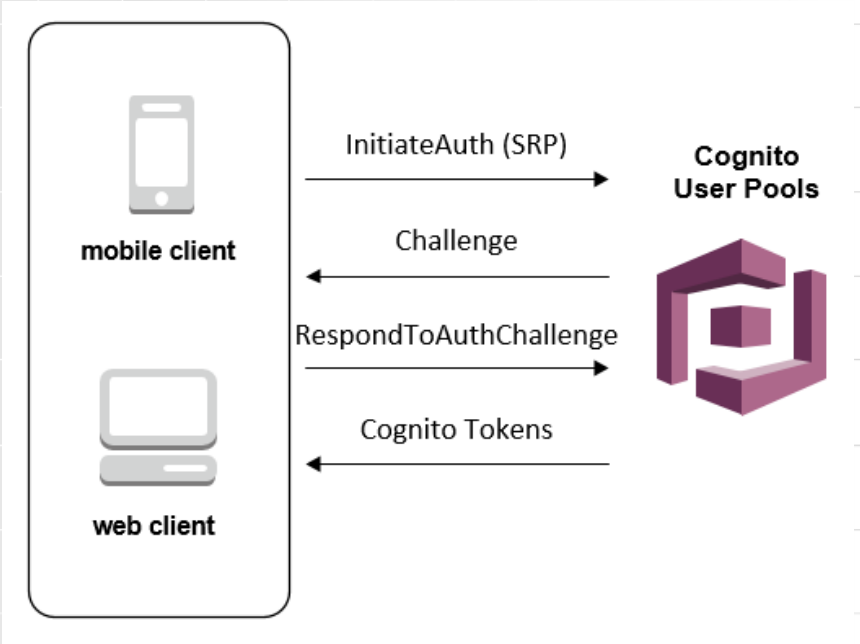
User Pools

- Jedna z **dwóch głównych funkcji oferowanych przez AWS Cognito**, służąca do zarządzania katalogiem użytkowników i obsługi ich uwierzytelniania w aplikacjach mobilnych i internetowych.



User Pools - główne cechy i funkcje

- Umożliwiają **tworzenie własnych katalogów użytkowników**.
- Umożliwiają **rejestrację**, **logowanie** i **zarządzanie profilami** użytkowników.
- Obsługują **różne metody uwierzytelniania**, w tym z użyciem **nazwy użytkownika i hasła** oraz **uwierzytelnianie za pomocą mediów społecznościowych** (Facebook, Google, Amazon).
- Pozwala **definiować role** i **oparte na nich uprawnienia dostępu**, wykorzystując AWS IAM (Identity and Access Management) do zarządzania tym, jakie zasoby są dostępne dla poszczególnych użytkowników.

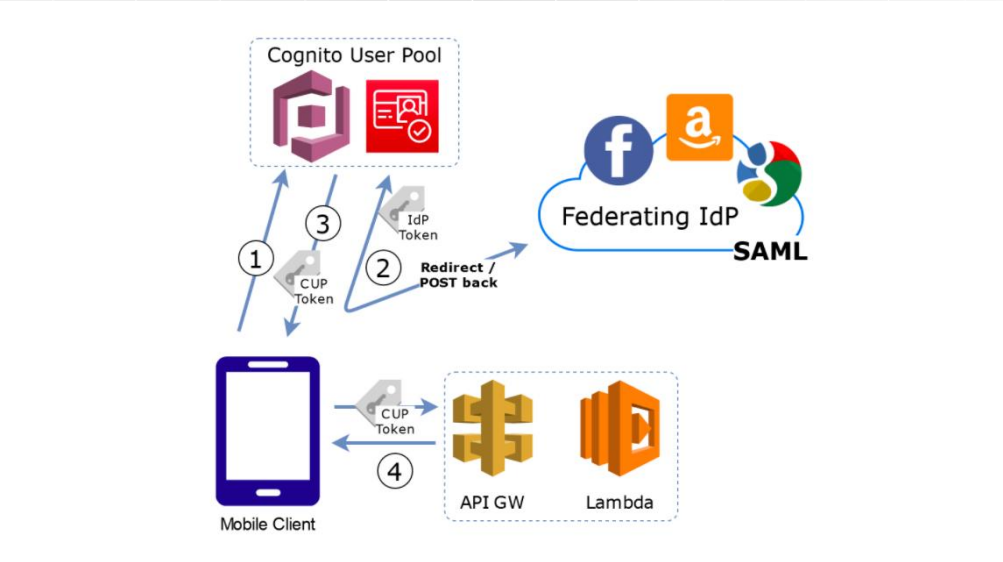


User Pools - zabezpieczenia

- Pozwala na **dodanie dodatkowej warstwy bezpieczeństwa** poprzez wymaganie drugiego czynnika uwierzytelnienia, np. SMS.
- Umożliwia określenie **wymagań dotyczących siły haseł**.
- **Pozwala na automatyczne blokowanie prób logowania** po przekroczeniu określonej liczby nieudanych prób.

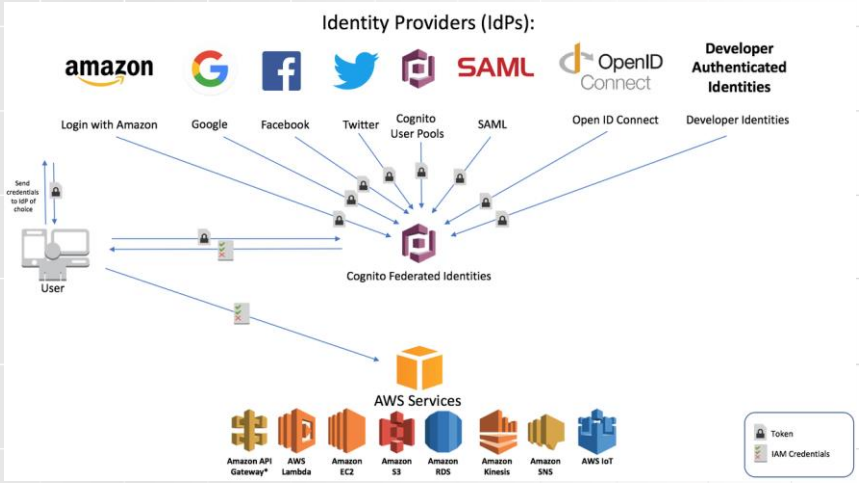
User Pools - personalizacja

- **Umożlwia personalizacje stron logowania** i **rejestracji**,
- User Pools można **integrować z AWS Lambda**, co pozwala na **uruchamianie niestandardowego kodu w odpowiedzi na różne zdarzenia** związane z cyklem życia użytkownika, np. przy rejestracji, potwierdzeniu użytkownika czy zmianie hasła.



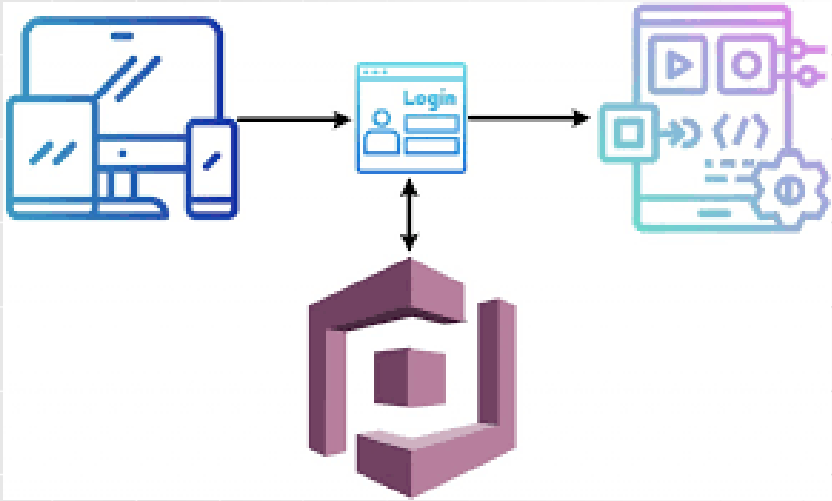
Identity Pools

- Znane również jako Federated Identity Pools
- Umożliwiają **zarządzanie tożsamościami użytkowników** i **udzielanie im dostępu do innych usług AWS**.
- Umożliwiają **integrację z różnymi dostawcami tożsamości** (np. Google, Facebook, Amazon, Apple) oraz **z własnymi systemami uwierzytelniania** poprzez SAML lub OpenID Connect.
- Wykorzystują **role IAM do nadawania uprawnień użytkownikom na podstawie ich tożsamości**. Użytkownicy otrzymują **tymczasowy dostęp do zasobów AWS** w oparciu o te role.
- **Możliwość implementacji własnych mechanizmów uwierzytelniania przez AWS** Lambda, co pozwala na tworzenie niestandardowych rozwiązań uwierzytelniających.



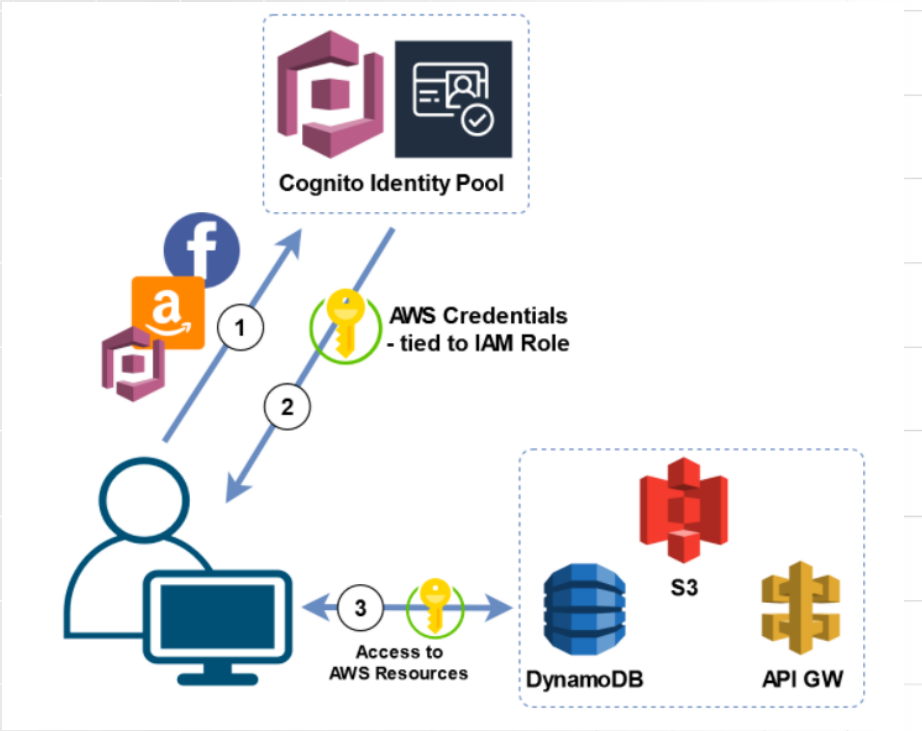
Identity Pools - zarządzanie dostępem

- **Role Based Access Control** (RBAC) - **Możliwość definiowania ról i zasad IAM**, które określają, **jakie operacje są dozwolone dla użytkowników autoryzowanych przez Identity Pool**.
- **Dynamiczne przypisywanie ról** - Możliwość stosowania **zasad**, które **dynamicznie przypisują role** na podstawie atrybutów sesji użytkownika, takich jak **identyfikator dostawcy tożsamości** czy **atrybuty użytkownika**.



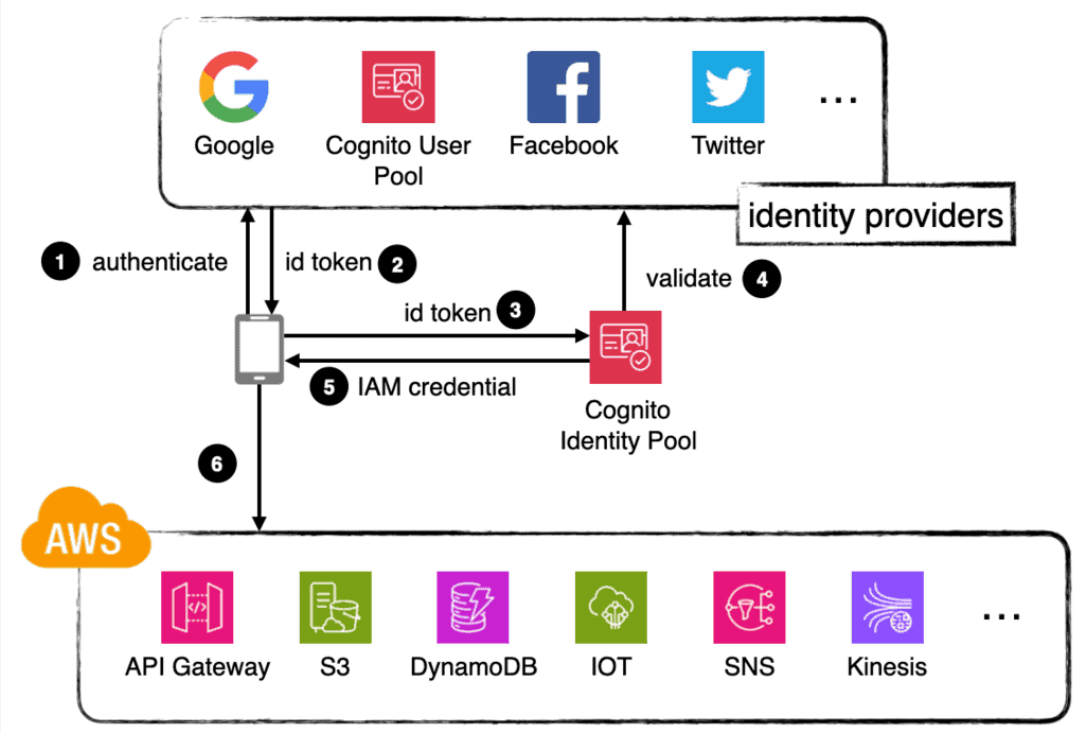
Identity Pools - zabezpieczenia

- Możliwość stosowania **warunkowych polityk bezpieczeństwa**, które mogą ograniczać dostęp na podstawie różnych czynników, jak lokalizacja użytkownika, urządzenie czy zachowania.
- Możliwość **włączenia wieloskładnikowego uwierzytelniania** dla dodatkowej warstwy bezpieczeństwa.



Identity Pools - zastosowanie

- Idealne **rozwiązanie dla aplikacji, które wymagają dostępu do zasobów AWS**, takich jak przechowywanie danych w S3 czy przetwarzanie w Lambda.
- Mogą być **używane do uwierzytelniania i autoryzacji urządzeń IoT**.



User Pools vs Identity Pools

- Służą jako **pełnoprawne rozwiązanie do zarządzania użytkownikami**. Pozwalają na **tworzenie i utrzymanie bazy użytkowników** dla **aplikacji internetowych** i **mobilnych**. Umożliwiają **rejestrację**, **logowanie** oraz **zarządzanie profilami** użytkowników.
- Skupiają się na **zarządzaniu użytkownikami i ich uwierzytelnianiu**

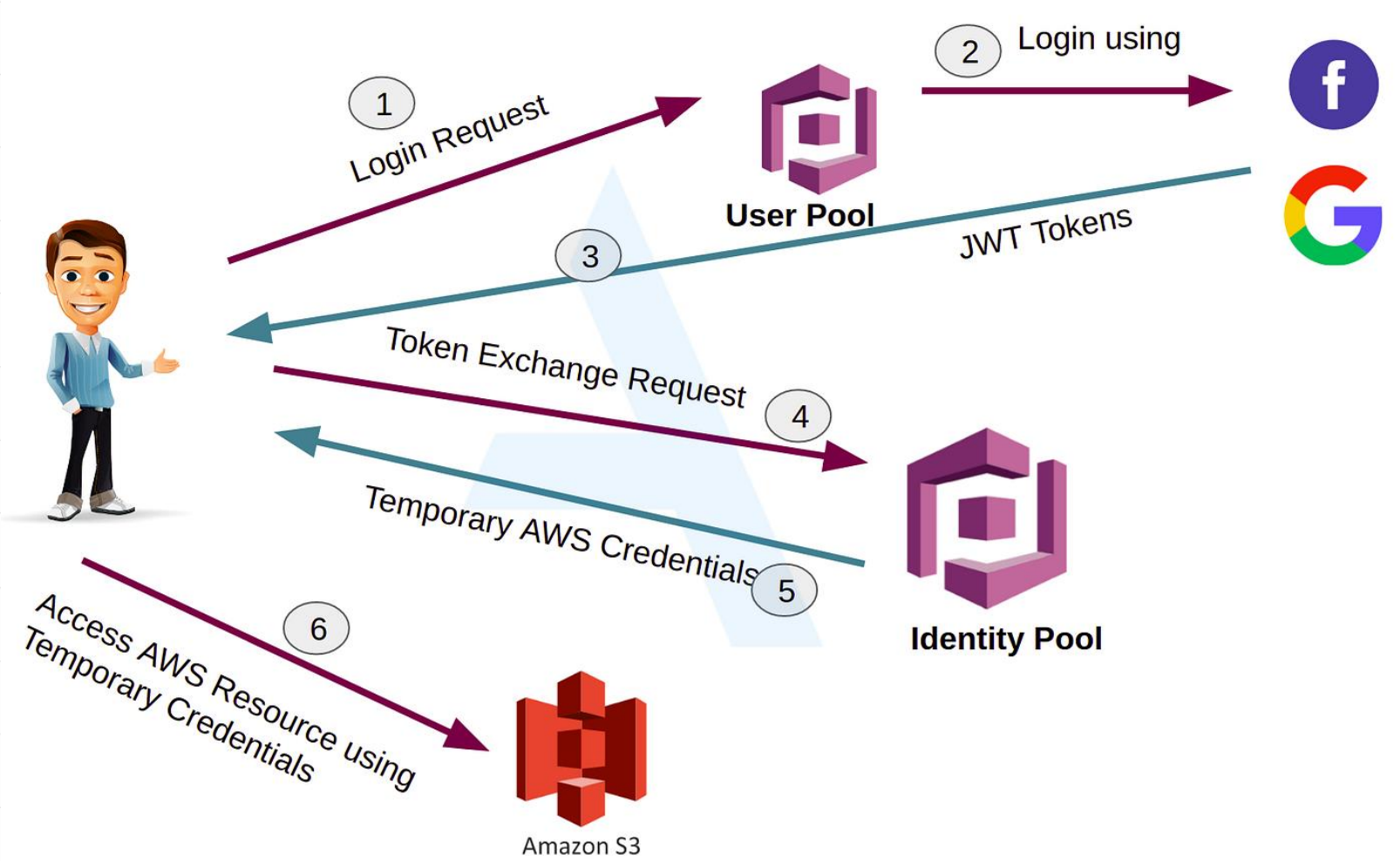
- Umożliwiają **zarządzanie tożsamościami** i **dostępem użytkowników do zasobów AWS**. Umożliwiają **integrację z różnymi źródłami** tożsamości, w tym z **User Pools**, aby przyznawać tymczasowe poświadczenia AWS do dostępu do zasobów.
- Koncentrują się na **autoryzacji dostępu do zasobów AWS**.
- Oferują **większą elastyczność** w **integracji z różnymi systemami tożsamości** niż User Pools.
- **Umożliwiają bardziej zaawansowane zarządzanie dostępem**, korzystając z ról IAM i polityk bezpieczeństwa.

User Pools vs Identity Pools

- Gdy istnieje potrzeba pełnej funkcjonalności zarządzania użytkownikami.
- Gdy aplikacja wymaga bezpośredniego uwierzytelniania użytkowników, bez konieczności dostępu do zasobów AWS.

- Gdy aplikacja wymaga dostępu do zasobów AWS.
- Gdy istnieje potrzeba pozwolenia użytkownikom logowania za pomocą różnych dostawców tożsamości.

Proces autoryzacji i uwierzytelniania

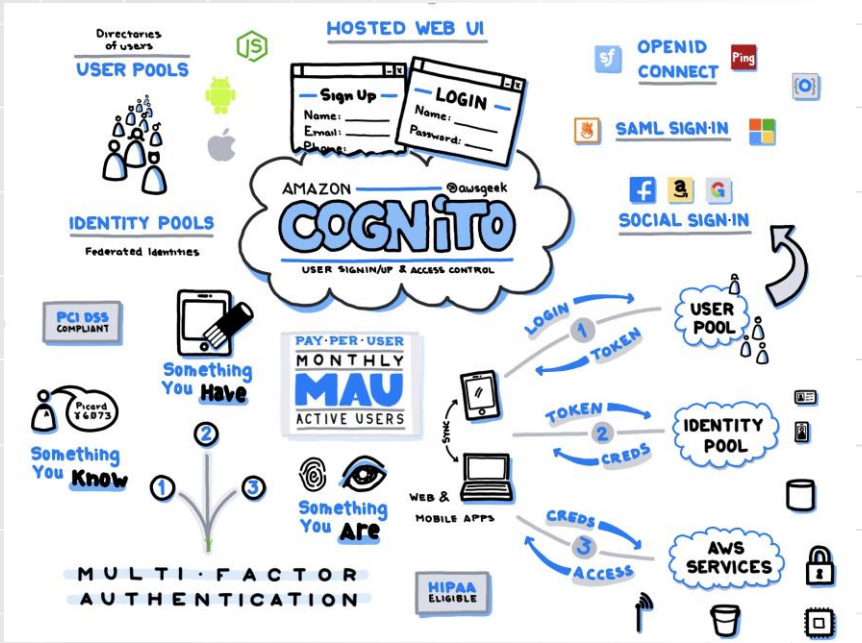


Wrocław
University
of Science
and Technology

AWS Cognito - Zabezpieczenia i zgodność

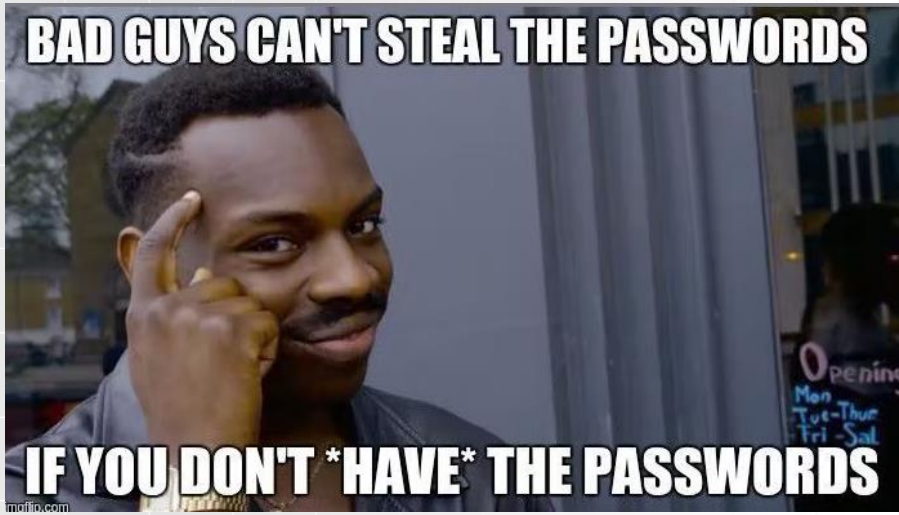
Funkcje bezpieczeństwa

- Pozwala na włączenie wieloskładnikowego uwierzytelniania, co znacząco zwiększa bezpieczeństwo poprzez wymaganie dodatkowej metody weryfikacji tożsamości użytkownika (np. SMS, telefon, aplikacja uwierzytelniająca).
- Zapewnia automatyczne szyfrowanie danych przechowywanych, jak i transmisji przy użyciu protokołu HTTPS. Możliwe jest również użycie własnych kluczy szyfrujących zarządzanych przez AWS Key Management Service (KMS) dla dodatkowej kontroli.



Funkcje bezpieczeństwa

- Pozwala określić **polityki bezpieczeństwa** dla użytkowników, takie jak **zasady dotyczące skomplikowania hasła**, **czasu jego ważności** i **blokady konta po określonej liczbie nieudanych** prób logowania.
- Integruje się z **AWS CloudTrail**, co **umożliwia rejestrowanie i monitorowanie wszystkich zapytań do usługi Cognito API**, zapewniając możliwość przeprowadzania szczegółowych audytów bezpieczeństwa.



Wrocław
University
of Science
and Technology

Dziękuję za uwagę