

The image features a large green shape on the left side, which has a white semi-circular cutout. The word "Uwierzytelnianie" is written in dark blue text within this white area. A dark blue horizontal bar with rounded ends extends from the green shape towards the right side of the image.

# **Uwierzytelnianie**

# Plan

---

1. Uwierzytelnianie
2. Hasła
3. Kerberos

# Uwierzytelnianie a autoryzacja

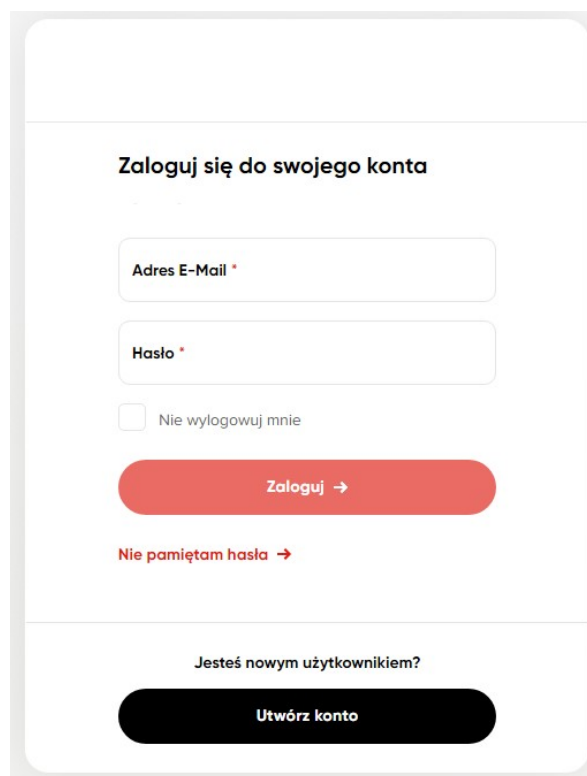
1. Identyfikacja - możliwość rozróżnienia użytkowników, np. w systemie operacyjnym
2. Uwierzytelnianie - proces weryfikacji tożsamości użytkownika;
3. Autoryzacja - proces przydzielania praw (dostępu do zasobów) użytkownikowi.

# Uwierzytelnianie a autoryzacja

Uwierzytelnianie jest procesem weryfikacji, czy "jesteś tym, za kogo się podajesz,,.

Autoryzacja jest procesem weryfikacji, czy "możesz robić to, co próbujesz zrobić".

# Uwierzytelnianie z funkcją skrótu



A mockup of a login form with a light gray border and rounded corners. The form is divided into two sections by a horizontal line. The top section is titled 'Zaloguj się do swojego konta' and contains two input fields for 'Adres E-Mail' and 'Hasło', both marked with a red asterisk. Below these is a checkbox labeled 'Nie wylogowuj mnie'. A red button with the text 'Zaloguj →' is positioned below the checkbox. A red link 'Nie pamiętam hasła →' is located below the button. The bottom section is titled 'Jesteś nowym użytkownikiem?' and features a black button with the text 'Utwórz konto'.

Zaloguj się do swojego konta

Adres E-Mail \*

Hasło \*

☐ Nie wylogowuj mnie

Zaloguj →

Nie pamiętam hasła →

Jesteś nowym użytkownikiem?

Utwórz konto

# Uwierzytelnianie z HMAC

```
openssl dgst -sha256 -hmac "klucz_hmac" <<< "w pierwszych słowach ..."
```

```
echo -n "w pierwszych słowach .." | openssl dgst -sha256 -mac HMAC -macopt  
hexkey:01234567ABCDEF00
```

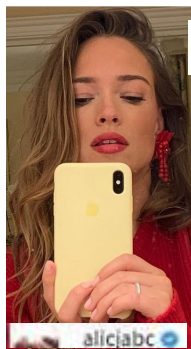
# Uwierzytelnianie certyfikatem klucza publicznego

Protokół challenge-response z kluczem publicznym

1. Alicja komunikuje się z Bolkem przedstawiając się jako Alicja
2. Bolek generuje liczbę losową LLB i wysyła ją Alicji
3. Alicja szyfruje liczbę LLB używając swojego klucza prywatnego i kryptogram wysyła do Bolka
4. Bolek deszyfruje kryptogram otrzymany od Alicji używając jej klucza publicznego i jeśli w wyniku otrzyma LLB to tożsamość Alicji jest potwierdzona

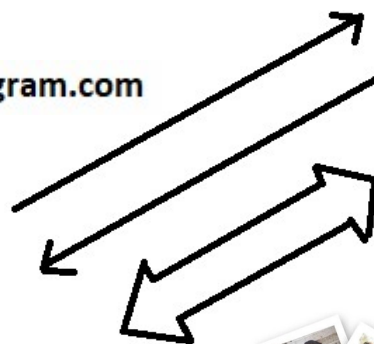
# Uwierzytelnianie w PKI

ROOT.crt



instagram.com

SSL/TLS(instgram.crt)





# Uwierzytelnianie- klasyfikacja

W zależności od kanału komunikacyjnego stosuje się różne metody i protokoły uwierzytelniania.

- w stosunku do dokumentów papierowych – podpisy, pieczęcie, parafowanie, znak wodny (metody), poświadczenie notarialne (protokół);
- w stosunku do osób i innych istot żywych – zabezpieczenie biometryczne, dokument tożsamości, hasło, karta mikroprocesorowa (smart card), biochip, token (generator kodów);
- w stosunku do wiadomości i dokumentów elektronicznych – podpis cyfrowy, kod uwierzytelniania wiadomości (message authentication code);
- w stosunku do podmiotów w komunikacji elektronicznej – metody oparte na dowodzie posiadania hasła (kryptografia symetryczna – np. HMAC) lub klucza prywatnego (kryptografii asymetrycznej), dowód z wiedzą zerową, hasło jednorazowe.

[wiki]

# Uwierzytelnianie- klasyfikacja

Jedną z funkcjonalnych klasyfikacji uwierzytelniania jest podział na metody wykorzystujące:

- **coś co wiesz** (something you know) – informacja będąca w wyłącznym posiadaniu uprawnionego podmiotu, na przykład hasło lub klucz prywatny;
- **coś co masz** (something you have) – przedmiot będący w posiadaniu uprawnionego podmiotu, na przykład klucz (do zamka) lub token (generator kodów);
- **coś czym jesteś** (something you are) – metody biometryczne.

[wiki]

# Uwierzytelnianie dwuskładnikowe

Od 14 września 2019 zmienił się sposób logowania do serwisów bankowości elektronicznej. Wszystko to przez unijną dyrektywę PSD-2 (z ang. *Payment Services Directive 2*). Do tej pory, aby uzyskać dostęp do konta wystarczyło, znać numer klienta i hasło – od teraz wymagany jest dodatkowy krok w procesie potwierdzania tożsamości, czyli wpisanie na stronie kodu z SMS-a wysłanego na numer telefonu powiązany z kontem.

# Uwierzytelnianie dwuskładnikowe

Istnieje kilka innych popularnych metod uwierzytelniania dwuskładnikowego (2FA). Oto niektóre z nich:

- SMS-owy kod weryfikacyjny - Użytkownik otrzymuje kod weryfikacyjny na swój telefon komórkowy, który musi wprowadzić na stronie logowania. Kod jest ważny tylko przez krótki czas i jest używany tylko raz.
- Aplikacje generujące kody - W tym przypadku użytkownik pobiera aplikację generującą kody (np. Google Authenticator lub Microsoft Authenticator), która generuje jednorazowe kody, które muszą zostać wprowadzone na stronie logowania.
- Biometria - W tej metodzie użytkownik uwierzytelnia się za pomocą swojego ciała, np. skanując swoją twarz lub odcisk palca.
- Klucz fizyczny - Jest to małe urządzenie, które użytkownik może podłączyć do swojego komputera lub urządzenia mobilnego, aby potwierdzić swoją tożsamość.
- Aplikacje autoryzacyjne - W tej metodzie użytkownik musi zatwierdzić logowanie do swojego konta poprzez aplikację autoryzacyjną, która działa w tle na jego urządzeniu mobilnym lub komputerze.
- Karty z kodami - W tej metodzie użytkownik otrzymuje zestaw kart z kodami, które muszą zostać wprowadzone podczas logowania. Każdy kod jest używany tylko raz.

# Uwierzytelnianie TOTP

Time based One-Time Password

<https://youtu.be/CmeTFbennLU>

# U2F



<https://youtu.be/D1UcHiRbtPM>

<https://youtu.be/Zr0PffkN09w>

# Hasła

Ala ma kota a kot ma Alę i 3 psy → Amkak2mAi#p

Litwo Ojczyzno moja ty jesteś jak zdrowie ile Cię trzeba cenić Ten tylko się dowie -> L)mtj^ZiCt(Tt@d

# Menadżer haseł (aplikacja, przeglądarka)

Funkcjonalności, które realizuje menadżer haseł, obejmują:

**Generowanie silnych haseł:** Menadżer haseł generuje silne i unikalne hasła, które są praktycznie niemożliwe do odgadnięcia przez potencjalnych atakujących. Dzięki temu unikasz sytuacji, w których używasz łatwych do odgadnięcia haseł, takich jak "123456" lub „admin”.

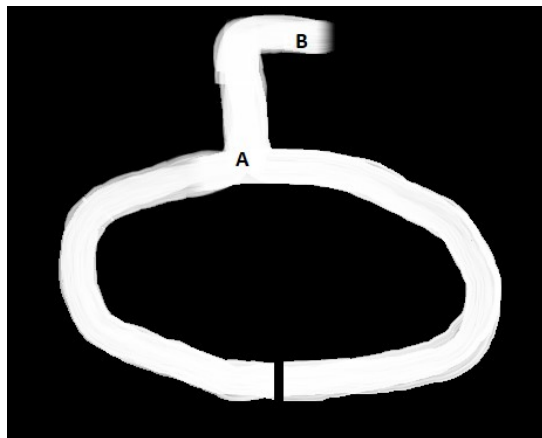
**Szyfrowanie haseł:** Menadżer haseł szyfruje hasła i przechowuje je w bezpiecznym miejscu, takim jak chmura lub lokalna pamięć urządzenia. Dzięki temu hasła są chronione przed potencjalnymi atakami hakerskimi.

**Automatyczne wypełnianie formularzy:** Menadżer haseł automatycznie wypełnia formularze z danymi uwierzytelniającymi, co pozwala na łatwe logowanie się na różne strony internetowe. W ten sposób nie musisz ręcznie wprowadzać swojego loginu i hasła do każdej strony, co oszczędza czas i zmniejsza ryzyko wprowadzenia błędnego hasła.

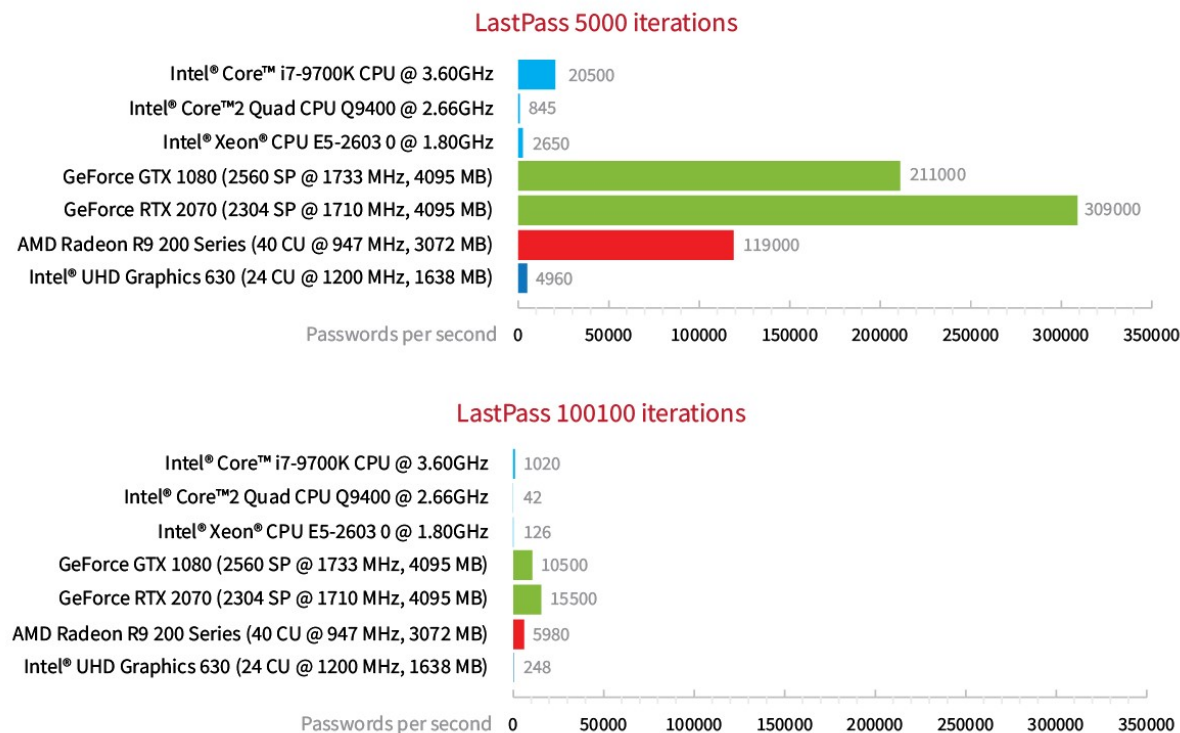


# Menadżer haseł w chmurze

Dostawcy usług menedżerów haseł w chmurze zazwyczaj nie mają dostępu do hasła głównego użytkownika, dzięki czemu nie są w stanie odczytać przechowywanych haseł. Jest to tzw. Dowód z wiedza zerową (ang. zero knowledge proof), czyli sposób przechowywania danych, w którym usługodawca nie ma wiedzy o treści przechowywanych danych.



# Menadżer haseł w chmurze



<https://blog.elcomsoft.com/2020/04/breaking-lastpass-instant-unlock-of-the-password-vault/>

# Kerberos

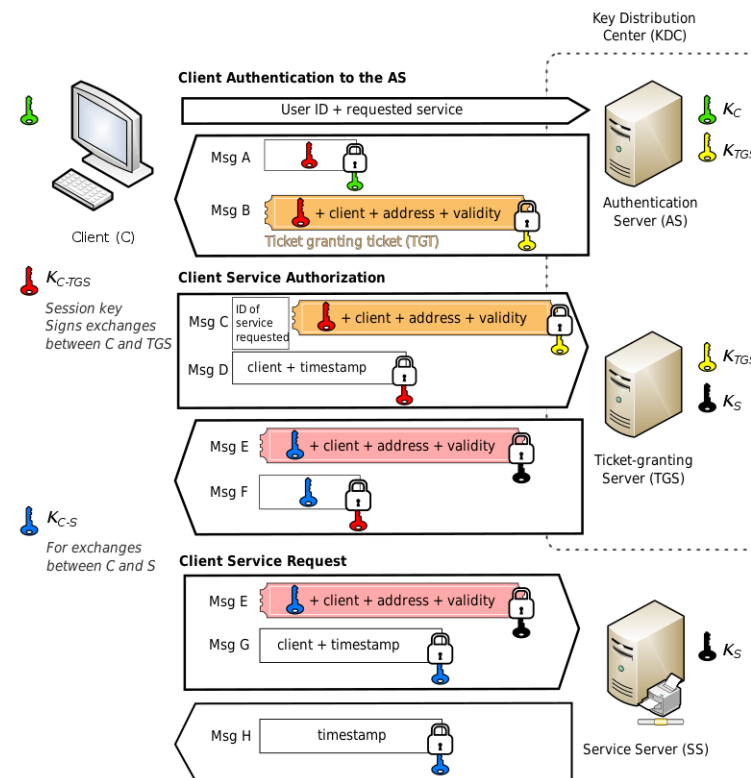
Protokół Kerberos to system uwierzytelniania, który zapewnia bezpieczeństwo w sieciach komputerowych.

Wykorzystuje on kryptografię symetryczną.

Składa się on z trzech podstawowych etapów:

1. Uwierzytelnienie
2. Udzielanie biletu (Ticket Granting)
3. Korzystanie z biletu (usługi)

# Kerberos



# Kerberos

## Kerberos Initial Authentication

1. User enters UID and Password (P) into the client application

2. Application encrypts timestamp (TS) with Password



Client Workstation

5. Application performs decryption using password (P). TGT received.

UID + P{TS}

P{TGT}

3. AS gets the user's password (P) from the DB and decrypts the TS

4. Generates a TGT and encrypts using password (P)



Authentication Server



www.cyphere.com  
info@cyphere.com  
+44 (0) 333 050 9002



# Uwierzytelnianie



THE END