# Objaśnienie KS 3.3.9:Dostępne uwierzytelnianie (ulepszone) (poziom AA)

Kryterium sukcesu (KS)

[Test funkcji poznawczych](file:///D:\github\objasnienia\WCAG-22_KS-339.html#dfn-cognitive-function-test) (taki jak zapamiętywanie hasła lub rozwiązywanie łamigłówki) nie jest wymagany na żadnym etapie [procesu](file:///D:\github\objasnienia\WCAG-22_KS-339.html#dfn-process) uwierzytelniania, chyba że etap ten zapewnia co najmniej jedną z poniższych:

**Alternatywa**

Inna metoda uwierzytelniania, która nie opiera się na teście funkcji poznawczych.

**Mechanizm**

Dostępny jest [mechanizm](file:///D:\github\objasnienia\WCAG-22_KS-339.html#dfn-mechanism) pomagający użytkownikowi w ukończeniu testu funkcji poznawczych.

## W skrócie

**Cel**

Umożliwiaj logowanie przy mniejszym wysiłku umysłowym.

**Co zrobić**

Nie zmuszaj użytkowników do rozpoznawania obiektów lub obrazów i multimediów dostarczonych przez użytkownika w celu zalogowania się.

**Dlaczego to jest ważne**

Niektóre osoby z problemami poznawczymi nie są w stanie rozwiązywać zagadek, w tym identyfikować obiektów i informacji nietekstowych, które wcześniej dostarczyły.

## Intencja

Celem tego kryterium sukcesu jest zapewnienie dostępnej, łatwej w użyciu i bezpiecznej metody logowania, uzyskiwania dostępu do treści i wykonywania zadań. Kryterium to jest takie samo jak w przypadku [Dostępnego uwierzytelniania](https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication), ale bez wyjątków dla obiektów i treści dostarczanych przez użytkownika.

Jakikolwiek wymagany krok procesu uwierzytelniania:

* nie może wyświetlać do wyboru obrazów, filmów lub klipów audio, w których użytkownicy muszą wybrać obraz, który podali;
* nie może wyświetlać do wyboru obrazów, w których użytkownicy muszą wybrać obrazy zawierające określony obiekt, taki jak samochód.

## Korzyści

Korzyści z tego kryterium sukcesu są takie same jak w przypadku [Dostępnego uwierzytelniania](https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication.html#benefits).

Osoby z problemami poznawczymi związanymi z pamięcią, czytaniem (np. dysleksja), liczbami (np. dyskalkulia) lub ograniczeniami w przetwarzaniu percepcji będą w stanie uwierzytelnić się niezależnie od poziomu ich zdolności poznawczych.

## Przykłady

Przykłady tego kryterium sukcesu są takie same jak przykłady [dostępnego uwierzytelniania](file:///D:\github\objasnienia\WCAG-22_KS-338.html#examples).

* Strona internetowa wykorzystuje odpowiednio oznaczone pola nazwy użytkownika (lub adresu e-mail) i hasła jako uwierzytelnienie logowania (spełnienie kryterium sukcesu [1.3.5 Określenie pożądanej wartości](file:///D:\github\objasnienia\WCAG-22_KS-135.html) i kryterium sukcesu [4.1.2: Nazwa, rola, wartość](file:///D:\github\objasnienia\WCAG-22_KS-412.html)). Przeglądarka użytkownika lub zintegrowane rozszerzenie menedżera haseł innej firmy może określić cel wprowadzania danych i automatycznie wypełnić nazwę użytkownika i hasło.
* Strona internetowa nie blokuje funkcji wklejania. Użytkownik może korzystać z zewnętrznego menedżera haseł do przechowywania poświadczeń, kopiowania ich i wklejania bezpośrednio do formularza logowania.
* Strona internetowa używa WebAuthn, aby użytkownik mógł uwierzytelnić się za pomocą swojego urządzenia zamiast nazwy użytkownika/hasła. Urządzenie użytkownika może korzystać z dowolnej dostępnej modalności. Typowe metody stosowane w laptopach i telefonach to skanowanie twarzy, odcisk palca i PIN (osobisty numer identyfikacyjny). Witryna nie wymusza żadnego konkretnego sposobu, zakłada się, że użytkownik skonfiguruje metodę, która mu odpowiada.
* Strona internetowa oferuje możliwość logowania się za pomocą zewnętrznego dostawcy przy użyciu metody OAuth.
* Strona internetowa, która wymaga uwierzytelniania dwuskładnikowego, umożliwia wiele opcji dla drugiego czynnika, w tym metodę opartą na USB, w której użytkownik po prostu naciska przycisk, aby wprowadzić token czasowy.
* Strona internetowa wymagająca uwierzytelniania dwuskładnikowego wyświetla kod QR, który może zostać zeskanowany przez aplikację na urządzeniu użytkownika w celu potwierdzenia tożsamości.
* Strona internetowa wymagająca uwierzytelniania dwuskładnikowego wysyła powiadomienie na urządzenie użytkownika. Użytkownik musi użyć mechanizmu uwierzytelniania swojego urządzenia (na przykład zdefiniowanego przez użytkownika kodu PIN, odcisku palca, rozpoznawania twarzy), aby potwierdzić tożsamość.

## Powiązane zasoby

Zasoby służą wyłącznie celom informacyjnym i nie sugerują żadnego ich poparcia.

* [Analiza luk w dostępności poznawczej Temat 1: Uwierzytelnianie i bezpieczeństwo](https://www.w3.org/TR/coga-gap-analysis/#table1)
* [Dokumenty dotyczące dostępności poznawczej 4. Technologie bezpieczeństwa i prywatności w sieci](https://w3c.github.io/coga/issue-papers/#web-security-and-privacy-technologies) oraz [technologie bezpieczeństwa i prywatności w sieci](https://w3c.github.io/coga/issue-papers/privacy-security.html)
* [Uczynienie treści użytecznymi dla osób z zaburzeniami poznawczymi i trudnościami w uczeniu się 4.7.1 Zapewnienie logowania, które nie opiera się na pamięci lub innych umiejętnościach poznawczych](https://www.w3.org/TR/coga-usable/#provide-a-login-that-does-not-rely-on-memory-or-other-%20%20%20%20%20%20%20%20%20%20%20%20%20cognitive-skills-pattern)
* [Dokument dotyczący technologii bezpieczeństwa i prywatności opracowany przez Cognitive Task Force](https://rawgit.com/w3c/coga/master/issue-papers/privacy-security.html).
* [Specyfikacja WebAuthN](https://www.w3.org/TR/webauthn/).
* [API uwierzytelniania internetowego na MDN](https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API).
* [Strona demonstracyjna WebAuthN](https://webauthn.io/).
* [OAuth w Wikipedii](https://en.wikipedia.org/wiki/OAuth).
* [„Niech wklejają hasła”, z brytyjskiego Narodowego Centrum Cyberbezpieczeństwa](https://www.ncsc.gov.uk/blog-post/let-them-paste-passwords)

## Techniki

Każdy numerowany element w tej sekcji przedstawia technikę lub kombinację technik, które Grupa Robocza WCAG uważa za wystarczające do spełnienia tego kryterium sukcesu. Nie jest jednak konieczne stosowanie tych konkretnych technik. Aby uzyskać informacje na temat korzystania z innych technik, zobacz [Objaśnienie technik dla kryteriów sukcesu WCAG](file:///D:\github\objasnienia\WCAG-objasnienie-technik.html), w szczególności podrozdział „Inne techniki”.

### Techniki wystarczające

1. [G218: Uwierzytelnianie linków e-mail](https://www.w3.org/WAI/WCAG22/Techniques/general/G218)
2. [H100: Zapewnianie odpowiednio oznaczonych danych wejściowych e-mail i hasła](https://www.w3.org/WAI/WCAG22/Techniques/html/H100)
3. Udostępnianie WebAuthn jako alternatywy dla nazwy użytkownika/hasła (potencjalna przyszła technika)
4. Zapewnienie logowania strony trzeciej przy użyciu OAuth (potencjalna przyszła technika)
5. Korzystanie z dwóch technik w celu zapewnienia uwierzytelniania dwuskładnikowego (potencjalna przyszła technika)

### Błędy

Poniżej wymieniono typowe błędy, które Grupa Robocza WCAG uważa za naruszenie tego kryterium sukcesu.

1. [F109: Niespełnienie kryterium sukcesu 3.3.8 i 3.3.9 z powodu uniemożliwienia ponownego wprowadzenia hasła lub kodu w tym samym formacie.](https://www.w3.org/WAI/WCAG22/Techniques/failures/F109)