# Objaśnienie KS 3.3.8:Dostępne uwierzytelnianie (minimum) (poziom AA)

Kryterium sukcesu (KS)

[Test funkcji poznawczych](file:///D:\github\objasnienia\WCAG-22_KS-338.html#dfn-cognitive-function-test) (taki jak zapamiętywanie hasła lub rozwiązywanie łamigłówki) nie jest wymagany na żadnym etapie [procedury](file:///D:\github\objasnienia\WCAG-22_KS-338.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-338.html#dfn-mechanism) pomagający użytkownikowi w ukończeniu testu funkcji poznawczych.

**Rozpoznawanie obiektów**

Test funkcji poznawczych polega na rozpoznawaniu obiektów.

**Treść osobista**

Test funkcji poznawczych ma na celu rozpoznanie [treści nietekstowych](file:///D:\github\objasnienia\WCAG-22_KS-338.html#dfn-non-text-content), które użytkownik dostarczył na stronę internetową.

„Rozpoznawanie obiektów” i „Treść osobista” mogą być reprezentowane przez obrazy, wideo lub audio.

Przykłady mechanizmów spełniających to kryterium obejmują:

1. obsługa wprowadzania haseł przez menedżery haseł w celu ograniczenia konieczności zapamiętywania oraz
2. funkcje kopiuj i wklej, aby zmniejszyć obciążenie poznawcze związane z ponownym wpisywaniem.

## W skrócie

**Cel**

Umożliwiaj logowanie przy mniejszym wysiłku umysłowym.

**Co robić**

Nie zmuszaj ludzi do rozwiązywania, przypominania sobie lub przepisywania czegoś, aby się zalogować.

**Dlaczego to jest ważne**

Niektóre osoby z problemami poznawczymi nie mogą rozwiązywać zagadek, zapamiętywać nazwy użytkownika i hasła lub ponownie wpisywać jednorazowych kodów dostępu.

## Intencja

Celem tego kryterium sukcesu jest zapewnienie dostępnej, łatwej w użyciu i bezpiecznej metody logowania. Większość witryn internetowych korzysta z nazw użytkowników i haseł do logowania. Zapamiętanie lub przepisanie nazwy użytkownika, hasła lub jednorazowego kodu weryfikacyjnego stanowi bardzo duże lub niemożliwe obciążenie dla osób z pewnymi problemami poznawczymi.

Chociaż strony internetowe mogą wykorzystywać rozpoznawanie obiektów lub treści nietekstowych dostarczonych przez użytkownika w celu spełnienia tego kryterium sukcesu, takie techniki nie wspierają w pełni społeczności osób z niepełnosprawnościami poznawczymi i należy ich unikać, jeśli to możliwe. Zapoznaj się z [Dostępne uwierzytelnianie (wzmocnione)](https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication-enhanced), aby uzyskać wskazówki dotyczące większej integracji i dostępności.

### Testy funkcji poznawczych

Zapamiętanie hasła specyficznego dla danej witryny jest [testem funkcji poznawczych](file:///D:\github\objasnienia\WCAG-22_KS-338.html#dfn-cognitive-function-test). Wiadomo, że takie testy są problematyczne dla wielu osób z problemami poznawczymi. Niezależnie od tego, czy chodzi o zapamiętywanie losowych ciągów znaków, czy też wykonywanie gestów na ekranie dotykowym, testy funkcji poznawczych wykluczą niektóre osoby. W przypadku korzystania z testu funkcji poznawczych musi być dostępna co najmniej jedna inna metoda uwierzytelniania, która nie jest testem funkcji poznawczych.

Jeśli w procesie uwierzytelniania jest więcej niż jeden krok, na przykład w przypadku uwierzytelniania wieloskładnikowego, wszystkie kroki muszą być zgodne z tym kryterium sukcesu. Musi istnieć ścieżka uwierzytelniania, która nie opiera się na testach funkcji poznawczych.

Możliwość odzyskania lub zmiany adresu e-mail i hasła jest ważną częścią uwierzytelniania. Jeśli użytkownik uwierzytelnia się za pomocą alternatywnych informacji w celu odzyskania konta, musi istnieć metoda, która nie jest testem funkcji poznawczych.

Wiele organizacji jest zobowiązanych do stosowania uwierzytelniania dwuskładnikowego, które łączy niezależne źródła w celu potwierdzenia tożsamości użytkownika. Źródła te mogą polegać na łączeniu uwierzytelniania poprzez:

* wiedzę (np. hasło, litery w haśle lub zapamiętana ścieżka przeciągnięcia);
* (np. posiadanie kodu weryfikacyjnego wygenerowanego lub odebranego na urządzeniu lub zeskanowanie kodu QR na urządzeniu zewnętrznym);
* dane biometryczne (np. skanowanie odcisków palców, rozpoznawanie twarzy lub dynamika naciśnięć klawiszy).

Większość metod uwierzytelniania opartych na wiedzy opiera się na teście funkcji poznawczych, więc muszą być dostępne mechanizmy pomagające użytkownikom. Gdy uwierzytelnianie polega na wykonaniu czynności na oddzielnym urządzeniu, powinno być możliwe wykonanie tej czynności bez konieczności przepisywania informacji. Może nie być możliwe poznanie metod uwierzytelniania opartych na urządzeniach dostępnych dla użytkownika; oferowanie wyboru metod może pozwolić im wybrać ścieżkę, która najbardziej im odpowiada.

### Metody uwierzytelniania

Strony internetowe mogą wykorzystywać wprowadzanie nazwy użytkownika (lub adresu e-mail) i hasła jako metodę uwierzytelniania, jeśli autor zezwoli programowi użytkownika (przeglądarkom i menedżerom haseł innych firm) na automatyczne wypełnianie pól. Ogólnie rzecz biorąc, jeśli formularz logowania spełnia [kryterium sukcesu 1.3.5 Określenie pożądanej wartości](https://www.w3.org/WAI/WCAG22/Understanding/identify-input-purpose), a kontrolki formularza mają odpowiednią dostępną nazwę zgodnie z kryterium sukcesu [4.1.2 Nazwa, rola, wartość](https://www.w3.org/WAI/WCAG22/Understanding/name-role-value), program użytkownika powinien być w stanie niezawodnie rozpoznać pola i automatycznie je wypełnić. Jeśli jednak program użytkownika jest aktywnie blokowany przed wypełnieniem pól (na przykład przez skrypt), wówczas strona nie spełni tego kryterium, ponieważ uniemożliwia działanie mechanizmu.

### Kopiuj i wklej

Kopiowanie i wklejanie pozwala uniknąć przepisywania. Użytkownicy mogą skopiować swoje dane logowania z lokalnego źródła (takiego jak samodzielny menedżer haseł innej firmy) i wkleić je w polach nazwy użytkownika i polach hasła w formularzu logowania lub w internetowych interfejsach wiersza poleceń z prośbą o podanie hasła. Zablokowanie możliwości wklejania danych do pól uwierzytelniania lub użycie innego formatu między skopiowanym tekstem a polem wprowadzania (na przykład „Wprowadź trzeci, czwarty i szósty znak swojego hasła”) zmusiłoby użytkownika do przepisania informacji, a tym samym nie spełniłoby tego kryterium, chyba że dostępna jest inna metoda.

### Systemy uwierzytelniania dwuskładnikowego (kody weryfikacyjne)

Oprócz nazw użytkowników i haseł, niektóre witryny mogą korzystać z uwierzytelniania dwuskładnikowego, prosząc użytkownika o wprowadzenie kodu weryfikacyjnego (zwanego również kodem dostępu lub hasłem jednorazowym). Usługa wymagająca ręcznego przepisania kodu weryfikacyjnego nie zapewnia zgodności. Podobnie jak w przypadku nazw użytkowników i haseł, użytkownik musi mieć możliwość przynajmniej wklejenia kodu (np. z samodzielnego zewnętrznego menedżera haseł, aplikacji do obsługi wiadomości tekstowych lub klucza bezpieczeństwa opartego na oprogramowaniu) lub umożliwienia programom użytkownika automatycznego wypełniania pól.

Istnieją scenariusze, w których kod weryfikacyjny musi zostać odebrany lub wygenerowany na urządzeniu dodatkowym. Na przykład uwierzytelnianie w przeglądarce internetowej na laptopie wymaga kodu weryfikacyjnego, który jest wysyłany jako wiadomość tekstowa SMS na telefon komórkowy. Jednak w większości przypadków możliwe jest wysłanie kodu bezpośrednio na urządzenie główne, gdzie można go skopiować i wkleić (na przykład kopiując kod na urządzeniu dodatkowym i wysyłając go e-mailem na urządzenie główne lub korzystając ze współdzielonego schowka między urządzeniami, w którym kopiowanie treści na urządzeniu dodatkowym udostępnia ją do wklejenia na urządzeniu głównym). Ocena, czy kod można płynnie przenieść z urządzenia dodatkowego na urządzenie podstawowe, wykracza poza zakres tego kryterium sukcesu. Do celów oceny treści internetowych, które opierają się na uwierzytelnianiu przy użyciu tego typu systemów urządzeń dodatkowych, zakłada się, że zapewniona jest możliwość udostępniają kodu w schowku użytkownika. Ocena tego kryterium wymaga zatem jedynie sprawdzenia, czy zawartość strony internetowej umożliwia wklejenie zawartości schowka w powiązanym polu wyzwania uwierzytelniania.

Należy pamiętać, że systemy dwuskładnikowe, które nie opierają się na kodach - w tym sprzętowe urządzenia uwierzytelniające (takie jak YubiKey), aplikacje pomocnicze (na tym samym urządzeniu głównym lub na urządzeniu dodatkowym), które oczekują od użytkownika potwierdzenia, że to rzeczywiście on próbuje się zalogować, oraz metody uwierzytelniania zapewniane przez system operacyjny użytkownika (takie jak Windows Hello lub Touch ID/Face ID w macOS i iOS) - nie są [testem funkcji poznawczych](file:///D:\github\objasnienia\WCAG-22_KS-338.html).

### Rozpoznawanie obiektów

Jeśli [CAPTCHA](https://www.w3.org/TR/turingtest/) jest używane jako część procesu uwierzytelniania, musi istnieć metoda, która nie obejmuje testu funkcji poznawczych, chyba że spełnia wyjątek. Jeśli test opiera się na czymś ustawionym przez stronę internetową, takim jak zapamiętywanie lub przepisywanie słowa lub rozpoznawanie obrazu dostarczonego przez stronę internetową, byłby to test funkcji poznawczych. Rozpoznawanie obiektów lub obrazków dostarczonych przez użytkownika jest testem funkcji poznawczych, jednak jest on wyłączony na poziomie AA.

Obiekt w tym kontekście oznacza ogólną angielską definicję („materialna rzecz, którą można zobaczyć i dotknąć”) i może obejmować pojazdy i zwierzęta. Jeśli test wykracza poza rozpoznawanie (np. pomnożenie liczby kotów przez liczbę psów), nie spełnia to wyjątku.

Niektóre formy rozpoznawania obiektów mogą wymagać zrozumienia konkretnej kultury. Na przykład taksówki mogą wyglądać inaczej w różnych miejscach. Jest to problem dla wielu osób, w tym osób z niepełnosprawnościami, ale nie jest on uważany za kwestię związaną z dostępnością.

Niektóre CAPTCHA i testy funkcji poznawczych używane do uwierzytelniania mogą pojawiać się tylko w określonych sytuacjach, takich jak obecność blokerów reklam lub po wielokrotnym wprowadzeniu nieprawidłowego hasła. Kryterium to ma zastosowanie w przypadku korzystania z tych testów, niezależnie od tego, czy są one używane za każdym razem, czy tylko uruchamiane przez określone scenariusze.

Istnieje szereg technologii, które można zastosować, aby zapobiec nadużyciom procesu uwierzytelniania przez skrypty.

* [1.1.1. Dostęp ograniczony limitem](https://www.ietf.org/archive/id/draft-private-access-tokens-01.html#name-rate-limited-access)
* [1.1.2. Geolokalizacja klienta](https://www.ietf.org/archive/id/draft-private-access-tokens-01.html#name-client-geo-location)
* [1.1.3. Uwierzytelnianie metodami zapewniającymi prywatność](https://www.ietf.org/archive/id/draft-private-access-tokens-01.html#name-private-client-authenticati)

Żaden z tych systemów nie jest w 100% skuteczny. Mogą one jednak zmniejszyć prawdopodobieństwo wyświetlenia CAPTCHA.

### Treść osobista

Treści osobiste są czasami wykorzystywane jako drugi czynnik uwierzytelniania. Na przykład, w ramach tworzenia konta użytkownik mógłby przesłać zdjęcie, a podczas logowania zostałby poproszony o wybranie tego zdjęcia spośród kilku możliwych alternatyw. W tym przypadku należy zadbać o zapewnienie odpowiedniego bezpieczeństwa, ponieważ nieuprawnieni użytkownicy mogą być w stanie odgadnąć prawidłową treść osobistą, gdy zostanie im przedstawiony wybór.

Treści osobiste oparte na tekście nie kwalifikują się do tego wyjątku, ponieważ opierają się na przypominniu sobie (a nie rozpoznawaniu) i wpisaniu (a nie wybieraniu elementu). Podczas gdy treści osobiste oparte na obrazach nadal będą stanowić barierę dla niektórych osób, wersje tekstowe stanowią znacznie większą barierę.

### Ukrywanie znaków

Innym czynnikiem, który może przyczyniać się do obciążenia poznawczego, jest ukrywanie znaków podczas pisania. Chociaż to kryterium wymaga, aby użytkownicy nie musieli wpisywać (transkrybować) hasła, istnieją scenariusze, w których jest to konieczne, takie jak tworzenie hasła do zapisania przez menedżera haseł. Zapewnienie funkcji opcjonalnego wyświetlania hasła może zwiększyć szansę powodzenia dla niektórych osób z problemami poznawczymi lub osób, które mają trudności z dokładnym wpisywaniem.

## Korzyści

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

## Przykłady

Przykłady tego kryterium sukcesu są takie same jak przykłady [Dostępnego uwierzytelniania (ulepszonego)](file:///D:\github\objasnienia\WCAG-22_KS-339.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: Zapewnienie 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)