

*Instrukcja  
użytkownika*



FIDO2 Klucz Biometryczny



**AUTHTREND**

## Klucz bezpieczeństwa USB z odciskiem palca

- Urządzenie HID, nie wymaga sterownika
- Przenośny klucz do dowolnego systemu Windows, Mac lub Chromebook
- Do 10 odcisków palców, < 1 sek., FAR < 1/50 000, FRR < 2%
- Certyfikat FIDO2





- Każdy klucz ma swój unikalny kod
- Jest równy numerowi seryjnemu
- Sprawdź kod klucza, aby uzyskać informacje o produkcji, obsłudze klienta i gwarancji





Zapoznaj się z poniższym filmem, aby zapoznać się z poniższymi 3 krokami: <https://youtu.be/-9ZCtPG-1J0>

### Krok 1

Rejestrowanie odcisku palca w ATKey



Samodzielna rejestracja (zgłoszenie patentowe) <https://youtu.be/IDrcZxWXAL4>  
lub za pomocą ustawień systemu Windows (kompilacja 1903)  
lub za pomocą aplikacji "ATKey dla Windows"

### Krok 2

Zarejestruj ATKey w urządzeniu lub usłudze

FIDO2

### Step 3

Dopasowywanie odcisków palców do uwierzytelniania

Logowanie bez hasła w usłudze Azure AD

<https://youtu.be/Q1CyIOa8IV8>

Logowanie bez hasła na konto Microsoft lub inne uwierzytelnianie FIDO2 za pośrednictwem przeglądarek w systemach Windows, Mac i Chromebook

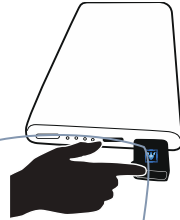
Usługi sprawdzania gotowości kluczy bezpieczeństwa FIDO można znaleźć tutaj: <https://www.dongleauth.info/>

Zaloguj się do Google, Facebook, Dropbox, Salesforce, Gitlab przez przeglądarkę Chrome jako 2. składnik

Możesz sprawdzić kompatybilną usługę z włączoną obsługą FIDO2 ATKey.Pro tutaj: <https://authentrend.com/compatible-with-atkeys/>



## Rejestracja samodzielna Nie jest wymagane żadne urządzenie ani aplikacja.

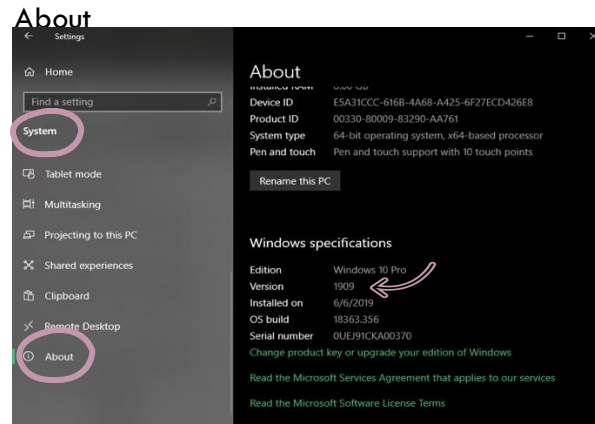


- Włóż ATKey.Pro do portu USB
- Sprawdź film na YouTube tutaj, aby uzyskać szczegółowe informacje: [https://www.youtube.com/watch?v=uoSf\\_B9hTY8](https://www.youtube.com/watch?v=uoSf_B9hTY8)
- Dioda LED świeci na NIEBIESKO, szybkie kliknięcie przycisku bocznego 3 razy, aby przejść do trybu rejestracji:
- Jeśli nie ma zarejestrowanego odcisku palca, dioda LED zmieni kolor na BIAŁY.
- Jeśli są jakieś zarejestrowane odciski palców, dioda LED na ZIELONO, zweryfikuj zarejestrowany odcisk palca, aby rozpocząć rejestrację nowego palca.
- Połóż konkretny palec na czujniku, dotknij i podnieś palec (dioda LED na BIAŁO, dioda LED świeci na zielono lub czerwono po dotknięciu odcisku palca, od wolnego do szybszego), powtórz to więcej niż 12 razy, aż dioda LED pokaże cyjan (13. raz), a następnie odcisk palca zostanie zarejestrowany.
- Jeśli chcesz zrezygnować z samodzielnej rejestracji, kliknij przycisk raz, dioda LED zmieni kolor na niebieski, powróci do normalnego stanu.



## Rejestrowanie w ustawieniach systemu Windows

- Jeśli Twój system operacyjny to Windows 10 build 1903 lub nowszy wersję, możesz zarządzać ATKey jako kluczem bezpieczeństwa.
- Kod PIN, dodawanie/usuwanie odcisków palców, resetowanie
- przejdź do strony "Ustawienia systemu Windows", aby uzyskać szczegółowe informacje Windows Settings => System =>

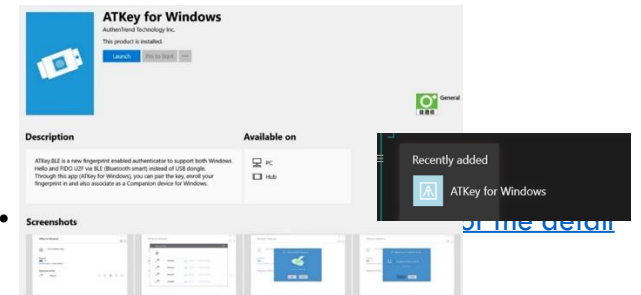


- Jeśli NIE korzystasz z systemu Windows 10 w wersji 1903 lub nowszej (Mac, Chromebook, Linux, ...), możesz rejestrować się samodzielnie lub użyć Chrome Canary do rejestrowania odcisków palców i zarządzania nimi.



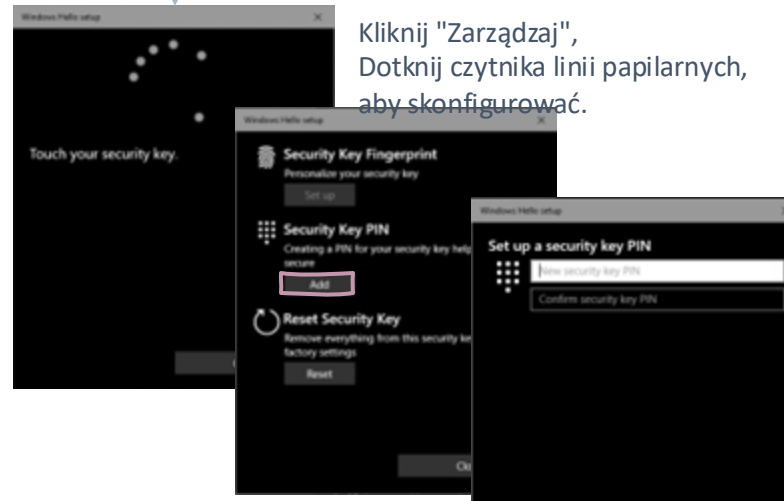
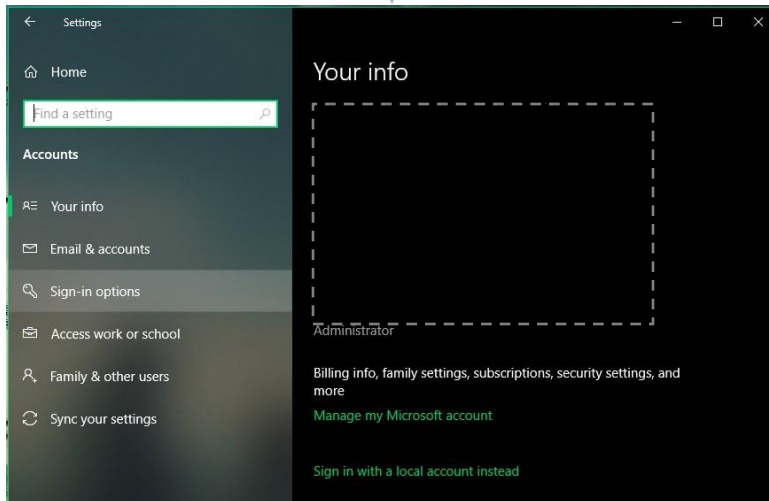
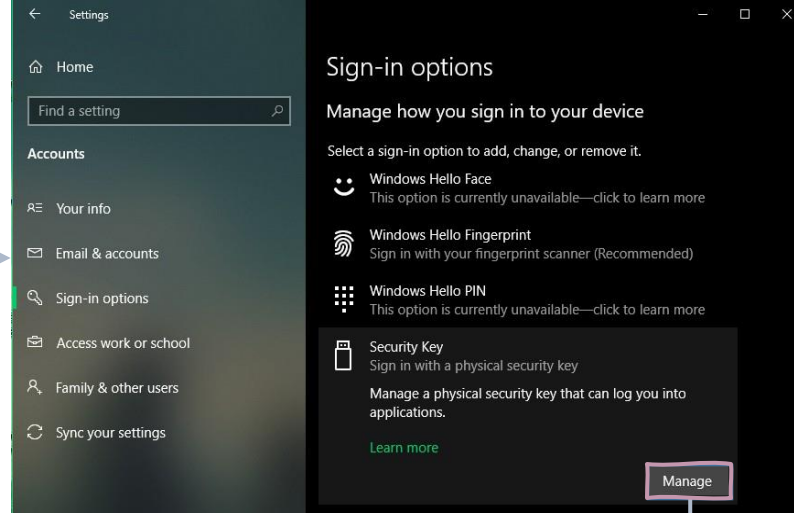
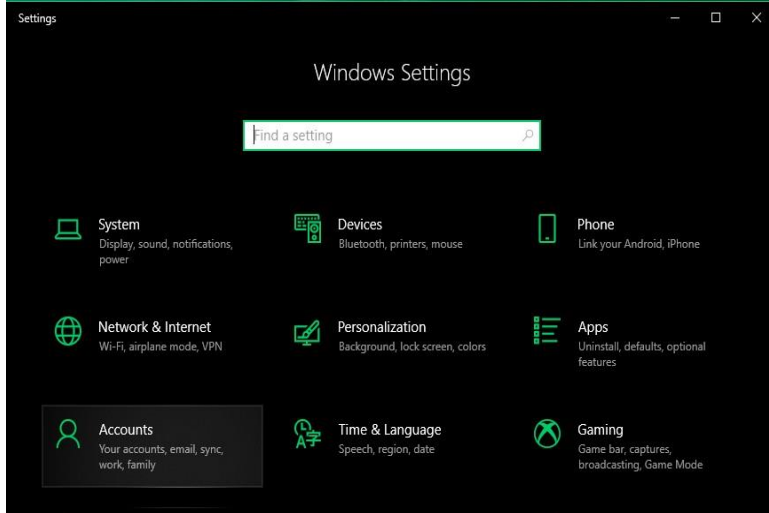
## ATKey dla aplikacji Windows

- Pobierz aplikację "ATKey for Windows" ze Sklepu Windows, aby zarządzać ATKey:
- Rejestrowanie odcisku palca
- Dodaj/usuń odcisk palca
- Informacje o ATKey
- Companion ATKey do systemu Windows (logowanie Windows Hello)
- Wyszukaj "ATKey" lub "AuthenTrend" w Sklepie Windows, aby znaleźć aplikację, pobrać i zainstalować.





Ustawienia Windows => Konto => Opcje logowania => Klucz bezpieczeństwa => Dodaj "Kod PIN" i zarejestruj "Odciski palców"



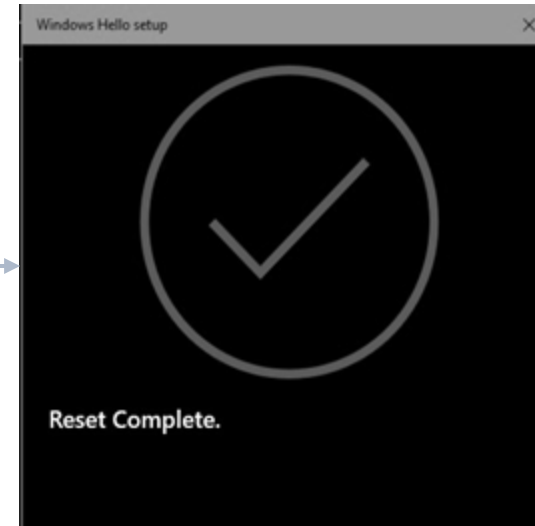
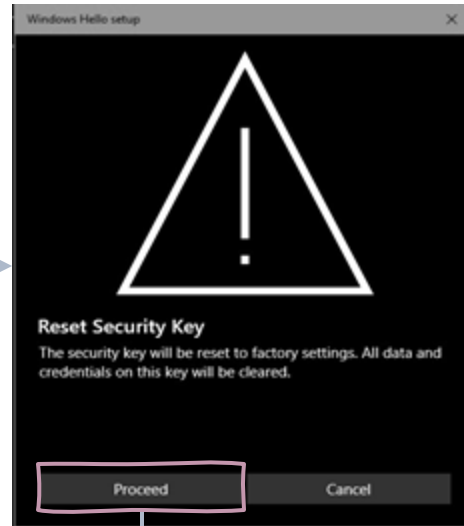
- Konfiguracja "Odcisk palca klucza bezpieczeństwa"
- Wpisz kod PIN, postępując zgodnie z podpowiedzią ekranową, aby zarejestrować odcisk palca, aż do "Wszystko gotowe!"

Najpierw dodaj "PIN klucza bezpieczeństwa"; ten kod PIN zostanie zapisany w ATKey.Pro.

Kliknij "Zarządzaj",  
Dotknij czytnika linii papilarnych,  
aby skonfigurować.



Ustawienia Windows => Konto => Opcje logowania => Klucz bezpieczeństwa => Resetuj klucz bezpieczeństwa (Usuń kod PIN i usuń wszystkie odciski palców)



Click "Process"

[Firmware 1.00.6 lub nowsza wersja]

1. niebieskozielona dioda LED
2. Wyjmij ATKey.Pro i włóż ponownie do portu USB
3. niebieskozielona dioda LED
4. Dotknij dowolnym palcem, aby zresetować lub anulować - zrób to (zresetuj) w ciągu 10 sekund

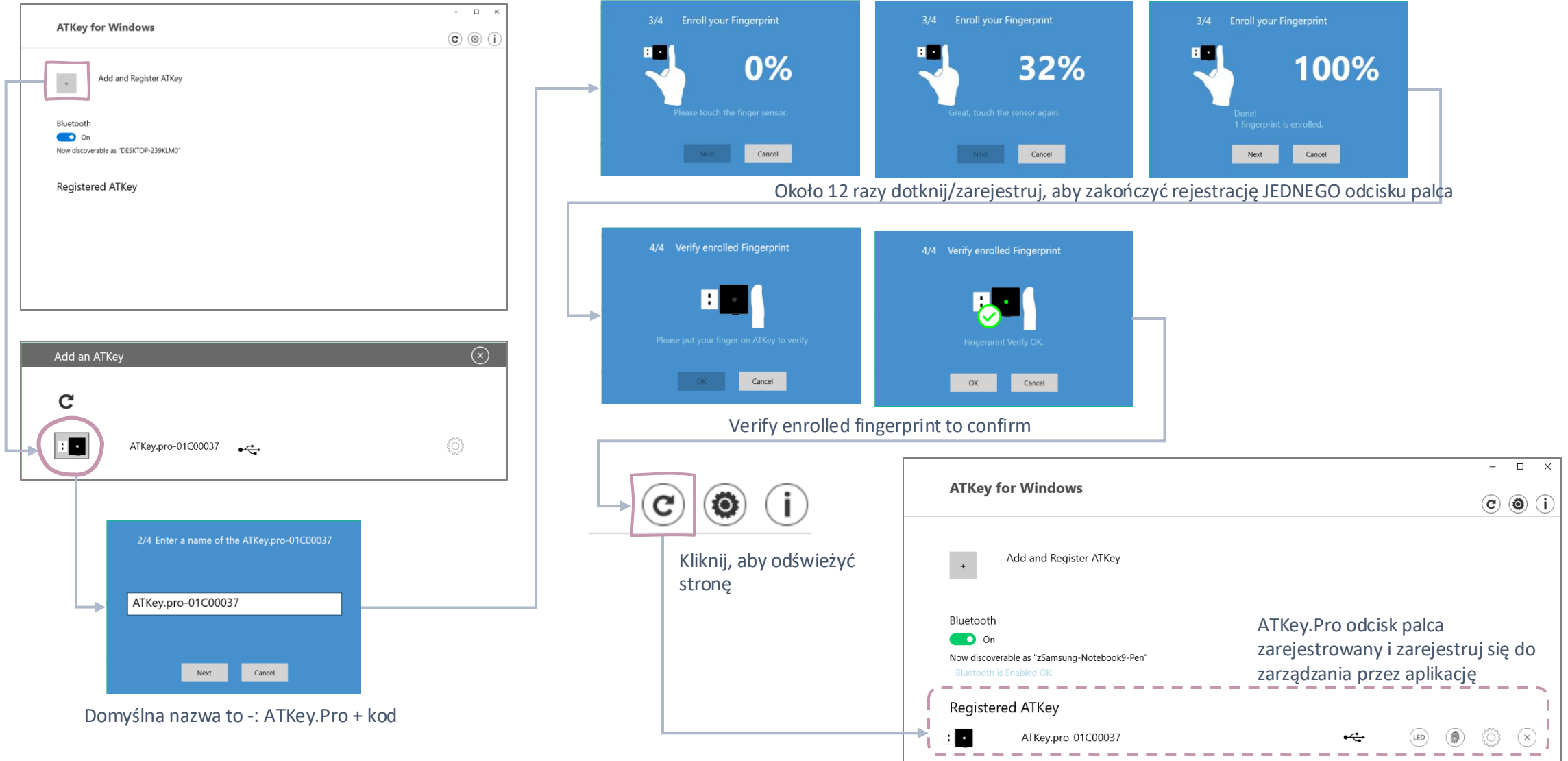
[Firmware 1.00.5 lub poprzedniawersion]

1. niebieska dioda LED
2. Wyjmij ATKey.Pro i włóż ponownie do portu USB
3. niebieska dioda LED
4. Dotknij dowolnym palcem, aby zresetować lub anulować - zrób to (zresetuj) w ciągu 10 sekund

*Firma Microsoft wymagała specyfikacji dla resetowania tokena uwierzytelniającego: aby zapobiec przypadkowemu uruchomieniu tego mechanizmu, wymagana jest obecność użytkownika. W przypadku tokenów uwierzytelniających bez wyświetlacza, żądanie MUSI wpłynąć do uwierzytelniacza w ciągu 10 sekund od włączenia uwierzytelnienia.*



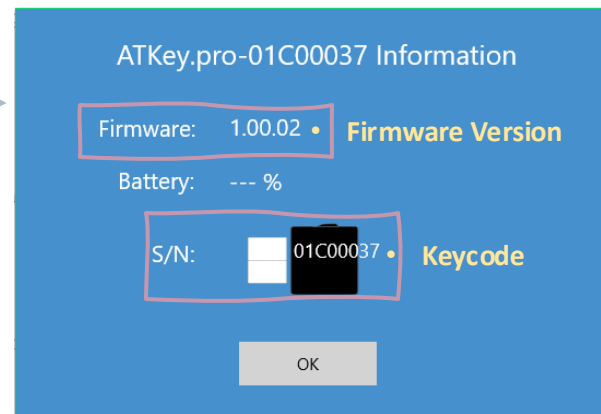
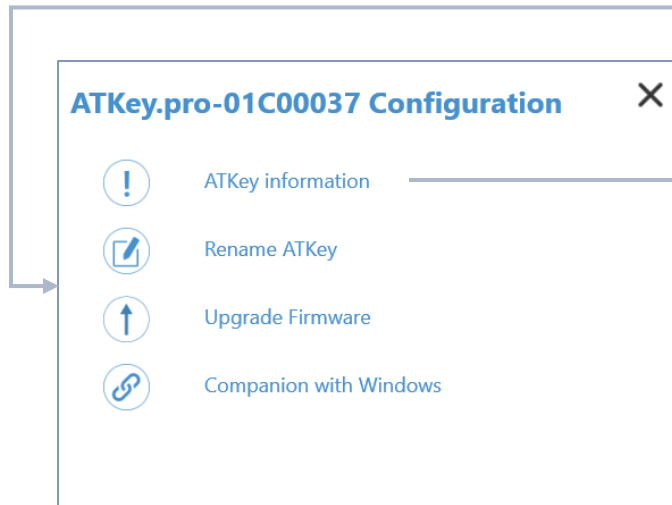
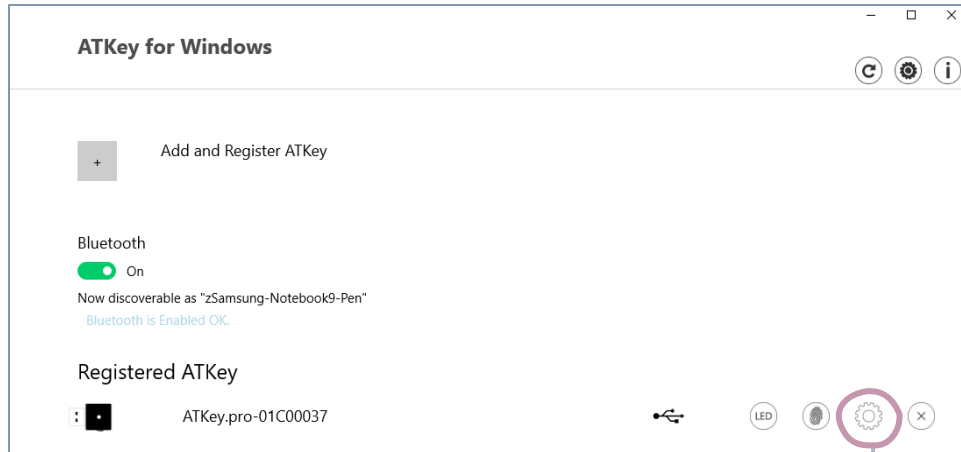
- Uruchom aplikację "ATKey dla Windows" (wersja 2.0.57.0 lub nowsza)
- Kliknij "Dodaj i zarejestruj ATKey" – upewnij się, że wkładki ATKey.Pro do portu USB, a dioda LED świeci na niebiesko





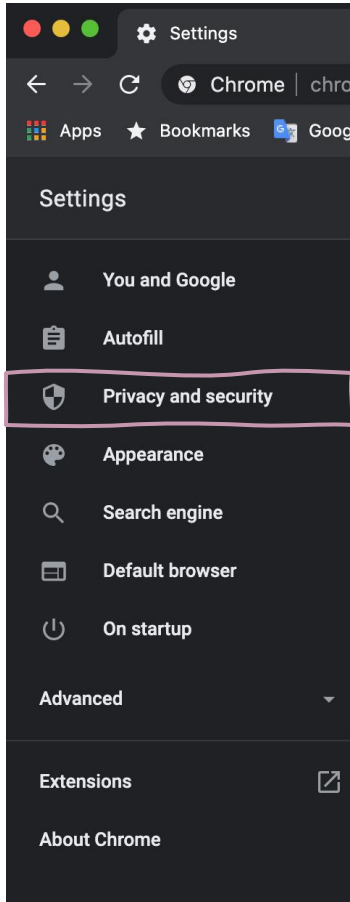


Zarządzanie ATKey – informacje, zmiana nazwy

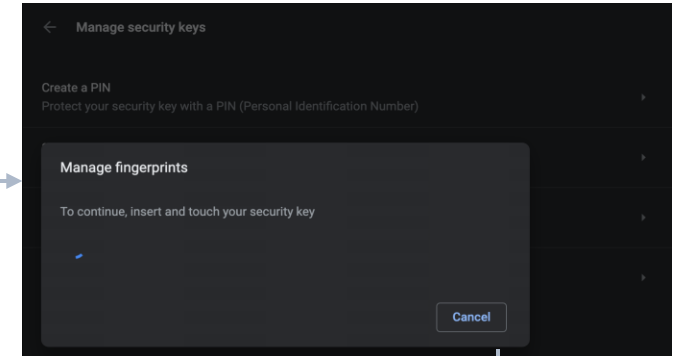
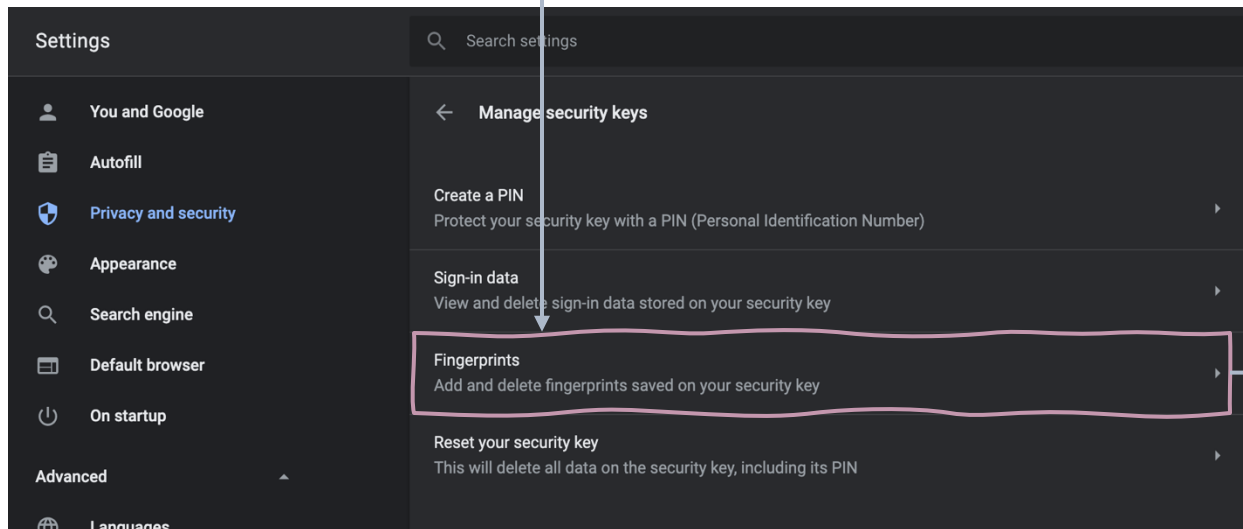
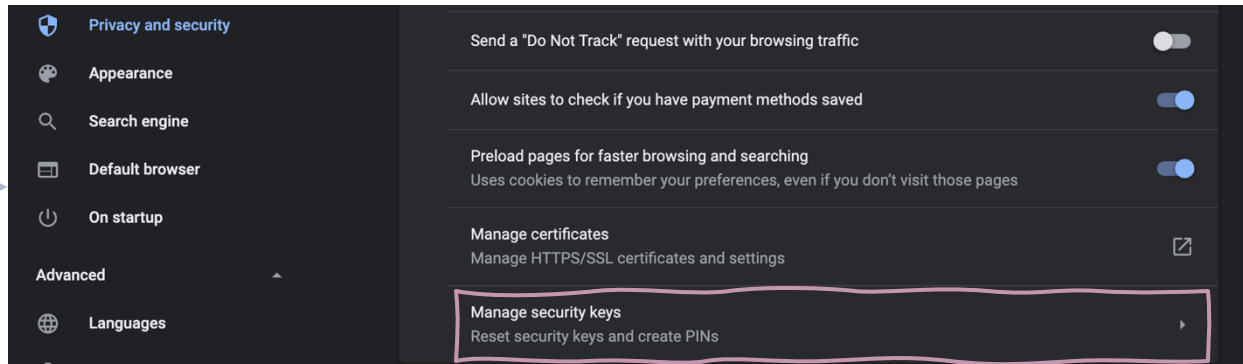




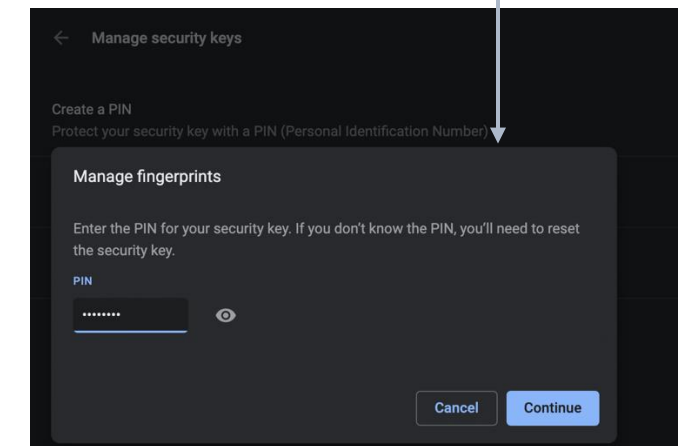
- Jeśli używasz systemu innego niż Windows 10 lub system Windows 10 jest starszy niż kompilacja 1903
- Zarejestruj odcisk palca w ATKey.Pro za pomocą
- Rejestracja autonomiczna
- lub Chrome Canary (<https://www.google.com/chrome/canary/>)



Z "Ustawień" =>  
"Prywatność i  
bezpieczeństwo"



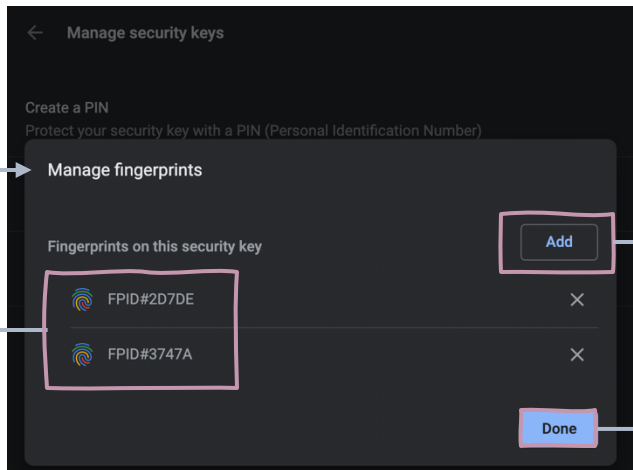
Potrzeby użytkownika w zakresie obecności  
- Dotknij klucza sprzętowego dowolnym palcem



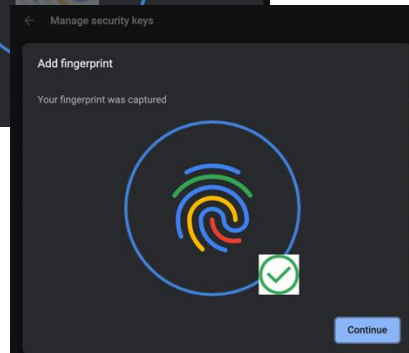
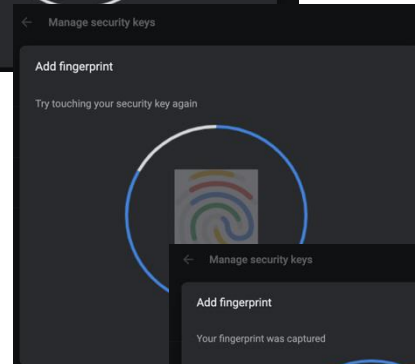
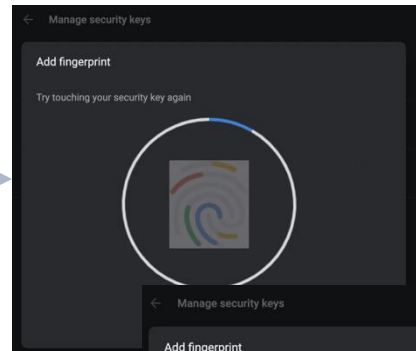
Przypisz kod PIN do klucza



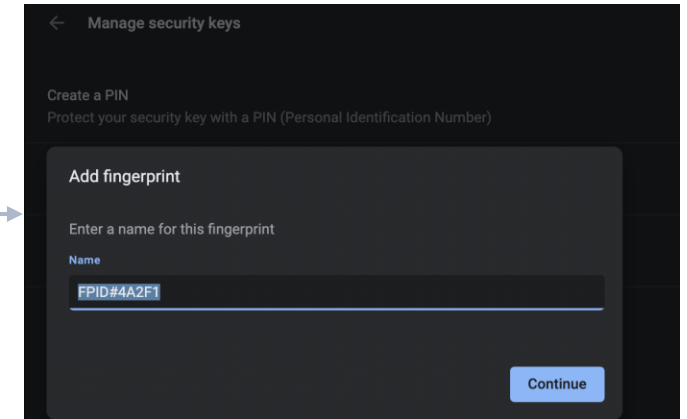
- Jeśli używasz systemu innego niż Windows 10 lub system Windows 10 jest starszy niż kompilacja 1903
- Zarejestruj odcisk palca w ATKey.Pro za pomocą
- Rejestracja autonomiczna
- lub Chrome Canary (<https://www.google.com/chrome/canary/>)



- Kliknij "Dodaj", aby pobrać odcisk palca (zarejestrować nowy palec)
- Tutaj wyświetla listę zarejestrowanych odcisków palców z przypisanymi nazwami



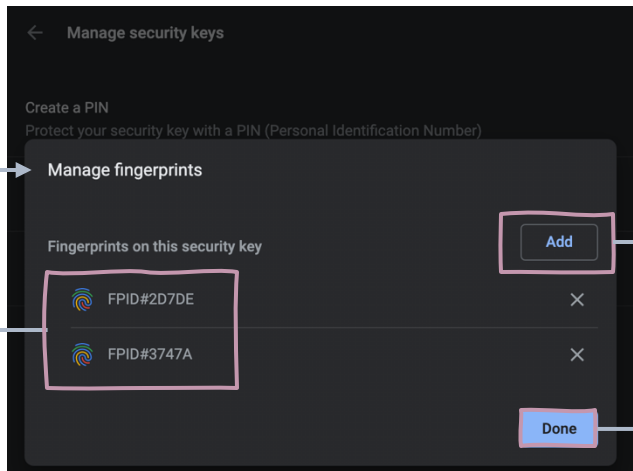
Zarejestruj odcisk palca, dopóki nie zostanie to zrobione



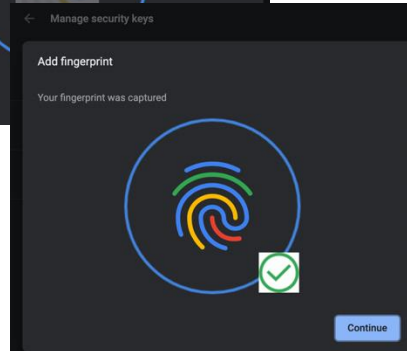
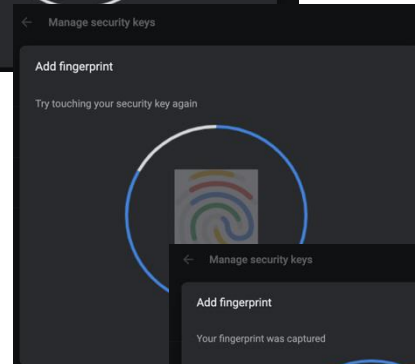
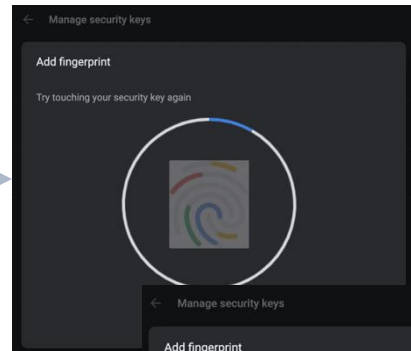
Przypisywanie nazwy zarejestrowanego odcisku palca



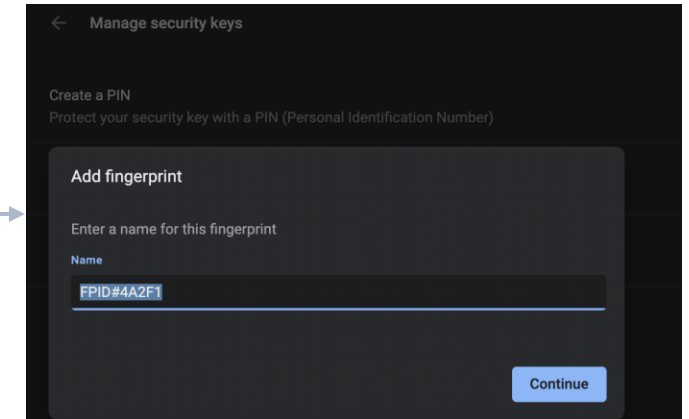
- Jeśli używasz systemu innego niż Windows 10 lub system Windows 10 jest starszy niż kompilacja 1903
- Zarejestruj odcisk palca w ATKey.Pro za pomocą
- Rejestracja autonomiczna
- lub Chrome Canary (<https://www.google.com/chrome/canary/>)



- Kliknij "Dodaj", aby pobrać odcisk palca (zarejestrować nowy palec)
- Tutaj wyświetla listę zarejestrowanych odcisków palców z przypisanymi nazwami



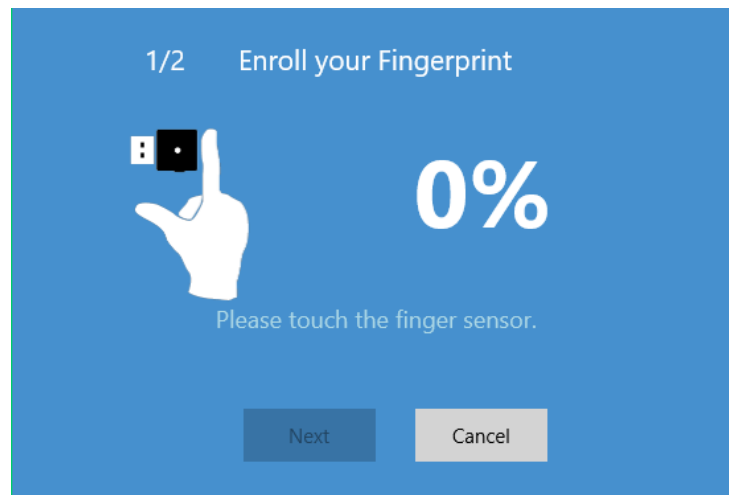
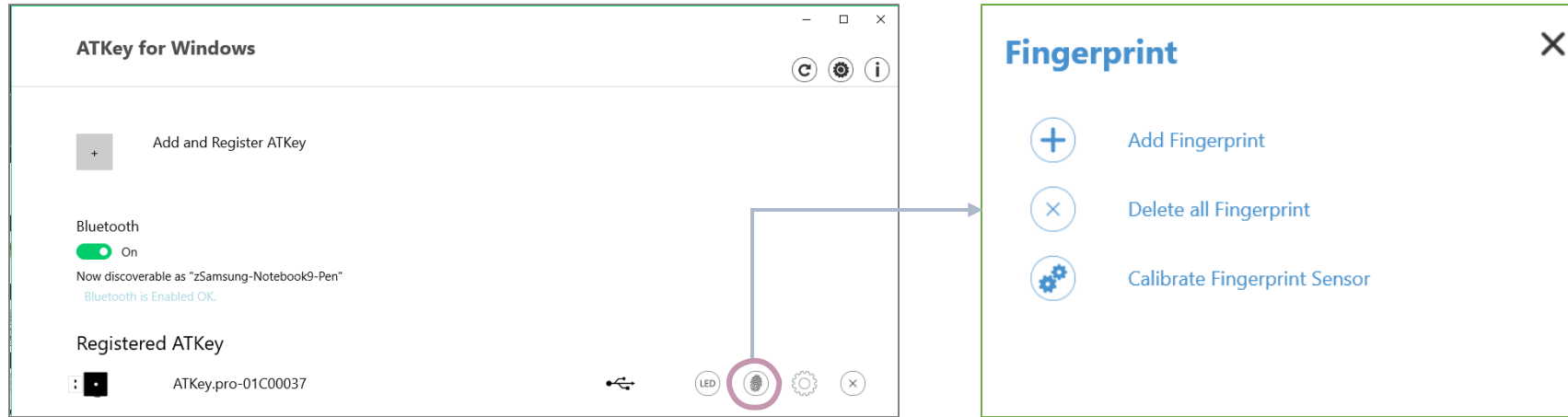
Zarejestruj odcisk palca, dopóki nie zostanie to zrobione



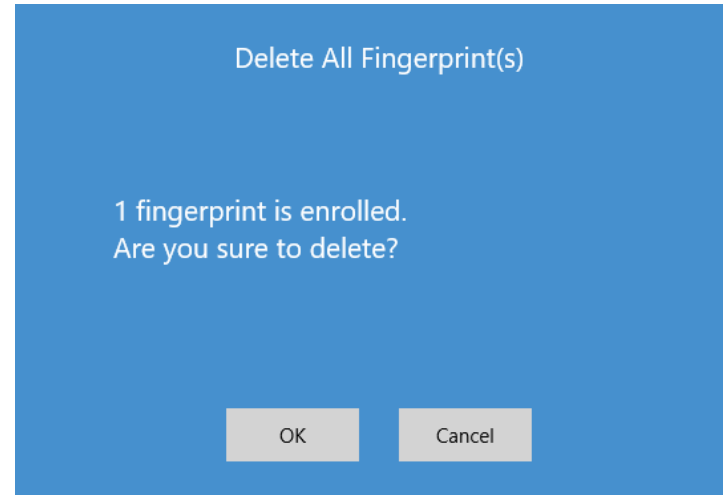
Przypisywanie nazwy zarejestrowanego odcisku palca



Zarządzanie ATKey – dodawanie/usuwanie odcisków palców, kalibracja czytnika linii papilarnych



- Zarejestruj nowy odcisk palca za pomocą ~12 razy dotyk, zgodnie z komunikatem interfejsu użytkownika; Do 10 odcisków palców



- Tutaj usuniesz wszystkie zarejestrowane odciski palców, "OK", aby je usunąć
- Do autoryzacji potrzebny jest kod PIN systemu Windows.

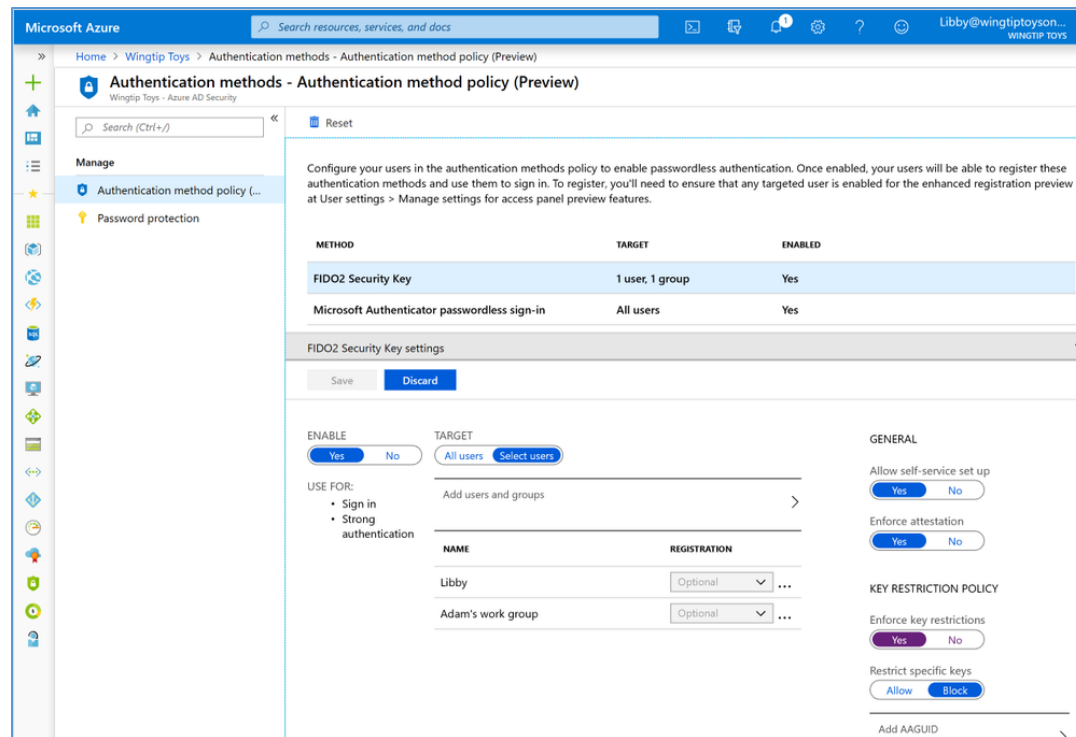


- Jeśli czujesz, że coś jest nie tak z odciskiem palca, wykonaj kalibrację, aby ponownie skalibrować czujnik
- **Nie kładź palca podczas kalibracji; Dioda LED będzie migać na BIAŁO, a następnie z powrotem na niebiesko**

- Czy Twoja firma/organizacja udziela licencji na usługę Azure AD?
- Jeśli tak, czy Twoje zasady uwierzytelniania zezwalają na "dodaj metodę", w tym "klucz bezpieczeństwa"?
- Zapoznaj się z poniższymi linkami, aby dowiedzieć się, jak włączyć klucz zabezpieczeń dla usługi Azure AD:
- Klucze bezpieczeństwa bez hasła
- System Windows 10 bez hasła
- Lokalna bez hasła
- Opcje uwierzytelniania bez hasła — klucz bezpieczeństwa

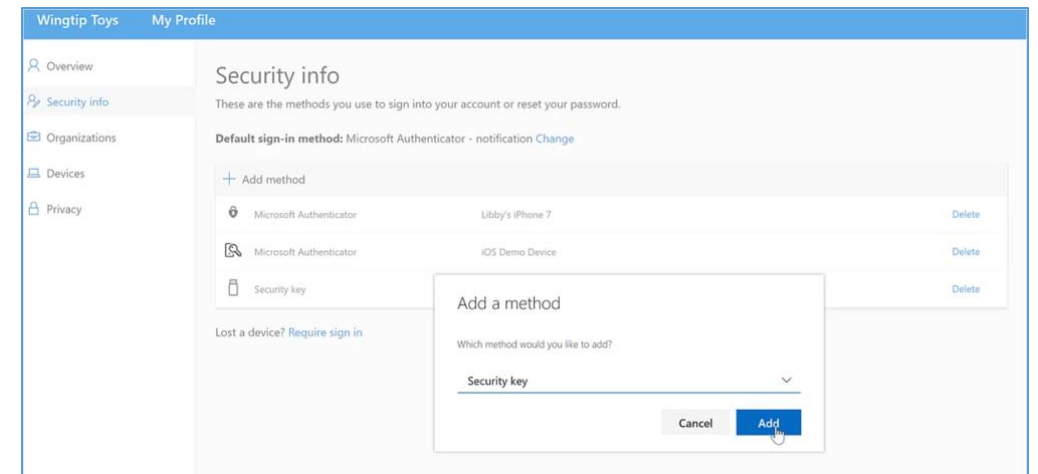
1

Nowy blok Metody uwierzytelniania w portalu administracyjnym usługi Azure AD, który umożliwia przypisywanie poświadczeń bez hasła przy użyciu kluczy zabezpieczeń FIDO2 i logowanie bez hasła za pomocą aplikacji Microsoft Authenticator do użytkowników i grup.



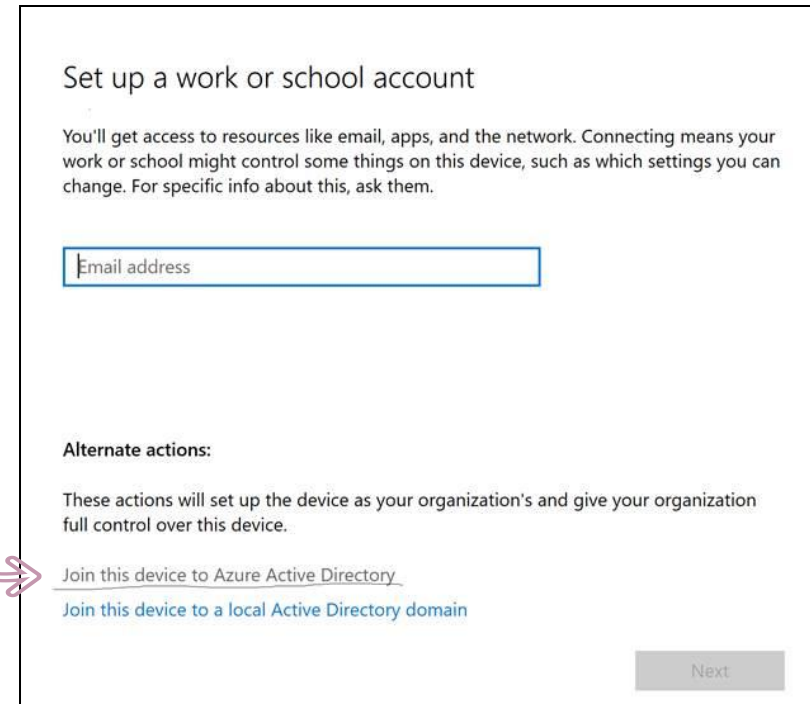
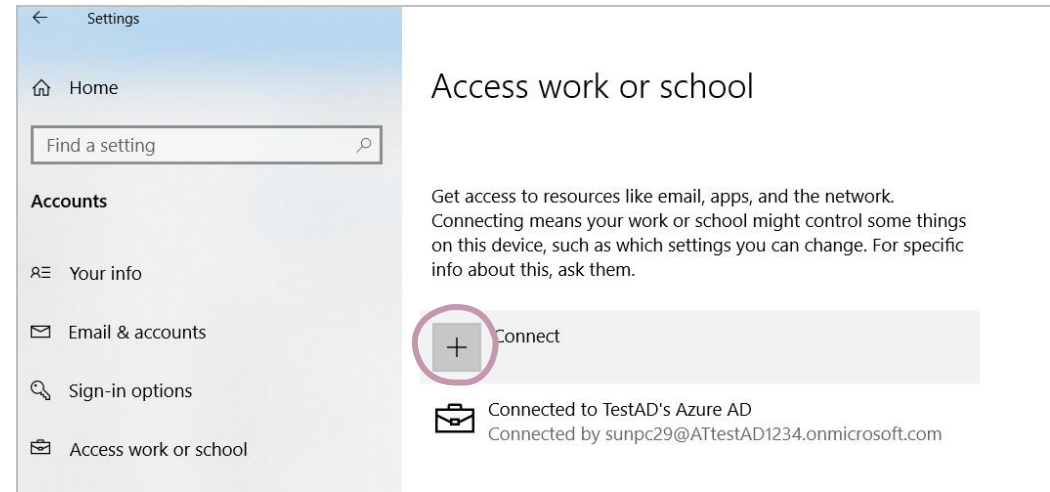
2

2. Zaktualizowane możliwości w konwergentnym portalu rejestracyjnym dla Twojego użytkowników do tworzenia kluczy zabezpieczeń FIDO2 i zarządzania nimi.





- Rejestracja użytkowników i zarządzanie kluczami zabezpieczeń FIDO2
- Przejdź do <https://myprofile.microsoft.com>
- Zaloguj się za pomocą identyfikatora/hasła lub aplikacji
- Kliknij opcję Security Information (Informacje zabezpieczające)
- Jeśli użytkownik ma już zarejestrowaną co najmniej jedną metodę usługi Azure Multi-Factor Authentication, może natychmiast zarejestrować klucz zabezpieczeń FIDO2.
- Jeśli nie mają zarejestrowanej co najmniej jednej metody Azure Multi-Factor Authentication, muszą ją dodać.
- Dodaj klucz zabezpieczeń FIDO2, klikając pozycję Dodaj metodę i wybierając pozycję Klucz zabezpieczeń
- Wybierz urządzenie USB lub urządzenie NFC
- Przygotuj swój klucz i wybierz Dalej
- Pojawi się okno z prośbą o utworzenie/wprowadzenie kodu PIN dla klucza bezpieczeństwa, a następnie wykonanie wymaganego gestu dla klucza, biometrycznego lub dotykowego.
- Zostaniesz powrócony do połączonego środowiska rejestracji i poproszony o podanie zrozumiałej nazwy tokena, aby można było określić, który z nich, jeśli masz ich wiele. Kliknij Dalej.
- Kliknij Gotowe, aby zakończyć proces

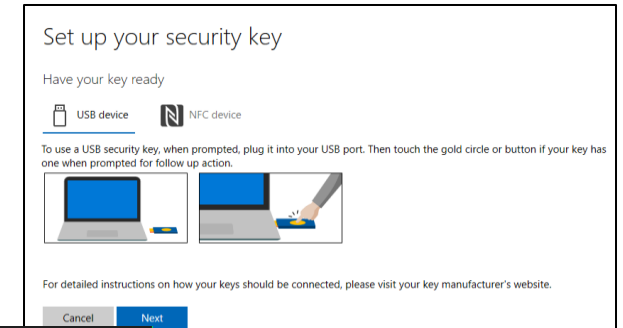




## Logowanie bez hasła do konta Microsoft za pomocą klucza zabezpieczeń :

- W przypadku logowania bez hasła do konta Microsoft — Windows 10 build 1809 lub nowsza wersja za pośrednictwem przeglądarki Edge/Chrome, tryb USB:Możesz zalogować się, aby dodać ATKey.Pro jako klucz bezpieczeństwa dla swojego konta Windows stąd: <https://account.microsoft.com/account>

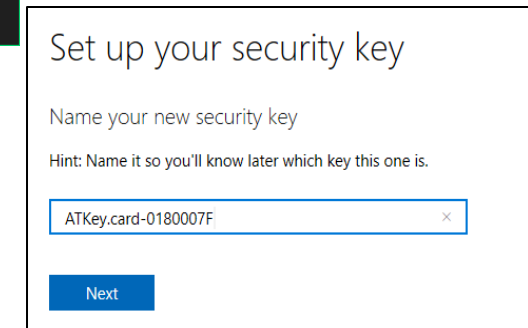
- Najpierw zaloguj się za pomocą identyfikatora/hasła
- Krok po kroku, aby skonfigurować klucz bezpieczeństwa
- Kliknij "Bezpieczeństwo" na pasku banera
- Kliknij "więcej opcji bezpieczeństwa" od dołu
- W sekcji "Windows Hello i klucze bezpieczeństwa" kliknij "Konfiguracja security key"



1) Dotknij zarejestrowanego odcisku palca, aby go zweryfikować



2) Dopasowany odcisk palca, wpisz nazwę klucza (nazwa domyślna po kodzie)



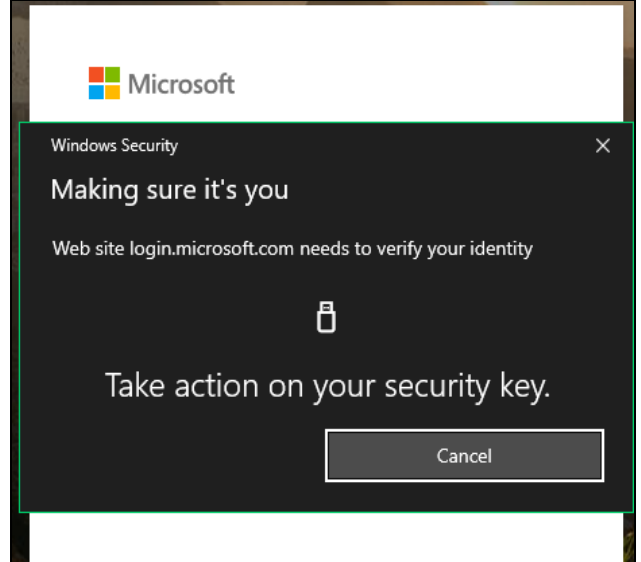
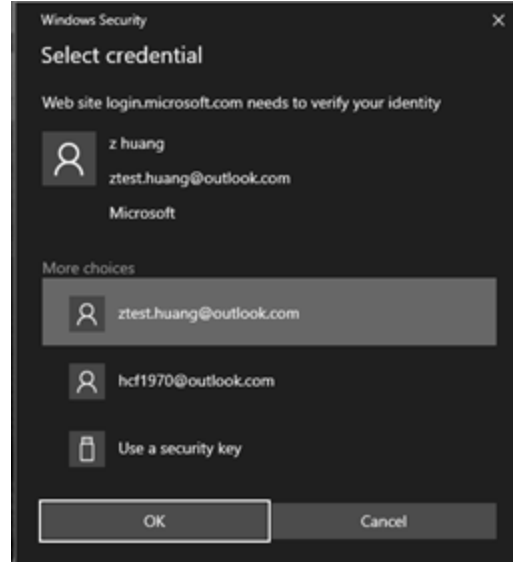
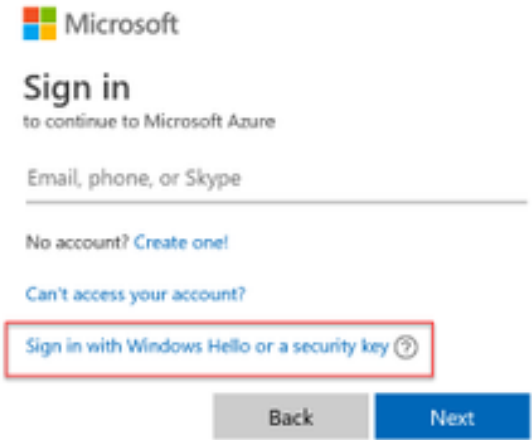


▶ **Możesz znaleźć wszystkie zarejestrowane klucze, kliknąc "Zarządzaj metodami logowania"**

Manage your sign-in methods			
NAME	SIGN-IN METHODS	ADDED ON	LAST USED
ATKey.card-0180007F	 Security key	1/16/2019 8:40 AM	1/16/2019 8:40 AM

▶ **Wyloguj się w celu zalogowania się za pomocą klucza**

**zabezpieczeń (bez hasła)**





ATKey.Pro ma certyfikat FIDO2, może być kluczem zabezpieczeń do uwierzytelniania dwuskładnikowego.



Możesz też wyszukać i znaleźć dostępny serwer z certyfikatem FIDO U2F

tutaj: <https://fidoalliance.org/certification/fido-certified-products/?appSession=8YT7Z25V0DOH6M41OQG26WI22N0F6D5MF9W19F58545OZWKJPBOH5XMB874A6596S8432G491GGF12B5Y7PIAM6PKR09S5G9Z3Q9T0FLK91C5445079DO1NWZFP8714Q>

But, Tylko przeglądarka Chrome

Wyszukiwarka Google:

Włączanie weryfikacji 2-etapowej,

<https://support.google.com/accounts/answer/185839?co=GENIE.Platform%3DDesktop&hl=en>

Użyj klucza bezpieczeństwa do weryfikacji

dwuetapowej, <https://support.google.com/accounts/answer/6103523?co=GENIE.Platform%3DAndroid&hl=en>

Facebook: <https://www.facebook.com/help/148233965247823>

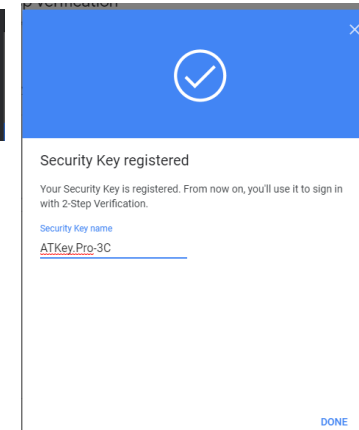
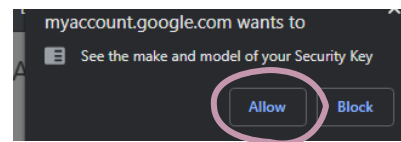
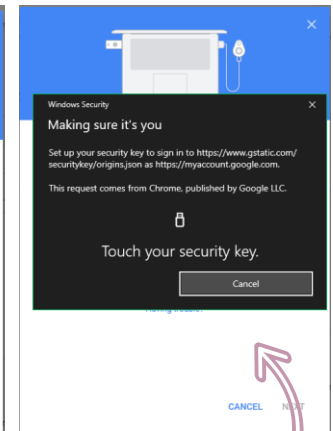
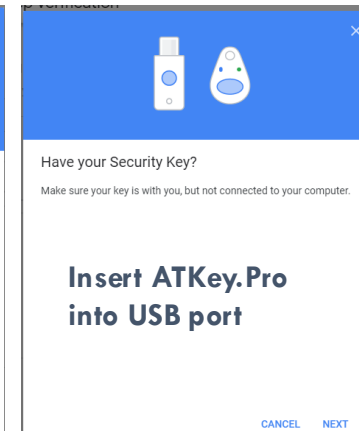
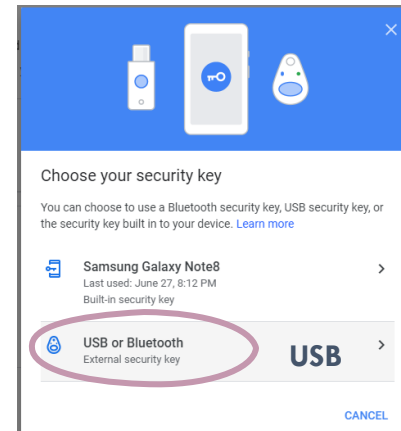
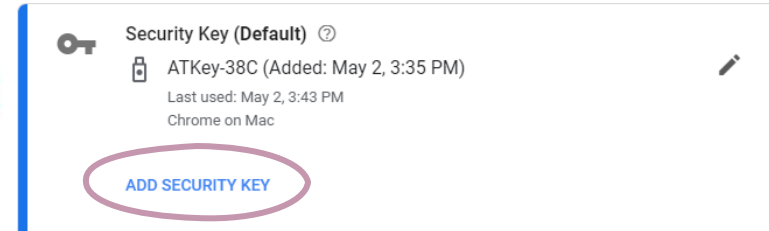
Gitlab: Włącz 2FA za pomocą urządzenia

U2F, [https://docs.gitlab.com/ee/user/profile/account/two\\_factor\\_authentication.html](https://docs.gitlab.com/ee/user/profile/account/two_factor_authentication.html)

Salesforce: [https://help.salesforce.com/articleView?id=security\\_u2f\\_enable.htm&type=5](https://help.salesforce.com/articleView?id=security_u2f_enable.htm&type=5)

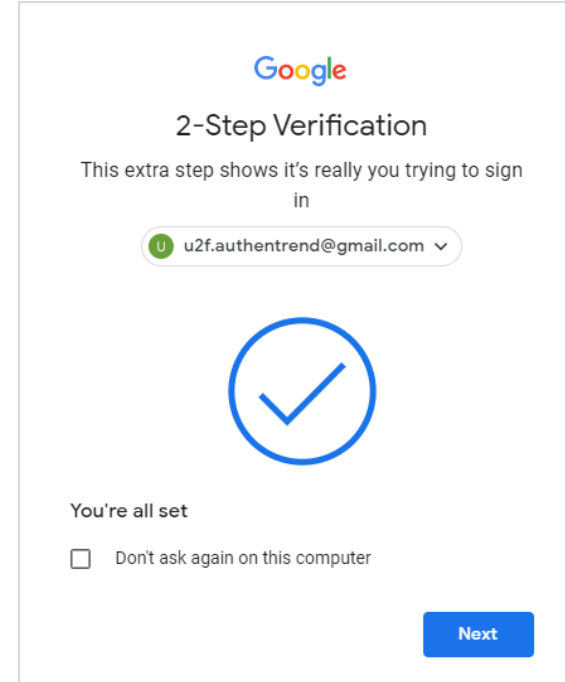
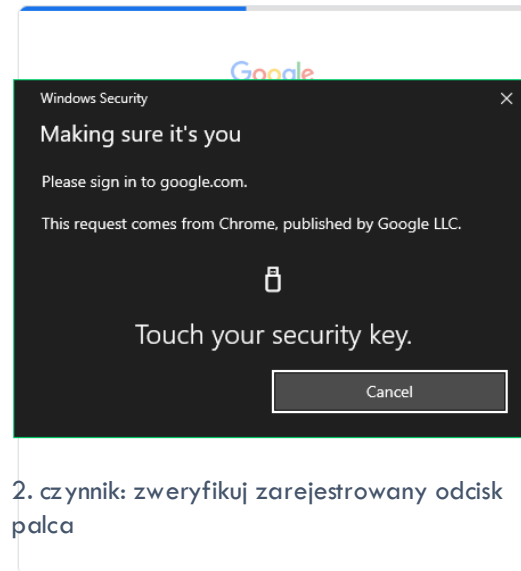
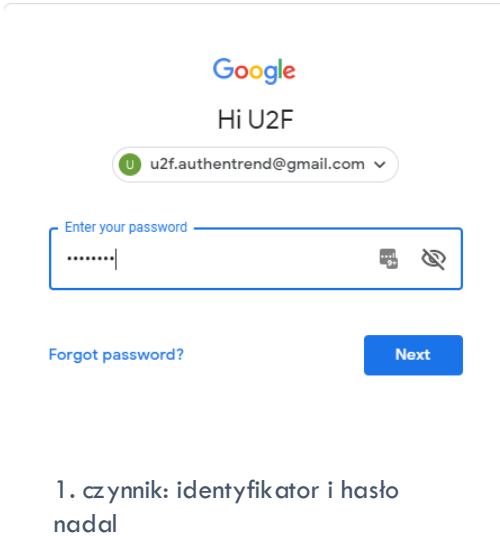
Dropbox: <https://help.dropbox.com/teams-admins/team-member/enable-two-step-verification>

(Np.) Konto Google – dodaj ATKey.Pro jako zabezpieczenie do konta Google:

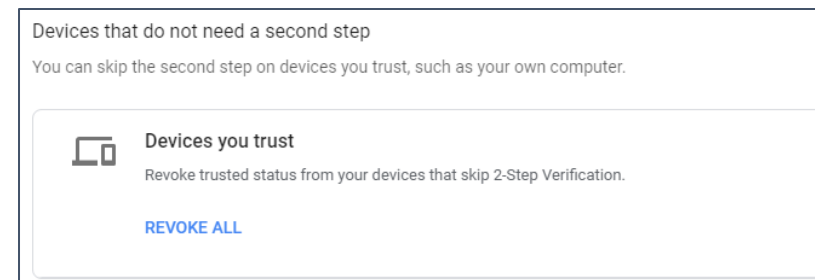


Dotknij zarejestrowanego odcisku palca, aby zweryfikować

- (Np.) Konto Google – zaloguj się przez ATKey.Pro

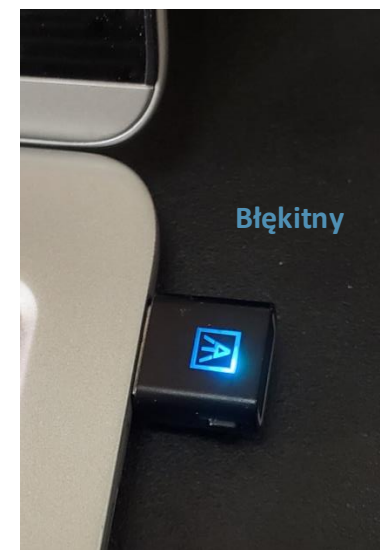
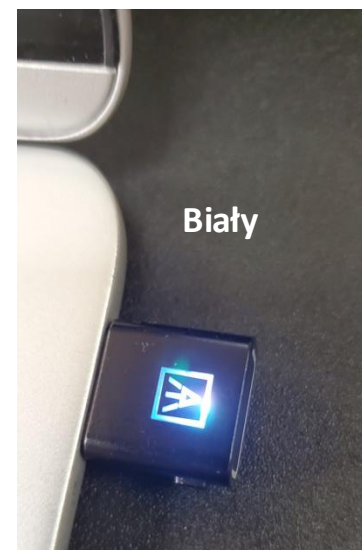
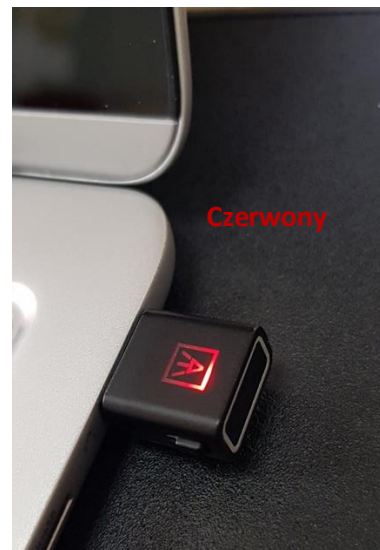
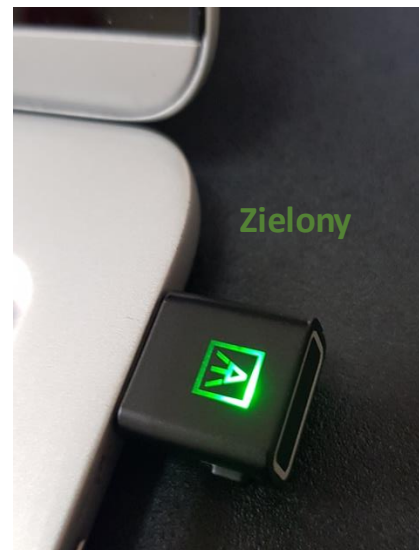
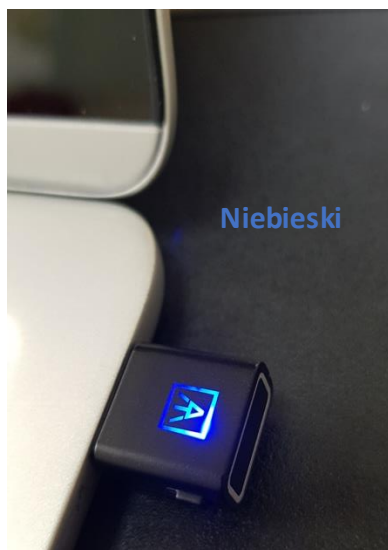


Gotowe i zaloguj się!  
 Jeśli chcesz zalogować się na swoje konto Google za pomocą ATKey.Pro później, odznacz "Nie pytaj ponownie na tym komputerze" (domyślnie jest to zaznaczone).  
 Ale jeśli sprawdziłeś i zalogowałeś się, ale chcesz użyć ATKey.Pro jako drugiego składnika, aby zalogować się ponownie, odwołaj wszystkie "urządzenia, którym ufasz", jak poniżej:





- Do 10 odcisków palców, gdy jest pełny (10 odcisków palców), użytkownik nie może zarejestrować nowych palców.
- W przypadku nowej rejestracji odcisku palca zawsze wymagana jest autoryzacja na podstawie zarejestrowanych odcisków palców (najpierw sprawdź za pomocą zarejestrowanego odcisku palca).
- Aby zarejestrować odcisk palca, użytkownicy muszą dotykać czujnika w sposób ciągły około 12 razy, aby ukończyć "szablon".
- Zgodnie ze specyfikacją FIDO2 preferowane jest dodanie kodu PIN do ATKey.Pro; użytkownik może dodać kod PIN do ATKey.Pro za pomocą ustawień systemu Windows (kompilacje 1903 lub nowsze) lub dodając z ATKey dla systemu Windows (wersja 2.0.58.0 lub nowsza).
- Zgodnie ze specyfikacją FIDO2, pozwala na 3-krotną ciągłą awarię podczas jednego "cyklu" (diody LED będzie statyczna na CZERWONO), użytkownik musi usunąć klucz sprzętowy z hosta i ponownie włożyć go na kolejny cykl; jeśli nie powiedzie się przez 5 cykli w sposób ciągły, klucz zostanie zablokowany; Użytkownik może zresetować go ręcznie.



<p>LED Miga</p>	<p>Dotknij zarejestrowanego odcisku palca, aby go zweryfikować</p>			<p>Rejestracja samodzielna (od wolnego do szybkiego, a następnie wykonywane przez ZIELONY, co oznacza zapisany odcisk palca zweryfikowany PASS); Kalibracja odcisków palców (na biało, wraca do niebieskiego)</p>	<p>Wymaga dotyku użytkownika (ale każdy palec jest w porządku)</p>
<p>Stacyjny włączony</p>	<p>Zasilanie włączone, stan normalny</p>	<p>Odcisk palca zweryfikowany PASS (na sekundę)</p>	<ul style="list-style-type: none"> <li>• Weryfikacja odcisku palca nie powiodła się</li> <li>• Wymaż odcisk palca</li> <li>• resetowania</li> </ul>	<ul style="list-style-type: none"> <li>• Kalibracja czytnika linii papilarnych</li> <li>• Włącz zasilanie, ale rozruch oprogramowania układowego nie powiódł się</li> </ul>	

# Certification

In recognition of Authentrend's achievement of FIDO2® Certification

**Company:** Authentrend

**Product:** ATKey.Pro

**Specification:** FIDO2

**Specification Version:** 2.0 (2018-07-02)

**Implementation Class:** Authenticator

**Level:** L1

**Functional Policy Version:** 1.3.7

**Authenticator Policy Version:** 1.1.1

**Security Requirements Version:** 1.3

**Interoperability Date:** September 10<sup>th</sup>, 2019

**Conformance Self-Validation Date:** September 9<sup>th</sup>, 2019

**VQ Approval Date:** October 8<sup>th</sup>, 2019

**Derivative:** No

**Source Certificate(s):** N/A



Certificate No.


FIDO20020191008001


Issued


October 8<sup>th</sup>, 2019



 [www.authentrend.com](http://www.authentrend.com)

 [contact@authentrend.com](mailto:contact@authentrend.com)

 [AuthenTrend](#)

 [AuthenTrend](#)

**AUTHENTREND**