Zmiana sposobu logowania do aplikacji CEIDG

Od 15 marca 2021 r. logowanie do Aplikacji urzędnika jest możliwe jedynie za pośrednictwem systemu Login.gov.pl (Węzeł Krajowej Identyfikacji Elektronicznej) z wykorzystaniem dostępnych tam metod identyfikacji, w tym Profilu Zaufanego i usług bankowości elektronicznej.
Zmiana wynika m.in. z tego, że logowanie na stronach rządowych GOV.PL powinno być spójne, bezpłatne i zgodne z prawem europejskim.

UWAGA: Zmiana sposobu logowania nie wpłynie na uprawnienia i dostępy nadane urzędnikom – wszystkie ustawienia zostaną zachowane. Zmieni się tylko sposób identyfikacji użytkownika przy logowaniu.

Posiadany certyfikat kwalifikowany nadal może być wykorzystywany do podpisywania wniosków w CEIDG.

Jeśli nie posiadasz jeszcze Profilu Zaufanego, załóż go tutaj (link do Login.gov.pl) https://pz.gov.pl/pz/registerMainPage.

Jeśli nie pamiętasz loginu i hasła do Profilu Zaufanego, zachęcamy do kontaktu z pomocą techniczną: https://pz.gov.pl/pz/contact

Pytania i odpowiedzi na temat logowania się do Aplikacji urzędnika za pomocą m.in. Profilu Zaufanego (PZ)

1. **Czy jeśli posiadam prywatny PZ logując się do banku, muszę mieć również osobny Profil Zaufany przypisany pod urząd gminy?**

Profil Zaufany jest przypisany do osoby fizycznej. Oznacza to, że bez względu na to, czy podpisują Państwo prywatny dokument, czy wniosek przedsiębiorcy jako pracownik urzędu, to używają Państwo tego samego narzędzia, w ten sam sposób. W Profilu Zaufanym można dodać informację o tym, że jest się pracownikiem danego urzędu, ale wciąż będzie to profil prywatny, a nie urzędowy.

W systemie CEIDG będą Państwo weryfikowani na podstawie numeru PESEL oraz nadal będą Państwo logować się do swojego konta urzędnika, dlatego też dopisanie danych urzędu do PZ nie będzie miało znaczenia.

2. **Czy logowanie poprzez Profil Zaufany do aplikacji urzędnika wiąże się z potrzebą wykorzystywania telefonu komórkowego, np. telefonu służbowego?**

Logowanie Profilem Zaufanym wymaga autoryzacji, którą użytkownik wybiera sam podczas zakładania Profilu Zaufanego. Profil Zaufany, który nie jest powiązany z bankiem, wymaga odbierania sms-ów z hasłem. Profil Zaufany powiązany z bankiem wymaga weryfikacji zgodnej z polityką banku: może to być sms lub inna forma przesłania hasła, np. kody jednorazowe z karty kodów.

3. **Proszę o wyjaśnienie co ma na celu zmiana sposobu logowania do CEIDG, ponieważ Profil Zaufany jest zakładany dla prywatnej osoby, a nie dla pracownika urzędu. Konieczność założenia PZ będzie wiązała się z zakupem telefonu służbowego dla każdego pracownika. Założenie profilu do celów CEIDG uniemożliwi korzystanie z niego prywatnie. Ponadto odbieranie smsów w trakcie obsługi klienta przez urzędnika naraża nas na wysłuchiwanie nieprzyjemnych komentarzy.**

Profil Zaufany jest przypisany do osoby fizycznej i nie ma żadnych przeciwskazań do tego, by używać go jednocześnie do celów prywatnych oraz do celów służbowych - nie ma tu konfliktu interesów. W taki sam sposób mogą się Państwo podpisać tym samym długopisem zarówno na dokumencie służbowym, jak i na prywatnym. Oba podpisy należą do konkretnej osoby, nie do jej stanowiska.

Nie ma też potrzeby kupowania telefonów służbowych, gdyż sms-y z Profilu Zaufanego powinny przychodzić na telefon prywatny. Odbieranie sms-ów koniecznych do podpisania wniosku w czasie pracy również nie stanowi problemu. Dokładnie w ten sam sposób pracuje obecnie większość urzędników obsługujących CEIDG oraz wszyscy lekarze wystawiający zwolnienia lekarskie lub e-recepty. Każdemu pytającemu o powód odebrania sms-a wystarczy przekazać, że jest to kod weryfikacyjny konieczny do załatwienia jego sprawy.

4. **Czy pracodawca jest bezpieczny skoro swoimi Profilami Zaufanymi w pełni dysponują pracownicy realizujący obowiązki zawodowe?**

Tak – pracodawca bowiem mając kontrolę nad systemem, w którym można potwierdzać tożsamość Profilem Zaufanym tak konfiguruje system, aby nadać uprawnienia tylko określonym osobom. Zatem gdyby do systemu chciał zalogować się za pomocą PZ ktoś, kto nie ma uprawnień, to system to rozpozna i nie pozwoli na zalogowanie. Przykładowo każdy może zalogować się Profilem Zaufanym do Internetowego Konta Pacjenta (na stronie https://pacjent.gov.pl/) ale do portalu https://gabinet.gov.pl/ do którego logowanie jest również możliwe za pomocą PZ, dostają się już tylko osoby uprawnione, pracujące w systemie ochrony zdrowia. Te dwa portale dobrze obrazują, że w zależności od tego gdzie używany jest PZ lekarz używa go jako pacjent albo jako lekarz – w obu przypadkach mając pełną kontrolę nad swoją e-tożsamością używaną w Internecie. Znaczenie ma również to, że nie ma potrzeby pamiętać różnych sposobów logowania do różnych miejsc.

Dwuskładnikowy Profil Zaufany jest na tyle bezpieczny (hasło znane tylko posiadaczowi PZ i telefon będący pod jego kontrolą), że pozwala na dostęp do danych w różnych systemach.

5. **Dlaczego przy zakładaniu Profilu Zaufanego istotne jest podanie numeru własnego (prywatnego) telefonu komórkowego i własnego (prywatnego) adresu poczty elektronicznej?**

Profil Zaufany pozwala na potwierdzenie tożsamości w usługach publicznych w Internecie bez względu na to, czy jego posiadacz występuje jako:

a) osoba fizyczna reprezentująca siebie,

b) osoba fizyczna reprezentująca podmiot publiczny, w którym pracuje.

Aby lepiej wyjaśnić dlaczego w obu powyższych przypadkach kluczowe jest, aby zarówno telefon jak i adres poczty elektronicznej były pod pełną kontrolą osoby posiadającej Profil Zaufany, trzeba wyjaśnić do czego oba powyższe elementy są potrzebne.

Profil Zaufany można używać bezpośrednio (wtedy logujemy się za pomocą identyfikatora użytkownika i hasła, które sami ustalamy na etapie rejestracji) lub pośrednio - używając tego samego sposobu logowania jakiego używamy w usługach bankowości elektronicznej lub Poczty Polskiej (tzw. konto Envelo).

Aby Profil Zaufany był bezpieczny i aby zlecić w systemie teleinformatycznym jakąkolwiek dyspozycję, nie wystarczy tylko się zalogować. Logowanie to tylko pierwszy klucz do Profilu Zaufanego. Każda operacja, w której wyrażamy swoją wolę wymaga dodatkowego zabezpieczenia (drugiego klucza), tak skonstruowanego aby było wiadomo, że klucz ten posiada i zarządza nim wyłącznie posiadacz Profilu Zaufanego. W przypadku PZ tym drugim kluczem jest numer telefonu komórkowego, na który wysyłane są jednorazowe poufne kody potrzebne do zlecenia określonego działania.

Przykładowo lekarz zalogowany do systemu ZUS wystawiający zwolnienie lekarskie celem potwierdzenia tego zwolnienia z wykorzystaniem Profilu Zaufanego potrzebuje drugiego klucza – jednorazowego kodu przesłanego sms-em. Ten sam lekarz, gdy używa PZ jako osoba fizyczna (tego samego profilu zaufanego), aby złożyć zeznanie podatkowe, zawnioskować o dowód osobisty czy podpisać jakikolwiek inny dokument online w prywatnej sprawie, również potrzebuje użyć drugiego klucza, czyli odebrać kody jednorazowe przesyłane smsem. Należy zauważyć, że zarówno odpowiedzialność lekarza przy wystawianiu zwolnień, jak i oczywista potrzeba pełnej kontroli nad dostępem do jego danych w portalu podatkowym, skutkuje tym, że nie do przyjęcia jest aby to pracodawca lekarza mógł odbierać smsy z kodami jednorazowymi. Nawet gdyby telefon był przez pracodawcę wypożyczony, to w każdej chwili ten pracodawca mógłby zażądać jego zwrotu, nie mówiąc już o wypowiedzeniu umowy firmie telekomunikacyjnej. Spowodowałaby to utratę kontroli osoby fizycznej nad jej profilem zaufanym.

6. Czy logowanie do Profilu Zaufanego za pomocą bankowości elektronicznej jest bezpieczne?

Banki działają w ramach przepisów ustawy Prawo bankowe, która nakłada na nie szczególne obwiązki w zakresie rozpoznawania tożsamości klientów.

Nie bez znaczenia jest to, że korzystając z internetowego konta bankowego nauczyliśmy się jak to robić bezpiecznie, właśnie po to aby nie utracić kontroli nad swoimi finansami. Korzystanie

z pośrednictwa konta bankowego jest dla wielu użytkowników także wygodne. Pozwala im się logować w sposób znany i co za tym idzie, przyjazny.

7. Czy bank wie, gdzie wykorzystujemy Profil Zaufany używany za jego pośrednictwem?

Nie ma takiej wiedzy - bank wie jedynie, kiedy użyliśmy Profilu Zaufanego, ale nie wie już do czego został on użyty. Niektórzy użytkownicy wolą jednak, aby ich bank w ogóle nie wiedział nawet tego, że Profil Zaufany jest używany. Takie osoby mogą odłączyć PZ od banku.

8. Jeśli chciałbym odłączyć Profil Zaufany od banku, jak to zrobić?

Należy zalogować się na stronie https://pz.gov.pl/ (oczywiście za pośrednictwem banku), a następnie kolejno:

1) wybrać „Mój profil zaufany”.
2) zanotować wyświetloną nazwę użytkownika (jeżeli jej nie pamiętamy)
3) wybrać „Przedłuż ważność”
4) wykonać kolejno potrzebne czynności (podać adres email i nr telefonu komórkowego i potwierdzić to kodem jednorazowym)
5) jeszcze raz przejść do aplikacji banku, aby potwierdzić odłączenie.

Po wykonaniu tych operacji można się już logować za pomocą nazwy użytkownika i hasła bez pośrednictwa banku. Należy pamiętać, że hasło nie jest tym samym hasłem co w systemie banku. Aby ustalić hasło należy po wybraniu „Zaloguj” na stronie https://pz.gov.pl/ podać nazwę użytkownika (te z pkt 2) i wybrać opcję "Nie pamiętam hasła”. Na nasz adres poczty przyjdzie wiadomość pozwalająca na ustalenie hasła. Dlatego tak ważne jest aby również adres poczty elektronicznej powiązany z naszym Profilem Zaufanym był naszym adresem prywatnym, a nie adresem służbowym od pracodawcy.

9. Jak potwierdzić Profil Zaufany bez wychodzenia z domu?

W związku z pandemią koronawirusa, zachęcamy do potwierdzania Profilu Zaufanego:

- za pośrednictwem konta w systemie polskiego banku, który ma zgodę na potwierdzanie Profilu Zaufanego (ich lista znajduje się na stronie https://pz.gov.pl/dt/registerByXidp);
- za pomocą kwalifikowanego podpisu elektronicznego - ta opcja wymaga zainstalowanego wcześniej oprogramowania PZ Signer;

Pliki instalatora dla poszczególnych systemów operacyjnych znajdują się poniżej:

Windows64: https://epuap.gov.pl/signing/plugin/win64/PKSigner.exe

Windows32: https://epuap.gov.pl/signing/plugin/win32/PKSigner.exe

Linux: https://epuap.gov.pl/signing/plugin/linux/PKSigner-installer.sh

macOS: https://epuap.gov.pl/signing/plugin/osx/PKSigner.dmg

- za pomocą nowego dowodu osobistego z warstwą elektroniczną - ta opcja wymaga posiadania czytnika umożliwiającego połączenie dowodu z komputerem (tzw. czytnik NFC) oraz zainstalowanego wcześniej oprogramowania e-dowodu;

Przypominamy, że PZ można założyć także za pośrednictwem Poczty Polskiej (link: https://www.envelo.pl/profil-zaufany-epuap/). Dostępna jest także e-usługa umożliwiająca założenie

tymczasowego profilu zaufanego (TPZ). Taki profil jest ważny 3 miesiące (tradycyjny jest ważny 3 lata). Potwierdzenie tymczasowego profilu zaufanego odbywa się w trakcie wideospotkania z urzędnikiem. Sprawdź, jak założyć tymczasowy profil zaufany.

10. Jaka jest podstawa prawna wprowadzonej zmiany logowania do aplikacji CEIDG, np. przez Profil Zaufany?

Zmiany, które przeprowadzamy, są etapem modernizacji rejestru CEIDG i odpowiadają zasadom wdrażanym w innych usługach administracji publicznej zgodnie z eIDAS.
Sama zmiana logowania jest decyzją biznesową, której celem jest zapewnienie bezpieczeństwa, spójności sposobu logowania i wykorzystanie darmowych, publicznych rozwiązań.
W realizacji usług elektronicznych - również usług CEIDG - użytkownik przechodzi przez dwa etapy:

1. Identyfikacja elektroniczna, tzw. uwierzytelnianie ("logowanie do systemu") - tu wykorzystywane są środki do identyfikacji. W usługach publicznych taką identyfikację zapewnia Węzeł Krajowy https://login.gov.pl/login/main, a w nim dostępny np. Profil Zaufany;
2. Podpisywanie (wykorzystanie usług zaufania) - tu natomiast różnego rodzaju metody, dostępne i zgodne z przepisami prawa - podpisy np. Podpis zaufany, Podpis kwalifikowany, Podpis osobisty (na e-Dowodzie).

Należy zaznaczyć, że podpis elektroniczny nie służy do identyfikacji podpisującego. Środki identyfikacji są przywiązane bowiem bezpośrednio do osoby, którą identyfikują, dlatego też mogą one wymagać określonych poziomów zabezpieczeń, czyli np. przepisania hasła wysyłanego na telefon. Ten etap służy do identyfikacji osoby, a nie pracownika jako takiego.

11. Czy ze względu na nowy sposób logowania do CEIDG, urzędnik ma obowiązek założenia Profilu Zaufanego? Czy pracodawca może jakoś "zmusić" pracownika do założenia PZ, skoro pracownik nie ma potrzeby posiadania PZ, lub nie chce używać prywatnego PZ do celów służbowych. Czy w takim wypadku jeżeli jest to prywatny PZ, pracownik popołudniu w domu może takie wnioski przetwarzać np. znajomym? Logowanie do CEIDG przebiega u mnie przy pomocy PZ przez bank, nie chciałbym zmieniać sposobu logowania na login i hasło ze względu na to, że logowanie przez bank jest bardziej bezpieczne (w prywatnych logowaniach).

Profil Zaufany zakłada dla siebie osoba fizyczna. Nie ma znaczenia, czy jest pracownikiem urzędu, stacji benzynowej, studentem, czy emerytem. Identycznie jest w przypadku certyfikatu kwalifikowanego, który również należy do osoby fizycznej, a nie do urzędu. Nie ma "nieprywatnych" Profili Zaufanych.
Pracodawca nie może wymagać od pracownika założenia osobnego Profilu Zaufanego do celów służbowych, ponieważ jest to technicznie niemożliwe. Może natomiast oczekiwać, że pracownik realizujący zadania wymagające użycia Profilu Zaufanego, taki profil uzyska i będzie się nim posługiwać. Obowiązek logowania się do CEIDG wyłącznie Profilem Zaufanym dla osoby pracującej przy obsłudze CEIDG jest właśnie taką potrzebą, o której Pan pisze.
Kwestia przyjmowania wniosków po pracy jest identyczna dla logowania certyfikatem oraz profilem.

Jeśli zabierze Pan swój certyfikat z urzędu i będzie Pan wprowadzał wnioski w domu, to będzie to dokładnie taka sama czynność, jak przy logowaniu Profilem Zaufanym. Jeśli urząd, w którym Pan pracuje, przyjął taką formę pracy zdalnej i jest Pan w stanie zapewnić bezpieczeństwo danych znajdujących się na wnioskach papierowych oraz na Pańskim komputerze w domu, to nie ma tu absolutnie żadnej różnic. Dlatego też jeśli nie robi Pan tego teraz, to nie ma powodu by nagle miał Pan zacząć wykonywać takie czynności po 15 marca 2021 r., ponieważ zmiana sposobu logowania nie wpływa na to, w jaki sposób obsługuje Pan przedsiębiorców.
Nie musi Pan zmieniać metody logowania z bankowości elektronicznej na sms. To od użytkownika Profilu Zaufanego zależy jaką formę wybierze i jeśli logowanie przez bank jest dla Pana wygodnie, to może Pan przy nim pozostać.