INSTRUKCJA ADMINISTRATORA

Generowanie certyfikatu niekwalifikowanego

dla instancji testowej systemu EZD RP

System:	EZD RP – Elektroniczne Zarządzanie Dokumentacją Rzeczypospolitej Polskiej
Dokument:	Instrukcja konfiguracji podpisu niekwalifikowanego
Przeznaczenie:	Administrator merytoryczny EZD RP
Środo wisko:	**WYŁĄCZNIE instancja testowa / szkoleniowa**
Opracowanie:	Lubelskie Centrum Innowacji i Technologii (LCIT)
Data:	Maj 2026

⚠ UWAGA — WYŁĄCZNIE DO CELÓW TESTOWYCH!
Certyfikat niekwalifikowany wygenerowany tą metodą nie posiada mocy prawnej.
Nie używaj go w systemie produkcyjnym ani do podpisywania dokumentów oficjalnych.
Stosuj wyłącznie na instancji testowej lub szkoleniowej EZD RP.

1. CEL I ZAKRES DOKUMENTU

Niniejsza instrukcja jest przeznaczona dla administratorów merytorycznych systemu EZD RP, którzy przygotowują środowisko testowe lub szkoleniowe do przeprowadzania ćwiczeń z pracownikami.

Dokument opisuje krok po kroku, jak:

- wygenerować certyfikat niekwalifikowany (self-signed) przy użyciu programu Adobe Acrobat Reader DC,
- zaimportować certyfikat do magazynu certyfikatów systemu Windows,
- skonfigurować podpis niekwalifikowany na koncie użytkownika w EZD RP,
- zarządzać certyfikatami dla wielu kont kierowniczych przed szkoleniem.

Certyfikat niekwalifikowany umożliwia symulowanie procesu podpisywania dokumentów na kontach kierowniczych podczas ćwiczeń pracowników w systemie — bez konieczności posiadania kwalifikowanego certyfikatu elektronicznego.

2. WYMAGANIA WSTĘPNE

Przed przystąpieniem do konfiguracji upewnij się, że spełnione są następujące wymagania:

Oprogramowanie

Wymaganie	Wersja / szczegół	Status
Adobe Acrobat Reader DC	Wersja bezpłatna (Reader) lub płatna (Acrobat)	**WYMAGANE**
System operacyjny Windows	Windows 10 lub Windows 11 (64-bit)	**WYMAGANE**
Dostęp do EZD RP (instancja testowa)	Konto z rolą administratora merytorycznego	**WYMAGANE**
Przeglądarka internetowa	Google Chrome (zalecana) lub Edge	**WYMAGANE**
Uprawnienia administratora Windows	Do instalacji certyfikatu w magazynie	OPCJONALNE

ℹ Adobe Acrobat Reader DC jest dostępny bezpłatnie na stronie: https://get.adobe.com/reader/
Upewnij się, że korzystasz z aktualnej wersji programu (2024 lub nowszy).

Dane potrzebne do wypełnienia certyfikatu

Przygotuj następujące dane dla każdego użytkownika, dla którego tworzysz certyfikat:

- Imię i Nazwisko użytkownika (dokładnie jak w EZD RP),
- Jednostka organizacyjna (np. Dział IT, Sekretariat),
- Nazwa organizacji (np. Muzeum Zamek w Janowcu),
- Adres e-mail użytkownika (jak w systemie),
- Hasło do zabezpieczenia pliku .pfx (zapamiętaj je — będzie potrzebne przy imporcie).

3. CZYM JEST CERTYFIKAT NIEKWALIFIKOWANY W EZD RP?

System EZD RP obsługuje kilka rodzajów podpisów elektronicznych. Do celów testowych i szkoleniowych stosuje się podpis niekwalifikowany, który nie wymaga posiadania zewnętrznego certyfikatu od centrum certyfikacji.

Cecha	Podpis KWALIFIKOWANY	Podpis NIEKWALIFIKOWANY (testowy)
Moc prawna	TAK — równoważny podpisowi własnoręcznemu	NIE — wyłącznie do celów testowych
Certyfikat	Wydany przez akredytowane centrum certyfikacji	Samopodpisany (self-signed), generowany lokalnie
Koszt	Płatny (karta kryptograficzna + certyfikat)	Bezpłatny — generowany w Adobe Reader
Zastosowanie	Dokumenty oficjalne w systemie produkcyjnym	Ćwiczenia i szkolenia w instancji testowej
Wymagany sprzęt	Czytnik kart + karta kryptograficzna	Komputer z systemem Windows + Adobe Reader

✓ Certyfikat niekwalifikowany jest idealnym rozwiązaniem dla fazy szkoleniowej projektu EZD RP. Umożliwia administratorowi przygotowanie kont kierowniczych do symulowania podpisywania dokumentów przed uruchomieniem produkcyjnym, kiedy pracownicy nie mają jeszcze certyfikatów kwalifikowanych.

4. CZĘŚĆ I — GENEROWANIE CERTYFIKATU W ADOBE ACROBAT READER

Poniższe kroki opisują proces tworzenia nowego cyfrowego identyfikatora (certyfikatu self-signed) bezpośrednio w programie Adobe Acrobat Reader DC. Czynności należy wykonać na komputerze użytkownika, który będzie podpisywał dokumenty.

⚠ Wykonaj te kroki na KAŻDYM komputerze użytkownika, dla którego chcesz skonfigurować podpis niekwalifikowany.

1	**Otwórz ustawienia programu Adobe Acrobat Reader DC** Uruchom Adobe Acrobat Reader DC. W menu górnym wybierz: Edycja → Preferencje (lub naciśnij skrót klawiszowy Ctrl+K).
2	**Przejdź do ustawień tożsamości i certyfikatów** W oknie Preferencje, w kolumnie po lewej stronie, kliknij kategorię [Podpisy]. Następnie w sekcji [Tożsamości i certyfikaty zaufane] kliknij przycisk [Więcej...].
3	**Dodaj nowy identyfikator elektroniczny** W oknie [Cyfrowy identyfikator i certyfikaty zaufane] upewnij się, że po lewej stronie zaznaczona jest opcja [Identyfikatory cyfrowe]. Kliknij przycisk [Dodaj ID] (ikona plusa lub przycisk w górnym pasku).
4	**Wybierz typ nowego identyfikatora** Wyświetli się kreator. Zaznacz opcję: [Nowy identyfikator elektroniczny, który chcę utworzyć teraz]. Kliknij przycisk [Dalej].
5	**Wybierz miejsce przechowywania** Zaznacz opcję: [Nowy plik cyfrowego ID PKCS#12]. Plik z rozszerzeniem .pfx zostanie zapisany na dysku. Kliknij [Dalej].
6	**Wypełnij dane tożsamości certyfikatu** Wypełnij formularz danymi użytkownika: Imię i nazwisko, Jednostka organizacyjna, Nazwa organizacji, Adres e-mail. W polu Kraj wybierz: PL - POLSKA. Algorytm klucza: 2048-bitów RSA. Użyj dla: Podpisy elektroniczne i kodowanie danych. Kliknij [Dalej].

7	**Ustaw lokalizację pliku i hasło** Wskaż folder, gdzie ma zostać zapisany plik .pfx (np. Pulpit lub dedykowany folder). Wpisz hasło dostępu do pliku (minimum 6 znaków). Powtórz hasło w polu potwierdzenia. ZAPAMIĘTAJ hasło — będzie wymagane przy każdym imporcie! Kliknij [Zakończ].

✓ Po kliknięciu [Zakończ] plik .pfx pojawi się w wybranej lokalizacji.
Certyfikat jest jednocześnie automatycznie rejestrowany w Adobe Reader.
Możesz go zobaczyć na liście [Identyfikatory cyfrowe] w ustawieniach podpisów.

ℹ Nazwa pliku .pfx powinna zawierać imię i nazwisko użytkownika dla ułatwienia zarządzania.
Przykład: Jan_Kowalski_EZD_test.pfx
Przechowuj pliki .pfx w bezpiecznym miejscu — zawierają klucz prywatny użytkownika.

5. CZĘŚĆ II — IMPORTOWANIE CERTYFIKATU DO MAGAZYNU CERTYFIKATÓW WINDOWS

Po wygenerowaniu pliku .pfx należy go zaimportować do magazynu certyfikatów systemu Windows. Ten krok jest konieczny, aby przeglądarka internetowa (Chrome/Edge) mogła przekazać certyfikat do systemu EZD RP.

ℹ Jeśli certyfikat był generowany na tym samym komputerze, plik .pfx jest już dostępny lokalnie. Jeśli tworzysz certyfikaty dla innych użytkowników — skopiuj odpowiedni plik .pfx na ich komputer przed importem.

8	**Otwórz Kreatora importu certyfikatów** Przejdź do folderu, gdzie zapisano plik .pfx. Kliknij dwukrotnie na plik .pfx. Uruchomi się systemowy [Kreator importu certyfikatów] systemu Windows.
9	**Wybierz zakres magazynu** Kreator zapyta: [Gdzie chcesz przechowywać certyfikat?]. Zaznacz opcję: [Bieżący użytkownik] (nie [Komputer lokalny]). Kliknij [Dalej].
10	**Potwierdź ścieżkę do pliku** W kolejnym kroku ścieżka do pliku .pfx zostanie uzupełniona automatycznie. Sprawdź, czy jest poprawna i kliknij [Dalej].
11	**Podaj hasło i ustaw opcje klucza** Wpisz hasło, które zostało ustawione podczas tworzenia certyfikatu w Adobe Reader. WAŻNE: Zaznacz pole [Oznacz ten klucz jako eksportowalny] — umożliwi to ewentualny eksport certyfikatu w przyszłości. Kliknij [Dalej].
12	**Wybierz magazyn certyfikatów** Zaznacz opcję: [Umieść wszystkie certyfikaty w następującym magazynie]. Kliknij przycisk [Przeglądaj...]. W oknie wyboru zaznacz: [Osobisty] (ang. Personal). Kliknij [OK], następnie [Dalej].
13	**Zakończ import** Kreator wyświetli podsumowanie. Magazyn certyfikatów: Osobisty. Sprawdź poprawność danych i kliknij [Zakończ]. System wyświetli komunikat: [Import został ukończony pomyślnie].

✓ Import zakończony pomyślnie! Certyfikat jest teraz dostępny w magazynie [Osobisty] systemu Windows i może być używany przez przeglądarki Chrome i Edge.

Jak sprawdzić, czy certyfikat jest w magazynie Windows?

Aby zweryfikować poprawność importu:

- Naciśnij Win+R i wpisz: certmgr.msc → Enter
- Przejdź do: Certyfikaty — bieżący użytkownik → Osobisty → Certyfikaty
- Na liście powinien pojawić się certyfikat z imieniem i nazwiskiem użytkownika

6. CZĘŚĆ III — KONFIGURACJA PODPISU W SYSTEMIE EZD RP

Ostatni etap polega na przypisaniu certyfikatu do konta użytkownika w systemie EZD RP. Czynności należy wykonać na koncie użytkownika w przeglądarce internetowej.

⚠ KRYTYCZNA UWAGA — SPOSÓB ZAPISU USTAWIEŃ!
W systemie EZD RP konfiguracja podpisu jest zapisywana w niekonwencjonalny sposób.
Po kliknięciu OK przy wyborze certyfikatu NIE klikaj przycisku [Zapisz] w ustawieniach!
Zamiast tego — ODŚWIEŻ stronę przeglądarki (F5 lub Ctrl+R).
Kliknięcie [Zapisz] może spowodować utratę ustawień certyfikatu.

14	**Zaloguj się do EZD RP na koncie użytkownika** Otwórz przeglądarkę internetową (Chrome lub Edge). Przejdź do adresu testowej instancji EZD RP. Zaloguj się na konto użytkownika, dla którego konfigurowany jest podpis.
15	**Przejdź do ustawień konta** Po zalogowaniu kliknij na imię i nazwisko użytkownika wyświetlane w prawym górnym rogu ekranu. Z rozwijanego menu wybierz opcję: [Ustawienia].
16	**Otwórz sekcję podpisów** Na stronie ustawień znajdź sekcję [Podpisy]. Kliknij przycisk [Edytuj] (ikona ołówka lub przycisk obok nazwy sekcji).
17	**Ustaw rodzaj podpisu i dodaj certyfikat** W polu [Rodzaj podpisu] wybierz z listy: [Podpis niekwalifikowany]. Następnie kliknij przycisk [DODAJ CERTYFIKAT]. System wyświetli okno systemowe Windows z listą dostępnych certyfikatów z magazynu [Osobisty]. Znajdź certyfikat z imieniem i nazwiskiem użytkownika i kliknij [OK].
18	**Zapisz ustawienia przez odświeżenie strony** PO WYBRANIU certyfikatu i kliknięciu OK — NIE klikaj przycisku [Zapisz] w EZD RP! Zamiast tego odśwież stronę przeglądarki klawiszem F5 (lub Ctrl+R). Przejdź ponownie do Ustawienia → Podpisy i sprawdź, czy certyfikat nadal widnieje. Jeśli tak — konfiguracja zakończona sukcesem.

✓ Konfiguracja zakończona! Użytkownik może teraz podpisywać dokumenty w EZD RP używając podpisu niekwalifikowanego podczas ćwiczeń szkoleniowych.

ℹ Jak sprawdzić, czy podpis działa?
1. Przejdź do przykładowego dokumentu w EZD RP (instancja testowa).
2. Wybierz opcję podpisania dokumentu.
3. System powinien wyświetlić okno z certyfikatem i umożliwić podpisanie.

7. ZARZĄDZANIE CERTYFIKATAMI WIELU UŻYTKOWNIKÓW

Przy przygotowywaniu szkoleń dla wielu pracowników administrator musi skonfigurować certyfikaty na wielu komputerach.

Zalecana procedura przygotowania instancji testowej systemu przed rozpoczęciem zadań utrwalających oraz testów funkcjonalnych systemu

Nr	Zadanie	Szczegóły
1	Przygotuj listę uczestników	Zbierz: imię, nazwisko, e-mail, jednostka, stanowisko dla każdego uczestnika szkolenia.
2	Wygeneruj certyfikaty z wyprzedzeniem	Generuj certyfikaty .pfx. Zapisz je w folderze z podfolderami nazwanymi imieniem i nazwiskiem.
3	Użyj wspólnego hasła	Na potrzeby instancji testowej możesz użyć jednego hasła dla wszystkich certyfikatów (np. EzdTest2026). Zanotuj je i przekaż uczestnikom.
4	Skopiuj pliki .pfx na stanowiska	Skopiuj odpowiedni plik .pfx na pulpit każdego stanowiska szkoleniowego przed zajęciami.
5	Importuj certyfikaty przed szkoleniem	Zaimportuj certyfikat do magazynu Windows (kroki 8-13) na każdym stanowisku pracy ról kierowniczych.

6	Skonfiguruj EZD RP	Skonfiguruj podpis w EZD RP (kroki 14-18) dla każdego konta. Pamiętaj: F5 zamiast [Zapisz]!

ℹ Certyfikaty szkoleniowe mogą być wielokrotnie używane.
Nie ma potrzeby generowania nowych certyfikatów przed każdą sesją szkoleniową.
Certyfikat pozostaje ważny przez 5 lat od daty jego wygenerowania.

8. NAJCZĘSTSZE PROBLEMY I ROZWIĄZANIA

Problem	Przyczyna	Rozwiązanie
Certyfikat nie pojawia się w oknie wyboru EZD RP	Certyfikat nie został zaimportowany do magazynu Windows lub trafił do złego magazynu	Sprawdź w certmgr.msc → Osobisty → Certyfikaty. Jeśli brak — powtórz kroki 8-13.
Po wybraniu certyfikatu i odświeżeniu F5 — znika z ustawień	Konfiguracja nie została prawidłowo zapisana lub problem z sesją przeglądarki	Wyczyść pamięć podręczną przeglądarki. Powtórz kroki 14-18. Nie używaj trybu prywatnego.
Błąd [Nieprawidłowe hasło] podczas importu .pfx	Wpisano błędne hasło lub plik .pfx jest uszkodzony	Upewnij się, że wpisujesz hasło z rozróżnieniem małych/wielkich liter. Spróbuj ponownie wygenerować certyfikat.
Brak opcji [Podpis niekwalifikowany] w EZD RP	Ta opcja może być niedostępna — wymaga uprawnień do konfiguracji podpisu	Sprawdź, czy konto ma przypisane odpowiednie role. Skontaktuj się z administratorem merytorycznym.
Adobe Reader nie wyświetla opcji [Podpisy] w preferencjach	Otwierana jest przeglądarkowa wersja PDF zamiast programu Adobe Reader	Upewnij się, że otwierasz PROGRAM Adobe Acrobat Reader DC, nie plik PDF w przeglądarce.

9. PODSUMOWANIE — LISTA KONTROLNA

Użyj poniższej listy kontrolnej, aby upewnić się, że wszystkie kroki zostały wykonane prawidłowo:

Część	✓	Zadanie
I	☐	Otwarto Adobe Acrobat Reader DC (nie przeglądarkę!)
I	☐	Przejście: Edycja → Preferencje → Podpisy → Tożsamości → Więcej...
I	☐	Kliknięto [Dodaj ID]
I	☐	Wybrano: Nowy ID → Plik PKCS#12
I	☐	Wypełniono: Imię/Nazwisko, Org. jedn., Org., E-mail, Kraj=PL, Algorytm=RSA 2048
I	☐	Ustawiono lokalizację zapisu i hasło (ZANOTOWANE!)
I	☐	Wygenerowano plik .pfx — widoczny na dysku
II	☐	Dwukrotne kliknięcie pliku .pfx → Kreator importu
II	☐	Wybrano: Bieżący użytkownik
II	☐	Wpisano hasło + zaznaczono [Oznacz klucz jako eksportowalny]
II	☐	Wybrano magazyn: Osobisty
II	☐	Import zakończony komunikatem [Ukończono pomyślnie]
II	☐	Zweryfikowano obecność certyfikatu w certmgr.msc → Osobisty
III	☐	Zalogowano do EZD RP na koncie użytkownika (instancja testowa)
III	☐	Przejście: Imię/Nazwisko (prawy górny róg) → Ustawienia → Podpisy → Edytuj
III	☐	Wybrano: Rodzaj podpisu = Podpis niekwalifikowany
III	☐	Kliknięto [DODAJ CERTYFIKAT] → wybrano certyfikat z listy → OK
III	☐	Odświeżono stronę klawiszem F5 (NIE klikano [Zapisz])
III	☐	Zweryfikowano, że certyfikat nadal widnieje po odświeżeniu

✓ Wszystkie kroki wykonane? Użytkownik jest gotowy do ćwiczeń w systemie EZD RP!
W razie problemów skontaktuj się z LCIT: konfiguracja.ezdrp@lcit.lubelskie.pl godz. 7:30–15:30, dni robocze.