



CitiDirect BE® Import szyfrowany

CitiService
Pomoc Techniczna CitiDirect BE
tel. 801 343 978, +48 22 690 15 21
poniedziałek - piątek; 8:00 - 17:00
helpdesk.ebs@citi.com

Spis treści

1. Wprowadzenie	3
2. Wymagania techniczne	3
3. Opis czynności w procesie importu plików szyfrowanych	3
3.1 Uzyskanie certyfikatu x509 v3 do podpisu	3
3.2 Wyodrębnienie (eksport) klucza publicznego certyfikatu x509 v3	3
3.3 Wgranie wyodrębnionego klucza publicznego certyfikatu x509 v3 do CitiDirect BE	6
3.4 Pobieranie klucza publicznego CitiDirect BE do szyfrowania	7
3.5 Modyfikacja schematu importu dla obsługi plików szyfrowanych i podpisanych lub tylko podpisanych	8

1. Wprowadzenie

Proces szyfrowania i podpisywania plików importowych ma na celu zapewnienie poufności informacji w nich zawartych, np. danych przelewów placowych. Proces ten polega na zamianie czytelnej zawartości pliku w tzw. kryptogram, czyli zawartość niemożliwą do odczytania przez osobę niepowołaną oraz złożenie podpisu elektronicznego w celu uwierzytelnienia.

2. Wymagania techniczne

Do zabezpieczenia procesu szyfrowania i podpisywania plików importu będziesz potrzebował:

- certyfikatu w formacie x509 v3 do podpisu zaszyfrowanego pliku,
- klucza publicznego PKCS7 pobranego z CitiDirect BE do szyfrowania,
- aplikacji/narzędzia do szyfrowania i podpisywania plików zgodnych ze standardem S/MIME PKCS7 (może to być moduł szyfrujący zaimplementowany bezpośrednio w programie ERP lub samodzielna aplikacja instalowana na komputerze),
- dostęp do modułu S/MIME w aplikacji CitiDirect BE (w celu pobrania klucza publicznego do szyfrowania oraz wgrania certyfikatu x509 do podpisu),
- dostęp do modułu importu w aplikacji CitiDirect BE (w celu wgrania zaszyfrowanego pliku).

3. Opis czynności w procesie importu plików szyfrowanych

3.1 Uzyskanie certyfikatu x509 v3 do podpisu.

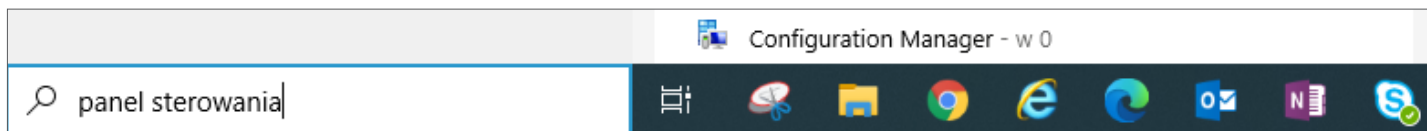
Certyfikat x509 v3 możesz pobrać od ogólnodostępnych zaufanych dostawców certyfikatów, np.:

- Verisign
- Thawte Consulting
- Comodo
- GlobalSign
- British Telecom
- KIR
- Certum

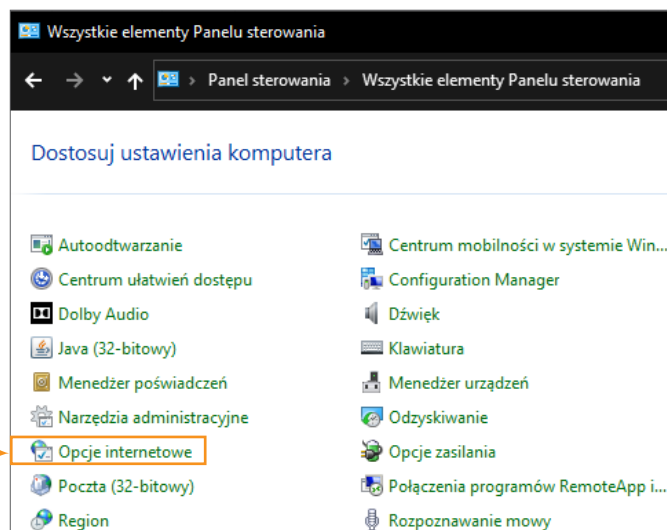
WAŻNE: W procesie szyfrowania plików importu użyty może być tylko tzw. certyfikat niekwalifikowany, co oznacza, że nie można do tego celu użyć certyfikatów wydanych przez autoryzowane centra certyfikacji na nośnikach typu karta lub pendrive, wydanych.

3.2 Wyodrębnienie (eksport) klucza publicznego certyfikatu x509 v3.

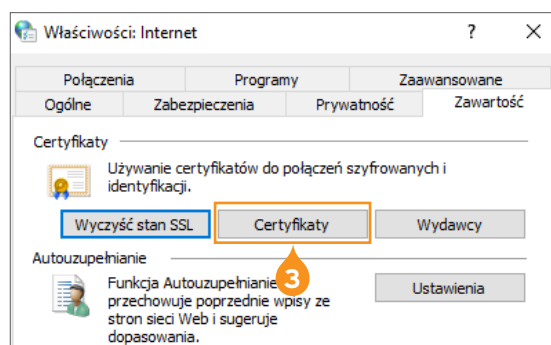
1. W oknie wyszukiwania na pasku systemu Windows wpisz „panel sterowania” i naciśnij klawisz **Enter**.



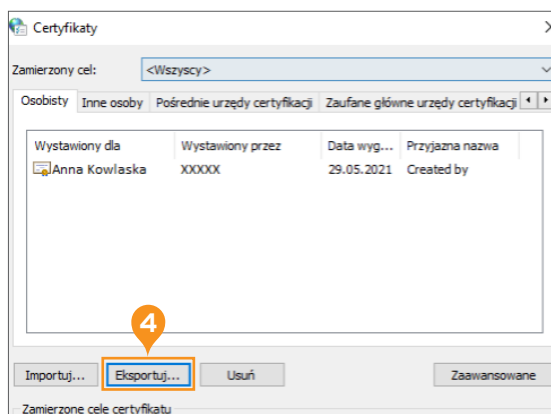
2. Po wyświetleniu zawartości Panelu Sterowania uruchom **Opcje Internetowe**.



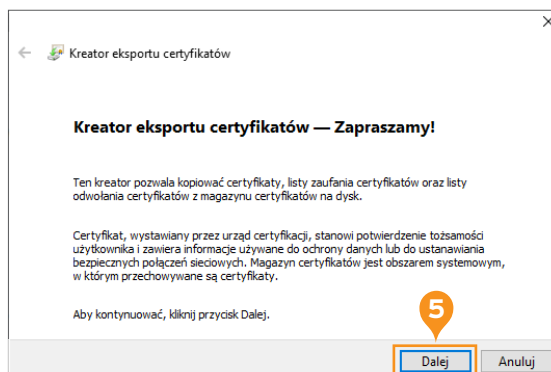
3. W Opcjach Internetowych przejdź do zakładki Zawartość i kliknij przycisk **Certyfikaty**.



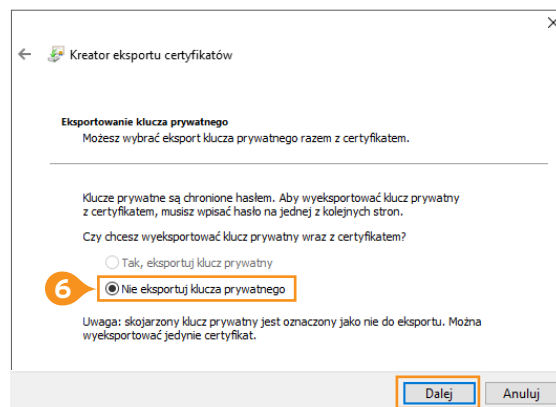
4. Na liście zaznacz właściwy certyfikat i kliknij przycisk **Eksportuj**.



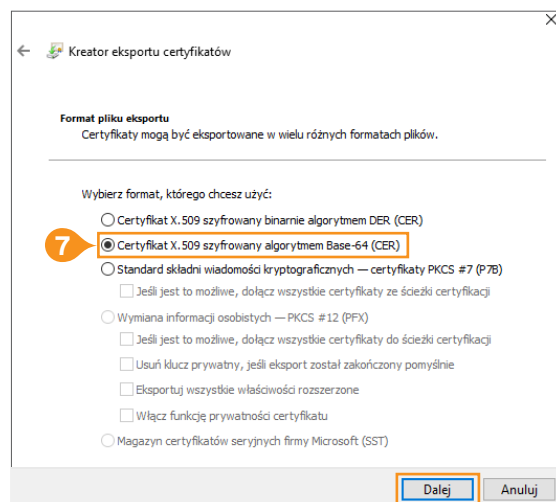
5. W zaproszeniu do Kreatora eksportu certyfikatów kliknij na przycisk **Dalej**.



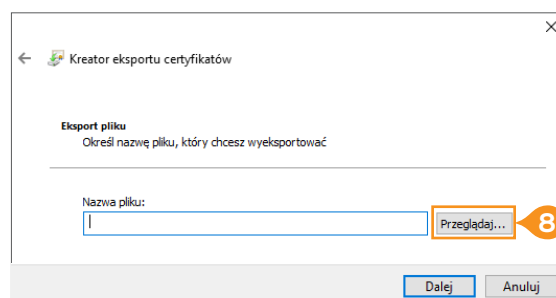
6. Zaznacz opcję **Nie eksportuj klucza prywatnego** i kliknij przycisk **Dalej**.



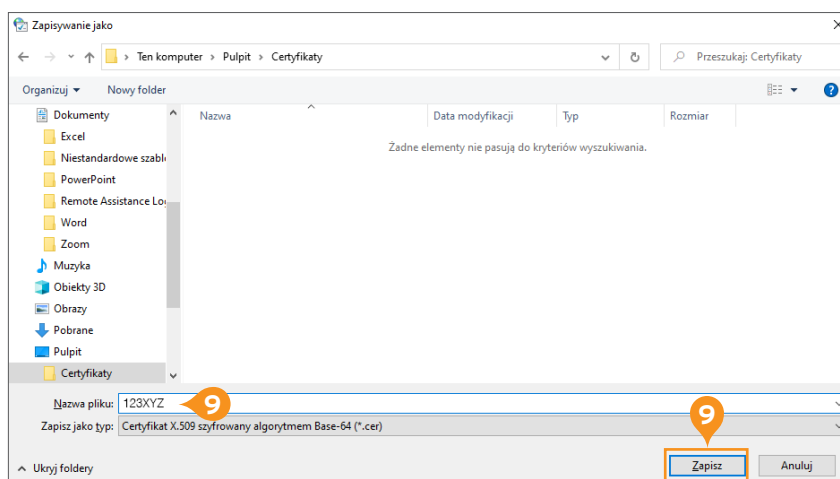
7. Zaznacz opcję **Certyfikat X.509 szyfrowany algorytmem Base-64 (CER)** i kliknij **Dalej**.



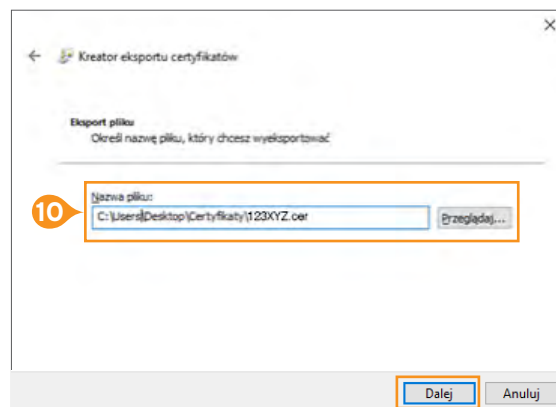
8. W oknie eksportu pliku kliknij przycisk **Przeglądaj**.



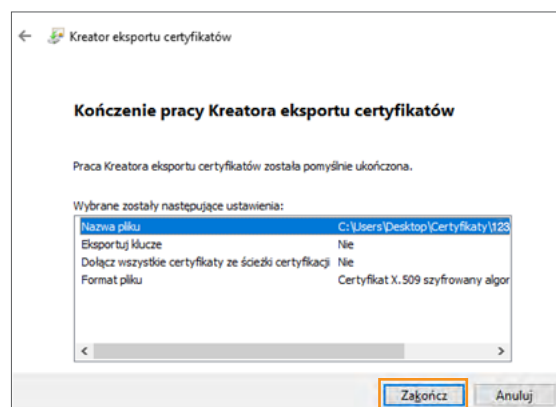
9. W oknie zapisywania wybierz folder docelowy, podaj nazwę pliku i kliknij **Zapisz**.



10. W oknie potwierdzenia ścieżki pliku kliknij **Dalej**.



11. W oknie kończenia eksportu kliknij **Zakończ**.



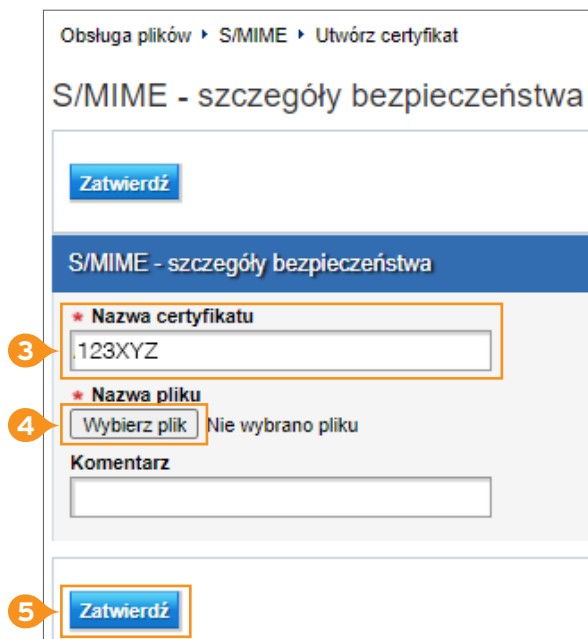
Uwaga: Otrzymasz potwierdzenie pomyślnego ukończenia eksportu. Klucz publiczny został zapisany w wybranym przez Ciebie folderze.

3.3 Wgranie wyodrębnionego klucza publicznego certyfikatu x509 v3 do CitiDirect BE.

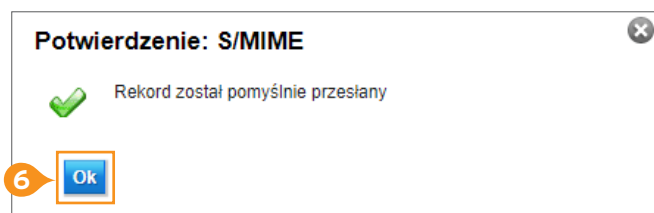
1. Z głównego menu wybierz zakładkę **Obsługa plików**.
2. W zakładce Obsługa plików wybierz opcję **Utwórz certyfikat** w sekcji S/MIME.



3. Wpisz nazwę certyfikatu.
4. Wciśnij przycisk **Wybierz plik**. W oknie eksploratora wybierz właściwy plik certyfikatu i kliknij **Otwórz**.
5. Wybierz przycisk **Zatwierdź**.

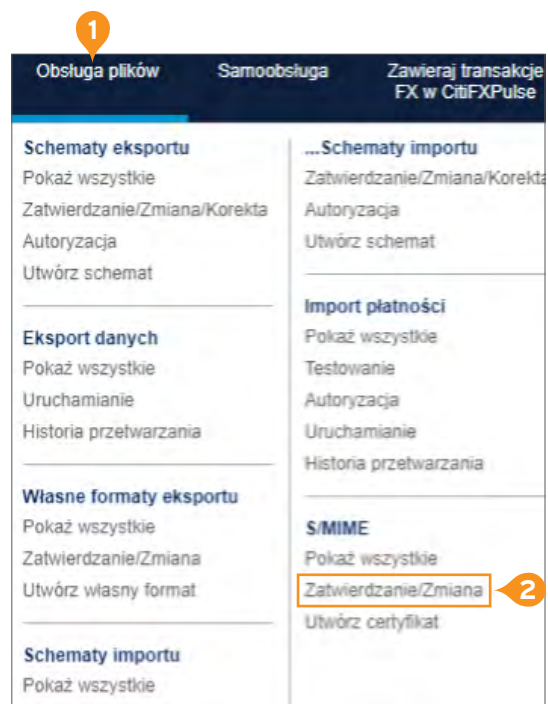


6. System wyświetli potwierdzenie o pomyślnym wgraniu certyfikatu. Kliknij przycisk **OK**.

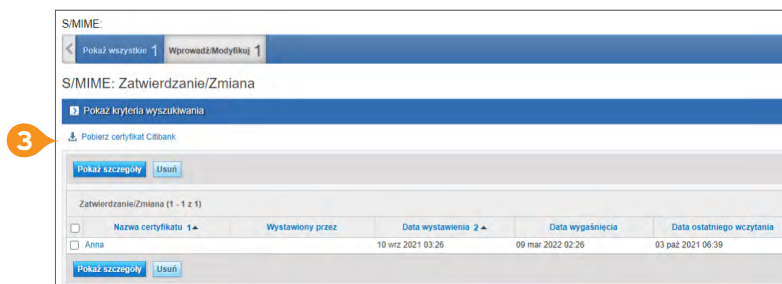


3.4 Pobieranie klucza publicznego CitiDirect BE do szyfrowania.

1. Z głównego menu wybierz zakładkę **Obsługa plików**.
2. W zakładce Obsługa plików wybierz opcję **Zatwierdzenie/Zmiana** w sekcji S/MIME.

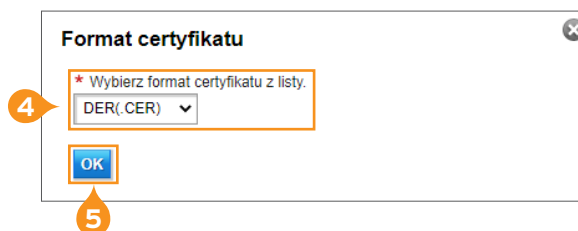


3. Kliknij na **Pobierz certyfikat Citibank**.



4. Wybierz format certyfikatu DER (.CER).

5. Kliknij na przycisk **OK**.

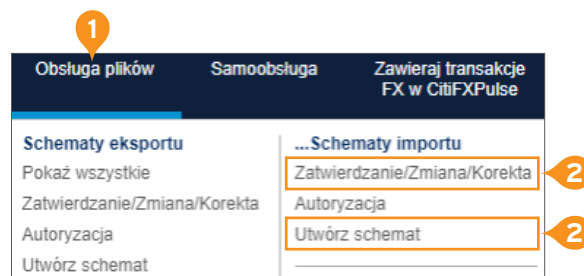


6. Plik o nazwie CitibankCertificate.cer zapisze się w domyślnej lokalizacji pobierania dla wybranej przeglądarki.

3.5 Modyfikacja schematu importu dla obsługi plików szyfrowanych i podpisanych (tylko podpisanych).

1. Z głównego menu wybierz zakładkę **Obsługa plików**.

2. W zakładce Obsługa plików wybierz opcję **Zatwierdzenie/Zmiana/Korekta** w sekcji Schematy importu lub **Utwórz schemat**.

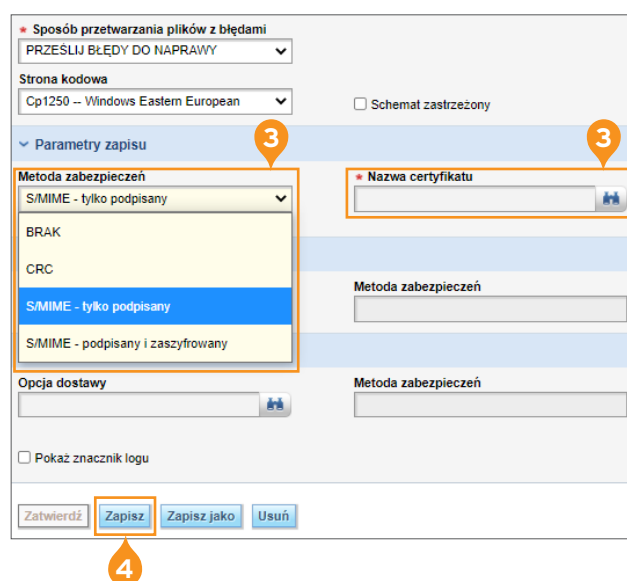


3. Uzupełnij parametry zapisu:

- **Metoda zabezpieczeń:** wybierz metodę zabezpieczeń: **S/MIME - tylko podpisany** lub **S/MIME - podpisany i zaszyfrowany**.

- **Nazwa certyfikatu:** kliknij w lornetkę i wybierz w nowym oknie stworzony poprzednio certyfikat.

4. Kliknij na przycisk **Zapisz**.



Na liście dostępnych schematów importu w sekcji **Zatwierdzenie/Zmiana/Korekta** zaznacz modyfikowany schemat importu i kliknij przycisk **Zatwierdź**.

Schemat importu po zatwierdzeniu przez Użytkownika ma status **Wymagany test**. Na tym etapie, po wybraniu z górnego menu zakładki **Obsługa plików → Testowanie** w sekcji Import płatności, można wykonać kilka importów próbnych lub bez testowania zakończyć ten etap, klikając przycisk **Test został ukończony**.

Po zakończeniu testowania, należy zautoryzować schemat importu w zakładce **Obsługa plików → Autoryzacja** w sekcji **Schematy importu**.

Ważne:

1. Wybór metody zabezpieczenia pliku zależy tylko od Ciebie. W przypadku wyboru metody S/MIME – podpisany, nie ma potrzeby pobierania klucza publicznego CitiDirect BE do szyfrowania.
2. Po wykonaniu powyższych czynności system CitiDirect BE jest gotowy do obsługi plików z wybraną metodą zabezpieczeń. Pozostałe czynności przygotowawcze obejmują Twój system generowania i zabezpieczania plików, włącznie z podpięciem właściwych certyfikatów.

Więcej przydatnych wskazówek dotyczących CitiDirect BE znajdziesz [TUTAJ >>](#)

www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

The logo for Citi Handlowy, featuring the word "citi" in a smaller font with a red arc above the "i", followed by "handlowy" in a larger font, and a registered trademark symbol (®) to the right.

Linki umieszczone w naszych komunikatach prowadzą do stron internetowych lub materiałów marketingowych naszego Banku lub naszych partnerów, które mają charakter informacyjny. Nie wykorzystujemy linków do zbierania danych wrażliwych od naszych Klientów. Jeśli cokolwiek budzi Państwa zastrzeżenia, prosimy o kontakt z CitiService lub nadawcą komunikatu ze strony Banku. Znaki Citi oraz Citi Handlowy stanowią zarejestrowane znaki towarowe Citigroup Inc., używane na podstawie licencji. Spółce Citigroup Inc. oraz jej spółkom zależnym przysługują również prawa do niektórych innych znaków towarowych tu użytych. Bank Handlowy w Warszawie S.A. z siedzibą w Warszawie, ul. Senatorska 16, 00-923 Warszawa, zarejestrowany przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr. KRS 000 000 1538; NIP 526-030-02-91; wysokość kapitału zakładowego wynosi 522 638 400 złotych, kapitał został w pełni opłacony.