COMARCH
DMS

Krajowy System e-Doręczenia

Spis treści

1 Informacje ogólne 3
2 Certyfikat 3
2.1 Zakup Pieczęci elektronicznej Szafir 3
2.2 Postępowanie, gdy operator posiada certyfikat 5

1 Informacje ogólne

W systemie Comarch DMS istnieje możliwość integracji z usługą e-Doręczenia, integracja polega na możliwości pobierania wiadomości przychodzących na skrzynkę oraz na możliwości wysyłania wiadomości w ramach usługi e-Doręczenia z poziomu systemu Comarch DMS.

2 Certyfikat

Aby zintegrować system do zarządzania dokumentami (np. Comarch DMS) z usługą e-Doręczenia **konieczne jest posiadanie kwalifikowanego certyfikatu**. W związku z tym podmioty niepubliczne – m.in. spółki, które chcą zintegrować Comarch DMS z usługą e-Doręczenia – w celu pobierania i wysyłania wiadomości są **zobligowane do zakupu komercyjnego certyfikatu kwalifikowanego**.

Do integracji Comarch DMS z usługą e-Doręczenia, rekomendowany jest zakup **Pieczęci elektronicznej Szafir** wystawianej przez **Krajową Izbę Rozliczeniową** z wykorzystaniem żądania CSR.

2.1 Zakup Pieczęci elektronicznej Szafir

Aby zakupić Pieczęć elektroniczną Szafir, należy kolejno:

- Wygenerować żądanie certyfikatu CSR – poprzez wykorzystanie środowiska **OpenSSL**
  - OpenSSL to oprogramowanie open source, oferujące prosty interfejs wiersza polecenia służący do generowania kluczy.

    Oprogramowanie dostępne jest np. na stronie: https://slproweb.com/products/Win32OpenSSL.html
  - Do przygotowania żądania CSR potrzebny będzie klucz prywatny.
    - Aby wygenerować klucz prywatny, należy przejść do terminala i użyć polecenia: *openssl genrsa -out private_key.key 2048*

      Polecenie tworzy klucz prywatny o nazwie private_key.key o długości 2048 **Bezwzględnie należy zabezpieczyć klucz prywatny – nie może być udostępniany nikomu.**
  - Następnie za pomocą klucza prywatnego zostanie utworzone żądanie(CSR), do konsoli należy wkleić i wykonać komendę: *openssl req -new -key private_key.key -out request.pem*

    W efekcie otrzymamy plik request.pem z zapisanym żądaniem CSR, wygenerowany za pomocą klucza prywatnego private_key.key
    - W trakcie wykonywania komendy, w konsoli zostanie wyświetlony komunikat w którym trzeba będzie podać dodatkowe informacje: CountryName(kod kraju w formacie dwuliterowym), State or Province Name(województwo), Locality Name(miasto), Organization Name(pełna nazwa organizacji), Organizational Unit Name(dział organizacji), Common Name(nazwa lub domena dla której wystawiany jest certyfikat).
  - Po utworzeniu żądania CSR można zweryfikować jego zawartość za pomocą polecenia:

    openssl req -text -noout -verify -in request.pem

Wyświetlony wynik powinien być zgodny z danymi podanymi w poprzednim podpunkcie (CountryName, State or Province Name, Locality Name, Organization Name, Organizational Unit Name, Common Name).

Jeżeli dane są poprawne, plik request.pem można będzie przesłać do podmiotu certyfikującego w celu uzyskania kwalifikowanej pieczęci elektronicznej

- **Wygenerowany klucz prywatny należy zapisać oraz zabezpieczyć przed dostępem osób nieupoważnionych. Klucz prywatny, w pełnej jego formie, wraz z nagłówkami i stopką, będzie niezbędny do przeprowadzenia integracji z usługą e-Doręczenia.**
- Wygenerowane żądanie CSR **request.pem** należy przekazać do podpisu przy użyciu podpisu kwalifikowanego.
- Żądanie CSR (plik *request.pem*) musi być podpisane podpisem kwalifikowanym w formacie CAdES – jeśli Twoja aplikacja do podpisywania nie pozwala na złożenie podpisu w tym formacie, skorzystaj z Aplikacji Szafir do składania i weryfikacji podpisu elektronicznego: https://www.elektronicznypodpis.pl/aplikacje-i-sterowniki.
  - W aplikacji Szafir przejdź do sekcji **Konfiguracja**,
  - Zmień aktywną konfigurację,
  - Ustaw format na **CAdES (PKCS#7)**,
  - W sekcji **Parametry podpisu** zaznacz opcję **Zapisz podpisywane dane razem z podpisem**,
  - Zapisz konfigurację i podpisać plik żądania certyfikatu, korzystając z aplikacji Szafir,
  - Po podpisaniu żądania otrzymamy plik z rozszerzeniem *.sig*, który będzie można przekazać do KIR.
- Kolejny krok wymaga przejścia do sklepu Krajowej Izby Rozliczeniowej i odszukania produktu Pieczęć elektroniczna Szafir. Można skorzystać z tego linku.
- Na stronie sprzedawcy konieczne jest wybranie terminu ważności kwalifikowanej pieczęci elektronicznej. Dostępne opcje to: 1 rok lub 2 lata.
- Wybrać właściwą dla swojej organizacji wersję pieczęci wśród wymienionych poniżej:
  - **Pieczęć elektroniczna kwalifikowana z wgraniem żądania CSR online** – Rozwiązanie wymaga posiadania kwalifikowanego podpisu, który jest niezbędny do podpisania żądania CSR związanego z certyfikatem. Dzięki temu sprawę można załatwić w pełni online.

    Jeżeli żądanie CSR zostało już wygenerowane, należy je podpisać osobiście lub przekazać do podpisu osobie, która będzie odbierała zakupioną pieczęć elektroniczną. Szczegóły procesu podpisywania znajdują się w poprzednich krokach.
  - **Pieczęć elektroniczna z dostarczeniem żądania CSR do placówki KIR** – rozwiązanie nie wymaga posiadania podpisu kwalifikowanego, ale konieczna jest fizyczna wizyta w jednym z dwunastu Regionalnych Centrów Sprzedaży KIR (Krajowa Izba Rozliczeniowa), aby dostarczyć wygenerowany CSR z żądaniem certyfikatu.
- Wybrać opcję **Nowy zestaw**, jeśli pieczęć kupujesz po raz pierwszy. Proszę nie zaznaczać opcji **Certyfikat do PSD2**.
- Kliknąć **Dodaj do koszyka**,
- Przejść do koszyka i kliknąć **Złóż zamówienie**.

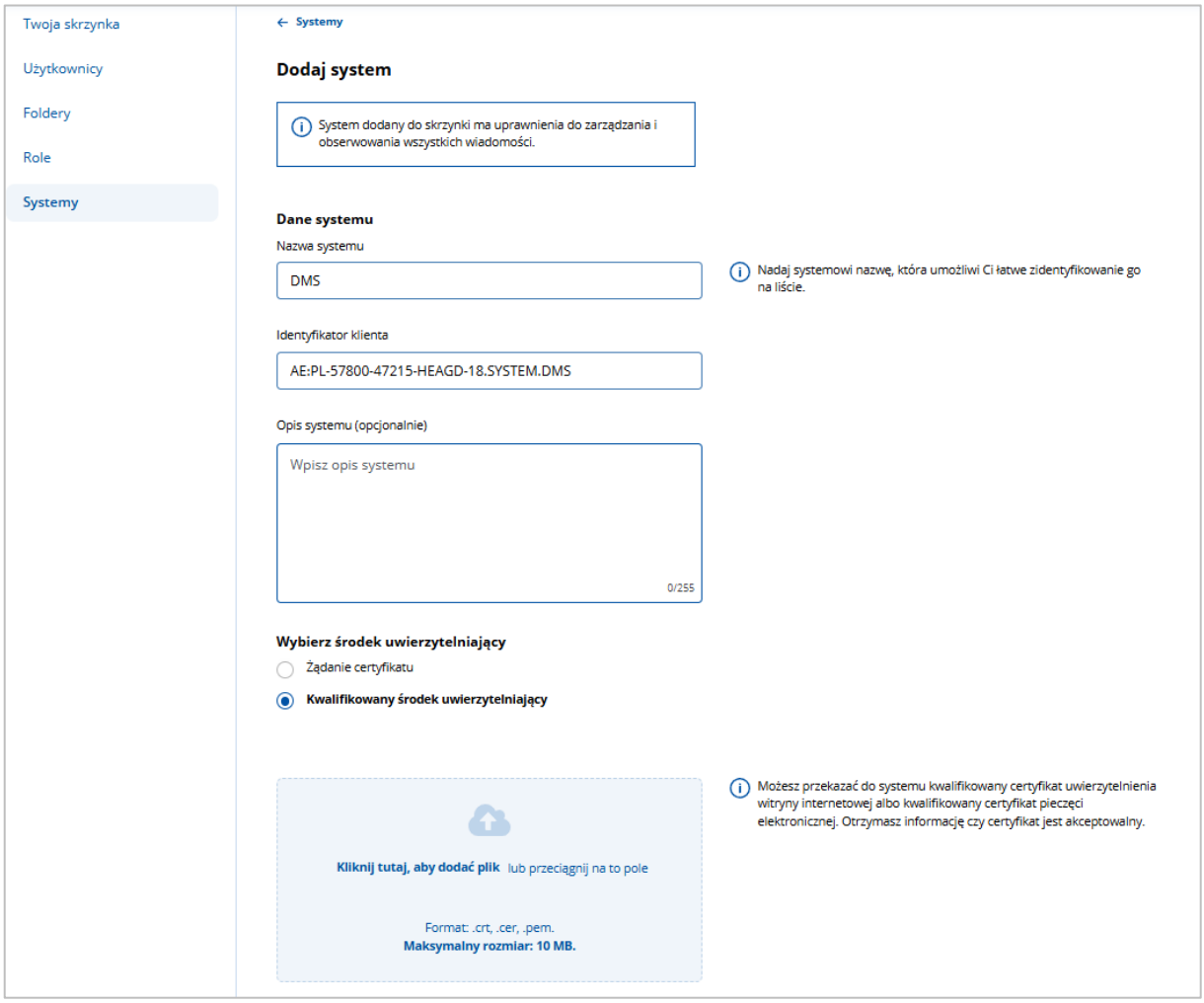
- Kliknąć **Uzupełnij dane**, w kolejnym kroku uzupełnić dane osoby upoważnionej do odebrania pieczęci elektronicznej,
- Przejść w dół do sekcji **Dane do certyfikatu pieczęci elektronicznej** i uzupełnić dane zgodnie z potrzebami organizacji oraz zgodnie z danymi przekazanymi w żądaniu CSR.
- Następnie należy przejść niżej do ostatniej sekcji:
  - **Certyfikat online: Wgram żądanie PKCS#10** – w tym kroku należy przesłać plik CSR w rozszerzeniu *.sig*, który został podpisany kwalifikowanym podpisem.
  - **Certyfikat w placówce KIR: Dostarczę żądanie PKCS#10 do placówki KIR** – w tym kroku należy wybrać oddział, do którego zostanie dostarczone żądanie certyfikatu CSR.
- Przejść do kroku 2 – **Dane do zamówienia**, a następnie do kroku 3 – **Podsumowanie i płatność**. W ramach wspomnianych kroków wykonać niezbędne działania opisane na stronie.
- Pobrać wygenerowane zamówienie wraz z umową i przekazać je do podpisu. Należy upewnić się, że dokumenty zostaną podpisane przez osobę reprezentującą spółkę zgodnie z KRS lub przez osobę posiadającą odpowiednie pełnomocnictwo.

2.2 Postępowanie, gdy operator posiada certyfikat

Otrzymany zamówiony certyfikat będzie zapisany w pliku z rozszerzeniem **.crt**.

Plik należy przygotować do dalszej pracy, zgodnie z poniższymi krokami (kolejno):

- Plik certyfikatu należy umieścić w folderze lokalnego komputera
- Uruchomić plik klikając w niego dwukrotnie. W nowym oknie kliknąć **Otwórz**;
- Przejść do zakładki **Szczegóły** i nacisnąć **Kopiuj do pliku…**;
- W oknie kreatora eksportu certyfikatów przejść dalej i w kroku **Format pliku eksportu** zaznaczyć **Certyfikat X.509 szyfrowany algorytmem Base-64 (CER)**, następnie kliknąć **Dalej**,
- Wprowadzić nazwę tworzonego pliku i kliknąć **Dalej**;
- W ostatnim kroku **Kończenie pracy kreatora eksportu certyfikatów** wyświetlone zostanie podsumowanie wraz ze ścieżką do miejsca zapisu nowego pliku certyfikatu. Domyślnie będzie to ten sam katalog, w którym znajduje się źródłowy certyfikat. Kliknąć **Zakończ**;
- W katalogu zostanie zapisany nowy plik o wskazanej nazwie, a kreator potwierdzi zakończenie eksportu. Teraz można zamknąć wszystkie wcześniej otwarte okna;
- Nowy plik z certyfikatem w rozszerzeniu **.cer** zostanie wykorzystany do dodania nowego systemu w usłudze e-doręczenia. Plik należy wgrać w oknie Uprawnienia w skrzynce e-Doręczeń -> Systemy -> Dodaj system jako Kwalifikowany środek uwierzytelniający



Rys 1. Dodawanie systemu jako Kwalifikowanego środka uwierzytelniającego w usłudze e-Doręczenia

- Po wgraniu uzyskanego w powyższych krokach certyfikatu z rozszerzeniem .cer, można przystąpić do konfiguracji w Comarch DMS menu Ustawienia -> zakładka Integracje w trybie jednospółkowym lub ustawienia odpowiedniej spółki w trybie wielospółkowym, gdzie konieczne będzie podanie nazwy systemu dodanego w usłudze e-Doręczenia oraz wgranie klucza prywatnego utworzonego w początkowej części niniejszego dokumentu (zob. Integracje (dawna zakładka „KSeF") – Baza Wiedzy programu Comarch DMS - dla trybu jednospółkowego - lub Połączenia z ERP – Baza Wiedzy programu Comarch DMS – dla trybu wielospółkowego).

COMARCH ERP