Zasady uwierzytelniania w KSeF w Comarch BPM

Od wersji 2026.0.1 przyjęto następującą kolejność autoryzacji:

1. Uwierzytelnienie operatora działakącego z KSeF na podstawie istniejącego i aktywnego tokenu
2. W przypadku, gdy dotychczasowe tokeny są nieważne lub jeśli uwierzytelnianie następuje po raz pierwszy, kolejność autoryzacji jest następująca:
    1. **Uwierzytelnienie tokenem wprowadzonym w polu „Token KSeF“** (w sekcji „Integracja z usługą KSeF“ w zakładce „Integracje“ dla pracy w trybie jednofirmowym lub w ustawieniach danej spółki na zakładce „Połączenia z ERP“ dla pracy w trybie wielofirmowym) – maksymalnie do 31.12.2026
    2. **Uwierzytelnienie certyfikatem KSeF wybranym w ramach pola „Odcisk certyfikatu KSeF“** (w sekcji „Integracja z usługą KSeF“ w zakładce „Integracje“ dla pracy w trybie jednofirmowym lub w ustawieniach danej spółki na zakładce „Połączenia z ERP“ dla pracy w trybie wielofirmowym) – w przypadku, gdy zostały spełnione następujące warunki:

        - token nie został skonfigurowany albo opcja uwierzytelniania tokenem jest nieważna (od 1.01.2027r.)

    oraz

        - certyfikat KSeF jest ważny (certyfikat ma ważność 2 lata od daty wydania certyfikatu)

    oraz

- certyfikat KSeF jest nieważny lub nie został skonfigurowany

Uwaga
Aby uwierzytelnienie poprzez wybór certyfikatu podczas próby pobierania faktur z KseF w punkcie ACD typu „Import dokumentów zakupu z KSeF“ zakończyło się powodzeniem, operator musi zainstalować dany certyfikat w Magazynie certyfikatów Windows swojej maszyny .

Jeżeli nie udało się uwierzytelnić za pomocą żadnej z powyższych metod, wówczas wyświetlony zostaje komunikat o błędzie.