

Propozycje podpisu elektronicznego w aplikacji EZD

W naszej wizji system EZD powinien zastąpić jak najwięcej papieru, zwłaszcza w obiegu wewnątrz instytucji. Jednak wiele dokumentów, ze względu na odpowiedzialność finansową wymaga podpisu – w wersji papierowej odręcznego.

Uważamy, że w obiegu elektronicznym podpisu odręcznego nie można zastąpić checkbox'em *akceptuję* wypełnianym przez decydenta zalogowanego do systemu. Dlatego konieczne jest stosowanie podpisu elektronicznego.

W jaki sposób i jaki podpis elektroniczny stosować w obiegu wewnętrznym.

1. Należy stosować podpis bezpieczny (karta kryptograficzna), by uzyskać wysoki stopień niezaprzeczalności.
2. Podpisywane powinny być wszystkie decyzje i zatwierdzenia zwłaszcza związane ze sprawami finansowymi. Oznacza to, że podpisujących i podpisów będzie dużo.
3. Do podpisywania dokumentów wewnętrznych należy stosować podpis bezpieczny (klucz prywatny nie opuszcza nośnika), ale nie kwalifikowany (z certyfikatem publicznym).
4. Oznacza to konieczność utrzymywania własnego urzędu/serwera certyfikatów.
5. Dzięki własnej infrastrukturze podpisu:
 - jest taniej,
 - nie jest się ograniczonym urzędowymi 2 latami – weryfikacja jest możliwa "wiecznie"
 - można realnie obsługiwać "zgubienia" i "zapomnienia" karty o czym poniżej.
6. Dla każdego użytkownika powinny być wyrobione dwa podpisy (karty):
 - podstawowy
 - rezerwowy
7. Kartę podpisu podstawowego użytkownik ma pod swoją pieczęcią i używa do codziennej pracy.
8. Karty podpisu rezerwowego zdeponowane są np. w dziale kadr.
9. W przypadku zostawienia karty podpisu podstawowego "w domu" użytkownikowi wypożycza się kartę podpisu rezerwowego za pokwitowaniem do zwrotu.
10. W przypadku zgubienia karty podpisu podstawowego, np. podpis rezerwowy staje się podstawowy i jest wyrabiany nowy podpis rezerwowy.
11. W EZD powinny być zaewidencjonowane wszystkie podpisy podstawowe, rezerwowe i historia ich użytkowania (wypożyczeń, zwrotów)
12. System powinien pozwalać na użycie tylko podpisu aktualnego, np. wypożyczonego zamiast "zostawionego w domu".
13. Idealem byłoby, gdyby EZD posiadał wbudowany urząd certyfikatów pozwalający w pełni obsługiwać certyfikaty, w tym tworzyć je.
14. Weryfikacja podpisanej treści (dokumentu) powinna być wykonywana na potrzeby codziennej pracy w ramach systemu EZD przez wbudowane mechanizmy. Ale to zbyt mało do celów kontrolnych. Propozycja rozwiązania poniżej.
15. Proponujemy następujący mechanizm podpisywania i weryfikacji:
 - zawartość (zwykle kilku) pól bazy danych) tworząca treść do podpisania zostaje zapisana w formacie xml;
 - podpisaniu ulega treść xml zgodnie ze standardami typowymi dla tego formatu;
 - podpisana treść xml jest przechowywana w bazie danych;
 - weryfikacja podpisu w systemie polega na sprawdzeniu identyczności między polami bazy danych a przechowywaną treścią xml i sprawdzeniu poprawności podpisu treści xml;
 - zapis treści w xml może być wyeksportowany jako plik xml z podpisem na zewnątrz systemu, by prawidłowość podpisu mogła zostać zweryfikowana typowymi, publicznymi narzędziami do weryfikacji.