

# Podpisy elektroniczne

Konstrukcja podpisu elektronicznego bazuje na algorytmach szyfrowania z kluczem publicznym. Podstawą działania tego typu szyfrów są dwa klucze: klucz prywatny oraz klucz publiczny. Klucz prywatny, dla zachowania bezpieczeństwa, musi pozostać pod wyłączną kontrolą jego właściciela, zaś klucz publiczny wraz z informacjami o właścicielu, w postaci certyfikatu klucza publicznego jest udostępniany wszystkim zainteresowanym.

W dużym uproszczeniu do składania podpisów elektronicznych wykorzystuje się klucz prywatny, zaś do weryfikacji podpisu można użyć tylko i wyłącznie klucza publicznego pochodzącego z danej pary. Dzięki tej własności podpis elektroniczny pozwala jednoznacznie ustalić, kto jest autorem podpisanego dokumentu.

## Zalety korzystania z podpisu elektronicznego:

**Unikalność** – każdy dokument elektroniczny posiada unikalny podpis elektroniczny ściśle związany z danym dokumentem. Nie można zatem podpisu elektronicznego przygotowanego dla danego dokumentu dołączyć do innego dokumentu. Taka manipulacja zostanie wykryta w momencie weryfikacji podpisu elektronicznego.

**Integralność** – jakakolwiek zmiana dokumentu opatrzonego podpisem elektronicznym zostanie automatycznie wykryta w momencie weryfikacji przez odbiorcę podpisu elektronicznego dołączonego do dokumentu. Co ważne w przeciwieństwie do podpisu własnoręcznego weryfikacja podpisu elektronicznego zostanie wykonana w aplikacji i nie wymaga ona żadnej specjalistycznej wiedzy od osoby, która weryfikuje podpis.

**Niezaprzeczalność** – tylko osoba posiadająca dane służące do składania podpisów, czyli tzw. klucz prywatny, korespondujący z danymi zawartymi w certyfikacie mogła wygenerować podpis elektroniczny pod danym dokumentem.

**Potwierdzenie tożsamości** – dane osoby składającej podpis elektroniczny zawarte w certyfikacie zostały potwierdzone przez podmiot świadczący usługi certyfikacyjne. Jeżeli podpis elektroniczny, został pozytywnie zweryfikowany, mógł on zostać złożony jedynie przez osobę wskazaną w certyfikacie, która posiadała klucz prywatny tworzący z danym kluczem publicznym jedną parę. Dzięki tym zaletom podpis elektroniczny zapewnia bezpieczną i niezaprzeczalną komunikację w sieci internetowej.

## Zastosowanie w praktyce

W praktyce złożenie bezpiecznego podpisu elektronicznego, równoważnego z mocą prawa podpisom własnoręcznym jest stosunkowo proste. Aby to zrobić trzeba się zaopatrzyć w zestaw do jego składania. Na podstawowy zestaw składa się:

- certyfikat kwalifikowany;
- karta kryptograficzna;
- aplikacja do składania i weryfikacji bezpiecznych podpisów elektronicznych;
- oraz czytnik kart.

Sam proces złożenia podpisu polega na wskazaniu dokumentu do podpisania i postępowaniu zgodnie

z zaleceniami aplikacji, która poprosi o włożenie karty do czytnika i podanie kodu PIN, co pozwoli, przy pomocy klucza prywatnego zapisanego na karcie wygenerować podpis elektroniczny pod wskazanym dokumentem. Bezpieczny podpis elektroniczny, często traktowany jest jako odpowiednik podpisu własnoręcznego. Tymczasem zapewnia on znacznie więcej niż podpis własnoręczny. W przypadku dokumentu papierowego nawet po jego podpisaniu możliwe jest dokonanie zmian. Podpis elektroniczny całkowicie wyklucza tego typu manipulacje na dokumentach elektronicznych. Co ciekawe i co wynika z powyższych wywodów „nie sprzedajemy podpisów elektronicznych” a jedynie narzędzia do ich składania. Każdy użytkownik zestawu może przy użyciu swojego klucza prywatnego zapisanego na karcie kryptograficznej i aplikacji podpisującej złożyć tyle podpisów elektronicznych ile zechce.

Moc prawna "bezpiecznego podpisu elektronicznego" zrównująca go z podpisem własnoręcznym, pozwala stosować go w coraz to nowych obszarach. Możliwości zastosowania tej technologii do dokumentów elektronicznych są praktycznie nieograniczone. Ponadto wiele aktów prawnych, obok tradycyjnej formy podpisu, pozwala praktycznie wykorzystywać bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanych certyfikatów.

W chwili obecnej istnieje kilka zastosowań bezpiecznych podpisów elektronicznych i kwalifikowanych certyfikatów, które funkcjonują w praktyce. Są to między innymi:

- e-zdrowie
- e-deklaracje
- e-faktura
- e-KRS
- Podpis dla ZUS
- Przesyłanie danych do Generalnego Inspektora Informacji Finansowej (GIIF)
- Kontakty z urzędami administracji publicznej