

Tomasz Kawecki

Time Stamping – elektroniczne datowanie dokumentów



Fot. Matthew Bowden

Wraz z migracją gospodarki i kontaktów biznesowych w sferę elektroniczną, coraz ważniejsze staje się zagadnienie czasu i potwierdzania wiarygodności dokumentów. Podczas pracy z dokumentami elektronicznymi użytkownicy często zastanawiają się, kto jest autorem dokumentu i kiedy ten dokument tak naprawdę powstał. **Z zagadnieniem autorstwa dokumentu związany jest podpis elektroniczny, który wraz z certyfikatem elektronicznym pozwala na zidentyfikowanie autora dokumentu.** Nie istnieje jeszcze usługa, która umożliwiłaby odczytywanie daty stworzenia dokumentu w sposób wiarygodny, jednakże **dostępna jest usługa elektronicznego znakowania czasem dokumentów, która pozwala na wiarygodne stwierdzenie, że w danym czasie istniał dokument o danej postaci.**

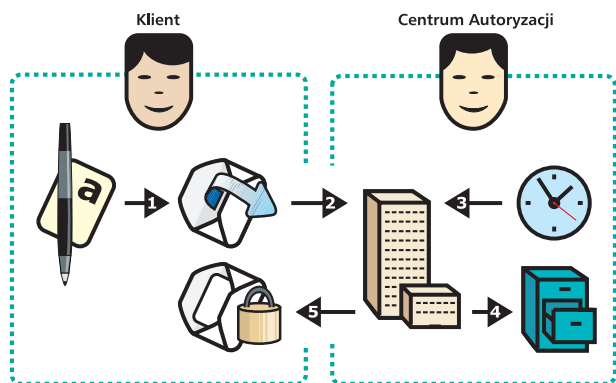
W kontaktach biznesowych dokumenty często muszą być przesyłane w określonym terminie, aby odbiorca przesyłki był pewny, że dokument nie zostanie zmieniony później. Również w życiu codziennym, składając zeznania podatkowe, wystawiając przelewy otrzymujemy od osób upoważnionych potwierdzenia, że dokumenty, które zostały złożone, będą odebrane w terminie. W przypadku problemów administracyjnych posiadanie znacznika potwierdza, że dokument został złożony w określonym terminie. Można w ten sposób uniknąć dodatkowych kosztów związanych, np. z płaceniem odsetek karnych. Poświadczenie daty na dokumencie przez notariusza jest kosztowne oraz kłopotliwe. **Dzięki zastosowaniu elektronicznego datowania dokumentów można uniknąć kosztów, straty czasu i niekompetencji osób trzecich.**

Elektroniczne datowanie dokumentów poprawia bezpieczeństwo procesów biznesowych, uniemożliwiając antydatowanie umów, sporządzanie dokumentów z datą wsteczną, dokonywania zmian w dokumentach po oznakowaniu czasem, zaprzeczanie uczestnictwa w transakcji itp., a ponadto wspomaga tworzenie elektronicznych systemów rejestracji dokumentów.

W roku 2001 organizacja IETF opublikowała standard RFC 3161, dostarczający niezbędnych pojęć i schematów potrzebnych do elektronicznego datowania dokumentów. Działanie systemu elektronicznego datowania dokumentów jest bardzo proste i polega na połączeniu się aplikacji klienta z centrum autoryzacji TSA (*Time Stamping Authority*) i wysłaniu skrótu dokumentu o określonej długości, który powstaje po zastosowaniu funkcji skrótu, np. MD5 (*Message Digest*, 128 bitów), SHA-1 (*Secure Hash Algorithm*, 160 bitów) SHA-256 (*Secure Hash Algorithm*, 256 bitów). Można zatem już zauważyć, że datowany dokument jest bezpieczny, ponieważ nikt w centrum autoryzacji nie odczyta jego treści. Skróć dokumentu (lub dowolnego pliku) przechodzi weryfikację poprawności, a następnie zostaje oznaczony dokładnym czasem i odesłany do aplikacji klienta. Centrum autoryzacji przesyła

W kontaktach biznesowych dokumenty często muszą być przesyłane w określonym terminie, aby odbiorca przesyłki był pewny, że dokument nie zostanie zmieniony później.

znacznik czasu w określonej postaci, która zawiera charakterystykę urządzeń i skrótu dokumentu (bądź innego pliku), który był poddany datowaniu. Proces elektronicznego datowania dokumentów przedstawia rysunek.



Elektroniczne datowanie dokumentów

1. Obliczenie skrótu dokumentu.
2. Przesłanie obliczonego skrótu za pomocą Internetu do centrum autoryzacji.
3. Pobranie danych o dokładnym czasie (zegar atomowy).
4. Zapisanie znacznika czasu do archiwum.
5. Odesłanie elektronicznego znacznika czasu do użytkownika.

Należy pamiętać, że **elektroniczne datowanie dokumentów nie potwierdza daty stworzenia dokumentu czy jego modyfikacji, a jedynie podaje czas, w którym dokument istniał w określonej postaci.**

Znakowaniu czasem można również poddawać inne pliki, z których obliczony zostanie skrót.

W ustawie z dnia 18 września 2001 r. o podpisie elektronicznym czytamy, iż „...znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów kodeksu cywilnego”, co oznacza, że **elektroniczne datowanie dokumentów jest równoważne z poświadczeniem daty przez notariusza.**

W Internecie można z łatwością odnaleźć dwa polskie centra, które świadczą usługi elektronicznego datowania dokumentów. Są to Centrum Certyfikacji Signet (www.signet.pl) oraz Centrum Certyfikacji Unizeto CERTUM. W pierwszym przypadku usługa jest bezpłatna, a w drugim bezpłatna dla osób prywatnych, organizacji niedochodowych i zrzeszeń oraz fundacji i szkolnictwa – pozostali płacą 0,25 zł za pojedynczą

usługę znakowania. Różnice cenowe pomiędzy poświadczeniem daty przez notariusza (od 25 zł) a centrami certyfikacji w Internecie są zatem znaczące. Elektroniczne znakowanie dokumentów umożliwia również Krajowa Izba Rozliczeniowa SA.

Każdy urząd TSA, który chce uzyskać wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, musi spełniać określone warunki, z których najważniejsze to:

1. TSA musi korzystać z usług wiarygodnego dostawcy czasu.
2. Każdy dokument, który uzyskał stempel czasu musi posiadać swój unikalny identyfikator.
3. TSA musi zapisać w żetonie czasu technikę wykorzystaną do jego utworzenia.
4. Żetony czasu nie mogą umożliwiać uzyskania informacji na temat klienta centrum autoryzacji osobom niepowołanym.

W Unii Europejskiej pierwsze zapisy dotyczące znakowania czasem pojawiły się w dyrektywie 1999/93/EC z 13 grudnia 1999 r., gdzie wspomniano, iż usługi związane z podpisem elektronicznym powinny obejmować znakowanie czasem. **Według kolejnych przepisów unijnych, każde poświadczenie daty na terenie jednego z krajów członkowskich jest ważne w pozostałych krajach członkowskich z wyjątkiem Szwecji i Austrii.**

Istnieją trzy podstawowe typy systemów znakowania czasem:

1. System prosty, w którym istnieje jeden urząd TSA, a dane z innych urzędów tego typu nie są brane pod uwagę, co umożliwia działanie w porozumieniu z klientem i np. celowe fałszowanie elektronicznego potwierdzenia daty.
2. System łączony, w którym dane z innych urzędów są włączane podczas znakowania czasem dokumentów, co utrudnia ich fałszowanie, ponieważ użytkownik musiałby działać w porozumieniu ze wszystkimi centrami autoryzacyjnymi.
3. System rozproszony polega na współpracy co najmniej dwóch centrów TSA i publikowaniu specjalnego rekordu bezpieczeństwa zamiast włączania znaczników czasu jednego centrum w ramach znaczników wystawianych przez inne centrum. Po takiej publikacji żaden znacznik czasu wystawiony wcześniej nie może być zmieniony.