**34. Podpis elektroniczny**

*­W tym temacie pewnie chodzi o* ***podpis cyfrowy*** *a nie* ***podpis elektroniczny*** *(są to pojęcia często mylone).* *Ale gdyby komisja się upierała to poniżej kilka słów wyjaśnienia:*

Podpis **elektroniczny** (electronic signature) to operacja podpisywania konkretnych danych (dokumentu) przez osobę fizyczną. Podpisywanie to **dołączanie** **danych** w postaci elektronicznej, do konkretnego! **dokumentu**. Razem, taki zestaw może posłużyć do identyfikacji osoby składającej podpis elektroniczny.

Dokument opatrzony podpisem elektronicznym może być – przy spełnieniu dodatkowych przesłanek – równoważny pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym. Podpis elektroniczny będzie mógł być uznany za równoważny podpisowi własnoręcznemu jeśli spełnia warunki umożliwiające uznanie go za podpis elektroniczny bezpieczny. Zgodnie z ustawą **bezpieczny podpis elektroniczny** to podpis elektroniczny, który:

* jest **przyporządkowany wyłącznie** do osoby składającej ten podpis,
* jest sporządzany za pomocą podlegających **wyłącznej kontroli osoby** **składającej** **podpis** elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
* jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza **zmiana** tych danych **jest** **rozpoznawalna**.

Skutki prawne związane ze złożeniem oświadczenia woli opatrzonego **bezpiecznym** podpisem elektronicznym weryfikowanym przy pomocy ważnego **kwalifikowanego certyfikatu** określa **kodeks** **cywilny**. Zgodnie z tym przepisem [**oświadczenie woli**](http://pl.wikipedia.org/wiki/O%C5%9Bwiadczenie_woli) podpisane takim podpisem ma takie same skutki prawne, jak oświadczenie woli podpisane podpisem własnoręcznym.

**Certyfikat kwalifikowany** to taki, który został wystawiony jego właścicielowi z zastosowaniem odpowiednich procedur weryfikacji tożsamości a ponadto klucz prywatny (służący do składania podpisów) jest przechowywany w sposób bezpieczny (np. na karcie elektronicznej).

Zgodnie z prawem polskim tylko podpis kwalifikowany ma automatycznie takie samo znaczenie jak podpis odręczny. Inne rodzaje podpisu mogą być wiążące prawnie jedynie na podstawie umów cywilnych pomiędzy kontrahentami je stosującymi. Podobne prawodawstwo obowiązuje w większości krajów Unii Europejskiej, chociaż występuje między nimi wiele drobnych różnic, na przykład jeśli chodzi o obowiązek korzystania z bezpiecznego urządzenia (*SSCD*).

Bezpieczny podpis elektroniczny nie zastępuje całkowicie podpisu własnoręcznego. W szczególności nie może go zastąpić, gdy ustawa wymaga podpisu własnoręcznego, jak np. przy **testamencie własnoręcznym** lub **podpisie notarialnie uwierzytelnionym**.

Bezpieczny podpis elektroniczny weryfikowany za pomocą kwalifikowanego certyfikatu spełnia w obrocie prawnym i gospodarczym m.in. następujące funkcje:

* identyfikacyjną,
* dowodową,
* kontraktową.

W prawie wspólnotowym skutki prawne podpisu elektronicznego są przedmiotem regulacji *Dyrektywy o Wspólnotowej Infrastrukturze Podpisów Elektronicznych*. Prawo unijne wyróżnia następujące rodzaje podpisu elektronicznego:

* **Podpis elektroniczny** – czyli deklaracja tożsamości autora, złożona w formie elektronicznej pod dokumentem. Dane w postaci elektronicznej, które służą do identyfikacji osoby go składającej.
* **Zaawansowany (bezpieczny)** podpis elektroniczny – czyli podpis, który za pomocą odpowiednich środków technicznych (kryptograficznych) jest jednoznacznie i w sposób trudny do sfałszowania związany z dokumentem oraz autorem. Kategoria ta odnosi się do większości systemów tradycyjnie nazywanych podpisem elektronicznym i wykorzystujących różne algorytmy kryptograficzne dla zapewnienia bezpieczeństwa.
* **Kwalifikowany** podpis elektroniczny – czyli taki podpis zaawansowany, który został złożony przy pomocy **certyfikatu kwalifikowanego** oraz przy użyciu **bezpiecznego urządzenia** do składania podpisu (SSCD).

Podsumowując, pojęcie podpis elektroniczny (electronic signature) jest wprowadzone przez unijną Dyrektywę i jednoznacznie określa, że jest to operacja podpisywania konkretnych danych (dokumentu) przez osobę fizyczną.

Od strony technicznej podpis elektroniczny jest realizowany za pomocą mechanizmów **podpisu cyfrowego**.

Podpis cyfrowy służy zapewnieniu między innymi następujących funkcji:

1. **autentyczności**, czyli pewności co do autorstwa dokumentu,
2. **niezaprzeczalności nadania informacji**, nadawca wiadomości nie może wyprzeć się wysłania wiadomości, gdyż podpis cyfrowy stanowi dowód jej wysłania (istnieją także inne rodzaje niezaprzeczalności),
3. **integralności**, czyli pewności, że wiadomość nie została zmodyfikowana po złożeniu podpisu przez autora.

**Podpis cyfrowy** (digital signature) to matematyczny sposób potwierdzania autentyczności cyfrowego dokumentu. **Istnieje wiele schematów podpisów cyfrowych, obecnie jednak najpopularniejszym jest schemat podpisu dokumentów cyfrowych w systemach kryptograficznych z kluczem publicznym i jednokierunkową funkcją skrótu** - w systemie tym do oryginalnej wiadomości dołączany jest skrót dokumentu, zaszyfrowany prywatnym kluczem nadawcy. Skrót sporządzony jest za pomocą funkcji haszującej, np. MD5 (zalecana do 1999 roku), SHA1 (zalecana do 2010 roku), SHA2. W roku 2012 będzie wybrany algorytm SHA3 (spośród tych zgłoszonych do publicznego konkursu organizowanego przez amerykański instytut NIST). Potwierdzenie autentyczności wiadomości jest możliwe po odszyfrowaniu skrótu kluczem publicznym nadawcy i porównaniu go z wytworzonym przez siebie skrótem odebranego dokumentu.

Innymi słowy: Strona uwierzytelniająca wylicza skrót (ang. **hash**) podpisywanej wiadomości. Następnie **szyfruje** ten skrót swoim kluczem prywatnym i jako podpis cyfrowy **dołącza** do oryginalnej wiadomości. Dowolna osoba posiadająca klucz publiczny może sprawdzić autentyczność podpisu, poprzez odszyfrowanie skrótu za pomocą klucza publicznego nadawcy i porównanie go z własnoręcznie wyliczonym na podstawie wiadomości. Działają tak np. certyfikaty SSL na zabezpieczonych stronach WWW (https).

Szyfrowanie/deszyfrowanie odbywa się przy użyciu algorytmów kryptografii (*asymetrycznych, bo jest klucz prywatny i publiczny*) takich, jak RSA czy ELGamal (2 najpopularniejsze). Podpis tej samej wiadomości w RSA jest zawsze identyczny. W ElGamalu i DSA każdy kolejny podpis tej samej wiadomości zwykle jest inny – co ma znaczenie w niektórych zastosowaniach.

*Co do kluczy prywatnych i publicznych*: we wszystkich kryptosystemach (czy to RSA czy Elgamal) uzyskanie klucza **prywatnego** **na podstawie** **publicznego** musi być **obliczeniowo trudne**. Klucz publiczny może być obliczony na podstawie prywatnego, co zresztą ma miejsce podczas generacji kluczy w ElGamal.

Najpopularniejsze standardy pozwalające na złożenie podpisu elektronicznego to **X.509 oraz PGP**.

**PGP** jest systemem zdecentralizowanym, w którym poziom autentyczności danego klucza jest determinowany przez sumę podpisów, złożonych przez różne osoby znające posiadacza klucza (model Sieć zaufania). System ten jest powszechnie wykorzystywany w Internecie oraz w środowiskach korporacyjnych (np. niektóre systemy EDI).

**Sieć zaufania** (ang. web of trust) to zdecentralizowana metoda uwierzytelniania osób, w której nie ma hierarchicznej struktury organizacji uwierzytelniających, a zaufanie do poszczególnych certyfikatów jest sumą podpisów złożonych przez innych uczestników sieci.

Każdy uczestnik sieci podpisuje klucze osób, które osobiście zweryfikował. Podpis stanowi poświadczenie, że osoba podpisująca jest przekonana o autentyczności klucza oraz tym, że faktycznie należy on do osoby, która deklaruje że jest jego właścicielem.

Jeśli ktoś z uczestników sieci chce sprawdzić czy pewien klucz rzeczywiście należy do danej osoby, próbuje ułożyć łańcuch zaufania w postaci: "Ja zweryfikowałem że X to X i podpisałem jego klucz KX, X zweryfikował że Y to Y i podpisał jego klucz KY, itd., Z zweryfikował że sprawdzany klucz rzeczywiście należy do tej osoby."

System **X.509** jest systemem scentralizowanym, w którym autentyczność klucza jest gwarantowana przez hierarchię centrów certyfikacji formalnie poświadczających związek klucza z tożsamością jego właściciela. Ze względu na jednoznaczną odpowiedzialność, łatwiejszą do osadzenia w prawie, X.509 jest obecnie dominującym systemem, na którym opiera się aktualnie obowiązujące prawodawstwo o podpisie elektronicznym.

"Podpis" składany przez **centrum/urząd certyfikacji** pod certyfikatem osoby fizycznej nazywa się "poświadczeniem elektronicznym" *(chyba dlatego, że ‘podpis’ to w polskim prawie słowo zarezerwowane dla osób fizycznych)*, zaś sam certyfikat centrum - "zaświadczeniem certyfikacyjnym".

W Polsce instytucją certyfikującą pozostałych wystawców certyfikatów (centra certyfikacji/urzędy certyfikacji) jest Narodowe Centrum Certyfikacji. Podmioty wydające certyfikaty kwalifikowane to: Krajowa Izba Rozliczeniowa SA, Polska Wytwórnia Papierów Wartościowych SA (Sigillum) i Unizeto Technologies SA (Certum).

*Ważniejsze pojęcia:*

CA - Certification Authority - **urząd certyfikacji** - wystawia certyfikaty, listy CRL, certyfikuje inne CA.

RA - Registration Authority - **urząd rejestracji** - zbiera wnioski o wydanie certyfikatu, weryfikuje tożsamość subskrybentów.

**Subskrybent** - właściciel certyfikatu.