

*Między nieznaną przyszłością, a tym co w krwi się dopiero budzi  
powstaje nowa tajemnica ...*

*Czas płynie...  
siłą woli i cierpliwości rzeźbiony jest kolejny dzień*

---

*Najwspanialszym przyjaciołom,  
którzy zawsze są blisko mnie  
składam podziękowania*

U n i w e r s y t e t   M i k o ł a j a   K o p e r n i k a  
W y d z i a ł   P r a w a   i   A d m i n i s t r a c j i

Katarzyna Misiowska

*Podpis elektroniczny w prawie  
porównawczym*

Praca magisterska napisana  
w Katedrze Prawa Cywilnego  
i Obrotu Gospodarczego  
pod kierunkiem  
prof. dr hab. Mirosława Nesterowicza

T o r u ń   2 0 0 1

# *Spis treści*

---

<b>Wstęp</b>	<b>6</b>
<b>Część I Cywilno – prawne zagadnienia podpisu elektronicznego</b>	<b>9</b>
<b>Rozdział 1 Podpis elektroniczny i jego rodzaje</b>	<b>10</b>
1.1. Zagadnienia wstępne	10
1.1.1 Podpis a technologia jego tworzenia	10
1.1.2 Rodzaj podpisu elektronicznego z uwagi na skutki jego zastosowania	11
1.2. Austria	11
1.3. Niemcy	12
1.4. Polska	12
1.5. Podpis elektroniczny w innych państwach	13
1.5.1. Australia	13
1.5.2. Finlandia	13
1.5.3. Hong Kong	14
1.5.4. Illinois	14
1.5.5. India	14
1.5.6. Irlandia	15
1.5.7. Japonia	15
1.5.8. Kolumbia	15
1.5.9. Singapur	16
1.5.10. Wielka Brytania	17
1.5.11. USA	17
1.6. ONZ – UNCITRAL	18
1.7. Unia Europejska	19
1.8. Podsumowanie	19
1.8.1 Aspekt 1. Definicja podpisu elektronicznego z uwagi na technologię jego tworzenia	19
1.8.2 Aspekt 2. Definicja – czym jest podpis elektroniczny	20
1.8.3 Aspekt 3. Konstrukcja definicji podpisu elektronicznego a praktyka	20
<b>Rozdział 2 Skutki podpisu elektronicznego</b>	<b>22</b>
2.1. Zagadnienia wstępne	22
2.2. Austria	22
2.2.1. Ogólne skutki prawne	22
2.2.2. Szczegółowe skutki prawne	23
2.3. Niemcy	25
2.4. Polska	25
2.4.1 Skutki z zastosowania bezpiecznego podpisu elektronicznego	26
2.5. ONZ – UNCITRAL	26
2.6. Unia Europejska	27
2.6.1 Skutki zastosowania zaawansowanego podpisu elektronicznego	27
2.7 Podsumowanie	28

<b>Rozdział 3 Podpisujący i weryfikujący podpis</b>	<b>33</b>
3.1. Zagadnienia wstępne	33
3.2. Austria	33
3.3. Niemcy	34
3.4. Polska	34
3.4.1. Podpisujący	34
3.4.2. Weryfikujący podpis	34
3.5. ONZ – UNCITRAL	35
3.5.1. Podpisujący	35
3.5.2. Weryfikujący podpis	35
3.6. Unia Europejska	37
3.6.1. Podpisujący	37
3.6.2. Weryfikujący podpis	37
3.7. Podsumowanie	38
<b>Część II Administracyjno – prawne zagadnienia podpisu elektronicznego</b>	<b>40</b>
<b>Rozdział 1 Usługodawcy certyfikacyjni</b>	<b>41</b>
1.1. Zagadnienia wstępne	41
1.2. Austria	42
1.2.1. Pojęcie usługodawcy certyfikacyjnego	42
1.2.2. Rozpoczęcie działalności certyfikacyjnej	42
1.2.3. Datownik	43
1.2.4. Rejestry	43
1.2.5. Zawieszenie działalności	43
1.3. Niemcy	44
1.4. Polska	44
1.4.1. Pojęcie podmiotu świadczącego usługi certyfikacyjne	44
1.4.2. Wymogi dla usługodawców certyfikacyjnych	45
1.4.3. Działalności certyfikacyjna	50
1.4.4. Znakowanie czasem	50
1.4.5. Odpowiedzialność usługodawcy certyfikacyjnego	51
1.4.6. Ochrona danych	51
1.4.7. Dokumentacja	52
1.5. ONZ – UNITRAL	53
1.6. Unia Europejska	54
<b>Rozdział 2 Certyfikaty</b>	<b>56</b>
2.1. Zagadnienia wstępne	56
2.2. Austria	56
2.2.1. Pojęcie i rodzaje certyfikatów	56
2.2.2. Wymogi dla usługodawcy certyfikacyjnego	57
2.2.3. Sprawdzanie tożsamości	59
2.2.4. Unieważnienie certyfikatu	59
2.3. Niemcy	60
2.4. Polska	62
2.4.1. Pojęcie i rodzaje certyfikatów	62
2.4.2. Unieważnianie certyfikatów	63
2.5. ONZ – UNITRAL	66

2.6. Unia Europejska	66
<b>Rozdział 3 Nadzór</b>	<b>67</b>
3.1. Zagadnienia wstępne	67
3.2. Austria	67
3.2.1. Organ nadzoru	67
3.2.2. Środki nadzoru	69
3.2.3. Spółka Telekom-Control GmbH	70
3.2.4. Współpraca z organem nadzorczym	71
3.3. Polska	71
3.3.1. Organ i środki nadzoru	71
<b>Część III Techniczne zagadnienia podpisu elektronicznego</b>	<b>75</b>
<b>Rozdział 1 Szyfrowanie</b>	<b>76</b>
1.1. Zagadnienia wstępne	76
1.2. Kryptografia symetryczna	77
1.2.1. Algorytm DES – istota działania	77
1.2.2. Szybkość i bezpieczeństwo	78
1.2.3. Schemat działania algorytmów wykorzystywanych w kryptografii symetrycznej w uproszczeniu	79
1.3. Kryptografia asymetryczna	81
1.3.1. Algorytm RSA – istota działania	81
1.3.2. Schemat działania algorytmów wykorzystywanych w kryptografii asymetrycznej	82
<b>Rozdział 2 Uwierzytelnianie</b>	<b>85</b>
2.1. Zagadnienia wstępne	85
2.2. Jednokierunkowa funkcja skrótu	85
2.3. Polityka certyfikacyjna i proces certyfikacji	90
2.3.1. Podmioty biorące udział w elektronicznej wymianie dokumentów i ich obowiązki	91
2.3.2. Proces uzyskania certyfikatu	92
<b>Zakończenie</b>	<b>94</b>
<b>Bibliografia</b>	<b>96</b>
Dokumenty i materiały	96
Opracowania książkowe	97
Artykuły	97
Inne źródła	100

W obecnym stanie rozwoju technologicznego coraz częściej używaną formą składania oświadczeń woli staje się forma elektroniczna. Jest to możliwe dzięki powszechności dostępu do Internetu i związanej z nim komunikacji sieciowej. Coraz więcej osób zamiast wyjść z domu i załatwić sprawy na poczcie, w banku, w zusie, w sklepie, wymienić informacje ze znajomymi – włącza komputer i załatwia te sprawy przez sieć. Z sieci korzystają uczniowie i studenci, kobiety i mężczyźni, ludzie o różnych profesjach i zainteresowaniach: biznesmani i prawnicy, ekonomiści i majordomusi. Nie wychodząc z domu można porozmawiać z ludźmi w czasie rzeczywistym (np. przez IRC<sup>1</sup>, ICQ<sup>2</sup>, CHAT<sup>3</sup>), podzielić się swoją wiedzą i zasięgnąć opinii na dany temat (np. poprzez grupy dyskusyjne, używając kont pocztowych

e-mail), obejrzeć oferty znanych firm (e-sklepy), przejrzeć prasę (np. [www.rzeczpospolita.pl](http://www.rzeczpospolita.pl)), zobaczyć co dzieje się w Polsce i w świecie itd. Możliwości korzystania z Internetu jest mnóstwo. Z jednej strony upowszechnianie nowoczesnych technik komunikacji pozwala na rozwój handlu, nauki, kultury, z drugiej strony stwarza niebezpieczeństwo naruszeń prywatności użytkowników i ataków hackerów. Postęp w tej dziedzinie jest możliwy tylko za sprawą stworzenia takich instrumentów prawnych, które umożliwią bezpieczny obrót prawny i pozwolą na skuteczne i bezpieczne wskazanie tożsamości podmiotów uczestniczących w elektronicznym obrocie prawnym. Obie strony muszą mieć pewność, że poufne informacje, które wysyłają i które zostają do nich wysyłane przychodzą w niezmienionej postaci, nikt nie ma względu w ich treść, a nadawcą jest rzeczywiście ten, kto się za niego podaje. Rozwiązaniem tego problemu jest wprowadzenie instytucji podpisu elektronicznego.

---

<sup>1</sup> IRC – *Internet Relay Chat* – usługa dająca możliwość rozmowy grupy ludzi w czasie rzeczywistym. Rozmowy odbywają się na tzw. kanałach, gdzie może rozmawiać na raz kilkudziesięciu osób jednocześnie.

<sup>2</sup> ICQ - *Od I seek you* – “szukam cię” – jest to usługa podobna do IRC, również rozmowy odbywają się w czasie rzeczywistym, z tą jednak różnicą, że odbywa się to na zasadzie wysyłania i otrzymywania krótkich wiadomości tekstowych, dodatkowa funkcją tej usługi jest możliwość wysyłania krótkich wiadomości tekstowych (SMS) do użytkowników sieci komórkowych.

<sup>3</sup> Chat – rozmowa, usługa podobna do IRC, z tą różnicą, że korzysta się z niej za pomocą korzystania ze stron www.

Przedstawienie tematu podpisu elektronicznego w różnych systemach prawnych nie jest sprawą prostą. Z uwagi na złożoność zagadnienia praca została pomyślana jako opracowanie składające się z trzech części. Każda część z innej strony przedstawia zagadnienia podpisu elektronicznego, co pozwala dokonać swoistej systematyki zagadnień. Dwie pierwsze części to elementy składowe pewnej całości nie mogące samodzielnie zaistnieć bez pozostałej. Trzecia część to technologiczne rozwiązania podpisu elektronicznego.

Pierwsza część zawiera zagadnienia cywilno – prawne. W tej części wyjaśnione zostanie pojęcie podpisu elektronicznego i jego rodzajów. Jakie wywoła skutki zastosowanie podpisu elektronicznego oraz kto i w jakim zakresie może posługiwać się podpisem elektronicznym.

Druga część zawiera zagadnienia administracyjno – prawne. Przedstawiony zostanie cały aparat wykonawczy. Aparat ten jest ściśle związany z jedyną sprawdzoną i współcześnie wykorzystywaną technologią tworzenia podpisu elektronicznego tj. technologią wykorzystującą kryptografię. Każdy podmiot przystępujący do wymiany elektronicznie podpisanych dokumentów będzie musiał przejść określoną drogę od usługodawców certyfikacyjnych po uzyskanie certyfikatu. Dlatego działalność usługodawców certyfikacyjnych, ich obowiązki i odpowiedzialność oraz nadzór nad działalnością podmiotów zajmujących się certyfikacją to główne tematy tej części pracy.

Trzecia część to opis technologii kryptograficznej wykorzystywanej przez niekwestionowanego lidera w tym zakresie – USA. Stany Zjednoczone mają najbardziej rozbudowaną sieć na świecie, a technologie kryptograficzne u nich są lepiej rozwinięte niż w krajach europejskich. Wzbogacenie pracy o ten wątek sprawi, że praca stanie się, nie tylko ciekawsza, ale dzięki temu jaśniej i pełniej będzie mogła przedstawić istotę podpisu elektronicznego nie tylko od strony prawnej, ale także praktycznej. Pomimo tego, że technologia kryptograficzna zostanie przedstawiona tylko w stopniu, w jakim pozwoli zrozumieć istotę podpisu od strony praktycznej, powiększa niestety rozmiary mojej pracy. Zawsze jest coś kosztem czegoś. W tym wypadku umieszczenie wątku o kryptografii odbyło kosztem pominięcia regulacji USA. Czy wybór był trafny – okaże się pod koniec pracy. Ponadto zostanie przedstawione jak z polityką certyfikacyjną radzą sobie niektóre polskie podmioty.

W pracy opierałam się na ustawodawstwach wybranych państw europejskich oraz regulacjach organizacji międzynarodowych:

1. Austria: Federalna Ustawa o Podpisie Elektronicznym (SigG)<sup>4</sup>
2. Niemcy: Artykuł 3 (ustawa o podpisie cyfrowym – Gesetz zur digitalen Signatur – Signaturgesetz – SigG) ustawy z dnia 22 lipca 1997r o usługach informacyjnych i komunikacyjnych (Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste).
3. Polska: ustawa o podpisie elektronicznym z 2001r<sup>5</sup>
4. Uncitral: ustawa modelowa dotycząca zagadnień prawnych związanych z Elektronicznym Przekazem Danych (Electronic Data Interchange – EDI)<sup>6</sup> oraz projekt modelowej ustawy o podpisie elektronicznym<sup>7</sup>,
5. Unia Europejska: Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 13 grudnia 1999r w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego – 99/93 WE<sup>8</sup>

Omówienie poszczególnych rozdziałów tematycznych następuje wg wyżej przedstawionej alfabetycznej kolejności państw i później organizacji międzynarodowych. Przedstawienie zagadnienia zawsze zaczyna się od zaprezentowania stanowiska austriackiego. W związku z tym zostaje ono omówione najdokładniej, a pozostałe regulacje będą porównywane do tego stanowiska.

Zadaniem, które postawiłam sobie przed napisaniem pracy było przedstawienie całego mechanizmu, istoty i celu podpisu elektronicznego uwzględniając podobieństwa i różnice wybranych systemów prawnych.

---

<sup>4</sup> tłumaczenie pochodzi ze strony <http://www.ipipan.pl>

<sup>5</sup> źródło <http://www.sejm.gov.pl>

<sup>6</sup> tłumaczenie pochodzi z: Wojciech Kocot „Zawieranie umów sprzedaży według Konwencji Wiedeńskiej” Warszawa 1998r.

<sup>7</sup> tłumaczenie pochodzi z artykułu: Jerzy Gawel, Marek Świerczyński „Podpis elektroniczny” Kwartalnik Prawa Prywatnego Polska Akademia Umiejętności Rok X, z.1, Kraków 2001, str. 208-212.

<sup>8</sup> tłumaczenie pochodzi ze strony <http://www.sejm.gov.pl>

***Cz ę ś ć I***

---

*Cywilno – prawne zagadnienia podpisu elektronicznego*

# ***R o z d z i a ł 1***

## ***Podpis elektroniczny i jego rodzaje***

### ***1.1. Zagadnienia wstępne***

#### ***1.1.1 Podpis a technologia jego tworzenia***

Z definicją podpisu elektronicznego powiązana jest kwestia technologii jego tworzenia. W tym zakresie istnieją dwie koncepcje. Pierwsza z nich daje pierwszeństwo ściśle określonej technologii tworzenia podpisu, natomiast druga pod względem technologicznym jest neutralna.

Pierwsza koncepcja jest oparta o ściśle określoną technologię. W naszych czasach jedyną wykorzystywaną technologią do tworzenia podpisów elektronicznych jest technologia kryptograficzna. Jeżeli na dokumencie elektronicznym składany jest podpis w oparciu o tą technologię – jest to podpis cyfrowy i takim pojęciem powinno się posługiwać dla określenia podpisu elektronicznego wytworzonego tą metodą. Trzeba zaznaczyć, że podpis cyfrowy jest tylko jednym z wielu możliwych sposobów elektronicznego podpisywania dokumentów. Pojęć „podpis cyfrowy” i „podpis elektroniczny” nie można używać zamiennie. Podpis cyfrowy jest podpisem elektronicznym, natomiast nie każdy podpis elektroniczny będzie podpisem cyfrowym, a tylko ten, który będzie oparty na infrastrukturze klucza publicznego.

Drugie podejście w tej kwestii to neutralność technologiczna. Jest to stanowisko olbrzymiej większości państw i organizacji międzynarodowych. Nie dyskryminuje ono żadnej z metod tworzenia podpisu elektronicznego, wręcz przeciwnie. Wszystkie technologie nawet te, które jeszcze nie istnieją, jeżeli spełnią określone<sup>9</sup> warunki, zostaną zaakceptowane. O ile chodzi o podpis otwarty na technologię używa się pojęcia podpis elektroniczny. Podpis elektroniczny to pojęcie szerokie. Zawiera w swej treści różne sposoby elektronicznej identyfikacji człowieka. Oprócz podpisu cyfrowego możemy wymienić jeszcze inne sposoby np. biometryczne - odcisk palca, wzór dna oka lub DNA, które w przyszłości możliwe,

że będą używane. Wszystkie państwa i organizacje międzynarodowe, które hołdują opcji neutralności technologicznej posługują się pojęciem podpisu elektronicznego. Do tego bloku należą uregulowania np.: Austrii, Polski, projekt ustawy modelowej UNITRAL i Dyrektywa Unii Europejskiej.

### ***1.1.2 Rodzaj podpisu elektronicznego z uwagi na skutki jego zastosowania***

Drugą kwestią, na którą należy zwrócić uwagę to podział podpisu elektronicznego na rodzaje z uwagi na skutki jego zastosowania. O podziale na rodzaje mówi się dopiero wtedy, gdy nie ma ograniczenia do ściśle określonej technologii jego tworzenia, czyli w systemach hołdujących opcji neutralności technologicznej. Co do zasady istnieją dwa rodzaje podpisu elektronicznego: zwykły<sup>10</sup> i szczególny. Każdy z nich musi spełnić określone wymagania i wywołuje określone skutki prawne.

Poniżej zostanie przedstawione stanowiska poszczególnych państw i organizacji międzynarodowych, rodzaje podpisów elektronicznych i warunki jakie muszą spełniać.

---

## *1.2. Austria*

Austria znajduje się w bloku popierającym koncepcję neutralności technologicznej tworzenia podpisu elektronicznego. W związku z tym ustawa austriacka posługuje się pojęciem podpisu elektronicznego, a nie podpisu cyfrowego i zawiera definicję dwóch kategorii podpisów tj. zwykłego podpisu elektronicznego<sup>11</sup> i bezpiecznego podpisu elektronicznego. Podpis elektroniczny zwykły to dane elektroniczne dołączone do innych danych elektronicznych lub z nimi związane, służące do uwierzytelnienia, czyli do potwierdzenia tożsamości sygnatariusza.

---

<sup>9</sup> chodzi tu w ogólnym zarysie o bezpieczeństwo: pewność, integralność i poufność danych.

<sup>10</sup> w aktach państw i organizacji nie ma pojęcia „zwykły” i „szczególny”, są tylko „podpis elektroniczny” i w zależności od państwa np. „bezpieczny podpis elektroniczny”. „Bezpieczny podpis elektroniczny” w porównaniu do „podpisu elektronicznego” nie obdarzonego żadnym przymiotnikiem

i wyraźnie wywołujący inne skutki prawne, niewątpliwie jest szczególną kategorią podpisu, w związku z czym posłużyłam się pojęciami „zwykły” i „szczególny” dla odróżnienia obu tych kategorii podpisów elektronicznych na potrzeby mojej pracy.

Bezpieczny podpis elektroniczny natomiast to zgodnie z § 2 pkt. 3 w/w ustawy to podpis elektroniczny spełniający następujące warunki:

- a) jest przydzielony wyłącznie sygnatariuszowi,
- b) umożliwia ustalenie tożsamości sygnatariusza,
- c) jest utworzony przy użyciu urządzeń, które znajdują się pod wyłączną kontrolą sygnatariusza,
- d) jest powiązany z opatrzonymi tym podpisem danymi w sposób umożliwiający stwierdzenie, czy nastąpiła jakakolwiek zmiana w danych po złożeniu podpisu,
- e) jest oparty na kwalifikowanym certyfikacie oraz jest utworzony przy użyciu środków technicznych i procedur zgodnych z wymaganiami w zakresie zabezpieczeń stawianych przez ustawę i przez rozporządzenie wydane na jej podstawie.

---

### *1.3. Niemcy*

Niemieckie uregulowanie celowo posługuje się pojęciem podpisu cyfrowego. Oznacza to, że Niemcy, jako nieliczni, przyznali priorytet określonej technologii tworzenia podpisu tj. technologii opartej o kryptografię klucza jawnego.

Podpis cyfrowy na gruncie prawa niemieckiego to swoista wyrobiona pieczęć uzyskana za pomocą klucza prywatnego. Służy do sygnowania cyfrowych informacji, których autentyczność zostaje stwierdzona dzięki kluczowi publicznemu. W klucz publiczny i certyfikat tego klucza należy zaopatrzyć się w odpowiednim urzędzie.

Jak widać jest to szczegółowa definicja, zawierająca w swej treści wiele technicznych pojęć jak: klucz prywatny, klucz publiczny, certyfikat, urząd do wydawania certyfikatów.

---

### *1.4. Polska*

Zgodnie z polską ustawą podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis

---

<sup>11</sup> w ustawie występuje pojęcie „podpisu elektronicznego” przymiotnik „zwykły” został dodany umownie dla odróżnienia od bezpiecznego podpisu elektronicznego.

elektroniczny. W ustawie występuje również pojęcie bezpiecznego podpisu elektronicznego. Jest to podpis elektroniczny, który:

- a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- b) 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,
- c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

## 1.5. Podpis elektroniczny w innych państwach

### **1.5.1. Australia**

Ustawa o transakcjach elektronicznych z 1999r<sup>12</sup> :

Jeżeli zgodnie z prawem Związku wymagany jest podpis osoby, taki wymóg uważa się za spełniony w związku z komunikacją elektroniczną jeżeli:

- a) we wszystkich przypadkach - używa się metody w celu identyfikacji osoby oraz wykazania jej zgody na komunikowaną informację; oraz
- b) we wszystkich przypadkach - mając na względzie wszystkie stosowne okoliczności w czasie, kiedy użyta metoda była w takim stopniu wiarygodna, w jakim jest to właściwe na potrzeby w jakich informacja była komunikowana; oraz
- c) jeżeli wymagane jest przekazanie podpisu jednostce Związku lub osobie działającej w imieniu Związku, a jednostka żąda, aby użyta metoda opisana w paragrafie (a) spełniała szczególne wymogi technologii informatycznej - wymóg jednostki został spełniony; oraz
- d) jeżeli wymagane jest przekazanie podpisu osobie, która nie jest ani jednostką Związku ani osobą działającą w imieniu Związku - osoba do której wymagane jest przekazanie podpisu zgadza się na spełnienie wymogu w drodze użycia metody opisanej w paragrafie (a).

### **1.5.2. Finlandia**

Ustawa o usługach elektronicznych w administracji<sup>13</sup>:

---

<sup>12</sup> informacje zaczerpnięte ze strony <http://www.prawo.hoga.pl>

<sup>13</sup> ibidem

Podpis elektroniczny oznacza zestaw danych, które potwierdzają integralność i autentyczność wiadomości elektronicznej przez użycie metody, która jest dostępna do publicznej kontroli.

### **1.5.3. Hong Kong**

Zarządzenie w sprawie transakcji elektronicznych<sup>14</sup>:

Podpis cyfrowy w relacji do zapisu elektronicznego oznacza podpis elektroniczny osoby podpisującej wygenerowany poprzez transformację zapisu elektronicznego przy użyciu kryptosystemu asymetrycznego oraz funkcji hash'ującej w ten sposób, że osoba, która posiada początkowy przetransformowany w odwrotną stronę zapis elektroniczny oraz klucz publiczny osoby podpisującej, może określić:

- a) czy transformacja była generowana przy użyciu klucza prywatnego zgodnego z kluczem publicznym osoby podpisującej; i
- b) czy początkowy zapis elektroniczny był zmieniany od czasu wygenerowania transformacji.

### **1.5.4. Illinois**

Ustawa o bezpieczeństwie handlu elektronicznego z 1998r<sup>15</sup>:

Podpis elektroniczny to podpis w formie elektronicznej dołączony albo logicznie związany z zapisem elektronicznym.

### **1.5.5. India**

Ustawa o Technologii Informacyjnej 2000r<sup>16</sup>:

Podpis cyfrowy oznacza potwierdzenie autentyczności każdego zapisu elektronicznego przez podpisującego w drodze użycia elektronicznej metody lub procedury zgodnej z przepisami artykułu 3 (używając kryptosystemu asymetrycznego i funkcji hash'ującej).

Bezpieczny podpis cyfrowy: Jeżeli przez użycie bezpiecznej procedury uzgodnionej przez zainteresowane strony jest możliwe zweryfikowanie, że podpis cyfrowy, w granicach w jakich był złożony, był:

---

<sup>14</sup> ibidem

<sup>15</sup> informacje zaczerpnięte z artykułu: Jerzy Gawęł, Marek Świerczyński „Podpis elektroniczny” Kwartalnik Prawa Prywatnego Rok X, 2001, z.1 Polska Akademia Umiejętności, Kraków 2001, str.198-199.

- a) unikalny dla osoby składającej podpis;
- b) zdalny do identyfikacji takiej osoby;
- c) stworzony za pomocą środków, które znajdują się pod wyłączną kontrolą podpisującego i związany z elektronicznym zapisem do którego się odnosi w taki sposób, że w razie zmiany zapisu elektronicznego podpis cyfrowy staje się nieważny, to taki podpis cyfrowy może być uważany za bezpieczny podpis cyfrowy.

### ***1.5.6. Irlandia***

Ustawa o handlu elektronicznym 2000r<sup>17</sup>:

Podpis elektroniczny oznacza dane w formie elektronicznej dołączone, inkorporowane lub logicznie związane z innymi danymi elektronicznymi i które służą jako metoda potwierdzenia autentyczności osoby od której pochodzi, i zawiera zaawansowany podpis elektroniczny.

### ***1.5.7. Japonia***

Prawo dotyczące podpisów elektronicznych i usług certyfikacyjnych<sup>18</sup>:

Podpis elektroniczny oznacza zaszyfrowany środek użyty w celu wskazania osoby tworzącej odnośnie do informacji zapisanej w zapisie elektromagnetycznym i który operuje metodą pozwalającą na weryfikację czy nastąpiła lub nie nastąpiła zmiana wypowiedzianej informacji.

### ***1.5.8. Kolumbia***

Prawo o handlu elektronicznym<sup>19</sup>:

Podpis cyfrowy powinien być rozumiany jako wartość numeryczna przynależna lub załączona do wiadomości, która poprzez użycie procedury matematycznej, połączona z hasłem osoby inicjującej i z tekstem wiadomości, pozwala ustalić, że taka wartość została uzyskana wyłącznie przez hasło osoby inicjującej, a początkowa wiadomość nie została zmieniona po wykonaniu transformacji.

---

<sup>16</sup> <http://www.hoga.prawo.pl>

<sup>17</sup> ibidem

<sup>18</sup> ibidem

<sup>19</sup> ibidem

### **1.5.9. Singapur**

Ustawa o transakcjach elektronicznych z 1998r<sup>20</sup>:

Podpis elektroniczny definiuje się jako litery, znaki, cyfry oraz inne symbole w formie cyfrowej dołączone lub logicznie powiązane z zapisem elektronicznym, oraz wykonywane lub przyjmowane na potrzeby potwierdzenia autentyczności lub zatwierdzenia zapisu elektronicznego.

Bezpieczny podpis elektroniczny: Jeżeli poprzez użycie zalecanej bezpiecznej procedury lub właściwej z handlowego punktu widzenia bezpiecznej procedury uzgodnionej przez zainteresowane strony możliwa jest weryfikacja tego, że podpis elektroniczny w czasie złożenia był:

- a) unikalny dla osoby składającej podpis;
- b) zdalny do identyfikacji takiej osoby;
- c) stworzony za pomocą środków, które znajdują się pod wyłączną kontrolą podpisującego; oraz
- d) związany z elektronicznym zapisem do którego się odnosi w taki sposób, że w razie zmiany zapisu elektronicznego podpis elektroniczny staje się nieważny, to taki podpis elektroniczny może być uznawany za bezpieczny podpis elektroniczny.

Podpis cyfrowy jest definiowany jako podpis elektroniczny składający się z transformacji zapisu elektronicznego przy użyciu kryptosystemu asymetrycznego oraz funkcji hash'ującej w ten sposób, że osoba, która posiada początkowy przetransformowany w odwrotną stronę zapis elektroniczny oraz klucz publiczny osoby podpisującej, może dokładnie określić:

- a) czy transformacja była wytworzona przy użyciu klucza prywatnego zgodnego z kluczem publicznym osoby podpisującej; i
- b) czy początkowy zapis elektroniczny był zmieniany od czasu wytworzenia transformacji.

Bezpieczny podpis cyfrowy: Gdy jakaś część zapisu elektronicznego jest podpisana podpisem cyfrowym, podpis cyfrowy powinien być traktowany jako bezpieczny podpis cyfrowy odnośnie do takiej części zapisu jeżeli:

---

<sup>20</sup> ibidem oraz <http://www.prawo.hoga.pl>

- a) podpis cyfrowy został stworzony podczas okresu operacyjnego obowiązującego certyfikatu i jest zweryfikowany w odniesieniu do klucza publicznego zamieszczonego w takim certyfikacie; oraz
- b) certyfikat jest uważany za godny zaufania, w tym ściśle wiąże klucz publiczny z tożsamością osoby ponieważ:
  - certyfikat został wydany przez licencjonowane władze certyfikacyjne działające zgodnie z przepisami art. 42;
  - certyfikat został wydany przez władze certyfikacyjne spoza Singapuru urzędowo dopuszczone w tym celu przez Kontrolera zgodnie z przepisami art. 43;
  - certyfikat został wydany przez departament lub ministerstwo Rządu, organ Państwa lub statutową korporację zatwierdzoną przez Ministra, aby działać jako władza certyfikacyjna na warunkach jakie może on na podstawie przepisów narzucić lub skonkretyzować; lub
  - strony wyraźnie uzgodniły między sobą (nadawca i adresat), aby użyć podpisu cyfrowego jako bezpiecznej procedury, a podpis cyfrowy był właściwie zweryfikowany w odniesieniu do klucza publicznego nadawcy.

### **1.5.10. Wielka Brytania**

Ustawa o komunikacji elektronicznej z 2000r<sup>21</sup>:

Podpis elektroniczny jest wszystkim w formie elektronicznej jeżeli:

- a) jest inkorporowane lub w inny sposób logicznie związane z komunikacją elektroniczną lub elektronicznymi danymi; oraz
- b) inkorporacja lub związanie wyraża się w celu ustalenia autentyczności komunikacji lub danych, lub integralności komunikacji lub danych, lub jednego i drugiego.

### **1.5.11. USA**

Ustawa o podpisach elektronicznych w handlu krajowym i globalnym (Electronic Signatures in Global and National Commerce Act) z 24.01.2000r<sup>22</sup> :

---

<sup>21</sup> ibidem

<sup>22</sup> informacje na temat rozwiązań prawnych USA zaczerpnęłam z artykułu: Arkadiusz Koper „Podpis elektroniczny prawna gwarancja bezpieczeństwa rynku informatycznego (cz.I)” Internet Multimedia Oprogramowanie Komputer w firmie nr 6(17) czerwiec 2001r INFOR, str.15-18 oraz ze strony <http://www.prawo.hoga>

Podpis elektroniczny oznacza elektroniczny dźwięk, symbol lub proces, dołączony lub logicznie powiązany z zapisem i wykonywany lub przyjęty przez osobę z zamiarem podpisania zapisu.

---

## *1.6. ONZ – UNCITRAL<sup>23</sup>*

---

Projekt ustawy modelowej stoi na stanowisku neutralności technologicznej, a zatem posługuje się pojęciem podpisu elektronicznego. Według ustawy podpis elektroniczny oznacza dane w formie elektronicznej, załączone do wiadomości elektronicznej albo logicznie z nią powiązane, które mogą być wykorzystywane do identyfikacji podpisującego związanego z wiadomością elektroniczną i wskazującą zatwierdzenie przez podpisującego informacji zawartej w tej wiadomości.

Ideę neutralności technologicznej zastosowaną w ustawie dodatkowo wzmacnia art. 3. Mówi on, że żaden z przepisów ustawy modelowej nie ma zastosowania do wyłączenia, ograniczenia lub pozbawienia skutku prawnego jakiegokolwiek metody tworzenia podpisów elektronicznych, która spełnia wymagania albo w inny sposób spełnia wymagania prawa właściwego. Przepis ten zawiera zasadę uznawania innych metod tworzenia podpisu, o ile spełniają warunki z art. 6 projektu ustawy.

Wyłączyć zastosowanie tego przepisu można jedynie na podstawie art. 5, który mówi, że jest to możliwe jedynie za porozumieniem stron, chyba że to porozumienie byłoby nieważne albo bezskuteczne.

Strony korzystające z podpisu elektronicznego działają na zasadzie swobody zawierania umów. Mają pełną swobodę w zakresie zwiększenia lub zmniejszenia wymagań dla podpisu elektronicznego pamiętając jednak, że nie może to w żaden sposób naruszyć przepisów prawa właściwego dla danego stosunku prawnego. Art. 5 z jednej strony daje możliwości zmiany poprzez porozumienie, a z drugiej to samo porozumienie ogranicza prawem krajowym.

---

<sup>23</sup> UNCITRAL (United Nations Commission on International Trade Law) Komisja Międzynarodowego Prawa Handlowego Organizacji Narodów Zjednoczonych – powołana 17 grudnia 1996r uchwałą Zgromadzenia Ogólnego ONZ – Rezolucja 2205(XXI), złożona z przedstawicieli poszczególnych porządków prawnych

Popierając zasadę neutralności technologicznej w akcie Unii Europejskiej używa się pojęcia podpis elektroniczny. Oznacza dane w formie elektronicznej, które dodane są do innych danych elektronicznych są z nimi logicznie powiązane i służą do autoryzacji. W Dyrektywie występuje też druga, wyższa kategoria podpisu elektronicznego tj. zaawansowany podpis elektroniczny. Zaawansowany podpis elektroniczny to podpis elektroniczny spełniający następujące wymagania:

- a) przyporządkowany jest wyłącznie podpisującemu,
- b) umożliwia identyfikację podpisującego,
- c) stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą i
- d) jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych może zostać wykryta.

### ***1.8.1 Aspekt 1. Definicja podpisu elektronicznego z uwagi na technologię jego tworzenia***

Definicje stworzone np. przez prawo Austrii, Polski, Unii Europejskiej i UNCITRAL hołdują jednej opcji – neutralności technologicznej tworzenia podpisów. Uregulowania te są otwarte na różne metody tworzenia podpisu. Definicje są skonstruowane w taki sposób, aby nie faworyzować, ani też nie dyskryminować żadnej z metod tworzenia podpisu. Uwidocznione jest przez to elastyczne podejście prawne do kwestii sformułowania definicji podpisu elektronicznego, które swym zasięgiem obejmuje różne technologie tworzenia podpisów, a tym samym będzie w stanie dopasować się do szybkich zmian technologicznych i ciągle zmieniających się warunków na arenie telekomunikacyjnej.

Rozwiązanie prawne stojące na stanowisku neutralności w stosunku do technologii tworzenia podpisu, zdaje się być na tyle elastyczne, że nie ulegnie tak szybko próbie czasu. Z drugiej jednak strony może powodować większe ryzyko zróżnicowania prawnego wynikającego z trudności interpretacyjnych. Oparcie regulacji prawnej o ściśle określoną technologię daje większą pewność obrotu

gospodarczego, ale jest też mniej elastyczne i ustawa o nią oparta szybciej będzie wymagać nowelizacji.

Niemcy hołdują zasadzie, że żeby nad wszystkim móc panować, żeby nie było żadnych nieścisłości nie tylko w zakresie interpretacji, to trzeba dokładnie określić technologię. Usankcjonowały pod względem prawnym tylko jeden rodzaj podpisu elektronicznego mianowicie podpis cyfrowy oparty o technologię wykorzystującą kryptografię z kluczem jawnym. Stanowisko UE w sprawie podpisu elektronicznego jest jasne, a Niemcy będące państwem członkowskim będą musiały dostosować swoją ustawę do wymogów zawartych w Dyrektywie.

W tym miejscu niezbędna jest uwaga, że ustawa niemiecka powstała w 1997r czyli wcześniej niż została uchwalona Dyrektywa UE. Wszystkie późniejsze regulacje są dostosowane do zasady neutralności technologicznej. Mogły opierać się na doświadczeniach państw, które już wprowadziły przepisy o podpisie elektronicznym i uniknąć błędów najczęściej popełnianych w regulacjach polegających na odwołaniu się do konkretnych rozwiązań technologicznych.

### ***1.8.2. Aspekt 2. Definicja – czym jest podpis elektroniczny***

Przyglądając się różnym systemom prawnym można powiedzieć, że podpis elektroniczny to dane elektroniczne dołączone do innych danych elektronicznych lub z nimi logicznie powiązane, służące do potwierdzenia tożsamości podpisującego. Regulacje, które posługują się pojęciem podpisu elektronicznego tak właśnie go definiują. W tym nie ma specjalnych różnic. Różnice można dostrzec w specjalnym podpisie elektronicznym.

### ***1.8.3 Aspekt 3. Konstrukcja definicji podpisu elektronicznego a praktyka***

Definicja podpisu elektronicznego zwłaszcza w regulacjach hołdujących neutralności technologicznej jest skonstruowana w taki sposób, że z jednej strony jest otwarta na różne technologie tworzenia podpisu – w tym zakresie idealnie spełnia swój cel, natomiast z drugiej strony daje duże możliwości interpretacyjne na to, co faktycznie może być podpisem elektronicznym. Kryteria, którym poddane będą dane są ujęte w sposób bardzo ogólny.

Z reguły zwykłemu podpisowi elektronicznemu (nazwanemu tak dla ułatwienia odróżnienia go od innych rodzajów) towarzyszy drugi rodzaj podpisu elektronicznego – zwany różnie przez różnych prawodawców: bezpieczny, zaawansowany. Kryteria dla tego podpisu są już bardziej wyszukane, zawierają więcej wymogów i tak bardzo odpowiada tym kryteriom podpis elektroniczny oparty na technologii kryptografii asymetrycznej – jedynej używanej współcześnie.

## ***R o z d z i a ł 2***

### ***Skutki podpisu elektronicznego***

---

#### ***2.1. Zagadnienia wstępne***

---

W poprzednim rozdziale zostało powiedziane, że podpis elektroniczny można dzielić z uwagi na skutki jakie wywołuje czyli zostaną wywołane takie skutki, jaki został zastosowany podpis elektroniczny. Relacje pomiędzy rodzajem podpisu elektronicznego, a skutkiem jego zastosowania są ściśle. Podział ten występuje w systemach prawnych, które popierają koncepcję neutralności technologicznej, bowiem te regulacje tak formułują definicję podpisu, aby nie dyskryminować, ani też nie faworyzować żadnej z technologii jego tworzenia. W związku z tym może pojawić się podpis wygenerowany przez technologię, która nie była dotąd znana, ale spełnia specjalne wymagania ustawowe. Taki zwrot w sytuacji został już omówiony w poprzednim rozdziale. A co w przypadku, gdy zostanie wygenerowany podpis stosujący technologię, która nie spełnia wymagań, bądź nie została zastosowana żadna z technologii tworzenia podpisu. Taki podpis to zwykły podpis elektroniczny, który wywołuje ogólne skutki prawne. Poniżej zostaną przedstawione rodzaje skutków prawnych, oraz warunki, jakie muszą zostać spełnione, aby doszło do wywołania poszczególnych rodzajów skutków prawnych.

#### ***2.2. Austria***

---

Skutki podpisu elektronicznego wiążą się z tym, jaki rodzaj podpisu użyjemy w celu ich wywołania. W ustawie austriackiej zostały zdefiniowane pojęcia: podpis elektroniczny i bezpieczny podpis elektroniczny. W związku z tym są także dwojakiego rodzaju skutki zastosowania w/w podpisów. Ustawa nazywa je: ogólne skutki prawne i szczegółowe skutki prawne.

##### ***2.2.1. Ogólne skutki prawne***

Ogólne skutki prawne to pierwszy z rodzajów skutków prawnych przewidzianych przez ustawę austriacką. Powstają przez zastosowanie zwykłego podpisu elektronicznego, czyli podpisu o najniższym stopniu zabezpieczenia –

będącego tylko  
w formie elektronicznej, nie opartego na kwalifikowanym certyfikacie i nie utworzonego wykorzystując specjalne technologie tworzenia.

Wynika z tego, że nazwisko i imię napisane pod tekstem elektronicznego dokumentu będzie spełniało wymogi zwykłego podpisu elektronicznego, bowiem

1. są to dane elektroniczne,
2. są dołączone do innych danych w dokumencie i
3. niewątpliwie służą do uwierzytelnienia czyli do potwierdzenia tożsamości składającego podpis.

Taki podpis będzie wywoływał ogólne skutki podpisu elektronicznego bo:

1. występuje tylko w formie elektronicznej,
2. nie jest oparty na kwalifikowanym certyfikacie wydanym przez akredytowanego usługodawcę certyfikacyjnego i,
3. nie został utworzony przy użyciu środków technicznych i procedur z art. 18.

### ***2.2.2. Szczegółowe skutki prawne***

Drugim rodzajem skutków prawnych są szczegółowe skutki prawne. Powstają przez zastosowanie drugiego z podpisów elektronicznych tj. bezpiecznego podpisu elektronicznego. Do szczegółowych skutków prawnych zalicza się:

1. spełnienie wymogów formy pisemnej dokumentów opatrzonech bezpiecznym podpisem elektronicznym („bezpieczny podpis elektroniczny spełnia wymogi prawne stawiane wobec podpisu ręcznego, a w szczególności wymogi dotyczące formy pisemnej, która została określona w § 886 Austriackiego Kodeksu Cywilnego, chyba, że prawo lub porozumienie stron reguluje to inaczej”) i
2. przyznania domniemania autentyczności dokumentu prywatnego z § 284 Austriackiego KPC.

Bezpieczny podpis elektroniczny, żeby wywoływał w/w skutki musi spełniać określone warunki. Dotyczą one zabezpieczenia technicznego i procedur tworzenia bezpiecznych podpisów elektronicznych. Pełen zakres wymagań przedstawiony został w § 18 ustawy austriackiej o podpisie elektronicznym. Zwraca się dużą uwagę w nim na niezawodność środków technicznych (które są stosowane przy generowaniu i przechowywaniu danych do tworzenia podpisu oraz przy tworzeniu bezpiecznych podpisów elektronicznych) w wykrywaniu sfałszowania danych

opatrzone podpisem elektronicznym. Ponadto muszą one zapobiegać nieupoważnionemu użyciu procedur i danych do tworzenia podpisu, muszą także uniemożliwić zmianę danych opatrzone podpisem, muszą zapewnić, by dane, które mają zostać podpisane, zostały uwidocznione sygnatariuszowi przed uruchomieniem procedury złożenia podpisu. Prawdopodobieństwo niepowtarzalności danych do tworzenia podpisu musi być bliskie pewności. Dane do tworzenia podpisu muszą być należycie zabezpieczone przed kryptoanalizą oraz musi być zagwarantowane utrzymanie ich w tajemnicy. Do tworzenia i przechowywania certyfikatów kwalifikowanych muszą być stosowane środki techniczne i procedury, które zapobiegają sfałszowaniu (podrobieniu lub przerobieniu) certyfikatów. Do weryfikacji danych opatrzone bezpiecznym podpisem muszą być stosowane środki techniczne i procedury, które zapewniają spełnienie następujących warunków:

- a) dane opatrzone podpisem nie mogą zostać zmienione,
- b) podpis będzie można niezawodnie zweryfikować, a wyniki weryfikacji prawidłowo uwidocznisz,
- c) osoba dokonująca weryfikacji będzie mogła określić, do których danych odnosi się podpis elektroniczny,
- d) osoba dokonująca weryfikacji będzie mogła określić, któremu sygnatariuszowi został przydzielony dany podpis elektroniczny oraz czy został użyty pseudonim sygnatariusza,
- e) będzie można rozpoznać zmiany w danych opatrzone podpisem, które pociągają za sobą implikacje dla zabezpieczeń.

Środki techniczne i procedury używane do tworzenia bezpiecznych podpisów elektronicznych muszą stale być w odpowiedni sposób weryfikowane, z wykorzystaniem aktualnych w danym czasie rozwiązań technicznych. Zgodność z wymaganiami

w zakresie zabezpieczeń musi być potwierdzona przez instytucję zatwierdzającą.

Pomimo spełnienia w/w warunków są sytuacje, kiedy odmawia się skutków prawnych formy pisemnej. Zostały one określone w § 886 Austriackiego KC. I są to:

1. czynności prawne przewidziane przez prawo rodzinne i spadkowe, dla których wymagana jest forma pisemna lub wobec których stawiane są ściślejsze wymagania formalne,

2. oświadczenia woli, czynności prawne, których ważność jest uwarunkowana potwierdzeniem oficjalnym, poświadczeniem sądowym lub notarialnym bądź zachowaniem aktu notarialnego,
3. oświadczenia woli, czynności prawne i wnioski, których wprowadzenie do księgi wieczystej, rejestru handlowego lub innego rejestru jest uwarunkowane potwierdzeniem oficjalnym, poświadczeniem sądowym lub notarialnym bądź zachowaniem formy aktu notarialnego,
4. deklaracje gwarancji, o których mowa w § 1346 ust.2 Austriackiego KC.

Odmawia się szczegółowych skutków prawnych również, gdy zostanie udowodnione, że wymagania co do tworzenia i zabezpieczania bezpiecznego podpisu elektronicznego nie zostały spełnione, bądź też, że nastąpiło naruszenie środków podjętych w celu spełnienia tych wymagań.

---

### *2.3. Niemcy*

Regulacja niemiecka jako jedna z nielicznych dała priorytet technologii tworzenia podpisu opartej o metodę kryptograficzną. Podpis wygenerowany tą metodą to podpis cyfrowy. Zastosowanie go wywołuje tylko jednego rodzaju skutki a mianowicie dokument elektroniczny spełni wymogi dokumentu pisemnego i zachowa ważność, o ile podpis cyfrowy spełni określone w ustawie wymogi. Wymogi te dotyczą bezpieczeństwa i pewności co do tworzenia podpisu. Zostaną szczegółowo omówione w następnej części pracy.

---

### *2.4. Polska*

Polskie ustawodawstwo należy do tego bloku państw i organizacji międzynarodowych, które rozróżniają dwa rodzaje podpisów elektronicznych. W związku z tym są dwójakiego rodzaju skutki prawne. Zastosowanie zwykłego podpisu elektronicznego wywoła podobne skutki co w ustawie austriackiej, dlatego pozwalam sobie pominąć tą kwestię i od razu przejść do skutków wynikających z zastosowania bezpiecznego podpisu elektronicznego.

### **2.4.1 Skutki z zastosowania bezpiecznego podpisu elektronicznego**

Bezpieczny podpis elektroniczny wywoła takie same skutki prawne jak podpis odręczny o ile:

1. został wygenerowany na podstawie kwalifikowanego certyfikatu w okresie jego ważności, przy pomocy bezpiecznych urządzeń i danych podlegających wyłącznej kontroli osoby składającej podpis (w przypadku zawieszenia certyfikatu wywołuje skutki prawne z chwilą uchylecia tego zawieszenia),
2. zapewnia bezpieczeństwo, pewność i integralność tych danych,
3. zawiera wskazanie kwalifikowanego certyfikatu.

---

## **2.5. ONZ – UNCITRAL**

Art. 7 ustawy modelowej UNCITRAL o handlu elektronicznym mówi o skutku podpisu elektronicznego jakim jest zrównanie podpisu elektronicznego z odręcznym w taki sposób, żeby wywoła on takie same skutki. Wymienione zostały dwie przesłanki od spełnienia, których uzależnione jest uznanie równorzędności podpisu elektronicznego z podpisem odręcznym. I są to:

- a) istnienie skutecznej metody identyfikacji inicjatora takiej informacji i autoryzacji przez inicjatora zawartych w niej danych, oraz
- b) metoda ta musi być niezawodna i w pełni służyć celowi, dla którego wiadomość elektroniczna została wytworzona i zakomunikowana, w świetle towarzyszących okoliczności, a w szczególności umowy między inicjatorem a adresatem<sup>24</sup>.

Projekt ustawy modelowej o podpisie elektronicznym natomiast w art. 6 zapewnia takie same skutki prawne zastosowania podpisu elektronicznego, co podpisanie dokumentu własnoręcznie. Zapewnienie to wynika z faktu, że będą stosowane tylko techniki tworzenia podpisu elektronicznego, które są wystarczająco godne zaufania w świetle nie tylko art. 6 ustawy, ale i umowy stron. Weryfikatorem tych technik będzie specjalny podmiot zaopatrzony w odpowiednie kompetencje. Technika tworząca podpis elektroniczny musi być tak niezawodna, jak to wynika z celu stworzenia wiadomości elektronicznej w świetle wszelkich towarzyszących okoliczności,

---

<sup>24</sup> tłumaczenie ustawy modelowej UNCITRAL o handlu elektronicznym - W. Kocot „Zawieranie umów sprzedaży według konwencji wiedeńskiej” Warszawa 1998r

a w szczególności porozumienia stron. Dla spełnienia tego wymagania wyliczone zostały następujące warunki:

- a) dane tworzące podpis są, w kontekście, w którym zostały użyte, wyłącznie związane z podpisującym,
- b) dane tworzące podpis były w czasie podpisywania pod wyłączną kontrolą podpisującego,
- c) jakakolwiek zmiana podpisu elektronicznego dokonana po podpisaniu jest wykrywalna i
- d) tam, gdzie celem prawnych wymagań dla podpisu elektronicznego jest zapewnienie zabezpieczenia odnośnie do integralności informacji, z którą jest związany, jakakolwiek zmiana dokonana w tej informacji po czasie podpisania jest wykrywalna.

---

## *2.6. Unia Europejska*

Dyrektywa podobnie jak ustawa austriacka choć nie wprost – wyróżnia dwa rodzaje skutków prawnych: skutki zastosowania zwykłego podpisu elektronicznego i zaawansowanego podpisu elektronicznego. Zastosowanie zwykłego podpisu elektronicznego wywoła takie same skutki co w regulacji austriackiej, dlatego pozwalam sobie pominąć tą kwestię i przejść do omówienia skutków powstających po zastosowaniu podpisu elektronicznego zaawansowanego.

### ***2.6.1 Skutki zastosowania zaawansowanego podpisu elektronicznego***

Skutkami dla zastosowania zaawansowanego podpisu elektronicznego są:

1. spełnienie wymogów prawnych co do podpisu w odniesieniu do danych w formie elektronicznej w ten sam sposób, co podpis odręczny w odniesieniu do danych znajdujących się na papierze,
2. dopuszczenie jako dowód w postępowaniu sądowym.

Podpis musi spełnić następujące warunki, żeby można było mówić o odniesieniu powyższych skutków:

1. musi opierać się na kwalifikowanej autoryzacji i
2. musi zostać stworzony przez bezpieczne urządzenie generujące podpisy.

Powyższe warunki są treścią dwóch załączników do Dyrektywy. Załącznik I stanowi o wymaganiach względem autoryzacji kwalifikowanej. Autoryzacja kwalifikowana musi zawierać następujące dane:

- a) informację, że dana autoryzacja została wystawiona jako autoryzacja kwalifikowana,
- b) dane dostawcy usług autoryzujących i państwa, w którym ma swoją siedzibę,
- c) nazwę podpisującego lub pseudonim, który jako taki można zweryfikować,
- d) miejsce atrybutu, który jest przyznawany w zależności od przeznaczenia autoryzacji,
- e) dane do sprawdzania podpisu, które odpowiadają danym do generowania podpisu kontrolowanym przez podpisującego,
- f) dane odnośnie początku i końca obowiązywania autoryzacji,
- g) kod identyfikacyjny autoryzacji,
- h) zaawansowany podpis elektroniczny wystawiającego dostawcy usług autoryzujących,
- i) jeżeli konieczne – ograniczenia zakresu obowiązywania autoryzacji oraz
- j) jeżeli konieczne – granice wartości transakcji, do której można stosować autoryzację.

Załącznik III do Dyrektywy zawiera wymagania dla urzędzeń tworzących podpisy. Minimum, które muszą zapewnić bezpieczne urządzenia tworzące podpisy poprzez odpowiednie techniki i procedury to:

- a) dane do tworzenia podpisu użyte do tworzenia podpisu praktycznie pojawiają się tylko raz oraz zapewniona jest ich poufność,
- b) dane do tworzenia podpisu użyte do tworzenia podpisu nie mogą, przy zachowaniu rozsądnego zabezpieczenia, być uzyskane oraz podpisy są chronione przed fałszowaniem przy użyciu dostępnej technologii,
- c) dane do tworzenia podpisu użyte do tworzenia podpisu chronione są przez prawnie podpisującego przed użyciem przez innych w sposób godny zaufania.

---

## *2.7 Podsumowanie*

Skutki zastosowania podpisu elektronicznego ściśle wiążą się z rodzajem podpisu. Dla jasnego i przejrzystego zobrazowania relacji podpisu elektronicznego ze skutkami jakie wywołuje pozwoliłam sobie stworzyć tabelę.



<b>PODPIS ELEKTRONICZNY</b>		
<i>podział z uwagi na technologię</i>		
<p style="text-align: center;"><b>PODPIS CYFROWY</b>            technologia kryptograficzna            np.            1. ustawa niemiecka – podpis cyfrowy</p>	<p style="text-align: center;"><b>PODPIS ELEKTRONICZNY</b>            neutralność technologiczna            np.            1. ustawa austriacka (A),            2. ustawa polska (P),            3. projekt ustawy modelowej UNCITRAL (U),            4. Dyrektywa Unii Europejskiej (UE)</p>	
<p>1. został oparty o jedną stosowaną technologię – technologię kryptograficzną,            2. wywołuje jednego rodzaju skutki, są to skutki takie same jak wywołane przez szczególny podpis elektroniczny, bowiem podpis cyfrowy spełnia wymagania dla szczególnego podpisu elektronicznego.            3. nie może być mowy o użyciu innej technologii niż kryptograficzna, bowiem tylko ona została usankcjonowana w przepisach prawnych, taka sytuacja ma miejsce np. w Niemczech,            4. nie może być mowy o innych skutkach zastosowania podpisu cyfrowego nad szczególnymi skutkami podpisu elektronicznego, bowiem podpis cyfrowy jest podpisem elektronicznym szczególnym, spełnia wymogi podpisu elektronicznego szczególnego,            5. państwa, które postulują neutralność technologiczną dopuszczają też zastosowanie innych metod, technologii do tworzenia podpisu, o ile spełni wymogi szczególnego podpisu elektronicznego.</p>	<i>podział z uwagi na skutki</i>	
	<p style="text-align: center;"><b>ZWYKŁY</b>            np.            1. A            2. P            3. U            4. UE</p> <p style="text-align: center;">- <b>podpis elektroniczny</b></p>	<p style="text-align: center;"><b>SZCZEGÓLNY</b>            np.            1. w ustawie austriackiej – <b><u>bezpieczny podpis elektroniczny</u></b>            2. w ustawie polskiej również <b><u>bezpieczny podpis elektroniczny</u></b>,            3. w projekcie ustawy modelowej o podpisie elektronicznym UNCITRAL – <b><u>brak szczególnej formy podpisu elektronicznego</u></b>            4. w Dyrektywie Unii Europejskiej – <b><u>zaawansowany podpis elektroniczny</u></b></p>
	<p>1. rodzaj podpisu o najniższym stopniu zabezpieczenia            2. w związku z tym nie wywołuje szczególnych skutków prawnych, bowiem nie spełnia wymogów ustawowych, a tylko ogólne skutki prawne</p>	<p>1. spełniający wymagania ustawowe dla stopnia bezpieczeństwa podpisu,            2. wywołuje szczególne skutki prawne            3. podpis cyfrowy spełnia te warunki, dlatego on również wywołuje szczególne skutki prawne.</p>

**Tabela: Rodzaje podpisu elektronicznego (szary – podział ze względu na technologię, biały – ze względu na skutki)**

Są różne rodzaje podpisów elektronicznych i w związku z tym wywołują różne skutki prawne. Podpis cyfrowy nie dzieli się na rodzaje i nie wywołuje różnych skutków. Jest jeden podpis cyfrowy i wywołuje tylko jednego rodzaju skutki a mianowicie szczególne skutki prawne. Tylko w regulacjach popierających stanowisko neutralności technologicznej tworzenia podpisu może być mowa o rodzajach podpisu i o różnych rodzajach skutków jego zastosowania. Kryterium wyróżnienia poszczególnych rodzajów podpisów elektronicznych jest bezpieczeństwo ich tworzenia, poufność i integralność danych. W zależności od zastosowania określonego rodzaju podpisu elektronicznego wywoływane są różne skutki prawne. Można też powiedzieć, że w zależności od tego, jakie chcemy wywołać skutki prawne, stosujemy takie podpisy elektroniczne. Zanim podpiszemy, trzeba się najpierw zastanowić, o jakie skutki nam chodzi i jak ważne są dane, które opatrzymy elektronicznym podpisem. Ogólnie rzecz ujmując w dużej większości systemów prawnych są dwa rodzaje podpisów elektronicznych zwykły i szczególny. Im wyższa klasa podpisu, tym więcej wymogów do spełnienia. Zazwyczaj warunki te dotyczą technologii tworzenia podpisu, bezpieczeństwa, pewności i integralności danych opatrzonych tym podpisem. Podpis elektroniczny szczególny będzie wykorzystywany do podpisania danych, na bezpieczeństwie, pewności i integralności których nam szczególnie zależy. Dlatego zrozumiałe jest, że wymagania co do technologii tworzenia są szczególne. Tylko wtedy, gdy podpis elektroniczny spełni wymogi dla podpisu szczególnego można mówić o szczególnych skutkach prawnych jak zrównanie podpisu elektronicznego w skutkach w podpisem odręcznym i możliwość wykorzystania tak podpisanego dokumentu jako dowodu w postępowaniu sądowym. W przeciwnym wypadku wywołuje tylko ogólne skutki prawne, które w żaden sposób nie korzystają z ochrony przewidzianej dla podpisu szczególnego. Poniżej tabela przedstawiająca skutki podpisu elektronicznego w relacji do jego rodzaju.

<b>PODPIS ELEKTRONICZNY</b>			
	<b>podpis elektroniczny zwykły</b>	<b>podpis elektroniczny szczególny</b>	<b>podpis cyfrowy</b>
	technologicznie neutralny		technologia kryptograficzna
<b>BEZPIECZEŃSTWO PODPISU ELEKTRONICZNEGO</b> warunki dla podpisu elektronicznego			
<b>NIEZAPRZECZALNOŚĆ</b> pewność co do tego, że nadawcą jest ten, kto się za niego podaje, nikt jeśli wyśle podpisaną przez siebie wiadomość nie może wyprzeć się swego autorstwa	nie zapewnia	zapewnia	zapewnia
<b>POUFNOŚĆ</b> – pewność, że podmiot nieuprawniony nie miał wglądu w treść informacji	nie zapewnia	zapewnia	zapewnia
<b>INTEGRALNOŚĆ DANYCH</b> – pewność, że dane nie zostały zmodyfikowane lub zniszczone przez nieuprawniony podmiot	nie zapewnia	zapewnia	zapewnia
<b>SKUTKI ZASTOSOWANIA PODPISU ELEKTRONICZNEGO</b>			
spełnienie wymogów formy pisemnej dokumentów opatrzonych tym podpisem	nie wywołuje	wywołuje	wywołuje
dowód w sprawie w postępowaniu przed sądem	nie wywołuje	wywołuje	wywołuje
ogólne skutki podpisu elektronicznego	wywołuje	-----	-----

**Tabela: Porównanie podpisów elektronicznych**

## *R o z d z i a ł 3*

### *Podpisujący i weryfikujący podpis*

---

#### *3.1. Zagadnienia wstępne*

---

Z poprzednich rozdziałów dowiedzieliśmy się jakie są definicje podpisu elektronicznego, jaki wpływ na definicję ma technologia jego tworzenia, jakie skutki prawne wywołuje zastosowanie podpisu elektronicznego oraz jakie podpis powinien spełniać wymagania, aby wywołać określone skutki prawne. W tym rozdziale o tym, kto może podpisywać i na jakich zasadach. Obok podmiotu podpisującego występuje podmiot, który weryfikuje ten podpis. Poniżej o tych dwóch kategoriach podmiotów.

#### *3.2. Austria*

---

Podpisującymi, czyli sygnatariuszami zgodnie z ustawą austriacką są:

1. osoby fizyczne, którym zostały przydzielone dane do tworzenia podpisu i odpowia dające im dane do weryfikacji podpisu i
2. usługodawcy certyfikacyjni, którzy używają certyfikatów do świadczenia usług certyfikacyjnych.

Osoby fizyczne mogą tworzyć podpis we własnym imieniu, a także w imieniu osoby trzeciej. Ponadto są zobowiązane dbać o dane do tworzenia podpisu, aby nie dostały się w niepowołane ręce. Jest to bardzo ważne z uwagi na interes nie tylko podpisującego, ale wszystkich, którzy z nim kontraktują, prowadzą korespondencję elektroniczną. Dostęp do danych do tworzenia podpisu musi być ograniczony najlepiej do jednej osoby – podpisującego i ewentualnie osoby upoważnionej. Sygnatariusz może zażądać unieważnienia certyfikatu w przypadku zagubienia danych do tworzenia podpisu, uzasadnionego podejrzenia ich naruszenia lub zmiany faktów potwierdzonych certyfikatem. Z uwagi na wielość podmiotów mogących podpisywać każdy odpowiada w zakresie, w jakim nie sprostał wymaganiom.

Choć ustawa nie mówi o tym wprost, to w treści poszczególnych paragrafów można wywnioskować, że weryfikującymi podpis są te same podmioty, które

podpisują, tylko że teraz występują w roli weryfikującego podpis. Ich atrybutem jest posiadanie danych do weryfikacji podpisu elektronicznego.

---

### 3.3. Niemcy

Według prawa niemieckiego podpisującym jest osoba, która zgodnie z obowiązującą polityką certyfikacyjną uzyskała certyfikat dla swojego klucza publicznego. Podpisywać może również osoba przez nią upoważniona. Weryfikującym podpis jest osoba, która za pomocą odpowiedniej kombinacji zastosowań kluczy asymetrycznych jest w stanie odczytać zaszyfrowaną wiadomość, stwierdzić, że pochodzi od określonego nadawcy i że po drodze nie została w żaden sposób naruszona.

---

### 3.4. Polska

#### 3.4.1. Podpisujący

Podpisujący wg polskiej ustawy to:

1. osoba fizyczna,
2. osoba prawna lub
3. jednostka organizacyjna nie posiadająca osobowości prawnej.

Warunkiem jest posiadanie odpowiedniego sprzętu i skonfigurowanego oprogramowania do składania podpisów elektronicznych lub poświadczania elektronicznego przy wykorzystaniu danych do składania podpisu elektronicznego.

Osoba fizyczna może tworzyć podpis we własnym imieniu lub w imieniu innej osoby fizycznej, prawnej albo w imieniu jednostki organizacyjnej nie posiadającej osobowości prawnej. Dysponuje ona danymi do składania podpisu elektronicznego. Są to niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane do składania podpisu elektronicznego. Sprzęt i oprogramowanie do składania bezpiecznych podpisów elektronicznych ponadto musi spełniać wymogi określone w ustawie.

#### 3.4.2. Weryfikujący podpis

Osoba weryfikująca podpis elektroniczny to osoba podejmująca czynności, które pozwolą na identyfikację osoby składającej podpis elektroniczny, na

stwierdzenie, że podpis został złożony za pomocą danych służących do składania podpisu elektronicznego przyporządkowanych do tej osoby, a także, że dane opatrzone tym podpisem nie uległy zmianie po złożeniu podpisu elektronicznego. Osoba weryfikująca wykorzystuje w tym celu dane służące weryfikacji podpisu elektronicznego

i urządzenie do weryfikacji podpisu elektronicznego – sprzęt i oprogramowanie, które umożliwia identyfikację osoby fizycznej, która złożyła podpis, lub podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenie służące do weryfikacji poświadczenia elektronicznego.

---

### 3.5. ONZ – UNCITRAL

#### **3.5.1. Podpisujący**

Podpisującym jest osoba, która włada danymi tworzącymi podpis i działa w swoim imieniu lub imieniu osoby, którą reprezentuje. Została ona zobowiązana do dołożenia należytej staranności, aby uniknąć nieautoryzowanego wykorzystania danych tworzących podpis. W przypadku, gdy dane tworzące podpis zostały ujawnione lub okoliczności znane podpisującemu wskazują na rzeczywiste ryzyko, że dane tworzące podpis zostały przechwycone jest zobowiązana do natychmiastowego powiadomienia osoby, która może opierać się na podpisie elektronicznym oraz osoby dostarczającej usługi związane z podpisem elektronicznym. Ponadto musi dołożyć należytej staranności w celu zapewnienia dokładności i kompletności wszelkich istotnych danych dostarczonych przez podpisującego, które zawarte są w certyfikacie lub są dla niego istotne przez czas jego trwania. Podpisujący jest odpowiedzialny za uchybienia, którym nie sprostał.

#### **3.5.2. Weryfikujący podpis**

Stroną polegającą jest osoba, która może działać na podstawie certyfikatu lub podpisu elektronicznego. Ponosi ona konsekwencje prawne swoich uchybień jeżeli zobowiązana do podjęcia należytych działań w celu weryfikacji pewności podpisu elektronicznego działań tych nie wykonała zgodnie z zaleceniem. W przypadku, gdy podpisowi elektronicznemu towarzyszy certyfikat jest ona

zobowiązana ponadto do weryfikacji ważności, zawieszenia lub odebrania certyfikatu i przestrzegania ograniczeń wynikających z certyfikatu.

### **3.6.1. Podpisujący**

Podpisującym jest osoba posiadająca urządzenie do generowania podpisów, która działa w imieniu własnym lub w imieniu osób prawnych lub fizycznych, lub stron, których jest przedstawicielem. Dane do generowania podpisów to jednorazowe dane jak kod lub klucz prywatny kryptograficzny, które są używane przez podpisującego do tworzenia podpisu elektronicznego. Istnienie dwóch rodzajów urządzeń do generowania podpisów elektronicznych to konsekwencja zamieszczenia w Dyrektywie dwóch rodzajów podpisów elektronicznych. I tak do generowania zwykłego podpisu elektronicznego wykorzystywane jest zwykle urządzenie generujące podpisy. Pod tym pojęciem rozumie się skonfigurowane oprogramowanie lub sprzęt do zaimplementowania danych do generowania podpisu elektronicznego. Do generowania zaawansowanego podpisu elektronicznego stosuje się bezpieczne urządzenie generujące podpisy. To urządzenie musi spełniać wymagania z Załącznika III Dyrektywy. Załącznik ten został omówiony w poprzednim rozdziale.

### **3.6.2. Weryfikujący podpis**

Do weryfikowania podpisu elektronicznego wykorzystuje się urządzenie sprawdzające podpisy, czyli skonfigurowane oprogramowanie lub sprzęt używany do zaimplementowania danych do sprawdzania podpisu. Załącznik IV Dyrektywy zawiera wytyczne odnośnie bezpiecznego sprawdzania podpisu. Zgodnie z tym załącznikiem w ramach racjonalnego bezpieczeństwa należy zapewnić, aby dane użyte do kontroli podpisu odpowiadały danym, które pokazuje kontrolujący. Podpis musi być sprawdzany w sposób godny zaufania, a wynik tej kontroli był właściwie pokazywany. Kontrolujący może w razie potrzeby, w sposób godny zaufania stwierdzić treść podpisanych danych. Prawdziwość i ważność autoryzacji są sprawdzane w sposób godny zaufania. Wynik sprawdzenia i tożsamość podpisującego są pokazywane we właściwy sposób. Użycie pseudonimu musi zostać podane w sposób jednoznaczny. Ważne zmiany związane z bezpieczeństwem muszą zostać rozpoznane.

### *3.7. Podsumowanie*

---

Podpisujący i weryfikujący podpis to w ogólnym uproszczeniu strony, które są zainteresowane przesyłaniem sobie elektronicznej korespondencji. Podpisującym i weryfikującym podpis w praktyce są to te same podmioty, które występują w różnych rolach. Gdy wysyłają korespondencję są podpisującymi, gdy otrzymują – weryfikującymi. Ważne jest, żeby móc skutecznie podpisywać to podpisujący musi spełnić określone wymagania. Rzeczą idzie również o to, że to od podpisującego zależy jakiego podpisu użyje do podpisania wiadomości.

PODPISUJĄCY I WERYFIKUJĄCY								
	Austria		Polska		Niemcy	UNICITRAL	UE	
	zwykły podpis elektroniczny	bezpieczny podpis elektroniczny	zwykły podpis elektroniczny	bezpieczny podpis elektroniczny	podpis cyfrowy	podpis elektroniczny	zwykły podpis elektroniczny	zaawansowany podpis elektroniczny
podmioty	<ul style="list-style-type: none"> <li>- osoby fizyczne,</li> <li>- usługodawcy certyfikacyjni</li> </ul>		<ul style="list-style-type: none"> <li>- osoby fizyczne</li> <li>- osoby prawne,</li> <li>- jednostki organizacyjne nie posiadające osobowości prawnej</li> </ul>		<ul style="list-style-type: none"> <li>- osoby fizyczne,</li> <li>- osoby prawne</li> </ul>	<ul style="list-style-type: none"> <li>- osoby posiadające dane do tworzenia i weryfikacji podpisu elektronicznego</li> </ul>	<ul style="list-style-type: none"> <li>- osoby posiadające urządzenie do tworzenia i weryfikacji podpisów elektronicznych</li> </ul>	
warunki, do spełnienia <sup>25</sup>	<ul style="list-style-type: none"> <li>- wynikające z przepisów k.c.</li> </ul>	<ul style="list-style-type: none"> <li>- ponad te wynikające z przepisów k.c. musi posiadać dane do tworzenia podpisu i odpowiadające im dane do weryfikacji podpisu,</li> <li>- wynikające z obowiązku zachowania tajemnicy danych,</li> <li>- uzyskanie odpowiedniego certyfikatu</li> </ul>	<ul style="list-style-type: none"> <li>- wynikające z przepisów w k.c.</li> </ul>	<ul style="list-style-type: none"> <li>- posiadanie odpowiedniego sprzętu, oprogramowania, danych do składania podpisu i weryfikacji,</li> <li>- uzyskanie odpowiedniego o certyfikatu</li> </ul>	<ul style="list-style-type: none"> <li>- posiada odpowiedni sprzęt, oprogramowanie specjalnie do generowania podpisu cyfrowego,</li> <li>- uzyskanie odpowiedniego o certyfikatu</li> </ul>		<ul style="list-style-type: none"> <li>- posiada urządzenie do generowania zwykłego podpisu elektronicznego,</li> </ul>	<ul style="list-style-type: none"> <li>- posiada urządzenie do generowania zaawansowanego podpisu elektronicznego,</li> <li>- uzyskanie odpowiedniej autoryzacji</li> </ul>

**Tabela: Podpisujący i weryfikujący podpis w zestawieniu porównawczym**

<sup>25</sup> warunki dotyczące uzyskania certyfikatów zostały tutaj wymienione w ogólności niejako uprzedzając fakty, szczegółowe omówienie kwestii zagadnień administracyjno - prawnych w następnej części pracy

## ***Cz ę ś ć II***

---

*Administracyjno – prawne zagadnienia podpisu  
elektronicznego*

# *Rozdział 1*

---

## *Usługodawcy certyfikacyjni*

---

### *1.1. Zagadnienia wstępne*

---

Tam gdzie chodzi o weryfikację tożsamości podmiotów biorących udział w elektronicznej wymianie dokumentów niezbędna trzecia strona, która w sposób bezstronny będzie wykonywać te czynności. Ta tematyka została celowo pominięta w poprzedniej części w rozdziale przedstawiającym strony wymiany elektronicznie podpisanych dokumentów i przeniesiony do części administracyjno – prawnych zagadnień podpisu elektronicznego, bowiem podpis elektroniczny to instytucja wymagająca szczególnego aparatu wykonawczego, w którym dużą rolę pełnią usługodawcy certyfikacyjni. Aparat administracyjny składa się z następujących podmiotów:

1. najniższy szczebel to podmioty uprawiające działalność certyfikacyjną,
2. na wyższym szczeblu stoją podmioty zatwierdzające działalność podmiotów uprawiających działalność certyfikacyjną,
3. na najwyższym szczeblu podmioty pełniące nadzór nad podmiotami, które świadczą usługi certyfikacyjne.

Działalność certyfikacyjna to cały szereg usług, które wymagają spełnienia określonych warunków. W tym rozdziale przybliżona zostanie osoba usługodawcy certyfikacyjnego, czyli podmiotu znajdującego w hierarchii najniższą pozycję. Zostanie wyjaśnione kim jest i czym się zajmuje, na czym polega jego działalność, jakim musi sprostać obowiązkom oraz jaką ponosi odpowiedzialność. Wydawanie certyfikatów niewątpliwie wchodzi w zakres działalności certyfikacyjnej. Jednak z uwagi na dużą rozpiętość tej tematyki pozwoliłam sobie wyłączyć tą kwestę z tego rozdziału i poświęcić tylko temu zagadnieniu odrębny, następny rozdział.

### **1.2.1. Pojęcie usługodawcy certyfikacyjnego**

Usługodawcą certyfikacyjnym wg ustawy austriackiej jest osoba fizyczna lub prawna, względnie inny podmiot zdolny do czynności prawnych, który wydaje certyfikaty lub świadczy inne usługi związane z podpisami i certyfikatami. Te inne usługi związane z podpisami i certyfikatami to:

- a) dostarczanie produktów sygnaturowych,
- b) udostępnianie procedury składania podpisów elektronicznych,
- c) wydawanie i odnawianie certyfikatów oraz administrowanie certyfikatami,
- d) świadczenie usług katalogowania, unieważniania, rejestracji, opatrywania datownikiem, komputerowego przetwarzania oraz
- e) udzielanie porad w związku z podpisami elektronicznymi.

### **1.2.2. Rozpoczęcie działalności certyfikacyjnej**

Prowadzenie usług certyfikacyjnych nie wymaga żadnego specjalnego zezwolenia. Każdy, kto zechce prowadzić taką działalność jest zobowiązany niezwłocznie zawiadomić organ nadzorczy o rozpoczęciu działalności. Przez rozpoczęciem działalności usługodawca jest zobowiązany złożyć reguły zabezpieczenia i certyfikacji dla każdej świadczonej przez siebie usługi związanej z podpisami elektronicznymi. Muszą one opisywać, w jaki sposób zapewni on zgodność

z wymaganiami stawianymi przez ustawę federalną i przez rozporządzenie wydane na jej podstawie. Raz zgłoszone reguły zobowiązany jest przestrzegać przez cały czas prowadzenia działalności certyfikacyjnej. Każdą zmianę świadczonych przez siebie usług musi zgłosić do organu nadzorczego. Musi poinformować organ nadzorczy również o każdej okoliczności, która uniemożliwia prowadzenie działalności

w sposób niezakłócony i zgodny z regułami zabezpieczenia i certyfikacji. Reguły te muszą określać czy świadczone są także usługi w zakresie katalogowania i unieważniania oraz w jakiej formie są prowadzone. Certyfikat usługodawcy certyfikacyjnego może być używany tylko w zakresie prowadzenia usług certyfikacyjnych.

### ***1.2.3. Datownik***

Jedną z czynności certyfikacyjnych jest znakowanie datownikiem. Datownik to potwierdzenie wydane przez usługodawcę certyfikacyjnego i opatrzone przez niego podpisem elektronicznym. Potwierdzenie to poświadcza fakt przedłożenia określonych danych elektronicznych w określonym czasie. Potwierdzenie to jest sygnowane podpisem elektronicznym usługodawcy certyfikacyjnego. Fakt prowadzenia tych usług usługodawca musi udokumentować w deklaracji reguł zabezpieczenia i certyfikacji. Przy prowadzeniu tej usługi usługodawca jest zobowiązany stosować środki, zabezpieczenia i procedury określone przez ustawę.

### ***1.2.4. Rejestry***

Prowadzenie rejestrów to następna usługa z czynności certyfikacyjnych. Usługodawca certyfikacyjny jest zobowiązany prowadzić rejestry i muszą być one prowadzone w taki sposób, żeby była zapewniona możliwość weryfikacji danych zawartych w rejestrach, ich autentyczności oraz daty wprowadzenia do rejestru. W rejestrze odnotowuje się:

- a) środki zabezpieczenia podjęte w celu zapewnienia zgodności z wymaganiami stawianymi przez ustawę i rozporządzenie,
- b) fakty wydania, zablokowania i unieważnienia certyfikatów.

Na żądanie sądu lub innych kompetentnych władz jest zobowiązany udostępnić rejestry.

### ***1.2.5. Zawieszenie działalności***

Działalność certyfikacyjna może zostać z różnych przyczyn zawieszona. W tym przypadku prowadzący tą działalność jest obowiązany do unieważnienia wszystkich wydanych i ważnych certyfikatów albo zapewnić przejęcie administrowania nimi przez innego usługodawcę certyfikacyjnego. O tym fakcie informuje organ nadrzędny i sygnatariusza. Usługodawca jest zobowiązany zapewnić kontynuowanie usług unieważnienia nawet po unieważnieniu jego certyfikatu. W przypadku nie dostosowania się do tego wymogu organ nadzorczy zarządzi kontynuowanie usług unieważnienia na koszt tego usługodawcy.

Usługodawca certyfikacyjny to osoba fizyczna bądź prawna, która potwierdza przyporządkowanie osobie fizycznej klucza publicznego, posiadający przy tym zatwierdzenie odpowiedniego organu.

Usługodawca certyfikacyjny zobowiązany jest do niezwłocznego zawiadomienia o podjęciu działalności certyfikacyjnej. Musi zadbać o to, żeby podjęte czynności w sprawie wydawania ważnych certyfikatów nie przejmowali inni usługodawcy certyfikacyjni. Prowadzi dokumentację w sprawie środków bezpieczeństwa przestrzegania ustawy i wydanego na jej podstawie rozporządzenia, jak również wystawionych certyfikatów, po to, aby dane i ich autentyczność można było sprawdzić w każdym czasie.

#### **1.4.1. Pojęcie podmiotu świadczącego usługi certyfikacyjne**

Ustawa polska posługuje się pojęciem podmiotu świadczącego usługi certyfikacyjne, co jest odpowiednikiem austriackiego usługodawcy certyfikacyjnego. Wyróżnia trzy rodzaje podmiotów świadczących usługi certyfikacyjne a mianowicie:

- a) zwykły podmiot świadczący usługi certyfikacyjne,
- b) kwalifikowany podmiot świadczący usługi certyfikacyjne oraz
- c) akredytowany podmiot świadczący usługi certyfikacyjne.

Zwykły podmiot świadczący usługi certyfikacyjne to przedsiębiorca w rozumieniu przepisów ustawy z dnia 19 listopada 1999r Prawo o działalności gospodarczej, Narodowy Bank Polski albo organ władzy publicznej, świadczący co najmniej jedną z usług certyfikacyjnych (tj. wydawanie certyfikatów, bądź znakowanie czasem, bądź inne usługi związane z podpisem elektronicznym). Kwalifikowanym podmiotem świadczącym usługi certyfikacyjne jest podmiot świadczący usługi certyfikacyjne wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, natomiast pod pojęciem akredytowanego podmiotu świadczącego usługi certyfikacyjne należy rozumieć kwalifikowany podmiot świadczący usługi certyfikacyjne posiadający akredytację, czyli decyzję administracyjną potwierdzającą, że podmiot świadczący usługi certyfikacyjne spełnia wymogi określone w ustawie.

### ***1.4.2. Wymogi dla usługodawców certyfikacyjnych***

Podjęcie działalności w zakresie świadczenia usług certyfikacyjnych nie wymaga zezwolenia ani koncesji. Organy władzy publicznej i NBP mogą świadczyć usługi certyfikacyjne na użytek własny lub innych organów władzy publicznej a jednostka samorządu terytorialnego także na potrzeby mieszkańców ją zamieszkujących i tylko w celach niezarobkowych. Szczególne warunki dotyczą wyższych kategorii podmiotów świadczących usługi certyfikacyjne a mianowicie kwalifikowanego

i akredytowanego podmiotu świadczącego usługi certyfikacyjne. Jeśli chodzi o kwalifikowany podmiot świadczący usługi certyfikacyjne przede wszystkim jest on zobowiązany uzyskać wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne i uzyskania zaświadczenia certyfikacyjnego. Natomiast akredytowany ponadto musi posiadać akredytację udzieloną przez ministra właściwego do spraw gospodarki. Akredytacji i wpisu dokonuje się na wniosek podmiotu, który zamierza świadczyć lub świadczy usługi certyfikacyjne. Wniosek taki od strony formalnej musi zawierać następujące dane:

- a) imię i nazwisko lub nazwę (firmę) wnioskodawcy,
- b) określenie polityki certyfikacyjnej, zgodnie z którą mają być tworzone i stosowane kwalifikowane certyfikaty lub świadczone inne usługi związane z podpisem elektronicznym,
- c) miejsce zamieszkania lub siedzibę firmy oraz adres wnioskodawcy,
- d) aktualny wypis z rejestru przedsiębiorców i rejestru dłużników niewypłacalnych,
- e) imiona i nazwiska osób wykonujących czynności certyfikacyjne, które podmiot ten zatrudnia lub zamierza zatrudnić,
- f) informacje o kwalifikacjach i doświadczeniu zawodowym oraz zaświadczenia o niekaralności osób wykonujących czynności związane ze świadczeniem usług certyfikacyjnych,
- g) wskazanie technicznych i organizacyjnych możliwości wykonywania czynności w zakresie świadczenia usług certyfikacyjnych,
- h) określenie sposobu zapobiegania ujawnianiu informacji, których wykorzystanie mogłoby naruszać interes odbiorców usług certyfikacyjnych,

- i) dokumenty przedstawiające sytuację majątkową oraz plan organizacyjny i finansowy działalności wnioskodawcy,
- j) dowód uiszczenia opłaty za rozpatrzenie wniosku o udzielenie akredytacji lub o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
- k) dane służące do weryfikacji poświadczeń elektronicznych składanych przez podmiot w ramach świadczonych przez niego usług certyfikacyjnych,
- l) numer identyfikacji podatkowej wnioskodawcy,
- m) numer identyfikacyjny REGON wnioskodawcy.

W przypadku braków formalnych wnioskodawca w terminie 7 dni może uzupełnić wniosek. Termin ten może zostać przedłużony na umotywowaną prośbę wnioskodawcy złożoną przed upływem tego terminu. Od dnia złożenia wniosku o wpis minister właściwy do spraw gospodarki w terminie miesiąca podejmuje decyzje o wpisie lub odmowy wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Jeśli chodzi o podjęcie decyzji w sprawie udzielenia akredytacji, minister właściwy do spraw gospodarki podejmuje taką decyzję w terminie dwóch miesięcy od dnia złożenia wniosku o udzielenie akredytacji. Uzyskanie akredytacji przez podmiot świadczący usługi certyfikacyjne stanowi potwierdzenie, że jest on instytucją posiadającą wystarczający potencjał merytoryczny i techniczny dla wystawcy kwalifikowanych certyfikatów i spełnia on określone w ustawie wymagania. Minister odmówi udzielenia akredytacji jeżeli:

- a) wniosek i dołączone do niego dokumenty nie spełniają warunków określonych w ustawie,
- b) w dokumentach organizacyjnych podmiotu są zamieszczone postanowienia mogące zagrażać bezpieczeństwu albo w inny sposób naruszać interes odbiorców usług certyfikacyjnych,
- c) przedstawiony przez podmiot plan organizacyjny i finansowy działalności lub jego sytuacja majątkowa nie zabezpieczają w należyty sposób interesów odbiorców usług certyfikacyjnych,
- d) podmiot został umieszczony w rejestrze dłużników niewypłacalnych,
- e) wskazane we wniosku techniczne i organizacyjne możliwości wykonywania czynności w zakresie świadczenia usług certyfikacyjnych nie zabezpieczają należycie interesów odbiorców usług certyfikacyjnych,

- f) osoby wykonujące czynności związane z wykonywaniem usług certyfikacyjnych nie dają rękojmi należytego wykonywania powierzonych czynności w zakresie świadczenia usług certyfikacyjnych.

Odmowa wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne nastąpi w sytuacji gdy wniosek i dołączone do niego dokumenty nie spełniają warunków określonych w ustawie lub gdy podmiot został umieszczony w rejestrze dłużników niewypłacalnych. W przypadku udzielenia akredytacji minister niezwłocznie wpisuje podmiot świadczący usługi certyfikacyjne do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Wpis akredytowanego podmiotu świadczącego usługi certyfikacyjne obejmuje:

- a) imię i nazwisko lub nazwę (firmę) akredytowanego podmiotu świadczącego usługi certyfikacyjne,
- b) sposób reprezentacji akredytowanego podmiotu świadczącego usługi certyfikacyjne oraz numer wpisu do rejestru przedsiębiorców i oznaczenie sądu prowadzącego ten rejestr,
- c) imiona i nazwiska osób reprezentujących akredytowany podmiot świadczący usługi certyfikacyjne,
- d) nazwę polityki certyfikacji, w ramach której dany podmiot może wydawać kwalifikowane certyfikaty lub świadczyć inne usługi związane z podpisem elektronicznym,
- e) numer i datę wydania decyzji o udzieleniu akredytacji lub o cofnięciu akredytacji,
- f) informacje o sumie ubezpieczenia i warunkach umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, oraz nazwę zakładu ubezpieczeń.

Wpis natomiast kwalifikowanego podmiotu świadczącego usługi certyfikacyjne do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne obejmuje:

- a) imię i nazwisko lub nazwę (firmę) kwalifikowanego podmiotu świadczącego usługi certyfikacyjne,
- b) sposób reprezentacji kwalifikowanego podmiotu świadczącego usługi certyfikacyjne oraz numer wpisu do rejestru przedsiębiorców i oznaczenie sądu prowadzącego ten rejestr,
- c) imiona i nazwiska osób reprezentujących kwalifikowany podmiot świadczący usługi certyfikacyjne,

- d) nazwę polityki certyfikacji, w ramach której dany podmiot może wydawać kwalifikowane certyfikaty lub świadczyć inne usługi związane z podpisem elektronicznym,
- e) informacje o sumie ubezpieczenia i warunkach umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, oraz nazwę zakładu ubezpieczeń,
- f) datę dokonania wpisu lub wydania decyzji o wykreśleniu wpisu.

Ponadto na kwalifikowany podmiot świadczący usługi certyfikacyjne zostały nałożone następujące wymogi:

1. jeśli wydaje kwalifikowane certyfikaty obowiązany jest:

- a) zapewnić techniczne i organizacyjne możliwości szybkiego i niezawodnego wydawania, zawieszania i unieważniania certyfikatów oraz określenia czasu dokonania tych czynności,
- b) stwierdzić tożsamość osoby ubiegającej się o certyfikat,
- c) zapewnić środki przeciwdziałające fałszerstwom certyfikatów i innych danych poświadczanych elektronicznie przez te podmioty, w szczególności przez ochronę urządzeń i danych wykorzystywanych przy świadczeniu usług certyfikacyjnych,
- d) zawrzeć umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych,
- e) poinformować osobę ubiegającą się o certyfikat, przed zawarciem z nią umowy, o warunkach uzyskania i używania certyfikatu, w tym o wszelkich ograniczeniach jego użycia,
- f) używać systemów do tworzenia i przechowywania certyfikatów, w sposób zapewniający możliwość wprowadzania i zmiany danych jedynie osobom uprawnionym,
- g) jeżeli podmiot zapewnia publiczny dostęp do certyfikatów to ich publikacja wymaga uprzedniej zgody osoby, której wydano ten certyfikat,
- h) udostępniać odbiorcy usług certyfikacyjnych pełny wykaz bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych oraz wykaz warunków technicznych, jakim te urządzenia powinny odpowiadać,
- i) zapewnić, w razie tworzenia przez niego danych służących do składania podpisu elektronicznego, poufność procesu ich tworzenia, a także nie przechowywać i nie kopiować tych danych ani innych danych, które mogłyby służyć do ich

odtworzenia, oraz nie udostępniać ich nikomu innemu poza osobą, która będzie składała za ich pomocą podpis elektroniczny,

- j) zapewnić, w razie tworzenia przez niego danych służących do składania podpisu elektronicznego, aby dane te z prawdopodobieństwem graniczącym z pewnością wystąpiły tylko raz,
  - k) publikować dane, które umożliwią weryfikację (w tym również w sposób elektroniczny) autentyczności i ważności certyfikatów oraz innych danych poświadczanych elektronicznie przez ten podmiot oraz zapewnić nieodpłatny dostęp do tych danych odbiorcom usług certyfikacyjnych.
3. Jeżeli natomiast świadczy usługi certyfikacyjne polegające na znakowaniu czasem obowiązany jest:
- a) zapewnić środki przeciwdziałające fałszerstwom certyfikatów i innych danych poświadczanych elektronicznie przez te podmioty, w szczególności przez ochronę urządzeń i danych wykorzystywanych przy świadczeniu usług certyfikacyjnych,
  - b) zawrzeć umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych,
  - c) udostępniać odbiorcy usług certyfikacyjnych pełny wykaz bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych oraz wykaz warunków technicznych, jakim te urządzenia powinny odpowiadać,
  - d) używać systemów do znakowania czasem, tworzenia i przechowywania zaświadczeń certyfikacyjnych w sposób zapewniający możliwość wprowadzania i zmiany danych jedynie osobom uprawnionym a także zapewnić, że czas w nich określony jest czasem z chwili składania poświadczenia elektronicznego i uniemożliwiają one oznaczenie czasem innym niż w chwili wykonania usługi znakowania czasem.

Osoby wykonujące czynności związane ze świadczeniem usług certyfikacyjnych zatrudnionych przez podmioty świadczące usługi certyfikacyjne muszą spełniać określone warunki:

- a) posiadać pełną zdolność do czynności prawnych,
- b) nie być skazana prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, za przestępstwo skarbowe lub przestępstwa, o których mowa w rozdziale VIII ustawy,

- c) posiadać niezbędną wiedzę i umiejętności w zakresie technologii tworzenia certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym.

### ***1.4.3. Działalności certyfikacyjna***

Podmiot świadczący usługi certyfikacyjne wydaje certyfikat na podstawie umowy. Przed jej zawarciem obowiązany jest poinformować w odpowiedniej formie tj. na piśmie lub za pomocą informacji trwale zapisanej na nośniku elektronicznym, oraz w odpowiedni sposób (jasny i powszechnie zrozumiały) o dokładnych warunkach użycia certyfikatu tj.:

- a) o sposobie rozpatrywania skarg i sporów,
- b) o zakresie i ograniczeniach jego stosowania,
- c) o skutkach prawnych składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu,
- d) o systemie dobrowolnej akredytacji i rejestracji podmiotów kwalifikowanych i ich znaczeniu,
- e) w przypadku certyfikatów nie będących certyfikatami kwalifikowanymi także o tym, że podpis elektroniczny weryfikowany przy pomocy tego certyfikatu nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

Podmiot świadczący usługi certyfikacyjne jest obowiązany uzyskać pisemne potwierdzenie zapoznania się z tą informacją przed zawarciem umowy. Sama umowa o świadczenie usług certyfikacyjnych powinna być sporządzona w formie pisemnej pod rygorem nieważności. Niemniej nieważność umowy o świadczenie usług certyfikacyjnych nie powoduje nieważności certyfikatu, o ile jeżeli przy jego wydaniu podmiot zapoznał się z treścią informacji i poświadczył pisemnie fakt zapoznania się z nią ponadto uzyskano pisemną zgodę na stosowanie danych służących do weryfikacji podpisu elektronicznego, które zawarte są w wydanym certyfikacie.

### ***1.4.4. Znakowanie czasem***

Podpis elektroniczny może być znakowany czasem. Znakowanie czasem to usługa polegająca na dołączeniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenie czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tą usługę. W sytuacji gdy to

znakowanie świadczy kwalifikowany podmiot certyfikacyjny, podpis wywoła skutki prawne daty pewnej w rozumieniu przepisów KC. Uważa się, że podpis został złożony nie później niż w chwili dokonywania tej usługi. Domniemanie to istnieje do dnia utraty ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji tego znakowania. Przedłużenie istnienia domniemania wymaga kolejnego znakowania czasem podpisu elektronicznego wraz z danymi służącymi do poprzedniej weryfikacji przez kwalifikowany podmiot świadczący tę usługę.

#### ***1.4.5. Odpowiedzialność usługodawcy certyfikacyjnego***

Podmiot świadczący usługi certyfikacyjne odpowiada wobec odbiorców usług certyfikacyjnych za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych przez siebie usług. Niewykonanie lub nienależyte wykonanie tych obowiązków może być usprawiedliwiona jedynie tym, że jest następstwem okoliczności, za które podmiot świadczący usługi certyfikacyjne nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności. Nie odpowiada natomiast wobec odbiorców usług certyfikacyjnych za szkody wynikające z użycia certyfikatu poza zakresem określonym w polityce certyfikacji, która została wskazana w certyfikacie, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie. Ponadto nie odpowiada wobec odbiorców usług certyfikacyjnych za szkodę wynikłą z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek osoby składającej podpis elektroniczny. Podmiot świadczący usługi certyfikacyjne, który udzielił gwarancji za certyfikat odpowiada wobec odbiorców usług certyfikacyjnych za wszelkie szkody spowodowane użyciem tego certyfikatu. Wyjątkiem jest sytuacja, kiedy szkoda wynikła z użycia certyfikatu poza zakresem określonym w polityce certyfikacji, która została wskazana w tym certyfikacie.

#### ***1.4.6. Ochrona danych***

Informacje związane ze świadczeniem usług certyfikacyjnych, których nieuprawnione ujawnienie mogłoby narazić na szkodę podmiot świadczący usługi certyfikacyjne lub odbiorcę usług certyfikacyjnych, a w szczególności dane służące do składania poświadczeń elektronicznych, są objęte tajemnicą. Nie są objęte

tajemnicą informacje o naruszeniach ustawy przez podmiot świadczący usługi certyfikacyjne. Do zachowania tej tajemnicy są obowiązane następujące osoby:

- a) osoby reprezentujące podmiot świadczący usługi certyfikacyjne,
- b) osoby pozostające z podmiotem świadczącym usługi certyfikacyjne w stosunku pracy, w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze,
- c) osoby pozostające w stosunku pracy, w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze z podmiotami świadczącymi usługi na rzecz podmiotu świadczącego usługi certyfikacyjne,
- d) osoby i organy, które weszły w jej posiadanie w sposób wskazany w ustawie.

Osoby te i organy mają obowiązek udzielenia informacji o naruszeniach ustawy przez podmiot świadczący usługi certyfikacyjne. Wyjątkiem są dane służące do składania poświadczeń elektronicznych. Udostępnienie tych danych może nastąpić wyłącznie na żądanie n/w podmiotów:

- a) sądu lub prokuratora – w związku z toczącym się postępowaniem,
- b) ministra właściwego do spraw gospodarki – w związku ze sprawowaniem przez niego nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne
- c) innych organów państwowych upoważnionych do tego na podstawie odrębnych ustaw – w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne.

Obowiązek zachowania tajemnicy trwa przez okres 10 lat od ustania stosunków prawnych w/w. Obowiązek zachowania tajemnicy danych służących do składania poświadczeń elektronicznych trwa bezterminowo.

#### ***1.4.7. Dokumentacja***

Podmiot świadczący usługi certyfikacyjne przechowuje i archiwizuje dokumenty i dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami certyfikacyjnymi w sposób zapewniający bezpieczeństwo przechowywanych dokumentów i danych. W przypadku kwalifikowanych podmiotów świadczących usługi certyfikacyjne obowiązek przechowania dokumentów i danych trwa przez okres 20 lat od chwili powstania danego dokumentu lub danych. W przypadku zaprzestania działalności przez kwalifikowany podmiot świadczący usługi certyfikacyjne, dokumenty i dane przechowuje minister właściwy do spraw gospodarki albo wskazany przez niego podmiot. Za

przechowywanie dokumentów i danych minister właściwy do spraw gospodarki pobiera opłatę, której wysokość nie może przekroczyć równowartości w złotych 1 EURO za każdy wydany certyfikat, którego dokumentacja podlega przechowywaniu. Stawka ta jest obliczana według kursu średniego ogłaszanego przez Narodowy Bank Polski, obowiązującego w dniu zaprzestania działalności przez kwalifikowany podmiot świadczący usługi certyfikacyjne. Podmiot świadczący usługi certyfikacyjne jest zobowiązany do zniszczenia danych służących do składania poświadczeń elektronicznych niezwłocznie po unieważnieniu lub po upływie okresu ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji tych poświadczeń.

---

### *1.5. ONZ – UNITRAL*

Świadczący usługi certyfikacyjne to osoba, która nie tylko wydaje certyfikaty, ale może również świadczyć inne usługi związane z podpisami elektronicznymi. Na usługodawcę certyfikacyjnego są nałożone określone warunki, aby jego działania mogły wywołać skutki prawne. Powinien on działać w zgodzie z posiadanymi danymi oraz ustaloną polityką i praktykami. Dla zapewnienia dokładności i kompletności danych zawartych w certyfikacie lub będących dla niego istotne certyfikujący jest zobowiązany dochować należytej staranności. Z certyfikatu musi jasno wynikać kim jest świadczący usługi, że podpisujący jest wiarygodny i że dane tworzące podpis były wiarygodne w momencie wydania certyfikatu. Ponadto tam gdzie to ma znaczenie musi zapewnić dostępność środków, za pomocą których będzie można stwierdzić z certyfikatu bądź w inny sposób, jaka metoda została wykorzystana do uwierzytelnienia podpisującego, jakie są ograniczenia w stosowaniu danych do tworzenia podpisu i certyfikatu, jaki jest zakres odpowiedzialności świadczącego usługi certyfikacyjne, ważność danych tworzących podpis i potwierdzenie, że nie zostały ujawnione, jakie środki do zawiadomienia w sytuacji ewentualnego nieautoryzowanego wykorzystania danych tworzących podpis zostaną podjęte, oraz czy oferowana jest usługa czasowego odwołania. Są sytuacje, gdy ustawa nakłada obowiązek jej zastosowania. Usługodawca powinien korzystać z godnych zaufania systemów, procedur oraz zasobów ludzkich przy wykonywaniu swoich usług. Należy przy tym zwracać uwagę na zasoby finansowe, mienie, zatrudnionych pracowników, jakość systemu, sprzętu i oprogramowania, procedury

dla przetwarzania certyfikatów i aplikacji dla certyfikatów oraz zachowywania danych, dostępność informacji dla podpisujących wskazanych w certyfikatach i potencjalnych stron polegających, prawidłowość oraz zasięg audytów niezależnego organu, istnienie deklaracji państwa, akredytowanego organu lub świadczącego usługi certyfikacyjne, potwierdzającego zgodność lub istnienie wszystkich czynników, o których była wyżej mowa lub innych nie wymienionych, acz istotnych czynników.

---

### *1.6. Unia Europejska*

W Dyrektywie UE usługodawca certyfikacyjny jest określony pojęciem dostawca usług autoryzacyjnych konsekwentnie do używania pojęcia autoryzacja zamiast certyfikat itp. a zatem dostawcą usług autoryzacyjnych jest jednostka, osoba fizyczna lub prawna, która wystawia autoryzacje lub udostępnia inne usługi związane z podpisem elektronicznym. Na dostawców tych zostały nałożone określone wymagania, aby działalność przez nich prowadzona odnosiła zamierzony skutek prawny. Muszą oni udowodnić niezawodność w świadczeniu usług autoryzacyjnych. Usługi zarządzania muszą być szybkie, bezpieczne i pewne, a w przypadku odwołania natychmiastowe. Dostawcy usług muszą dokładnie określić daty, godziny wystawienia i cofnięcia autoryzacji. Zanim zostaną wystawione autoryzacje musi być sprawdzona tożsamość osoby i jej niezbędne atrybuty. Personel, który będzie zatrudniony musi legitymować się odpowiednią wiedzą, doświadczeniem i kwalifikacjami: kompetencje w zakresie managerstwa, znajomości technologii podpisu elektronicznego, stosownych procedur bezpieczeństwa, który będzie stosował właściwe procedury administracyjne i zarządzania odpowiadające uznanym normom. Usługodawcy muszą stosować godne zaufania systemy i produkty, które są chronione przed zmianami i które zapewniają techniczne i kryptograficzne bezpieczeństwo procedur. Przeciwno fałszowaniu autoryzacji zobowiązani są do przedsięwzięcia odpowiednich środków. Gdy są tworzone dane do generowania podpisu musi być zapewniona poufność podczas ich tworzenia. Ponadto muszą dysponować odpowiednim zasobem środków pieniężnych, aby ewentualnie móc ponieść odpowiedzialność za szkody. W stosunku do autoryzacji kwalifikowanej zobowiązani są nagrywać wszystkie istotne informacje, aby móc w późniejszym czasie np. w postępowaniu sądowym posłużyć się tymi zapisami dla

udowodnienia autoryzacji. Dane do generowania podpisu osób, którym oferuje się wykonywanie kluczowych usług zarządzania nie mogą być w żaden sposób gromadzone i kopiowane. Osoba, która zamierza korzystać z usług dostawcy musi zostać uprzednio poinformowana o warunkach stosowania autoryzacji, ograniczenia jej stosowania, istnieniu systemu akredytacji i postępowaniu w przypadku skarg i postępowania pojednawczego. Spełnienie tego obowiązku musi odbyć się w sposób elektroniczny, poprzez przesłanie informacji elektronicznej. Ważne części tych informacji można udostępnić osobom trzecim na ich wniosek. Dostawcy muszą stosować godne zaufania systemy do gromadzenia autoryzacji w formie umożliwiającej sprawdzenie. Systemy te muszą pracować w taki sposób, że tylko osoby uprawnione będą mogły wprowadzać i zmieniać dane, ponadto będzie można sprawdzić prawdziwość informacji, publicznie cofnąć autoryzacje (ale tylko w przypadkach, gdzie została wyrażona zgoda właściciela autoryzacji), będą widoczne dla operatora zmiany techniczne, które wpływają negatywnie na zachowanie tych wymogów bezpieczeństwa.

## ***Rozdział 2***

---

### ***Certyfikaty***

#### ***2.1. Zagadnienia wstępne***

---

Wydawanie certyfikatów to jedna z usług prowadzącego działalność certyfikacyjną. Niniejszy rozdział został całkowicie poświęcony usłudze wydawania certyfikatów. Materiał dotyczący tego tematu zostanie przedstawiony wg ustalonego schematu: najpierw wyjaśnienie czym są certyfikaty i jak można je dzielić, potem jakim warunkom powinien sprostać usługodawca certyfikacyjny, aby móc wydawać ważne certyfikaty.

#### ***2.2. Austria***

---

##### ***2.2.1. Pojęcie i rodzaje certyfikatów***

Ustawa austriacka wyróżnia dwa rodzaje certyfikatów: zwykły<sup>26</sup> i kwalifikowany. Certyfikat zwykły to informacja elektroniczna wiążąca dane do weryfikacji podpisu z określoną osobą, której tożsamość jest określona przez certyfikat. Certyfikat kwalifikowany natomiast to nic innego jak certyfikat zwykły, ale obwarowany specjalnymi wymogami co do treści i co do podmiotu usługodawcy certyfikacyjnego. Certyfikat ten musi być ponadto opatrzony bezpiecznym podpisem elektronicznym. Jeśli chodzi o wymagania co do treści certyfikat kwalifikowany musi zawierać następujące minimum informacji:

- a) oznaczenie, że jest certyfikatem kwalifikowanym,
- b) nazwę usługodawcy certyfikacyjnego i kraju, w którym został ustanowiony,
- c) imię i nazwisko sygnatariusza bądź pseudonim sygnatariusza wraz z oznaczeniem, że to pseudonim,
- d) informacja na temat pełnomocnictw lub innych ważnych atrybutów prawnych sygnatariusza (o ile tego zażąda wnioskodawca),
- e) dane do weryfikacji podpisu przydzielone sygnatariuszowi,
- f) data początkowa i końcowa okresu ważności certyfikatu,

- g) niepowtarzalny identyfikator certyfikatu,
- h) ograniczenie zakresu certyfikatu (o ile takie występuje),
- i) ograniczenie wartości zawieranych transakcji przy użyciu certyfikatu (o ile takie występuje).

Na żądanie wnioskodawcy w certyfikacie kwalifikowanym mogą zostać zamieszczone inne ważne informacje prawne.

### **2.2.2. Wymogi dla usługodawcy certyfikacyjnego**

Certyfikaty kwalifikowane to szczególny rodzaj certyfikatów. Usługodawca je wydający musi spełniać szereg warunków. Przede wszystkim musi wykazać się niezawodnością, jaka wymagana jest do świadczenia usług związanych z podpisami i certyfikatami. Musi świadczyć szybkie i zabezpieczone usługi katalogowania. Unieważniania certyfikatów musi następować natychmiast i być odpowiednio zabezpieczone. Przy wydawaniu certyfikatów kwalifikowanych oraz świadczeniu usług katalogowania i unieważniania usługodawca musi stosować dane określające czas (datownik) o gwarantowanej dokładności, a także zapewnić zawsze możliwość ustalenia czasu wydania lub unieważnienia certyfikatu kwalifikowanego. Sprawdzanie tożsamości i innych ważnych danych osoby, dla której wydawany jest certyfikat powinno odbywać się na podstawie oficjalnych dokumentów (najlepiej ze zdjęciem – to zapewnia wiarygodność tym danym). Pracownicy zatrudnieni w firmie certyfikacyjnej muszą odznaczać się rzetelnością, specjalistyczną wiedzą, doświadczeniem

i kwalifikacjami, a w szczególności umiejętnościami i wiedzą w zakresie technologii bezpiecznych podpisów i odpowiednich procedur zabezpieczeń wymaganych dla świadczenia usług. Ponadto usługodawca certyfikacyjny powinien stosować odpowiednie procedury administracji i zarządzania, zgodnie z uznanymi standardami, legitymować się odpowiednim zapleczem finansowym do tego by spełnić wymagania stawiane przez ustawę i rozporządzenie, a także po to by móc podjąć działania na wypadek roszczeń o odszkodowanie np. polegających na zawarciu ubezpieczenia od odpowiedzialności cywilnej. Musi również prowadzić odpowiedni dziennik, gdzie rejestruje wszystkie istotne fakty dotyczące certyfikatów kwalifikowanych. Dziennik ten musi przechowywać przez określony czas,

---

<sup>26</sup> w ustawie występuje pojęcie „certyfikat” bez żadnego przymiotnika, dla potrzeb odróżnienia go od

odpowiednio do charakteru certyfikatów. Na wypadek zaistnienia pewnych sytuacji określonych w ustawie stwierdzeniem „w razie potrzeby” usługodawca certyfikacyjny zobowiązany jest przechowywać dzienniki także w formie elektronicznej, po to aby w postępowaniu sądowym można było udowodnić fakt certyfikacji. Jest zobowiązany podjąć środki ostrożności, uniemożliwiające przechowywanie lub kopiowanie danych do tworzenia podpisów poszczególnych sygnatariuszy, zarówno przez usługodawcę certyfikacyjnego jak i przez osoby trzecie. Wydając certyfikaty kwalifikowane musi stosować niezawodne systemy, produkty i procedury, które zapewniają ochronę przed modyfikacją oraz zapewniają techniczne i kryptograficzne zabezpieczenie usług związanych z podpisami i certyfikatami odnoszących się do tworzenia i przechowywania certyfikatów. Musi zagwarantować, że dane do tworzenia podpisu zostaną zachowane w tajemnicy. Dzięki temu dane do certyfikatów kwalifikowanych nie będą mogły zostać przerobione lub podrobione w sposób niezauważony. Certyfikaty kwalifikowane mogą być udostępniane publicznie za zgodą sygnatariusza. Przy dostarczaniu danych do tworzenia podpisu oraz przy tworzeniu i przechowywaniu certyfikatów kwalifikowanych usługodawca certyfikacyjny musi stosować środki techniczne i procedury zgodne z wymaganiami ustawy. Spełnienia powyższych warunków w odniesieniu do bezpiecznych podpisów elektronicznych może być poświadczony w trakcie procedury dobrowolnej akredytacji. Fakt, że jest to bezpieczny podpis elektroniczny musi być zaznaczony w certyfikacie lub katalogu dostępnym powszechnie i bez przerwy przez sieć informatyczną w sytuacji, gdy usługodawca certyfikacyjny udostępnia procedurę składania bezpiecznego podpisu elektronicznego. Na żądanie sądu lub innych władz usługodawca certyfikacyjny będzie zobowiązany zweryfikować bezpieczny podpis oparty na certyfikacie kwalifikowanym wydanym przez tego usługodawcę.

Na żądanie zainteresowanego usługodawca certyfikacyjny w certyfikacie zamieszcza informacje dotyczące pełnomocnictw i innych ważnych informacji, pod warunkiem, że fakty zostaną w sposób wiarygodny udowodnione a także zamiast imienia i nazwiska pseudonim wnioskodawcy. Jest jeden warunek tego zamieszczenia. Pseudonim nie może mieć charakteru obraźliwego, nie może również stwarzać możliwości pomylenia z nazwiskami czy znakami innych podmiotów.

---

certyfikatu kwalifikowanego posłużyłam się przymiotnikiem „zwykły”

### **2.2.3. Sprawdzenie tożsamości**

Zanim nastąpi wydanie certyfikatu kwalifikowanego muszą zostać zgromadzone odpowiednie dane oraz należy sprawdzić tożsamość wnioskodawcy. Sprawdzenie na podstawie dokumentów ze zdjęciem uważane jest za wiarygodny sposób sprawdzania tożsamości. Jest to czynność ważna o tyle, że przez wydanie certyfikatu kwalifikowanego usługodawca certyfikacyjny potwierdza, że danej osobie zostały przydzielone określone dane do certyfikacji podpisu. Wydanie certyfikatu następuje na wniosek zainteresowanego. Może być on złożony zarówno do organu prowadzącego usługi w zakresie certyfikacji jak i do organu wskazanego przez usługodawcę certyfikacyjnego, który to sprawdza tożsamość wnioskodawcy.

### **2.2.4. Unieważnienie certyfikatu**

Certyfikat w okresie ważności wywołuje określone skutki prawne. Zrozumiałym jest, że po upływie okresu ważności nie wywołuje już żadnych skutków prawnych. Może się jednak zdarzyć na skutek zaistniałych okoliczności, że certyfikat przestanie wywoływać skutki przed upływem terminu ważności. Dzieje się tak

w przypadku unieważnienia certyfikatu. Unieważnienie może nastąpić z urzędu lub na wniosek. Unieważnienie z urzędu ma miejsce w razie śmierci sygnatariusza, zmiany faktów potwierdzonych w certyfikacie, w razie zaprzestania działalności certyfikacyjnej, a usługi katalogowania i unieważniania nie zostaną przejęte przez innego usługodawcę certyfikacyjnego, kiedy wyjdzie na jaw, że certyfikat został wydany na podstawie fałszywych danych, oraz kiedy zachodzi obawa, że certyfikat zostanie wykorzystany w sposób niewłaściwy.

Unieważnienie certyfikatu może nastąpić, jeżeli powyższe okoliczności zostaną stwierdzone w sposób nie budzący wątpliwości. Jeżeli natomiast nie można tego udowodnić natychmiast, usługodawca jest zobowiązany zablokować certyfikat do momentu wyjaśnienia. Blokada lub unieważnienie certyfikatu musi być opatrzone datą i godziną, od której te czynności stały się skuteczne. Niedopuszczalne jest dokonanie tych czynności z mocą wsteczną. Niezwłocznie po dokonaniu blokady lub unieważnienia certyfikatu powiadamia się sygnatariusza lub jego następcę prawnego. Usługodawca certyfikacyjny publikuje listę unieważnionych i zablokowanych certyfikatów w sieci informatycznej. Unieważnienie certyfikatu może nastąpić przez

organ nadzorczy. Dzieje się tak, kiedy usługodawca certyfikacyjny dostanie zakaz prowadzenia działalności, lub zawiesi tą działalność, a jego usługi w zakresie katalogowania i unieważniania nie zostaną przejęte przez innego usługodawcę certyfikacyjnego.

Unieważnienie z innych przyczyn niż w/w następuje na wniosek sygnatariusza lub osoby przez niego upoważnionej, oraz organu nadzorczego.

### *2.3. Niemcy*

---

Certyfikat w rozumieniu ustawy niemieckiej to cyfrowe zaświadczenie o przyporządkowaniu klucza publicznego do osoby fizycznej, nie pozostawiające wątpliwości co do tego, do kogo należą klucze. Pod względem formalnym certyfikat musi zawierać nazwisko posiadacza certyfikatu, które podlega uprzedniemu sprawdzeniu w celu wykluczenia możliwości omyłki. Certyfikat zostaje naznaczonym unikatowym znakiem, po którym rozpoznaje się posiadacza certyfikatu. Ponadto certyfikat musi zawierać przyporządkowany klucz publiczny podmiotu, dla którego został wydany, oznaczenie algorytmu szyfrowania, który wykorzystuje się do odszyfrowania danych, bieżący numer certyfikatu, początek i koniec ważności certyfikatu, nazwę usługodawcy certyfikacyjnego i jego klucz publiczny oraz ograniczenie użytkowania kluczy. Ponadto musi się też znaleźć informacja o pełnomocnictwie.

Przyszły usługodawca certyfikacyjny potrzebuje zatwierdzenie, że spełnia określone warunki. To zatwierdzenie wydawane jest na wniosek. Usługodawcy certyfikacyjny musi posiadać wymaganą pewność, zatrudniać odpowiednich fachowców i specjalistów, sprawdzać tożsamość wnioskodawcy, zamieszczać na certyfikacie odpowiednie dane. Na żądanie wnioskodawcy w certyfikacie wykazuje się również informacje co do dopuszczenia pełnomocnictw, pseudonim zamiast nazwiska. Usługodawca certyfikacyjny podejmie kroki, żeby uniemożliwić sfałszowanie danych, żeby została zachowana tajemnica klucza prywatnego. Przechowywanie klucza prywatnego w miejscu certyfikacji jest zabronione. Usługodawca certyfikacyjny podejmie kroki również, aby przeciwdziałać praktykom uprawiania certyfikacji w jego zakładzie przez nieuprawnione osoby. Przygotowanie do wygenerowania kluczy, jak również wystawienia certyfikatów wymaga

zastosowania technicznych komponentów. Od tych komponentów zależy ważność, bowiem one umożliwiają sprawdzenie certyfikatu.

### 2.4.1. Pojęcie i rodzaje certyfikatów

Regulacja polska wymienia dwa rodzaje certyfikatów: krajowe i zagraniczne, przy czym krajowe dzielą się na zwykłe i kwalifikowane. Certyfikat zwykły to elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny

i które umożliwiają identyfikację tej osoby. Certyfikat kwalifikowany natomiast to certyfikat zwykły, ale wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne i zawierający odpowiednie dane. Oto minimum informacji, które z urzędu muszą znaleźć się w certyfikacie kwalifikowanym

- a) numer certyfikatu,
- b) wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji,
- c) określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę oraz numer akredytacji lub pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
- d) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone,
- e) dane służące do weryfikacji podpisu elektronicznego,
- f) oznaczenie początku i końca okresu ważności certyfikatu,
- g) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat,
- h) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji,
- i) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa.

Oprócz w/w danych na wniosek osoby składającej podpis w certyfikacie może znaleźć się wskazanie czy osoba ta działa we własnym imieniu, albo jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej, albo w charakterze członka organu albo

organu osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej, albo jako organ władzy publicznej.

Przed wydaniem certyfikatu podmiot świadczący usługi certyfikacyjne jest zobowiązany sprawdzić prawdziwość danych potrzebnych do wydania certyfikatu, następnie powiadomić odpowiednie podmioty i pouczyć o możliwości unieważnienia certyfikatu na ich wniosek.

Oprócz certyfikatu ustawa polska wyróżnia również zaświadczenie certyfikacyjne i poświadczenie elektroniczne. Zaświadczenie certyfikacyjne to elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu, które umożliwiają identyfikację tego podmiotu lub organu, natomiast poświadczenie elektroniczne to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne oraz spełniają następujące wymagania:

- a) są sporządzone za pomocą urządzeń i danych podlegających wyłącznej kontroli podmiotu dokonującego poświadczenia elektronicznego,
- b) jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

#### **2.4.2. Unieważnianie certyfikatów**

Certyfikat jest ważny w okresie w nim wskazanym. Niemniej może być unieważniony przed upływem tego terminu w następujących sytuacjach:

- a) został wydany na podstawie nieprawdziwych lub nieaktualnych danych,
- b) usługodawca certyfikacyjny nie dopełnił obowiązków określonych w ustawie,
- c) osoba składająca podpis elektroniczny weryfikowany na podstawie tego certyfikatu nie dopełniła obowiązków,
- d) podmiot świadczący usługi certyfikacyjne zaprzestał świadczenia usług certyfikacyjnych, a jego praw i obowiązków nie przejął inny kwalifikowany podmiot,
- e) zażądała tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie,
- f) zażądał tego minister właściwy do spraw gospodarki,

g) osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych.

Unieważnienie certyfikatu przed upływem terminu ważności z powodu niedopełnienia obowiązków określonych ustawą nie wyłącza odpowiedzialności podmiotu świadczącego usługi certyfikacyjne za szkodę względem osoby składającej podpis elektroniczny. W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, podmiot świadczący usługi certyfikacyjne jest obowiązany niezwłocznie zawiesić certyfikat i podjąć działania niezbędne do wyjaśnienia tych wątpliwości. Zawieszenie to nie może trwać dłużej niż 7 dni. Po upływie tego okresu mimo niemożności wyjaśnienia tych podejrzeń podmiot świadczący usługi certyfikacyjne jest zobowiązany do niezwłocznego unieważnienia certyfikatu. Zawieszenie certyfikatu może zostać uchylone, ale jeśli już certyfikat został unieważniony, nie może być następnie uznany za ważny. W przypadku unieważnienia lub zawieszenia certyfikatu, podmiot świadczący usługi certyfikacyjne zawiadamia niezwłocznie osobę składającą podpis elektroniczny weryfikowany na jego podstawie. Zawieszenie lub unieważnienie certyfikatu nie może nastąpić z mocą wsteczną.

Podmiot świadczący usługi certyfikacyjne publikuje listę zawieszonych i unieważnionych certyfikatów. Informacje o unieważnieniu lub zawieszeniu certyfikatów publikowane są najpóźniej w godzinę po tym fakcie. Informacje te ponadto zostają zamieszczone w każdej liście publikowanej przed dniem upływu okresu ważności certyfikatu oraz na pierwszej liście publikowanej po upływie tego okresu. Lista zawieszonych i unieważnionych kwalifikowanych certyfikatów powinna zawierać w szczególności:

- a) numer kolejny listy i wskazanie, że lista została opublikowana zgodnie z określoną polityką certyfikacji i dotyczy certyfikatów wydanych zgodnie z tą polityką,
- b) datę i czas opublikowania listy z dokładnością określoną w polityce certyfikacji,
- c) datę przewidywanego opublikowania kolejnej listy,
- d) określenie podmiotu świadczącego usługi certyfikacyjne wydającego listę i państwa, w którym ma on siedzibę, oraz w przypadku akredytowanego podmiotu świadczącego usługi certyfikacyjne – numer akredytacji, a w przypadku

- kwalfikowanego podmiotu świadczącego usługi certyfikacyjne – numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
- e) numer każdego zawieszzonego lub unieważnionego certyfikatu oraz wskazanie, czy został on unieważniony czy zawieszony,
  - f) datę i czas z dokładnością określoną w polityce certyfikacji,
  - g) zawieszenia lub unieważnienia każdego certyfikatu,
  - h) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, publikującego listę.

Oprócz certyfikatów krajowych ustawa polska wymienia jeszcze jedną kategorię certyfikatów powstałą u uwagi na podmiot je wydający i są to certyfikaty zagraniczne. Certyfikaty zagraniczne to takie, które zostały wydane przez podmiot nie mający siedziby na terytorium RP i nie świadczący usług na jej terytorium. Niemniej certyfikaty te mogą zostać zrównane z certyfikatami krajowymi, o ile spełnią jedną z poniższych przesłanek:

- a) podmiotowi świadczącemu usługi certyfikacyjne, który wydał ten certyfikat, została udzielona akredytacja,
- b) przewiduje to umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, o wzajemnym uznaniu certyfikatów,
- c) podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, spełnia wymagania ustawy i została mu udzielona akredytacja w państwie członkowskim Unii Europejskiej,
- d) podmiot świadczący usługi certyfikacyjne, mający siedzibę na terytorium Wspólnoty Europejskiej spełniający wymogi ustawy, udzielił gwarancji za ten certyfikat,
- e) certyfikat ten został uznany za kwalifikowany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi,
- f) podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, został uznany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi.

Certyfikat to dane w wiadomości albo inny zapis potwierdzający związek pomiędzy podpisującym a danymi tworzącymi podpis. Początkowo w projekcie można było znaleźć pojęcie certyfikatu tożsamości (identity certificate), ale zrezygnowano z tego rozwiązania. W sytuacji rozstrzygnięcia do jakiego stopnia certyfikat jest prawnie skuteczny projekt ustawy nie bierze pod uwagę geograficznego położenia miejsca wydania certyfikatu lub miejsca prowadzenia działalności wystawcy lub podpisującego. Certyfikat wydany poza państwem przyjmującym niniejszą ustawę ma taki sam skutek prawny w państwie ją przyjmującym jak certyfikat w nim wydany, jeżeli zapewnia odpowiednio równoważny stopień pewności. Przy określeniu czy certyfikat zapewnia ten stopień należy wziąć pod uwagę uznane międzynarodowe standardy i wszelkie istotne czynniki. Jeżeli strony uzgodnią między sobą użycie określonych typów certyfikatów, takie porozumienie jest uznawane za wystarczające dla potrzeb międzynarodowego uznania, chyba że takie porozumienie nie byłoby ważne albo skuteczne według prawa właściwego.

W Dyrektywie UE nie ma pojęcia certyfikat. Występuje pojęcie autoryzacja. Są dwa rodzaje autoryzacji: zwykła i kwalifikowana. Autoryzacja zwykła to zaświadczenie elektroniczne, za pomocą którego dane do sprawdzania podpisu są przyporządkowane osobie i potwierdzają tożsamość tej osoby. Autoryzacja kwalifikowana to autoryzacja:

- a) spełniająca określone wymogi, o których była już mowa w poprzedniej części, w rozdziale o skutkach podpisu elektronicznego,
- b) wystawiana przez dostawcę usług autoryzacyjnych, który musi spełniać określone warunki (o tych warunkach również była już mowa w poprzedniej części pracy).

## ***Rozdział 3***

---

### ***Nadzór***

#### ***3.1. Zagadnienia wstępne***

---

Ostatnim i najwyższym postawionym ogniwem w hierarchii organów aparatu wykonawczego jest instytucja nadzoru. Ten rozdział traktuje o organach nadzoru, ich obowiązkach i uprawnieniach. Jest on o tyle ważny w strukturze administracji, że to on ma ostatni głos w kwestii istnienia usługodawcy certyfikacyjnego i idących za tym konsekwencji.

#### ***3.2. Austria***

---

Według prawa austriackiego instytucja nadzoru, aby móc fachowo wypełniać swoje obowiązki, musi zostać uprzednio do tego przygotowana. Ponadto musi zagwarantować wymaganą niezawodność, niezależność, neutralność i bezstronność. Za przygotowaną uważa się wtedy, gdy będzie w stanie to zagwarantować. Musi zatrudniać odpowiednio wykwalifikowaną kadrę, posiadać odpowiednie wyposażenie techniczne i warunki finansowe. Pracownicy muszą legitymować się specjalistyczną wiedzą, doświadczeniem i kwalifikacjami, a w szczególności wiedzą w zakresie podpisów elektronicznych, odpowiednich procedur zabezpieczeń, kryptografii, technologii komunikacyjnej oraz technologii kart inteligentnych. Muszą umieć korzystać ze środków technicznych niezbędnych do wypełniania obowiązków spoczywających na instytucji. Pozwolenie czy licencje na prowadzenie takiej działalności wydaje Kanclerz Federalny w porozumieniu z Ministrem Sprawiedliwości na wniosek zainteresowanego w drodze rozporządzenia<sup>27</sup>.

##### ***3.2.1. Organ nadzoru***

Nadzór nad przestrzeganiem postanowień ustawy i rozporządzeń na jej podstawie wydanych będzie organ nadzoru – Komisja Kontroli Telekomunikacji ustanowiona na mocy § 110 ustawy Prawo telekomunikacyjne.

---

<sup>27</sup> przypomnienie źródło tłumaczenie ustawy austriackiej

Do obowiązków Komisji w szczególności będzie należało:

- a) kontrolowanie w zakresie realizacji reguł zabezpieczenia i certyfikacji zawartych w deklaracji,
- b) monitoring w zakresie stosowania odpowiednich środków technicznych przez usługodawców certyfikacyjnych dostarczających bezpieczne podpisy elektroniczne,
- c) dokonywanie akredytacji usługodawców certyfikacyjnych zgodnie z postanowieniami ustawy,
- d) nadzór nad organizacją instytucji zatwierdzającej.

Ponadto zobowiązana jest zapewnić:

- a) powszechną i nieprzerwaną dostępność przez sieć informatyczną katalogu ważnych, zablokowanych i unieważnionych certyfikatów wszystkich usługodawców certyfikacyjnych,
- b) powszechną i nieprzerwaną dostępność przez sieć informatyczną katalogu usługodawców certyfikacyjnych zgłoszonych w Austrii, katalogi usługodawców akredytowanych przez organ nadzorczy oraz katalogu zagranicznych usługodawców certyfikacyjnych zgłoszonych w Austrii.

Katalog certyfikatów usługodawców certyfikacyjnych będzie zawierać certyfikaty kwalifikowane upoważniające tych usługodawców do świadczenia usług certyfikacyjnych. Organ nadzorczy może także wydawać takie certyfikaty. Każdy katalog publikowany przez organ nadzoru będzie opatrzony bezpiecznym podpisem elektronicznym tego organu. Certyfikat organu nadzorczego zostanie opublikowany w Dzienniku Urzędowym wydawanym przez Wiener Zeitung.

Następnym zagadnieniem są koszty działalności organu i prac wykonywanych przez spółkę TelekomControl GmbH. Zgodnie z ustawą koszty te będą pokrywane z opłat pobieranych od usługodawców certyfikacyjnych, zgodnie z rozporządzeniem.

W razie potrzeby organ nadzorczy może zasięgać porad odpowiednich osób lub instytucji jak np. instytucji zatwierdzającej.

Członkowie organu nadzorczego przy wykonywaniu swych funkcji nie są związani żadnymi instrukcjami. Organ nadzorczy jest ostatnią instancją decyzyjną i może odwoływać się do sądu administracyjnego.

### 3.2.2. Środki nadzoru

Środki nadzoru są używane wobec usługodawców certyfikacyjnych w celu przymuszenia ich do wykonania ustawowych obowiązków.

Środki nadzoru, które w szczególności organ nadzoru jest obowiązany użyć:

- a) zabronić używania nieodpowiednich środków technicznych i procedur przy stosowaniu niektórych lub wszystkich usług,
- b) unieważnić certyfikat usługodawcy certyfikacyjnego lub certyfikat sygnatariusza,
- c) nakazać usługodawcy certyfikacyjnemu unieważnienie certyfikatu sygnatariusza.

Ponadto organ nadzorczy może zakazać prowadzić działalność usługodawcy certyfikacyjnemu w całości lub części w przypadkach uchybień wymogom ustawy, a w szczególności w razie:

- a) braku rzetelności niezbędnej przy świadczeniu usług związanych z podpisami i certyfikatami,
- b) braku niezbędnej wiedzy specjalistycznej,
- c) braku dostatecznych zasobów finansowych,
- d) braku stosowania reguł zabezpieczenia i certyfikacji określonych w deklaracji,
- e) braku świadczenia usług katalogowania i unieważniania lub świadczenia ich w sposób nienależyty, bądź braku wypełniania obowiązków blokowania lub unieważniania,
- f) nie wypełnianie obowiązków powiadamiania,
- g) gdy środki techniczne i procedury nie spełniają wymagań ustawowych.

Konsekwencją zakazania ustawodawcy certyfikacyjnemu działalności jest unieważnienie certyfikatów wydanych przez danego usługodawcę, a także jego certyfikatu. Drugą konsekwencją jest spowodowanie, że usługi związane z podpisami i certyfikatami w całości lub w części zostaną przejęte przez innego usługodawcę. Oczywiście muszą zostać powiadomieni o tym fakcie sygnatariusze, a na przejęcie usług muszą wyrazić zgodę obaj usługodawcy. Usługodawca jest zobowiązany do zapewnienia kontynuowania unieważniania certyfikatów, nawet po unieważnieniu.

W przeciwnym wypadku organ nadzorczy wykona to na koszt usługodawcy, który nie dopełnił obowiązku.

Jeżeli możliwe jest użycie środków naprawczych organ nadzorczy wstrzyma decyzję o zakazie działalności usługodawcy certyfikacyjnemu. Warunkiem

zastosowania tych środków jest zapewnienie powodzenia w uzyskaniu rezultatu w postaci przestrzegania postanowień ustawy i wydanych na jej podstawie rozporządzeń. Organ nadzorczy w celu zapewnienia powodzenia temu przedsięwzięciu może nałożyć pewne obowiązki lub zagrozić podjęciem pewnych działań, jeśli usługodawca nie dostosuje się do zaleceń organu nadzorczego w określonym terminie.

### **3.2.3. Spółka Telekom-Control GmbH**

Spółka ta świadczy usługi dla organu nadzorczego. Ma on w szczególności prawo do korzystania z następujących usług:

- a) pomoc w nadzorze usługodawców certyfikacyjnych oraz kontroli produktów technicznych, procedur i innych środków używanych w celu świadczenia usług związanych z podpisami i certyfikatami, a także w kontroli kwalifikacji zatrudnianych pracowników,
- b) rejestracja usługodawców certyfikacyjnych, którzy składają zawiadomienie o rozpoczęciu działalności,
- c) utrzymywanie katalogu: usługodawców certyfikacyjnych, certyfikatów innych usługodawców certyfikacyjnych, akredytowanych usługodawców certyfikacyjnych,
- d) kontynuacja usług unieważniania po usługodawcy certyfikacyjnym, którego działalność została zawieszona lub zakazana, jeśli usługi te nie zostały przejęte przez innego usługodawcę certyfikacyjnego,
- e) badanie zgodności z warunkami dobrowolnej akredytacji,
- f) pomoc w ustaleniu równoważności zagranicznych raportów testowych,
- g) wprowadzenie zakazu czasowego prowadzenia działalności usługodawcy certyfikacyjnego w przypadku uzasadnionego podejrzenia niedopełnienia wymagań  
w zakresie ustawowych zabezpieczeń lub na żądanie usługodawcy certyfikacyjnego,
- h) zastosowanie środków nadzorczych.

Telekom-Control GmbH wspomaga organ nadzorczy w wypełnianiu przezeń obowiązków. Przy wykonywaniu tych obowiązków może korzystać z porad różnych osób czy instytucji w szczególności instytucji zatwierdzającej. Pracownicy spółki są

zobowiązani do wykonywania poleceń dyrektora lub członka zarządu, który współpracuje z organem nadzorczym.

Spółka rozpatruje roszczenia i skargi klientów lub innych zainteresowanych osób przeciw usługodawcom certyfikacyjnym w sprawach, w których nie zdołano wypracować zadowalającego rozwiązania z usługodawcą. Dołoży ona wszelkich starań, aby znaleźć rozwiązanie, które zadowoli obie strony. Usługodawca certyfikacyjny w tym zakresie jest zobowiązany współpracować ze spółką, w szczególności dostarczać jej wszelkich informacji do oceny sytuacji. W odpowiednim czasie ustali ona wytyczne do realizacji i opublikuje je w odpowiedniej formie.

### ***3.2.4. Współpraca z organem nadzorczym***

Usługodawca certyfikacyjny jest zobowiązany współpracować z organem nadzorczym, w szczególności zapewniać swobodny dostęp do pomieszczeń, obiektów biurowych i operacyjnych w godzinach pracy, przedłożyć lub udostępnić do kontroli księgi oraz inne rejestry i dokumenty, udzielić wszelkich informacji i pomocy. Kontrolę należy wykonywać w sposób, który spowoduje jak najmniejsze utrudnienie pracy dla zainteresowanych stron, a tym samym uniknie niepotrzebnego i niepożądanego przyciągania uwagi.

Na żądanie organu nadzorczego pomocy udzielą również funkcjonariusze Służby Bezpieczeństwa.

---

## ***3.3. Polska***

### ***3.3.1. Organ i środki nadzoru***

Organem sprawującym nadzór nad podmiotami świadczącymi usługi certyfikacyjne jest minister właściwy do spraw gospodarki. Sprawuje on nadzór w zakresie przestrzegania przepisów ustawy, zapewniając tym samym ochronę interesów odbiorców usług certyfikacyjnych. To zadanie może realizować poprzez:

- a) akredytację podmiotów świadczących usługi certyfikacyjne,
- b) prowadzenie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
- c) wydawanie i unieważnianie zaświadczeń certyfikacyjnych,

- d) kontrolę działalności podmiotów świadczących usługi certyfikacyjne pod względem zgodności z ustawą,
- e) nakładanie kar przewidzianych w ustawie

### 3.3.1.1 Prowadzenie rejestrów kwalifikowanych podmiotów świadczących usługi certyfikacyjne

Prowadzenie tych rejestrów minister może powierzyć n/w podmiotom, które spełniają wymagania ustawy dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne w zakresie bezpieczeństwa, wydawania, przechowywania i unieważniania certyfikatów i nie świadczą usług certyfikacyjnych polegających na wydawaniu certyfikatów:

- w trybie przepisów o zamówieniach publicznych – podmiotowi świadczącemu usługi certyfikacyjne wytwarzanie i wydawanie zaświadczeń certyfikacyjnych, publikację listy wydanych zaświadczeń certyfikacyjnych oraz danych służących do weryfikacji wydanych zaświadczeń certyfikacyjnych,
- na wniosek prezesa NBP – Narodowemu Banku Polskiemu lub wskazany we wniosku podmiot pozostający z NBP w stosunku zależności – do wykonywania usług, o których była wyżej mowa.

### 3.3.1.2. Cofnięcie akredytacji lub wykreślenie wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne

Środki te podjęte zostaną w sytuacji, gdy podmiot świadczący usługi certyfikacyjne:

- a) prowadzi działalność niezgodnie z przepisami ustawy w sposób zagrażający interesom odbiorców usług certyfikacyjnych, lub
- b) złoży wniosek o cofnięcie akredytacji lub wykreślenie wpisu w rejestrze, lub
- c) planuje zakończenie działalności i zawiadamia o tym ministra właściwego do spraw gospodarki, lub
- d) odmówi poddania się kontroli.

Wydanie decyzji o cofnięciu akredytacji skutkuje wykreśleniem wpisu z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Zamiast decyzji może wezwać podmiot do usunięcia nieprawidłowości jednocześnie nakładając karę pieniężną w zależności o wagi nieprawidłowości do 50.000 zł. Kara ta podlega egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji. Wydając decyzję u cofnięciu akredytacji minister właściwy do spraw gospodarki może jednocześnie unieważnić zaświadczenie certyfikacyjne i umieścić je na liście unieważnionych zaświadczeń certyfikacyjnych kwalifikowanych podmiotów

świadczących usługi certyfikacyjne. Unieważnienie zaświadczenia certyfikacyjnego powoduje nieważność poświadczeń elektronicznych wydanych po dacie unieważnienia zaświadczenia certyfikacyjnego.

#### 3.3.1.3. Kontrola działalności podmiotów świadczących usługi certyfikacyjne

Kontrola przeprowadzana jest z urzędu lub na żądanie prokuratora lub sądu albo innych organów państwowych upoważnionych do tego na podstawie ustaw w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne. Kontrola prowadzona jest pod względem czy prowadzona działalność certyfikacyjna jest zgodna z wymaganiami ustawy. W tym celu pracownicy i kierownicy są obowiązani współpracować z kontrolerami i osobami upoważnionymi. W razie stwierdzenia nieprawidłowości zostaje wyznaczony termin do ich usunięcia w terminie 14 dni.

## ***Cz ę ś ć III***

---

*Techniczne zagadnienia podpisu elektronicznego*

# *R o z d z i a ł 1*

## *Szyfrowanie*

### *1.1. Zagadnienia wstępne*

Podpis elektroniczny wymaga zastosowania określonej technologii. Najbardziej znaną i stosowaną jest technologia oparta o kryptografię. Podpis wygenerowany tą metodą jest podpisem cyfrowym, dlatego od tej pory będę posługiwać się tym właśnie pojęciem. W stosowaniu tej technologii niezaprzeczalnym liderem są Stany Zjednoczone. Mają one najbardziej rozbudowaną sieć, w związku z czym tam przez Internet dochodzi do skutku najwięcej transakcji handlowych. Mają największe osiągnięcia w dziedzinie elektronicznego transferu danych oraz ich uwierzytelniania. Z uwagi na ich duże w tej kwestii doświadczenie nieco uważniej przyjrzałam się technologii, którą oni posługują się od lat. Na potrzeby tej pracy wykorzystałam schematy działań i zastosowań algorytmów do szyfrowania, zarządzania kluczami i podpisów cyfrowych stosowane przez pakiety produktów uważanych za najpopularniejsze i najczęściej używane jak PEM<sup>28</sup> czy PGP<sup>29</sup>. Zapewniają one poufność, uwierzytelnianie pochodzenia danych, spójność wiadomości, uniemożliwienie nie przyznania się do autorstwa wiadomości i zarządzania kluczami.

Szyfrowanie ogólnie mówiąc to przekształcanie czytelnej informacji czyli tekstu jawnego w niezrozumiały ciąg znaków. Opiera się na dwóch podstawach: algorytmie i kluczu. Algorytm jest przekształceniem matematycznym, za pomocą którego tekst jawny przekształca się w ciąg nieczytelnych znaków i odwrotnie. Klucz to losowy ciąg bitów, którego używa się łącznie z algorytmem. Każdy klucz powoduje inny sposób pracy algorytmu. Są różne rodzaje algorytmów i różne rodzaje kluczy, jedne i drugie mają różne zastosowanie. Z uwagi na ich różną złożoność, szybkość i bezpieczeństwo są wykorzystywane do różnych celów jak np. do szyfrowania

<sup>28</sup> PEM (Privacy-Enhanced Mail) standard dla sieci Internet, który definiuje metody szyfrowania wiadomości i procedury uwierzytelniania w celu zapewnienia bezpieczeństwa korespondencji.

<sup>29</sup> PGP jest programem do ochrony poczty elektronicznej

dokumentów, zarządzania kluczami, podpisów cyfrowych. W tej części pracy zostaną przedstawione podstawowe rodzaje kryptografii, wybrane algorytmy, oraz zaprezentowaniem schematów i zastosowań poszczególnych rodzajów kryptografii.

---

## 1.2. *Kryptografia symetryczna*

### 1.2.1. *Algorytm DES – istota działania*

Algorytmem wykorzystywanym w kryptografii symetrycznej jest m.in. algorytm DES. Algorytm DES (ang. *Data Encryption Standard*) zwany czasem iterowanym szyfrem blokowym jest międzynarodowym algorytmem szyfrującym, zaprojektowanym w firmie IBM na początku lat siedemdziesiątych. W 1976r został zaadaptowany przez NBS (National Bureau of Standards – Narodowe Biuro Standardów obecnie NIST – National Institute of Standards and Technology) jako rządowy standard szyfrowania. Stosowany w prawie wszystkich rodzajach łączności elektronicznej i przechowywania danych. DES jest algorytmem blokowym. Oznacza to, że całość danych dzielone są na określone części – bloki. W przypadku DES blok ma 8 bajtów – cały dokument jest dzielony na takie 8 bajtowe części. Na raz algorytm szyfruje 8 bajtów tekstu jawnego i powstaje 8 bajtów tekstu zaszyfrowanego. Deszyfruje również w porcjach 8 bajtowych. Algorytm składa się z 16 powtarzających się prostych funkcji zwanych iteracjami. Im większa liczba iteracji lub cykli zapewnia większe bezpieczeństwo. Dodanie dalszych iteracji algorytmowi DES nie poprawi w sposób znaczący jego bezpieczeństwa, które jest i tak bardzo wysoko oceniane. Złamany może być tylko przez łamanie brutalne. Łamanie brutalne to łamanie z tekstem jawnym i aby było możliwe do wykonania wymaga bardzo małego fragmentu tekstu zaszyfrowanego i tak samo małego odpowiadającego mu tekstu jawnego. Istota polega na tym, że metodą prób i błędów eliminuje się po kolei wszystkie możliwe klucze, aż do znalezienia tego właściwego, którego tekst odszyfrowany będzie w 100% zgodny z tekstem jawnym. Jest to ewidentne wskazanie, że jest to klucz właściwy i można odszyfrowywać resztę tekstu. Łamanie brutalne jest na tyle niebezpieczne, że nie można mu w żaden sposób zapobiec, zawsze istnieje ryzyko, że dla odszyfrowania tekstu będą wykorzystywane wszystkie możliwe klucze, aż do znalezienia tego właściwego. Skoro nie można zapobiec łamaniu to można spróbować zniechęcić do łamania

poprzez podniesienie kosztów tego ataku w kwestii czasu i pieniędzy. Oprócz wyżej zaprezentowanego algorytmu są jeszcze inne.

### 1.2.2. Szybkość i bezpieczeństwo

Wybierając algorytm należy pamiętać o dwóch najważniejszych kwestiach: o bezpieczeństwie i szybkości. Bezpieczeństwo algorytmu szyfrującego opiera się na bezpieczeństwie klucza. Poniżej tabela podsumowująca aspekt bezpieczeństwa wybranych algorytmów stosowanych w kryptografii symetrycznej z uwzględnieniem długości klucza i atakiem na nie.

Algorytm	Długość klucza	Najlepszy atak	Uwagi
DES	56 bitów	łamanie brutalne	łamanie brutalne wykonalne
Potrójny DES <sup>30</sup>	112 bitów	łamanie brutalne	łamanie brutalne niewykonalne
IDEA <sup>31</sup>	128 bitów	łamanie brutalne	zbyt nowy algorytm
RC2	zmienna	nieznany	szczegóły algorytmu nie są znane
RC4 <sup>32</sup>	zmienna	nieznany	szczegóły algorytmu nie są znane

**Tabela: Bezpieczeństwo wybranych algorytmów<sup>33</sup>**

Komentując zamieszczone w tabelce informacje widzimy, że jeżeli chodzi o bezpieczeństwo to najlepszym algorytmem zdaje się być potrójny DES. Jest on uważany za bardzo silny, ponieważ nikomu nie udało się go złamać. Niemniej nie można udowodnić ponad wszelką wątpliwość, że ten algorytm jest niełamałny, ale istnieje olbrzymia ilość dowodów, że tak właśnie jest. Wadą tego algorytmu jest jego powolność. Jest on najwolniejszy z trzech czołowych z tabeli algorytmów.

W literaturze podkreśla się, że nie ma stu procentowo bezpiecznych algorytmów. Wszystkie dadzą się złamać – to kwestia sprzętu i czasu. Nawet te, które uznane są za najbezpieczniejsze nikt nie zaryzykuje twierdzenia, że są one

<sup>30</sup> Potrójny DES – wariant algorytmu DES, w którym następuje trzykrotne szyfrowanie wiadomości z apomoca DES. Jeżeli do każdego szyfrowania użyjemy innego klucza, to wynikowy algorytm jest znacznie bardziej bezpieczny niż pojedynczy DES. Szerzej Bruce Schneier „Ochrona ...”

<sup>31</sup> IDEA – (ang. *International Data Encryption Algorithm*) jest międzynarodowym algorytmem szyfrowania danych. Wynaleziony przez Jamesa Massey’a i Xuejia Lai-a w 1991r szerzej Bruce Schneier „Ochrona ...”

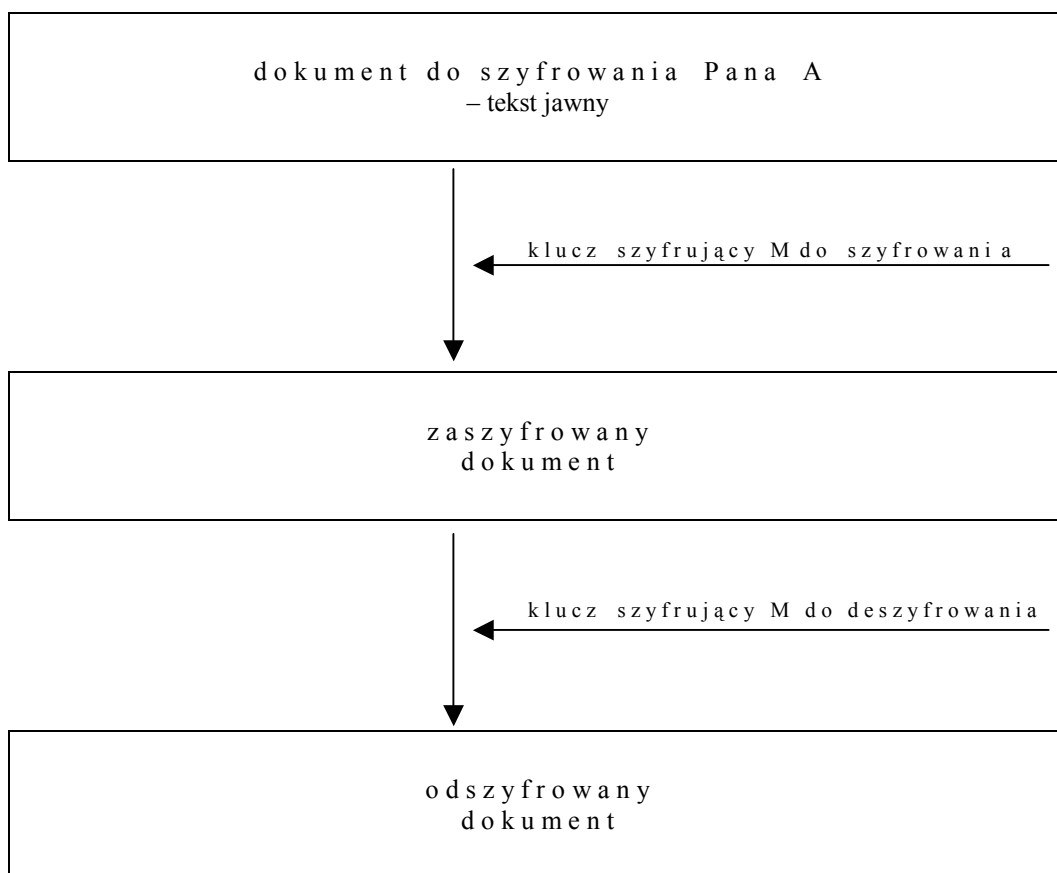
<sup>32</sup> RC2 i RC4 są to algorytmy prawnie strzeżone, wynalezione przez Rona Rivesta, szczegóły algorytmów nie zostały opublikowane. Szerzej Bruce Schneier „Ochrona ...”

<sup>33</sup> Bruce Schneier „Ochrona poczty elektronicznej. Jak chronić prywatność korespondencji w Internecie” Wydawnictwo Naukowo Techniczne. Warszawa. 1996

stuprocentowo bezpieczne, albowiem co do zasady nie zostało udowodnione niełamalność żadnego algorytmu. Niemniej jest jeden wyjątek – algorytm z kluczem jednorazowym. Jest jedynym schematem szyfrującym, w którym można udowodnić, że jest absolutnie nieprzełamywalny. Największą popularnością cieszy się on w środowisku szpiegowskim z uwagi na fakt, że po pierwsze nie wymaga żadnego sprzętu do implementacji i po drugie jest całkowicie bezpieczny. Wymaga on wytworzenia wielu zestawów pasujących do siebie ciągów kluczy szyfrujących. Każdy z tych ciągów składa się z pewnej liczby losowych znaków klucza. Te znaki klucza nie są generowane przez jakiegokolwiek rodzaju kryptograficzny generator klucza, a wybierane za pomocą prawdziwie losowego procesu. Każda strona otrzymuje dopasowany zestaw ciągów. Każdy znak klucza w ciągu jest używany do zaszyfrowania jednego i tylko jednego tekstu jawnego, po czym już nigdy nie zostaje użyty ponownie. Jest to istota nieprzełamywalności klucza, nieprzełamywalności, którą jak w żadnym innym algorytmie można udowodnić. Mimo pewności co do bezpieczeństwa algorytm ten nie jest używany, ponieważ jest niepraktyczny. Liczba kluczy jednorazowych, którą trzeba wygenerować musi być co najmniej równa rozmiarowi tekstu jawnego, a klucze te muszą być zmieniane z upływem czasu. Z tym można pracować w programach użytkowych o małej szybkości transmisji, ale nie w nowoczesnych systemach komunikacyjnych o dużej szybkości.

### ***1.2.3. Schemat działania algorytmów wykorzystywanych w kryptografii symetrycznej w uproszczeniu***

Kryptografia symetryczna opiera się na kluczu pojedynczym, który musi być znany przez zainteresowane strony, a nie może być udostępniony pod żadnym pozorem osobom trzecim. Strony te posługują się tym samym kluczem do zaszyfrowania jak i odszyfrowania wiadomości. Poniżej schemat działania.



**Rys. Schemat działania kryptografii opartej o klucz współdzielony.**

Pan A chcąc przesłać dokument Panu B szyfruje wiadomość przy pomocy klucza szyfrującego M. Pan B chcąc odczytać wiadomość od A deszyfruje ją tym samym kluczem M. Klucz M musi pozostać dla bezpieczeństwa przesyłanych wiadomości w tajemnicy, bowiem kto nie zna klucza nie może odszyfrować wiadomości i poznać treści dokumentu. Mankamentem tego systemu jest to, że trzeba uzgadniać klucz tajny, przechowywać go w bezpiecznym miejscu i współdzielić ze wszystkimi osobami, z którymi będą wymieniać się zabezpieczonymi wiadomościami. Atakując mechanizm zarządzania kluczami osiągnie się znacznie więcej niż przez atak algorytmów. Wynaleziono inny rodzaj kryptografii, gdzie te problemy zostaną wyeliminowane lub zminimalizowane. Jest to kryptografia asymetryczna.

### 1.3.1. Algorytm RSA – istota działania

Algorytmem wykorzystywanym w kryptografii asymetrycznej jest m.in. algorytm RSA. Nazwa pochodzi od pierwszych liter nazwisk autorów: Rona Rivesta, Adi Shamira i Lena Adlemana. Na istotę składa się godny uwagi aspekt matematyczny

i jak zwykle bezpieczeństwo oraz szybkość szyfrowania i deszyfrowania. Z punktu widzenia matematycznego, algorytm RSA oparty jest o liczby pierwsze. Wytworzenie klucza jawnego wymaga pomnożenia dwóch dużych<sup>34</sup> liczb pierwszych, aby uzyskać iloczyn tych liczb. Działanie matematyczne stosunkowo proste. Z dwóch liczb uzyskuje się trzecią. Jednakże uzyskanie klucza prywatnego z klucza jawnego (czyli z tej trzeciej dokładnie te dwie, które były na początku) jest związana z rozłożeniem tego iloczynu na czynniki pierwsze (czyli proces niejako odwrotny). Jeżeli iloczyn jest liczbą wystarczająco dużą, to rozłożenie go na czynniki pierwsze nie jest zadaniem łatwym do wykonania, niemniej możliwym. Kwestią kluczową jest tu nie możliwość, a czas dokonania tej operacji. Oczywiście przy dużych liczbach nie można tego dokonać w sensownym czasie. Chodzi tu o to, aby nawet cała potęga sprzętu i najtęższe w tej dziedzinie umysły nie były w stanie dokonać tego w rozsądnym terminie. Dla zobrazowania sytuacji i przybliżenia problemu dla celów pracy pozwalam sobie na przytoczenie wyliczeń matematycznych, które wskazują hipotetycznie czas, zasoby sprzętowe i koszty omawianej operacji. Pamiętajmy, że są jedynie wartości szacunkowe i hipotetyczne. W rzeczywistości w tak dalekiej przyszłości mogą okazać się absurdem. W tym miejscu winna jestem jeszcze jedną uwagę, mianowicie duża część informatyków posługuje się długościami liczb wyrażonych w bitach. 100 cyfr to ok. 332 bity. Mając to na uwadze, za pomocą poniższej tabeli można dokonać stosownych przeliczeń.

<i>Rok</i>	<i>Liczba cyfr w liczbie</i>							
	<i>100</i>	<i>150</i>	<i>200</i>	<i>250</i>	<i>300</i>	<i>350</i>	<i>400</i>	<i>450</i>

<sup>34</sup> duży w znaczeniu liczby zawierające trzysta i więcej cyfr

<b>1995</b>	740,00	$10^7$	$4x10^{10}$	$2x10^{13}$	$10^{15}$	$10^{17}$	$10^{19}$	$10^{20}$
<b>2000</b>	74,00	$10^6$	$4x10^9$	$2x10^{12}$	$3x10^{14}$	$10^{16}$	$10^{18}$	$10^{19}$
<b>2005</b>	7,40	$10^5$	$4x10^8$	$2x10^{11}$	$3x10^{13}$	$10^{15}$	$10^{17}$	$10^{18}$
<b>2010</b>	0,74	$10^4$	$4x10^7$	$2x10^{10}$	$3x10^{12}$	$2x10^{14}$	$10^{16}$	$10^{17}$
<b>2015</b>	0,07	$10^3$	$4x10^6$	$2x10^9$	$3x10^{11}$	$2x10^{13}$	$10^{15}$	$10^{16}$
<b>2020</b>	0,00	$10^2$	$4x10^5$	$2x10^8$	$3x10^{10}$	$2x10^{12}$	$10^{14}$	$10^{15}$
<b>2025</b>	0,00	10,00	$4x10^4$	$2x10^7$	$3x10^9$	$2x10^{11}$	$10^{13}$	$2x10^{14}$
<b>2030</b>	0,00	1,00	$4x10^3$	$2x10^6$	$3x10^8$	$2x10^{10}$	$10^{12}$	$2x10^{13}$

**Tabela: Koszt rozłożenia liczby na czynniki pierwsze wyrażona w USD<sup>35</sup>**

Przypuszcza się, bowiem nie zostało to nigdy dowiedzione, że bezpieczeństwo algorytmu zależy od trudności rozłożenia dużych liczb na czynniki pierwsze

i że jest to jedyny sposób na złamanie algorytmu. Dlatego ważne jest utrudnienie faktoryzacji czyli rozłożenie na czynniki pierwsze, aby była niemożliwa do wykonania. Zawsze jednak wraz z rozwojem techniki i narodzinami mózgu matematyczno-informatycznego możliwe jest odkrycie innego sposobu złamania RSA.

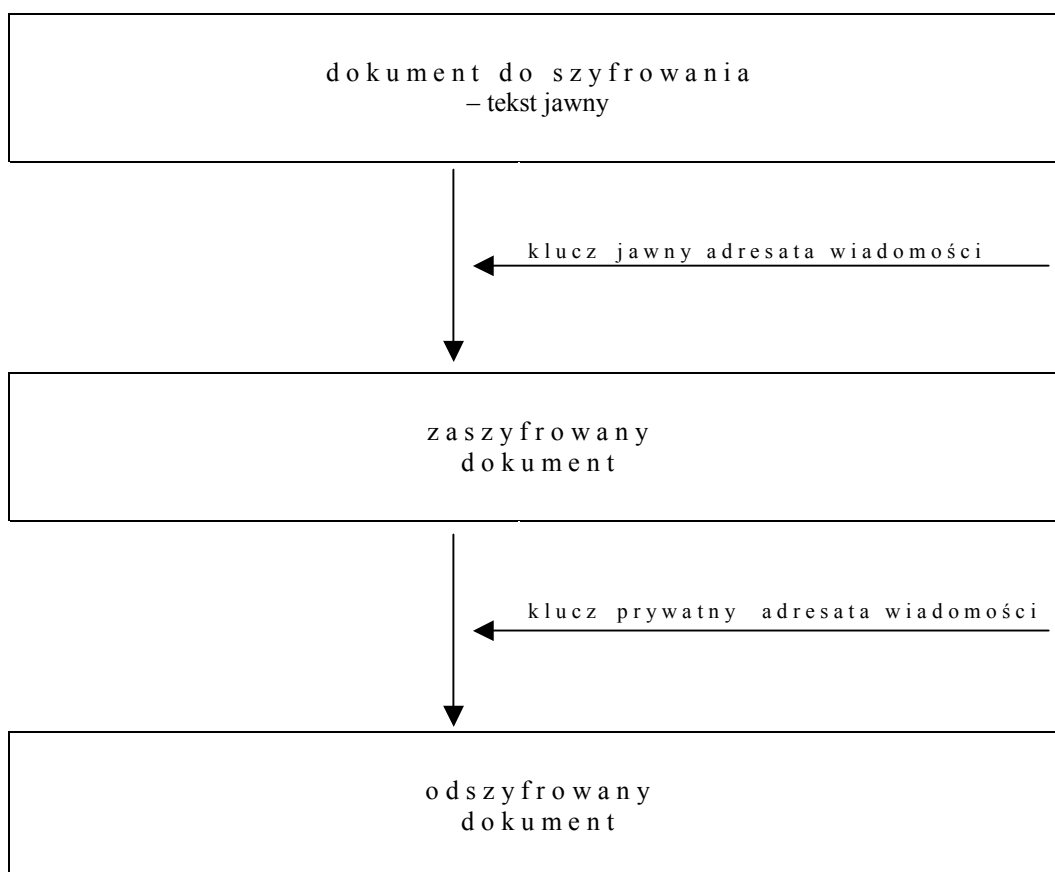
Dopóki nie wiemy nic o nowej metodzie przyjrzyjmy się wynikom tabeli. Łatwo można dojść do wniosku, że liczby 512 bitowe są mało bezpieczne do stosowania kryptografii z kluczem jawnym, oczywiście to wszystko zależy od tajności

i stopnia poufności wiadomości. Do wiadomości o wysokim stopniu poufności zalecałabym stosowanie 1024 bitowej liczby do długości klucza tak jak w klasie wojskowej. Następną sprawą techniczną jest generowanie tych par kluczy to kwestia ich generacji i używania programów do tego.

### ***1.3.2. Schemat działania algorytmów wykorzystywanych w kryptografii asymetrycznej***

Kryptografia z kluczem jawnym oparta jest o parę kluczy jawny (publiczny) i tajny (prywatny). Konkretny klucz jawny pasuje do konkretnego klucza

prywatnego. Nie można wyliczyć jednego klucza na podstawie drugiego. Klucz jawny jest kluczem publicznym, czyli powszechnie dostępnym. W związku z czym każdy może otrzymać jego kopię. W interesie posiadacza pary kluczy jest aby jak najwięcej podmiotów posiadało kopię jego klucza publicznego. Osoba A (czyli podmiot zainteresowany korespondencją z B) chcąc wysłać zaszyfrowaną wiadomość B sięga do jego klucza publicznego, aby tym kluczem zaszyfrować dla niego informację. B za pomocą swego klucza prywatnego może ją odszyfrować. Nawet przechwycona wiadomość nie jest czytelna dla nieuczciwego C, ponieważ nie posiada on klucza prywatnego B. Może posiadać klucz publiczny B, ale nie pomoże to w deszyfracji wiadomości. W ogólnym skrócie została przedstawiona istota kryptografii z kluczem jawnym. W rzeczywistości jest to nieco bardziej skomplikowany proces. Poniżej schemat działania w ujęciu uproszczonym.

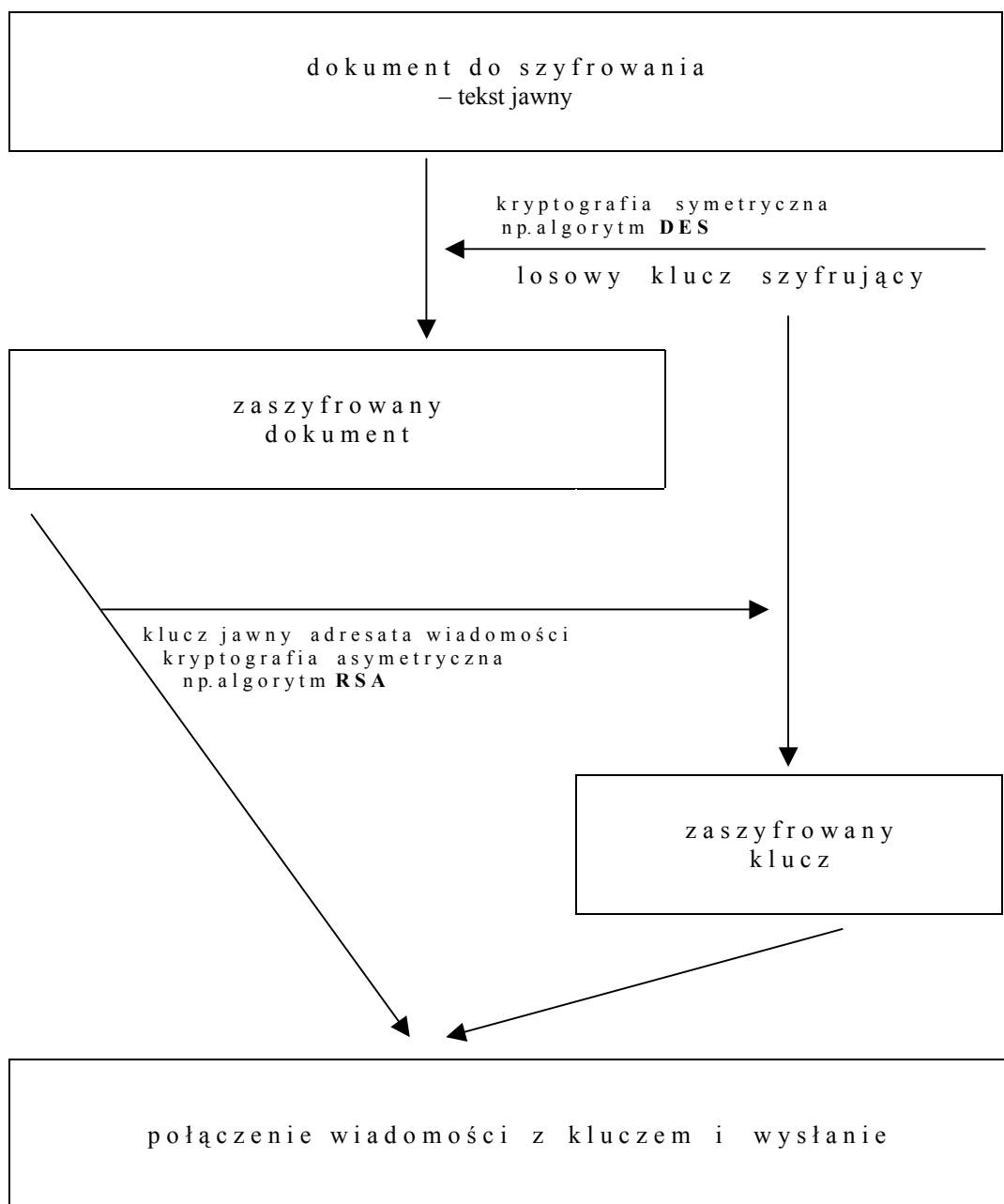


**Rys. Schemat działania algorytmu z kluczem jawnym w ujęciu uproszczonym**

<sup>35</sup> Bruce Schneier „Ochrona ...

Szyfrowanie z kluczem jawnym jest niewygodne i skomplikowane. Nie używa się jej do szyfrowania wszystkich wiadomości, bowiem trwało to by zbyt długo. Kryptografia z kluczem jawnym wykorzystywana jest do zarządzania kluczami.

W rzeczywistości łączy się działanie algorytmów wykorzystując kryptografię symetryczną i asymetryczną. Na przykładzie wygląda to tak:



Rys. Połączenie działania algorytmu stosującego kryptografię symetryczną i algorytmu stosującego kryptografię asymetryczną.

## *Rozdział 2*

---

### *Uwierzytelnianie*

---

#### *2.1. Zagadnienia wstępne*

---

Ważne jest dla adresata, że dokument, który do niego przychodzi drogą elektroniczną pochodzi od osoby, która podaje się za nadawcę tego dokumentu. Uwierzytelnienie nadawcy odbywa się za sprawą koncepcji podpisu cyfrowego. Z technicznego punktu widzenia jest to sekwencja bitów dołączona do dokumentu cyfrowego, na podstawie którego można potwierdzić autentyczność nadawcy. Wbrew pozorom i odmiennie niż w przypadku podpisu odręcznego dla każdego dokumentu podpis cyfrowy jest inny. Dzieje się to z prostej przyczyny, że zachodzą inne procesy niż przy zwykłym podpisywaniu dokumentu.

Podpis cyfrowy spełnia następujące kryteria:

- a) niepodrabialny, nikt nie może wygenerować oryginalnego podpisu cyfrowego jak tylko nadawca,
- b) autentyczny, pochodzi od osoby, która podaje się za nadawcę,
- c) nie może być użyty jeszcze raz, podpis cyfrowy jest używany tylko raz i za każdym razem jest inny,
- d) niezmienialny, po podpisaniu nie można zmienić podpisu, w przeciwnym wypadku traci ważność,
- e) nie można się go wyprzeć, prawidłowo podpisany dokument stanowi dowód, że pochodzi on od nadawcy, a nadawca nie może się go wyprzeć.

---

#### *2.2. Jednokierunkowa funkcja skrótu*

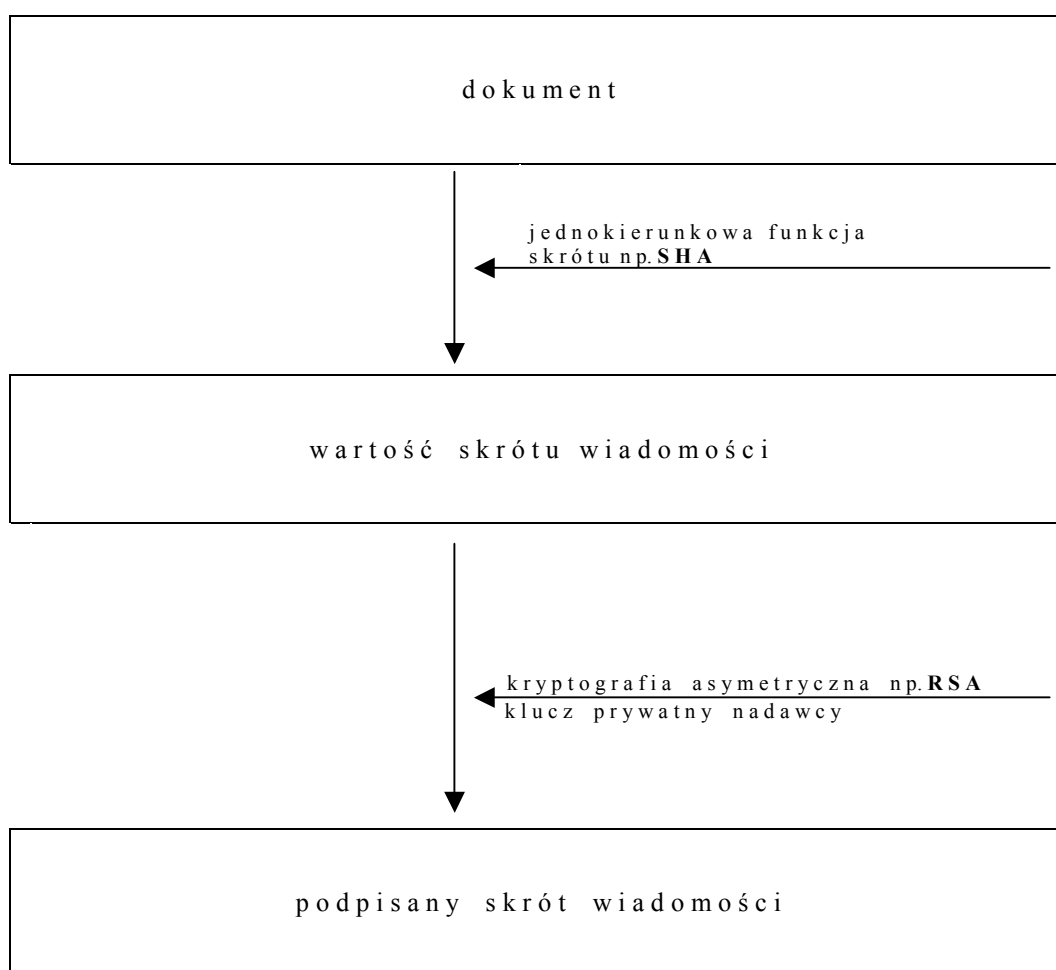
---

Jednokierunkowa funkcja skrótu (inaczej skrót, funkcja ściągająca, funkcja kompresująca, kryptograficzna suma kontrolna, kontrola spójności danych, kod spójności danych, kod wykrywania ingerencji, kod uwierzytelniania wiadomości, kod uwierzytelniania danych) jest to specjalna funkcja kryptograficzna do przekształcania wiadomości o dowolnych rozmiarach w niezrozumiały tekst. Nie jest to szyfrowanie, bowiem poddanie wiadomości tej operacji „niszczy” wiadomość a

działanie przeciwne nie jest możliwe. Ponadto funkcja nie korzysta z klucza. Te właściwości sprawiają, że jest ona wykorzystywana do identyfikacji wiadomości.

W wyniku poddania wiadomości działaniu tej funkcji tworzy się skrót wiadomości. Jest on wystarczająco długi, dzięki temu szansa na to, aby dwa różne dokumenty dały ten sam skrót jest dosłownie nikła. Następnie wykorzystuje się algorytm podpisów cyfrowych kryptografii z kluczem jawnym i klucz prywatny do podpisania skrótu wiadomości. Poniżej schemat obrazujący ten proces.

Jest wiele algorytmów wykorzystywanych jako jednokierunkowa funkcja skrótu np. MD5, SHA, MD2, MD4, Snefru, N-Hash i RIPE MD itp.



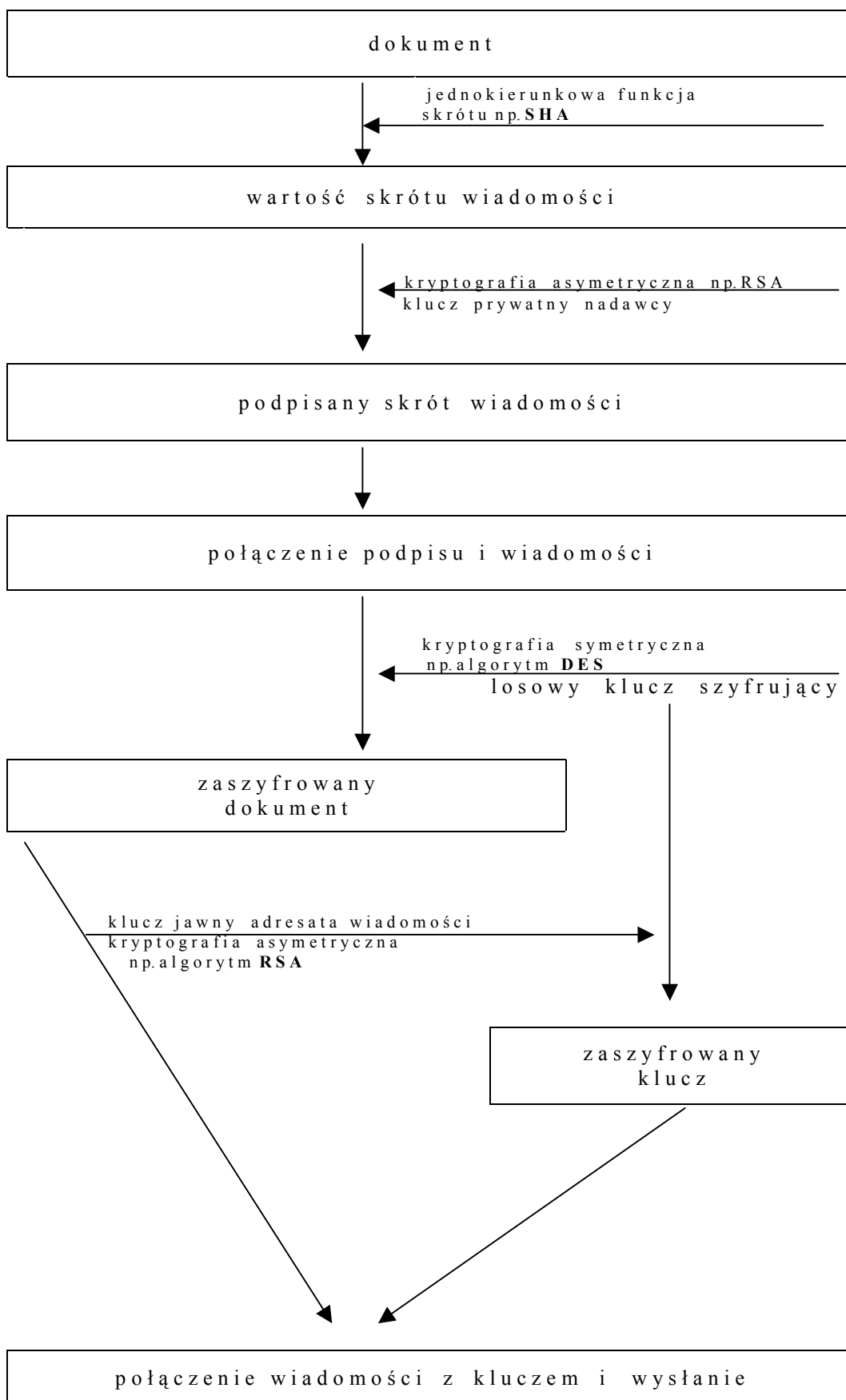
**Rys. Podpis cyfrowy**

Szyfrowanie zapewnia bezpieczeństwo i poufność korespondencji, a podpisy cyfrowe dają uwierzytelnienie nadawcy. Połączenie wszystkich tych procesów

szyfrowania i tworzenia podpisów cyfrowych daje dopiero pożądane bezpieczeństwo czyli

- a) poufność wiadomości – mamy pewność, że nikt nie ma wglądu do przesyłanych dokumentów, nie może zapoznać się z ich treścią,
- b) nienaruszalność danych – nikt nie może zmieniać, poprawiać, ani w żaden inny sposób naruszać treści tych wiadomości w sposób, który nie zostanie zauważony,
- c) pewność co do tego, od kogo pochodzą dokumenty, nikt nie może się wyprzeć tego, że to on jest nadawcą.

Połączenie tych procesów obrazuje poniższy schemat.



Rys. Podpisywanie i szyfrowanie

Za pomocą specjalnej matematycznej funkcji zwanej jednokierunkową funkcją skrótu tworzy się skrót tej wiadomości. Następnie wykorzystuje się algorytm podpisów cyfrowych kryptografii z kluczem jawnym jak np. RSA i klucz prywatny do podpisania skrótu wiadomości. Należy połączyć wiadomość i podpis cyfrowy. W celu podpisania tej wiadomości należy wygenerować klucz szyfrujący za pomocą algorytmu konwencjonalnego jak np. DES. W celu zaszyfrowania klucza pobiera się klucz jawny odbiorcy wiadomości i szyfruje się, po czym łączy wiadomość z zaszyfrowanym kluczem i w ten sposób końcowa zabezpieczoną wiadomość można przesłać nadawcy.

Nadawca, aby odczytać rozdziela zaszyfrowaną wiadomość od zaszyfrowanego klucza losowego, deszyfruje losowy klucz za pomocą algorytmu z kluczem jawnym i swojego klucza prywatnego. Deszyfruje wiadomość za pomocą algorytmu konwencjonalnego i odszyfrowanego klucza. Oddziela wiadomość od podpisu i za pomocą jednokierunkowej funkcji skrótu oblicza wartość skrótu wiadomości. Pobiera klucz jawny nadawcy i deszyfruje podpis za pomocą algorytmu podpisów cyfrowych z kluczem jawnym i klucza jawnego nadawcy. Porównuje odszyfrowany podpis nadawcy z wartością skrótu wiadomości. Jeżeli są takie same to podpis uznaje i akceptuje wiadomość jako oryginalną.

W przypadku algorytmów wykorzystywanych przez kryptografię z kluczem pojedynczym zostały omówione wady i zalety. Jeśli natomiast chodzi o kryptografię asymetryczną problem został celowo pominięty. Z uwagi na złożoność i ważność zagadnienia postanowiłam poświęcić temu oddzielny rozdział.

W ogromie użytkowników uczestniczących w wymianie elektronicznej, w obliczu ogromnego postępu technologicznego, żeby nie narazić się na oszustwa, zachodzi potrzeba poddania niejako kontroli kluczy jawnych użytkowników, neutralnego zabezpieczenia zarządzania kluczami jawnymi i potwierdzeniu, że dany klucz należy do danego podmiotu i nie jest używany przez żaden inny podmiot. Do tego potrzebny jest ktoś, kto będzie zajmował się tym i tylko tym przez cały czas – Zaufana Trzecia Strona.

Strony wymiany elektronicznej dążą do uzyskania certyfikatu – czyli swego rodzaju zaświadczenia potwierdzającego identyfikację danej osoby i zawierającego jej klucz publiczny. Zaświadczenie to jest podpisywane przez specjalny organ do tego upoważniony, który wydaje certyfikaty. Od stopnia zaufania tego organu zależy

czy będziemy mieli zaufanie do wydanego przez niego certyfikatu, że jest dostatecznie sprawdzony i że jest poprawny.

### *2.3. Polityka certyfikacyjna i proces certyfikacji*

---

Różne programy mają różne pojęcie zaufania i reprezentują różną politykę certyfikacyjną. I choć jest kilka systemów godnych uwagi jak np. PEM, PGP, to tym razem przedstawię politykę certyfikacyjną popieraną przez polski ZUS<sup>36</sup>. Zakład Ubezpieczeń Społecznych corocznie przyjmuje interesantów, którzy składają papierowe dokumenty z różnymi rozliczeniami. Złożenie tych dokumentów wymaga osobistego<sup>37</sup> stawienia się w placówce ZUS. W tym celu zatrudniana jest olbrzymia ilość urzędników do przyjmowania i przetwarzania tych dokumentów. Świat zmierza

w kierunku usprawniania prostych i jednocześnie ważnych czynności w życiu codziennym. ZUS zdaje się, że chce sprostać wymaganiom stawianym przez nowo powstające społeczeństwo informatycznie i usprawnić pracę swych jednostek stosując elektroniczne rozwiązania w przesyłaniu dokumentów. Współpraca w tym zakresie została zaproponowana najbardziej przedsiębiorczej grupie, którą obejmuje obowiązek ubezpieczenia społecznego – płatnikom<sup>38</sup>. Oczywiście propozycja w właściwej tego słowa treści dotyczy płatników nie objętych obowiązkiem elektronicznego rozliczania z ZUS. Na płatników rozliczających składki za ponad 20 ubezpieczonych nałożony został obowiązek<sup>39</sup> elektronicznego przesyłania dokumentów.

---

<sup>36</sup> źródłem informacji była strona <http://www.zus.gov.pl>

<sup>37</sup> osobistego w sensie fizycznego osoby zainteresowanej, pełnomocnika lub osoby, która te dokumenty przyniesie do zus-u

<sup>38</sup> płatnik – podmioty wymienione w art. 4 ustawy z dnia 13.10.1998r o systemie ubezpieczeń społecznych (Dz. U. 1998r, Nr 137, poz. 887 z późniejszymi zmianami)

<sup>39</sup> obowiązek ten wynika z ustawy z dnia 11.01.2001r o zmianie ustawy o systemie ubezpieczeń społecznych oraz niektórych innych ustaw (Dz.U. 2001, Nr 8), zostało również wydane rozporządzenie z dnia 03.07.2001r w sprawie warunków, jakie muszą spełniać płatnicy składek przekazujący dokumenty ubezpieczeniowe w formie dokumentu elektronicznego poprzez teletransmisję danych.

### ***2.3.1. Podmioty biorące udział w elektronicznej wymianie dokumentów i ich obowiązki***

Podmiotami biorącymi udział w elektronicznej wymianie dokumentów są ZUS i płatnicy. Trzecią stroną jest Centrum Certyfikacji.

Płatnicy zanim przystąpią do elektronicznej wymiany dokumentów muszą sprostać następującym wymogom:

- a) muszą zaopatrzyć się w odpowiednie oprogramowanie tj. Program Płatnika<sup>40</sup> i Płatnik – Przekaz Elektroniczny<sup>41</sup>,
- b) posiadać komputer zgodny z wymogami określonymi w dokumentacji<sup>42</sup>, z systemem Windows 95 lub Windows NT Workstation wyposażony w modem 28.8 kbps,
- c) posiadać konto internetowe,
- d) zarejestrować się w Punkcie Rejestracji w ZUS ie i
- e) uzyskać certyfikat dla swojego klucza publicznego z Centrum Certyfikacji.

ZUS uczestniczy poprzez swoje jednostki organizacyjne, jakimi są Punkty Rejestracji zlokalizowane w jednostkach terenowych ZUS-u. Punkty Rejestracji zajmują się przyjmowaniem n/w wniosków i wydawaniem potwierdzeń tych operacji:

- a) o rejestrację nowych płatników, którzy zgłaszają chęć przystąpienia do elektronicznej wymiany dokumentów,
- b) o modyfikacje danych identyfikacyjnych płatnika,
- c) unieważnienie rejestracji płatnika,
- d) unieważnienie certyfikatu klucza publicznego płatnika z powodu kompromitacji klucza prywatnego

W tym celu niezbędne jest sprawdzanie tożsamości płatników bądź osób przez niego upoważnionych.

Centrum Certyfikacji to usługodawca certyfikacyjny, którego funkcję pełni Spółka z o.o. UNIZETO ze Szczecina. Jest ona odpowiedzialna za administrowanie certyfikatami klucza publicznego uczestników elektronicznej wymiany dokumentów a w szczególności:

- a) wydawanie certyfikatów klucza publicznego i wystawianie potwierdzenia,

---

<sup>40</sup> szczegółowe informacje <http://www.zus.gov.pl>

<sup>41</sup> ibidem

- b) unieważnianie certyfikatów i wystawianie potwierdzenia,
  - c) odnawianie certyfikatów i wystawianie potwierdzenia,
  - d) udostępnianie swego certyfikatu klucza publicznego,
  - e) ogłaszanie listy certyfikatów unieważnionych (CRL),
  - f) udostępnianie na żądanie pełnej lub częściowej listy certyfikatów unieważnionych (ZRL),
  - g) weryfikowanie wiarygodności certyfikatów klucza publicznego.
- Wymiana informacji między Centrum Certyfikacji a płatnikiem lub jednostką organizacyjną ZUS następuje tylko na drodze elektronicznej.

### **2.3.2. Proces uzyskania certyfikatu**

W dużym skrócie<sup>43</sup> proces uzyskania prowadzący do uzyskania certyfikatu wygląda następująco:

1. zaopatrzenie się w odpowiednie oprogramowanie, sprzęt i konto mailowe,
2. wygenerowanie wniosku o rejestrację aplikacji Płatnik – Przekaz Elektroniczny, w tym momencie generuje się para kluczy, z której jeden – publiczny musi uzyskać certyfikat z CC<sup>44</sup>, aby płatnik mógł się elektronicznie rozliczać,
3. rejestracja tego wniosku w PR<sup>45</sup> w ZUS-ie i uzyskanie elektronicznego i papierowego potwierdzenia tej operacji,
4. zarejestrowanie elektronicznego potwierdzenia rejestracji z PR w aplikacji Płatnik – Przekaz Elektroniczny,
5. wygenerowanie wniosku o wydanie certyfikatu do CC,
6. uzyskanie certyfikatu dla swojego klucza publicznego z CC,

---

<sup>42</sup> chodzi o instrukcje obsługi programów Program Płatnika i Płatnik – Przekaz Elektroniczny dostępnych razem z instrukcjami ze strony <http://pp.zus.gov.pl>

<sup>43</sup> szczególnie o tym procesie ze strony <http://www.zus.gov.pl>

<sup>44</sup> CC – Centrum Certyfikacji

<sup>45</sup> PR – Punkt Rejestracji

BEGIN CERTIFICATE-----  
MIIE7zCCA9egAwIBAgIDBZKRMA0GCSqGSIb3DQEBBQUAMIGmMQswCQYDVQQGEwJQ  
TDEbMBkGA1UECBMSWmfjaG9kbmlvcG9tb3Jza2llMREwDwYDVQQHEwhTemN6ZWNP  
bjEnMCUGA1UEChMeWmF1ZmFuYSBUcnp1Y2lhIFN0cm9uYSBVbml6ZXRvMSQwIgdYD  
VQQLExtDZW50cnVtIENlcnR5ZmlrYWwqaSBDQS1aRVexGDAWBgnVBAMTD1VOSVpF  
VE9UVFBDOVpFVzAeFw0wMTA5MTYwMDAwMDBaFw0wMjA5MzAyMzU5NTlaMH4xCzAJ  
BgNVBAYTAIBMMRQwEgYDVQQIEwtYXpvd2llY2tpZTERMA8GA1UEBxMIV2Fyc3ph  
d2ExDDAKBgNVBAoTA1pVUzEIMCMGA1UECXMtT3Nyb2RlayBQcnpldHdhcnphbmlh  
IERhbnljaDERMA8GA1UEAxYlUjBfMV9PT1AwgZ0wDQYJKoZIhvcNAQEBBQADgYsA  
MIGHAaGBALcivSc/BUFY74yXqssbP7DhMlqgryc+cF+dLu0IiiKge2ZXHllaFDIS  
MY4sXIKD1C3JDJ1EeZ2DUwZk5f386RxF2iDnP/RrJ4tasiWzXbfJ69o9miuQ+41  
8eYU6fJd2ImmQ7+1CmL4qv3QvWXk3QpjOyu6g5GtPxU1w9yRD64jAgEDo4IB0TCC  
Ac0wMgYDVR0QAQH/BCgwJoARGA8yMDAxMDkxNjAwMDAwMFqBERgPMjAwMjA5MTU  
yMzU5NTlaMB0GA1UdDgQWBBSU5v8EleCK9mQLWsr3MZC2fYKVZDAOBgNVHQ8BAf8E  
BAMCBaAwQQYDVR0gBDowOAYEKwYBAjAwBgECFitodHRwOi8vd3d3LmNjLnVuZXQu  
cGwvcMvwb3p5dG9yaXVtL3BvbGl0eWthMBoGA1UdEQQTMBGBD2prb2NoYW5AdW51  
dC5wbDAYBgNVHRIEETAPgQ1jYXpld0B1bmV0LnBsMDgGA1UdIwEB/wQuMCyAFO/g  
+tR+EqMmRF53a4eyJl7qW/YXoRgBD1VOSVpFVE9UVFBDOVpFV4IBCTAPBgNVHRME  
CDAGAQAQAeAMIGVBBgNVHR8EgY0wYowQ6AuoCyBKmh0dHA6Ly93d3cuY2MudW51  
dC5wbCxmHA6Ly9mdHAuY2MudW5ldC5wbKIRgQ9VTklaRVRPVFRQQ0FaRVcwQ6Au  
oCyBKmh0dHA6Ly93d3cuY2EudW5ldC5wbCxmHA6Ly9mdHAuY2EudW5ldC5wbKIR  
gQ9VTklaRVRPVFRQQ0FaRVcwDAYEZysHAQQEAwIFIDANBgkqhkiG9w0BAQUFAAOC  
AQEAQTUNUFF+hovLij2Z1noXyENFWSEVlh8mI4OagzBDBYDy7P4rm+oZ2AFNtbU4  
uL6NLpxMPQTy2RT/rdQuItfs8GxPeJv64dhxfVT2c3VxxhzAzKHdQ+XXGHO3hc  
QO4zfghyPDTK7ICarMMmrvUwdX+0yRiurmX75D2Onocxt4TCONZo8Jsl5yYn5R/N  
S4X9fNYphOhirru99ApzbY1TMePCNOF9JCVyQDIIsF/y43JggHHj3sI5yJurSywN  
nc1DccFID+PdTtakgLOEIFuzdzgTn2jw6pLXMKslRDwNc1SyIsC6+Uh2ymrVNDId  
67zZqltR4zay2NB3CT42ukq0hQ== -----END CERTIFICATE-----

**Rys. Zaszyfrowany certyfikat**

7. zarejestrowanie certyfikatu w aplikacji Płatnik – Przekaz Elektroniczny, od tej pory płatnik może elektronicznie podpisywać swoje dokumenty.

## Zakończenie

---

Współczesna epoka to epoka społeczeństwa informatycznego, którego częścią stajemy się albo z wyboru, albo za sprawą nakładanych na nas obowiązków. W tej epoce nie tylko w Polsce, ale i na świecie wciąż jedyną nie tyle znaną, co wykorzystywaną metodą generowania podpisu elektronicznego jest metoda kryptograficzna. To jej podporządkowany jest aparat administracyjny w poszczególnych regulacjach i przepisy prawne dotyczące administracyjno – prawnych aspektów podpisu elektronicznego.

Przemierzając materiał zawarty w pracy, porównując różne systemy prawne można dojść do określonych wniosków.

1. Podpis elektroniczny o odpowiednim stopniu zabezpieczenia<sup>46</sup> jest praktycznie nie do podrobienia. Podpis elektroniczny wbrew pozorom i ogólnemu pogładowi na podpis nie jest stały, a za każdym razem inny. Dla każdej wiadomości jest generowany inny podpis i nie jest on taki sam jak ten wygenerowany przed chwilą dla innej wiadomości. Wynika to z zastosowania techniki, metody generowania podpisu i zastosowania algorytmów z kluczem pojedynczym i publicznym oraz jednokierunkowej funkcji skrótu. A zatem można powiedzieć, że jest bezpieczniejszy niż podpis odręczny. Na bezpieczeństwo składają się ten i kilka innych aspektów. Jednakże w tym stwierdzeniu też można doszukać się kilku „ale”, kilku „pod warunkiem”.
2. Przede wszystkim trzeba mieć świadomość, że zabezpieczenie dokumentu podpisem elektronicznym dotyczy tylko danego dokumentu, tylko danej wiadomości,  
a nie dotyczy komputera, za pomocą którego łączymy się z siecią i wysyłamy podpisaną wiadomość. Komputer, z którego wychodzimy na zewnątrz tj. do sieci musi być zabezpieczony różnymi programami antywirusowymi, różnej klasy firewall'ami i innymi środkami. Ponadto niezbędne jest zabezpieczenie klucza prywatnego. Najlepiej ważne dane i klucz przechowywać na innym komputerze nie podłączonym do sieci. Niezastosowanie się chociażby do jednego z

---

<sup>46</sup> nie dotyczy zwykłego podpisu elektronicznego

powyższych zaleceń może skutkować zniwelowaniem zabezpieczenia dokumentu podpisem elektronicznym<sup>47</sup>. W wieku technologii cyfrowych, gdzie nawet termin „wojna” jest na nowo definiowany, odpowiedzialność podpisujących jest bardzo duża, z której nie zawsze można zdawać sobie sprawę.

3. Cel, dla którego zostały stworzone regulacje dotyczące podpisu elektronicznego zostanie osiągnięty, o ile podpisujący będą zachowywać się odpowiedzialnie. Tylko w takich warunkach swobodnie może rozwijać się bezpieczny, elektroniczny obrót prawny.

---

<sup>47</sup> dzieje się tak w sytuacji, kiedy nie został zabezpieczony komputer, co pozwoliło na wgląd w niego osobie nieuprawnionej. Nie byłoby to jeszcze najgorsze, gdyby nie obecność klucza prywatnego na tym komputerze. Złamanie hasła do klucza nie stanowi problemu. Problem stanowi złamanie podpisu elektronicznego, a konkretniej przeczytanie wiadomości, która została asygnowana podpisem elektronicznym o odpowiednim poziomie zabezpieczenia.

# *Bibliografia*

---

## *Dokumenty i materiały*

---

1. Dyrektywa 97/7/EC Parlamentu Europejskiego i Rady z 20 maja 1997r w sprawie ochrony konsumentów w odniesieniu do umów zawieranych na odległość,
2. Dyrektywa 1999/93/EC Komisji Europejskiej z 13.12.1999r w sprawie ram Wspólnotowych dla podpisu elektronicznego,
3. Gesetz zur digitalen Signatur (Signaturgesetz – SigG) vom 22.07.1997, verkündet als Artikel 3 des „Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - luKDG)“
4. Verordnung zur digitalen Signatur (Signaturverordnung – SigV in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997
5. Begründung zur Verordnung zur digitalen Signatur (in der Fassung des Beschlusses der Bundesregierung vom 8.10.1997),
6. Entwurf – MaBnahmenkatalog für digitale Signaturen – auf Grundlage von SigG und SigV, (Stand 18.11.1997, Version 1.0)
7. Ustawa polska o podpisie elektronicznym z 27.07.2001r,
8. Ustawa modelowa UNCITRAL (Model Law on Electronic Commerce) dotycząca zagadnień prawnych związanych z Elektronicznym Przekazem Danych (Electronic Data Interchange w skrócie EDI) i pokrewnych środków komunikacyjnych,
9. Projekt ustawy modelowej UNCITRAL o podpisach elektronicznych Polska Akademia Umiejętności i „Kwartalnik Prawa Prywatnego” Rok X:2001, z.1
10. Sprawozdanie Międzyresortowego Zespołu do spraw handlu metodami elektronicznymi. Analiza obowiązującego stanu prawnego z punktu widzenia możliwości wykorzystania istniejących regulacji prawnych w transakcjach zawieranych metodami elektronicznymi oraz proponowane kierunki rozwiązań prawnych. Dokument rządowy przyjęty przez Rade Ministrów w dniu 11.07.2000r [http://www.mg.gov.pl/struktur/hand\\_usl/sprawo.htm](http://www.mg.gov.pl/struktur/hand_usl/sprawo.htm),

11. Wytyczne w sprawie kryptografii (Guidelines for Cryptography Policy) – dokument OECD (Organization for Economic Co-operation and Development) z 27.03.1997

---

*Opracowania książkowe*

---

12. Barta J., Markiewicz R. „*Internet a Prawo*” Kraków 1998r
13. Barta J., Markiewicz R. „*Główne problemy prawa komputerowego*” Warszawa 1993r,
14. Bieniek Gerard, Ciepla Helena, Dmowski Stanisław, Gudowski Jacek, Kołakowski Krzysztof, Sychowicz Marek, Wiśniewski Tadeusz, Żuławska Czesława „*Komentarz do kodeksu cywilnego. Księga trzecia – zobowiązania*” Warszawa 1999,
15. Dmowski Stanisław, Rudnicki Stanisław „*Komentarz do kodeksu cywilnego. Księga pierwsza – część ogólna*” Warszawa 1999,
16. Kocot W. „*Zawieranie umów sprzedaży według Konwencji Wiedeńskiej*” Warszawa 1998r,
17. Parker T. „*TCP/IP*” 1997,
18. Schneier Bruce „*Ochrona poczty elektronicznej. Jak chronić prywatność korespondencji w sieci Internet?*”
19. praca zbiorowa pod redakcją Stokłosa Janusza., autorzy: Darłowski W., Lipski A., Janicka – Lipska I., Ochnio G., Kóska A., Szymański W., „*Ochrona danych w systemach komputerowych. Ćwiczenia laboratoryjne*” Poznań 1997r

---

*Artykuły*

---

20. Abram Henryk i Kwiecień Tomasz „*Wymagania dla nowo powstających systemów electronic commerce*”  
[http://www.sun.com.pl/fd/journal/sj5/sj\\_w\\_99.rtf](http://www.sun.com.pl/fd/journal/sj5/sj_w_99.rtf)
21. Barta Janusz, Markiewicz Ryszard „*Delikt w cyberprzestrzeni*” Rzeczpospolita, 1998r, Nr 83,
22. Barta Janusz, Markiewicz Ryszard „*Jak nie wpaść w sieci komputerowe*” Rzeczpospolita, 1997r, Nr 264

23. Barta Janusz, Markiewicz Ryszard „*Kryptografia czyli internetowe być albo nie być*” <http://arch.rp.pl/a/rz/1999/12/19991210/199912100063.html> ,
24. Barta Janusz, Markiewicz Ryszard „*Prawo cyberprzestrzeni i stare konwencje*” <http://arch.rp.pl/a/rz/1997/11/19971115/199711150007.html>
25. Barta Janusz, Markiewicz Ryszard „*Prawo sieci informatycznych*” cykl artykułów  
[http://www.rzeczpospolita.pl/gazeta/wydanie\\_970325/prawo/prawo\\_a\\_3.html](http://www.rzeczpospolita.pl/gazeta/wydanie_970325/prawo/prawo_a_3.html) ,  
[http://www.rzeczpospolita.pl/gazeta/wydanie\\_970327/prawo/prawo\\_a\\_4.html](http://www.rzeczpospolita.pl/gazeta/wydanie_970327/prawo/prawo_a_4.html) ,  
[http://www.rzeczpospolita.pl/gazeta/wydanie\\_970328/prawo/prawo\\_a\\_5.html](http://www.rzeczpospolita.pl/gazeta/wydanie_970328/prawo/prawo_a_5.html) ,
26. Barta Janusz, Markiewicz Ryszard „*Sieć jako siatka na zakupy*”  
[http://www.sun.com.pl/fd/journal/sj5/sj\\_w\\_99.rtf](http://www.sun.com.pl/fd/journal/sj5/sj_w_99.rtf),
27. Barta Janusz, Markiewicz Ryszard „*Transakcje, które biegną po łączach*”  
Rzeczpospolita 1998r, Nr 85,
28. Barta Janusz, Markiewicz Ryszard „*Twardy orzech do zgryzienia*”  
Rzeczpospolita 1998r, Nr 81,
29. Barta Janusz, Markiewicz Ryszard „*Wielość w jednym*” Rzeczpospolita, 1997r,  
Nr 269,
30. Bernat Artur „*Pretty Good Privacy wersja 2.6.2. Wykład wprowadzający w obsługę pakietu wymiany informacji kodowanej za pomocą poczty elektronicznej o nazwie PGP*”,
31. Chmura Radosław, Włodarczyk Wojciech „*Internet – problemy prawne*”  
<http://eber.kul.lublin.pl/~marka-r/publikac/internet2.html> ,
32. Dudek Sebastian „*Aukcje w Internecie. Sieć handlowa*” Gazeta prawna z 22-24 września 2000r,
33. Gamdzyk Przemysław „*Potrzebna, ale nie najważniejsza*”  
[http://www.computerworld.com.pl/online/2000/16/numer/Potrzebna\\_ale\\_nie\\_najwazniejsza.asp](http://www.computerworld.com.pl/online/2000/16/numer/Potrzebna_ale_nie_najwazniejsza.asp),
34. Izdebski Hubert „*Gospodarka elektroniczna – podstawowe zagadnienia prawne*”  
<http://www.teleforum.pl/0078/14.html>,
35. Jadczyk Adam „*Amerykański Kongres przyjął ustawę o podpisie elektronicznym*”  
<http://www.computerworld.com.pl/wiadomości/archiwum/2/5/2599.asp>,
36. Kaczor Jacek „*Nazwisko i podpis*” Gazeta prawna z 2-3 sierpnia 2000r,

37. Konarski Xawery „*Internet i prawo. Prawo cywilne, a Internet*”  
<http://biznesnet.pl/index.phtml?pg=ebiz&a=455> ,
38. Konrad Mariusz „*Regulacje wspólnotowe dotyczące Internetu*”  
<http://www.kondrat.pl/artykuly/regulacje.html> ,
39. Kondrat Mariusz „*Handel elektroniczny – regulacje europejskie*”  
<http://www.kondrat.pl/e-handel/> ,
40. Konieczna Anna „*Dokument elektroniczny – konieczność*”  
<http://www.landwellglobal.com/pl/pol/insights/articles/june2000.html> ,
41. Krawczyk Tomasz Ludwik „*Podpis e-lektroniczny. Przepisy Unii Europejskiej*”  
<http://www.emarketing.pl/index.phtml?s=0&p=0&k=298>, (2000.10.31)
42. Krawczyk Tomasz Ludwik „*Podpis elektroniczny*”  
<http://www.qra.nasze.pl/epodpis.html>, (2000.10.31),
43. Kruschewski Rafał „*Digitalme: ja wiem, co Ty wiesz*”  
[http://www.sun.com.pl/fd/journal/sj5/sj\\_w\\_99.rtf](http://www.sun.com.pl/fd/journal/sj5/sj_w_99.rtf),
44. M.P. „*Podpis elektroniczny później*” Rzeczpospolita z 4.11.2000r  
[http://www.rp.pl/gazeta/wydanie\\_001104/ekonomia/ekonomia\\_a\\_9.html](http://www.rp.pl/gazeta/wydanie_001104/ekonomia/ekonomia_a_9.html),
45. Możejko Eugeniusz „*Przyszłość w gospodarce elektronicznej*” Gazeta prawna z 18-20 sierpnia 2000r,
46. Obuchowicz Maciej „*Amerykański prezydent podpisał ustawę o podpisie elektronicznym*”  
<http://www.computerworld.com.pl/wiadomości/archiwum/2/6/2653.asp>
47. Okoń Zbigniew „*Kiedy podpis elektroniczny*”  
<http://www.value.hg.pl/lis00/lis00art1.html>
48. Okoń Zbigniew „*Nowe prawa wirtualnego konsumenta*”  
<http://www.internetstandard.com.pl/teksty.asp?katid=3&fr=1&tekstid=13> ,
49. Pietryga Tomasz „*Bezpieczny podpis elektroniczny*” Gazeta prawna z 4-6 sierpień 2000r,
50. Pitala Małgorzata „*Wybrane zagadnienia handlu elektronicznego w ujęciu nowej Dyrektywy Unii Europejskiej*”  
<http://www.landwellglobal.com/pl/pol/insights/articles/july2000-d.html> ,
51. Pniewski Paweł „*Dyrektywa Komisji Europejskiej w sprawie ram Wspólnotowych dla podpisu elektronicznego. Komentarz – artykuł pochodzi z Biuletynu ZBP nr 4/2000*” (data publikacji: 2000.09.18)  
[http://www.ebanki.px.pl/artykuly/dyrektywa\\_epodpis.html](http://www.ebanki.px.pl/artykuly/dyrektywa_epodpis.html),

52. Rafa J. „Prywatność więcej niż niezła. Ochrona poczty elektronicznej w Internecie” <http://www.wsp.krakow.pl/papers/pgp.html>,
53. Sieczka Lucyna „Elektroniczny podpis w Czechach” (data publikacji 2000.05.31) <http://www.gentv.com.pl/art000714.html>,
54. Sieczka Lucyna „Bezpieczny handel” (data publikacji 2000.06.19) <http://www.gentv.com.pl/art000714.html>,
55. Sitnicki Ignacy „Klucz do podpisu. Bezpieczeństwo obrotu prawnego w Internecie” <http://arch3.rzeczpospolita.pl/a/rz/2000/04/20000419/200004190041.html> ,
56. Szymborski Krzysztof „Prawo sieci” [http://www.computerworld.com.pl/online/1999/48/numer/prawo\\_sieci.asp](http://www.computerworld.com.pl/online/1999/48/numer/prawo_sieci.asp)
57. Trojański Mariusz, „Elektroniczna wymiana dokumentów” (2000.12.03) <http://www.www-mag.com.pl/porady/cybercash/c019/index.html>,
58. Zieliński Jarosław „Czym jest Internet” <http://www.winter.pl/czym/html>, (data publikacji 6.07.1998r ze zmianami 18.07.1998r)
59. Zieliński Jarosław „Usługi informacyjne w Internecie” <http://www.winter.pl/informacyjne.html>, (data publikacji 05.12.1997r ze zmianami 10.11.1998r)
60. Zieliński Jarosław „Powstanie Internetu” <http://www.winter.pl/powstanie.html>,

---

#### Inne źródła

61. Co nowego? Elektroniczne podpisy w MS Office 2000 <http://www.antywirus.pl/conowego/990618.html>,
62. Computer Emergency Response Team Naukowej i Akademickiej Sieci Komputerowej „Poselski projekt ustawy o podpisie elektronicznym” <http://www.cert.org.pl/NEW/nowosci62.html>,
63. CNN. com. technology. computing “Legalized e-signatures bring convenience, risk” <http://europe.cnn.com/2000/TECH/computing/09/29/e.signature/index.html>
64. Ebanki „Metody uwierzytelniania stosowane w bankach internetowych w Polsce” [http://www.ebanki.px.pl/technika/uwierz\\_bankowi.html](http://www.ebanki.px.pl/technika/uwierz_bankowi.html),
65. Ebanki „Podpis cyfrowy” [http://www.ebanki.px.pl/technika/podpis\\_cyfrowy.html](http://www.ebanki.px.pl/technika/podpis_cyfrowy.html),

66. „Prawo nowych technologii. Bibliografia”  
<http://www.prawnik.civ.pl/pwi/bibliografia.htm> ,
67. Polska Agencja Prasowa. Dziennik Internetowy „Powstaje poselski projekt ustawy o podpisie elektronicznym” Wydanie nr 895, Warszawa z 7 grudnia 2000r  
<http://dziennik.pap.com.pl/internet/20001207192318.html>,
68. Prometheus Interactive „Internet” <http://www.prometeus.com.pl/>,
69. Magellan Software „Podpis elektroniczny”  
<http://www.magsoft.pl/nawosci/Rok%202000/podpiselektroniczny.html>
70. PGP – Podpis elektroniczny, PGP – wstęp  
[http://www.webmedia.pl/marrad/pgp/pgp\\_r\\_po.html](http://www.webmedia.pl/marrad/pgp/pgp_r_po.html),
71. Planet, „Bezpieczeństwo systemu bankowości internetowej *Pl@net*. Podpisy elektroniczne, Kryptografia symetryczna, Kryptografia niesymetryczna, Protokoły SSL, Bezpieczeństwo” <http://www.fortisbank.com.pl/default.html>,
72. Uhlig Maciej „Ogólne omówienie różnic w zaawansowaniu zastosowań sieci internetowych w Polsce i na świecie” <http://www.cto.us.edu.pl/iift.html>,
73. VaGla.pl Prawo i Internet <http://www.vagla.pl>,
74. VizeSign rozwiązanie wspomagające podpis cyfrowy  
<http://www.radiotechmkt.com.pl/podpis.htm>,