KANCELARIA SEJMU
BIURO STUDIÓW
I EKSPERTYZ

WYDZIAŁ
INFORMACJI

Biuro Studiów i Ekspertyz

Luty 2001

Niemiecka ustawa o podpisie cyfrowym

tłum.: E. Misior

Materiały
i Dokumenty

Nr 307

Ustawa o podpisie cyfrowym

BGBl. 1997 I s. 1870

§ 1 Cel i zakres zastosowania

(1) Celem ustawy jest stworzenie ramowych warunków dla podpisów cyfrowych, w których będą one uważane za bezpieczne, a sfałszowanie podpisów cyfrowych lub fałszerstwo podpisanych danych będzie można stwierdzić wiarygodnie.
(2) Zastosowanie innych procedur dla podpisów cyfrowych pozostawia się do wyboru, jeżeli zgodnie z niniejszą ustawą przepis prawny nie zaleca podpisów cyfrowych.

§ 2 Definicje

(1) Podpisem cyfrowym w rozumieniu niniejszej ustawy jest pieczęć do danych cyfrowych utworzona przy pomocy prywatnego klucza do podpisu, która pozwala rozpoznać posiadacza klucza do podpisu oraz niesfałszowanie danych przy pomocy przynależącego klucza publicznego zaopatrzonego w certyfikat dla kluczy do podpisów otrzymany od wystawcy certyfikatów lub urzędu, o którym mowa w § 3.
(2) Wystawcą certyfikatów w rozumieniu niniejszej ustawy jest osoba fizyczna lub prawna, która poświadcza przyporządkowanie do osób fizycznych publicznych kluczy do podpisów i ma na to pozwolenie zgodnie z § 4.
(3) Certyfikatem w rozumieniu niniejszej ustawy jest cyfrowe zaświadczenie zaopatrzone w cyfrowy podpis o przyporządkowaniu publicznego klucza do podpisu osobie fizycznej (certyfikat klucza do podpisu) lub specjalne cyfrowe zaświadczenie zawierające dalsze dane przy jednoznacznym powołaniu się na certyfikat klucza do podpisu (certyfikat atrybutu).
(4) Stemplem czasu w rozumieniu niniejszej ustawy jest zaopatrzone w cyfrowy podpis cyfrowe zaświadczenie wystawcy certyfikatów, że w określonym momencie znajdowały się u niego określone dane cyfrowe.

§ 3 Właściwy urząd

Wydawanie pozwolenia i wystawianie certyfikatów używanych do podpisywania certyfikatów oraz nadzór nad przestrzeganiem niniejszej ustawy i rozporządzenia, o którym mowa w § 16, przysługują urzędom wymienionym w § 66 ustawy o telekomunikacji.

§ 4 Pozwolenie od wystawcy certyfikatów

(1) Działalność wystawcy certyfikatu wymaga pozwolenia wydanego przez właściwy urząd. Należy je wydać na wniosek.
(2) Wydania pozwolenia należy odmówić, jeżeli fakty usprawiedliwiają założenie, że wnioskodawca nie posiada wiarygodności wymaganej od wystawców certyfikatów, o ile wnioskodawca nie wykaże, że posiada wiedzę fachową wymaganą w takiej działalności lub gdy można oczekiwać, że przy podjęciu działalności wystawcy certyfikatów nie będą spełnione pozostałe warunki wymagane od wystawcy certyfikatów zgodnie z niniejszą ustawą i rozporządzeniem, o którym mowa w § 16.
(3) Wymaganą wiarygodność posiada ten, kto gwarantuje, że jako wystawca certyfikatów będzie przestrzegał miarodajnych przepisów prawnych. Wymaganą wiedzą fachową dysponuje się wtedy, gdy osoby pracujące u wystawcy certyfikatów posiadają konieczną wiedzę, doświadczenie i umiejętności. Pozostałe warunki wymagane od wystawcy certyfikatów zachodzą wtedy, gdy działania prowadzące do wypełnienia wymagań bezpieczeństwa niniejszej ustawy i rozporządzenia, o którym mowa w § 16, we właściwym czasie zostaną ujęte w koncepcji bezpieczeństwa, a wprowadzenie ich w życie zostanie sprawdzone i potwierdzone przez instytucję uznaną przez właściwy urząd.

(4) Pozwolenie może być obwarowane postanowieniami dodatkowymi, jeżeli jest to konieczne, aby przy podejmowaniu działalności i podczas jej trwania wystawca certyfikatów spełniał warunki niniejszej ustawy i rozporządzenia, o którym mowa w § 16.
(5) Właściwy urząd wystawia certyfikaty dla kluczy do podpisów używanych przy podpisywaniu certyfikatów. Przepisy dotyczące przyznawania certyfikatów przez wystawcę certyfikatów obowiązują odpowiednio w przypadku właściwych urzędów. Winny one certyfikaty wystawione przez siebie trzymać jako możliwe do sprawdzenia i wywołania przez każdego za pomocą publicznie dostępnych połączeń telekomunikacyjnych. Dotyczy to także informacji o adresach i numerach telefonicznych wystawców certyfikatów, o zablokowaniu wystawionych przez nie certyfikatów, o zawieszeniu i zakazie działalności wystawcy certyfikatów oraz o cofnięciu i odwołaniu pozwoleń.
(6) Za publiczne usługi zgodnie z niniejszą ustawą i rozporządzeniem, o którym mowa w § 16, ponosi się koszty (opłaty i wydatki).

§ 5 Przyznawanie certyfikatów
(1) Wydawca certyfikatów winna wiarygodnie zidentyfikować osoby, które składają wniosek o certyfikat. Przyporządkowanie publicznego klucza do podpisu do osoby zidentyfikowanej należy potwierdzić certyfikatem i klucz oraz certyfikaty atrybutu, które każdy może sprawdzić przy pomocy publicznie dostępnych połączeń telekomunikacyjnych i za zgodą posiadacza klucza do podpisu trzymać w gotowości do wywołania.
(2) Wystawca certyfikatów na żądanie wnioskodawcy winien włączyć dane osoby trzeciej o prawie do reprezentowania go oraz o dopuszczeniu ze względów zawodowo-prawnych lub innych do certyfikatu klucza do podpisu lub certyfikatu atrybutu, jeżeli wiarygodnie wykazano zgodę osoby trzeciej na przyjęcie prawa do reprezentowania lub dopuszczenie jej do tego.
(3) Na żądanie wnioskodawcy wystawca certyfikatów winien zamiast jego nazwiska umieścić w certyfikacie pseudonim.
(4) Wystawca certyfikatów winien podjąć działania, aby dane do certyfikatów nie były fałszywe lub sfałszowane w sposób niezauważony. Powinien ponadto podjąć dalsze działania, aby zapewnić utrzymanie w tajemnicy prywatnych kluczy do podpisów. Niedopuszczalne jest magazynowanie prywatnych kluczy do podpisów u wystawcy certyfikatów.
(5) Wystawca certyfikatów winien zatrudniać wiarygodny personel do prowadzenia działalności certyfikacyjnej. Do przygotowania kluczy do podpisów oraz wystawianie certyfikatów winna używać komponentów zgodnie z § 14. Dotyczy to także komponentów technicznych umożliwiających sprawdzanie certyfikatów zgodnie z ustępem 1 zdanie 2.

§ 6 Obowiązek informowania
Wystawca certyfikatów winien zgodnie z § 5 ust. 1 informować wnioskodawcę o działaniach niezbędnych do przyczynienia się do bezpieczeństwa cyfrowych podpisów i ich wiarygodnej kontroli. Winien ponadto informować wnioskodawcę, jakie komponenty techniczne spełniają warunki, o których mowa w § 14 ust. 1 i 2, oraz o przyporządkowaniu cyfrowych podpisów sporządzonych przy pomocy prywatnych kluczy do podpisów. Winien zwrócić wnioskodawcy uwagę, że w razie potrzeby dane trzeba na nowo podpisywać podpisem cyfrowym, zanim wartość zabezpieczenia istniejącego podpisu zmniejszy się z powodu upływu czasu.

§ 7 Treść certyfikatów
(1) Certyfikat klucza do podpisu musi zawierać następujące dane:
1. nazwę posiadacza klucza do podpisów, którego na wypadek możliwości omyłkowej zamiany należy zaopatrzyć w dodatek lub niezmienny pseudonim, który będzie łatwy do poznania jako taki i przyporządkowany do posiadacza klucza do podpisu,
2. przyporządkowany publiczny klucz do podpisu,

3. określenie algorytmów, przy pomocy których można używać publicznego klucza posiadacza klucza do podpisu oraz publicznego klucza wystawcy certyfikatu,
4. numer bieżący certyfikatu,
5. początek i koniec ważności certyfikatu,
6. nazwę wystawcy certyfikatu oraz
7. informacje, czy wykorzystanie klucza do podpisu ogranicza się do określonych zastosowań co do rodzaju i zakresu.

(2) Dane o przedstawicielstwie dla osoby trzeciej oraz o dopuszczeniu ze względów zawodowoprawnych lub innych można włączyć zarówno do certyfikatu klucza do podpisu lub do certyfikatu atrybutu.
(3) Inne dane certyfikat klucza do podpisu może zawierać jedynie za zgodą osoby, której to dotyczy.

§ 8 Blokada certyfikatów
(1) Wystawca certyfikatu może zablokować certyfikat, jeżeli zażąda tego posiadacz klucza do podpisu lub jego przedstawiciel, certyfikat zostanie uzyskany na podstawie fałszywych danych do § 7, wystawca zakończy swoją działalność a nie będzie jej kontynuować inny wystawca certyfikatów lub blokadę zarządzi właściwy urząd zgodnie z § 13 ust. 5 zdanie 2. Blokada musi zawierać datę, od której obowiązuje. Niedopuszczalna jest blokada działająca wstecz.
(2) Jeżeli certyfikat zawiera dane osoby trzeciej, także ona może zażądać blokady tego certyfikatu.
(3) Właściwy urząd blokuje certyfikaty wystawione przez siebie zgodnie z § 4 ust. 5, jeżeli wystawca certyfikatu zawiesi swoją działalność lub gdy pozwolenie zostanie odebrane lub odwołane.

§ 9 Stempel czasu
Wystawca certyfikatów winien na żądanie wyposażyć dane cyfrowe w stempel czasu. Odpowiednio obowiązuje § 5 ust. 5 zdanie 1 i 2.

§ 10 Dokumentacja
Wystawca certyfikatów winien tak dokumentować działania zabezpieczające w celu przestrzegania niniejszej ustawy i rozporządzenia, o którym mowa w § 16, oraz wystawione certyfikaty, aby dane i ich nie sfałszowanie można było sprawdzić w każdej chwili.

§ 11 Zakończenie działalności
(1) Wystawca certyfikatów, gdy kończy swoją działalność, winien zgłosić to możliwie wcześnie we właściwym urzędzie i zatroszczyć się o to, aby przy zakończeniu działalności ważne certyfikaty przejął inny wystawca lub aby je zablokować.
(2) Dokumentację, o której mowa w § 10, wystawca winien przekazać wystawcy certyfikatów, który przejmie certyfikaty lub przekazać właściwemu urzędowi w innym przypadku.
(3) Wystawca winien we właściwym urzędzie niezwłocznie zgłosić wniosek o rozpoczęcie postępowania upadłościowego lub ugodowego.

§ 12 Ochrona danych
(1) Wystawca certyfikatów może zbierać dane osobowe jedynie bezpośrednio u osoby zainteresowanej, jeżeli jest to niezbędne dla celów certyfikatu. Zbieranie danych u osób trzecich jest dopuszczalne jedynie za zgodą osoby zainteresowanej. Dane można użyć w celach innych niż wymienione w zdaniu 1 jedynie wtedy, gdy zezwala na to niniejsza ustawa lub inne rozporządzenie lub gdy zgadza się na to osoba zainteresowana.

(2) W przypadku posiadacza klucza do podpisu używającego pseudonimu wystawca certyfikatów winien na prośbę przesłać dane dotyczące jego tożsamości do właściwej instytucji, jeżeli jest to konieczne przy ściganiu przestępstw lub wykroczeń porządkowych, dla obrony przed zagrożeniem bezpieczeństwa publicznego lub porządku albo dla wypełnienia ustawowych zadań urzędów ochrony konstytucji Federacji i krajów związkowych, Federalnych Służb Informacyjnych, Wojskowych Służb Wywiadowczych lub Urzędu Policji Kryminalnej. Informację należy dokumentować. Urząd zwracający się z prośbą winien poinformować posiadacza klucza do podpisów o ujawnieniu jego pseudonimu, gdy tylko wypełnianie ustawowych zadań nie będzie już przez to zagrożone lub gdy o poinformowaniu przesądza interes posiadacza klucza do podpisu.
(3) § 38 federalnej ustawy o ochronie danych ma zastosowanie przy założeniu, że kontroli można dokonać także wtedy, gdy nie istnieje podejrzenie, że naruszono przepisy o ochronie danych.

§ 13 Kontrola i realizacja zobowiązań
(1) Właściwy urząd może wobec wystawcy certyfikatów podjąć kroki w celu zapewnienia przestrzegania niniejszej ustawy i rozporządzenia. W tym celu może zwłaszcza zabronić korzystania z nieodpowiednich komponentów technicznych i całkowicie lub częściowo zakazać działalności wystawcy certyfikatów. Osobom, które wywołują wrażenie, że dysponują pozwoleniem, o którym mowa w § 4, mimo że tak nie jest, można zabronić działalności.
(2) Dla celów kontroli zgodnie z ustępem 1 zdanie 1 wystawcy certyfikatów winni zezwolić właściwemu urzędowi na wchodzenie do pomieszczeń służbowych i zakładowych w godzinach pracy, na żądanie okazywać do wglądu księgi, notatki, pokwitowania, pisma i pozostałe dokumenty, które wchodzą w zakres zainteresowań, udzielać informacji oraz zapewnić wymaganą pomoc. Osoba zobowiązana do udzielania informacji może odmówić udzielenia informacji na takie pytania, na które odpowiedź naraziłaby ją samą lub członków jej rodziny wymienionych w § 383 ust. 1 pkt 1 do 3 kpc na groźbę ścigania z powodu przestępstwa lub postępowania zgodnie z ustawą o wykroczeniach porządkowych. Osobę zobowiązaną do udzielania informacji należy poinformować o tym prawie.
(3) W przypadku niewywiązania się z obowiązków wynikających z niniejszej ustawy lub rozporządzenia lub w przypadku istnienia przyczyny uzasadniającej odmowę wydania pozwolenia właściwy urząd winien odwołać udzielone pozwolenie, jeżeli działania, o których mowa w ustępie 1 zdanie 2 nie rokują powodzenia.
(4) W przypadku cofnięcia lub odwołania pozwolenia lub zawieszenia działalności wystawcy certyfikatów właściwy urząd winien zapewnić przejęcie działalności przez innego wystawcę certyfikatów lub rozwiązać umowę z posiadaczem klucza do podpisu. Dotyczy to także wniosków o otworzenie postępowania upadłościowego lub ugodowego, jeżeli nie będzie się kontynuować działalności, na którą wydano pozwolenie.
(5) Cofnięcie lub odwołanie pozwolenia nie narusza ważności certyfikatu wydanego przez wystawcę certyfikatów. Właściwy urząd może zarządzić blokadę certyfikatów, jeżeli fakty uzasadniają założenie, że certyfikaty są sfałszowane lub nie są dostatecznie zabezpieczone przed fałszerstwem lub komponenty techniczne użyte przy stosowaniu kluczy do podpisu wykazują braki w zabezpieczeniu umożliwiające niezauważalne fałszowanie podpisów cyfrowych lub niezauważalne fałszowanie podpisanych danych.

§ 14 Komponenty techniczne
(1) Do tworzenia i magazynowania kluczy do podpisów oraz do tworzenia i kontroli podpisów cyfrowych konieczne są komponenty techniczne z zabezpieczeniami które w sposób wiarygodny pozwolą rozpoznać fałszerstwo podpisu cyfrowego i fałszowanie podpisanych danych i które będą chronić prywatne klucze do podpisów przed nieupoważnionym użyciem.

(2) Do wytworzenia danych, które mają być podpisane, konieczne są komponenty techniczne z zabezpieczeniami, które utworzenie podpisu cyfrowego pozwolą uprzednio jednoznacznie zgłosić i ustalić, do których danych odnosi się cyfrowy podpis. Dla sprawdzenia podpisanych danych wymagane są komponenty techniczne, które pozwalają ustalić, czy podpisane dane są niezmienione, do jakich danych odnosi się cyfrowy podpis i jakiemu posiadaczowi klucza do podpisu należy przyporządkować podpis cyfrowy.
(3) W przypadku komponentów technicznych, przy pomocy których trzyma się do sprawdzenia lub wywołania certyfikaty kluczy do podpisu zgodnie z § 5 ust. 1 zdanie 2, konieczne są działania zabezpieczające wykazy certyfikatów przed nieuprawnioną zmianą lub nieuprawnionym wywoływaniem.
(4) W przypadku komponentów technicznych, o których mowa w ustępach 1 do 3, konieczne jest, aby były dostatecznie kontrolowane stosownie do stanu techniki i aby instytucja uznana przez właściwy urząd potwierdziła spełnienie wymagań.
(5) W przypadku komponentów technicznych wytwarzanych prawomocnie zgodnie z regulacjami lub wymaganiami obowiązującymi w innym państwie członkowskim Unii Europejskiej lub innym państwie-sygnatariuszu układu o Wspólnym Obszarze Gospodarczym lub wprowadzanych do obrotu oraz gwarantujących takie samo bezpieczeństwo, punktem wyjścia jest fakt, że spełnione są wymagania, o których mowa w ustępach 1 i 3, dotyczące właściwości bezpieczeństwa technicznego. W uzasadnionych przypadkach indywidualnych na żądanie właściwego urzędu należy wskazać, że są spełnione wymagania, o których mowa w zdaniu 1. Jeżeli przy wykazywaniu wymagań w rozumieniu ustępów 1 do 3 dotyczących właściwości zabezpieczenia technicznego przewidziano okazanie potwierdzenia wydanego przez instytucję uznaną przez właściwy urząd, uwzględnia się także potwierdzenia ze strony instytucji dopuszczonej w innych państwach członkowskich Unii Europejskiej lub w innych państwach sygnatariuszach układu o Wspólnym Obszarze Gospodarczym, jeżeli raporty kontrolne tych instytucji są równoważne pod względem wartości z kontrolami i procedurami kontrolnymi instytucji uznanych przez właściwe urzędy.

§ 15 Certyfikaty zagraniczne
(1) Cyfrowe podpisy, które można skontrolować przy pomocy publicznego klucza do podpisów, dla których istnieje zagraniczny certyfikat z innego państwa członkowskiego Unii Europejskiej lub innego państwa sygnatariusza układu o Wspólnym Obszarze Gospodarczym, jeżeli wykazują takie samo bezpieczeństwo, należy uznać za równoznaczne z cyfrowymi podpisami zgodnie z niniejszą ustawą.
(2) Ustęp 1 dotyczy także innych państw, jeżeli istnieją odpowiednie ponadpaństwowe lub międzypaństwowe porozumienia.

§ 16 Rozporządzenie
Rząd federalny jest upoważniony do wydania w drodze rozporządzenia przepisów prawnych koniecznych do wykonania §§ 3 do 15 dotyczących
1. bliższych szczegółów procedury wydawania, cofania i odwoływania pozwolenia oraz procedury zawieszania działalności wystawców certyfikatów,
2. czynności, o których mowa w § 4 ust. 6, objętych obowiązkową opłatą oraz wysokość opłaty,
3. bliższego określenia obowiązków wystawcy certyfikatów,
4. okresu ważności certyfikatów dla kluczy do podpisów,
5. bliższego sprecyzowania kontroli wystawcy certyfikatów,
6. bliższych wymagań dotyczących komponentów technicznych i kontroli komponentów technicznych oraz potwierdzenia, że wymagania są spełnione,
7. okresu oraz procedury, według której nadaje się nowy podpis cyfrowy.

Rozporządzenie o podpisach cyfrowych (SIgV)

Na podstawie § 16 ustawy z dnia 22 lipca 1007 o podpisie (BGBl. I s. 1870, 1872) rząd federalny zarządza

Spis treści

§ 1 Postępowanie przy wydawaniu, wycofaniu i odwołaniu pozwoleń

(1) O pozwolenie na działalność wystawcy certyfikatów, o czym mowa w § 4 ust. 1 ustawy o podpisach, należy złożyć pisemny wniosek we właściwym urzędzie.

(2) W celu kontroli warunków wydawania pozwolenia właściwy urząd przyjmuje konieczne ustalenia. Może zażądać od wnioskodawcy, aby dostarczył wymagane dokumenty, w szczególności aktualny wyciąg z rejestru handlowego oraz aktualne świadectwa prowadzenia, o czym mowa w § 30 ust. 5 federalnej ustawy o rejestrze centralnym dla ustawowych przedstawicieli instytucji certyfikujących . Dla stwierdzenia wymaganej wiedzy fachowej wnioskodawca powinien udowodnić, że personel uczestniczący w procedurach certyfikacji lub przy wystawianiu stempli czasu posiada wymagane kwalifikacje zawodowe.

(3) Przed odrzuceniem, cofnięciem lub odwołaniem pozwolenia właściwy urząd winien wysłuchać wnioskodawcę i dać mu możliwość usunięcia powodów będących przyczyną odrzucenia, wycofania lub odwołania.

§ 2 Koszty

(1) Przy następujących świadczeniach publicznych powstają koszty (opłaty i wydatki)

1. wydawanie pozwolenia na działalność wystawcy certyfikatów,
2. odrzucenie wniosku o wydanie pozwolenia,
3. cofnięcie lub odwołanie pozwolenia,
4. całkowite lub częściowe odrzucenie sprzeciwu,
5. wystawienie certyfikatu,

6. kontrola raportów kontrolnych i poświadczeń, o czym owa w § 15 ust. 1,
7. kontrole zgodnie z § 15 ust. 2, jeżeli w ramach kontroli stwierdzone zostanie poważne wykroczenie przeciw ustawie o podpisach lub przeciw niniejszemu rozporządzeniu,
8. przejęcie dokumentacji, o czym mowa w § 11 ust. 2 ustawy o podpisach.

Koszty powstają także wtedy, gdy wniosek o przyznanie pozwolenia lub sprzeciw zostanie wycofany po rozpoczęciu rzeczowego opracowania ale przed jego zakończeniem.

(2) Przy obliczaniu opłat za świadczenia publiczne, o których mowa w ustępie 1 pkt 1, 5, 6, 7 i 8 podstawą winny być następujące stawki godzinowe:

1. urzędnicy państwowi średniego szczebla lub pracownicy o porównywalnym statusie:
   85 DM
2. urzędnicy państwowi wyższego szczebla lub pracownicy o porównywalnym statusie:
   106 DM
3. urzędnicy państwowi najwyższego szczebla lub pracownicy o porównywalnym statusie:
   135 DM.

Za każdy rozpoczęty kwadrans należy obliczyć jedną czwartą powyższych stawek godzinowych. Jeżeli pracownicy właściwego urzędu wykonują świadczenia poza urzędem, należy ponadto doliczyć opłaty za czas podróży zawarty w przyjętym czasie pracy lub inaczej ustalony przez właściwy urząd oraz zawiniony przez dłużnika z tytułu kosztów czas oczekiwania.

(3) W przypadkach odrzucenia lub wycofania wniosku o wydanie pozwolenia oraz cofnięcia lub odwołania pozwolenia obowiązuje § 15 ustawy o kosztach administracyjnych. W przypadku całkowitego lub częściowego odrzucenia sprzeciwu można pobrać opłatę do wysokości opłaty pobieranej za zaskarżony akt administracyjny. W przypadku odrzucenia i w przypadkach wycofania sprzeciwu dotyczącego wyłącznie decyzji stanowiącej o kosztach można pobrać opłatę do wysokości 10% spornej kwoty.

§ 3 Postępowanie przy wydawaniu certyfikatów

(1) Wystawca certyfikatów winien dokonać identyfikacji wnioskodawcy zgodnie z § 5 ust. 1 zdanie 1 ustawy o podpisach na podstawie federalnego dowodu osobistego lub paszportu podróżnego lub w inny odpowiedni sposób. Wniosek o wydanie certyfikatu musi być własnoręcznie podpisany. Jeżeli wniosek o certyfikat jest zaopatrzony w cyfrowy podpis wnioskodawcy, wystawca certyfikatu może odstąpić od ponownej identyfikacji i własnoręcznego podpisu.

(2) Jeżeli zgodnie z § 5 ust. 2 ustawy o podpisach w certyfikacie ujęto dane o prawie do przedstawicielstwa dla osoby trzeciej, należy wiarygodnie wykazać prawo do przedstawicielstwa i musi istnieć zgoda osoby trzeciej pisemna lub opatrzona podpisem cyfrowym. Osobę trzecią należy poinformować pisemnie lub w formie cyfrowej o treści certyfikatu i o możliwości blokady, o czym mowa w § 9 ust. 1. Zwłaszcza dopuszczenie wynikające z prawa pracy lub innego prawa należy udokumentować okazując dokument dopuszczenia.

§ 4 Pouczenie wnioskodawcy

(1) Wystawca certyfikatów winien w ramach § 6 zdanie 1 i 3 ustawy o podpisach pouczyć wnioskodawcę zwłaszcza o następujących niezbędnych działaniach dla zapewnienia bezpieczeństwa podpisu cyfrowego:

1. Nośnik danych z prywatnym kluczem do podpisu należy przechowywać osobiście. W przypadku jego utraty należy niezwłocznie zlecić blokadę certyfikatu klucza do podpisu. Jeżeli nośnik danych z prywatnym kluczem do podpisu nie jest już potrzebny, należy uczynić go nieprzydatnym do użytku i zlecić blokadę certyfikatu klucza do podpisu, jeżeli jego ważność jeszcze nie wygasła.

2. Osobisty numer identyfikacyjny lub inne dane służące do identyfikacji nośnika danych z prywatnym kluczem do podpisu należy trzymać w tajemnicy. W razie ujawnienia lub podejrzenia ujawnienia owych danych identyfikacyjnych należy niezwłocznie dokonać ich zmiany.
3. W celu tworzenia i kontroli cyfrowych podpisów oraz w celu przedstawienia danych, które mają być podpisane lub danych podpisanych, które należy sprawdzić należy zastosować komponenty techniczne odpowiadające zarządzeniom ustawy o podpisie i niniejszemu rozporządzeniu i których bezpieczeństwo potwierdzono w oparciu o ustawę o podpisie i niniejsze rozporządzenie. Należy je chronić przed dostępem osób nieupoważnionych.
4. Jeżeli certyfikat zawiera ograniczenia, o których mowa w § 7 ust. 1 ustawy o podpisach lub dane, o których mowa w § 7 ust. 2 ustawy o podpisach, i ma to znaczenie dla wypowiedzi o podpisanych danych, certyfikat należy dołączyć do danych i włączyć do cyfrowego podpisu.
5. Jeżeli dla zastosowania podpisanych danych istotne znaczenie ma określony moment, należy dołączyć stempel czasu.
6. Jeżeli dane będą potrzebne przez dłuższy czas w formie podpisanej, należy ponowić podpis cyfrowy zgodnie z § 18.
7. W przypadku kontrolowania podpisów cyfrowych należy ustalić, czy certyfikat klucza do podpisu i certyfikat atrybutu były ważne w chwili tworzenia podpisu, czy certyfikat klucza do podpisu zgodnie z § 7 ust. 1 pkt 7 ustawy o podpisach zawiera ograniczenia oraz czy w danym przypadku przestrzegano punktów 4 i 5.
(2) Jeżeli wnioskodawca posiada już certyfikat, można zaniechać ponownego pouczenia.

§ 5 Tworzenie i przechowywanie kluczy do podpisów oraz danych identyfikujących
(1) Jeżeli klucze do podpisów tworzone są przez posiadacza, wystawca certyfikatów winien się przekonać, że ów stosuje w tym celu oraz w celu przechowywania i używania prywatnych kluczy do podpisów właściwych komponentów technicznych zgodnie z ustawą o podpisach i z niniejszym rozporządzeniem.
(2) Jeżeli klucze do podpisów są przygotowywane przez wystawcę certyfikatów, winien on podjąć działania, które wykluczą ujawnienie prywatnych kluczy i przechowywanie ich u wystawcy certyfikatów. Dotyczy to także osobistych numerów identyfikacyjnych lub innych danych służących do identyfikacji posiadacza klucza do podpisu wobec nośnika danych z prywatnym kluczem do podpisu.

§ 6 Przekazanie kluczy do podpisów i danych identyfikujących
Jeżeli wystawca certyfikatów przygotowuje klucz do podpisu lub dane identyfikujące, o których mowa w § 5 ust. 2, winien przekazać prywatny klucz do podpisu oraz dane identyfikacyjne posiadaczowi klucza do podpisu osobiście i kazać pisemnie potwierdzić ich przekazanie, chyba że ów zażąda pisemnie innego przekazania. Wraz z przekazaniem klucza do podpisu lub certyfikatu klucza do podpisu winien przekazać właściwemu urzędowi publiczny klucz do podpisu.

§ 7 Okres ważności certyfikatów
Okres ważności certyfikatu może wynosić najwyżej pięć lat i nie może przekraczać okresu przydatności zastosowanych algorytmów i przynależnych do nich parametrów, o których mowa w § 17 ust. 2 Ważność certyfikatu atrybutu kończy się najpóźniej wraz z ważnością certyfikatu klucza do podpisu, do którego się odnosi.

§ 8 Publiczne wykazy certyfikatów
(1) Instytucja certyfikująca winna prowadzić wykaz wystawionych przez siebie certyfikatów zgodnie z zaleceniami § 5 ust. 1 zdanie 2 przynajmniej tak długo, jak długo za przydatny

uważany jest algorytm wymieniony w certyfikacie wraz z należącymi do niego parametrami o których mowa w § 17 ust..
(2) Właściwy urząd winien prowadzić wykaz wystawionych przez siebie certyfikatów przez okres wymieniony w ust. 1 zgodnie z zaleceniami § 4 ust. 5 zdanie 3 ustawy o podpisach. Dotyczy to także certyfikatów dla publicznych kluczy do podpisów naczelnych zagranicznych wystawców certyfikatów, jeżeli zagraniczne certyfikaty zostały uznane. W przypadku zagranicznych certyfikatów zawartych w wykazie właściwy urząd winien potwierdzić uznanie podpisem cyfrowym. Właściwy urząd winien przyłączenia telekomunikacyjne, pod którymi można wywołać certyfikaty oraz ich publiczne klucze niezwłocznie opublikować w Monitorze Federalnym i ogłosić u wystawców certyfikatów.
(3) Po upływie terminu określonego w ustępie 1 wystawcy certyfikatów oraz właściwy urząd do chwili upływu terminu wymienionego w § 13 ust. 2 winni umożliwić na wniosek kontrolę certyfikatów w indywidualnym przypadku.

§ 9 Postępowanie przy blokowaniu certyfikatów
(1) Wystawca certyfikatów winien posiadaczowi klucza do podpisu oraz osobom trzecim, od których pobrano do certyfikatu dane w celu pełnomocnictwa do reprezentowania., i właściwemu urzędowi podać do wiadomości numer telefonu, pod którym zawsze będą mogli zlecić natychmiastową blokadę certyfikatów i zalecić procedurę ich autentyzacji.
(2) Wystawca certyfikatów winien zablokować certyfikat na warunkach podanych w § 8 ustawy o podpisach, jeżeli istnieje wniosek pisemny lub zaopatrzony w cyfrowy podpis posiadacza klucza do podpisu lub jego przedstawiciela lub upoważnionej osoby trzeciej zgodnie z ustępem 1 lub gdy zastosowano uzgodnioną procedurę autentyzacji.
(3) Blokadę certyfikatów należy jednoznacznie oznaczyć podając datę godzinę w spisie, o którym mowa w § 8 ustawy o podpisach. Blokady nie wolno anulować.

§ 10 Wiarygodność personelu
Wystawca certyfikatów winien upewnić się co do wiarygodności osób, które pracują przy procedurze certyfikacji lub przy wystawianiu stempli czasu. Może w szczególności zażądać okazania świadectwa z rejestru skazanych zgodnie z § 30 ust. 1 ustawy o federalnym rejestrze centralnym. Osoby niewiarygodne należy wykluczyć z procedury certyfikacji i wystawiania stempli czasu.

§ 11 Ochrona komponentów technicznych
Wystawca certyfikatów winien poczynić przygotowania do ochrony przed dostępem osób nieupoważnionych do prywatnych kluczy do podpisów oraz komponentów technicznych użytych do wystawienia certyfikatów i stempli czasu oraz do utrzymywania certyfikatów w gotowości do kontroli.

§ 12 Koncepcja bezpieczeństwa
(1) Koncepcja bezpieczeństwa, o której mowa w § 4 ust. 3 zdanie 3 ustawy o podpisach winna obejmować wszystkie działania zabezpieczające, a w szczególności przegląd zastosowanych komponentów technicznych oraz opis organizacji działalności certyfikacyjnej. W przypadku zmian istotnych dla bezpieczeństwa należy niezwłocznie dopasować do nich koncepcję.
(2) Właściwy urząd prowadzi katalog przydatnych działań zabezpieczających, który publikuje w Monitorze Federalnym. Działania należy uwzględnić przy wypracowywaniu koncepcji bezpieczeństwa. Katalog układa się według danych Federalnego Urzędu Bezpieczeństwa Techniki Informacyjnej. Winny w tym brać udział eksperci z dziedziny ekonomii i nauki.

§ 13 Dokumentacja
(1) Dokumentacja, o której mowa w § 10 ustawy o podpisach winna obejmować koncepcję bezpieczeństwa łącznie ze zmianami, raporty kontrolne oraz potwierdzenia, o których mowa w § 15 ust. 1, umowne uzgodnienia z wnioskodawcami oraz certyfikaty otrzymane z właściwego urzędu. Do wniosków o certyfikaty i uzgodnień z wnioskodawcami, które wpłynęły, należy załączyć kserokopię przedłożonego dowodu osobistego lub innego dokumentu stwierdzającego tożsamość, dokumentu koniecznego dla przyjęcia danych osób trzecich, nadanie pseudonimu, dowód zaleconego pouczenia wnioskodawcy i osób trzecich, wydane certyfikaty z datą wydania i przekazania, blokadę certyfikatów i informacje, o których mowa w § 12 ust. 3 ustawy o podpisach. Jeżeli wystawca certyfikatów przygotowuje klucze do podpisu lub dane identyfikacyjne zgodnie z § 12 ust. 2, należy udokumentować moment przekazania i potwierdzenia przekazania. Notatki prowadzone w formie cyfrowej muszą być potwierdzone cyfrowo.
(2) Dokumentację, o której mowa w ustępie 1,, należy przechowywać co najmniej 35 lat od chwili wystawienia certyfikatu klucza do podpisu i tak zabezpieczyć, aby w tym okresie można było mięć do niej dostęp. Dokumentację informacji, o czym mowa w § 12 ust. 2 zdanie 2 ustawy o podpisach, przechowuje się dwanaście miesięcy.

§ 14 Zawieszenie działalności
(1) Jeżeli wystawca certyfikatów chce zawiesić swoją działalność zgodnie z § 11 ust. 1 ustawy o podpisach, winien poinformować o tym właściwy urząd najpóźniej cztery miesiące wcześniej.
(2) Przed zakończeniem swojej działalności wystawca certyfikatów dla każdego nie zablokowanego i w chwili zakończenia działalności niewygasłego certyfikatu winien poinformować posiadacza klucza do podpisu w terminie przynajmniej trzech miesięcy, że chce zakończyć swoją działalność jako wystawca certyfikatów i poinformować go, czy jego certyfikat przejmie inny wystawca i wymienić go. Jeżeli certyfikatów nie przejmie inny wystawca, po upływie terminu wymienionego w ustępie 1 należy zablokować wszystkie certyfikaty, które w danym momencie nie są jeszcze zablokowane lub które nie wygasły. Należy poinformować o tym posiadaczy certyfikatów klucza do podpisu, które mają być zablokowane.
(3) Informacje dla właściwego urzędu i pouczenie posiadacza klucza do podpisu należy przekazać w formie pisemnej lub cyfrowej z cyfrowym podpisem.
(4) Wystawca certyfikatów, który przejmuje dokumentację zgodnie z § 11 ust. 2 ustawy o podpisach lub w pozostałym przypadku właściwy urząd winny prowadzić wykaz certyfikatów zgodnie z § 8 ust. 1 i 3.

§ 15 Kontrola wystawców certyfikatów
(1) Wystawca certyfikatów przed podjęciem działalności po zmianach z powodu bezpieczeństwa oraz regularnie w odstępie dwuletnim winien zlecać przeprowadzenie kontroli zgodnie z § 4 ust. 3 zdanie 3 ustawy o podpisach i składać we właściwym urzędzie raport kontrolny oraz potwierdzenie tego, że wypełniła zalecenia wynikające z ustawy o podpisach oraz niniejszego rozporządzenia.
(2) Właściwy urząd może zarządzić kontrolę w odpowiednich odstępach czasowych oraz w przypadku podejrzenia naruszenia przepisów ustawy o podpisach lub niniejszego rozporządzenia.

§ 16 Wymagania w odniesieniu do komponentów technicznych
(1) Komponenty techniczne niezbędne przy wytwarzaniu kluczy do podpisów muszą mieć takie właściwości, aby klucz występował tylko raz przy prawdopodobieństwie graniczącym z

pewnością i aby z publicznego klucza nie można było obliczyć klucza prywatnego. Konieczne jest zagwarantowanie utrzymania w tajemnicy prywatnego klucza; nie można tworzyć duplikatów. Zmiany techniki zabezpieczenia w komponentach technicznych muszą być rozpoznawalne dla użytkownika.
(2) Komponenty techniczne konieczne do wytwarzania lub kontroli podpisów cyfrowych muszą mieć takie właściwości, aby z podpisu nie można było obliczyć prywatnego klucza do podpisu ani sfałszować podpisu w inny sposób. Prywatny klucz do podpisu wolno użyć dopiero po zidentyfikowaniu posiadacza i nie wolno go ujawnić przy używaniu. Do identyfikacji posiadacza klucza do podpisu można dodatkowo wykorzystać cechy biometryczne. Komponenty techniczne konieczne do zarejestrowania danych identyfikacyjnych muszą mieć takie właściwości, aby nie ujawniły danych identyfikacyjnych i aby były magazynowane wyłącznie na nośniku danych z prywatnym kluczem do podpisu. Zmiany techniki zabezpieczenia w komponentach technicznych muszą być rozpoznawalne dla użytkownika.
(3) Komponenty techniczne konieczne do przedstawienia danych, które mają być podpisane, winny mieć takie właściwości, aby osoba podpisująca jednoznacznie mogła określić dane, do których odnosi się jej podpis i aby cyfrowy podpis następował tylko na jej polecenie, które należy uprzednio jednoznacznie zgłosić. Komponenty techniczne konieczne do kontroli podpisanych danych muszą mieć takie właściwości, aby osoba kontrolująca mogła jednoznacznie ustalić dane objęte cyfrowym podpisem oraz posiadacza i aby prawidłowość cyfrowego podpisu została wiarygodnie sprawdzona i trafnie wskazana. Komponenty techniczne do kontrolowania certyfikatów muszą jednoznacznie pozwolić rozpoznać, czy kontrolowane certyfikaty w określonym momencie znajdowały się w wykazie certyfikatów i czy nie były zablokowane. Komponenty techniczne muszą zgodnie z potrzebą pozwolić wystarczająco rozpoznać treść danych do podpisu i danych już podpisanych. Jeżeli komponenty techniczne, o których mowa w zdaniach 1 do 4 zostaną zaoferowane osobom trzecim w celach zawodowo-handlowych, należy zapewnić jednoznaczną interpretację danych, a komponenty techniczne przy korzystaniu muszą być automatycznie sprawdzane pod względem prawdziwości. Zmiany techniki zabezpieczenia w komponentach technicznych muszą być rozpoznawalne dla użytkownika.
(4) Komponenty techniczne, przy pomocy których będą kontrolowane certyfikaty, o których mowa w § 4 ust. 5 zdanie 3 lub § 5 ust. 1 zdanie 2 ustawy o podpisach, muszą mieć takie właściwości, aby tylko osoby upoważnione mogły dokonywać wpisów i zmian, aby nie można było w sposób niezauważony anulować blokady certyfikatu i aby informacje można było sprawdzić w odniesieniu do ich prawdziwości. W informacjach musi być podane, czy sprawdzone certyfikaty w określonym czasie były umieszczone w wykazie certyfikatów i czy nie były zablokowane. Jedynie certyfikaty trzymane w gotowości do sprawdzenia nie mogą być wywoływane publicznie. Zmiany techniki zabezpieczenia w komponentach technicznych muszą być rozpoznawalne dla użytkownika.
(5) Komponenty techniczne, przy pomocy których tworzone będą stemple czasu, o których mowa w § 9 ustawy o podpisach, muszą mieć takie właściwości, aby czas ustawowy obowiązujący w chwili wytwarzania stempla czasu można było bez fałszowania włączyć do stempla. Zmiany techniki zabezpieczającej muszą być rozpoznawalne dla użytkownika.
(6) Właściwy urząd prowadzi katalog przydatnych działań zabezpieczających, który publikuje w Monitorze Federalnym. Działania należy uwzględnić w komponentach technicznych. Katalog sporządza się według danych Federalnego Urzędu ds. Bezpieczeństwa Techniki Informacyjnej. Winni brać w tym udział eksperci z dziedziny ekonomii i nauki.

§ 17 Kontrola komponentów technicznych
(1) Kontrola komponentów technicznych, o której mowa w § 14 ust. 4 ustawy o podpisach, winna się odbywać w oparciu o "Kryteria oceny bezpieczeństwa systemów techniki informacyjnej" (GMBl. 1992, s. 545). Kontrola w przypadku komponentów technicznych do wytwa-

rzania kluczy do podpisów lub do magazynowania lub stosowania prywatnych kluczy do podpisów i w przypadku komponentów technicznych, które oferuje w celach handlowo-zawodowych się osobom trzecim do użytku musi obejmować przynajmniej poziom kontroli E4, a w pozostałych przypadkach poziom E2. Moc mechanizmów zabezpieczających musi mieć ocenę "wysoki", a algorytmy i przynależące do nich parametry muszą zgodnie z ustępem 2 mieć ocenę przydatności.
(2) Właściwy urząd publikuje w Monitorze Federalnym przegląd algorytmów i przynależnych parametrów, które należy uznać za przydatne do wytwarzania kluczy do podpisów, do HASHEN danych przewidzianych do podpisu albo do wytwarzania lub kontroli cyfrowych podpisów, oraz datę, do której przydatność obowiązuje w danym przypadku. Data powinna być określona przynajmniej na sześć lat od chwili oceny i opublikowania. Przydatność należy na nowo określać co rok oraz w razie potrzeby. Przydatność istnieje, jeżeli w określonym czasie zgodnie ze stanem nauki i techniki można z prawdopodobieństwem graniczącym z pewnością wykluczyć takie fałszerstwo cyfrowych podpisów lub fałszowanie podpisanych danych, którego nie da się stwierdzić. Przydatność ustala się według danych Federalnego Urzędu ds. Bezpieczeństwa Techniki Informacyjnej. Winni brać w tym udział eksperci z dziedziny ekonomii i nauki.
(3) W potwierdzeniu spełnienia wymagań wobec komponentów technicznych, o czym mowa w § 14 ust. 4 ustawy o podpisach należy podać, dla jakich wymagań zgodnie z § 16 obowiązuje potwierdzenie i pod jakimi warunkami zastosowania, jakie zastosowano algorytmy i przynależne parametry zgodnie z ustępem 2 i do jakiego momentu są one co najmniej przydatne oraz według jakiego stopnia sprawdzane były komponenty techniczne, o których mowa w ustępie 1. Egzemplarz raportu kontrolnego i potwierdzenia należy zdeponować we właściwym urzędzie. Może on przy punktach dotyczących braków wykazanych podczas kontroli lub odnośnie do potwierdzonych komponentów technicznych lub wyrywkowo zasięgnąć opinii niezależnej osoby trzeciej, czy komponenty techniczne, o których mowa w ustępie 1 zostały sprawdzone i czy spełniają one wymagania ustawy o podpisie oraz wymagania niniejszego rozporządzenia. Jeżeli nie zapewni się ich lub okaże się, że potwierdzone komponenty techniczne nie zostały dostatecznie sprawdzone lub że nie spełniają wymagań, właściwy urząd może ogłosić unieważnienie wydanych potwierdzeń.
(4) Właściwy urząd ogłasza w *Monitorze Federalnym* instytucje uznane na podstawie § 14 ustawy o podpisach oraz komponenty techniczne, które zgodnie z ustępem 3 otrzymały od nich potwierdzenie i bezpośrednio podaje do wiadomości wystawcom certyfikatów.

§ 18 Odnowiony podpis cyfrowy
Jeżeli dane w formie podpisanej są potrzebne dłużej niż czas, na który algorytmy użyte do ich wytworzenia i sprawdzania i przynależne parametry zostały ocenione jako przydatne, dane przed upływem czasu przydatności algorytmów i przynależnych parametrów należy zaopatrzyć w nowy cyfrowy podpis. Musi on mieć nowe algorytmy lub przynależne parametry, zawierać poprzednie podpisy cyfrowe i mieć stempel czasu.

§ 19 Wejście w życie
Niniejsze rozporządzenie wchodzi w życie 1 listopada 1997 r.

Niemiecka ustawa o podpisie cyfrowym
wersja robocza

BGBl. 1997 I s. 1870