Kryptografia i bezpieczeństwo systemów informatycznych

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2025/2026

inf.ug.edu.pl/~amb/

Podpis elektroniczny w Polsce

Źródła prawa

- USTAWA z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2001 r. Nr 130, poz. 1450)

Rozporządzenia do Ustawy o podpisie elektronicznym (Dz.U.02.128.1094 – 1001):

- Określenie warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.
- Sposób i szczegółowe warunki spełnienia obowiązku ubezpieczenia odpowiedzialności cywilnej przez kwalifikowany podmiot.

Źródła prawa c.d.

- Wzór i szczegółowy zakres wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym.
- Wysokość opłaty za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym.
- Sposób prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzór tego rejestru oraz szczegółowy tryb postępowania w sprawach o wpis do rejestru.
- Określenie zasad wynagradzania za przeprowadzenie kontroli podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym.
- Określenie szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym.

Ustawa o podpisie elektronicznym, art. 1 i 3

- Art. 1. Ustawa określa warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi.
- Art. 3. Użyte w ustawie wyrażenia oznaczają:

  1) podpis elektroniczny – 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 elektroniczny,

  na razie nie jest jasne, że chodzi o cały zestaw: zakodowany skrót podpisanego dokumentu, dane podpisującego, oraz podpis zaufanego centrum potwierdzający te dane (razem: certyfikat podpisującego)

Ustawa, art. 3 (Użyte w ustawie wyrażenia oznaczają:)

- 2) bezpieczny podpis elektroniczny – podpis elektroniczny, który:

  a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,

  czy można mieć wspólny podpis dla grupy osób? czy można się podpisać za kogoś? NIE

  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, *czy komputer osobisty podlega wyłącznej kontroli właściciela – raczej nie*

Ustawa, art. 3 (Użyte w ustawie wyrażenia oznaczają:)

- 2) bezpieczny podpis elektroniczny – podpis elektroniczny, który:

  c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna,

  warunek jest spełniony dla każdego rodzaju podpisu opartego o skrót wiadomości
- 3) osoba składająca podpis elektroniczny – osobę fizyczną posiadającą urządzenie służące do składania podpisu elektronicznego, która działa w imieniu własnym albo w imieniu innej osoby fizycznej, prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej,

  można działać w cudzym imieniu, ale podpisać się trzeba osobiście

Ustawa, art. 3: dwa klucze

- 4) dane służące do składania podpisu elektronicznego – niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tę osobę do składania podpisu elektronicznego,

  to jest właśnie klucz prywatny, tajny, tylko właściciel jest w stanie złożyć podpis elektroniczny
- 5) dane służące do weryfikacji podpisu elektronicznego – niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane do identyfikacji osoby składającej podpis elektroniczny,

  to musi być klucz publiczny+dane osobowe, można sprawdzić czy podpis został złożony przy użycia odpowiadającego mu klucza prywatnego, można się dowiedzieć, kto składał podpis

Ustawa, art. 3: urządzenie do składania podpisu elektronicznego

- 6) urządzenie służące do składania podpisu elektronicznego – sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający złożenie podpisu lub poświadczenia elektronicznego przy wykorzystaniu danych służących do składania podpisu lub poświadczenia elektronicznego,
- 7) bezpieczne urządzenie służące do składania podpisu elektronicznego – urządzenie służące do składania podpisu elektronicznego spełniające wymagania określone w ustawie,

  urządzenie, to może być komputer, ale bezpieczne, to raczej karta kryptograficzna

  poświadczenie elektroniczne, to naprawdę podpis elektroniczny, ale nie osoby fizycznej, lecz centrum certyfikacji

Ustawa, art. 3: urządzenie do weryfikacji podpisu elektronicznego

- 8) urządzenie służące do weryfikacji podpisu elektronicznego – sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający identyfikację osoby fizycznej, która złożyła podpis elektroniczny, przy wykorzystaniu danych służących do weryfikacji podpisu elektronicznego lub w sposób umożliwiający identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne, przy wykorzystaniu danych służących do weryfikacji poświadczenia elektronicznego,
- 9) bezpieczne urządzenie służące do weryfikacji podpisu elektronicznego – urządzenie służące do weryfikacji podpisu elektronicznego spełniające wymagania określone w ustawie,

  nie ma na świecie innych urządzeń do weryfikacji, tylko komputer

Ustawa, art. 3: certyfikat

- 10) certyfikat – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby,

  w certyfikacie zawarte są:

  1. *klucz publiczny (służy do weryfikacji podpisu),*
  2. *dane osobowe właściciela (umożliwiają identyfikację osoby),*
  3. *podpis, czyli poświadczenie elektroniczne, wystawcy certyfikatu (odpowiada za przyporządkowanie klucza publicznego do właściciela)*
- 11) zaświadczenie certyfikacyjne ...podmiotu świadczącego usługi certyfikacyjne lub organu, o którym mowa w art. 30 ust. 1, i które umożliwiają identyfikację ...

  to samo co certyfikat, ale dla centrum certyfikacji – a nie osoby fizycznej

Ustawa, art. 3: certyfikat kwalifikowany

- 12) kwalifikowany certyfikat – certyfikat spełniający warunki określone w ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w ustawie,

  technologicznie rzecz biorąc niczym się nie różni od zwykłego. Ale wystawca musi dochować pewnych zasad. Np. naprawdę sprawdzić tożsamość właściciela certyfikatu.

Ustawa, art. 3: znakowanie czasem

- 16) znakowanie czasem – usługę polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę,
  - *dane opatrzone podpisem lub poświadczeniem elektronicznym – nasz dokument*
  - *dane w postaci elektronicznej logicznie powiązane z powyższymi – podpis skrótu*
  - *czyli do podpisanego skrótu dołącza się znacznik czasu i potwierdza podpisem, wiadomo, że nie robi tego nigdy osoba fizyczna*

Ustawa, art. 3 (Użyte w ustawie wyrażenia oznaczają:)

- 18) odbiorca usług certyfikacyjnych – osobę fizyczną, osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej, która:

  a) zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych, lub

  b) w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane elektronicznie poświadczone przez podmiot świadczący usługi certyfikacyjne,

  a więc są dwie bardzo różne kategorie odbiorców:
  - *ci, którzy zakupili certyfikat i składają podpis elektroniczny,*
  - *oraz oraz ci, którzy tak podpisane dokumenty otrzymują i używają czyjegoś certyfikatu do weryfikacji podpisu*

Ustawa, art. 3: poświadczenie elektroniczne

- 19) poświadczenie elektroniczne – dane w postaci elektronicznej, ...
- 20) dane służące do składania poświadczenia elektronicznego ...
- 21) dane służące do weryfikacji poświadczenia elektronicznego ...

  poświadczenie elektroniczne, technologicznie jest to podpis elektroniczny (bezpieczny), ale składany przez wystawcę certyfikatów, a nie osobę fizyczną

Ustawa, art. 3: weryfikacja podpisu

- 22) weryfikacja bezpiecznego podpisu elektronicznego – czynności, które pozwalają na identyfikację osoby składającej podpis elektroniczny, oraz pozwalają stwierdzić, 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.
  1. *za pomocą klucza publicznego weryfikuje się podpis (skrótu) dokumentu,*
  2. *ustala się tożsamość właściciela tego klucza,*
  3. *oraz sprawdza, że dokument się nie zmienił*

  (inaczej niż w przypadku dokumentów papierowych)

Ustawa, art.5. (skutki prawne)

- 1. Bezpieczny podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu. Bezpieczny podpis elektroniczny złożony w okresie zawieszenia kwalifikowanego certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylenia tego zawieszenia.
- 2. Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej.

Skutki prawne podpisu elektronicznego, art. 5 c.d.

- 1. Bezpieczny podpis elektroniczny...
- 2. Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym...

  nie jest jasne to rozróżnienie

- 1. ...weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu.
- 2. ...weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu

  w pierwszym przypadku badamy, czy certyfikat był ważny w momencie składania podpisu, niekoniecznie teraz, w drugim przypadku jakby zapomniano, że certyfikat mógł stracić ważność

Skutki prawne podpisu elektronicznego, art. 5 c.d.

- 1. ...weryfikowany przy pomocy kwalifikowanego certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu.
- 2. ...weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej.

  nie ma wątpliwości, że podpis elektroniczny jest równie dobry jak odręczny. Nie można go stosować, jeśli wymagany jest specjalny formularz, specjalna oprawa składania podpisu, obecność np. notariusza. Ale to są wyjątki.

Skutki prawne podpisu elektronicznego, art. 5 c.d.

- 1. ...Bezpieczny podpis elektroniczny złożony w okresie zawieszenia kwalifikowanego certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylenia tego zawieszenia.

  certyfikat można unieważnić/mija termin ważności. Ale można też tymczasowo zawiesić, gdy zachodzą podejrzenia, że klucz prywatny został skompromitowany. Ta usługa nie musi być dostępna dla wszystkich certyfikatów.

Ustawa art. 6. (skutki prawne c.d.)

- 1. Bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie, jako składającą podpis elektroniczny.
- 2. Przepis ust. 1 nie odnosi się do certyfikatu po upływie terminu jego ważności lub od dnia jego unieważnienia oraz w okresie jego zawieszenia, chyba że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed jego unieważnieniem albo zawieszeniem.

  znakowanie czasem na pewno ułatwia dowód ważności podpisu elektronicznego

Skutki prawne podpisu elektronicznego, art. 6 c.d.

- 3. Nie można powoływać się, że podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.

  gdy certyfikat jest kwalifikowany, to na pewno znajduje się na karcie kryptograficznej i składający podpis nie może się go wyprzeć

Ustawa art. 7. (skutki prawne, znakowanie czasem)

- 1. Podpis elektroniczny może być znakowany czasem.
- 2. Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu Cywilnego.
- 3. Uważa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne 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.

Skutki prawne podpisu elektronicznego, jeszcze inaczej

- Art. 8. Nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego.
- Art. 14. 3. w przypadku wydawania certyfikatów niebędących certyfikatami kwalifikowanymi, informacja, o której mowa w ust. 2, powinna również zawierać wskazanie, że podpis elektroniczny weryfikowany przy pomocy tego certyfikatu nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

  właściwie nie jest jasne jakie skutki prawne ma podpis weryfikowany certyfikatem niekwalifikowanym

Obowiązki wystawcy certyfikatów, art 10

- 1. Kwalifikowany podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty jest obowiązany:

  1) zapewnić techniczne i organizacyjne możliwości szybkiego i niezawodnego wydawania, zawieszania i unieważniania certyfikatów oraz określenia czasu dokonania tych czynności,

  dlaczego miałby mieć obowiązek szybko wydawać certyfikaty?

  2) stwierdzić tożsamość osoby ubiegającej się o certyfikat,

  3) 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,

Obowiązki wystawcy certyfikatów, art. 10 c.d.

- 9) 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,
  - *klucz prywatny ma być prywatny, ma być nieznany również wystawcy certyfikatów (mimo, że jest on godny zaufania)*
  - *klucz prywatny jest generowany na karcie kryptograficznej, jednak proces generowania rozpoczyna się od losowego ziarna dostarczonego przez centrum certyfikacji, gdyby je zachować, istniałoby niebezpieczeństwo powtórzenie procesu generowania*

Obowiązki wystawcy certyfikatów, art. 10 c.d.

- 10) zapewnić, w razie tworzenia przez niego danych służących do składania podpisu elektronicznego, aby dane te z prawdopodobieństwem graniczącym z pewnością wystąpiły tylko raz,

  klucz prywatny ma być niepowtarzalny, ale nie wolno sprawdzać tego przez porównanie z dotychczasowymi (są one nieznane), niepowtarzalność wynika z losowania

Obowiązki wystawcy certyfikatów, art. 10 c.d.

- 11) 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.

  klucz publiczny podpisującego jest zawarty w certyfikacie, weryfikacja certyfikatu czy znacznika czasu, wymaga klucza publicznego wystawcy, skąd wziąć ten klucz?

  Odp: wystawca musi o to jakoś zadbać

Odpowiedzialność wystawcy certyfikatów (art. 11)

- 2. Podmiot świadczący usługi certyfikacyjne nie odpowiada 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.
- 3. Podmiot świadczący usługi certyfikacyjne nie odpowiada wobec odbiorców usług certyfikacyjnych za szkodę wynikłą z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek osoby składającej podpis elektroniczny.

  certyfikat nie potwierdza prawdziwości innych danych, jedynie tożsamość właściciela klucza publicznego

Bezpieczne urządzenia (art.18)

- 1. Bezpieczne urządzenie służące do składania podpisu elektronicznego powinno co najmniej:

  1) uniemożliwiać pozyskiwanie danych służących do składania podpisu lub poświadczenia elektronicznego,

  np. poprzez zaszycie klucza prywatnego na karcie kryptograficznej

  2) nie zmieniać danych, które mają zostać podpisane lub poświadczone elektronicznie oraz umożliwiać przedstawienie tych danych osobie składającej podpis elektroniczny przed chwilą jego złożenia,

  czy tekst w edytorze Word jest przedstawiony osobie składającej podpis? a w przeglądarce z włączoną Javą? raczej wątpliwe

Bezpieczne urządzenia (art.18 c.d.)

- 2. Bezpieczne urządzenie służące do weryfikacji podpisu elektronicznego powinno spełniać następujące wymagania:

  nie jest jasne czym innym niż komputer ma być to urządzenie

  1) dane używane do weryfikacji podpisu elektronicznego odpowiadają danym, które są uwidaczniane osobie weryfikującej ten podpis,

  dane do weryfikacji, to klucz publiczny, dane uwidaczniane osobie, to raczej dane osobowe właściciela certyfikatu

  3) osoba weryfikująca może w sposób nie budzący wątpliwości ustalić zawartość podpisanych danych,

  czyli zawartość ma być przedstawiona tak samo jak podpisującemu

  6) użycie pseudonimu jest jednoznacznie wskazane,

Kwalifikowany certyfikat (art. 20)

- 1. Kwalifikowany certyfikat zawiera co najmniej następujące dane:

  1) numer certyfikatu,

  2) wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji,

  3) określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę oraz numer pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,

  4) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone,

  5) dane służące do weryfikacji podpisu elektronicznego,

Kwalifikowany certyfikat c.d.

- ...co najmniej następujące dane:

  6) oznaczenie początku i końca okresu ważności certyfikatu,

  7) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat,

  czyżby dalsze dane nie były podpisane?

  8) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji,

  9) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa, o której mowa w art. 14 ust. 1.

Ważność kwalifikowanego certyfikatu (art. 21)

1. Certyfikat jest ważny w okresie w nim wskazanym.

2. Podmiot świadczący usługi certyfikacyjne unieważnia certyfikat kwalifikowany przed upływem okresu jego ważności, jeżeli: ...*wiele przyczyn*...5) zażąda tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie,

7. Certyfikat, który został zawieszony, może zostać następnie unieważniony lub jego zawieszenie może zostać uchylone.

8. Certyfikat, który został unieważniony, nie może być następnie uznany za ważny.

11. Zawieszenie lub unieważnienie certyfikatu nie może następować z mocą wsteczną.

Lista certyfikatów unieważnionych (art. 22)

1. Podmiot świadczący usługi certyfikacyjne publikuje listę zawieszonych i unieważnionych certyfikatów.

3. Lista zawieszonych i unieważnionych kwalifikowanych certyfikatów powinna zawierać w szczególności: ...

- 6) datę i czas, z dokładnością określoną w polityce certyfikacji, zawieszenia lub unieważnienia każdego certyfikatu,
- 7) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, publikującego listę.

5. Zawieszenie i unieważnienie certyfikatu wywołuje skutki prawne od momentu, o którym mowa w ust. 3 pkt 6, który nie może być wcześniejszy niż data i czas publikacji poprzedniej listy zawieszonych i unieważnionych certyfikatów.

Odpowiedzialność za fałszerstwa

- Art. 47: Kto składa bezpieczny podpis elektroniczny za pomocą danych służących do składania podpisu elektronicznego, które zostały przyporządkowane do innej osoby, podlega grzywnie lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie.
- Art. 48: Kto, świadcząc usługi certyfikacyjne, kopiuje lub przechowuje dane służące do składania bezpiecznego podpisu lub poświadczenia elektronicznego lub inne dane, które mogłyby służyć do ich odtworzenia, podlega grzywnie lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie.
- Art. 49: 1. Kto, świadcząc usługi certyfikacyjne, wydaje certyfikat zawierający nieprawdziwe dane, o których mowa w art. 20 ust. 1, podlega grzywnie lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie.
  3. Tej samej karze podlega osoba, która posługuje się certyfikatem, o którym mowa w ust. 1.

Odpowiedzialność za fałszerstwa, c.d.

- Art. 50: Kto, świadcząc usługi certyfikacyjne, wbrew obowiązkowi, o którym mowa w art. 21 ust. 2 pkt 5 i 6, zaniecha unieważnienia certyfikatu, podlega grzywnie lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie.
- Art. 51: Kto, świadcząc usługę znakowania czasem jako kwalifikowany podmiot świadczący usługi certyfikacyjne, umożliwia oznaczenie danych czasem innym niż z chwili wykonywania tej usługi oraz poświadcza elektronicznie tak powstałe dane, podlega grzywnie lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie.

Ustawa art.58. (elektroniczne podania)

- Art. 58...2. w terminie 4 lat od dnia wejścia w życie ustawy organy władzy publicznej umożliwią odbiorcom usług certyfikacyjnych wnoszenie podań i wniosków oraz innych czynności w postaci elektronicznej, w przypadkach gdy przepisy prawa wymagają składania ich w określonej formie lub według określonego wzoru.
- 3. Minister właściwy do spraw gospodarki w porozumieniu z ministrem właściwym do spraw administracji publicznej określi, w drodze rozporządzenia, warunki techniczne i warunki bezpieczeństwa udostępniania formularzy i wzorów, o których mowa w ust. 2.
- 4. Minister właściwy do spraw finansów publicznych, w terminie roku od dnia wejścia w życie ustawy, dostosuje przepisy regulujące sposób wnoszenia opłat za czynności administracyjne do wymogów obrotu prawnego z wykorzystaniem podpisu elektronicznego.