Krajowa Izba Rozliczeniowa S.A.

POLITYKA CERTYFIKACJI KIR
dla
USŁUGI ZNAKOWANIA CZASEM

Wersja 1.2

Historia dokumentu

Numer wersji	Status	Data wydania
1.0	Dokument zatwierdzony przez Zarząd KIR – wersja poprzednia obowiązująca do 28 lutego 2010 r.	22.06.2005 r.
1.1	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca do 1 marca 2015 r.	1.03.2010 r.
1.2	Dokument zatwierdzony przez Zarząd KIR – wersja obowiązująca od 2 marca 2015 r.	26.02.2015 r.

SPIS TREŚCI

1. WSTĘP

„Polityka certyfikacji KIR dla kwalifikowanej usługi znakowania czasem”, zwana dalej Polityką, zgodnie z ustawą o podpisie elektronicznym określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania znaczników czasu. Identyfikator niniejszej Polityki ma postać: 1.2.616.1.113571.1.3.

Krajowa Izba Rozliczeniowa S.A. NIP: 526-030-05-17, zarejestrowana w Sądzie Rejonowym pod nr rejestru RHB-30600, jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne w rozumieniu przepisów ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450), wpisanym do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne w zakresie usługi znakowania czasem pod numerem 6 na podstawie decyzji nr 20/014499/05 Ministra Gospodarki i Pracy z dnia 5 września 2005 roku.

Krajowa Izba Rozliczeniowa S.A. świadczy usługi znakowania czasem zgodnie z obowiązującym prawem polskim oraz zasadami dotyczącymi kwalifikowanych podmiotów świadczących usługi certyfikacyjne określonymi w ustawie o podpisie elektronicznym oraz towarzyszących jej rozporządzeniach i niniejszą Polityką.

Krajowa Izba Rozliczeniowa S.A. świadczy usługi znakowania czasem na podstawie wpisu Krajowej Izby Rozliczeniowej do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne i wydanego przez ministra właściwego do spraw gospodarki lub podmiot działający w jego imieniu ministra zaświadczenia certyfikacyjnego.

Wszelką korespondencję związaną ze świadczeniem usług certyfikacyjnych należy kierować na adres siedziby KIR:

Krajowa Izba Rozliczeniowa S.A.
ul. Pileckiego 65
02-801 Warszawa
z dopiskiem „znakowanie czasem”,

tel. 801 500 207
e-mail: bok@kir.pl

lub na adres terenowych jednostek KIR, jak również drogą elektroniczną na adresy zamieszczone na stronie internetowej KIR.

2. DEFINICJE

Znakowanie czasem – usługa polegająca na dołączaniu do danych w postaci elektronicznej oznaczenia czasu w chwili wykonywania tej usługi oraz poświadczania elektronicznego tak powstałych danych.

Odbiorca usług – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która zawarła z KIR umowę na świadczenie usług certyfikacyjnych polegających na znakowaniu czasem.

Subskrybent – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, posiadająca certyfikat, działająca w imieniu własnym albo innej osoby fizycznej, prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej, uprawniona do zgłoszenia żądań o znaczniki czasu na podstawie Umowy.

Poświadczenie elektroniczne – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne oraz spełniają następujące warunki:

a) są sporządzone za pomocą podlegających wyłącznej kontroli podmiotu świadczącego usługi certyfikacyjne bezpiecznych urządzeń do składania podpisów i danych służących do składania poświadczenia elektronicznego;

b) jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

Certyfikat – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisów elektronicznych (klucz publiczny) są przyporządkowane do subskrybenta.

Kwalifikowany Certyfikat – certyfikat spełniający warunki określone w ustawie o podpisie elektronicznym, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymagania określone w ustawie o podpisie elektronicznym.

Klucz prywatny – dane służące do składania podpisów elektronicznych lub poświadczeń elektronicznych w rozumieniu ustawy o podpisie elektronicznym.

Klucz publiczny – dane służące do weryfikacji podpisów elektronicznych lub poświadczeń elektronicznych w rozumieniu ustawy o podpisie elektronicznym.

Lista CRL – lista zawieszonych i unieważnionych certyfikatów.

Ustawa o podpisie elektronicznym – ustawa z dnia 18 września 2001 roku o podpisie elektronicznym (Dz. U. nr 130, poz. 1450) wraz z późniejszymi zmianami.

Ustawa o ochronie danych osobowych – ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. nr 101, poz.926) wraz z późniejszymi zmianami.

Umowa – umowa na świadczenie usług certyfikacyjnych polegających na znakowaniu czasem, zawarta pomiędzy KIR a odbiorcą usług.

Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, służą do identyfikacji subskrybenta.

Znacznik czasu – poświadczony elektronicznie zbiór danych, o których mowa w załączniku nr 2.

3. ZAKRES ZASTOSOWANIA POLITYKI

Polityka jest stosowana do świadczenia przez KIR usług certyfikacyjnych polegających na znakowaniu czasem na żądanie subskrybentów, wskazanych przez odbiorcę usług na mocy umowy.

4. ŚWIADCZENIE USŁUG CERTYFIKACYJNYCH

4.1. Umowa na świadczenie usług certyfikacyjnych

Podstawą do świadczenia usług certyfikacyjnych polegających na znakowaniu czasem jest umowa.

Umowa może zostać zawarta z osobą fizyczną, osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej. Po zawarciu umowy odbiorca usług wskazuje subskrybentów, na których żądania będą wydawane znaczniki czasu. Wskazanie subskrybentów po zawarciu umowy, jak również zmiana danych dotyczących subskrybentów, nie wymagają zmiany umowy i odbywa się poprzez zgłoszenie subskrybentów lub danych na odpowiednim formularzu.

4.2. Zakres stosowania znaczników czasu

Usługa znakowania czasem świadczona przez KIR zgodnie z niniejszą Polityką oraz ustawą o podpisie elektronicznym i rozporządzeniami wydanymi na jej podstawie, wywołuje w szczególności skutki daty pewnej w rozumieniu Kodeksu cywilnego.

Zgodnie z ustawą o podpisie elektronicznym, 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 znacznika. Przedłużenie istnienia domniemania wymaga kolejnego znakowania czasem dokumentu oznakowanego.

4.3. Zobowiązania Krajowej Izby Rozliczeniowej S.A.

KIR zobowiązuje się do:

- świadczenia usług certyfikacyjnych polegających na znakowaniu czasem zgodnie z wymaganiami ustawy o podpisie elektronicznym i rozporządzeniami wydanymi na jej podstawie;
- stosowania procedur organizacyjnych i operacyjnych uniemożliwiających manipulowanie czasem wykorzystywanym do świadczenia usługi znakowania czasem;
- wykorzystywania do świadczenia usługi znakowania czasem danych służących do składania poświadczeń elektronicznych wygenerowanych wyłącznie dla tej usługi;
- ochrony swoich kluczy prywatnych wykorzystywanych do wydawania znaczników czasu zgodnie z niniejszą Polityką;
- ochrony, zgodnie z postanowieniami ustawy o ochronie danych osobowych, danych osobowych subskrybentów przekazanych przez odbiorcę usług na mocy umowy;
- wydawania znaczników czasu w odpowiedzi na poprawnie zweryfikowane żądania wydania znaczników czasu;
- weryfikowania poprawności żądań o wydanie znaczników czasu dostarczonych do KIR .

Subskrybent i inne podmioty trzecie ponoszą całe ryzyko związane ze szkodą wynikłą z podjęcia działań, mimo negatywnie lub niekompletnie zweryfikowanego albo nieważnego znacznika czasu, jak również w przypadku, gdy zaniechają weryfikacji statusu lub kompletności znacznika czasu.

Szczegółowe zobowiązania KIR może określać umowa.

4.4. Zobowiązania odbiorcy usług

Odbiorca usług zobowiązuje się do wskazania KIR subskrybentów uprawnionych do korzystania z usługi znakowania czasem w sposób nienaruszający interesów tych osób.

Szczegółowe zobowiązania odbiorcy usług może określać umowa.

Po otrzymaniu znacznika czasu wydanego przez KIR odbiorca usług lub subskrybent są zobowiązani do sprawdzenia, czy:

- poświadczenie elektroniczne złożone przez KIR jest prawidłowe;
- istnieją ograniczenia w stosowaniu znaczników czasu określone w niniejszej Polityce.

Odbiorca usług jest zobowiązany w szczególności:

- nie dokonywać modyfikacji znacznika czasu;
- używać znacznika czasu zgodnie z postanowieniami Polityki oraz do celów zgodnych z prawem i przeznaczeniem;
- wykonywać zobowiązania nałożone umową, niniejszą Polityką lub innym wiążącym go dokumentem.

4.5. Odpowiedzialność Krajowej Izby Rozliczeniowej S.A.

KIR odpowiada wobec odbiorców usług certyfikacyjnych w rozumieniu ustawy o podpisie elektronicznym, w tym subskrybentów i odbiorców usług, za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swoich obowiązków w zakresie świadczonych usług, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które KIR nie ponosi odpowiedzialności i którym nie mogła zapobiec mimo dołożenia należytej staranności.

KIR odpowiada za przechowywanie oraz archiwizowanie danych związanych ze świadczeniem usługi znakowania czasem.

KIR odpowiada za bezpieczeństwo kluczy infrastruktury w rozumieniu § 2 pkt 11 rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia 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 wykorzystywanych w procesie świadczenia usługi znakowania czasem, zwanych dalej „kluczami infrastruktury".

KIR nie odpowiada za szkody wynikłe z:

- przyczyn niezależnych od KIR, a w szczególności uszkodzeń infrastruktury telekomunikacyjnej spowodowanych przez osoby, za które KIR nie ponosi odpowiedzialności;
- wadliwości sprzętu teleinformatycznego nie będącego pod kontrolą KIR;
- akceptowania przez subskrybenta lub osoby trzecie nieważnych lub negatywnie albo niekompletnie zweryfikowanych znaczników czasu;
- siły wyższej;
- niewłaściwego użytkowania lub instalacji aplikacji oraz sprzętu kryptograficznego stosowanego przez subskrybenta lub osobę trzecią do obsługi znaczników czasu;
- odmowy realizacji usługi w przypadku nieważności lub zawieszenia certyfikatu subskrybenta, wad żądania wydania znacznika czasu, zaległości z opłatami lub w innych uzasadnionych przypadkach, w tym w przypadkach wskazanych w umowie lub niniejszej Polityce;
- zaprzestania świadczenia usługi znakowania czasem;
- tymczasowego wstrzymania świadczenia usługi znakowania czasem lub jej niedostępności, np. na skutek awarii lub modyfikacji systemu wykorzystywanego do świadczenia usługi lub oprogramowania albo sprzętu z nim współpracującego, czy zerwania łączy internetowych;
- upływu terminu ważności zaświadczenia certyfikacyjnego służącego do weryfikacji znacznika czasu;
- unieważnienia zaświadczenia certyfikacyjnego służącego do weryfikacji znacznika czasu.

Jeżeli reklamacja znacznika czasu nie zostanie zgłoszona w ciągu 24 godzin KIR nie odpowiada za szkody związane z wystąpieniem okoliczności reklamacyjnych, o których mowa w pkt 4.12.

Umowa może określić bardziej szczegółowo zakres odpowiedzialności KIR.

4.6. Odpowiedzialność odbiorcy usług

Odbiorca usług ponosi odpowiedzialność za prawidłowe wywiązywania się z obowiązków nałożonych umową, prawem, niniejszą Polityką lub innym wiążącym go dokumentem.

4.7. Odpowiedzialność finansowa

Łączna odpowiedzialność z tytułu świadczenia przez KIR usług certyfikacyjnych polegających na znakowaniu czasem nie może przekroczyć 1 000 000 EUR. Wysokość jednorazowego odszkodowania z tytułu użycia nieprawidłowego certyfikatu wydanego przez KIR nie może przekroczyć 250 000 EUR. Wskazana odpowiedzialność finansowa dotyczy okresów 1 roku kalendarzowego liczonych od dnia wpisania KIR do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

4.8. Opłaty

Opłaty z tytułu świadczenia usług certyfikacyjnych określa umowa.

4.9. Kontrola

W zakresie określonym w ustawie o podpisie elektronicznym, KIR podlega kontroli ministra właściwego do spraw gospodarki.

4.10. Kompromitacja klucza prywatnego KIR

W przypadku kompromitacji klucza prywatnego KIR wykorzystywanego do wydawania znaczników czasu, żądanie unieważnienia zaświadczenia certyfikacyjnego jest przekazywane do ministra właściwego do spraw gospodarki. Po unieważnieniu przez ministra zaświadczenia certyfikacyjnego, informacja o tym jest publikowana na liście CRL generowanej przez ministra właściwego do spraw gospodarki lub upoważniony przez niego podmiot.

4.11. Zaprzestanie świadczenia usług certyfikacyjnych w zakresie znakowania czasem przez KIR

Zgodnie z ustawą o podpisie elektronicznym KIR ma prawo do zaprzestania świadczenia usług certyfikacyjnych polegających na znakowaniu czasem. W takim przypadku wszyscy subskrybenci oraz odbiorcy usług zostaną o tym poinformowani z 90 dniowym wyprzedzeniem. Zgodnie z wymaganiami ustawy o podpisie elektronicznym, wszystkie wydane przez KIR znaczniki czasu i związane z tym dokumenty zostaną przekazane do ministra właściwego ds. gospodarki lub podmiotu wskazanego przez ministra.

4.12. Postępowanie reklamacyjne

Subskrybent lub odbiorca usług ma prawo do zareklamowania usługi znakowania czasem w szczególności, gdy:

- znacznik czasu zawiera błędy formalne;
- znacznik czasu nie zawiera wszystkich danych;
- dane oznakowane czasem są inne od przedłożonych do oznakowania w żądaniu znakowania czasem;
- przy tworzeniu znacznika czasu zbiór danych przedłożony do oznakowania nie został poświadczony elektronicznie przez KIR.

Reklamacja powinna zawierać uzasadnienie, w tym w szczególności wskazywać jedną z ww. okoliczności reklamacyjnych.
W przypadku stwierdzenia zasadności zgłoszonej reklamacji KIR przywraca odbiorcy usług lub subskrybentowi uprawnienie do skorzystania z usługi znakowania czasem. Subskrybent lub odbiorca usługi może zgłosić reklamację w ciągu 12 miesięcy od wysłania znacznika czasu do subskrybenta lub odbiorcy usług. Jeżeli jednak reklamacja nie zostanie zgłoszona w ciągu 24 godzin od wysłania

znacznika czasu do Subskrybenta, KIR nie odpowiada za szkody związane z wykorzystaniem znacznika czasu, mimo wystąpienia jednej z okoliczności reklamacyjnych.

Jakiekolwiek działanie podjęte w zaufaniu do wadliwego znacznika czasu uważa się za jego akceptację.

5. OPIS SPOSOBU TWORZENIA I PRZESYŁANIA DANYCH, KTÓRE ZOSTANĄ OPATRZONE POŚWIADCZENIAMI ELEKTRONICZNYMI

5.1. Bezpieczne urządzenia do składania podpisów

Do generowania znaczników czasu wykorzystywane są bezpieczne urządzenia do składania podpisów. Urządzenia te są wykorzystywane wyłącznie do świadczenia usług certyfikacyjnych w ramach niniejszej Polityki. Bezpieczne urządzenia do składania podpisów wykorzystywane w KIR posiadają certyfikat FIPS 140 level 3. Bezpieczne urządzenia do składania podpisów wykorzystywane w KIR są zabezpieczone przed nieupoważnionym dostępem. Dostęp do urządzeń mają jedynie upoważnione osoby. Każda próba dostępu do danego urządzenia, niezależnie od podejmowanej czynności oraz jej wyniku, w tym w szczególności czynności związane z wygenerowaniem danych służących do poświadczania elektronicznego znaczników czasu lub ich użyciem są monitorowane i rejestrowane w systemie teleinformatycznym wykorzystywanym do świadczenia usług certyfikacyjnych.

Dane służące do poświadczania elektronicznego znaczników czasu są zabezpieczone kluczami. Klucze te są dzielone na części według schematu progowego (m, n), gdzie wartość „m" wynosi 2, natomiast „n" wynosi 5. Każda z części jest przechowywana w osobnych modułach kluczowych będących w posiadaniu osób upoważnionych przez KIR lub w sejfach. Dane do składania poświadczeń elektronicznych pojawiają się w pełnej formie wyłącznie w komponencie technicznym.

5.2. Klucze infrastruktury

Klucze infrastruktury są wykorzystywane do:

- zapewnienia integralności przekazu danych związanych ze świadczeniem usług (żądania wydania znaczników czasu, informacje o błędach wynikłych w procesie wydawania znaczników czasu);
- zapewnienia integralności rejestrów zdarzeń przechowywanych w KIR;
- zapewnienia integralności danych związanych ze świadczeniem usług archiwizowanych w KIR;
- zabezpieczania dostępu do oprogramowania oraz urządzeń do składania podpisów wykorzystywanych do świadczenia usług certyfikacyjnych polegających na znakowaniu czasem.

5.3. Usługa znakowania czasem

Proces wydawania znaczników czasu przebiega w następujący sposób:

- odbiorca usług oraz wskazani przez niego subskrybenci zostają zarejestrowani w systemie;
- subskrybent przesyła do KIR żądanie wydania znacznika czasu;
- żądanie jest weryfikowane na podstawie danych przekazanych w procesie rejestracji;

- generowany jest znacznik czasu lub informacja o błędzie w przypadku negatywnej weryfikacji żądania przez KIR;
- przygotowany znacznik czasu lub komunikat o błędzie zostaje odesłany do subskrybenta tą samą drogą, którą zostało dostarczone przez subskrybenta żądanie wydania znacznika czasu;
- subskrybent lub odbiorca usług sprawdza poprawność otrzymanego znacznika czasu.

5.4. Żądanie wydania znacznika czasu

Znacznik czasu jest wydawany przez KIR w odpowiedzi na poprawne żądanie wydania znacznika czasu. Opis formatu żądania wydania znacznika czasu akceptowanego przez KIR określa Załącznik nr 2 do niniejszej Polityki. Żądanie wydania znacznika czasu powinno zawierać skrót dokumentu, do którego ma zostać wydany znacznik czasu, i być opatrzone podpisem elektronicznym weryfikowanym przy pomocy certyfikatu wydanego przez KIR lub bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu.

Bezpieczny podpis elektroniczny, jakim opatrywane jest żądanie wydania znacznika czasu oraz dane służące do składania i weryfikacji bezpiecznego podpisu elektronicznego powinny być tworzone przez subskrybenta zgodnie z wymaganiami ustawy o podpisie elektronicznym i rozporządzeniami wydanymi na podstawie ustawy.

6. OKRES WAŻNOŚCI ZNACZNIKÓW CZASU

Maksymalny okres ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji poświadczeń elektronicznych znaczników czasu wydanego przez ministra właściwego do spraw gospodarki lub podmiot przez niego wskazany wynosi 5 lat licząc od dnia wydania zaświadczenia.

Wydany przez KIR znacznik czasu jest ważny do końca okresu ważności zaświadczania certyfikacyjnego wydanego dla KIR wykorzystywanego do weryfikacji danego poświadczenia elektronicznego znacznika czasu. Jeżeli okres ważności lub przechowywania dokumentu, dla którego został wydany znacznik czasu, jest dłuższy, subskrybent powinien wystąpić o wydanie kolejnego znacznika czasu przed końcem okresu ważności zaświadczenia certyfikacyjnego, o którym mowa powyżej.

7. ZASADY IDENTYFIKACJI I UWIERZYTELNIANIA

Niniejszy rozdział reguluje procedury identyfikacji subskrybentów występujących o wydanie znaczników czasu.

7.1. Pierwsza rejestracja

Rozpoczęcie przez KIR świadczenia usług certyfikacyjnych polegających na znakowaniu czasem wymaga zawarcia z KIR umowy.

Po zawarciu umowy odbiorca usług powinien dostarczyć do KIR:

- listę subskrybentów upoważnionych do uzyskania znaczników czasu;
- listę certyfikatów, jakimi będą się posługiwali subskrybenci występujący o wydanie znaczników czasu.

7.2. Identyfikacja subskrybenta

Dane otrzymane od odbiorcy usług w procesie rejestracji są wykorzystywane do weryfikowania subskrybentów występujących z żądaniami wydania znaczników czasu.

Po otrzymaniu żądania weryfikowana jest poprawność żądania pod względem jego zgodności z formatem żądania wydania znacznika czasu określonym w Załączniku nr 2 do niniejszej Polityki. W przypadku niezgodności, żądanie wydania znacznika czasu jest odrzucane.

Po sprawdzeniu poprawności formatu żądania KIR sprawdza, czy subskrybent występujący o wydanie znacznika czasu jest upoważniony do otrzymania usługi i czy podpis elektroniczny, którym opatrzone jest żądanie wydania znacznika czasu, jest ważny. Do weryfikacji podpisu wykorzystywane są certyfikaty wskazane KIR przez odbiorcę usług w procesie rejestracji. Każdy z certyfikatów jest dodatkowo sprawdzany, czy nie został umieszczony na odpowiedniej dla danego certyfikatu liście CRL.

Żądanie wydania znacznika czasu jest również odrzucane w przypadku, gdy został przekroczony limit znaczników czasu ustalony z odbiorcą usług.

W przypadku, gdy weryfikacja znacznika czasu została zakończona niepowodzeniem, do subskrybenta przesyłany jest komunikat o błędzie.

8. TRYB TWORZENIA ORAZ UDOSTĘPNIANIA ZNACZNIKÓW CZASU

8.1. Algorytmy szyfrowe

KIR wydaje subskrybentom znaczniki czasu dla żądań o wydanie znaczników czasu wygenerowanych przy pomocy funkcji skrótu SHA-1.

8.2. Źródło czasu

Do świadczenia usługi znakowania czasem dokumentów elektronicznych KIR wykorzystuje własne zegary NTS-3000 firmy Elproma. KIR dysponuje dwoma zegarami NTS-3000, po jednym w każdym ośrodku. Zegary wykorzystywane do wydawania znaczników czasu są synchronizowane z Międzynarodowym Wzorcem Czasu (Universal Coordinated Time) na podstawie sygnału GPS docierającego do urządzenia z satelitów krążących wokół ziemi. Dokładność synchronizacji GPS wynosi +/-500 nanosekund. Każdy z zegarów udostępnia czas za pomocą trzech niezależnych interfejsów sieciowych wykorzystując protokoły przesyłania formatu czasu NTP oraz SNTP. Dokładność czasu na poziomie protokołu NTP wynosi +/- 10 milisekund. Wszystkie komputery wykorzystywane do świadczenia usługi znakowania czasem są automatycznie synchronizowane z wzorcem czasu Elproma NTS-3000.

8.3. Wydawanie znacznika czasu

KIR, wydając znacznik czasu, dołącza do danych zawartych w żądaniu wydania znacznika czasu, czas realizacji usługi. Tak przygotowane dane opatruje poświadczeniem elektronicznym, wykorzystując do tego celu bezpieczne urządzenie do składania podpisów elektronicznych. Poświadczenie elektroniczne składane przez KIR pod znacznikiem czasu jest generowane z wykorzystaniem algorytmu szyfrowego RSA i funkcji skrótu SHA – 1, których identyfikatory i charakterystykę określa załącznik nr 6 do niniejszej Polityki. Dane służące do składania poświadczenia elektronicznego wykorzystywane przez KIR mają długość 2048 bitów.

8.4. Publikacje informacji związanych z usługą znakowania czasem

Informacje dotyczące usług certyfikacyjnych polegających na znakowaniu czasem świadczonych przez KIR, w tym niniejsza Polityka, są udostępniane wszystkim zainteresowanym na stronie www.elektronicznypodpis.pl lub w siedzibie Krajowej Izby Rozliczeniowej S.A.

Zaświadczenia certyfikacyjne wydane dla KIR przez ministra właściwego do spraw gospodarki niezbędne do weryfikowania znaczników czasu są bezpłatnie udostępniane wszystkim zainteresowanym na stronie www.elektronicznypodpis.pl.

9. OPIS STRUKTURY ZNACZNIKA CZASU

W odpowiedzi na prawidłowe żądanie wydania znacznika czasu, KIR generuje znacznik czasu na podstawie źródła czasu, o którym mowa w pkt 8.2, i informacji zawartych w żądaniu. Znacznik czasu zawiera skrót dokumentu zawarty w żądaniu i czas aktualny z chwili generowania tego znacznika.

W przypadku niepoprawnego żądania lub innych przeszkód uniemożliwiających złożenie lub wydanie prawidłowego znacznika czasu, subskrybent otrzymuje informację o błędzie.

Składnia odpowiedzi i znacznika czasu zgodna jest z protokołem TSP zdefiniowanym w [RFC 3161] oraz [ETSI TS 101 861] i posiada następujący profil:

```
TimeStampResp ::= SEQUENCE  {
status                  PKIStatusInfo,
timeStampToken          TimeStampToken     OPTIONAL  }
```

Jeśli pole status wskazuje na błąd uniemożliwiający wygenerowania znacznika czasu, timeStampToken nie występuje.

```
PKIStatusInfo ::= SEQUENCE {
   status        PKIStatus,
   statusString  PKIFreeText     OPTIONAL,
   failInfo      PKIFailureInfo  OPTIONAL  }

PKIStatus ::= INTEGER {
   granted                (0),
   -- when the PKIStatus contains the value zero a TimeStampToken, as
      requested, is present.
   grantedWithMods        (1),
    -- when the PKIStatus contains the value one a TimeStampToken, with modifications, is present.
   rejection              (2),
   waiting                (3),
   revocationWarning      (4),
    -- this message contains a warning that a revocation is
    -- imminent
   revocationNotification (5)
    -- notification that a revocation has occurred   }

   -- When the TimeStampToken is not present
   -- failInfo indicates the reason why the
   -- time-stamp request was rejected and
   -- may be one of the following values.

PKIFailureInfo ::= BIT STRING {
   badAlg               (0),
     -- unrecognized or unsupported Algorithm Identifier
```

```
    badRequest          (2),
      -- transaction not permitted or supported
    badDataFormat       (5),
      -- the data submitted has the wrong format
    timeNotAvailable    (14),
      -- the TSA's time source is not available
    unacceptedPolicy    (15),
      -- the requested TSA policy is not supported by the TSA.
    unacceptedExtension (16),
      -- the requested extension is not supported by the TSA.
    addInfoNotAvailable (17)
      -- the additional information requested could not be understood
      -- or is not available
    systemFailure       (25)
      -- the request cannot be handled due to system failure  }

TimeStampToken ::= ContentInfo
     -- contentType is id-signedData ([CMS])
     -- content is SignedData ([CMS])

SignedData ::= SEQUENCE {
     version CMSVersion,
     digestAlgorithms DigestAlgorithmIdentifiers,
     encapContentInfo EncapsulatedContentInfo,
     certificates [0] IMPLICIT CertificateSet OPTIONAL,
     crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
     signerInfos SignerInfos }
```

W przypadku gdy w żądaniu pole certReq miało wartość TRUE, pole 'certificates' zawierać będzie certyfikat podmiotu świadczącego usługę oraz certyfikat atrybutu 'Time Attribute Certyfikat').

```
id-ct-TSTInfo  OBJECT IDENTIFIER ::= { iso(1) member-body(2)
   us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}

TSTInfo ::= SEQUENCE  {
   version                  INTEGER  { v1(1) },
   policy                   TSAPolicyId,
   messageImprint             MessageImprint,
     -- MUST have the same value as the similar field in
     -- TimeStampReq
   serialNumber               INTEGER,
    -- Time-Stamping users MUST be ready to accommodate integers
    -- up to 160 bits.
   genTime                   GeneralizedTime,
   accuracy                  Accuracy                 OPTIONAL,
   ordering                  BOOLEAN             DEFAULT FALSE,
   nonce                     INTEGER                  OPTIONAL,
     -- MUST be present if the similar field was present
     -- in TimeStampReq.  In that case it MUST have the same value.
   tsa                     [0] GeneralName          OPTIONAL,
   extensions                [1] IMPLICIT Extensions   OPTIONAL  }
```

10. SPOSÓB ZARZĄDZANIA DOKUMENTAMI ZWIĄZANYMI ZE ŚWIADCZENIEM USŁUG CERTYFIKACYJNYCH

Polityka jest udostępniana wszystkim zainteresowanym w postaci elektronicznej na stronie internetowej KIR pod adresem www.elektronicznypodpis.pl.

KIR przechowuje i archiwizuje dokumenty oraz dane w postaci elektronicznej, bezpośrednio związane ze świadczeniem usług certyfikacyjnych polegających na znakowaniu czasem, w sposób zapewniający bezpieczeństwo przechowywanych dokumentów i danych. Dostęp do dokumentów i danych związanych ze świadczeniem usługi znakowania czasem mają wyłącznie osoby upoważnione przez KIR, posiadające przeszkolenie w zakresie ochrony danych osobowych i dopuszczone do ich przetwarzania.

Dokumenty i dane w postaci elektronicznej są przechowywane w bazie danych osobowych systemu SZAFIR, zgłoszonej do rejestru prowadzonego przez Głównego Inspektora Ochrony Danych Osobowych. Przechowywanie odbywa się z wykorzystaniem technik zapewniających integralność danych zgodnie z wymaganiami ustawy o ochronie danych osobowych.

Przechowywaniu i archiwizacji przez okres 20 lat, od momentu utworzenia danego dokumentu i danych, podlegają:

- znaczniki czasu wydane przez KIR;
- zaświadczenia certyfikacyjne wydane dla KIR niezbędne do weryfikacji poprawności wydanych przez KIR znaczników czasu;
- umowy.

Przechowywaniu i archiwizacji przez okres 3 lat, od momentu utworzenia danych, podlegają rejestry zdarzeń związanych ze świadczeniem usługi znakowania czasem.

W przypadku zaprzestania przez KIR świadczenia usługi znakowania czasem dokumentów elektronicznych wszystkie wymienione powyżej dokumenty i dane będą przekazane do ministra właściwego do spraw gospodarki lub wskazanego przez niego podmiotu. Subskrybenci i odbiorcy usług nie będą ponosili żadnych kosztów z tytułu przekazania danych, o których mowa powyżej.

11. POUFNOŚĆ INFORMACJI I OCHRONA DANYCH OSOBOWYCH

KIR gwarantuje, że wszelkie informacje związane ze świadczeniem usług certyfikacyjnych w zakresie znakowania czasem dokumentów elektronicznych, w tym w szczególności dane osobowe odbiorców usług oraz subskrybentów, które nie zostały jednoznacznie zakwalifikowane jako jawne, podlegają ochronie przed ich ujawnieniem na zasadach określonych w obowiązujących przepisach prawa polskiego.

Ochronie podlegają informacje znajdujące się w posiadaniu KIR:

- wewnętrzne procedury dotyczące świadczenia usług certyfikacyjnych;
- klucze prywatne infrastruktury KIR wykorzystywanej do świadczenia usług certyfikacyjnych;
- archiwum, zapisy logów funkcjonowania systemu teleinformatycznego wykorzystywanego do świadczenia usług certyfikacyjnych;
- dane subskrybentów związane ze świadczeniem usługi znakowania czasem.

Przetwarzanie danych osobowych w KIR odbywa się na zasadach określonych w ustawie o ochronie danych osobowych i wydanych do niej przepisów wykonawczych. Każdej osobie, której dane osobowe są przetwarzane przez KIR w związku ze świadczeniem usługi znakowania czasem, przysługują uprawnienia wynikające z tej ustawy, z uwzględnieniem postanowień ustawy o podpisie elektronicznym.

12. ZABEZPIECZENIA TECHNICZNE I ORGANIZACYJNE

12.1. Ochrona fizyczna

Pomieszczenia, w których odbywa się przetwarzanie danych związanych z generowaniem znaczników czasu, podlegają ochronie fizycznej zgodnie z wymaganiami ustawy o podpisie elektronicznym i ustawy o ochronie danych osobowych. Zastosowane środki ochrony zabezpieczają przed:

- dostępem osób nieuprawnionych do pomieszczeń;
- skutkami naturalnych katastrof i zdarzeń losowych;
- pożarami;
- awarią infrastruktury;
- zalaniem wodą, kradzieżą, włamaniem i napadem.

Zastosowane środki ochrony fizycznej pomieszczeń obejmują między innymi:

- system kontroli dostępu do pomieszczeń;
- system ochrony przeciwpożarowej;
- system alarmowy klasy co najmniej SA3.

12.2. Zabezpieczenia techniczne

Dostęp do systemu teleinformatycznego, w ramach którego świadczone są usługi certyfikacyjne, jest zabezpieczony zgodnie z wymaganiami określonymi w ustawie o podpisie elektronicznym i przepisach wykonawczych do tej ustawy.

12.3. Ośrodek zapasowy

Na wypadek awarii podstawowego ośrodka uniemożliwiającej pracę KIR, prace systemu przejmuje zapasowy system zlokalizowany w siedzibie zapasowej. W przypadku awarii, zapasowy system na bieżąco przejmuje pracę związaną ze świadczeniem usługi znakowania czasem.

12.4. Zabezpieczenia kadrowe

Kadra zajmująca się świadczeniem usług certyfikacyjnych posiada kwalifikacje wymagane w ustawie o podpisie elektronicznym, a w szczególności wiedzę z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych.

Załącznik nr 1. Identyfikatory i wymagania dla algorytmów szyfrowych i funkcji skrótu

Lp	Algorytm	Identyfikator algorytmu	Wymagania
1.	RSA	{join-iso-ccitt(2) ds.(5) module (1) algorithm(8) encryptionAlgorithm(1) 1}	- minimalna długość klucza, rozumianego jako moduł p*q, wynosi 1020 bitów; - długości liczb pierwszych p i q, składających się na moduł, nie mogą się różnić więcej niż o 30 bitów.
2.	SHA – 1	{iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWAlgorithm(2) 26}	

Załącznik nr 2. Format żądania wydania znacznika czasu

Subskrybent występujący z żądaniem wydania znacznika czasu przygotowuje podpisane żądanie zgodnie ze składnią protokołu TSP wg [RFC 3161] oraz [ETSI TS 101 861] przy zastosowaniu następującego profilu wniosku:

Poza zdefiniowanym w RFC 3161 formatem żądania znacznika czasu zastosowany zostanie mechanizm podpisywania żądań zgodnie z CMS (PKCS#7) TimeStampReq. Akceptowane są wyłącznie żądania podpisane (CMS SignedData). Żądanie musi zawierać pojedynczy podpis elektroniczny. Żądanie musi zawierać certyfikat subskrybenta zgłaszającego żądanie o wygenerowanie znacznika czasu. Żądanie nie może zawierać innych certyfikatów. Żądanie nie może zawierać list CRL Wielkość żądania nie może przekroczyć maksimum ustalonego na 32000B.

```
TimeStampReqToken ::= ContentInfo
    -- contentType is id-signedData ([CMS])
    -- content is SignedData ([CMS])
```

SignedData będzie zawierało podpis elektroniczny zgodnie z CMS (PKCS#7) TimeStampReq.

```
SignedData ::= SEQUENCE {
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
    signerInfos SignerInfos }

TimeStampReq ::= SEQUENCE  {
  version                  INTEGER  { v1(1) },
  messageImprint           MessageImprint,
    --a hash algorithm OID = SHA-1 hash

  reqPolicy                TSAPolicyId              OPTIONAL,
  nonce                    INTEGER                  OPTIONAL,
  certReq                  BOOLEAN                  DEFAULT FALSE,
  extensions               [0] IMPLICIT Extensions  OPTIONAL  }

MessageImprint ::= SEQUENCE  {
  hashAlgorithm            AlgorithmIdentifier,
  hashedMessage            OCTET STRING  }

-- skrót z pliku musi być wykonany za pomocą algorytmu SHA1 (hashAlgorithm)

TSAPolicyId ::= OBJECT IDENTIFIER
```

Żądanie może nie zawierać identyfikatora polityki, jednak w przypadku, gdy go zawiera musi to być identyfikator polityki KIR. Żądania zawierające inny identyfikator polityki będą odrzucane.