Polityka Urzędu Znacznika Czasu

(Certum Time-Stamping Authority)

Wersja 1.1

Data: 26 listopada 2002

Status: poprzedni

Unizeto Sp. z o.o.
ul. Królowej Korony Polskiej 21
70-486 Szczecin
Polska
http://www.certum.pl

Klauzula: Prawa Autorskie

Wszelkie pytania związane z prawami autorskimi należy adresować do Unizeto Sp. z o.o., ul. Królowej Korony Polskiej 21, 70-486 Szczecin, Polska, tel. +48 91 4801 201, fax +48 91 4801 220, email: info@certum.pl.

Przedmowa

Dokument ten opracowano przy udziale wielu osób, w tym prawników, zespołu technicznego oraz specjalistów ds. bezpieczeństwa informacji. Dokument ten stanowi integralną część systemu wydawania i zarządzania wiarygodnymi znacznikami czasu.

Spis treści

Wstęp 1
1. Zakres tematyczny 1
2. Odnośniki literaturowe 1
3. Pojęcia i skróty 1
3.1. Pojęcia 1
3.2. Stosowane skróty 2
4. Założenia podstawowe 2
4.1. Serwis Znacznika Czasu (TSS) 2
4.2. Urząd Znacznika Czasu (TSA) 2
4.3. Subskrybenci 2
4.4. Zasady ogólne i polityka TSA 2
4.4.1. Przeznaczenie polityki 3
4.4.2. Szczegółowość polityki TSA 3
4.4.3. Ograniczenia polityki TSA 3
5. Polityka oznaczania czasem 4
5.1. Podstawowe informacje 4
5.2. Identyfikacja urzędu TSA 5
5.3. Przeznaczenie znaczników czasu 5
5.4. Zgodność z wymogami 5
6. Obowiązki i odpowiedzialność 6
6.1. Obowiązki TSA 6
6.1.1. Zobowiązania podstawowe 6
6.1.2. Zobowiązania wobec subskrybentów 6
6.2. Obowiązki subskrybentów 7
6.3. Obowiązki stron ufających 7
6.4. Odpowiedzialność finansowa 7
7. Wymagania dla TSA 7
7.1. Zasady funkcjonowania TSA 7
7.1.1. Zasady wydawania znaczników 7
7.1.2. Publikacja polityki TSA 7
7.2. Cykl życia klucza 7
7.2.1. Generowanie kluczy TSA 7
7.2.2. Ochrona kluczy TSA 7
7.2.3. Publikacja certyfikatów TSA 7
7.2.4. Aktualizacja kluczy TSA 7
7.2.5. Niszczenie kluczy TSA 7
7.2.6. Zarządzanie modułem kryptograficznym 7
7.3. Oznaczanie czasem 7
7.3.1. Żetony znacznika czasu 7
7.3.2. Synchronizacja zegara 7
7.4. Zarządzanie i funkcjonalność 7
7.4.1. Zarządzanie bezpieczeństwem 7
7.4.2. Klasyfikacja zagrożeń 7
7.4.3. Bezpieczeństwo personelu 7
7.4.4. Zabezpieczenia fizyczne 7
7.4.5. Procedury operacyjne 7
7.4.6. System kontroli dostępu 7

7.4.7. Zaufane środowisko 7
7.4.8. Ujawnienie kluczy TSA 7
7.4.9. Zakończenie działalności 7
7.4.10. Zgodność z wymogami prawa 7
7.4.11. Dzienniki zdarzeń TSA 7
7.5. Schemat organizacyjny 7
Historia dokumentu 7

Wstęp

Polityka Certyfikacji określa ogólne zasady stosowane przez Urząd Znacznika Czasu podczas wydawania żetonów (*ang. token*) zawierających podpisany znacznik czasu. Dokument ten definiuje uczestników tego procesu, określa ich obowiązki i odpowiedzialność oraz obszary zastosowań. Szczegółowy opis wspomnianych zasad przedstawiony jest w **Kodeksie Postępowania Certyfikacyjnego**[1]. Struktura i merytoryczna zawartość niniejszej polityki jest zgodna z zaleceniem ETSI[2]. Niniejsza polityka dotyczy usług oznaczania czasem świadczonych przez *Certum Time-Stmaping Authority* za pośrednictwem serwisu internetowego:

http://time.certum.pl

Znaczniki czasu wydawane zgodnie z niniejszą polityką znajdują zastosowanie przede wszystkim do zabezpieczania długoterminowych podpisów elektronicznych[3] oraz transakcji zawieranych w sieci globalnej. Dodatkowe informacje oraz pomoc serwisową można uzyskać pod adresem poczty elektronicznej: info@certum.pl.

1. Zakres tematyczny

Niniejszy dokument może zostać użyty przez strony ufające i subskrybentów urzędów certyfikacyjnych prowadzonych przez Unizeto Sp. z o.o. jako podstawa do potwierdzenia wiarygodności serwisów, stanowiących przedmiot niniejszego dokumentu. Polityka Urzędu Znacznika Czasu oparta jest o kryptografię klucza publicznego, wiarygodne źródła czasu oraz certyfikaty klucza publicznego.

2. Odnośniki literaturowe

Dokumenty normatywne i zalecenia, na podstawie których opracowano niniejszy dokument znajdują się w przypisach niniejszej polityki. Dodatkowe odnośniki do literatury fachowej znajdują się w **Kodeksie Postępowania Certyfikacyjnego**, w rozdziale „Literatura".

3. Pojęcia i skróty

3.1. Pojęcia

Żeton znacznika czasu (*ang. time-stamp token*) – element danych stosowany w procesie tworzenia podpisu elektronicznego i zawierający informację, która została przekształcona z wykorzystaniem technik kryptograficznych. Żeton taki jest podpisany jest przez Urząd Znacznika Czasu i stanowi niepodważalny dowód na to, że obiekt binarny, którego żeton dotyczy istniał przez datą podaną w żetonie.

---

[1] Aktualny Kodeks Postępowania Certyfikacyjnego jest dostępny pod adresem: https://www.certum.pl/CPS

[2] ETSI TS 102 023 V1.1.1 (2002-04), *Policy requirements for time-stamping authorities.*

[3] IETF RFC 3126, *Electronic Signature Formats for long term electronic signatures*, September 2001

Urząd Znacznika Czasu (*ang. time-stamping authority*) – zaufany system wydający i zarządzający żetonami znacznika wiarygodnego czasu.

Objaśnienia pozostałych pojęć znajdują się **Kodeksie Postępowania Certyfikacyjnego**, w dodatku „Słownik Pojęć".

3.2. Stosowane skróty

TSA	Urząd Znacznika Czasu
TSS	Serwis Znacznika Czasu
TST	żeton znacznika czasu
UTC	czas uniwersalny
PKI	Infrastruktura Klucza Publicznego

4.Założenia podstawowe

4.1. Serwis Znacznika Czasu (TSS)

Infrastruktura teleinformatyczna Unizeto Sp. z o.o. wydająca i zarządzająca żetonami znacznika czasu składa się z dwóch podstawowych komponentów:

- komponentu technicznego wydającego żetony znacznika czasu,
- logistyki systemu, zarządzającej, monitorującej i nadzorującej wydawanie żetonów znacznika czasu.

Logistyka systemowa zapewnia m.in. ciągłość dostępu do wiarygodnego źródła czasu UTC oraz prawidłowe zarządzanie komponentami programowymi systemu.

4.2. Urząd Znacznika Czasu (TSA)

Infrastruktura teleinformatyczna, o której mowa w § 4.1 „Serwis znacznika czasu" niniejszej polityki, która posiada zaufanie podmiotów, będących klientami Unizeto CERTUM oraz stron ufających związanych z ww. urzędem certyfikacyjnym.

4.3. Subskrybenci

Odbiorcami usług świadczonych przez urząd znacznika czasu są podmioty opisane w § 3 „Identyfikacja i uwierzytelnienie" **Kodeksu Postępowania Certyfikacyjnego**. Odbiorcami usług urzędu znacznika czasu, świadczonych w ramach Unizeto Sp. z o.o. mogą być też inne podmioty, w tym organizacje niedochodowe (*ang. non-profit*).

4.4. Zasady ogólne i polityka TSA

Niniejsza polityka Urzędu Znacznika Czasu stanowi cześć **Kodeksu Postępowania Certyfikacyjnego**, który reguluje zasady funkcjonowania Unizeto CERTUM oraz towarzyszących mu systemów niezaprzeczalności elektronicznej (*ang. non-repudiation*).

Urząd Znacznika Czasu wydaje żetony wszystkim zainteresowanym podmiotom bez żadnych ograniczeń natury technicznej. Ogólną zasadą jest nie pobieranie opłat od osób prywatnych i organizacji niedochodowych. Zasady odpłatności dla pozostałych podmiotów za ww. żetony opisane są w cenniku, znajdującym się na:

http://www.certum.pl/repozytorium

4.4.1. Przeznaczenie polityki

Niniejszy dokument przeznaczony jest do wiadomości publicznej. Dystrybucja niniejszego dokumentu jest ograniczona warunkami opisanymi w § 2.9 „Prawo do własności intelektualnej", **Kodeksu Postępowania Certyfikacyjnego**.

Zarządzanie zasobami ludzkimi oraz metody doboru kadry oraz bezpieczeństwo fizyczne systemu opisane jest również w ww. kodeksie.

4.4.2. Szczegółowość polityki TSA

Niniejszy dokument opisuje tylko ogólne zasady wydawania i zarządzania żetonami znacznika czasu. Szczegółowy opis systemu znajduje się dodatkowych dokumentach, które w większości nie są publiczne. Niepubliczne dokumenty, wraz z raportami, wynikami przeglądu sprzętu i wynikami kontroli wewnętrznych stanowią dokumentację, do której wgląd oprócz upoważnionego personelu posiada audytor *WebTrust*[4]. Wykaz ważniejszych dokumentów, stanowiących część dokumentacji audytorskiej, umieszczono w Tab. 1.

Tab.1 Ważniejsze dokumenty towarzyszące polityce TSA

L.p.	Nazwa dokumentu	Status	Sposób udostępniania
1	*Kodeks Postępowania Certyfikacyjnego*	*Jawny*	*https://www.certum.pl/CPS*
2	*Dokumentacja techniczna baz danych*	*Niejawny*	*Lokalnie - tylko uprawnione osoby oraz audytorzy*
3	*Procedura archiwizacji i niszczenia kluczy Unizeto CERTUM*	*Niejawny*	*Lokalnie - tylko uprawnione osoby oraz audytorzy*
4	*Procedury tworzenia kopii zapasowych i awaryjnego odtwarzania systemu Certum CA*	*Niejawny*	*Lokalnie - tylko uprawnione osoby oraz audytorzy*
5	*Procedury postępowania z modułem kryptograficznym*	*Niejawny*	*Lokalnie - tylko uprawnione osoby oraz audytorzy*
6	*Procedury generowania kluczy urzędu certyfikacji Unizeto CERTUM.*	*Niejawny*	*Lokalnie - tylko uprawnione osoby oraz audytorzy*
7	*Procedury wymiany oprogramowania serwerów Certum CA*	*Niejawny*	*Lokalnie - tylko uprawnione osoby oraz audytorzy*

4.4.3. Ograniczenia polityki TSA

Niniejsza polityka została opracowana w takim stopniu ogólności, który nie podaje szczegółów technicznych dotyczących systemu teleinformatycznego, struktury organizacyjnej, procedur operacyjnych czy zabezpieczeń fizycznych. Niniejsza polityka nie definiuje środowiska, w którym działa system wydawania żetonów znacznika czasu. Szczegóły techniczne i operacyjne

[4] *WebTrust Principles and Criteria for Certification Authorities* dostępne pod adresem: http://www.webtrust.org

Urzędu Znacznika Czasu zawarte są w **Kodeksie Postępowania Certyfikacyjnego** oraz dodatkowych dokumentach, przedstawionych w Tab. 1.

5. Polityka oznaczania czasem

5.1. Podstawowe informacje

Niniejsza polityka jest zbiorem zasad stosowanych podczas wydawania i zarządzania żetonami znacznika czasu oraz regulujących poziom bezpieczeństwa dla systemu TSA. Ogólne zasady funkcjonowania systemu wydawania żetonów znacznika czasu omówione zostały w § 4.4 „Zasady ogólne i polityka TSA" niniejszego dokumentu.

Żetony znacznika czasu wydawane są z dokładnością większą niż 1s.

Profil certyfikatu klucza publicznego, którym posługuje się Urząd Znacznika Czasu jest zgodny z zaleceniami IETF[5]. Rozszerzenia, jakie posiada certyfikat wystawiony przez nadrzędny urząd certyfikacyjny **CA-Certum** opisane są w § 7.1.2.6 „Certyfikaty wzajemne i certyfikaty dla potrzeb usług niezaprzeczalności" **Kodeksu Postępowania Certyfikacyjnego**. Profil podstawowych pól certyfikatu urzędu TSA został przedstawiony w Tab. 2.

Tab.2 Profil podstawowych pól certyfikatu

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Number	Unikalna wartość we wszystkich certyfikatach CA-Certum	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Common Name (CN) =	Certum Time-Stamping Authority
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto Sp. z o.o. posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar ten jest znany jako ogólnoświatowe wiarygodne źródło usług czasu klasy Stratum I.	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto Sp. z o.o. posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar ten jest znany jako ogólnoświatowe wiarygodne źródło usług czasu klasy Stratum I.	
Subject (nazwa DN)	Nazwa DN jest zgodna z wymaganiami X.501.	
Subject Public Key Info	Pole kodowane jest zgodne z wymaganiami określonymi w RFC 2459 i zawiera informacje o kluczu publicznym RSA. Długość klucza w bitach wynosi 2048	
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 2459.	

[5] IETF RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, August 2001

Urząd znacznika czasu, świadczący usługi w ramach infrastruktury Unizeto CERTUM wydaje znaczniki czasu zgodnie z zaleceniami ETSI[6]. Wszystkie znaczniki czasu zawierają identyfikator polityki urzędu[7], opisany w § 5.2 „Identyfikacja urzędu TSA" niniejszej polityki.

5.2. Identyfikacja urzędu TSA

Informacja (identyfikator) polityki, wg której realizowane są usługi wydawania i zarządzania znacznikami czasu została zdefiniowana w Tab. 3.

Tab.3 Identyfikator polityki TSA

Identyfikator polityki	Nazwa polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-tsa(5))[8]	Certum Time-Stamping Authority Identyfikuje politykę urzędu znacznika czasu, świadczącego usługi w ramach CA-Certum.

Identyfikator polityki urzędu TSA, świadczącego usługi w ramach infrastruktury klucza publicznego Unizeto CERTUM umieszczany jest w każdym znaczniku czasu. Polityka ta jest udostępniana stronom ufającym i klientom Unizeto CERTUM według zasad opisanych w § 4.4.2 „Szczegółowość polityki TSA" niniejszego dokumentu.

5.3. Przeznaczenie znaczników czasu

Dokument ten nie definiuje ograniczeń stosowalności żetonów znacznika czasu, wydawanych w ramach niniejszej polityki. Urząd Znacznika Czasu może świadczyć publiczne usługi oznaczania wiarygodnym czasem: transakcji elektronicznych, formularzy, archiwizowanych danych, dzienników systemowych, podpisów elektronicznych opisanych w dokumencie IETF[3], itp. Urząd Znacznika Czasu opcjonalnie świadczy usługi dla zamkniętych systemów korporacyjnych. Znaczniki czasy wydawane przez *Certum Time Stamping Authority* znajdują również zastosowanie w technologii Microsoft Authenticode, jako kontrasygnata urzędu znacznika czasu.

5.4. Zgodność z wymogami

Wydawane znaczniki czasu zawierają identyfikatory opisane § 5.2 „Identyfikacja urzędu TSA" niniejszego dokumentu. Urząd TSA obsługuje tylko żądania zawierające znacznik niniejszej polityki bądź nie zawierają go w ogóle. W przypadku notaryzacji transakcji elektronicznych dopuszcza się obsługę kryptograficznych funkcji skrótów[9] jako żądań znacznika wiarygodnego czasu.

Urząd Znacznika Czasu gwarantuje zgodność świadczonych usług z § 6.1 „Obowiązki TSA" oraz gwarantuje niezawodność mechanizmów kontrolnych opisanych w § 7 „Wymagania dla TSA" niniejszej polityki.

---

[6] ETSI TS 101 861,*Time stamping profile*, August 2001

[7] Nie dotyczy to znaczników wydawanych w technologii Microsoft Authenticode

[8] identyfikator obiektu Cetum CA: {iso(1) member-body(2) pl(616) organization(1) unizeto(113527) ccert(2) certum(2)}.

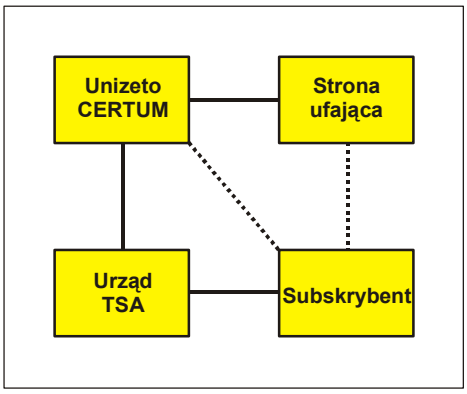
[9] NIST FIPS PUB 180-1, *Secure Hash Standard*, April 17, 1995

6. Obowiązki i odpowiedzialność

6.1. Obowiązki TSA

6.1.1. Zobowiązania podstawowe

W rozdziale tym przedstawione są zobowiązania, gwarancje i odpowiedzialność urzędu TSA, subskrybentów oraz użytkowników znaczników czasu (stron ufających). Zobowiązania te oraz odpowiedzialność regulowane są przez wzajemne umowy zawierane pomiędzy wymienionymi stronami (rys.1).



Rys.1 Umowy zawierane pomiędzy stronami

Umowy Unizeto CERTUM (w tym urzędu Certum TSA) ze stronami ufającymi oraz subskrybentami opisują wzajemne zobowiązania oraz odpowiedzialności, w tym odpowiedzialności finansowe Unizeto Sp. z o.o.

Kodeks Postępowania Certyfikacyjnego i Polityka Certyfikacji TSA są integralną częścią umów zawieranych między Unizeto CERTUM a subskrybentami, stronami ufającymi lub innymi podmiotami, które są dostawcami usług infrastruktury klucza publicznego w tym znacznika czasu.

Unizeto Sp. z o.o. gwarantuje, że wszystkie wymagania Urzędu Znacznika Czasu, w tym procedury, praktyki związane z wydawaniem znaczników, przeglądy systemu i audytu bezpieczeństwa są zgodne z opisem w § 7 „Wymagania dla TSA".

Urząd TSA działa zgodnie z ww. procedurami i nie dopuszcza się odstępstw od ich stosowania. Dodatkowe zobowiązania urzędu, subskrybentów i stron ufających zostały opisane w § 2.1 „Zobowiązania" **Kodeksu Postępowania Certyfikacyjnego**.

6.1.2. Zobowiązania wobec subskrybentów

Unizeto Sp. z o.o. gwarantuje ciągły dostęp do serwisów urzędu Certum TSA, w trybie 24/7/365 z wyłączeniem przewidzianych w oddzielnych dokumentach, przerw technologicznych, związanych z konserwacją sprzętu i systemu. Czas UTC, który zostaje umieszczony w żetonie znacznika czasu, podawany jest z dokładnością ±100 ms. Serwis gwarantuje zachowanie sprawności i dokładności przy wielu równocześnie podłączonych klientach. W przypadku dużego

obciążenia serwisu (ponad 2000 jednocześnie podłączonych klientów) dokładność ta może się zmienić do ±200 ms. Unizeto Sp. z o.o. gwarantuje ponadto, że:

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie tworzące system, który spełnia wymagania określone w CWA[10],
- jego działalność i świadczone usługi są zgodne z prawem, a w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami, opisanymi w § 5.1 „Podstawowe informacje" niniejszej polityki,
- wystawiane żetony nie zawierają żadnych sfałszowanych danych ani błędów.

Dodatkowe informacje definiujące zobowiązania Unizeto CERTUM zostały opisane w § 2.1.1 „Zobowiązania Unizeto CERTUM – CCP" **Kodeksu Postępowania Certyfikacyjnego**.

6.2. Obowiązki subskrybentów

Subskrybent pobierający żeton znacznika czasu, powinien zweryfikować podpis cyfrowy urzędu oraz sprawdzić listę CRL, pod kątem unieważnienie certyfikatu urzędu TSA. Aktualna lista CRL znajduje się zawsze pod adresem http://crl.certum.pl/ca.crl. Weryfikacji identyfikatora urzędu TSA można dokonać również za pośrednictwem serwisu OCSP, świadczącego usługi pod adresem http://ocsp.certum.pl. Dodatkowe obowiązki subskrybenta, wynikające z faktu odbioru usług znacznika czasu opisane zostały w § 2.1.3 „Zobowiązania subskrybenta końcowego" **Kodeksu Postępowania Certyfikacyjnego**.

6.3. Obowiązki stron ufających

Podstawowym obowiązkiem strony ufającej, jest weryfikacja podpisu pod żetonem, zawierającym znacznik czasu. Strona ufająca powinna sprawdzić ważność certyfikatu urzędu, oraz okres jego ważności. W przypadku weryfikacji znaczników czasu, po upływie ważności certyfikatu urzędu TSA strony ufające powinny:

- zweryfikować czy identyfikator urzędu TSA nie znajduje się na liście CRL,
- sprawdzić, czy kryptograficzna funkcja skrótu zastosowana w znaczniku w dalszym ciągu jest niekolizyjna (funkcja uznawana jest w dalszym ciągu za bezpieczną funkcję skrótu),
- upewnić się, że długości klucza kryptograficznego TSA, oraz stosowany przez urząd algorytm podpisu jest w dalszym ciągu uznawany za bezpieczny.

Niniejsza polityka nie precyzuje ograniczeń odnośnie użytkowania żetonów znacznika czasu, poza ogólnymi warunkami określonymi w umowie (patrz Załącznik 1.). Pozostałe wymagania stawiane stronom ufającym zostały opisane w § 2.1.4. „Zobowiązania stron ufających" **Kodeksu Postępowania Certyfikacyjnego**.

[10] CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*

6.4. Odpowiedzialność finansowa

Odpowiedzialność jednostki usługowej Certum TSA oraz stron powiązanych przez usługi świadczone przez tą jednostkę, wynika z rutynowych czynności wykonywanych przez te podmioty lub z czynności stron trzecich. Odpowiedzialność każdego z podmiotów jest określona w umowach dwustronnych lub wynika ze złożonych oświadczeń woli. Górne wartości odpowiedzialności finansowej Urzędu Znacznika Czasu, zestawiono w Tab. 3.

Tab.3 Maksymalne gwarancje finansowe

Nazwa polityki	Typ podmiotu	
	Osoba prywatna	Klient komercyjny
Certum Time-Stamping Authority (OID: 1.2.616.1.113527.2.2.5)	20 000 zł*	20 000 zł*

* - od subskrybentów, którzy nie zawarli stosownych umów z Urzędem Znacznika Czasu, Unizeto Sp. z o.o. będzie domagać się wysokich odszkodowań w procesach cywilnych. Zapis ten nie dotyczy podmiotów korzystających z oznaczania czasem w technologii Microsoft Authenticode.

Pozostałe gwarancje finansowe oraz zasady, na których są one udzielane zdefiniowane zostały w § 2.3 „Odpowiedzialność finansowa" **Kodeksu Postępowania Certyfikacyjnego**. Oznaczanie czasem obiektów dla potrzeb technologii Microsoft Authenticode zwolnione jest z opłat licencyjnych oraz obowiązku zawierania umów z Unizeto Sp. z o.o. przez klientów komercyjnych, organizacje niekomercyjne czy przez osoby prywatne.

7. Wymagania dla TSA

Urząd Znacznika Czasu posiada zaimplementowane mechanizmy kontrolne, umożliwiające świadczenie usług niezaprzeczalności zgodnie z zasadami niniejszej polityki. W celu nadzoru nad sprawnym działaniem systemu znakowania wiarygodnym czasem, rozliczania użytkowników oraz personelu ze swoich działań rejestrowane są wszystkie zdarzenia, występujące w systemie.

Wymaga się, aby każda ze stron, w jakikolwiek sposób powiązana z procedurami oznaczania wiarygodnym czasem, dokonywała rejestracji informacji i zarządzała nią adekwatnie do pełnionych obowiązków. Zapisy zarejestrowanej informacji tworzą tzw. dziennik zdarzeń i muszą być tak przechowywane, aby umożliwiały stronom dostęp do odpowiedniej i niezbędnej w danej chwili informacji, towarzyszyły przy rozstrzyganiu sporów pomiędzy stronami oraz pozwalały na wykrywanie prób włamań do systemu teleinformatycznego. Rejestrowane zdarzenia podlegają procedurom kopiowania. Kopie przechowywane są poza siedzibą Unizeto Sp. z o.o. Rodzaj rejestrowanych zdarzeń znajduje się w § 4.10.1 „Typy rejestrowanych zdarzeń" **Kodeksu Postępowania Certyfikacyjnego**.

7.1. Zasady funkcjonowania TSA

7.1.1. Zasady wydawania znaczników

Procedury, mechanizmy kontrolne i infrastruktura techniczna, opisane w § 6 „Obowiązki i odpowiedzialność" stanowią podstawy funkcjonowanie urzędu TSA. Pozostałe mechanizmy regulowane są przez **Kodeks Postępowania Certyfikacyjnego**, a w szczególności przez § 6.6.1. „Kontrola zmian systemu" oraz § 6.6.3 „Ocena cyklu zycia zabezpieczeń".

Ocena ryzyka, której następstwem są procedury bezpieczeństwa zostały opisane w § 6.5.1 „Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych", **Kodeksu Postępowania Certyfikacyjnego**.

Polityka Urzędu Znacznika Czasu jest częścią Kodeksu Postępowania Certyfikacyjnego, który wraz z towarzyszącymi mu dokumentami wewnętrznymi reguluje zasady funkcjonowania serwisu oznaczania wiarygodnym czasem.

Kodeks Postępowania Certyfikacyjnego reguluje zobowiązania podmiotów zewnętrznych, związanych z systemem wydawania znaczników czasu. Kodeks Postępowania Certyfikacyjnego oraz Polityka Urzędu Znacznika Czasu są dokumentami publicznymi, ogólnie dostępnymi na zasadach opisanych w § 2.9 „Prawo do własności intelektualnej" **Kodeksu Postępowania Certyfikacyjnego**.

Nad opracowaniem zasad i procedur, ich zmianami oraz dalekosiężnymi planami biznesowymi czuwa Zespół ds. Rozwoju Usług PKI. W skład zespołu wchodzą przedstawiciele zarządu Unizeto Sp. z o.o., konsultanci PKI, inżynierowie systemowi i prawnicy. Kontakt z ww. zespołem został zdefiniowany w § 1.5.1 „Dane jednostki administrującej Kodeksem" **Kodeksu Postępowania Certyfikacyjnego**.

Zgodność zasad funkcjonowania urzędu TSA ze stosowanymi w rzeczywistości praktykami reguluje § 2.7. „Audyt" **Kodeksu Postępowania Certyfikacyjnego**. Regulacje zmian w Kodeksie Postępowania Certyfikacyjnego lub niniejszej polityce opisane są w § 8.1. „Procedurze wprowadzania zmian", natomiast proces zatwierdzania zmian reguluje § 8.3. „Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego" ww. Kodeksu.

7.1.2. Publikacja polityki TSA

Kodeks Postępowania Certyfikacyjnego oraz Polityka Urzędu Znacznika Czasu są dokumentami publicznymi, ogólnie dostępnymi na zasadach opisanych w § 7.1.1 „Zasady wydawania znaczników".

Kontakt informacyjny w sprawach niniejszego dokumentu reguluje § 1.5.1 „Dane jednostki administrującej Kodeksem" **Kodeksu Postępowania Certyfikacyjnego**. Każdy żeton znacznika czasu, wydawany przez urząd Certum TSA posiada identyfikator polityki, zdefiniowany w § 5.2 „Identyfikacja urzędu TSA". Kryptograficzne funkcje skrótu, stosowane w procesie oznaczania wiarygodnym czasem są zgodne z wymaganiami normatywnymi NIST[8]. Zakładany czas ważności żetonu znacznika czasu wynosi 10 lat od chwili upływu ważności identyfikatora urzędu, przy założeniu, że nie wystąpią sytuacje opisane w § 6.3 „Obowiązki stron ufających". Dokładność czasu, który podawany jest w żetonie ze znacznikiem reguluje § 6.1.2 „Zobowiązania wobec subskrybentów" niniejszej polityki.

Ograniczenia związane z systemem urzędu TSA zdefiniowano w § 5.3 „Przeznaczenie znaczników czasu" niniejszej polityki. Zobowiązania subskrybentów opisano w § 6.2 „Obowiązki subskrybentów" niniejszej polityki. Zobowiązania stron ufających określono w § 6.3 „Obowiązki stron ufających" niniejszej polityki. Weryfikacja żetonu zawierającego znacznik czasu powinna

być prowadzona przy pomocy oprogramowania zdefiniowanego w § 1.4.2 „Rekomendowane aplikacje" **Kodeksu Postępowania Certyfikacyjnego**. Dzienniki systemowe podlegają archiwizacji przez okres czasu zdefiniowany w § 4.11.3 „Okres przechowywania archiwum" **Kodeksu Postępowani Certyfikacyjnego**. Certum TSA podlega regulacjom prawnym na terenie Rzeczypospolitej Polskiej. Odpowiedzialność finansowa urzędu TSA została zdefiniowana w § 6.4 „Odpowiedzialność finansowa" niniejszej polityki.

Skargi, wnioski i uwagi odnośnie funkcjonowania urzędu Certum TSA powinny być kierowane do kolegium zdefiniowanego w § 1.5.1 „Dane jednostki administrującej Kodeksem" **Kodeksu Postępowania Certyfikacyjnego**. Regulacje dotyczące tworzenia kopii zapasowych znajdują się w § 4.11 „Archiwizowanie danych" **Kodeksu Postępowania Certyfikacyjnego**. Certum TSA posiada ośrodek zapasowy na wypadek katastrofy oraz procedury regulujące zasady odtwarzania systemu. Aktualna wersja polityki Urzędu Znacznika Czasu jest publikowana elektronicznie w repozytorium, znajdującym się pod adresem:

http://www.certum.pl/repozytorium

7.2. Cykl życia klucza

7.2.1. Generowanie kluczy TSA

Klucze urzędu znacznika czasu są generowane przy użyciu sprzętowych modułów kryptograficznych, posiadających certyfikaty bezpieczeństwa NIST FIPS 140-1 level 3, przez zaufany personel ze zdefiniowanymi, zaufanymi rolami. Opis zasad regulujących dobór personelu przedstawiono w § 5.3 „Kontrola personelu" **Kodeksu Postepowania Certyfikacyjnego**. Środowisko w którym generowane są klucze urzędu, jest zgodne z zaleceniami dla zaufanych systemów operacyjnych[11] i spełnia wymagania EAL4[12]. Algorytm kluczy urzędu TSA opisano w § 5.1 „Podstawowe informacje" niniejszej polityki.

7.2.2. Ochrona kluczy TSA

Zasady odtwarzania kluczy kryptograficznych urzędu, na wypadek katastrofy, awarii systemu bądź konserwacji sprzętu opisano w osobnych dokumentach, wchodzących w skład dokumentacji Unizeto CERTUM i weryfikowanych okresowo przez audytora. Okoliczności towarzyszące generowaniu kluczy urzędu oraz zasady generowania kluczy opisane zostały w § 6.2. „Ochrona klucza prywatnego" **Kodeksu Postępowania Certyfikacyjnego**. Poziom bezpieczeństwa środowiska oraz sprzetowe moduły kryptograficzne opisano w § 7.2.1 „Generowanie kluczy TSA" niniejszej polityki.

7.2.3. Publikacja certyfikatów TSA

Certyfikaty urzędu TSA, wraz z towarzyszącymi im kluczami publicznymi publikowane są w oprogramowaniu, w tym w przeglądarkach internetowych. Dodatkowo, klucze te są publikowane na stronach internetowych pod adresem http://www.certum.pl. Klucze publiczne Urzędu Znacznika Czasu są podpisywane przez nadrzędny urząd certyfikacyjny **CA-Certum**. Dodatkowe informacje dotyczące publikowania certyfikatów klucza publicznego znajdują się w § 6.1.4 „Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym" **Kodeksu Postępowania Certyfikacyjnego**.

[11] http://www.nsa.gov

[12] ISO 15408

7.2.4. Aktualizacja kluczy TSA

Wymiana kluczy urzędu znacznika czasu następuje po upływie terminu ich ważności. Klucze te są następnie archiwizowane przez okres 5 lat, a następnie zniszczone. Klucz publiczny urzędu jest jeszcze przechowywany przez 20 lat, w celu weryfikacji wcześniej wystawionych znaczników czasu. Archiwizację kluczy opisano w § 6.2.5 „Archiwizacja klucza prywatnego", **Kodeksu Postępowania Certyfikacyjnego**.

7.2.5. Niszczenie kluczy TSA

Niszczenie kluczy urzędu opisane zostało w § 6.2.9 „Metody niszczenia klucza prywatnego" **Kodeksu Postępowania Certyfikacyjnego**. Dodatkowe informacje znajdują się w § 7.2.4 „Aktualizacja kluczy TSA" niniejszej polityki. System wydawania znaczników czasu, świadczący usługi w ramach Unizeto CERTUM odrzuca wnioski, w przypadku próby użycia przeterminowanych kluczy.

7.2.6. Zarządzanie modułem kryptograficznym

Moduły kryptograficzne, przeznaczone do świadczenia usług niezaprzeczalności, w tym oznaczania czasem dostarczane są przez producenta bezpośrednio do Unizeto Sp. z o.o. za pośrednictwem zaufanych firm kurierskich. Bezpośrednio po dostarczeniu sprawdzane są plomby producenta. Moduł jest następnie przekazywany do Unizeto CERTUM, jednostki, która zarządza systemami PKI w firmie Unizeto Sp. z o.o. Tutaj następuje kolejna weryfikacja plomb urządzenia, wykonywane są podstawowe testy modułu i wprowadzenie na stan. Moduł jest przechowywany w sejfie, do którego dostęp, ze względu na jego konstrukcje musi mieć dwoje ludzi. Ze wszystkich ww. operacji jest sporządzony raport.

Instalacja i uruchomienie modułu kryptograficznego prowadzona jest przez zaufany personel, w obecności świadków. Następnie wykonywane są testy funkcjonalności serwisu w oparciu o nowy moduł. W przypadku wycofania modułu z użytku lub przekazania modułu w celach serwisowych, klucze w module są niszczone zgodnie z dokumentacją producenta. Unizeto CERTUM posiada oddzielne procedury, regulujące zasady postępowania z modułem kryptograficznym. Procedury te nie są dostępne publicznie, lecz stanowią część dokumentacji kontrolowanej przez audytora.

7.3. Oznaczanie czasem

7.3.1. Żetony znacznika czasu

Każdy znacznik czasu, wydawany przez Certum TSA, posiada identyfikator polityki, o którym mowa w § 5.2 „Identyfikacja urzędu TSA" niniejszej polityki. W każdym żetonie ze znacznikiem czasu znajduje się unikalny identyfikator. Znaczniki czasu, wydawane przez Certum TSA zawierają czas i datę pobieraną z wiarygodnego źródła czasu UTC, zegarem podstawowym jest ntp.certum.pl (odbiornik satelitarny oraz atomowy wzorzec sekundy PPS). Urząd TSA posiada zegary zapasowe, na wypadek awarii zegara satelitarnego. Dokładność czasu, który jest umieszczany w znacznikach zdefiniowana jest w niniejszej polityce § 6.1.2 „Zobowiązania wobec subskrybentów", i nie jest konieczne umieszczenie tej informacji w żetonach znacznika czasu.

W przypadku awarii, bądź rozkalibrowania zegara podstawowego, system TSA pobiera czas z zegara zapasowego. Jeżeli zegar zapasowy ulegnie rozregulowaniu, uniemożliwiającemu podanie czasu z dokładnością opisaną w § 6.1.2 „Zobowiązania wobec subskrybentów" niniejszej polityki, znaczniki czasu nie powinny być wydawane.

Znaczniki czasu wydawane są na podstawie danych, dostarczanych przez podmioty zgłaszające żądanie TSQ. Żetony TSR zawierają w odpowiedzi (w znaczniku czasu) dane z żądania TSQ. Żądaniem może być też kryptograficzna funkcja skrótu, opisana w standardzie NIST[8]. Znaczniki czasu są podpisywane kluczem, którego certyfikat posiada profil i rozszerzenia określone w § 5.1 „Podstawowe informacje" niniejszej polityki. Znaczniki czasu posiadają identyfikatory, które jednoznacznie wiążą je z **Certum TSA** i są zgodne z wymogiem ETSI § 7.3.1h) „Time-stamp token".

7.3.2. Synchronizacja zegara

Zegar Certum TSA umieszcza czas w żetonach znacznika czasu z dokładnością podaną w § 6.1.2 „Zobowiązania wobec subskrybentów" niniejszej polityki. Kalibracja zegara włącza się automatycznie, po wykryciu rozbieżności większej niż ±100 ns, między czasem uniwersalnym UTC a zegarem podstawowym. Unizeto Sp. z o.o. posiada mechanizmy zabezpieczające przed niepowołanym działaniem, którego celem jest rozsynchronizowanie zegara, manipulacja przy nim bądź fizyczne zniszczenie zegara.

Unizeto Sp. z o.o. posiada mechanizmy pozwalające wykryć rozbieżności między czasem zegara a czasem podawanym w znaczniku czasu. Przeliczanie czasu jest zgodne z zaleceniami BIPM[13] oraz NTP[14].

7.4. Zarządzanie i funkcjonalność

7.4.1. Zarządzanie bezpieczeństwem

Zagadnienia zawiązane z zarządzaniem bezpieczeństwa opisano w § 5.2 „Kontrola zabezpieczeń organizacyjnych" **Kodeksu Postępowania Certyfikayjnego**.

7.4.2. Klasyfikacja zagrożeń

Opis metod i środków podjętych w celu zapewnienia ciągłości i stabilność pracy systemu Certum TSA opisano w § 5.1.1 „Nadzór nad bezpieczeństwem fizycznym Unizeto CERTUM – CCP" **Kodeksu Postępowania Certyfikacyjnego**.

7.4.3. Bezpieczeństwo personelu

Charakterystyka personelu, zaufane role jakie mu przydzielono opisano w § 5.3 „Kontrola personelu" **Kodeksu Postępowania Certyfikacyjnego**.

7.4.4. Zabezpieczenia fizyczne

Opis zabezpieczeń fizycznych, w tym zabezpieczenia przeciwpożarowe, antywłamaniowe, monitoring, kontrola dostępu itp. pisano w § 5 „Kontroli zabezpieczeń fizycznych, organizacyjnych oraz personelu" **Kodeksu Postępowania Certyfikacyjnego**. Zabezpieczenia te są zgodne z wymogami normatywnymi ISO[15].

---

[13] Bureau International des Poids et Mesures, http://www.bipm.org

[14] Network Time Protocol, http://www.ntp.org

[15] ISO/IEC 17799

7.4.5. Procedury operacyjne

System Certum TSA posiada zabezpieczenia proceduralne, zgodne z wymogami WebTrust[4] oraz ETSI[3]. Dokumenty te stanowią większości wewnętrzną dokumentację, nie publikowaną na zewnątrz, audytorowi jedynie przedstawianą audytorowi podczas okresowych przeglądów systemu.

7.4.6. System kontroli dostępu

Zagadnienia kontroli dostepu opisano w § 5.1.1.2 „Dostęp fizyczny" **Kodeksu Postępowania Certyfikacyjnego**.

7.4.7. Zaufane środowisko

Generowanie kluczy Certum TSA ma miejsce zawsze w zaufanym środowisku, opisanym w § 7.2.1 „Generowanie kluczy TSA". System produkcyjny spełnia wymogi bezpieczeństwa EAL411. Wszelkie zmiany w systemie są monitorowane i rejestrowane w dziennikach zdarzeń.

7.4.8. Ujawnienie kluczy TSA

W przypadku ujawnienia kluczy urzędu Certum TSA zastosowanie znajdują mechanizmy opisane w § 4.13 Kompromitacja i uruchamianie po awariach oraz klęskach żywiołowych" **Kodeksu Postępowania Certyfikacyjnego**.

7.4.9. Zakończenie działalności

W przypadku zaprzestania działalności uruchamiane zostają mechanizmy opisane w § 4.14 „Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji" **Kodeksu Postępowania Certyfikacyjnego**.

7.4.10. Zgodność z wymogami prawa

System Certum TSA działa zgodnie z wymogami polskiego prawa oraz wymogami normatywnymi, zdefiniowanymi w § 7.4.10 „Compliance with Legal Reguirements" dokumentu ETSI.

7.4.11. Dzienniki zdarzeń TSA

System Certum TSA posiada mechanizmy pozwalające na zarejestrowanie wszystkich zdarzeń, które towarzyszą wydaniu znacznika czasu. Informacje o typach zdarzeń, metodach ich archiwizacji itp. opisano w § 4.10 „Rejestrowanie zdarzeń oraz procedury audytu" **Kodeksu Postępowania Certyfikacyjnego**.

7.5. Schemat organizacyjny

Certum TSA wchodzi w skład Unizeto Sp. z o.o. Działalność zarejestrowano na terenie Rzeczypospolitej Polskiej. NIP: 852-000-64-44, adres ul. Królowej Korony Polskiej 21, 70-486 Szczecin. Tel. +48 91 4801 201. Kontakt elektroniczny: info@certum.pl.

Strukturę organizacyjną firmy przedstawiono w dokumencie *„Struktura organizacyjna Unizeto Sp. z o.o."*.

Historia dokumentu

Historia zmian dokumentu		
v1.0	05 września 2002 r.	Pierwsza wersja Polityki.
v1.1	26 listopada 2002 r.	Rozszerzenie usługi o wsparcie dla technologii Microsoft Authenticode oraz informacja o zmiany w pramatetrach zegarów atomowych. Dodano informacje dotyczące lokalizacji serwisu internetowego TSA.