Wizja

v. 1.00.01p

data wydania: 2019-03-08

HISTORIA ZMIAN		
Numer Wersji	**Data**	**Opis Zmian**
1.00.00p	2019-03-09	Wersja inicjalna
1.00.01p	2019-03-09	W poprzedniej wersji dokument opisywał zarówno strefę biznesową (tzw. komercyjną) jaki i minimalną strefę biznesową. Obecna wersja skupiła opisuje jedynie minimalna strefę biznesową, co pociągnęło za sobą znaczącą zmianę całego dokumentu. Kolejną ważna zmianą jest zmiana nazwy „strefa kryptograficzna” na „strefa operacyjna”. Nazwę tę zmieniono ze względu na występowanie operacji kryptograficznych także w części biznesowej, co mogło prowadzić do pewnych nieporozumień.

1 Wstęp

1.1 Cel

Celem tego dokumentu jest zebranie, analiza i zdefiniowanie, na dużym poziomie abstrakcji, potrzeb i cech systemu wspomagającego świadczenie usług certyfikacyjnych. Skupia się on na możliwościach, które system będzie oferował osobom zainteresowanym jego realizacją oraz przyszłym jego użytkownikom.

1.2 Zakres

Niniejszy dokument ma zastosowanie dla planowanego przez ZUT Szzcecin systemu wspomagającego świadczenie usług certyfikacyjnych, pod roboczą nazwą Integrated Certification Authority Software (ICAS).

1.3 Definicje, Akronimy i Skróty

- Usługi podstawowe – usługi certyfikacyjne związane z wydawaniem certyfikatów oraz zarządzanie ich cyklem życia (unieważnianie, zawieszanie oraz odwieszanie certyfikatów).
- Usługi dodatkowe – usługi certyfikacyjne związane z weryfikacją statusu certyfikatu w trybie on-line (OCSP), znakowaniem czasem (TSA), kurierem elektronicznym (DA) oraz serwerem poświadczeń (DVCS).

1.4 Referencje

[1] Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym.
[2] Rozporządzenie 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.
[3] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

1.5 Streszczenie

W rozdziale 2 znajduje się opis obecnej sytuacji w Unizeto Technologies S.A. związanej ze świadczeniem usług certyfikacyjnych. W rozdziale tym zawarte są także informacje na temat podziału projektu ICAS na dwa projekty wykonawcze oraz definicję problemu i określenie pozycji produktu.
W rozdziale 3 znajduje się opis użytkowników systemu.
W rozdziale 4 znajduje się opis produktu, jego przeznaczenie oraz opis budowy.
W rozdziale 5 zostały wymienione i opisane cechy systemu w podziale na strefy.
W rozdziale 6 zostały wymienione oraz opisane pozostałe wymagania, między innymi dotyczące architektury, bezpieczeństwa, wydajności, prawa, standardów itp.

2 Umiejscowienie systemu

Obecnie w ZUT funkcjonuje zestaw systemów do wydawania certyfikatów powszechnych, Każdy z tych systemów funkcjonuje w sposób odizolowany od pozostałych systemów. Ponadto większość z tych systemów bazuje na różnym oprogramowaniu.
Taka sytuacja powoduje trudności w zarządzaniu wydawaniem certyfikatów oraz w administracji tymi systemami. Obecnie nie funkcjonuje oprogramowanie integrujące systemy wyda-

wania certyfikatów ani na poziomie realizacji usługi, ani na poziomie administracji tymi systemami.
Kolejnym problemem jest sposób rozliczania świadczonych usług. Obecnie usługa wydawania certyfikatów jest rozliczana wyłącznie na podstawie umowy zawartej z subskrybentem (umowa na wydanie certyfikatu/certyfikatów), a usługi dodatkowe na zasadach ryczałtu. Oprogramowanie realizujące wydawanie certyfikatów i świadczenie usług dodatkowych (tj. znacznik czasu, kurier elektroniczny, serwer poświadczeń itd.) pozbawione jest modułu bilingowego. Zlecenia fakturowania wystawiane są ręcznie przez operatorów systemu.
W związku z powyższym, zrodziła się potrzeba stworzenia nowego systemu, który rozwiązywałby opisane problemy.

Niniejszy dokument dotyczy pierwszego z wymienionych projektów.

2.1 Definicja problemu

Tabela 1 Definicja problemu

Problem polegający na	braku jednolitego sposobu zarządzania usługami certyfikacyjnymi: powszechnymi i świadczonych na zasadach outsourcing'u.
Dotyczy	ZUT oraz tych firm i organizacji, które mają zamiar świadczyć usługi certyfikacyjne przy pomocy systemu oferowanego przez ZUT
Wpływa na	sposób zarządzania świadczonymi usługami certyfikacyjnymi.
Pomyślne rozwiązanie	uprości sposób zarządzania świadczonymi usługami certyfikacyjnymi.

2.2 Określenie pozycji produktu

Tabela 2 Pozycja produktu

Dla	ZUT oraz innych firm i organizacji,
Którzy	świadczą (lub chcą świadczyć) usługi certyfikacyjne.
ICAS	będzie zintegrowanym systemem,
Który	pozwala w jednolity (zintegrowany) sposób świadczyć i zarządzać usługami certyfikacyjnymi
W odróżnieniu od	systemu proConsI,
nasz produkt	będzie umożliwiał w sposób centralny zarządzanie świadczonymi usługami certyfikacyjnymi.

3 Opis użytkowników systemu

Tabela 3 Użytkownicy systemu

Rodzaj	Opis	Kto go reprezentuje
Subskrybent	Osoba lub instytucja korzystająca z usług certyfikacyjnych. Wypełnia i podpisuje wnioski dotyczące realizacji żądanej usługi certyfikacyjnej.	
Inspektor bezpieczeństwa	Nadzoruje wdrożenie i stosowanie procedur bezpiecznej eksploatacji systemów informatycznych stosowanych w urzędzie certyfikacji. Nadzoruje tworzenie kopii zapasowych rejestrów zdarzeń, które jest wykonywane przez operatorów systemu. Zapewnia środki przeciwdziałające fałszerstwom certyfikatów i innych danych poświadczanych elektronicznie poprzez ochronę urządzeń i danych wykorzystywanych przy świadczeniu usług certyfikacyjnych. Dba o poufność procesu tworzenia danych służących do składania podpisu elektronicznego oraz sprawuje nadzór nad dostępem do tych danych.	
Inspektor ds. rejestracji	Zatwierdza przygotowane zgłoszenia certyfikacyjne dotyczące wydawania, unieważniania oraz zawieszania certyfikatów. Realizuje procedurę odwieszania certyfikatów. Ponadto nadzoruje tworzenie i publikację list unieważnionych certyfikatów i poświadczeń certyfikacyjnych.	
Inspektor ds. audytu	Analizuje zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych (czynność tą wykonuje przynajmniej raz w każdym dniu roboczym), prowadzi audyty wewnętrzne pod kątem zgodności funkcjonowania urzędów certyfikacji zgodnie z Kodeksem Postępowania Certyfikacyjnego oraz obowiązującymi ustawami.	
Administrator systemu	Instaluje, konfiguruje i zarządza systemem ICAS oraz siecią teleinformatyczną. Pod nadzorem Inspektora Bezpieczeństwa, wykonuje kopie zapasowe oraz archiwizuje dane bezpośrednio związane z wykonywanymi usługami certyfikacyjnymi. Przynajmniej raz w każdym dniu roboczym, razem z inspektorem ds. audytu, analizuje informacje zapisane w rejestrach zdarzeń. Definiuje i zarządza komponentem technicznym (sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego). Nadzoruje publikację danych (certyfikaty urzędów certyfikacji oraz listy CRL) umożliwiających weryfikację, autentyczność i ważność certyfika-	

	tów oraz innych danych poświadczonych elektronicznie. Prowadzi rejestr zdarzeń.	
Operator PPT	Informuje o zakresie i ograniczeniach stosowania certyfikatu oraz o skutkach prawnych składania podpisów elektronicznych. Potwierdza tożsamość subskrybenta na podstawie dostarczonych przez niego dokumentów. Uzgadnia z subskrybentem procedurę zgłoszenia wniosku o unieważnienie/zawieszenie certyfikatu. Informuje o konieczności niezwłocznego zgłoszenia wniosku o unieważnienie certyfikatu w momencie podejrzenia utraty lub ujawnienia swoich danych, służących do składania bezpiecznego podpisu elektronicznego, innej osobie. Pomaga klientowi wypełnić wniosek dotyczący wydania certyfikatu.	
Operator PR	Wykonuje te same zadania co Operator PPT. Dodatkowo tworzy i podpisuje wniosek dotyczący wydania lub unieważnienia certyfikatu obsługiwanego subskrybenta.	

4 Ogólny opis produktu

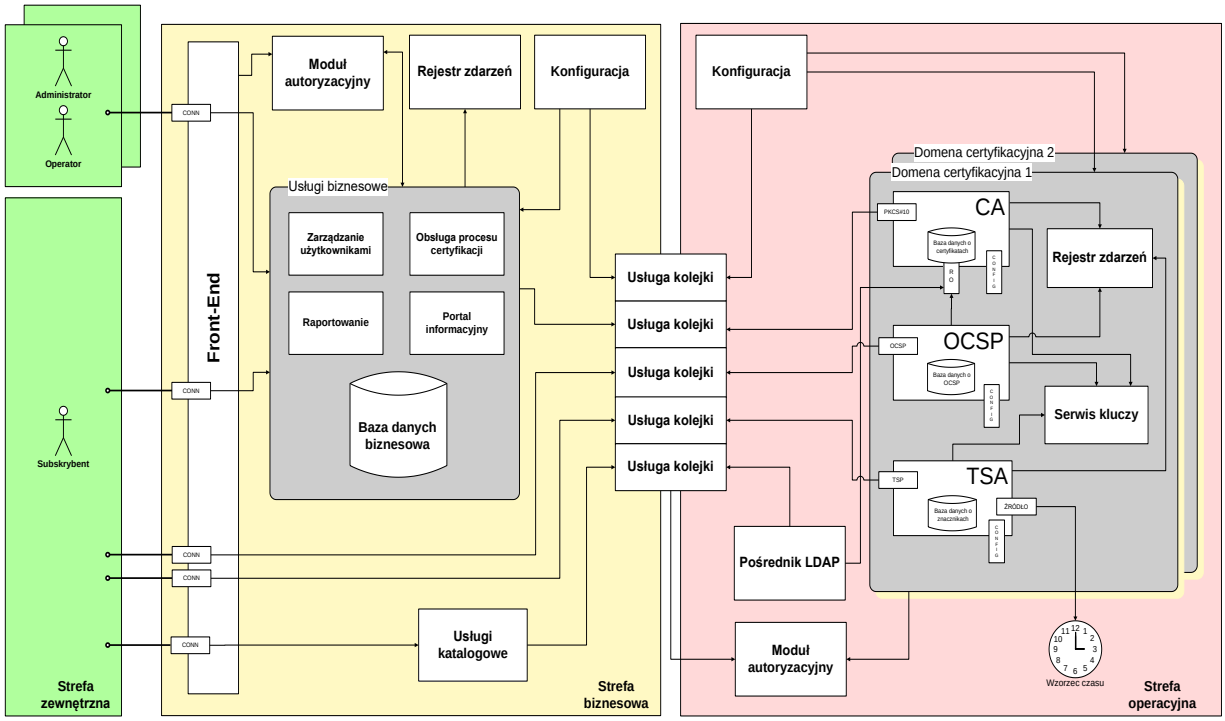
4.1 Przeznaczenie produktu

Przeznaczeniem systemu ICAS jest świadczenie usług certyfikacyjnych, podstawowych oraz dodatkowych, zgodnie z ustawą o podpisie elektronicznym [1].
System ICAS będzie umożliwiał wydawanie certyfikatów kwalifikowanych, powszechnych oraz innych, dla podmiotów obsługiwanych przez ZUT oraz innych firm i organizacji, które zakupią system ICAS. Wydawanie certyfikatów będzie realizowane zgodnie ze zdefiniowanymi politykami certyfikacji.
.
System ICAS, prócz świadczenia podstawowych usług będzie również świadczył usługi dodatkowe:

- Znakowanie czasem (TSA),
- Weryfikacja statusu certyfikatu w trybie on-line (OCSP),
- Serwer poświadczeń (DVCS) – weryfikacja podpisów, statusu certyfikatów oraz poświadczanie dokumentów (w kolejnej wersji systemu).
- Kurier Elektroniczny (DA) – elektroniczna poczta polecona (w kolejnej wersji systemu),

4.2 Budowa systemu

System ICAS będzie złożony z dwóch rozłącznych części: biznesowej i operacyjnej. Komunikacja pomiędzy obiema strefami będzie odbywać się wyłącznie w sposób pośredni z wykorzystaniem usługi kolejek. Dzięki takiemu podejściu zwiększone zostanie bezpieczeństwo części operacyjnej, gdzie przechowywane są certyfikaty oraz klucze urzędu. Ponadto podział ten umożliwia wymianę modułów jednej strefy bez naruszania drugiej.
Poniżej znajduje się schemat obrazujący podział na strefy: biznesową i operacyjną, podział na moduły w ramach poszczególnych stref oraz sposób komunikacji pomiędzy strefami i modułami.



Rysunek 1 Schemat logiczny.

4.3 Założenia i zależności

4.3.1 Zależności pomiędzy modułami

Poniżej zostały znajdują się diagramy, na których przedstawione są zależności pomiędzy modułami strefy operacyjnej i strefy biznesowej. Kolorem niebieskim oznaczono komponenty należące tylko strefy operacyjnej, zielonym tylko do strefy biznesowej, a żółtym moduły wspólne.

4.3.2 Założenia

a) Moduł TSA pobiera czas ze źródła czasu, a pozostałe moduły pobierają czas systemowy, przy założeniu, że systemy operacyjne tych modułów, w kontekście czasu, są synchronizowane ze źródłem czasu (np. przez protokół NTP). Każdy moduł/system operacyjny powinien być synchronizowany z jednym źródłem czasu (za źródłem czasu może stać wiele wzorców czasu).
b) Ponadto protokół CMP będzie realizowany przez strefę biznesowa w kolejnej wersji systemu.
c) Po wykonaniu systemu należy opracować procedury i narzędzia umożliwiające migrację danych z istniejących systemu obsługujących wydawanie certyfikatów kwalifikowanych powszechnych oraz korporacyjnych.

5 Cechy produktu

5.1 Strefa operacyjna

FEAT1: Generowanie certyfikatów

System zapewni generowanie certyfikatów typu X.509.

Priorytet: wysoki
Typ: funkcjonalne

FEAT3: Unieważnianie i zawieszanie certyfikatów

System umożliwi unieważnianie i zawieszanie certyfikatów.

Priorytet: wysoki
Typ: funkcjonalne

FEAT4: Odwieszanie certyfikatów

System umożliwi odwieszanie zawieszonych certyfikatów.

Priorytet: wysoki
Typ: funkcjonalne

5.2 Strefa biznesowa

FEAT21: Obsługa procesu wydawania certyfikatów

System zapewni obsługę procesu wydawania certyfikatów w sposób jednostkowy i masowy.

Priorytet: wysoki
Typ: funkcjonalne

6 Pozostałe wymagania

6.1 Architektura

SUPL3: Skalowalność

Profil eksploatacji powinien być łatwo dostosowywany do aktualnych potrzeb poprzez wykonanie zmian w warstwie sprzętowej projektu bez naruszenia jego struktury logicznej.

SUPL48: Jednostronna komunikacja ze strefą operacyjną

System zapewni brak dostępu do strefy operacyjnej spoza tej strefy. Komunikacja ze światem zewnętrznym będzie się odbywała wyłącznie z inicjatywy strefy operacyjnej.

6.2 Bezpieczeństwo

SUPL1: Uwierzytelnianie do chronionych zasobów

System powinien umożliwiać uwierzytelnianie do chronionych zasobów przy wykorzystaniu karty kryptograficznej, a w przypadku braku takiej karty przy wykorzystaniu hasła.

Uwierzytelnienie podmiotu musi nastąpić przed zezwoleniem systemu na wykonanie dowolnego działania zleconego przez ten podmiot. Liczba nieudanych, jednorazowych prób uwierzytelnienia nie może przekroczyć z góry założonej liczby nieudanych prób. Po każdym wyjściu z systemu (wylogowaniu się) musi nastąpić ponowne uwierzytelnienie.

SUPL47: Autoryzacja dostępu do kluczy urzędu certyfikacji

System zapewni autoryzację dostępu do kluczy urzędu certyfikacji na poziomie pojedynczego klucza.

6.3 Wydajność

SUPL5: Czas wydania listy CRL

W przypadku konieczności unieważnienia certyfikatu z powodu ujawnienia klucza prywatnego, system powinien umożliwić wydanie nowej listy CRL w ciągu 1 godziny od momentu zgłoszenia żądania.

6.4 Wymagania prawne

SUPL19: Ustawa o podpisie elektronicznym.

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym.

6.5 Standardy

SUPL26: The Directory: Selected Attribute Types

ISO/IEC 9594-6 X.520 The Directory: Selected Attribute Types

SUPL27: X.509 Certificate and CRL Profile

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 3280)

6.6 Inne wymagania

SUPL24: Wieloplatformowość

System powinien być oprogramowaniem wieloplatformowym. W pierwszej kolejności powinny być obsłużone następujące platformy: Microsoft Windows 2000/2003 Server, Solaris 8/9, Red Hat Advanced Server; oraz bazy danych: Oracle 8i/9i, Sybase 12.5 oraz Microsoft SQL Server 2000.

SUPL25: Wielojęzyczność

System powinien być systemem wielojęzycznym.

6.7 Specyfikacje

STRQ1: CWA Cryptographic module - Protection profile

Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP May 2004 (CWA 16167-2:2004 (E))

STRQ2: Realizacja projektu zgodnie z Common Criteria

Realizacja certyfikowanych modułów projektu zgodnie z Common Criteria.

6.8 Zalecenia

REC1: ETSI Policy requirements for time-stamping authorities

ETSI TS 102 023 Policy requirements for time-stamping authorities

REC2: ETSI Policy requirements for certification authorities issuing public key certificates

ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates