Załącznik nr 1

Warszawa, dnia 12.11.2019 r.

# Szczegółowy Opis Przedmiotu Zamówienia

# „Zaprojektowanie i wdrożenie scentralizowanego dostępu do zasobów, aplikacji i systemów IT dla pracowników i studentów ChAT"

**Dotyczy projektu: „CHAT przyszłości" nr POWR.03.05.00-00-z044/18 współfinansowany z Programu Operacyjnego Wiedza Edukacja Rozwój**

Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020

**Chrześcijańska Akademia Teologiczna w Warszawie**
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

## Spis treści

1. Zakres Przedmiotu Zamówienia ..... 4
2. Wymagania ogólne dla Wykonawcy (dot. wszystkich zadań) ..... 5
2.1. Wymagania ogólne ..... 5
2.2. Wymagania dla Harmonogramu i Projektu Technicznego ..... 5
2.3. Dokumentacja powykonawcza ..... 6
2.4. Testy odbiorcze/akceptacyjne ..... 7
2.5. Gwarancja i parametry SLA ..... 8
2.6. Zakres i warunki świadczenia Dedykowanej Asysty Technicznej ..... 10
2.7. Szkolenia dla administratorów ..... 10
3. ZADANIE I - Usługa uruchomienia środowiska wirtualnego Uczelni oraz usługi SSO wraz z dostawą i instalacją urządzeń ..... 12
3.1. ETAP I - Dostawa urządzeń i oprogramowania ..... 12
3.1.1. Specyfikacja techniczna serwera – minimalne wymagania: ..... 13
3.1.2. Opis równoważnych funkcjonalności dla Systemu Operacyjnego ..... 16
3.1.3. Specyfikacja techniczna Macierzy – minimalne wymagania ..... 19
3.1.4. Zakres wdrożenia dostarczonej macierzy ..... 22
3.2. ETAP II – Uruchomienie środowiska wirtualnego - Zakres usług wdrożeniowych ..... 22
3.2.1. Wymagania funkcjonalne dotyczące usługi wirtualizacji ..... 22
3.2.2. Migracja Systemów i Usług Zamawiającego na środowisko wirtualne ..... 24
3.2.3. Wymagania dla usługi zapewnienia ciągłości działania wdrożonego systemu wirtualizacji ..... 24
3.3. ETAP III - Wdrożenie usługi SSO w oparciu o Centralny Katalog Użytkowników ..... 27
3.3.1. Integracja systemu SSO dla systemów Uczelni ..... 28
4. ZADANIE 2 - Rozbudowa Systemu kontroli dostępu ..... 30
4.1. Usługi wdrożeniowe w ramach rozbudowy systemu kontroli dostępu ..... 30
4.1.1. Rozbudowa Systemu Kontroli Dostępu wraz z integracją z SSO (Usługa katalogowa) ..... 30
4.2. Specyfikacja techniczna elementów rozbudowy systemu Kontroli Dostępu ..... 31
4.2.1. Specyfikacja rozbudowy istniejącego systemu KD. ..... 31
4.2.2. Specyfikacja rozbudowy istniejącego systemu ELS. ..... 31
4.2.3. Specyfikacja systemu elektronicznego zabezpieczenia zbiorów bibliotecznych w technologii radiowej identyfikacji – RFID HF. ..... 32
Wymogi techniczne elementów systemu będącego przedmiotem przetargu: ..... 33
5. ZADANIE 3 - Rozbudowa infrastruktury Zamawiającego ..... 37
5.1. Rozbudowa serwera Zamawiającego ..... 37


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

# *Słownik pojęć*

| Pojęcie | Znaczenie |
|---|---|
| Awaria | nieprawidłowe działanie Urządzeń lub Oprogramowania, w szczególności brak możliwości używania Urządzeń lub Oprogramowania w sposób zgodny z ich przeznaczeniem lub z dokumentacją producenta i/lub dokumentacją powykonawczą; |
| Dzień Roboczy | dzień kalendarzowy od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy |
| Przedmiot Zamówienia | projekt techniczny, dokumentacja techniczna, dokumentacja powykonawcza oraz wszelkie inne materiały, dokumenty wytworzone przez Wykonawcę w wyniku realizacji przedmiotu Umowy w ramach „Zaprojektowanie i wdrożenie scentralizowanego dostępu do zasobów, aplikacji i systemów IT dla pracowników i studentów ChAT". |
| Środowisko Zamawiającego | Istniejąca infrastruktura w Lokalizacjach Zamawiającego która nie jest przedmiotem niniejszego postępowania |
| Usterka | uszkodzenie Sprzętu niepowodujące niezdolności do pełnego działania; |
| Wykonawca | Strona Umowy realizująca Przedmiot Zamówienia |
| Zgłoszenie | poinformowanie Wykonawcy o Awarii lub Usterce powodującej konieczność podjęcia przez niego interwencji lub zapytanie skierowane do Wykonawcy dotyczące funkcjonowania, konfiguracji lub zarządzania |

# 1. Zakres Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa sprzętu komputerowego z podziałem na 3 części. Zamawiający nie ogranicza liczby części na które jeden Wykonawca może złożyć ofertę:

- ZADANIE 1 - Usługa uruchomienia środowiska wirtualnego Uczelni oraz usługi SSO wraz z dostawą i instalacją urządzeń
- ZADANIE 2 - Rozbudowa Systemu Kontroli Dostępu
- ZADANIE 3 - Rozbudowa infrastruktury Zamawiającego


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

# 2. Wymagania ogólne dla Wykonawcy (dot. wszystkich zadań)

## 2.1. Wymagania ogólne

| Identyfikator | Opis wymagania |
|---|---|
| WOG.01 | Wykonawca przygotuje Harmonogram oraz Projekt techniczny realizacji wdrożenia dostarczonego sprzętu oraz oprogramowania na potrzeby realizacji Przedmiotu Zamówienia |
| WOG.02 | Wykonawca przeprowadzi testy akceptacyjne dostarczonego rozwiązania zgodnie z opisem w **pkt 2.4** |
| WOG.03 | Wykonawca po wykonaniu instalacji i konfiguracji Przedmiotu Zamówienia przekaże Zamawiającemu Dokumentację powykonawczą, która musi w szczególności zawierać zakres opisany w **pkt. 3.11, pkt 3.1.2 i pkt 4.2** |
| WOG.04 | Wykonawca przeprowadzi szkolenia zgodnie z opisem w **pkt. 2.5** |

W szczegółowych opisach przedmiotu zamówienia dla konkretnych Zadań określono minimalne wymagane parametry techniczne urządzeń, warunki i okres trwania gwarancji, obsługi serwisowej. Wykonawca może zaoferować modele zgodne z wymaganiami minimalnymi lub modele o wyższych parametrach.

## 2.2. Wymagania dla Harmonogramu i Projektu Technicznego

W ramach realizacji Umowy, Wykonawca w pierwszej kolejności przeprowadzi analizę Środowiska Zamawiającego i przedstawi do akceptacji Zamawiającemu Projekt Techniczny opisujący szczegółowo zaproponowaną architekturę techniczną na potrzeby realizacji przedmiotu zamówienia z wykorzystaniem zaoferowanego sprzętu i oprogramowania.

Przedmiot zamówienia będzie realizowany w oparciu o przygotowany uprzednio przez Wykonawcę Harmonogram Prac z wykorzystaniem wytycznych z poniższej tabeli. Harmonogram powinien być wcześniej uzgodniony i zaakceptowany przez Zamawiającego oraz systematycznie aktualizowany i utrzymywany w toku realizacji projektu.

Wykonawca w harmonogramie Projektu musi uwzględnić w szczególności podział na zadania, takie jak projektowanie, dostawy, usługi Wdrożenia, testowanie i odbiory, dostarczenie Dokumentacji oraz przeprowadzenie szkoleń dla każdego Etapu Przedmiotu Zamówienia.


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| Etap/część | Opis | Termin |
|---|---|---|
| 1. | **Analiza przedwdrożeniowa** | do **7 dni** od daty podpisania Umowy |
| 2. | **Wykonanie Projektu Technicznego** | do **14 dni** od daty podpisania Umowy |
| 3. | **Dostawa urządzeń** | do **40 dni** od daty podpisania Umowy |
| 4. | **Wdrożenie dostarczonej infrastruktury i oprogramowania** | do **70 dni** od daty podpisania Umowy |
| 5. | **Dokumentacja powykonawcza** | do **80 dni** od daty podpisania Umowy |
| 6. | **Odbiory/Testy Odbiorcze** | do **85 dni** od daty podpisania Umowy |
| 7. | **Szkolenia** | do **90 dni** od daty podpisania Umowy |

## 2.3. Dokumentacja powykonawcza

- Zamawiający wymaga dostarczenia przez Wykonawcę dokumentacji powykonawczej po wdrożeniu infrastruktury sprzętowo – programowej dla Produktów Zamówienia.
- Dostarczenie dokumentacji powykonawczej jest elementem niezbędnym do przeprowadzenia odbioru prac Zamawiającego dostarczonego sprzętu i oprogramowania.
- Dokumentacja powykonawcza powinna zawierać co najmniej:
    a. schematy połączeń logicznych i fizycznych ww. infrastruktury (w tym również sieci informatycznej) wraz z informacja o umiejscowieniu każdego z jej elementów,
    b. parametryzację i konfigurację każdego z dostarczonych elementów tej infrastruktury (urządzenia, oprogramowania) wraz ich opisem,
    c. informację o zmianach, które nastąpiły w infrastrukturze informatycznej Zamawiającego w trakcie wdrożenia wraz z dokładnym opisem w jakim zakresie i na jakim jej elemencie.
- Wykonawca w ramach dokumentacji powykonawczej dostarczy podstawowe procedury i instrukcje administracyjne.
- Wymagane jest aby procedury i instrukcje dotyczyły instalacji, konfiguracji oraz parametryzacji wdrożonej infrastruktury programowo-sprzętowej dla każdej z grup administratorów w tym m.in. w obszarach: sieć informatyczna, bezpieczeństwo teleinformatyczne, systemy operacyjne, środowisko wirtualizacyjne, backup danych, system kontroli dostępu.


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

- Wykonawca dostarczy również Procedury i instrukcje w zakresie:
  a. wykonania kopii bezpieczeństwa i ich odtworzenia,
  b. aktualizacji i wdrażania poprawek dla dostarczonej infrastruktury,
  c. postępowania w razie wystąpienia błędów lub awarii, rozwiązywania zaistniałych problemów i zgłaszania ich do Wykonawcy.
- Każda z procedur powinna zawierać co najmniej następujące dane:
  a. nazwa,
  b. opis,
  c. częstotliwość wykonywania,
  d. kroki do zrealizowania w procedurze,
  e. informacje (o ile są znane, jeśli jest ich dużo to przykłady bądź wzorce), na jakie należy zwrócić uwagę w trakcie wykonywania procedury,
  f. omówienie zawartości komunikatów jeśli są prezentowane,
  g. kroki jakie należy podjąć w przypadku natknięcia się na nietypowe sytuacje.
- Dokumentacja powykonawcza musi być dostarczona najpóźniej po zakończeniu prac wdrożeniowych i szkoleniowych.
- Dokumentacja powykonawcza powinna zostać dostarczona w języku polskim.

Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji wdrożenia, w tym dokumentacja powykonawcza charakteryzowały się wysoką jakością, a w szczególności:

  a. czytelną i zrozumiałą strukturą zarówno poszczególnych dokumentów jak i całej dokumentacji z podziałem na rozdziały, podrozdziały i sekcje,
  b. zachowaniem standardów oraz sposobu pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów, oraz fragmentów tego samego dokumentu, jak również całej dokumentacji.
- Zamawiający wymaga, aby cała dokumentacja, o której mowa powyżej, podlegała jego akceptacji.

## 2.4. Testy odbiorcze/akceptacyjne

1. Testom akceptacyjnym/odbiorczym muszą być poddane wszystkie elementy sprzętowe oraz funkcjonalności realizowane przez Sprzęt i oprogramowanie dostarczane przez Wykonawcę.
2. Przed przystąpieniem do Testów funkcjonalnych Wykonawca jest zobowiązany przedstawić projekt Dokumentację Powykonawczą aktualną na dzień zakończenia prac wdrożeniowych infrastruktury sprzętowo-programowej.

3. Po testach funkcjonalnych Wykonawca powinien uzupełnić dokumentację powykonawczą o ewentualne uwagi, które mogą pojawić się podczas testów.

Podstawą odbioru prac realizowanych przez Wykonawcę będzie:

| Identyfikator | Opis wymagań |
|---|---|
| TES.01 | sprawdzenie zgodności wykonanego wdrożenia z Projektem Technicznym opracowanym przez Wykonawcę, |
| TES.02 | wykonanie testów redundantnych elementów serwerów, poprzez ich odłączenie, wyłączenie lub wymontowanie w trakcie pracy. Czynności te nie mogą spowodować przerwy w działaniu serwerów wirtualnych (musi być zachowany dostęp do testowego systemu operacyjnego), |
| TES.03 | wykonaniu testów redundantnych elementów urządzeń sieci LAN, poprzez ich odłączenie, wyłączenie lub wymontowanie w trakcie pracy. |
| TES.04 | sprawdzeniu zgodności wykonanej konfiguracji dostarczonych urządzeń z Projektem Technicznym opracowanym przez Wykonawcę |
| TES.05 | przeprowadzenie testów działania procedur DR (zarówno odtwarzanie pojedynczych serwerów, maszyn wirtualnych plików, baz, systemów operacyjnych, jak również przełączanie wybranych systemów pomiędzy serwerami fizycznymi). |

## 2.5. Gwarancja i parametry SLA

| Identyfikator | Opis wymagań |
|---|---|
| GiSLA.01 | Wykonawca zobowiązuje się udzielić pełnej Gwarancji Wykonawcy (GW) dostarczone elementy Przedmiotu Zamówienia na okres 48 miesięcy (o ile zapisy zawarte w szczegółowym opisie przedmiotu zamówienia nie stanowią inaczej) oraz rękojmi na okres 12 miesięcy od daty końcowego protokołu odbioru. Gwarancja obejmie wszelkiego rodzaju wady, zarówno materiałowe, jak i wykonawcze. |
| GiSLA.02 | Całość dostarczonej Infrastruktury sprzętowej musi być objęta równocześnie gwarancją producenta w okresie 48 miesięcy. |
| GiSLA.03 | Gwarancja producenta musi być oparta o świadczenia gwarancyjne producenta sprzętu niezależnie od statusu partnerskiego Wykonawcy i ma objąć okres minimum 48 miesięcy od momentu podpisania końcowego protokołu odbioru. |
| GiSLA.04 | Wykonawca w trakcie okresu gwarancyjnego musi świadczyć również Usługę Serwisową (w skrócie US). |


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| Identyfikator | Opis wymagań |
|---|---|
| GiSLA.05 | Zaproponowana US musi umożliwiać również bezpośrednie zgłoszenie awarii sprzętu do producenta(ów) Infrastruktury sieciowej przez cały okres trwania serwisu gwarancyjnego. |
| GiSLA.06 | US ma być świadczona w dniu roboczym, realizowany w godzinach 8.00-16.00 liczony od daty zgłoszenia - w siedzibie Zamawiającego |
| GiSLA.07 | GW wraz z US będzie świadczone w miejscu instalacji sprzętu przez autoryzowane służby serwisowe Wykonawcy i/lub producenta. |
| GiSLA.08 | Czas Reakcji Wykonawcy na zgłoszenie nie może być dłuższy niż 4 godz. |
| GiSLA.09 | Czas Naprawy Awarii nie może być dłuższy niż 1 dzień roboczy od momentu Zgłoszenia. |
| GiSLA.10 | Czas Naprawy Usterki nie może być dłuższy niż 3 dni roboczych od momentu Zgłoszenia. |
| GiSLA.11 | Serwis Wykonawcy ma obowiązek przyjmowania zgłoszeń serwisowych w ramach US i GW przez telefon (w godzinach pracy Zamawiającego), email lub WWW. |
| GiSLA.12 | Jeżeli zgodnie z licencją producenta dostęp do aktualizacja oprogramowania wchodzącego w skład infrastruktury/oprogramowania w trakcie GW wymaga wykupienia odpowiedniego wsparcia u producenta to Wykonawca powinien takie wsparcie wykupić. |
| GiSLA.13 | Jeżeli do poprawnego działania wymaganych funkcjonalności Przedmiotu Zamówienia przez okres świadczenia wsparcia gwarancyjnego konieczne jest wykupienie subskrypcji oprogramowania to Wykonawca powinien ją zapewnić na cały okres świadczenia usług gwarancyjnych. |
| GiSLA.14 | Urządzenia wraz z zainstalowanym na nich oprogramowaniem muszą pochodzić z legalnego kanału dystrybucji producenta i być przeznaczone do użytkowania w Polsce. |
| GiSLA.15 | Zaoferowany serwis ma gwarantować dostęp Zamawiającemu do bazy wiedzy producenta związanej z oferowanym sprzętem/oprogramowaniem (urządzeniem, oprogramowaniem oraz niezbędnych narzędzi) przez okres minimum 48 miesięcy od momentu podpisania protokołu odbioru końcowego |
| GiSLA.16 | Wykonawca w ramach gwarancji pokryje wszystkie koszty związane z naprawą sprzętu, m.in. koszty transportu, ubezpieczenia, robocizny. |
| GiSLA.17 | Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych przetwarzanych z wykorzystaniem dostarczonych urządzeń i oprogramowania. |
| GiSLA.18 | W ramach realizacji usług GW i US, Wykonawca zobowiązany jest do uzgodnienia niezbędnego zakresu prac z Zamawiającym i umożliwieniu osobom przez niego wskazanym obserwacji ich realizacji. |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

## 2.6. Zakres i warunki świadczenia Dedykowanej Asysty Technicznej

1. Wykonawca zobowiązuje się świadczyć usługę Dedykowanej Asysty Technicznej w sposób profesjonalny zgodnie ze standardami obowiązującymi w branży informatycznej.
2. Wykonawca zobowiązuje się świadczyć usługę Dedykowanej Asysty Technicznej w wymiarze maksymalnie 8 roboczogodzin miesięcznie przez okres 12 m-cy od dnia zawarcia Umowy.
3. Usługa Dedykowanej Asysty Technicznej będzie świadczona w Dni Robocze od godziny 8:00 do godziny 16:00.
4. Zakres świadczonej usługi Dedykowanej Asysty Technicznej obejmuje w szczególności:
   a. konsultacje dotyczące zwiększania efektywności wykorzystania infrastruktury dostarczonej dla Zamawiającego
   b. rozwiązywanie problemów technicznych związanych z funkcjonowaniem dostarczonego Sprzętu oraz uruchomionego środowiska wirtualizacyjnego,
   c. instalację i konfigurację oprogramowania (w zakresie uaktualniania oprogramowania),
   d. wsparcie przy bieżącej eksploatacji infrastruktury Zamawiającego, w zakresie:
   e. konfiguracji sieci LAN a w szczególności:
      - konfiguracji serwerów
      - konfiguracji środowiska wirualizacyjnego
      - konfiguracji warstwy dostępowej do serwerów aplikacyjnych i bazodanowych

## 2.7. Szkolenia dla administratorów

W ramach realizacji umowy, w dniach uzgodnionych z Zamawiającym, Wykonawca przeprowadzi instruktarz z zakresu wdrożonej w ramach realizacji Przedmiotu Zamówienia infrastruktury programowo-sprzętowej w zakresie:

1. Administracji i konfiguracji dostarczonym serwerem.
   a. Szkolenie zostanie przeprowadzone dla 2 administratorów,
   b. Czas trwania szkolenia to min. 8 godz.
2. Administracji wdrożonym środowiskiem wirtualnym i system monitoringu dla tego środowiska.
   a. Szkolenie zostanie przeprowadzone dla 2 administratorów,
   b. Czas trwania szkolenia to min. 3 dni.
3. Administracji wdrożonym system do wykonywania kopii zapasowej oraz dostarczoną macierzą.
   a. Szkolenie zostanie przeprowadzone dla 2 administratorów,
   b. Czas trwania szkolenia to min. 4 dni.
4. Administracji rozbudowanym i wdrożonym systemem Kontroli Dostępu.


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

a. Szkolenie zostanie przeprowadzone dla 5 administratorów,
b. Czas trwania szkolenia to min. 1 dzień.

Powyższe instruktarze zostaną przeprowadzane na terenie Chrześcijańskiej Akademii Teologicznej w Warszawie, w terminach uzgodnionych z Zamawiającym, w godz. pracy 8-16. Przeszkolenia te należy uwzględnić w harmonogramie wdrożenia Przedmiotu Zamówienia.

Ponadto Wykonawca w ramach ceny oferty dostarczy vouchery na certyfikowane szkolenia producentów dostarczonych rozwiązań dla dwóch osób. Poniżej lista wymaganych szkoleń.

1. Installation, Storage, and Compute with Windows Server 2016
2. Securing Windows Server 2016


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

# 3. ZADANIE I - Usługa uruchomienia środowiska wirtualnego Uczelni oraz usługi SSO wraz z dostawą i instalacją urządzeń

## 3.1. ETAP I - Dostawa urządzeń i oprogramowania

Lista elementów infrastruktury sprzętowej, która musi zostać dostarczona w ramach postępowania została przedstawiona w tabeli poniżej.

| LP. | ELEMENT INFRASTRUKTURY | LICZBA MINIMALNA SZT. |
|---|---|---|
| 1. | Serwer | 1 szt. |
| 2. | Macierz | 1 szt. |
| 3. | Oprogramowanie wirtualizacyjne | 1 szt. |

Parametry techniczne oraz szczegółowe specyfikacje opisane zostały w dalszej części dokumentu.

Wszystkie dostarczone urządzenia w ramach zaoferowanego rozwiązania muszą być:

- nowe tzn. wyprodukowane nie wcześniej niż w 2019 roku oraz nieużywane;
- dostarczone urządzenia muszą posiadać oprogramowanie w wersji aktualnej;
- dostarczone urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży,

W ramach zakresu prac będących przedmiotem zamówienia należy:

- dostarczyć i rozładować urządzenia w siedzibie Zamawiającego,
- wykonać montaż, instalację fizyczną i uruchomić urządzenia i oprogramowanie w miejscu wskazanym przez Zamawiającego - Zamawiający zapewnia, że posiada odpowiednie (pod względem fizycznym) klimatyzowane pomieszczenie oraz zapewnia, że ma odpowiednią rezerwę zasilania,
- uaktualnić firmware wszystkich dostarczanych urządzeń i oprogramowania, których to dotyczy do najnowszej stabilnej wersji zalecanej przez producenta;
- wykonać niezbędne połączenia logiczne pomiędzy wszystkimi elementami systemu będącego przedmiotem zamówienia,
- wykonawca przeprowadzi wizję lokalną w zakresie posiadanej przez zamawiającego infrastruktury i systemu zarządzania,
- zintegrować dostarczone urządzenia ze środowiskiem Zamawiającego – w tym z istniejącymi systemami zarządzania i monitorowania infrastruktury.


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

Wykonawca realizując dostawy urządzeń musi zapewnić wszystkie potrzebne akcesoria montażowe, kable połączeniowe i przewody do podłączenia zasilania.

W ramach postępowania dostarczone zostanie również oprogramowanie wraz z niezbędnymi licencjami w zakresie:

- Systemu wirtualizacji wraz z mechanizmami zapewnienia ciągłości działania w tym wykonywania kopii zapasowych

### 3.1.1. Specyfikacja techniczna serwera – minimalne wymagania:

| LP. | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 1. | **Obudowa** | • Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.<br>• Zamawiający dopuszcza monitorowanie parametrów i konfigurację urządzenia przez poprzez dedykowany port serwera i dedykowaną aplikację. |
| 2. | **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| 3. | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| 4. | **Procesor** | Zainstalowane dwa procesory 12-rdzeniowe klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku:<br>• min. 1000 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dla dwóch procesorów<br>lub<br>• wyniku min. 130 punktów w teście SPEC CPU2017 Integer Rate Result wynik SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji dla dwóch procesorów.<br>Wynik dla oferowanego serwera (producent + model) załączyć do oferty – wydruk ze strony spec.org. |

| LP. | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 5. | **RAM** | 128GB DDR4 RDIMM 2666T/s (kości pamięci: 4x32GB); na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM. |
| 6. | **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, SDDC. |
| 7. | **Gniazda PCI** | Min. 3 slotów x8 generacji 3, Min. 2 sloty x16 generacji 3. |
| 8. | **Interfejsy sieciowe** | Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.<br><br>Możliwość instalacji wymiennie modułów udostępniających (min. dwóch rodzajów z listy poniżej):<br><br>• dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+.<br>• cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+.<br>• cztery interfejsy sieciowe 10Gb Ethernet w standardzie BaseT.<br>• dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28.<br>• dwa interfejsy sieciowe 10Gb Ethernet ze złączami BaseT.<br>• dwa interfejsy sieciowe 10Gb Ethernet ze złączami SFP+. |
| 9. | **Napęd optyczny** | Wbudowany DVD-RW lub zewnętrzny poprzez port USB |
| 10. | **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.<br><br>Zainstalowany 1x120GB SSD SATA 6Gbps.<br><br>Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 jednakowe nośniki typu flash o pojemności min. 64GB każdy z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| 11. | **Kontroler RAID** | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50. Wsparcie dla dysków samoszyfrujących. |
| 12. | **Wbudowane porty** | Min. 4 porty USB, (w tym min. 3 porty USB 3.0), 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232. |
| 13. | **System operacyjny** | Windows Server 2016/2019 Data Center lub równoważny (opis równoważności poniżej). |


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| LP. | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 14. | **Warunki gwarancji** | Okres gwarancji: minimum 4 lat od daty dostawy w miejscu instalacji zestawu.<br><br>Wykonawca zagwarantuje maksymalny czas naprawy w najbliższym dniu roboczym, realizowany w godzinach 8.00-16.00 liczony od daty zgłoszenia - w siedzibie Zamawiającego<br><br>W przypadku uszkodzenia dysku twardego w okresie gwarancji, uszkodzony dysk pozostaje u Zamawiającego, a w jego miejsce zostaje dostarczony nowy (bez dodatkowych kosztów).<br><br>Możliwość rozbudowy Sprzętu przez pracowników Zamawiającego bez utraty praw do gwarancji na pozostałe elementy jednostki. |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

### 3.1.2. Opis równoważnych funkcjonalności dla Systemu Operacyjnego.

Licencje na serwerowy system operacyjny muszą być dostarczone i przypisane do każdego rdzenia procesora fizycznego na serwerze. Wymagana przez Zamawiającego licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.

Warunki licencjonowania muszą zezwalać na:

- korzystanie z oprogramowania na fizycznym serwerze posiadającym dwa procesory po 12 rdzeni.
- W zakresie ilości fizycznych rdzeni w klastrze wymagane jest zapewnienie licencji dla następującej konfiguracji: 1 serwer fizyczny x 2 procesory fizyczne x 12 fizycznych rdzeni = 48 rdzenie fizyczne.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Współpraca z procesorami o architekturze x86-64.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Praca w roli kontrolera domeny Microsoft Active Directory.
4. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
5. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
6. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
7. Zawarta możliwość uruchamiania nieograniczonej ilości wirtualnych instancji systemu operacyjnego.
8. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
9. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
10. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
11. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
12. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

13. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    - pozwalają na zmianę rozmiaru w czasie pracy systemu,
    - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    - umożliwiają zdefiniowanie list kontroli dostępu (ACL).
14. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
15. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
16. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
17. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
18. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
19. Mechanizmy logowania w oparciu o:
    - Login i hasło,
    - karty z certyfikatami (smartcard),
    - wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
20. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
21. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
22. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
23. Obsługa zdalnego pulpitu – RDP.
24. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
25. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
26. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

c. zdalna dystrybucja oprogramowania na stacje robocze.
d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
e. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
   - dystrybucję certyfikatów poprzez http
   - konsolidację CA dla wielu lasów domeny,
   - automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
   - automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
f. szyfrowanie plików i folderów.
g. obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.
h. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
j. serwis udostępniania stron WWW.
k. wsparcie dla protokołu IP w wersji 6 (IPv6).
l. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   - obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   - obsługi 4-KB sektorów dysków
   - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   - możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

27. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

### 3.1.3. Specyfikacja techniczna Macierzy – minimalne wymagania

Przez macierz dyskową rozumie się zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe macierzy bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami (nie dopuszcza się żadnych połączeń typu IP/LAN poprzez zewnętrzne przełączniki)

| LP | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 1. | Obudowa | System musi być dostarczony ze wszystkimi komponentami niezbędnymi do instalacji w szafie rack 19" |
| 2. | Pojemność: | Macierz zawiera łącznie minimum:<br>• minimum **4** dyski 2,5" SSD SAS o pojemności minimum 960 GB każdy;<br>• minimum **8** dysków 3,5" NL-SAS o pojemności minimum 4TB każdy i prędkości obrotowej minimum 7,2k RPM;<br>System musi ponadto wspierać dyski:<br>- SAS: 900GB, 1200GB, 1800GB<br>- SATA/NL-SAS: 4TB, 6TB, 8TB , 10TB<br>- SSD: 800GB, 1,6TB, 3,2TB<br>System musi mieć możliwość rozbudowy do minimum **180** dysków w obrębie pary kontrolerów lub w obrębie klastra wielu kontrolerów (scale-out) w zależności od sposobu realizacji rozbudowy dla oferowanego rozwiązania.<br>Macierz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami). |
| 3. | Kontroler | Dwa aktywne kontrolery wyposażone w przynajmniej 32GB cache każdy.<br>W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.<br>Kontrolery macierzy obsługują tryb pracy w układzie active-active lub mesh active lub ALUA.<br>Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. |
| 4. | Interfejsy | Oferowana macierz musi mieć minimum:<br>- 4 porty Ethernet (iSCSI) 10Gb do podłączenia hostów – gniazda SFP+<br>- 4 porty SAS 12 Gb/s (do podłączenia półek dyskowych)<br>Macierz musi pozwalać na rozbudowę o dodatkowe 4 porty 10GbE lub 4 porty FC 16Gb.<br>Macierz musi zostać dostarczona z min. 4 kablami miedziane SFP+/SFP+ typu Twinax – 2 m, współpracujące z dostarczoną macierzą. |
| 5. | RAID | Wsparcie dla RAID: 0, 1, 5, 6, 10 lub równoważne zapewniające zabezpieczenie przed utratą do 3 dysków w grupie RAID<br>Opcjonalnie macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum **48** dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych.<br>Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy lub dedykowane oprogramowanie na kontrolerach macierzy. |
| 6. | Obsługiwane protokoły | Macierz musi udostępniać dane po iSCSI i Fiber Channel |

| LP | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 7. | Obsługa kompresji danych | Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:<br>• Kombinacja technologii kompresji i deduplikacji wybranego LUN;<br>• Brak użycia technologii kompresji i deduplikacji dla wybranego LUN;<br>Jeżeli do uruchomienia wymaganych funkcjonalności deduplikacji i kompresji są wymagane jakiekolwiek licencje lub elementy hardware wymaga się ich dostarczenia dla maksymalnej wymaganej pojemności |
| 8. | Działanie podczas awarii zasilania | W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik nie wymagający korzystania z podtrzymania jego zasilania. |
| 9. | Inne wymagania | • Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów:<br>• Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, VMware® ESX®, Oracle® Solaris,<br>• Macierz musi pozwalać na wykorzystanie dysków SSD w celu akceleracji odczytów.<br>• Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen.<br>• Macierz musi posiadać funkcjonalność klonowania danych<br>• Macierz musi posiadać możliwość rozbudowy za pomocą aktywacji licencji o funkcjonalność replikacji danych po FC lub IP (po zainstalowaniu portów FC na macierzy) w trybie synchronicznym i asynchronicznym, system musi pozwalać na wykonanie do 32 jednoczesnych replikacji.<br>• System musi wspierać replikowanie zdeduplikowanych i skompresowanych danych.<br>• Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumnów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumnie<br>• Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID<br>• Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków i automatyczne powiadamianie o problemach administratora i serwisu zewnętrznego |
| 10. | Integracje | Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z:<br>- Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter<br>- VMware VASA<br>- VMware Site Recovery Manager – wsparcie dla replikacji macierz z VMware<br>- Microsoft SCOM – integracja systemu macierzowego z monitoringiem i alarmami w Microsoft SCOM<br>- Microsoft Virtual Disk Service (VDS)<br>- Microsoft Virtual Shadow Service (VSS) |
| 11. | Szyfrowanie | Macierz musi zapewniać możliwość szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami. |


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| LP | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 12. | Zarządzanie | Macierz musi posiadać oprogramowanie do zarządzania macierzą w formie:<br>- przez przeglądarkę WWW (preferowane),<br>- lub dedykowanego oprogramowania do instalacji na stacji roboczej.<br>Wszystkie wymienione licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy.<br>Zamawiający wymaga by wszystkie wymienione funkcjonalności pozwalały na jednoczesne działanie tj. włączenie jednej funkcjonalności nie eliminowało działania innej. |
| 13. | | Każdy kontroler macierzy pozwala na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC SAN oraz NAS |
| 14. | | Dla obsługi operacji blokowych I/O w sieci IP/FC SAN kontrolery macierzy wspierają protokoły transmisji: FC lub iSCSI, a ich obsługa odbywa się jednocześnie. |
| 15. | | Macierz umożliwia wymianę portów do transmisji danych na porty obsługujące protokoły: iSCSI 1 Gb/s, iSCSI 10Gb/s. Wymiana portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, w przypadku konieczności licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencją na instalację i obsługę każdego z wymienionych protokołów transmisji danych. |
| 16. | | Wszystkie dyski wspierane przez oferowany model macierzy wykonane są w technologii hot-plug i posiadają podwójne porty SAS obsługujące tryb pracy full-duplex |
| 17. | Gwarancja | Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt), fabrycznie nowe, pochodzić z oficjalnego kanału sprzedaży w Polsce, być serwisowane przez producenta lub autoryzowany serwis producenta w języku polskim ze wsparciem na 3 lata z gwarantowanym czasem naprawy w ciągu 1 dnia roboczego od momentu zgłoszenia problemu. W przypadku autoryzowanego serwisu producenta na terenie Polski, wymagane jest potwierdzenie kompetencji w zakresie świadczenia usług serwisowych poprzez certyfikat ISO.<br><br>• Macierz musi być fabrycznie nowa.<br>• Min. 36 miesięcy gwarancji producenta, bądź partnera serwisowego legitymującego się dokumentami potwierdzającymi posiadanie stosownej autoryzacji, obejmująca serwis sprzętowy oraz wsparcie dla nowych wersji oprogramowania. Gwarancja liczona jest od daty podpisania bez uwag protokołu odbioru dostawy.<br>• Standardowy czas przystąpienia do naprawy – początek następnego dnia roboczego od daty zgłoszenia awarii.<br>• Standardowy czas naprawy wynosi 1 dzień roboczy od dnia przystąpienia do naprawy.<br>• Możliwość zgłaszania awarii bez ograniczenia czasowego (24x7).<br>• Uszkodzone dyski pozostają własnością Zamawiającego.<br>Macierz musi posiadać subskrypcje dla dostarczonego z macierzą oprogramowania oraz zapewniony dostęp do portalu serwisowego producenta umożliwiające uzyskanie dokumentacji technicznej urządzenia i systemu operacyjnego, aktualizacji firmware, bazy wiedzy przez cały okres objęcia gwarancją. |
| 18. | Certyfikaty i standardy | Deklaracja zgodności CE oferowanego urządzenia. |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

### 3.1.4. Zakres wdrożenia dostarczonej macierzy

| LP | OPIS WYMAGAŃ |
|---|---|
| 1. | Instalacja i konfiguracja konsoli Macierzy. |
| 2. | Instalacja i konfiguracji oprogramowania do monitorowania Macierzy. |
| 3. | Wykonania instalacji logicznej Macierzy, w tym konfiguracja dysków logicznych i udostępnienie zasobów dla środowiska Zamawiającego |

## 3.2. ETAP II – Uruchomienie środowiska wirtualnego - Zakres usług wdrożeniowych

### 3.2.1. Wymagania funkcjonalne dotyczące usługi wirtualizacji

Wszystkie minimalne funkcjonalności zamawianego Sprzętu i oprogramowania przedstawione w opisach komponentów wchodzących w skład dostarczanej infrastruktury, powinny być dostępne bez dodatkowych licencji lub subskrypcji w chwili odbioru przez Zamawiającego. W przypadku wymagania licencji lub subskrypcji dla przewidzianych funkcjonalności powinny one być dostarczone wraz z zamawianą infrastrukturą. W przypadku licencji lub subskrypcji ograniczonych czasowo, czas trwania nie powinien być krótszy od wymaganej gwarancji na dany sprzęt.

System wirtualizacji musi być kompletnym środowiskiem sprzętowo - programowym dedykowanym do:

- tworzenia, konfigurowania, monitorowania maszyn wirtualnych (głównie serwerów MS Windows i Linux) w liczbie co najmniej 10 szt. każdego rodzaju,
- udostępniania użytkownikom usług uruchomionych na stworzonych maszynach wirtualnych.

| Identyfikator | Opis wymagań |
|---|---|
| WFW.01. | Architektura rozwiązania musi integrować: procesory, pamięć operacyjną i pamięć masową oraz zapewniać skalowanie pionowe (architektura scale-out – rozbudowa poprzez bezprzerwowe dołożenie kolejnego urządzenia - węzła). |
| WFW.02. | Zamawiający wymaga, aby oferowane rozwiązanie do wirtualizacji posiadało funkcjonalność, w ramach której po wykryciu awarii jest możliwość uruchamiania ręcznego lub automatycznego zadań administracyjnych modyfikujących parametry maszyn wirtualnych, np. ilości vCPU, vRAM, vHDD |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| Identyfikator | Opis wymagań |
|---|---|
| WFW.03. | Zamawiający wymaga, aby oferowane rozwiązanie do monitorowania mogło automatycznie przeszukiwać zebrane dane w celu wynajdywania nadmiarowo przyznanych lub przeciążonych zasobów (CPU, RAM, HDD) |
| WFW.04. | Elementem oprogramowania systemu wirtualizacji musi być konsola do zarządzania tym systemem. |
| WFW.05. | Dostarczony przez Wykonawcę System wirtualizacji musi umożliwiać rozbudowę w przyszłości środowiska na bazie trzech serwerów fizycznych i macierzy dyskowej w taki sposób, aby zapewniona była redundancja (dostępność wszystkich usług uruchomionych na wirtualnych maszynach) na wypadek ewentualnej awarii:<br>• jednego, dowolnego serwera;<br>• jednego, dowolnego przełącznika;<br>• jednego, dowolnego fizycznego połączenia między sprzętowymi elementami<br>• systemu;<br>• jednego, dowolnego zasilacza funkcjonującego w systemie;<br>• jednego, dowolnego interfejsu funkcjonującego w systemie. |
| WFW.06. | Działający system wirtualizacji musi mieć redundantne porty do połączeń zewnętrznych (z sieciami LAN Zamawiającego) 1GbE (RJ-45) i 10Gb (SFP+) zlokalizowane w każdym serwerze i w macierzy. |
| WFW.07. | Umożliwi działom informatycznym zapewnianie różnych poziomów wysokiej dostępności aplikacji w zależności od priorytetów i potrzeb – bez konieczności stosowania złożonych rozwiązań nadmiarowego sprzętu lub oprogramowania tworzenia klastrów. |
| WFW.08. | Eliminuje konieczność planowania przestojów aplikacji wynikających z konserwacji serwerów dzięki bezpośredniej migracji maszyn wirtualnych pomiędzy serwerami bez przerywania pracy użytkowników lub ograniczenia dostępności usługi. |
| WFW.09. | Zawiera funkcję, która eliminuje konieczność planowania przestojów aplikacji wynikających z konserwacji pamięci masowej lub podczas migracji danych pomiędzy systemami pamięci masowej dzięki bezpośredniej migracji dysków maszyn wirtualnych bez przerywania pracy użytkowników lub ograniczenia dostępności usługi. |
| WFW.10. | Zawiera funkcję, która oferuje ekonomiczny, automatyczny mechanizm szybkiego ponownego uruchamiania wszystkich aplikacji w przypadku awarii sprzętu lub systemu operacyjnego. |
| WFW.11. | Zawiera funkcję, która umożliwia proste, ekonomiczne wykonywanie kopii zapasowych bez użycia agentów i odtwarzanie danych maszyn wirtualnych w mniejszych środowiskach. |
| WFW.12. | Zawiera usługi w zakresie skalowalności, które umożliwiają działom informatycznym płynne dostarczanie odpowiednich zasobów na potrzeby wszystkich aplikacji. |
| WFW.13. | Zawiera funkcjonalność, która pozwala dynamicznie równoważyć obciążenia serwerów w celu zapewnienia odpowiednich zasobów wszystkim aplikacjom na podstawie priorytetów biznesowych. Umożliwia to skalowanie aplikacji zgodnie z potrzebami. |
| WFW.14. | Zawiera funkcję, która umożliwia dodawanie procesorów i pamięci do maszyn wirtualnych zgodnie z potrzebami bez zakłóceń lub przestojów. |

| Identyfikator | Opis wymagań |
|---|---|
| WFW.15. | Pozwala dodawać (lub usuwać) do maszyn wirtualnych urządzenia dyskowe i sieciowe bez zakłóceń lub przestojów. |
| WFW.16. | Pozwala dodawać do działających maszyn wirtualnych wirtualną pamięć masową bez zakłóceń lub przestojów. |
| WFW.17. | Zamawiający oczekuje dostarczenia rozwiązania, które będzie zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz uruchomionej aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych na których uruchomiony jest wirtualizator posiadający tą funkcję |
| WFW.18. | Zamawiający wymaga dostarczenia możliwości otrzymywania uaktualnień do wirtualizatora. Zamawiający wymaga wsparcia technicznego od Wykonawcy (między innymi w przypadku ewentualnych problemów technicznych) |

### 3.2.2. Migracja Systemów i Usług Zamawiającego na środowisko wirtualne

| Identyfikator | Opis wymagań |
|---|---|
| MSW.01 | Wykonawca w porozumieniu z Zamawiającym na etapie analizy wdrożeniowej uzgodni, które Systemy Zamawiającego zostaną przeniesione na środowisko wirtualne. |
| MSW.02 | Wykonawca uruchomi środowisko wirtualne na dostarczonej infrastrukturze sprzętowej. |
| MSW.03 | Wykonawca przed przeniesieniem zapewni pełną kopię zapasową przenoszonych środowisk fizycznych. |
| MSW.04 | Wykonawca przedstawi procedurę testową potwierdzającą prawidłową migrację Systemów Zamawiającego na środowisko wirtualne zaakceptowaną przez Zamawiającego, która będzie podstawą do potwierdzenia prawidłowej migracji na środowisko wirtualne. |

### 3.2.3. Wymagania dla usługi zapewnienia ciągłości działania wdrożonego systemu wirtualizacji

Wykonawca w ramach prac wdrożeniowych z zakresu wdrożenia systemu wirtualizacji dodatkowo uruchomi poniższe funkcjonalności zapewnienia ciągłości działania i wykonywania automatycznych kopii zapasowych dla środowiska wirtualnego. Zamawiający dopuszcza zastosowanie zewnętrznej aplikacji.

| Identyfikator | Opis wymagania |
|---|---|
| CDSW.01 | Wykonawca uruchomi możliwość tworzenia kopii zapasowych dysków/partycji |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| Identyfikator | Opis wymagania |
|---|---|
| CDSW.02 | Wykonawca uruchomi możliwość tworzenia kopii zapasowych plików i folderów |
| CDSW.03 | Wykonawca uruchomi możliwość replikacji kopii zapasowych do wielu lokalizacji docelowych |
| CDSW.04 | Wykonawca uruchomi możliwość tworzenia kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT |
| CDSW.05 | Wykonawca uruchomi możliwość wykonywania kopii zapasowych w tym możliwość przywracania elementów aplikacji Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint i Microsoft Active Directory. |
| CDSW.06 | Wykonawca uruchomi możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej |
| CDSW.07 | Wykonawca uruchomi obsługę dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD |
| CDSW.08 | Wykonawca uruchomi konsolę zarządzającą dostępną z poziomu przeglądarki internetowej |
| CDSW.09 | Wykonawca przygotuje usługę zdalnej instalacji i aktualizacji agentów na komputerach klienckich. |
| CDSW.10 | Wykonawca w dostarczonym systemie zapewni możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP. |
| CDSW.11 | Wykonawca w dostarczonym systemie zapewni możliwość obsługi napędów taśmowych. |
| CDSW.12 | Wykonawca w dostarczonym systemie zapewni możliwość deduplikacji kopii zapasowych. |
| CDSW.13 | Wykonawca w dostarczonym systemie zapewni możliwość generowania planu przywracania kopii zapasowych. |
| CDSW.14 | Wykonawca w dostarczonym systemie zapewni możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach |
| CDSW.15 | Wykonawca w dostarczonym systemie przygotuje szablony schematów rotacji kopii zapasowych. |
| CDSW.16 | Wykonawca w dostarczonym systemie uruchomi automatyczne usuwanie nieaktualnych kopii zapasowych (retencja). |
| CDSW.17 | Wykonawca w dostarczonym systemie uruchomi sprawdzanie poprawności i konsolidacji kopii zapasowych (pełnych, przyrostowych i różnicowych) |
| CDSW.18 | Wykonawca w dostarczonym systemie umożliwi wykonywanie zadań i tworzenie kopii zapasowych z poziomu wiersza polecenia. |

| Identyfikator | Opis wymagania |
|---|---|
| CDSW.19 | Wykonawca w dostarczonym systemie umożliwi utworzenie ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła. |
| CDSW.20 | Wykonawca w dostarczonym systemie uruchomi współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft |
| CDSW.21 | Wykonawca w dostarczonym systemie uruchomi wysyłanie powiadomień pocztą e-mail |
| CDSW.22 | Wykonawca w dostarczonym systemie uruchomi szyfrowane kopii zapasowych algorytmem AES. |
| CDSW.23 | Wykonawca w dostarczonym systemie przygotuje funkcjonalność tworzenia dynamicznych grup urządzeń na podstawie nazwy urządzenia, ilości pamięci operacyjnej, zakresu adresów IP, typu systemu operacyjnego. |
| CDSW.24 | Wykonawca w dostarczonym systemie uruchomi wykonywanie czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie. |
| CDSW.25 | Wykonawca w dostarczonym systemie uruchomi funkcję aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem. |
| CDSW.26 | Wykonawca w dostarczonym systemie przygotuje min. 1 predefiniowany schemat tworzenia kopii zapasowych: G-F-S. |
| CDSW.27 | Wykonawca w dostarczonym systemie uruchomi priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle. |
| CDSW.28 | Wykonawca w dostarczonym systemie uruchomi możliwość włączania usług z minimalnymi prawami użytkownika. |
| CDSW.29 | Wykonawca w dostarczonym systemie uruchomi zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy. |
| CDSW.30 | Wykonawca w dostarczonym systemie zapewni pomoc techniczną w języku polskim. |
| CDSW.31 | Wykonawca w dostarczonym systemie zapewni administrowanie kontami użytkowników i jednostkami organizacyjnymi. |
| CDSW.32 | Wykonawca w dostarczonym systemie zapewni tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain. |
| CDSW.33 | Wykonawca w dostarczonym systemie zapewni wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków. |
| CDSW.34 | Wykonawca w dostarczonym systemie uruchomi:<br>• możliwość wykonywania usługi Migawek wielowoluminowych, |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| Identyfikator | Opis wymagania |
|---|---|
| | • możliwość wykonywania kopii zapasowej „sektor po sektorze",<br>• obsługę dysków dynamicznych,<br>• automatyczne ponawianie prób w przypadku niekrytycznych błędów (prób utworzenia kopii zapasowej),<br>• możliwość utworzenia nośnika startowego opartego na środowisku Linux lub WinPE. |
| CDSW.35 | Wykonawca uzgodnić z Zamawiającym rozmieszczenie poszczególnych komponentów środowiska w infrastrukturze technicznej Zamawiającego. |

## 3.3. ETAP III - Wdrożenie usługi SSO w oparciu o Centralny Katalog Użytkowników

Wykonawca w ramach realizacji Przedmiotu Zamówienia uruchomi na dostarczonej infrastrukturze minimalne następujące funkcjonalności:

Uruchomienie platformy usługi katalogowej w oparciu o:

- Usługi katalogowe oparte na dwóch kontrolerach domeny (szczegółowy zakres poniżej),
- Usługi rozpoznawania nazw domenowych DNS oraz nazw NetBIOS,
- Usługi przydzielania adresów oraz konfiguracji opcji TCP/IP z serwera DHCP,
- Usługi serwera plików z komponentami ograniczeń dyskowych, ochrony w zakresie rodzaju przechowywanych plików,
- Usługi dostępu zdalnego,
- Usługi kopii zapasowych środowiska wirtualnego oraz danych serwera plików,
- Usługi aktualizacji środowisk Microsoft,
- Usługi konfiguracji rekomendacji zabezpieczeń dla środowiska stacji roboczych oraz systemów serwerowych.

Jeżeli do prawidłowego działania usługi katalogowej wymagane jest dostarczenie dodatkowych licencji na urządzenia końcowe / użytkowników Wykonawca musi je dostarczyć. Do kalkulacji należy przyjąć co najmniej 50 komputerów końcowych / co najmniej 120 użytkowników.

Zamawiający jest podmiotem uprawnionym do zakupu i korzystania z licencji przewidzianych dla jednostek uczelnianych (EDU).

| Identyfikator | Opis wymaganych prac |
|---|---|
| CKU.01. | Instalacja oraz konfiguracja systemu operacyjnego. Zamawiający przygotuje maszyny wirtualnie z zainstalowany systemem. |
| CKU.02. | Instalacja i konfiguracja kontrolera domeny (podstawowego i zapasowego) |

| Identyfikator | Opis wymaganych prac |
|---|---|
| CKU.03. | Instalacja serwera usług terminalowych. |
| CKU.04. | Instalacja i konfiguracja serwera plików (przygotowanie struktury folderów oraz nadanie odpowiednich uprawnień, konfiguracja profili użytkowników, opracowanie i wdrożenie polityk praw dostępu do zasobów sieciowych (katalogi sieciowe), ustawienie limitów zajętości przestrzeni na poszczególnych użytkowników/grupy/zasoby. |
| CKU.05. | Wykonawca zaproponuje zarys polityk zgodnie z posiadaną wiedzą i przyjętymi dobrymi praktykami. Ostateczny kształt polityk zostanie wypracowany z Zamawiającym w trakcie spotkań roboczych podczas realizacji przedmiotu zamówienia. Zdefiniowanie polityki zgodnie z wymaganiami Zamawiającego. |
| CKU.06. | Implementacja struktury katalogowej: komputery i użytkownicy. |
| CKU.07. | Stworzenie struktury jednostek organizacyjnych, bazującej na strukturze organizacyjnej Zamawiającego, założenie kont domenowych i grup użytkowników dla wskazanych pracowników Zamawiającego umiejscowienie w strukturze jednostek organizacyjnych oraz przypisanie do odpowiednich grup zabezpieczeń. Zaprojektowanie i implementacja spójnego modelu nazewnictwa obiektów w Active Directory |
| CKU.08. | Przygotowanie procedury podłączania stacji roboczych do usługi katalogowej wraz z opracowaniem skryptów automatyzujących ten proces. |
| CKU.09. | Migracja profili lokalnych do domenowych 10 stacji roboczych opartych o Windows 7 Pro, Windows 10 Pro. |
| CKU.10. | Skonfigurowanie kopii zapasowej głównego i zapasowego kontrolera domeny. |
| CKU.11. | Migracja profili lokalnych do profili katalogowych. |

### 3.3.1. Integracja systemu SSO dla systemów Uczelni

Dla wskazanych przez Zamawiającego systemów Uczelni Wykonawca wdroży możliwość logowania się użytkowników przy wykorzystaniu mechanizmów SSO (Single Sign On) z użyciem wcześniej uruchomionego Centralnego Katalogu Użytkowników. Szczegóły realizacyjne zostaną przedstawione i uzgodnione z Zamawiającym na etapie projektu.

| Identyfikator | Opis wymaganych prac |
|---|---|
| ISSO.01 | Wykonawca dostarczy, zainstaluje i skonfiguruje Centralny Katalog Użytkowników (CKU) na potrzeby SSO. Wykonawca utworzy/zmigruje Użytkowników wewnętrznych do CKU. |
| ISSO.02 | Centralny Katalog Użytkowników musi opierać się na usługach katalogowych LDAP. W przypadku kiedy będzie to konieczne wykonawca zainstaluje lub skonfiguruje lub/i uruchomi |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

| Identyfikator | Opis wymaganych prac |
|---|---|
| | LDAP. |
| ISSO.03 | Integracja mechanizmów SSO z Centralnym Katalogiem Użytkowników opierać się musi o LDAP oraz SAML 2.0. |
| ISSO.04 | Wszystkie dostarczane w ramach Umowy aplikacje wchodzące w niniejszego zamówienia w celu autoryzacji i uwierzytelniania muszą wykorzystywać CKU. |
| ISSO.05 | Dane użytkowników do CKU będą pochodzić z istniejących systemów / istniejących katalogów LDAP, |
| ISSO.06 | Wykonawca wdroży panel do zarządzania Centralnym Katalogiem Użytkowników, w tym także integracją związaną z CKU. Szczegóły realizacyjne zostaną przedstawione i uzgodnione z Zamawiającym na etapie projektu. |

# 4. ZADANIE 2 - Rozbudowa Systemu kontroli dostępu

## 4.1. Usługi wdrożeniowe w ramach rozbudowy systemu kontroli dostępu

### 4.1.1. Rozbudowa Systemu Kontroli Dostępu wraz z integracją z SSO (Usługa katalogowa)

W chwili obecnej Zamawiający posiada wdrożony system Kontroli Dostępu w oparciu o rozwiązanie ROGER RACS4.

| Identyfikator | Opis wymaganych prac |
|---|---|
| RSKD.01 | Wykonawca przeprowadzi analizę przedwdrożeniową wynikiem której będzie projekt techniczny zawierający:<br>• plan rozmieszczenia urządzeń (czytników kart) – min. 8 punktów kontroli dostępu,<br>• plan rozmieszczenia urządzeń (czytników kart) – min. 5 punktów kodowania kart,<br>• plany zmian konfiguracji istniejącego systemu KD,<br>• projekt konfiguracji,<br>• listę dodatkowych elementów lub usług (jeśli zdaniem Wykonawcy są niezbędne),<br>• sposób integracji z systemem SSO. |
| RSKD.02 | Wykonawca dokona montażu i konfiguracji dostarczonych urządzeń Systemu KD, które będzie polegało na zainstalowaniu w miejscach uzgodnionych z Zamawiającym (zgodnie z Projektem), podłączeniu niezbędnego okablowania oraz skonfigurowaniu do dostarczonych urządzeń tak aby były one kompatybilne z posiadanym przez zamawiającego systemem ROGER. |
| RSKD.03 | Wykonawca dokona integracji istniejącego systemu ze Środowiskiem Zamawiającego, w tym integrację z Systemem SSO w uzgodnieniu z Zamawiającym. |
| RSKD.04 | Zakres wymiany danych i zasady pracy interfejsów (pkt dostępowych) muszą zostać sprecyzowane i opisane w Projekcie Technicznym. |
| RSKD.05 | W celu podłączenia dostarczonych i montowanych urządzeń wykorzystana będzie istniejąca u Zamawiającego sieć kablowa - o ile pozwalają na to warunki techniczne. W przeciwnym wypadku Wykonawca wykona odpowiednie okablowanie na własny koszt. Szacowana łączna całkowita długość okablowania 2 000 mb. |
| RSKD.06 | Zamawiający dopuszcza przeprowadzenie wizji lokalnej obiektu/miejsc, w których będą instalowane nowe punkty kontroli dostępu po wcześniejszym umówieniu spotkania. |
| RSKD.07 | Wykonawca musi uwzględnić wszystkie dodatkowe elementy niezbędne do prawidłowego uruchomienia dostarczonych elementów do Systemu Kontroli Dostępu (np. zworki, czytniki kart, zaczepy magnetyczne itp.). |


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

## 4.2. Specyfikacja techniczna elementów rozbudowy systemu Kontroli Dostępu

### 4.2.1. Specyfikacja rozbudowy istniejącego systemu KD.

Zbliżeniowe czytniki kart muszą być kompatybilne z aktualnie używanym przez Zamawiającego systemem ROGER RACS4. Ponadto Wykonawca musi zapewnić obsługę aktualnie użytkowanych kart działających w technologii UNIQUE (EM 125 kHz). Zasilanie dla elementów systemu Kontroli Dostępu musi być gwarantowane z zasilaczy buforowych. Wykonanie czytnika ma gwarantować odporność urządzenia na warunki atmosferyczne i zniszczenie.

Minimalne wymagania techniczne dla czytników kart:
- materiał poliwęglan, lub inny trwały i odporny na warunki atmosferyczne materiał,
- temperatura pracy -25°C – 60°C,
- certyfikat CE,
- stopień ochrony IP65,
- zasięg odczytu 2,5-5,0 cm.

Ostateczny zestaw niezbędnych elementów dla wskazanych miejsc lokalizacji punktów dostępowych musi dostarczyć Wykonawca i uwzględnić je w składanej ofercie.

### 4.2.2. Specyfikacja rozbudowy istniejącego systemu ELS.

Zgodnie z rozporządzeniem MNiSW z 16 kwietnia 2019 roku w sprawie dokumentacji przebiegu studiów (Dz. U. 2019, poz.787). Zamawiający jest zobowiązany do wydawania ELS (Elektronicznej Legitymacji Studenckiej). W związku z powyższym zachodzi konieczność zakupu i instalacji urządzeń do kodowania i odczytu danych dotyczących terminu ważności na spersonalizowanych ELS.

Urządzenia do kodowania i odczytu powinny być zgodne z wydawanymi przez Zamawiającego legitymacjami, a mianowicie:
Legitymacja ELS to elektroniczna karta procesorowa hybrydowa z dwoma interfejsami:
- stykowym określonym w normach ISO/IEC 7816 o pojemności pamięci 80 kB,
- bezstykowym określonym w normie ISO/IEC 14443 typ A, zgodnym ze standardem przemysłowym MIFARE® dla protokołu klasycznego o pojemności pamięci 1 kB (MIFARE® Standard Card IC MF1 IC S50 Functional Specification).

Ponadto powinny spełniać poniższe minimalne wymagania:
- interfejs USB 2.0 (Universal Serial Bus),
- zasilanie poprzez USB,
- żywotność do 100.000 cykli włożeniowych,
- wskaźnik statusu LED,
- wsparcie dla kart 5V, 3V oraz 1,8V Smart Cards, HID iCLASS®; MIFARE™ Classic/Ultra-light/Plus/DESFire,
- współpracujące systemy operacyjne Windows, Linux, Mac OS X,

- gwarancja min. 24 miesiące.

### 4.2.3. Specyfikacja systemu elektronicznego zabezpieczenia zbiorów bibliotecznych w technologii radiowej identyfikacji – RFID HF.

System będący przedmiotem zamówienia ma pracować w oparciu o technologię RFID HF (Radio Frequency Identification – identyfikacji za pomocą fal radiowych) w częstotliwości przeznaczonej do tego typu zastosowań – 13,56 MHz. Oferowany system RFID HF musi być zgodny z normami obowiązującymi w Unii Europejskiej. Urządzenia muszą posiadać niezbędne certyfikaty zgodności z normą CE.
Zamawiający wymaga, aby interfejs dla bibliotekarza oferowanych urządzeń udostępniony był w jęz. polskim. System RFID HF musi być zintegrowany z systemem bibliotecznym KOHA funkcjonującym w bibliotece.

Ta sama technologia RFID HF ma służyć do realizowania wszystkich funkcji systemu:
- identyfikacja zbiorów bibliotecznych,
- ochrona zbiorów bibliotecznych przed niekontrolowanym i bezprawnym ich wyniesieniem poza teren chroniony,
- obsługowe wypożyczenia i zwroty zbiorów bibliotecznych,
- kodowanie etykiet RFID,
- administrowanie systemem RFID,
- samodzielne wypożyczenia RFID z uwzględnieniem protokołu SIP2,
- wykonywanie skontrum i dziennego porządkowania zbiorów bibliotecznych.

**Specyfikacja ogólna systemu**

| Lp. | Opis produktu | Liczba zamawiana |
|---|---|---|
| 1 | Bramka nadawczo-odbiorcza RFID HF raportująca; trzyantenowy system bramek kontrolnych wykonany ze szkła organicznego (zabezpiecza przejście 100 cm + 100 cm) wraz ze sterownik RFID do bramek z funkcją zdalnego serwisu oraz z wbudowanym inteligentnym licznikiem osób odwiedzających) | 2 |
| 2 | Połączone stanowisko kodowania etykiet bibliotecznych RFID HF oraz wypożyczeń i zwrotów przez bibliotekarza musi zawierać: czytnik-koder etykiet RFID wraz z kablem USB 2.0. do podłączenia czytnika z komputerem oraz oprogramowanie (bez komputera stanowiskowego) a także czytnik karty czytelnika, legitymacje studenckie w standardzie MIFARE (UID) | 2 |
| 3 | Etykieta biblioteczna RFID HF z anteną aluminiową zabezpieczająca książki o rozmiarze 49x81mm TT PH S2 ISO 15693, 2,5 k bit pamięci, SLIX2. Zabezpieczona przed NFC. | 12.000 |
| 4 | Montaż urządzeń, instalacja oprogramowania, szkolenie personelu. Integracja z systemem bibliotecznym KOHA. | 1 |


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

Wymogi techniczne elementów systemu będącego przedmiotem przetargu:

1. Bramka nadawczo-odbiorcza RFID HF raportująca – 2 zestawy bramek 3 antenowych

Trzyantenowy system bramek kontrolnych wykonany z przeźroczystego szkła organicznego wraz ze sterownikiem RFID HF z funkcją zdalnego serwisu oraz z integrowanym z panelami bramki licznikiem osób.

W miejscach wskazanych przez Zamawiającego mają być zainstalowane bramki zabezpieczające, składające się z 3 anten RFID HF, osobny komplet na każde wejście. Każdorazowo przy wyjściu z biblioteki czytelnik przechodzi przez bramkę. Przy przejściu czytelnika system natychmiast powinien odczytywać informacje z etykiety RFID HF i przekazywać ją do systemu. Status książki ma być zapisany w etykiecie (EAS bit), aby system natychmiast zareagował świetlnie i dźwiękowo, w przypadku wynoszenia niewypożyczonych książek.
System powinien identyfikować równocześnie do min. 30 możliwych do odczytania obiektów.
Bramki nie mają mieć martwych kątów. Poziom detekcji i identyfikacji ma wynosić min. 95%.
Minimalne parametry techniczne bramek:

- alarm świetlny i dźwiękowy z natychmiastowym podawaniem do systemu danych odczytanych z etykiety RFID o pozycji wywołującej alarm,
- wykonanie podstawa tworzywo sztuczne w kolorze szarym o jasnym odcieniu, panel anteny – szkło organiczne - dostosowane do wymogów architektonicznych i wystroju biblioteki,
- grubość tafli szkła: 15 mm (± 5 mm),
- minimalne wymiary pojedynczej anteny: szer. 685 mm (± 15 mm), x wys. 1775 mm (± 75 mm) x grub. 70 mm (± 10 mm),
- zintegrowany sterownik RFID,
- przejście trzyantenowe, obszar chroniony: 100 + 100 cm,
- zasilanie anten systemu napięciem bezpiecznym dla człowieka, nie większym niż 24V,
- każda z anten ma być jednocześnie nadawcza i odbiorcza,
- czas reakcji alarmowej < 5ms,
- czas odczytania pamięci etykiety < 300 ms,
- pamięć czytnika powinna rejestrować do 150 zdarzeń,
- możliwość pracy z zasilaniem awaryjnym,
- możliwy zdalny serwis i strojenie przez Internet,
- możliwość ustalenia alarmu na osoby wchodzące lub wychodzące lub w obu kierunkach
- możliwość wywołania alarmu (wymaga aplikacji monitorowania),
- Inteligentny licznik osób odwiedzających zintegrowany z panelami bramki RFID HF,
- możliwość tymczasowej dezaktywacji bramki przez upoważniony personel biblioteki: programowe lub poprzez wyłączenie zasilania bramki

Urządzenie ma być przeznaczone do wykonywania statystyk odwiedzin w różnych konfiguracjach, np. dziennych, tygodniowych, kwartalnych, miesięcznych, rocznych. Służy do liczenia osób wchodzących. Urządzenie musi być wbudowane w panel anteny, tak aby stanowiło z nią integralną całość. Wymagany jest wbudowany licznik osób który na bieżąco wyświetla informację o ilości osób wchodzących na komputerze. Niezależnie od wyświetlanych informacji Zamawiający wymaga, aby stany licznika były przechowywane na komputerze

wskazanym przez Zamawiającego, z możliwością tworzenia na tej podstawie raportów alarmów i statystyk przejść.
Przechowywane przez Zamawiającego dane mają mieć możliwość eksportu do plików .xls i tekstowych.
Zamawiający wymaga, aby Wykonawca przed pod podpisaniem umowy przedstawił dostępne kolorystyki podstawy anten do wyboru przez Zamawiającego.

2. Połączone stanowisko kodowania etykiet bibliotecznych RFID HF oraz wypożyczeń i zwrotów przez bibliotekarza musi zawierać: czytnik - koder etykiet RFID HF wraz z kablem min. USB 2.0. do podłączenia czytnika z komputerem oraz oprogramowanie (bez komputera stanowiskowego).

Połączone stanowisko kodowania etykiet bibliotecznych RFID oraz wypożyczeń i zwrotów książek. Przy stanowiskach obsługi czytelnika mają być zainstalowane czytniki RFID, które będą zczytywać i identyfikować wypożyczane i zwracane do biblioteki woluminy. Czytniki powinny być zainstalowane nablatowo.

Stanowisko ma składać się z:
- czytnika - kodera etykiet RFID HF,
- anteny,
- oprogramowania,
- kabla USB,
- czytnika kart bibliotecznych (legitymacji ELS) MIFARE.

Dane techniczne czytnika - kodera etykiet RFID HF:
- urządzenie zapewniające stabilne ułożenie książki formatu A4.

Wymiary zewnętrzne urządzenia:
- długość 270 ± 90 mm,
- szerokość 235 ± 55 mm,
- wysokość 30 ± 15 mm,
- z zewnątrz mają być widoczne diody LED pokazujące status urządzenia,
- zasilanie czytnika z portu USB,
- waga max. 1,7 kg.

Obsługa programu – wymagane działanie:
Oprogramowanie powinno pozwalać na wykonanie trzech podstawowych czynności:
- kodowanie do pamięci etykiety kodu kreskowego książki,
- wypożyczanie książek z biblioteki,
- zwroty książek do biblioteki.

Wszystkie te czynności mają odbywać się w technologii RFID HF, czyli bezprzewodowego przekazywania danych pomiędzy etykietą umieszczoną w książce a czytnikiem RFID. Istotne jest prawidłowe umieszczanie książki na czytniku RFID.
Oprogramowanie musi być zintegrowane z systemem bibliotecznym.


Projekt współfinansowany przez Unię Europejską i budżet państwa ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020
ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

Komunikacja z systemem bibliotecznym może się odbywać się poprzez moduł SIP-2 (moduł SIP-2 po stronie Zamawiającego).
Urządzenia RFID przeznaczone do współpracy ze stanowiskami wypożyczalni powinny umożliwiać zmianę bitu EAS wskazanych etykiet oraz odczyt etykiet znajdujących się w przestrzeni odczytu.
Interfejs dla biblioteki w języku polskim.

3. Etykieta biblioteczna RFID HF z anteną aluminiową zabezpieczająca książki o rozmiarze 49x81 mm TT PH S2 ISO 15693, 2,5 kbit pamięci, chip NXP SLIX2.

Etykieta biblioteczna RFID HF z anteną aluminiową zabezpieczająca książki o rozmiarze 49x81 mm, pamięć 2,5 kbit Podstawowym elementem systemu jest etykieta biblioteczna RFID HF. Etykieta ta ma składać się z układu scalonego (chipa NXP SLIX2) i anteny.

Wymagane działanie:
Etykieta z anteną za pomocą fal radiowych komunikuje się z czytnikiem RFID i przesyła dane zawarte w chipie. Każda etykieta ma nadany unikalny numer, który identyfikuje książkę w bazie danych biblioteki. Etykieta jest zasilana w procesie komunikowania się przez czytnik RFID.
Etykiety biblioteczne wykonane zgodnie ze standardem ISO 15693 i normami europejskimi – i pracujące w paśmie częstotliwości: 13,56 MHz, przeznaczonej do aplikacji bibliotecznych.
Etykiety mają być przetestowane, sformatowane i przygotowane do bezpośredniego użycia w Bibliotece i kompatybilne z systemem bibliotecznym KOHA. Wymaga się aby oferowane etykiety były softwarowo zabezpieczone przed nieautoryzowanym skopiowaniem w technologii NFC.

Dane techniczne etykiety:
- rodzaj etykiety: RFID HF dedykowana do zastosowań bibliotecznych - standard I-Code SLIX2,
- read / write, czyli można dane z chipa zarówno odczytywać, jak i je zapisywać,
- ISO/IEC 15693,
- antykolizyjność, czyli możemy odczytywać w polu anteny wiele etykiet jednocześnie,
- częstotliwość pracy: 13,56 MHz,
- odporność na przepięcia elektrostatyczne min: +/- 2 kV,
- antena etykiety: aluminiowa,
- całkowita pamięć min: 2,5 k bit R/W EEPROM,
- pamięć do wykorzystania: 800 bity,
- bit zabezpieczający EAS chroniony hasłem,
- ustawiona flaga alarmowa EAS
- zabezpieczenie przed kopiowaniem,
- odporność na procesy przeprowadzane w próżniowej komorze dezynfekującej typowej dla książek,
- klej: RA-2,

- etykieta ma mieć nadany unikalny numer, który identyfikuje książkę jako własność Biblioteki,
- trwałość gwarancyjna układu scalonego: 10 lat,
- gwarantowana ilość zapisów i odczytów nie mniej niż: 100 000

Właściwości mechaniczne

- wymiar etykiety: 49 x 81 mm(± 2 mm),
- wymiar anteny: 45 x 76 mm (± 2 mm),
- powierzchnia: papier z możliwością nadruku TT,
- podkład: papier silikonowany,
- grubość etykiety: < 250 µm,
- temperatura pracy elektrycznej: co najmniej w zakresie 0 ℃/ + 60 ℃

**4.** Montaż urządzeń, instalacja oprogramowania, szkolenie personelu.

Wykonawca ma obowiązek pełnej integracji swoich urządzeń z systemem bibliotecznym KOHA. Wykonawca podłączy i uruchomi dostarczone urządzenia, aby w pełni działały i były kompatybilne z systemem bibliotecznym. Szkolenie personelu 1 dzień roboczy. Montaż urządzeń 2 dni robocze.


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360

# 5. ZADANIE 3 - Rozbudowa infrastruktury Zamawiającego

## 5.1. Rozbudowa serwera Zamawiającego

PROCESOR w ilości 1 szt. o poniższych wymaganiach:

| LP | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 1 | serwerowy procesor 6 rdzeniowy, 12 wątkowy, wyprodukowany w technologii 22 nm, identyczny z procesorem zainstalowanym w serwerze Zamawiającego. | Zamawiający posiada w rozbudowywanym serwerze procesor Intel Xeon E5-2420 v2 f=2.2 GHz z gniazdem LGA 1356, o mocy 80 W, pracujący w trybie operacyjnym 64 bit i współpracujący z pamięciami RAM typu DDR3. |

Kości pamięci RAM o poniższych wymaganiach:

| LP | CECHA | OPIS WYMAGAŃ |
|---|---|---|
| 1 | serwerowa karta pamięci RAM - 240 pinowa (w układzie DIMM) o przepustowości 12,8 GB/s | Zamawiający posiada w rozbudowywanym serwerze jeden moduł pamięci o pojemności 8GB, typu DDR3 z taktowaniem 1600 MHz. Po rozbudowie pamięć RAM serwera **musi mieć pojemność łączną 32 GB** i pracować w układzie DualChannel. Płyta główna serwera zamawiającego może obsłużyć maksymalnie 4 moduły RAM na procesor. |


ChAT przyszłości
Chrześcijańska Akademia Teologiczna w Warszawie
ul. Broniewskiego 48, 01-771 Warszawa
tel./fax: +48 22 831-95-97
telefon kom.: +48 506-002-360