Laboratorium Zaawansowanych Technik ICT, Obrazu oraz Bezpieczeństwa, Archiwizacji i Udostępniania Treści Cyfrowych (LZT)

Szczegółowy opis przedmiotu zamówienia

Spis treści

Szczegółowy opis przedmiotu zamówienia

1. Specyfikacja minimalnych wymagań technicznych

1.1. Sieciowy sprzętowy moduł bezpieczeństwa (HSM)

1. Sprzętowa akceleracja algorytmów PKI.
2. Obsługa algorytmów asymetrycznych: RSA, DSA, ECDSA.
3. Obsługa kluczy RSA o długości co najmniej 1024, 2048, 4096 i 8192 bitów.
4. Obsługa algorytmów kryptograficznych opartych o krzywe eliptyczne typu Brainpool oraz aprobowanych przez NIST.
5. Obsługa algorytmów symetrycznych: AES, DES, 3DES.
6. Obsługa algorytmów dla funkcji skrótów: SHA-1, SHA-256, SHA-384, SHA-512.
7. Wspierane interfejsy API: PKCS#11, Micosoft Crypto API (CSP), Microsoft Cryptography Next Generation (CNG), SQL Extensible Key Management (SQLEKM), Java Cryptography Extension (JCA/JCE), OpenSSL, wysokowydajny, dedykowany i natywny interfejs producenta.
8. Zgodność z certyfikatami bezpieczeństwa FIPS 140-2 na poziomie 3 i Common Criteria.
9. Procedury obsługi zgodne z zaleceniami RFC 3647.
10. Obsługa klastrowania wielu urządzeń HSM w celu uzyskania wysokiej dostępności (HA) i w celu skalowania wydajności.
11. Rozszerzona licencja umożliwiająca korzystanie z HSM dla nieograniczonej liczby użytkowników i systemów.
12. Rozszerzona licencja umożliwiająca korzystanie z wszystkich wspieranych długości kluczy szyfrujących.
13. Wysoka wydajność umożliwiająca obsługę ponad 4 tysięcy operacji kryptograficznych na sekundę.
14. Architektura dostępu uwzględniająca delegowanie uprawnień.
15. Obsługa mikroprocesorowych kart do autoryzacji i archiwizacji materiału kryptograficznego.
16. Czytnik kart mikroprocesorowych ze złączem USB.
17. Współpraca ze sprzętowym źródłem czasu.
18. Sprzętowe mechanizmy zabezpieczenia przed ingerencją w zegar HSM. Możliwość wykorzystania modułu dla usługi znakowania czasem.
19. Oprogramowanie do zarządzania w postaci aplikacji z interfejsem graficznym oraz w postaci aplikacji uruchamianej wsadowo z linii komend. Interfejs umożliwiający automatyzację czynności w przypadku integracji z platformą automatycznych testów.
20. Urządzenie jest przystosowane do montażu w szafie Rack 19”. Wysokość urządzenia nie przekracza 2U.
21. Wbudowany panel użytkownika (wyświetlacz i klawiatura) umożliwiający monitorowanie i wykonanie najważniejszych zadań administracyjnych w momencie fizycznego dostępu do urządzenia.
22. Redundantne zasilanie (2 niezależne źródła zasilania 230V) i interfejsy sieciowe (2 porty z wsparciem dla 802.3ad i protokołu LACP).
23. Certyfikaty CE, FCC Class B, IEC/EN 60950-1, RoHS II, WEEE.

1.2. Sieciowy serwer czasu z odbiornikiem GPS i wzorcem czasu (TIME)

1. Redundantne interfejsy sieciowe (2 porty z wsparciem dla 802.3ad i protokołu LACP).
2. Protokół sieciowy zaawansowanej synchronizacji NTP z obsługą wersji 2, 3 i 4.
3. Protokół sieciowy prostej synchronizacji SNTP z obsługą wersji 3 i 4 oraz TIME.
4. Protokół administracyjny HTTP/HTTPS/SSH.
5. Zewnętrzne źródło synchronizacji czasu oparte o GPS i antenę zewnętrzną.
6. Dokładność zegara po jednym dniu pracy bez GPS +/- 250us.
7. Przystosowany do użycia jako wzorzec czasu dla usługi kryptograficznej TSA. Serwer czasu jest kompatybilny z usługą elektronicznej pieczęci.
8. Oprogramowanie monitorujące działanie usługi oraz rejestrujące dostępność z punktu widzenia SLA. Możliwość tworzenia raportów w ujęciu dziennym, miesięcznym i rocznym. Monitoring powinien uwzględniać zarządzanie czasem dla nieograniczonej liczby urządzeń.
9. Szablony konfiguracji synchronizacji czasu dla urządzeń sieciowych i serwerów Linux wykorzystujące protokół NTP oraz PTP.

1.3. Zestaw narzędzi dla programistów do sprzętowego modułu bezpieczeństwa (SDKHSM)

SDK (Software Development Kit) to tzw. pakiet deweloperski umożliwiający implementowanie własnych aplikacji uruchamianych bezpośrednio na urządzeniach HSM.

1. SDK jest kompatybilne z dostarczonym w ramach zamówienia sieciowym sprzętowym modułem bezpieczeństwa.
2. SDK zapewnia możliwość tzw. customizacji (dostosowywania) oprogramowania modułu HSM do nowych wymagań i potrzeb związanych z przyszłymi pracami rozwojowymi.
3. SDK obejmuje kompletne środowisko do tworzenia i dystrybucji rozszerzeń funkcjonalnych do HSM.
4. Zestaw narzędzi dla programistów z niezbędnymi składnikami do pisania własnych skryptów i rozszerzeń do sprzętowych modułów bezpieczeństwa. Narzędzia obejmują prekonfigurowane graficzne środowisko programistyczne z obsługą debugowania.
5. SDK zawiera szczegółową dokumentację i gotowe wzorce implementacyjne dla obsługiwanych interfejsów API: PKCS#11, MS CAPI/CNG, JCA/JCE, native.

1.4. Oprogramowanie Centrum Certyfikacji współpracujące z HSM (CC)

1. Pełna integracja ze sprzętowym modułem bezpieczeństwa HSM (certyfikat bezpieczeństwa wg normy FIPS-140-2 na poziomie 2 i 3).
2. Możliwość uruchomienia instalacji testowej bez konieczności posiadania HSM oraz w trybie programistycznej symulacji HSM.
3. Obsługa wszystkich nowoczesnych i bezpiecznych algorytmów zalecanych przez eIDAS (funkcje skrótu SHA-256/SHA-512 i klucze RSA o długości 2048/4096/8192 bitów).
4. Automatyczna obsługa repozytorium certyfikatów, list CRL, usługi OCSP, znakowania czasem TSA.
5. Możliwość pracy w trybie podwyższonego bezpieczeństwa (tzw. tryb off-line).
6. Współpraca z klastrami wielu urządzeń HSM w celu uzyskania wysokiej dostępności (HA) i w celu skalowania wydajności.
7. Licencja umożliwiająca wykorzystanie dla nieograniczonej liczby użytkowników, systemów, certyfikatów i ośrodków certyfikacji.
8. Licencja umożliwiająca korzystanie z wszystkich wspieranych przez HSM długości kluczy szyfrujących.
9. Procedury planowania, instalacji, uruchomienia i eksploatacji Centrum Certyfikacji.
10. Dokumentacja zgodna z zaleceniami RFC 3647.
11. Oprogramowanie ma zostać wdrożone w instancji testowej bez wykorzystania HSM oraz w instancji produkcyjnej z wykorzystaniem HSM. Wdrożenie musi obejmować opracowanie kompletnej dokumentacji i procedur pracy dla CC (w szczególności polityka certyfikacji, kodeks certyfikacyjny, repozytorium OID).
12. Szczegółowa specyfikacja techniczna oraz wyniki przeprowadzonej analizy wymagań stanowią tajemnicę przedsiębiorstwa Zamawiającego. Z tego powodu nie są ujęte w tym dokumencie, który zawiera część jawną. Procedura dostępu do części poufnej została określona w głównym zapytaniu.

1.5. Oprogramowanie sieciowych usług składania i weryfikacji podpisu zgodna z EIDAS (EIDAS)

1. Składanie i weryfikacja podpisów elektronicznych zgodnych ze standardami eIDAS.
2. Zgodność ze standardami ETSI: EN 319 102, EN 319 132, EN 319 172, EN 319 312, TS 119 612.
3. Formaty podpisów elektronicznych: XADES, PADES, CADES oraz ASiC.
4. Obsługa list dostawców usług zaufania (TSL).
5. Weryfikacja certyfikatów na podstawie list CRL oraz za pomocą usługi OCSP.
6. Weryfikacja certyfikatów kwalifikowanych i niekwalifikowanych.
7. Weryfikacja: podpisów elektronicznych, pieczęci elektronicznych oraz znaczników czasu. Obejmuje weryfikację podpisu profilem zaufanym.
8. Architektura: usługi w modelu mikrousług uruchamianych w środowisku wirtualizacji na poziomie systemu operacyjnego (operating system level virtualization) – tzw. kontenery Docker.

9. Współpraca z klastrami wielu urządzeń HSM w celu uzyskania wysokiej dostępności (HA) i w celu skalowania wydajności.
10. Obsługa IPv4 i IPv6. Zgodność z protokołami HTTP/HTTPS oraz RESTful. Pełne wsparcie w zakresie wykorzystania zewnętrznych serwerów typu proxy i reverse proxy.
11. Możliwość wykorzystania sprzętowego modułu bezpieczeństwa HSM (protokoł PKCS#11 lub CSP).

1.6. Środowisko do wirtualizacji i dystrybucji oprogramowania (WDO)

1. Możliwość obsługi wielu instancji różnych systemów operacyjnych na jednym serwerze fizycznym.
2. Możliwość skonfigurowania wielordzeniowych maszyn wirtualnych, z możliwością przydzielenia każdej maszynie co najmniej 128GB pamięci operacyjnej oraz co najmniej 4 wirtualnych kart sieciowych, 4 porty szeregowe, 8 urządzeń USB.
3. Możliwość łatwej i szybkiej rozbudowy infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych usług.
4. Wsparcie dla systemów operacyjnych: Windows 7/8/10, Windows Server 2012/2016, RHEL/CentOS 5/6/7, Debian, Ubuntu 7.04.
5. Obsługa wielordzeniowych i wielowątkowych procesorów oraz nie mniej niż 512GB RAM. Możliwość przydzielenia większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
6. Konsola do zarządzania maszynami wirtualnymi i do konfigurowania pozostałych funkcjonalności.
7. Możliwość ciągłego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. CPU, pamięć RAM, przestrzeń dyskowa, dostęp do pamięci masowej, ruch sieciowy) oraz przechowywać i wyświetlać dane historyczne.
8. Możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania pracy systemu.
9. Możliwość wielokrotnego klonowania systemów operacyjnych.
10. Możliwość integracji z usługami katalogowymi Microsoft Active Directory i LDAP.
11. Mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej bez potrzeby wyłączania wirtualnych maszyn.
12. Możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi (bez konieczności wykorzystywania współdzielonego storage).
13. Możliwość wykorzystywania dysków SSD jako pamięć buforującą.
14. Rozwiązanie zapewniające odpowiednią redundancja i mechanizmy wysokiej dostępności (HA) automatyzujące usuwanie awarii.
15. Funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnych łączących maszyny wirtualne oraz sieci zewnętrzne.
16. Wirtualne karty i wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
17. Repozytorium pakietów oprogramowania z obsługą podpisu i jego weryfikacji. Wsparcie dla protokołów HTTP/HTTPS oraz FTP. Obsługa rozproszonych repozytoriów z automatyczną replikacją. Integracja z systemami ciągłej konsolidacji. Interfejs umożliwiający wybór różnych gałęzi stabilności oprogramowania (wersje stabilne, testowe, rozwojowe itp.). Obsługa kontroli dostępu oraz dystrybucji licencji. Możliwość integracji z CA i wykorzystania rozwiązań PKI do uwierzytelniania oraz podpisywania.
18. Środowisko ma umożliwić tworzenie i dystrybucję zaawansowanych produktów komputerowych jako:
    a. urządzeń specjalizowanych (tzw. appliance) łączących dedykowaną platformę sprzętową z oprogramowaniem,
    b. SaaS (ang. software as a service) dystrybuowanego w chmurze internetowej.

1.7. Rozbudowa i aktualizacja oprogramowania szkieletowej platformy aplikacyjnej do budowy systemów rozproszonych (RIS2)

Efektywność to podstawowa wymagana cecha technologii, która powinna zapewnić systemowym rozwiązaniom RIS posiadanym przez Wnioskodawcę przewagę nad konkurencją. Nowe rozwiązania zastosowane w RIS muszą

umożliwiać efektywne dostosowywanie systemu do zmieniających się potrzeb klienta biznesowego. Posiadane rozwiązania zorientowane na systemy automatyki przemysłowej takiej elastyczności nie posiadają.

Jako podstawowe wyznaczniki wymagań w tym zakresie przyjęto dobre praktyki z dziedziny współczesnych systemów IT takie jak: wykorzystanie możliwości oferowanych przez modele pracy w chmurze IaaS oraz PaaS, zwinne (Agile) metodyki rozwoju systemu oraz pryncypia DevOps, łącznie minimalizujące okres czasu niezbędny do uzyskania produktu rynkowego (Time to Market) przez klientów systemów automatyki przemysłowej.

Po zaimplementowaniu aktualizacji zintegrowana ulepszona technologia RIS musi zapewniać dużą efektywność poprzez uwzględnienie już na poziomie architektury oraz szkieletu aplikacyjnego uwarunkowań, wynikających z efektywnych procesów budowy, wdrażania, eksploatacji i rozwoju.

Mechanizmy zapewniające efektywność muszą obejmować m.in. zastosowanie wirtualizacji na poziomie systemu operacyjnego (tzw. kontenerów) komponentu sprzętowego, zunifikowane rozwiązania architektoniczne, sprzętowe i programowe wsparcie dla procedur z zakresu continous integration oraz continous delivery, stanowiące zbiór dobrych praktyk w branży IT a dotychczas niewykorzystywane w dziedzinie sterowania przemysłowego.

Ponieważ efektywność procesów budowy, wdrażania, rozbudowy systemu sterowania może pociągać za sobą zwiększenie ryzyk biznesowych, ulepszona technologia RIS musi zawierać również integralne mechanizmy zapewniające bezpieczeństwo i niezawodność. Integralne dla uzyskania efektywności jest dostarczenie razem z komponentami aplikacyjnymi założeń Modelu Procesu budowy, wdrażania, eksploatacji i rozwoju.

Ulepszone w wyniku aktualizacji Środowisko RIS wraz z Modelem Procesu musi tworzyć kompletny, spójny ekosystem, którego efektywność będzie oceniana przez:

- krótki czas wdrożenia systemu sterowania/zarządzania.
- szybkie wprowadzanie zmian do niego.

Główne parametry odbioru aktualizacji platformy RIS:

1. Czas pełnego cyklu automatycznego budowania, automatycznej integracji, wdrożenia w środowisku testowym, automatycznego testowania, tworzenia wersji dystrybucyjnej modułów oprogramowania, dystrybucji modułów oprogramowania na wszystkie komponenty sprzętowe przeciętnej instalacji powinien zostać skrócony co najmniej do poziomu 30%.
2. Ilość wersji konfiguracji całego systemu (w tym wersji modułów oprogramowania, wersji parametrów konfiguracyjnych, wersji oprogramowania układowego), które mogą jednocześnie zostać zainstalowane i gotowe do uruchomienia w komponentach sprzętowych systemu sterowania. Obecnie, z uwagi na brak rozwiązań zintegrowanego zarządzania konfiguracją i wersjami możliwe jest funkcjonowania tylko i wyłącznie 1 wersji. W wyniku wdrożenia aktualizacji, przy zastosowaniu przeciętnej konfiguracji komponentów sprzętowych musi być możliwe uzyskanie co najmniej 20 jednoczesnych wersji konfiguracji całego systemu.
3. Ilość wyizolowanych kontenerów dla modułów oprogramowania możliwych do jednoczesnego uruchomienia na przeciętnej konfiguracji komponentu sprzętowego. Dotychczas, z uwagi na brak rozwiązań wirtualizacyjnych nie jest możliwe wydzielenie wyizolowanych kontenerów, stąd wszystkie moduły muszą działać w jednym wspólnym środowisku. W wyniku wdrożenia aktualizacji, przy zastosowaniu przeciętnej konfiguracji komponentów sprzętowych musi być możliwe uruchomienie co najmniej 25 wyizolowanych kontenerów dla modułów oprogramowania.

Szczegółowa specyfikacja techniczna oraz wyniki przeprowadzonej analizy wymagań dla rozbudowy i aktualizacji RIS stanowią tajemnicę przedsiębiorstwa Zamawiającego. Z tego powodu nie są ujęte w tym dokumencie, który zawiera część jawną. Procedura dostępu do części poufnej została określona w głównym zapytaniu.

1.8. Wielowarstwowy analizator ruchu sieciowego o wysokiej przepustowości (ANAL)

1. Obsługa interfejsów w technologii 40GigaEthernet, 10GigaEthernet i 1GigaEthernet.
2. Administracja w oparciu o protokoły: SSH, HTTP/HTTPS, SNMP v1, v2c, v3, SNMP TRAP.

3. Rozbudowane mechanizmy filtrowania ruchu.
4. Język zapytań obejmujące wszystkie warstwy ruchu sieciowego. Kompatybilność z formatem tcpdump/Wireshark.
5. Mechanizmy notyfikacji dla wykrywanych anomalii.
6. Wysokowydajna pamięć nieulotna zapewniająca rejestrację ruchu z wydajnością powyżej 10 gigabitów przez okres co najmniej 5 minut.
7. Pamięć nieulotna zapewniająca rejestrację ruchu z wydajnością powyżej 1 gigabita przez okres co najmniej 8 h.
8. Analizator jest wyposażony w kieszeń umożliwiającą zgrywanie danych na zewnętrzne nośniki SATA 2,5/3,5”. Kieszeń obsługuje zarówno dyski talerzowe HDD oraz pamięciowe SSD.
9. Mechanizm monitorowania obciążenia i zbierania dziennika zdarzeń z urządzeń sieciowych (przełączniki, routery, firewalle). Raportowanie graficzne w różnych wariantach i okresach.
10. Moduł monitorowania obciążenia dla środowisk do wirtualizacji.
11. Moduł monitorowania konfiguracji urządzeń sieciowych.
12. Analizator jest wyposażony w ekran (lub ekrany) o rozdzielczości co najmniej 4 milionów pikseli.
13. Analizator ma umożliwić kompleksową diagnostykę i rozwiązywanie trudnych problemów sieciowych podczas realizacji prac rozwojowych dla zastosowań sieciowych i aplikacyjnych.
14. Analizator ma umożliwiać wykonywanie różnorodnego typu audytów bezpieczeństwa i testów wydajności infrastruktury.

1.9. Zaawansowany symulator rzeczywistego ruchu sieciowego z obsługą interfejsów 1/10/40GigaEthernet (SYM)

1. Obsługa interfejsów w technologii 40GigaEthernet, 10GigaEthernet i 1GigaEthernet.
2. Administracja w oparciu o protokoły: SSH, HTTP/HTTPS, SNMP v1, v2c, v3, SNMP TRAP.
3. Generowanie ruchu sieciowego ICMP/TCP/UDP w oparciu o popularne profile użytkowe.
4. Generowanie zaawansowanego ruchu sieciowego IPv4/IPv6 w oparciu o zaawansowane algorytmu programowane przy użyciu skryptów i języków programowania.
5. Wysokowydajna pamięć nieulotna o pojemności powyżej 512GB do przechowywania wzorców ruchu o wydajności odczytu powyżej 3GBajtów/s.
6. Pamięć nieulotna umożliwiająca przechowywanie historycznych dzienników generowanego ruchu o pojemności powyżej 6TB.
7. Generowanie ruchu wysokopoziomowego dla testów aplikacyjnych (w tym: testy wydajnościowe baz danych SQL, testy wydajnościowe platform wirtualizacyjnych, testy wydajnościowe serwerów WWW/RESTapi).
8. Możliwość uruchamiania dedykowanych modułów aplikacyjnych do generowania rzeczywistych szablonów ruchu dla dowolnych (w tym przyszłych) protokołów aplikacyjnych. Infrastruktura pisania i uruchamiania modułów powinna uwzględniać co najmniej 4 różne i popularne języki programowania.
9. Tworzenie harmonogramów i zapamiętanych customizacji dla profilów ruchu.
10. Obsługa profilów symulujących problemy sieciowe (przeciążenie sieci, ataki DDoS, DoS, skanowanie sieci).
11. Symulator ma umożliwić kompleksowe i zautomatyzowane przeprowadzanie testów wydajnościowych podczas realizacji prac rozwojowych dla zastosowań sieciowych i aplikacyjnych.
12. Symulator ma umożliwić wykonywanie audytów bezpieczeństwa i wydajności infrastruktury.

1.10. Zarządzalny przełącznik sieciowy (SW)

1. Obsługa interfejsów w technologii 10GigaEthernet i 1GigaEthernet.
2. Zgodność ze standardami sieciowymi IEEE 802.1x, 802.1s, 802.1w, 802.3x, 802.3ad, 802.1D, 802.1p, 802.1Q, 802.3u 100BASE-T, 802.3z 1000BASE-X, 802.3ab 1000BASE-T.
3. Obsługa protokołów rutowania RIP, OSPF.
4. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a) Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi.
    b) Mechanizm automatycznej konfiguracji portów do obsługi VoIP

   c) Możliwość ograniczania pasma dostępnego na port (rate limiting) z granulacją co 1Mbps dla ruchu wejściowego i wyjściowego.
5. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
   a) Wiele poziomów dostępu administracyjnego poprzez konsolę
   b) Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2
   c) Możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS lub TACACS+
   d) Monitorowanie zapytań i odpowiedzi DHCP (tzw. DHCP Snooping)
   e) Przełącznik powinien umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu.
   f) Ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe.
   g) Obsługa list kontroli dostępu (ACL) z uwzględnieniem adresów MAC i IP, portów TCP/UDP bez spadku wydajności urządzenia.
   h) Współpraca z systemami kontroli dostępu do sieci typu NAC, NAP itp.
6. Przełącznik musi zapewniać podstawową obsługę ruchu IP Multicast, w tym funkcjonalność IGMP.
7. Przełącznik musi umożliwiać obsługę grupowania portów w jeden kanał logiczny zgodnie z LACP.
8. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
9. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
10. Przełącznik musi mieć możliwość montażu w szafie 19”, wysokość nie większą niż 1RU oraz obudowę wykonaną z metalu.

1.11. Profesjonalny tablet graficzny LCD (TABG)

Profesjonalny tablet graficzny zintegrowany z wyświetlaczem IPS. Specyfikacja wymagań minimalnych:

1. Rozdzielczość ekranu: FullHD lub wyższa, zalecana UltraHD.
2. Przekątna ekranu: od 24” do 28”.
3. Obsługa sprzętowej kalibracji kolorów. Zalecane pokrycie Adobe RGB Gamut: 98% lub więcej
4. Wrażliwość nacisku: co najmniej 10 bitowa, zalecana 12 bitowa.
5. Pióro: czułe na nacisk, bezprzewodowe, bezbateryjne, dodatkowe przyciski, wymienne końcówki, różne typy końcówek.
6. Technologia pozycjonowania: rezonans elektromagnetyczny (rozdzielczość ponad 4000 DPI)
7. Port graficzny: DisplayPort/HDMI/DVI
8. Port komunikacyjny: USB
9. Komplet okablowania.
10. Oprogramowanie graficzne z dostępem do aktualizacji przez co najmniej 3 lata.
11. Kompatybilność z Windows 7/8/10 i Mac OS X.

1.12. System kalibracji i zarządzania kolorem (CMS)

1. System ma zapewnić przenośność barwy w przepływie pracy i niezależność barw od stosowanych urządzeń.
2. Obsługa kalibracji urządzeń typu: kamera cyfrowa, aparat fotograficzny, monitor komputerowy, ekran TV, projektor, drukarka, ploter.
3. Wsparcie dla algorytmów przekształcania modeli barw. Kompatybilność ze standardami DCI (Digital Cinema Initiatives). Zgodność z normami ETSI, wsparcie dla obrazu HDR (High-dynamic-range imaging), sRGB, Rec. 709, Rec. 2020, Rec. 2100, oraz standardem ACES. Kompatybilność z oprogramowaniem Adobe CC, DaVinci Resolve, Avid,
4. Brak ograniczeń licencyjnych na liczbę monitorów, stanowisk i urządzeń objętych systemem.

5. Sonda kalibracyjna dla monitorów LCD/LED/OLED. Sonda kalibracyjna dla drukarek. Sprzętowy pomiar metodą kolorymetryczną oraz spektrofotometryczną. Zestaw kalibracyjny dla aparatów i kamer. Referencyjne materiały projekcyjne.

1.13. Film promocyjno-instruktażowy (FPROM)

Zamawiający w ramach zaplanowanych działań marketingowych będzie wykorzystywał film promocyjno-instruktażowy o realizowanym projekcie. Wykonawca będzie zobowiązany o przekazanie materiałów multimedialnych dotyczących dostaw objętych niniejszą umową. Jakość materiałów powinna być nie gorsza niż UltraHD/4K dla materiałów wideo i 20 milionów pikseli dla materiału fotograficznego. Osoby realizujące instalację, konfigurację i wdrożenie elementów niniejszej dostawy mogą zostać zarejestrowane głosowo oraz sfilmowane. Wizerunek tych osób zostanie wykorzystany w tworzonym materiale audio-wizualnym. W związku z powyższym Wykonawca zobowiązuje się dostarczyć stosowne zgody na wykorzystanie wizerunku tych osób w tworzonym materiale multimedialnym.

Wykonawca zaproponuje dwie wersje scenariusza w terminie 2 tygodni od podpisania umowy. Zamawiający zaakceptuje zaproponowany scenariusz albo przekaże uwagi w terminie 10 dni od otrzymania scenariusza. Zamawiający zastrzega sobie prawo przekazania własnej wersji scenariusza jeżeli żadna z zaproponowanych wersji przez Wykonawce nie spełni jego oczekiwań.

Muzyka zaproponowana przez wykonawcę zamówienia, musi zostać zaakceptowana przez Wnioskodawcę. Licencja dotycząca muzyki jest kosztem Wykonawcy zamówienia.

Na realizację filmu przewidywane są 2 dni zdjęciowe. Zapewnienie niezbędnego sprzętu filmowego, oświetleniowego i dźwiękowego leży po stronie wykonawcy.

Czas projekcji filmu: 2-3 minuty (zgodnie z zaakceptowanym scenariuszem), obraz UltraHD/4K z efektami slow motion (do 1000 klatek na sekundę, zgodnie z zaakceptowanym scenariuszem).

Dodatkowo zostanie zmontowana wersja skrócona filmu o czasie projekcji 30 – 60 sekund.

Wykonawca przeniesie na Zamawiającego nieograniczone terytorialnie prawa własności intelektualnej do filmu i wszystkich elementów składowych (w tym w szczególności do scenariusza, muzyki, montażu, elementów multimedialnych i graficznych) na wszystkich znanych polach eksploatacji, ze szczególnym uwzględnieniem:

1. trwałego lub czasowego zwielokrotnienia w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie;
2. stosowania, wyświetlania, przekazywania i przechowywania niezależnie od formatu, systemu lub standardu
3. tłumaczenia, przystosowywania, zmiany układu lub dokonywania jakichkolwiek innych zmian;
4. rozpowszechniania oryginału lub kopii;
5. wyrażania zgody na rozporządzanie i korzystanie z opracowania.

Wykonawca zobowiązuje się do przeniesienia na Zamawiającego posiadanych licencji lub autorskich praw majątkowych, praw pokrewnych i udzielenia zezwolenia na wykonywanie praw zależnych utworów wykonanych przez Wykonawcę.

Film nie jest wydatkiem kwalifikowanym z punktu widzenia wniosku o dofinansowanie. Z tego powodu jest realizowany w całości z środków własnych Zamawiającego.

2. Gwarancja

Dostarczony sprzęt musi posiadać gwarancję na okres minimum 3 lat wraz z naprawą na miejscu instalacji z czasem 24h w dni robocze na przywrócenie sprawności sprzętu. W przypadku awarii nośników danych i materiału kryptograficznego uszkodzony nośnik pozostaje u Zamawiającego. W ramach gwarancji Zamawiający ma prawo dostępu do wszelkich aktualizacji dokumentacji, oprogramowania układowego i wspomagającego związanego z dostarczonym sprzętem.

3. Asysta techniczna

Dostarczone oprogramowanie musi zostać objęte co najmniej 1 roczną asystą techniczną. W ramach asysty technicznej Zamawiający ma dostęp do wszystkich aktualizacji oprogramowania i wsparcia technicznego. Wsparcie techniczne jest dostępne co najmniej przez 8h każdego dnia roboczego.

Czas na usuwanie zgłoszonych błędów w oprogramowaniu to maksymalnie 7 dni roboczych.