Znak postępowania: ZP-361-12/13/I

Załącznik nr 3 do SIWZ
(wzór)

Specyfikacja techniczna przedmiotu zamówienia

I. Część 1 – dostawa sprzętu komputerowego i oprogramowania na potrzeby Sądu Okręgowego w Białymstoku, ul. M. Skłodowskiej-Curie 1:

1. Firewall/UTM 1 szt.

Nazwa producenta ……..…….

Typ …….

Model (oznaczenie) ……

Lp.	Wymagania minimalne Zamawiającego	Charakterystyka proponowanego przez Wykonawcę wyrobu	Uwagi
1.	Urządzenie dostarczane jest jako dedykowane urządzenie sieciowe 2U, przystosowane do montażu w szafie rack.	TAK / NIE *)	
2.	Urządzenie powinno być wyposażone w 6 interfejsów Gigabit Ethernet 10/100/1000 TX.	TAK / NIE *)	
3.	W urządzeniu istnieje możliwość uruchomienia dodatkowych interfejsów sieciowych (Gigabit Ethernet, Gigabit Ethernet PoE, SFP, T1, E1)	TAK / NIE *)	
4.	Urządzenie obsługuje protokoły dostępowe warstwy 2 OSI co najmniej: Frame Relay, Ethernet (z obsługą co najmniej 4096 sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q) oraz Point-to-Point Protocol/High level Data Link Control.	TAK / NIE *)	
5.	Urządzenie powinno posiadać osobne moduły kontroli oraz przetwarzania ruchu w postaci osobnych zasobów sprzętowych.	TAK / NIE *)	
6.	W urządzeniu powinien być zainstalowany nadmiarowy zasilacz AC.	TAK / NIE *)	
7.	Urządzenie posiada minimum 2GB RAM pamięci operacyjnej (DRAM).	TAK / NIE *)	
8.	Urządzenie powinno pracować pod kontrolą modularnego systemu operacyjnego, w którym możliwe jest zrestartowanie poszczególnych usług bez przerwy w pracy urządzenia.	TAK / NIE *)	
9.	System zabezpieczeń powinien realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz oferować możliwość kontroli na poziomie aplikacji w oparciu o moduł prewencji włamań IPS	TAK / NIE *)	
10.	Urządzenie zabezpieczeń powinno posiadać dedykowany układ sprzętowy przyspieszający działanie modułu IPS.	TAK / NIE *)	
11.	Moduł IPS powinien wykrywać ataki bazując co najmniej na wymienionych metodach: Detekcja anomalii protokołów, detekcja w oparciu o sygnatury pełno-stanowe, detekcja w oparciu o złożenie metod detekcji anomalii protokołów oraz sygnatur pełno-stanowych	TAK / NIE *)	
12.	Sygnatury systemu IPS powinny być aktualizowane nie rzadziej niż raz na dzień.	TAK / NIE *)	
13.	System IPS powinien oferować różne możliwości reagowania na incydenty: Brak akcji, oznaczanie pakietów wartościami DSCP, zaprzestanie dalszego skanowania ruchu z wykrytym atakiem, zamykanie całego połączenia, zamykanie połączenia z wysłaniem pakietu RST do klienta, zamykanie połączenia z wysłaniem pakietu RST do serwera, zamykanie połączenia z wysłaniem pakietów RST	TAK / NIE *)	

	zarówno do klienta jak i do serwera oraz akcji rekomendowanej przez producenta platformy zabezpieczeń. Dodatkowo powinien oferować akcje dotyczące wyszczególnionego ruchu pomiędzy danymi adresami IP: powiadamianie, ciche blokowanie pakietów należących do danej sesji, zamykanie nowych sesji dotyczących danych adresów IP poprzez wysłanie pakietów RST		
14.	Powiadomienie systemu IPS powinno przybierać różne formy: Alarmowanie, wysyłanie maili, uruchomienie skryptów, ustawienie poziomów ważności zdarzeń.	TAK / NIE *)	
15.	Urządzenie powinno posiadać wbudowany moduł kontroli antywirusowej z możliwością skanowania całych plików, wielokrotnie spakowanych (co najmniej 4 poziomy) dla ruchu http, FTP, SMTP, POP3, IMAP. Baza wzorców wirusów nie powinna być mniejsza niż 400 000 wpisów.	TAK / NIE *)	
16.	Urządzenie zabezpieczeń posiada wbudowany moduł filtrowania treści stron WWW wywoływanych przez użytkowników umożliwiający blokowanie adresów URL oraz adresów IP w oparciu o dostarczone przez producenta lub własne kategorie. Włączenie filtrowania treści stron WWW nie wymaga dodatkowego serwera. Istnieje możliwość samodzielnego tworzenia lokalnych białych i czarnych list adresów URL. Zewnętrzna baza adresów URL, z której korzysta system, nie powinna być mniejsza niż 26 milionów adresów z podziałem na kategorie.	TAK / NIE *)	
17.	Urządzenie zabezpieczeń posiada wbudowany moduł do filtrowania ruchu pozwalający określić niepożądany w sieci typ ruchu na podstawie następujących kryteriów: MIME, rozszerzenia plików, polecenia protokołów, oraz dla ruchu http blokowanie kontrolek ActiveX, apletów Java, obiektów Cookie, plików EXE oraz ZIP.	TAK / NIE *)	
18.	Urządzenie zabezpieczeń posiada wbudowany moduł antyspamowy z możliwością blokowania oraz oznaczania wiadomości e-mail.	TAK / NIE *)	
19.	System zabezpieczeń powinien wykrywać i blokować ataki intruzów (in-line IDS), posiadać mechanizmy zarządzania pasmem sieci (QoS) oraz zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site.	TAK / NIE *)	
20.	Urządzenie zabezpieczeń posiada przepływność co najmniej 5,5 Gbps dla firewall (duże pakiety), 1 Gbps dla VPN (3DES), 800 Mbps dla IPS, 300 Mbps dla AV i obsługuje 375 000 jednoczesnych sesji.	TAK / NIE *)	
21.	System zabezpieczeń powinien działać w trybie rutera (tzn. w warstwie 3 modelu OSI).	TAK / NIE *)	
22.	Sieci VPN tworzone przez system zabezpieczeń działają poprawnie w środowiskach sieciowych, gdzie na drodze VPN wykonywana jest translacja adresów NAT. System zabezpieczeń posiada zaimplementowany mechanizm IPSec NAT Traversal dla konfiguracji VPN client-to-site oraz site-to-site.	TAK / NIE *)	
23.	Sieci VPN site-to-site mogą działać w konfiguracjach Meshed VPN oraz Hub&Spoke. System zabezpieczeń posiada zaimplementowane mechanizmy monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności (tzn. po wykryciu nieaktywności tunelu automatycznie następuje negocjacja IKE).	TAK / NIE *)	

24.	Konfiguracja VPN powinna odbywać się w oparciu o reguły polityki bezpieczeństwa (Policy-based VPN) oraz ustawienia rutingu (Routing-based VPN).	TAK / NIE *)	
25.	W jednym urządzeniu można definiować wirtualne rutery, gdzie każdy z nich posiada swoje indywidualne tabele rutingu. Urządzenie obsługuje ruting statyczny oraz protokoły dynamicznego rutingu jak OSPF i BGP. Urządzenie zabezpieczeń wykonuje ruting IP na bazie adresu miejsca przeznaczenia pakietów oraz adresu źródłowego (tzw. source-based routing).	TAK / NIE *)	
26.	Polityka bezpieczeństwa systemu zabezpieczeń uwzględnia strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).	TAK / NIE *)	
27.	System zabezpieczeń wykrywa i blokuje techniki i ataki stosowane przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan), blokuje adresy URL i niebezpieczne komponenty (m.in. Java/ActiveX/zip/exe), chroni sieci VPN przed atakami powtórzeniowymi (Replay Attack) oraz limituje maksymalną liczbę otwartych sesji z jednego adresu IP.	TAK / NIE *)	
28.	Zarządzanie mechanizmami zabezpieczeń w pełnym zakresie odbywa się z linii poleceń (CLI) oraz graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci są zabezpieczone kryptograficznie (tzn. wykonywane jest szyfrowanie komunikacji). System zabezpieczeń musi udostępniać możliwość zdefiniowania wielu kont administratorów o różnych poziomach uprawnień. Administratorzy powinni być uwierzytelniani za pomocą haseł statycznych, RADIUS, TACACS+.	TAK / NIE *)	
29.	Z jednej, centralnej konsoli zarządzania GUI odbywa się całość konfiguracji systemu operacyjnego (m.in. adresacja i ruting IP) i zabezpieczeń (m.in. obiekty, polityka bezpieczeństwa firewall i VPN).	TAK / NIE *)	
30.	System zabezpieczeń umożliwia wykonywanie uwierzytelniania tożsamości użytkowników za pomocą haseł statycznych i dynamicznych. Użytkownicy definiowani są w bazie lokalnej (tzn. bazie utrzymywanej na urządzeniu) oraz na zewnętrznych serwerach LDAP, RADIUS, TACACS+ lub SecurID (ACE/Server).	TAK / NIE *)	
31.	System zabezpieczeń współpracuje z wiodącymi urzędami certyfikacji (m.in. Verisign, Entrust, Microsoft) i wspiera standardy PKI (PKCS 7, PKCS 10) oraz protokół SCEP.	TAK / NIE *)	
32.	System zabezpieczeń musi obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT realizują m.in. dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. Udostępnianie w Internecie usług wielu serwerów powinno odbywać się z użyciem tylko jednego publicznego adresu IP.	TAK / NIE *)	
33.	System zabezpieczeń powinien posiadać możliwość pracy w konfiguracji odpornej na awarie. Moduł ochrony przed awariami monitoruje i wykrywa uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Urządzenia zabezpieczeń w klastrze powinny funkcjonować w trybie Active-Active.	TAK / NIE *)	

34.	W przypadku gdy do działania wymienionych wcześniej funkcji konieczne są licencje, system musi zostać w nie wyposażony. Licencje muszą być aktywne przez okres co najmniej 3 lat.	TAK / NIE *)	

*) - niepotrzebne skreślić

2. Kontroler sieci Wi-Fi + licencje – 1 szt.

Nazwa producenta ……..…….

Typ ……..

Model (oznaczenie) ……

Lp.	Wymagania minimalne Zamawiającego	Charakterystyka proponowanego przez Wykonawcę wyrobu	Uwagi
1.	Urządzenie umożliwiające zarządzanie minimum 128 punktami dostępowymi wraz z licencją na min.16 punktów dostępowych.	TAK / NIE *)	
2.	Kontroler musi spełniać następujące wymagania:	TAK / NIE *)	
	1) musi poprawnie obsługiwać punkty dostępowe pracujące w standardzie IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n (min. draft 2.0);	TAK / NIE *)	
	2) musi zarządzać centralnie wszystkimi punktami dostępowymi;	TAK / NIE *)	
	3) musi umożliwiać zbieranie informacji na temat innych punktów nadawczych będących w zasięgu propagowanej sieci;	TAK / NIE *)	
	4) musi zapewniać zarządzanie zgodnie z CAPWAP (RFC 5415)	TAK / NIE *)	
	5) musi zapewniać przydział użytkowników do VLAN-ów (IEEE 802.1Q) na podstawie informacji przesyłanej w atrybutach Access-Accept protokołu RADIUS;	TAK / NIE *)	
	6) musi umożliwiać skonfigurowanie podłączonych punktów dostępowych tak by wszystkie rozgłaszały co najmniej 16 SSID dla każdego z pasma 5GHz i 2,4 GHz indywidualnie, zapewniając możliwość zdefiniowania różnych metod szyfrowania dla każdego z SSID (WEP,WPA,WPA2,802.1x z EAP, wyłączenie szyfrowania) oraz rozdziału ruchu na odrębne VLAN-y (IEEE 802.1Q), z jednoczesnym uwzględnieniem przydziału dynamicznego opisanego w poprzednim punkcie;	TAK / NIE *)	
	7) kontroler musi zapewniać zarządzanie Access Pointami w zakresie przydziału mocy transmisji sygnału radiowego oraz doboru kanałów;	TAK / NIE *)	
	8) kontroler musi wspierać funkcjonalność Dynamic Frequency Selection;	TAK / NIE *)	
	9) kontroler musi umożliwiać dostęp do sieci poprzez współpracę z zewnętrznym serwerem RADIUS (RFC2865) obsługując równolegle (na jednym SSID) szyfrowanie WPA-enterprise/TKIP i WPA2-enterprise/AES;	TAK / NIE *)	
	10) musi posiadać obsługę mechanizmów QoS (802.1p, CAC WMM TSpec, kontrola pasma per użytkownik);	TAK / NIE *)	
	11) Wymagana jest obsługa pracy dwóch kontrolerów w trybie wysokiej dostępności (HA). Awaria kontrolera nie powoduje przerwy w pracy użytkowników	TAK / NIE *)	

	12) Wymagane jest zapewnienie wsparcia dla protokołu VoIP(SIP);	TAK / NIE *)	
	13) Wymagana jest obsługa telefonów bezprzewodowych typu Voice over IP,	TAK / NIE *)	
	14) kontroler bezprzewodowy musi generować informacje o ruchu w sieci zgodnie z RFC 2866 (RADIUS Acconting);	TAK / NIE *)	
	15) musi umożliwiać zarządzanie za pomocą interfejsu WWW (HTTPS), XML, SNMP v3 oraz z linii komend (SSH, port szeregowy);	TAK / NIE *)	
	16) musi być wyposażony w dwa redundantne zasilacze 230V;	TAK / NIE *)	
	17) musi posiadać min. 4 interfejsy GbE SFP oraz 4 porty 10/100/1000 Mbps RJ45, musi zapewniać współprace z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne;	TAK / NIE *)	
	18) musi zapewniać możliwość redundancji rozwiązania (N:1 oraz N:N);	TAK / NIE *)	
	19) Obsługuje usługi DHCP - klient (Adres IP, maska, Default Gateway, DNS Server) - serwer	TAK / NIE *)	
	20) Obsługa opcji Fast Roaming dla klientów bezprzewodowych	TAK / NIE *)	
	21) Możliwość specyfikacji godzin i dni pracy indywidualnych klientów	TAK / NIE *)	
	22) Zapewnia generację kluczy i zarządzanie nimi	TAK / NIE *)	
	23) Możliwość tworzenia wzorów konfiguracji typu template do łatwego powielania konfiguracji	TAK / NIE *)	
	24) Możliwość szyfrowania ruchu pomiędzy Portem Dostępowym i Kontrolerem	TAK / NIE *)	
	25) Zapewnia dokładne informacje o sesji użytkownika i parametrach: radia, śledzenie położenia (lokacja), historię migracji w ramach poszczególnych portów i kontrolerów, błędy, przynależność do grup użytkowników itp.	TAK / NIE *)	
	26) Zapewnia kontrolę i zarządzanie Punktami Dostępowymi, w tym: - Przechowuje informację konfiguracyjne - Przechowuje oprogramowanie systemowe Portu Dostępowego	TAK / NIE *)	
	27) Zapewnia obsługę Spanning Tree i per-VLAN Spanning Tree plus (PVST+)	TAK / NIE *)	
	28) Zapewnienie niezawodności rozwiązania poprzez min.: - Tworzenie logicznych kanałów poprzez agregację fizycznych połączeń portów LAN - Spanning Tree i per-VLAN Spanning Tree Plus (PVST+) - Wsparcie rozwiązania niezawodnościowego typu n:1 kontrolerów - Możliwość tworzenia grup urządzeń: Kontrolerów i AccessPointów zarządzanych jak jeden system z zapewnieniem jednego punktu wprowadzania zmian, balansowania obciążeń Kontrolerów i Access Pointów oraz bezprzerwową niezawodność systemu	TAK / NIE *)	
	29) Współpraca z zewnętrznymi aplikacjami typu EndPointSecurity	TAK / NIE *)	
	30) Współpraca z zewnętrznymi systemami typu RFID TAGs	TAK / NIE *)	
	31) Współpraca z zewnętrznymi systemami typu bezprzewodowy dedykowany IPS	TAK / NIE *)	

*) - niepotrzebne skreślić

3. <u>Access point - 16 szt.</u>

Nazwa producenta ……..…….

Typ ……..

Model (oznaczenie) ……

Lp.	Wymagania minimalne Zamawiającego	Charakterystyka proponowanego przez Wykonawcę wyrobu	Uwagi
1.	Punkt dostępowy wyposażony w dwa radia pracujące w standardach IEEE 802.11a, IEEE 802.11b/g IEEE 802. 11 n	TAK / NIE *)	
2.	Wyposażony w port LAN 1x 10/100/1000BaseT (RJ45)	TAK / NIE *)	
3.	Maksymalna moc nadajnika dla 802.11a : 21dBm	TAK / NIE *)	
4.	Maksymalna moc nadajnika dla 802.11g : 21dBm	TAK / NIE *)	
5.	Bezpieczeństwo: 1) 802.11i 2) Wi-Fi Protected Access 2 (WPA2) 3) WPA 4) 802.1X 5) Advanced Encryption Standards (AES) 6) Temporal Key Integrity Protocol (TKIP)	TAK / NIE *)	
6.	Typy EAP: 1) Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) 2) EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) 3) Protected EAP (PEAP) v0 lub EAP-MSCHAPv2 4) Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) 5) PEAPv1 lub EAP-Generic Token Card (GTC) 6) EAP-Subscriber Identity Module (SIM)	TAK / NIE *)	
7.	Wykrywanie nie autoryzowanych Punktów Dostępowych oraz klientów i metody zapobiegania atakom typu DoS: 1) Wykrywanie i skanowanie pasma i kanałów w czasie obsługi klientów bezprzewodowych 2) Wykrywanie zakłóceń radia 3) Wskazywanie miejsca źródła zakłóceń lub położenia nieautoryzowanego Punktu Dostępowego 4) Określenie czy nie autoryzowany Punkt Dostępowy wprowadza interferencje 5) Zabezpieczenie własnych klientów przed przypadkowym dołączeniem do nie autoryzowanych Punktów Dostępowych 6) Powiadamianie w trybie alarmowym o wykryciu nie autoryzowanego Punktu Dostępowego	TAK / NIE *)	
8.	Wykrywanie ataków typu DoS: 1) RF Jamming 2) Deauthenticate frazes 3) Broadcast deauthenticate frames 4) Disassociation frazes	TAK / NIE *)	

	5) Null probe responsem 6) Decrypt errors 7) Fake AP 8) SSID masquerade 9) Spoofed AP		
9.	Zabezpieczenia fizyczne: 1) Nie przetrzymuje konfiguracji (tzn. konfiguracja przechowywana na kontrolerze) 2) Fizyczna wymiana Punktu Dostępowego nie wymaga zmiany konfiguracji systemu 3) Maskująca obudowa – wykonanie i możliwość montażu nie ujawniająca standardowych anten, kabli podłączeniowych 4) Możliwość montażu pozioma lub pionowa 5) Brak portu konsolowego 6) Możliwość mocowania Portu Dostępowego zabezpieczeniem typu Kensington (jak notebook)	TAK / NIE *)	
10.	Obsługa standardów QoS w tym: 1) Kontrola QoS na bazie identyfikacji użytkownika lub portu dostępowego 2) Wsparcie dla WiFi Multimedia QoS Wsparcie dla WiFi Multimedia QoS 3) Wsparcie dla SpectraLink Voice Priority 4) QoS mapping – IEEE 802.1P – DiffServ	TAK / NIE *)	
11.	Całość ruchu obsługiwanego przez Punkt Dostępowy jest kontrolowana przez Kontroler Punktów Dostępowych: Konfiguracja Access Pointu umożliwia wskazanie wirtualnych sieci które mogą być przełączane lokalnie bez udziału kontrolera	TAK / NIE *)	
12.	Możliwość pracy w trybie: 1) Sieci Kratowej – wsparcie min. 15 punktów dostępowych a każdy musi obsłużyć min. 5 kolejnych Access Pointów i min. dwa punkty pośredniczące 2) Transparent Bridge L2	TAK / NIE *)	
13.	Dostępne szybkości transmisji 802.11a/b/g: 54 Mb/s 48 Mb/s 36 Mb/s 24 Mb/s 18 Mb/s 12 Mb/s 11 Mb/s 9 Mb/s 6 Mb/s 5,5 Mb/s 2 Mb/s 1 Mb/s	TAK / NIE *)	
14.	Częstotliwość pracy: 1) 2.4 – 2.4835 GHz 2) 5.150 – 5.850 GHz 3) Urządzenie posiada możliwość pracy w obu zakresach jednocześnie (dwa radia)	TAK / NIE *)	
15.	Obsługa minimum do 500 równoczesnych klientów	TAK / NIE *)	
16.	Nie dopuszcza się, aby punkt dostępowy posiadał zainstalowane anteny znajdujące się poza obudową urządzenia	TAK / NIE *)	
	Obsługiwane protokoły i standardy: 1) IEEE 802.11b – Wireless LAN 11 Mbps, 2,4 GHz		

	2) IEEE 802.11g – Wireless LAN 54 Mbps, 2,4 GHz 3) IEEE 802.11n – Wireless LAN 300 Mbps, 2,4 GHz 4) IEEE 802.11d 5) WPA2 6) EAP – Extensible Authenticalation Protocol 7) TLS – Transport Layer Security	TAK / NIE *)	

*) - niepotrzebne skreślić

4. Oprogramowanie do tworzenia kopii zapasowych – 1 szt.

Nazwa producenta ……..…….

Typ …….

Model (oznaczenie) ……

Lp.	Wymagania minimalne Zamawiającego	Charakterystyka proponowanego przez Wykonawcę wyrobu	Uwagi
1.	Oprogramowanie do archiwizacji powinno współpracować z infrastrukturą wirtualizacji opartą na VMware ESX oraz ESXi w wersjach 3.5, 4.0, 4.1, 5, 5.1 oraz 5.5, jak również Hyper-V 2008 R2 i Hyper-V 2012 (w tym obsługa formatu dysków wirtualnych *.vhdx)	TAK / NIE *)	
2.	Rozwiązanie powinno współpracować z hostami ESX i ESXi zarządzanymi przez VMware vCenter jak i hostami niezarządzanymi (standalone)	TAK / NIE *)	
3.	Rozwiązanie powinno współpracować z hostami Hyper-V zarządzanymi przez System Center Virtual Machine Manager, zgrupowanymi w klastry jak i niezarządzanymi (standalone)	TAK / NIE *)	
4.	Rozwiązanie nie może instalować żadnych swoich komponentów (agent) w archiwizowanych maszynach wirtualnych.	TAK / NIE *)	
5.	Rozwiązanie musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez VMware i Hyper-V	TAK / NIE *)	
6.	Rozwiązanie powinno mieć możliwość instalacji na następujących systemach operacyjnych: • Microsoft Windows Server 2008 SP2 (x64) • Microsoft Windows Server 2008 R2 • Microsoft Windows 7 SP1 • Windows Server 2012 • Windows 8	TAK / NIE *)	
7.	Rozwiązanie powinno dawać możliwość odzyskiwania całych obrazów maszyn wirtualnych z obrazów, pojedynczych plików z systemu plików znajdujących się wewnątrz wirtualnej maszyny. Rozwiązanie musi umożliwiać odzyskanie plików i/lub całych maszyn wirtualnych na zasadzie „one-click restore". Rozwiązanie musi umożliwiać odzyskiwanie plików z następujących systemów plików: • Linux: ▪ ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS • BSD : ▪ UFS, UFS2 • Solaria:	TAK / NIE *)	

	▪ ZFS • Mac : ▪ HFS, HFS+ • Windows: ▪ NTFS, FAT, FAT32, ReFS		
8.	Rozwiązanie powinno umożliwiać natychmiastowe odzyskanie wirtualnej maszyny i jej uruchomienie bez kopiowania na storage podłączony do hostów ESX (wbudowana funkcjonalność NFS Server) i Hyper-V	TAK / NIE *)	
9.	Rozwiązanie powinno umożliwiać bezpośrednie odzyskiwanie obiektów z takich usług jak Active Directory (użytkownicy i grupy), Microsoft Exchange (emaile i kontakty), Microsoft SharePoint (dokumenty) i Microsoft SQL (tabele i rekordy) z maszyn wirtualnych środowiska VMware i Hyper-V.	TAK / NIE *)	
10.	Rozwiązanie musi zapewniać szybkie odzyskiwanie danych ze skrzynek pocztowych Microsoft Exchange 2010/2013 bez potrzeby uruchamiania maszyny wirtualnej (odzyskiwanie bezpośrednio z bazy danych *.EDB)	TAK / NIE *)	
11.	Rozwiązanie musi zapewniać szybkie odzyskiwanie danych z witryn Microsoft SharePoint 2010 bez potrzeby uruchamiania maszyny wirtualnej (odzyskiwanie bezpośrednio z bazy danych *.MDF)	TAK / NIE *)	
12.	Rozwiązanie powinno umożliwiać indeksowanie plików zawartych w archiwach maszyn wirtualnych z systemem operacyjnym Windows w celu szybkiego ich przeszukiwania	TAK / NIE *)	
13.	Rozwiązanie powinno umożliwiać równoczesne przetwarzanie wielu maszyn wirtualnych	TAK / NIE *)	
14.	Rozwiązanie powinno w pełni korzystać z mechanizmów zawartych w VMware vStorage API for Data Protection a w szczególności być zgodnym z mechanizmem Changed Block Tracking	TAK / NIE *)	
15.	Rozwiązanie powinno umożliwiać wykorzystanie technologii CBT dla platformy VMware również dla maszyn wirtualnych, które posiadają już migawkę.	TAK / NIE *)	
16.	Rozwiązanie powinno mieć wbudowane mechanizmy podobne do technologii CBT również dla platformy Hyper-V w celu przyśpieszenia procesu backupu.	TAK / NIE *)	
17.	Rozwiązanie powinno korzystać z mechanizmów VSS (Windows Volume Shadowcopy) wbudowanych w najnowsze systemy operacyjne z rodziny Windows.	TAK / NIE *)	
18.	Rozwiązanie powinno mieć wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej	TAK / NIE *)	
19.	Rozwiązanie powinno mieć możliwość archiwizacji na napędach taśmowych	TAK / NIE *)	
20.	Rozwiązanie powinno mieć możliwość instalacji centralnej konsoli do zarządzania większą ilością serwerów archiwizujących oraz jednoczesnego zarządzania backupami środowiska VMware i Hyper-V	TAK / NIE *)	
21.	Dostęp do tej konsoli powinien być realizowany przez przeglądarkę WWW	TAK / NIE *)	
22.	Rozwiązanie powinno mieć wbudowany mechanizm informowania o pomyślnym lub niepomyślnym zakończeniu procesu archiwizacji poprzez email, zapis do Event Log'u Windows lub wysłanie komunikatu SNMP.	TAK / NIE *)	
23.	Rozwiązanie powinno mieć możliwość rozbudowy procesu archiwizacji o dowolne skrypty tworzone	TAK / NIE *)	

	przez administratora i dołączane do zadań archiwizacyjnych		
24.	Rozwiązanie powinno mieć wbudowaną możliwość replikacji wirtualnych maszyn pomiędzy hostami ESX i ESXi w tym możliwość replikacji ciągłej	TAK / NIE *)	
25.	Rozwiązanie powinno mieć wbudowaną możliwość replikacji maszyn wirtualnych pomiędzy hostami Hyper-V w tym możliwość replikacji ciągłej	TAK / NIE *)	
26.	Rozwiązanie powinno mieć możliwość tworzenia środowiska wirtualnego laboratorium w środowisku VMware lub Hyper-V	TAK / NIE *)	
27.	Rozwiązanie powinno mieć możliwość tworzenia środowiska wirtualnego laboratorium dla zreplikowanego środowiska VMware	TAK / NIE *)	
28.	Rozwiązanie powinno mieć możliwość występowania i zatwierdzania wniosków o tworzenie środowisk w wirtualnym laboratorium w środowisku VMware lub Hyper-V.	TAK / NIE *)	
29.	Rozwiązanie powinno zapewnić możliwość sprawdzenia poprawności wykonania archiwum poprzez odtworzenie wirtualnej maszyny w izolowanym środowisku i jej uruchomienie w środowisku VMware lub Hyper-V.	TAK / NIE *)	
30.	Rozwiązanie powinno zapewnić możliwość sprawdzenia poprawności wykonania replikacji poprzez odtworzenie wirtualnej maszyny w izolowanym środowisku i jej uruchomienie w środowisku VMware.	TAK / NIE *)	
31.	Rozwiązanie powinno być zgodne z konfiguracją rozproszonego przełącznika VMware (Distributed Virtual Switch)	TAK / NIE *)	
32.	Rozwiązanie powinno mieć możliwość integracji z środowiskiem VMware vCloud Director a w szczególności możliwość archiwizacji metadanych vCD i atrybutów vApps oraz odzyskiwanie tych elementów bezpośrednio do vCD.	TAK / NIE *)	
33.	Rozwiązanie powinno umożliwiać przedstawienie informacji o archiwizacji środowiska VMware bezpośrednio w webowym kliencie vSphere	TAK / NIE *)	
34	Rozwiązanie powinno mieć możliwość automatycznej zmiany numeracji IP maszyn przywracanych w środowiskach centrum zapasowego w przypadku awarii centrum podstawowego	TAK / NIE *)	
35.	Rozwiązanie musi umożliwiać zapisanie konfiguracji całej instalacji w celu przywrócenia jej po reinstalacji całego systemu.	TAK / NIE *)	
36.	Rozwiązanie powinno mieć możliwość dodatkowego skopiowania punktów przywracania do innej lokalizacji	TAK / NIE *)	
37.	Rozwiązanie powinno mieć możliwość wykonywania archiwizacji zgodnie z rotacyjnym schematem GFS (Grandfa	TAK / NIE *)	

* niepotrzebne skreślić

5. <u>VMware vSphere Standard – wsparcie aktywne na poziomie podstawowym do 31 grudnia 2014 r. (licencje na procesor) – 3 szt.</u>

Nazwa producenta ……..…….

Typ ……..

Model (oznaczenie) ……

……
/Miejscowość i data/

……..……
/Podpis osoby/osób upoważnionej do występowania w imieniu wykonawcy/
(pożądany czytelny podpis albo podpis i pieczątka z imieniem i nazwiskiem)

II. Część 2 – dostawa sprzętu komputerowego na potrzeby Sądu Rejonowego w Bielsku Podlaskim, ul. …….:

1. Komputery – 4 szt.

Nazwa producenta ……..…….

Typ ……..

Model (oznaczenie) ……

Lp.	Wymagania minimalne Zamawiającego	Charakterystyka proponowanego przez Wykonawcę wyrobu	Uwagi
	Typ		
1.	Stacja robocza. W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta.	TAK / NIE *)	
	Procesor		
2.	Osiągający w teście **SYSmark 2012 Preview Rating** wynik min. **128** punktów. (dot. tylko wydajności procesora bez względu na testowaną konfiguracje komputera).	TAK / NIE *)	
	Płyta główna		
3.	Płyta główna z wbudowanymi: min. 1 złączem PCI 32bit, min. 2 złączami PCI Express x16, min. 1 złączem PCIe x1; 4 złącza DIMM **z obsługą do 16GB** pamięci RAM, min. 4 złącza SATA w tym 1 szt. SATA 3.0	TAK / NIE *)	
	Parametry pamięci masowej		
4.	Minimum **250 GB.**	TAK / NIE *)	
	Pamięć operacyjna		
5.	Co najmniej **4GB.**	TAK / NIE *)	
	Porty		
6.	Wbudowane porty: 1 x RS232, 1 x VGA, 2 x PS/2, 2 x cyfrowe złącze (w tym min 1 x DisplayPort v1.1a), min. 10 x USB, w tym portów wyprowadzonych na zewnątrz komputera: min. 4 z przodu obudowy (w tym minimum 2 w standardzie 3.0) i 6 z tyłu, port sieciowy RJ-45, porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Możliwość podłączenia dwóch pracujących równolegle dodatkowych zewnętrznych kart graficznych. Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n	TAK / NIE *)	
	Wydajność grafiki		
7.	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 10.1, Shader 4.1 posiadająca min. 6EU (Graphics Execution Units) oraz Dual HD HW Decode.	TAK / NIE *)	
	Wyposażenie multimedialne		

8.	Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera Porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy.	TAK / NIE *)	
Karta sieciowa			
9.	Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem z poziomu konsoli zarządzania - niezależnie od stanu zasilania komputera - łącznie z obsługą stanu S3 (uśpienie) oraz S4-S5 (hibernacja i wyłączenie);	TAK / NIE *)	
Napęd optyczny			
10.	DVD R+/RW+, R-/RW- Nagrywanie płyt dwuwarstwowych DVD wraz z oprogramowaniem do nagrywania oraz odtwarzania płyt DVD	TAK / NIE *)	
	Czytnik kart mikroprocesowych		
11.	Zgodny z ISO 7816-1, 2, 3, 4 lub równoważną (w przypadku nie zintegrowanego czytnika z klawiaturą komputera)	TAK / NIE *)	
Klawiatura			
12.	Na złączu USB, 104 klawisze QWERTY. Czytnik kart mikroprocesorowych zgodny z ISO 7816-1, 2, 3,4 lub równoważną (zintegrowany w klawiaturze komputera).	TAK / NIE *)	
Mysz			
13.	Optyczna z rolka na złączu USB, podkładka	TAK / NIE *)	
Obudowa			
14.	1. Typu MiniTower z obsługą kart PCI Express wyłącznie o pełnym profilu, wyposażona w min. 4 kieszenie: 2 szt 5,25" zewnętrzne i 2 szt 3,5" wewnętrzne, 2. Obudowa powinna fabrycznie umożliwiać montaż min 2 szt. dysku 3,5" lub dysków 2,5" 3. Suma wymiarów obudowy nie może przekraczać 99 cm, waga max 10 kg, 4. Zasilacz w sieci 230V 50/60Hz prądu zmiennego o mocy max 280W i efektywności min. 90% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 87% przy obciążeniu zasilacza na poziomie 100%, 5. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego i 3,5" dysku twardego bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). 6. Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera. 7. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki). 8. Obudowa musi być wyposażona w zamek który nie wystaje poza obrys obudowy.	TAK / NIE *)	

	9. Obudowa musi posiadać wbudowany wizualny lub dźwiękowy system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, a w szczególności musi sygnalizować: - uszkodzenie lub brak pamięci RAM - uszkodzenie złączy PCI i PCIe, płyty głównej - uszkodzenie kontrolera Video - uszkodzenie dysku twardego - awarię BIOS'u - awarię procesora Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wymaganych wolnych slotów		
Zgodność z systemami operacyjnymi i standardami			
15.	Zgodnie z punktem 3 specyfikacji	TAK / NIE *)	
Bezpieczeństwo			
16.	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Obudowa w jednostce centralnej musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym producenta komputera.	TAK / NIE *)	
Zdalne zarządzanie			
17.	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.: ▪ monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; ▪ zdalną konfigurację ustawień BIOS, ▪ zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; ▪ zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej. ▪ sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji	TAK / NIE *)	
BIOS			
18.	1. BIOS zgodny ze specyfikacją UEFI 2. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: ▪ wersji BIOS, ▪ nr seryjnym komputera wraz z datą jego wyprodukowania, ▪ ilości i sposobu obłożenia slotów pamięciami RAM, ▪ typie procesora wraz z informacją o ilości rdzeni,		

	wielkości pamięci cache L2 i L3, ▪ pojemności zainstalowanego dysku twardego ▪ rodzajach napędów optycznych ▪ MAC adresie zintegrowanej karty sieciowej ▪ kontrolerze audio 3. Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) 4. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń 5. Możliwość polegająca na kontrolowaniu urządzeń wykorzystujących magistralę komunikacyjną PCI, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych. Pod pojęciem kontroli Zamawiający rozumie funkcjonalność polegającą na blokowaniu/odblokowaniu slotów PCI. 6. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. 7. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe. 8. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej, portu równoległego, portu szeregowego z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. 9. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. 10. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przodzie obudowy, tylko tylnich portów.	TAK / NIE *)	
Certyfikaty i standardy			
19.	1. Raport z testu wydajności SYSmark 2012 Preview Rating potwierdzający osiągnięcie przez procesor stacji roboczej wyniku na poziomie min. 128 punktów (dopuszcza się wydruk ze strony internetowej http://www.bapco.com/support/fdrs/SYSmark2012web.html) 2. Zaświadczenie niezależnego podmiotu zajmującego się poświadczaniem zgodności działań producenta stacji roboczej z normami jakościowymi, potwierdzające wdrożenie przez producenta oferowanego produktu normy PN-EN ISO 9001:2008 lub równoważnej, w zakresie co najmniej projektowania i produkcji sprzętu komputerowego – certyfikat ISO 9001:2008 lub równoważny dla producenta urządzenia; 3. Dokument poświadczający poprawną współpracę oferowanego modelu stacji roboczej z oferowanym systemem operacyjnym (dopuszcza się wydruk ze strony internetowej producenta oprogramowania); 4. Deklaracja zgodności CE oferowanej stacji roboczej;	TAK / NIE *)	

	5. Certyfikat lub wydruk ze strony internetowej http://www.eu-energystar.org lub http://www.energystar.gov potwierdzający, że oferowany monitor spełnia normę Energy Star co najmniej 5.0 lub równoważną; 6. Zaświadczenie niezależnego podmiotu zajmującego się poświadczaniem zgodności działań producenta monitora z normami jakościowymi potwierdzające wdrożenie przez producenta oferowanego produktu normy PN-EN ISO 9001:2008 lub równoważnej, w zakresie co najmniej projektowania, i produkcji monitorów komputerowych – certyfikat ISO 9001:2000 lub równoważny dla producenta monitora; 7. Dokument poświadczający iż czytnik kart mikroprocesorowych jest zgodny z normą ISO 7816 - 1, 2, 3, 4 lub równoważną np. oświadczenie Wykonawcy lub producenta, (w przypadku niezintegrowanego czytnika z klawiaturą komputera) 8. Przynajmniej jeden z certyfikatów bezpieczeństwa dla układu elektronicznego karty mikroprocesorowej: - ITSEC E3 HIGH lub wyższy poziom lub równoważny - Common Criteria EAL4 lub wyższy poziom lub równoważny, - FIPS 140-2 Level3 lub wyższy poziom lub równoważny.		
Ergonomia			
20.	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 25 dB	TAK / NIE *)	
Warunki gwarancji			
21.	Zgodnie z warunkami określonymi we wzorze umowy stanowiącym Załącznik nr 10 do siwz. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.	TAK / NIE *)	
Wsparcie producenta			
22.	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.	TAK / NIE *)	
Oprogramowanie			
23.	Microsoft Windows 7 Professional (32-bit lub 64-bit) MS Office Standard 2013 MS SQL 2008 CAL (lub równoważny) w przypadku wymiany SQL na nowszą wersję niż zainstalowana w wydziale, Adobe Reader CE - najnowsza wersja obowiązująca na 30 dni kalendarzowych przed uplywem terminu składania ofert (lub równoważny),	TAK / NIE *)	
Wyposażenie dodatkowe			
24.	**Wymagania dla kart mikroprocesorowych (wykorzystywanej do autoryzacji użytkowników w systemie Windows 7 lub Windows 8):** 1. Należy dostarczyć 2 karty na każdą stację roboczą. 2. Karty muszą realizować algorytm RSA 3. Karty musza funkcjonować zgodnie z normą ISO-7816 cześć 1.2,3,4,8 lub równoważną 4. Karty muszą posiadać co najmniej 64 kB pamięci		

	zapisywalnej (EEPROM) 5. Karty w ramach wewnętrznej pamięci EEPROM muszą przechowywać klucze, certyfikaty i inne obiekty 6. Karty muszą realizować podpis RSA przy użyciu klucza prywatnego znajdującego się na karcie, /. wykorzystaniem algorytmu RSA zgodnie ze specyfikacją PKCS//i w wersji 1.5.. 7 Karty muszą posiadać bibliotekę dynamiczną DLL 32 i 64 bitową dla systemów Windows XP/2008R.2/Vista/7/8 z implementacją interfejsu PKCS/1 w wersji min. 2.01, zgodnej ze standardem PKCS/M 1 opublikowanym przez firmę RSA Security. 8. Karty muszą posiadać bibliotekę dynamiczną z implementacją interfejsu PKCS/11 1 umożliwiającą generowanie nowej pary kluczy RSA, zapis klucza prywatnego (opcjonalnie publicznego), realizację podpisu RSA i zapis certyfikatu na kartę.. 9. Karty muszą posiadać generator liczb losowych wykorzystywany przez kartę do generowania kluczy na karcie. Generator ten musi być oparty na zjawisku fizycznym. 10. Karty muszą umożliwić przechowywanie co najmniej sześciu kluczy prywatnych o długości od 1024 do 2048. bitów wraz z ich certyfikatami o typowej wielkości 2 kB 11. Karta musi umożliwiać elastyczne definiowanie profilu definiującego zasady kontroli dostępu do obiektów chronionych na karcie, w tym: a) Możliwość definiowania min. 3 odrębnych kodów PIN oraz związanych z nimi 3 odrębnych kodów PUK, kontroli dostępu do obiektów chronionych na karcie, b) Możliwość definiowania minimalnych i maksymalnych długości każdego kodu PIN oraz PUK oraz liczby błędnych prób ich podawania, po których następuje zablokowanie dostępu do kluczy prywatnych i obiektów danych chronionych kodem, c) Możliwość definiowania liczby operacji dostępu do danych, na którą ważne jest jednorazowe podanie danego kodu PIN (1, kilka operacji, brak limitu), d) Możliwość zabezpieczonej, ponownej inicjalizacji zablokowanej karty bez możliwości dostępu do zablokowanych sekretów (karta z zablokowanymi kodami PUK może być sformatowana i ponownie użyta, ale obiekty zablokowane ulegają skasowaniu), e) Możliwość zabezpieczonej, ponownej inicjalizacji zablokowanej karty bez możliwości dostępu do zablokowanych sekretów (karta z zablokowanymi kodami PUK może być sformatowana i ponownie użyta, ale obiekty zablokowane ulegają skasowaniu), 12. Karty muszą umożliwiać zapisywanie dowolnych obiektów danych 13. Karta musi zarządzać dynamicznie przydziałem i zwalnianiem pamięci (wielokrotne usuwanie i zapisywanie ponownie kluczy kryptograficznych i obiektów danych nie powoduje zmniejszenia dostępnej pamięci karty na te dane).. 14. Karta musi pozwalać na efektywne i elastyczne wykorzystanie pamięci na dane i nie rezerwować na sztywno obszarów pamięci danych bez ich rzeczywistego wykorzystania. 15. Karta musi umożliwiać wielokrotne definiowanie profilu pamięci karty, ilości kodów PIN/PUK, ich parametrów (długości, ilości błędnych prób). 17. Karta i jej oprogramowanie musi współpracować z Microsoft Windows XP/2008 R.2/VISTA/7/8 (w wersji 32bity i 64bity), Windows Terminal Services (RDP), logowaniem Windows Kerberos/PKI uwierzytelnianiem w	TAK / NIE *)	

	przeglądarce Internet Explorer za pośrednictwem interfejsu MS CSP oraz uwierzytelnianiem w przeglądarce Mozilla Firefox za pośrednictwem interfejsu PKCS#!11. 18. Karta musi umożliwiać pracę wieloaplikacyjną przy udostępnianiu przez oba interfejsy (PKCS//11 i MS CSP). Klucze i obiekty danych zapisywane za pośrednictwem jednego interfejsu są dostępne dla drugiego interfejsu. 19. Karta musi zapewniać wsparcie dla możliwości jednoczesnego uwierzytelnienia do wszystkich kluczy chronionych oddzielnymi kodami PIN – utrzymanie uwierzytelnienia do jednego klucza prywatnego podczas uwierzytelniania do innych kluczy. Przesyłanie kodu PIN /PUK do karty musi odbywać się w zabezpieczonym (poufnym i integralnym) kanale typu Secure Messaging między komputerem PC a aplikacją na karcie. 20. Dostarczone oprogramowanie do kart musi umożliwić współpracę z czytnikami posiadającymi klawiaturę typu „PINPAD", działającymi zgodnie ze specyfikacją PC/SC v.2.01, pozwalającą w bezpieczny sposób wprowadzić PIN bez udziału innych komponentów niż czytnik. W przypadku współpracy oprogramowania z czytnikami posiadającymi klawiaturę PINPAD umożliwiającą wprowadzenie bezpiecznego kodu PIN aplikacja nie powinna pozwalać na wprowadzanie kodu PIN w inny sposób niż za pośrednictwem klawiatury czytnika. 21. Kody PIN i PUK dla wszystkich dostarczanych kart muszą być identyczne i powinny przyjmować w momencie dostawy wartości wskazane pisemnie przez Zamawiającego w momencie podpisywania umowy lub musi istnieć możliwość nadawania tych kodów przez Zamawiającego lub Użytkownika. 22. Żadna z dostarczanych kart w momencie dostawy nie może zawierać jakichkolwiek danych w postaci elektronicznej typu klucz lub certyfikat cyfrowy zapisanych w elektronicznej części karty dostępnych dla użytkownika z poziomu dostarczonych AP1. 23. Każda karta musi posiadać unikalny w skali producenta numer seryjny. Dane takie jak numer seryjny karty, nazwa producenta oraz nazwa modelu karty muszą być w sposób trwały naniesione na powierzchnię karty i widoczne dla użytkownika przy czym numer seryjny karty musi być kodowany w systemie dziesiętnym. Numer karty musi być umieszczony w takim miejscu karty aby był widoczny w całości po włożeniu karty do czytnika. Numer seryjny karty nie może być krótszy niż 8 cyfr inie może być dłuższy niż 16 cyfr. Numer ten musi być również możliwy do odczytania z poziomu aplikacji z użyciem dostarczonych bibliotek programowych w polu numer seryjny. W bibliotece PKCSf12 numer ten powinien być prezentowany w polu „SerialNumber" struktury „CK TOKEN INFO". 24. Każda karta musi zostać dostarczona z aplikacją do zarządzania kartą działającą w środowisku systemu operacyjnego Microsoft Windows XP/VISTA/7/8. Aplikacja ta musi posiadać przynajmniej następującą funkcjonalność: a) Umożliwia instalację oprogramowania w systemie operacyjnym z zastosowaniem aplikacji typu „instalator". b) Interfejs użytkownika w języku polskim c) Graficzny interfejs użytkownika umożliwiający interakcję z użyciem klawiatury i urządzenia wskazującego typu myszka komputerowa. d) Prezentacja informacji o nazwie i wersji aplikacji oraz producencie aplikacji.		

	e) Prezentacja informacji o statusie karty (przynajmniej w zakresie czy wyczerpano limity błędnych prób wprowadzania kodów zabezpieczających typu PIN i PUK dla poszczególnych kodów występujących w karcie) f) Zmiana kodu PIN g) Odblokowanie kodu PIN z użyciem kodu PUK w przypadku wyczerpania limitu błędnych prób dla kodu PIN h) Zapoznanie się z zawartością karty w zakresie obiektów typu klucze i certyfikaty i) Prezentacji zawartości osadzonych na karcie certyfikatów j) Prezentacji numeru seryjnego karty k) Importowanie certyfikatu i klucza prywatnego z pliku zgodnego z formatem PKCS#12 l) Rejestrowanie certyfikatu zawartego na karcie w systemie operacyjnym m) Kasowanie wskazanego przez operatora klucza n) Kasowanie wskazanego przez operatora certyfikatu o) Ustawianie certyfikatu domyślnego dla interfejsu CSP. Z dostawą kart muszą zostać dostarczone minimum trzy nośniki CD lub DVD oznaczone nazwą producenta i zawartym na nich oprogramowaniem każda zawierające aplikację do zarządzania kartą. Nośniki muszą zawierać instrukcję obsługi aplikacji do zarządzania kartą w formacie PDF. 25. Karta musi posiadać puste białe pole umożliwiające nadrukowanie na nim informacji o użytkowniku takich jak np. imię, nazwisko, identyfikator służbowy czy zdjęcia. Pole powinno umożliwiać umieszczenie zdjęcia o wielkości 20mm x 30 mm oraz czytelnych danych posiadacza karty. Zakres i rozkład danych określono w Rozporządzeniu Ministra Sprawiedliwości z dnia 28 października 2010 r. w sprawie legitymacji służbowej funkcjonariusza Służby Więziennej (Dziennik Ustaw z 9 listopada 2010 Nr 212 poz. 1394) w części dotyczącej rewersu legitymacji 26. Karta musi pozwalać na jej graficzną personalizację z użyciem drukarki term o sublimacyjnej (kolorowej) do personalizacji kart 27. Na dostarczane oprogramowanie muszą zostać udzielone stosowne niewygasające, bezterminowe licencje. Licencje te nie mogą wprowadzać żadnych ograniczeń w zakresie możliwości posługiwania się dostarczonymi kartami i oprogramowaniem w ramach wszystkich jednostek organizacyjnych na terenie Polski a w tym jednostek podległych 28. Wraz z dostarczonym oprogramowaniem musi zostać zapewnione prawo do pobierania aktualizacji i poprawek dla dostarczonego oprogramowania ze strony internetowej WWW producenta oprogramowania do kart przez okres 3 lat licząc od daty podpisania protokołu odbioru. Wykonawca przekaże Zamawiającemu adres strony oraz inne niezbędne dane w celu zapewnienia wymienionego prawa 29. Wraz z dostarczonymi kartami należy zapewnić telefoniczne wsparcie w języku polskim producenta/dystrybutora kart na okres minimum 1 roku dla trzech administratorów w dni robocze w godzinach od 9:00 do 17:00 w zakresie rozwiązywania zgłaszanych przez Zamawiającego problemów związanych z dostarczonymi kartami i oprogramowaniem. Wymaga się, aby czas rozwiązania zgłoszonego problemu nie przekraczał 7 kolejnych dni roboczych 30. Dostawca udzieli minimum 12 miesięcznej gwarancji nie uwzględniającej uszkodzeń mechanicznych		

	Wymagania dla czytników kart mikroprocesorowych: 1. Należy dostarczyć na każdą stację roboczą 1 czytnik kart mikroprocesorowych jako urządzenie zewnętrzne stacji roboczej, podłączone przez port USB 2.0 (lub wbudowane). 2. Czytnik kart musi być zgodny ze standardem PC/SC. 3. Czytnik kart musi działać z systemami operacyjnymi Microsoft Windows XP/Vista/7/8 4. Czytnik musi umożliwiać odczyt dostępnych na rynku kart kryptograficznych zgodnych z normą ISO-7816 lub równoważną , a w szczególności umożliwiać współpracę z kartą w standardzie PKCS/tł 1 co najmniej w wersji 2.01, 5. Czytnik musi zapewnić niezaprzeczalną, jednoznaczną swoją identyfikację poprzez unikalny w skali producenta wewnętrzny numer seryjny, zapisany trwale, w sposób uniemożliwiający jego modyfikację przez użytkownika czy zatarcie. Sposób identyfikacji czytnika polega na programowym odczycie nazwy producenta czytnika i numeru seryjnego czytnika poprzez (wymaganą w' ramach dostawy) bibliotekę niezbędną do odczytania w/w informacji. 6. Czytnik musi posiadać zabezpieczenie przed wgraniem nieautoryzowanego (innego niż producenta) oprogramowania wewnętrznego oraz nie pozwalać na bezpośredni dostęp i modyfikację zawartości pamięci wewnętrznej. Próba wgrania niewłaściwego oprogramowania nie może powodować zablokowania działania czytnika. 7. Czytnik musi posiadać sygnalizację optyczną (np. diodową) akceptacji karty, pracy z kartą. 8. Czytnik musi współpracować z oferowanymi w ramach niniejszego zamówienia kartami mikroprocesorowymi. Dostarczony sprzęt musi być zgodny z regulacjami RoHS		
	Monitor		
25.	Monitor nie musi pochodzić od producenta stacji roboczej. Matryca min. 19" TFT, format 5:4 , wejście D-SUB, DisplayPort, kąty patrzenia (pion/poziom) min 170/170 stopni, min. rozdzielczość 1280x1024 przy 60Hz, jasność min. 250 cd/m², kontrast statyczny min. 1000: 1, czas reakcji max. 8ms, regulacja wysokości, regulacja pochylenia (tilt), wbudowany HUB USB min 2xUSB 2.0, wbudowany zasilacz, typowy pobór mocy 17W, a w trybie stand-by mniej niż 0,5W, wbudowane lub mocowane dedykowane przez producenta głośniki. Zgodność z normami: Zgodnie z punktem 3 specyfikacji. Kable (DisplayPort, zasilający) umożliwiające podłączenie monitora do oferowanego komputera.	TAK / NIE *)	

*) - niepotrzebne skreślić

……
/Miejscowość i data/

……
/Podpis osoby/osób upoważnionej do występowania w imieniu wykonawcy/
(pożądany czytelny podpis albo podpis i pieczątka z imieniem i nazwiskiem)