Załącznik nr 2A do SIWZ nr DZP.381.111.2018.DW

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

L.P.	**NAZWA SPRZĘTU** Minimalne parametry wymagane przez Zamawiającego	**Liczba sztuk**	**OPIS TECHNICZNY OFEROWANEGO SPRZĘTU** Należy wskazać wszystkie elementy składowe oferowanego sprzętu w odniesieniu do kolumny z lewej strony	**INDEX**
	CZĘŚĆ A			
1.	**ROUTER** Specyfikacja: 1.Przeznaczenie: XDSL (sieci lokalne; telewizja kablowa) 2.Interfejsy WAN: 10/100/1000 Mb/s Cable/xDSL (RJ45) 3.Ilość portów WAN: min. 1 szt. ; 4.Interfejsy LAN: RJ45 5.Ilość portów LAN 10/100/1000: min. 4 szt. 6.Złącza: min. 1 x USB 2.0 7.Standard: IEEE 802.11 a/b/g/n/ac ; 8.Częstotliwość WiFi: 2.4 GHz 5 GHz 9.Szybkość dla 2.4 GHz: 300 Mbps ; szybkość dla 5 GHz: 867 Mbps 10.Rodzaj anteny: zewnętrzna, odkręcana 11.Szyfrowanie: 64/128-bit WEP, WPA , WPA-PSK , WPA2 , WPA2-PSK 12.Zarządzanie: WWW ; 13.Zasilanie: zasilacz AC 14.Akcesoria: Zasilacz, Kabel Ethernet	1		108056

2	**ROUTER** Specyfikacja: 1.Typ złącza: Ethernet 2.WiFi: Tak 3.Protokół Wi-Fi: 802,11n (300 Mbps) 4.Łącze: Kablowe 5.Antena WIFI: 2x 5 dBi 6.Częstotliwość pracy WIFI: 2,4 GHz 7.Pamięć min.: 8 MB Flash, 32 MB RAM 8.Szyfrowanie-1: 64,128-bit WEP, WPA2-PSK, WPA-PSK 9.Szyfrowanie-2: WPA-Enterprise , WPA2-Enterprise 10.Obsługa WPS: Tak 11.Typy połączenia WAN: PPTP, L2TP, PPPoE, Statyczny IP, Automatyczny IP 12.Porty min.: WAN-RJ45 10/100 BaseT, LAN-RJ45 10/100 BaseT 13.Waga max.: 180 g 14.Tryby pracy: Router WIFI, Range extender, Access point	1		108329

3	**SWITCH** Specyfikacja: 1.Typ urządzenia : przełącznik Easy Smart 2.Porty min.: 8x RJ-45 10/100/1000Mb/s (Autonegocjacja / Auto-MDI/MDIX) 3.Zasilanie : zasilacz zewnętrzny (na wyjściu: 9V/0,6A) 4.Standardy i protokoły : IEEE 802.3, 802.3u, 802.3ab, 802.3x, 802.1q, 802.1p 5.Pobór prądu : maksymalnie: 5,46W (220V/50Hz) 6.Bufor : 2 Mb 7.Zestaw zawiera : kabel zasilający | gumowe nóżki | płyta CD | instrukcja obsługi 8.Dodatkowe informacje : bezwentylatorowy, biurkowy	2		108667
4	**SWITCH** Specyfikacja: 1.Rodzaj obudowy: Rack 2.Opis produktu: 24 x 10/100 Smart PoE, 4 x Gigabit 3.Porty 10/100Mb/s: min.24 4. Porty Gigabit: min. 4 5. Porty SFP: min.2 6. Porty PoE: min.24 7. Budżet PoE (Wat): 192 8. Tablica MAC: 4K 9. Wielkość bufora: 1MB 10.Ilość VLAN min. : 128 11.Ilość tabeli adresów MAC: min. 8000 12.Ilość wpisów ACL: min. 480 13. Ilość tras statycznych : min. 32	2		110238

	14.Ilość grup typu multicast: min. 1024 15.Zarządzanie protokołem IPv6, usługą Qo5 i ACL: TAK 16.Konfiguracja przez WWW: Tak 17.SNMP v1/v2 oraz v3 : Tak 18.Standard MIBs (RFC1213, RFC1643 oraz RFC1493) : Tak 19.Aktualizacja oprogramowania przez TFTP: Tak 20.Ochrona DoS: Tak 21.Zasilacz: Wewnętrzny 100-240VAC 50-60Hz 22.Pobór prądu (Wat) max.: 256 23.Wentylatory min.: 1 24.Emisja hałasu max. (dBA): 39 25.Temperatura pracy: 0° do 50° C 26.MTBF min.: 237497 godzin 27.Waga (kg) max. : 3.57			
5	**KARTA SIECIOWA** Specyfikacja: 1.Standard: IEEE 802.11 b/g/n 2.Interfejs: USB 2.0 3.Rodzaj komunikacji: bezprzewodowa 4.Typ: zewnętrzna 5.Szybkość transmisji danych: max 150 Mbps 6.Częstotliwość: 2.4 GHz 7.Modulacja: 16-QAM, 64-QAM, BPSK, CCK, DBPSK, OFDM, QPSK 8.Szyfrowanie: 64/128-bit WEP WPA-PSK/WPA2-PSK 9.Zasięg na zewnątrz budynku: max. 150 m 10.Obsługiwane systemy operacyjne: Windows 2000, 7, 8, Vista, XP, XP x64 11.Waga max: 2g. 12.Temperatura pracy [st. C]: 0 - 40	5		110189/1

6	**ROUTER** Specyfikacja: 1.Tryb pracy : Access point, bridge, repeater, router 2.Funkcje urządzenia: router xDSL 3.Interfejsy WAN: 10/100Mbit Cable/xDSL (RJ45) 4.Ilość portów WAN: min. 1 szt. 5.Pamięć Flash: min.4MB 6.Pamięć RAM: min.32 MB 7.Ilość portów LAN 10/100/1000: min. 4 szt. 8.Wbudowany punkt dostępowy Wi-Fi: Tak 9.Standard : IEEE 802.11 a/b/g/n 10.Częstotliwość: 2.4 GHz 11.Szybkość dla 2.4 GHz: min. 300 Mbps 12.Obsługa VPN: Tak 13.Waga max. 140g	1		110189/2
7	**KARTA SIECIOWA** Specyfikacja: 1.Karta sieciowa WiFi: 2.Interfejs: M.2 2230, 1216 3.Pasma: 2.4 GHz, 5 GHz 4.Wbudowany Bluetooth: tak (Bluetooth 4.2) 5.Rodzaj anteny: Wewnętrzna 6.Zastosowane technologie: 64/128-bit; WEP; WPA; WPA 2 7.Obsługiwane prędkości: 1167 Mbps 8.Standardy sieciowe: IEEE 802.11a; IEEE 802.11ac; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n 9.Obsługiwane systemy operacyjne: Linux; Windows 7; Windows 8; Windows 8.1	1		109713

8	**SWITCH 24 porty** Specyfikacja: 1.Rodzaj urządzenia: Switch 2.Szybkość łącza min.: 1 Gbps 3.Liczba portów min.: 24 4.Typ złącza: Ethernet 5.Standardy i protokoły: IEEE 802,3i, IEEE 802,3u, IEEE 802,3ab , IEEE 802, 6.Porty min.: 24 portów RJ45 10/100/1000Mb/s 7.Automatyczna negocjacja szybkości połącz: Tak 8.Automatyczne krosowanie: Auto-MDI/MDIX 9.Wydajność przełączania min.: 48Gb/s 10.Tablica adresów MAC: 8K 11.Szybkość przekierowań pakietów: 35,7Mpps 12.Ramka Jumbo: 10KB 13.Architektura przełączania: Store-and-Forward 14.Certyfikaty: FCC, CE, RoHS	2		109198

.....
data i podpis osoby uprawnionej
do reprezentowania Wykonawcy

	CZĘŚĆ B			
1	**FIREWALL UTM** **Wymagania Ogólne** Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. **Redundancja, monitoring i wykrywanie awarii** 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	2		108686

	3. Monitoring stanu realizowanych połączeń VPN. **Interfejsy, Dysk, Zasilanie:** 1. System realizujący funkcję Firewall musi dysponować minimum: • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System musi być wyposażony w zasilanie AC. **Parametry wydajnościowe:** 1. W zakresie Firewall'a obsługa nie mniej niż 1.3 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 3 Gbps dla pakietów 64 B. 4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 650 Mbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 2 Gbps. 6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 400 Mbps. 7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 200 Mbps. 8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 175 Mbps. **Funkcje Systemu Bezpieczeństwa:** W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci			

	osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. **Polityki, Firewall** 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. **Połączenia VPN** 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2.			

	• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. **Routing i obsługa łączy WAN** 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. · Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. **Zarządzanie pasmem** 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma,			

	oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. **Kontrola Antywirusowa** 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). **Ochrona przed atakami** 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. **Kontrola aplikacji** 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.			

	2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. **Kontrola WWW** 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. **Uwierzytelnianie użytkowników w ramach sesji** 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.			

	• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. **Zarządzanie** 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. **Logowanie** 1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny			

	system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. **Certyfikaty** Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall. • ICSA lub NSS Labs dla funkcji IPS. • ICSA dla funkcji IPSec VPN. • ICSA dla funkcji SSL VPN.			

.....
data i podpis osoby uprawnionej
do reprezentowania Wykonawcy

	CZĘŚĆ C			
	ACCESS POINT - SYSTEM WI - FI Parametry techniczne:	3		109689/1

Porty	Ethernet (Auto MDX, auto-sensing 10/100/1000 Mbps)
Przyciski	Reset
Anteny	2 zintegrowane (wsparcie 2x2 MIMO)
Standardy Wi-Fi	802.11 a/b/g/n/ac
Zasilanie	Passive Power over Ethernet (24V)
Maksymalny pobór prądu	6.5W
Max TX Power 2.4 GHz 5 GHz	 24 dBm 22 dBm
BSSID	do 4
Szyfrowanie	WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i
Certyfikaty	CE, FCC, IC
Mocowanie	Naścienne / sufitowe (mocowanie w komplecie)
Temperatura pracy	-10°C to 70°C (14°F to +158° F)
Wilgotność	5% - 95%
Zaawansowane zarządzanie ruchem	
VLAN	802.1Q
QoS	WLAN prioritization
WMM	Voice, video, best effort, and

	background
Jednocześnie podłączeni klienci	200+
Wspierane prędkości transmisji (Mbps)	
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11n	MCS0 - MCS23 (6.5 Mbps do 450 Mbps), HT 20/40
802.11ac	MCS0 - MCS9 (6.5 Mbps do 867 Mbps), VHT 20/40/80
802.11b	1, 2, 5.5, 11
802.11g	6, 9, 12, 18, 24, 36, 48, 54

<table>
<tr>
<td>3</td>
<td>KONTROLER PROGRAMOWY DO SYSTEMU WI-FI A WBUDOWANĄ TECHNOLOGIĄ CHMURY

Parametry techniczne:

<table>
<tr><td>Masa max.</td><td>110 g</td></tr>
<tr><td>Procesor</td><td>Min. 4 rdzeniowy</td></tr>
<tr><td>RAM</td><td>2 GB DDR</td></tr>
<tr><td>Interfejs sieciowy</td><td>(1) 10/100/1000 Ethernet Port</td></tr>
<tr><td>Przyciski</td><td>(1) Reset do ustawień fabrycznych</td></tr>
<tr><td colspan="2">Metoda zasilania:</td></tr>
<tr><td>PoE</td><td>48V 802.3af lub
Pasywne PoE</td></tr>
<tr><td>Micro-USB</td><td>5V</td></tr>
<tr><td>Źródło zasilania</td><td>802.3af PoE lub
Micro-USB 5V, Minimum 1A</td></tr>
<tr><td>Maksymalny pobór mocy</td><td>5W</td></tr>
<tr><td>Certyfikacja</td><td>CE, FCC, IC</td></tr>
<tr><td>Temperatura pracy</td><td>0 do 40° C</td></tr>
<tr><td>Wilgotność pracy</td><td>20 do 90%</td></tr>
</table>
</td>
<td>1</td>
<td></td>
<td>109689/2</td>
</tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

.....

data i podpis osoby uprawnionej
do reprezentowania Wykonawcy