Załącznik nr 1A do SWZ

**Specyfikacja techniczna i wymagania**

## Założenia ogólne

Celem realizacji zamówienia jest rozbudowa systemu kontroli dostępu dla wybranych pomieszczeń w budynku Wydziału Filologicznego Uniwersytetu Łódzkiego.

Zestawienie i specyfikacja klamek oraz hubów komunikacyjnych objętych zamówieniem znajduje się w załączniku nr 1B „Zapotrzebowanie”, gdzie zawarto informacje dotyczące między innymi:

1. Modelu, wersji i ilości klamek
2. Ilości hubów komunikacyjnychAperio oraz Genetec SCL Cloud Link

## Wymagania dotyczące oferenta

Zakres oferty obejmuje dostawę okuć bezprzewodowych Assa Abloy Aperio wraz z osprzętem i licencjami umożliwiającymi podłączenie okuć do istniejącego systemu kontroli dostępu Genetec Security Center.

Dobór typu licencji pozostaje po stronie oferenta.

W związku z powyższym oferent powinien posiadać certyfikat producenta platformy zarządzającej Genetec Security Center dokumentujący ukończenie szkolenia i pozytywne zdanie egzaminu.

Firma/osoba reprezentująca firmę jako załączniki do oferty musi przedstawić następujące certyfikaty:

* Security Center – Synergis Technical Certification
* Security Center – Enterprise Technical Certification

Oferent dodatkowo powinien udokumentować referencję potwierdzającą na przestrzeni ostatnich 2 lat dostawę minimum 100 szt. okuć Aperio wraz z minimum 100 szt. licencji pozwalającymi na włączenie okuć Aperio do oprogramowania Genetec Security Center.

## Specyfikacja funkcjonalności

### 3.1 Okucia bezprzewodowe

Dla wyznaczonych przejść przewiduje się instalację elektronicznych okuć zintegrowanych z funkcjonalnością kontroli dostępu. W okuciach muszą pozostać istniejące wkładki ze względu na stosowany system jednego klucza typu master do otwierania wszystkich zamków.

Wymagane cechy techniczne i funkcjonalne okuć:

* Zintegrowany multi-technologiczny czytnik zbliżeniowy z możliwością odczytu:

1. numerów seryjnych procesorów kart Mifare Classic/Mifare Plus/Mifare DESFire CSN (ISO 14443A) lub danych z sektorów pamięci;
2. numerów seryjnych kart iCLASS/iCLASS SE CSN (ISO 15693)/iCLASS Seos lub danych z sektorów pamięci;
3. szyfrowanych danych w standardzie SIO (Secure Identity Object);
4. wbudowany moduł Bluetooth do stosowania mobile access

* Dostępny tryb pracy typu office (dwukrotne przyłożenie transpondera otwiera drzwi na stałe i ponowne dwukrotne przyłożenie zamyka na stałe).
* Dane dotyczące użytkowników oraz ich kart dostępowych/kodów PIN muszą być przechowywane zarówno w aplikacji odpowiedzialnej za kontrolę dostępu, jak i w sterownikach drzwiowych (dostępy poszczególnych drzwi/grup, godziny, harmonogramy czasowe, kalendarz).
* Komunikacja z systemem kontroli dostępu powinna być realizowana z wykorzystaniem protokołu TCP/IP, a autoryzacja przeprowadzana przez system KD.
* Luźna klamka zewnętrzna - klamka wewnętrzna zasprzęglona na stałe (swobodne wyjście)
* Możliwość przechowywania w pamięci minimum 10 awaryjnych kart (używanych wyłącznie w przypadku utraty komunikacji z anteną radiową/kontrolerem drzwiowym)
* Diody LED do wizualizacji stanu pracy.
* Odległość odczytu do 40mm.
* Zgodność z IP 52 (drzwi wewnętrzne) oraz IP54 (drzwi zewnętrzne)
* Wymiary nie przekraczające 315 x 45 x 10/20 mm (H x W x D)
* Standard radiowy IEEE 802.15.4 (2.4 GHz)
* Zakres temperatur pracy od 0°C do 60°C
* Dopuszczalna grubość drzwi od 40 do 100 mm
* Zasilanie bateryjne – żywotność nie mniej jak 30 000 cykli
* Monitorowanie stanu drzwi, użycia klamki lub otworzenia drzwi z użyciem klucza **(opcja)**

W przypadku zastosowania dedykowanych do komunikacji modułów wymagane są następujące cechy techniczne i funkcjonalne:

* Połączenie z systemem kontroli dostępu za pomocą magistrali TCP/IP (adresowalnej).
* Możliwość podłączenia minimum 16 urządzeń radiowych (okuć lub zamków bezprzewodowych) za pomocą jednej anteny.
* Zintegrowany bufor pamięci dla rejestracji zdarzeń i uprawnień identyfikatorów.
* Możliwość pracy w trybie on-line i offline.
* Zintegrowana antena z możliwością montażu anteny zewnętrznej .
* Zaszyfrowana komunikacja radiowa (AES 128 bit).
* Diody LED do wizualizacji stanu pracy.
* Aprobaty CE, ETL, FCC, IC, C-Tick.
* Zasilanie PoE.
* Standard radiowy IEEE 802.15.4 (2.4 GHz) - 16 kanałów (11-26).
* Możliwość osiągnięcia zasięgu powyżej 30m.
* Czułość odbiornika nie mniej niż 100dBm.
* Bezprzewodowa moc transmisji nie mniej niż 10 dBm/MHz.

### 3.2 Kontroler

Wymagana całkowita zgodność z Genetec Synergis Cloud Link.

* Możliwość obsługi min. 64 przejść przez jeden kontroler, z wykorzystaniem modułów rozszerzających.
* Obsługa protokołów OSDP, bezpiecznego OSDP, Wiegand.
* Obsługa czytników biometrycznych, pasków magnetycznych, czytników F/2F i jego nadzorowanych technologii.
* Obsługa czytnika z klawiaturą.
* Wbudowany układ pamięci kryptograficznej i szyfrowanie danych.
* Komunikacja hosta chroniona przez TLS 1.2/1.1
* Złącze rozszerzające kontroler/IO chronione przez AES (seria 3 SIO)
* Kontrola dostępu do sieci za pomocą 802.1X
* Wsparcie dla OpenSSL
* Możliwość zachowania danych przez okres min. 3 miesiący po utracie zasilania
* Możliwość podłączenia min 4 czytników z użyciem protokołu OSDP.
* Min. 6 wejść monitorujących oraz min 4 wyjścia przekaźnikowe.
* Moduł wspiera łączenie aktywności innych urządzeń w obrębie systemu w celu generowania działań zaprogramowanych przez system.
* Globalna funkcja „antipasspback” w trybie online oraz w trybie offline.

### 3.3 Kontroler główny SCL

Wymagana całkowita zgodność z Genetec Synergis

* Obsługa PoE,
* Dwa porty Gigabit Ethernet,
* Możliwość pracy i podejmowania decyzji w trybie offline,
* Wbudowane zarządzanie poziomem zagrożeń,
* Trzy rodzaje funkcji passback (hard, soft, global),
* Komunikacja peer-to-peer,
* Obsługa odwiedzających,
* 600.000 użytkowników oraz 150 000 zdarzeń offline,
* Cztery wbudowane porty RS-485
* Szyfrowana komunikacja z oprogramowaniem nadrzędnym,
* Obsługa OSDP v2 Secure Channel