MicroMade

bibinet

SIECIOWY SYSTEM KONTROLI DOSTĘPU I REJESTRACJI CZASU PRACY

Instrukcja Instalacji 1.10.12.01

MicroMade
Gałka i Drożdż sp. j.

64-920 PIŁA, ul. Wieniawskiego 16

Tel./fax: 67 213.24.14

E-mail: mm@micromade.pl

Internet: www.micromade.pl

Spis treści

1. Informacje ogólne

System bibinet przeznaczony jest do obsługi systemu kontroli dostępu i rejestracji czasu pracy. Sprawdza się zarówno w małej jak i dużej firmie - maksymalnie obsługuje 15 000 pracowników. Minimalny system to pojedynczy kontroler pełniący funkcję kontroli dostępu bądź rejestracji czasu pracy podłączony do pojedynczego komputera. Natomiast, dzięki możliwości dołączania urządzeń do wielu komputerów i wykorzystaniu w komunikacji internetu, maksymalne możliwości systemu bibinet są praktycznie nieograniczone.

Wersja 1.10 systemu bibinet potrafi obsługiwać urządzenia włączane w sieć Ethernet co znacznie upraszcza instalację systemu szczególnie w odległych lokalizacjach. Komunikacja z tymi urządzeniami jest szyfrowana z siłą 3DES i może odbywać się zarówno przez sieć lokalną LAN jak i publiczną Internet.

Jako opcja dostępna jest funkcja podglądu raportów pracowniczych przez przeglądarkę internetową.

1.1 Wymagania sprzętowe

Do pracy w sieci bibinet zalecany jest następujący komputer o parametrach nie gorszych niż:

- minimum 4 GB pamięci RAM
- HDD - 100 MB wolnego miejsca
- Port USB 1.1
- Karta sieciowa Ethernet
- Zainstalowany protokół TCP/IP
- Udostępnione do komunikacji porty : 0xb1b0, 0xb1b1 i 0xb1b2 (dziesiętnie: 45488, 45489 i 45490)
- Stały numer IP lub numer otrzymywany z serwera DNS
- System Windows XP Prof. (nie zalecany), Windows Vista Business (nie zalecany), Windows 7/8/10, Windows Server 2003 (nie zalecany)/2008/2012/2016/2019,
- Systemy linii Windows Home można wykorzystać do pracy jako:
  - Instalacja jednostanowiskowa
  - Terminal
  - Węzeł sieci, do którego nie dołącza się terminali.

Uwaga!
Program NIE pracuje pod systemem Windows 98, Windows 2000, Windows 2000 Server i starszymi wersjami Windows oraz systemami linii Windows Home.

Węzeł systemu bibinet i podłączone do niego terminale muszą pracować:

- w jednej domenie albo
- w grupie roboczej.

Nie można mieszać tych dwóch sposobów identyfikacji w ramach jednego węzła systemu bibinet.

Dodatkowo terminale i serwer powinny być w tym samym segmencie sieci. W przypadku różnych segmentów potrzebna jest konfiguracja routera uwzględniająca obsługę RPC, co jest dosyć skomplikowane (dlatego niezalecane).

1.2 Struktura sieci komputerowej

Program bibi wersja 1.10 powinien pracować w środowisku Windows® 7/8/10, Windows® Server 2008/2012/2016/2019 i jest przystosowany do pracy w sieci Ethernet opartej na protokole TCP/IP.

Struktura systemu oparta jest o węzły sieci. W każdym węźle sieci zainstalowano oprogramowanie bibinet serwer. Węzłem musi być komputer do którego podłączamy urządzenia systemu bibinet.

Do komputera będącego węzłem sieci bibinet można podłączać dodatkowe komputery – terminale (zgodnie z posiadaną licencją).

1.2.1 Serwery systemu bibinet

Serwer bibinet to komputer na którym wykonano instalację węzła sieci bibinet. Do tego komputera podłączone są standardowo urządzenia systemu bibinet (interfejsy, kontrolery, rejestratory czasu pracy). Na nim przechowywana jest baza z danymi systemu.

Dane przechowywane przez serwer zapisywane są w jednym pliku o zapisie strukturalnym. Każdy obiekt w pliku zabezpieczany jest sumą kontrolną CRC32. Dodatkowo, cały plik zabezpieczony jest cyfrowym podpisem MD5. Przy uruchomieniu programu sprawdzana jest spójność danych. Nie jest możliwe uruchomienie programu, jeżeli ktoś ingerował w ten plik.

Codziennie wykonywany jest automatyczny backup bazy danych w formacie *.cab w katalogu ..\MicroMade\bibinet\Server\Data\Archiwum. Backup dodatkowo może być robiony na wskazanym serwerze FTP albo dysku sieciowym. Dzięki architekturze rozproszonej, na wszystkich komputerach stanowiących węzły sieci bibi.net, znajduje się ta sama baza danych. Stanowi to dodatkową kopię bezpieczeństwa.

W systemie bibinet można utworzyć wiele węzłów współpracujących ze sobą (maksymalnie 256).

Węzły sieci potrafią porozumiewać się ze sobą zarówno wewnątrz sieci lokalnej jak i poprzez routery i sieć Internet. Taka rozproszona architektura pozwala na budowanie praktycznie nieograniczonego systemu kontroli dostępu.

Do każdego węzła można podłączyć nieograniczoną ilość terminali.

1.2.2 Terminale w sieci bibi.net

Terminalem sieci bibi.net jest komputer, na którym uruchamiane są programy - klienci. Terminalem może być zarówno komputer będący węzłem sieci bibi.net, jak i dowolny inny komputer z sieci lokalnej.

Dzięki zastosowaniu technologii COM/DCOM, do serwera może być dołączona nieograniczona liczba klientów. Aplikacja klient uruchamiana na terminalu łączy się przez sieć lokalną z serwerem i uzyskuje dostęp do bazy danych obejmującej całą sieć bibi. Wytworzenie potrzebnych raportów jest zawsze bardzo szybkie, gdyż wszystko odbywa się lokalnie.

Do komputera, który jest terminalem nie można dołączać urządzeń sieci bibinet za wyjątkiem czytnika administratora systemu, który służy do wprowadzania kart (identyfikatorów) do systemu.

2. Urządzenia systemu bibinet

W systemie bibinet możemy wyróżnić kilka podstawowych grup urządzeń:

- kontrolery bibi spełniające podstawowe zadania kontroli dostępu i rejestracji czasu pracy
- czytniki
- terminale (czytniki z wyjściem sterującym)
- rejestratory czasu pracy
- moduły rozszerzeń (moduły dodatkowych wejść/wyjść, wyświetlacze)
- terminale do obsługi czytników innych producentów (z interfejsem Wiegand'a)
- autonomiczne urządzenia kontroli dostępu

2.1 Kontrolery

Obecnie w systemie bibinet funkcjonują następujące kontrolery:

- kontroler dwóch przejść **bibi-K22**, (dostępny także w zestawie z zasilaczem buforowym i modułem bezpiecznikowym MM-F01 w obudowie metalowej MM-OM1 jako **bibi-K22.KIT**)
- kontroler ośmiu przejść **bibi-K25**
- kontroler windy **bibi-K28** (współpracuje z modułem rozszerzeń bibi-D53)

Kontrolery mogą pełnić zarówno funkcje Kontroli Dostępu jak i Rejestracji Czasu Pracy. Posiadają wbudowany interfejs sieciowy TCP/IP do komunikacji z komputerem zarządzającym systemem. Komunikacja może odbywać się zarówno przez sieć lokalna jak i publiczną (Internet). Cała transmisja jest szyfrowana.

Wstępna konfiguracja kontrolerów ustawiana jest przy pomocy specjalnego programu **biSprzetLAN.exe.** Określa się w tym programie powiązania między urządzeniami (czytnikami, terminalami, modułami rozszerzeń) podłączonymi do magistrali **bibiBUS** (RS485) kontrolera. Dalsza konfiguracja może być wykonywana przez stronę www kontrolera oraz przez program bibi (w zakładce Opcje systemu bibinet). Po skonfigurowaniu kontrolery mogą pracować samodzielnie – niezależnie od komputera. Posiadają zegar czasu rzeczywistego oraz nieulotną pamięć typu Flash pozwalającą na zapamiętanie 15 tys kart i zarejestrowanie 50 tys zdarzeń. Przy pracy on-line wszystkie zarejestrowane zdarzenia są na bieżąco pobierane do komputera.

Kontrolery posiadają własną magistralę bibiBUS pracującą w standardzie RS 485. Magistrala ta pozwala na przesłanie w czasie rzeczywistym informacji z czytników do kontrolera, oraz przesyłanie do oddalonych modułów rozkazów sterowania przejściami.

Do magistrali bibi-BUS można dołączać:

- czytniki kart zbliżeniowych **bibi-R40** i **bibi-R50** - odporne na warunki atmosferyczne
- eleganckie czytniki kart zbliżeniowych **bibi-R41** i **bibi-R51** z frontem szklanym (możliwe dowolne nadruki)
- czytniki kart z ekranem dotykowym LCD **bibi-R42** i **bibi-R52** dedykowane do ewidencji czasu pracy
- eleganckie czytniki kart zbliżeniowych **bibi-R43** i **bibi-R53** z frontem szklanym i z klawiaturą PIN-kodów
- terminale **bibi-T40** i **bibi-T50** - czytniki z wejściami kontrolnymi oraz z wyjściem do sterowania ryglem
- terminale **bibi-T41** i **bibi-T51** - czytniki szklane z wejściami kontrolnymi oraz z wyjściem do sterowania ryglem
- wyświetlacze czasu systemowego **bibi-D50**.
- moduły dodatkowych wejść/wyjść **bibi-D51, bibi-D52, bibi-D53**
- czytniki bezprzewodowe **bibi-R44** i **bibi-R54** (przez moduł **bibi-D54**)
- terminale **bibi-T30** przeznaczone do obsługi czytników innych producentów (z interfejsem Wiegand'a)

Dołączone do magistrali **bibiBUS** urządzenia można ze sobą dowolnie wiązać, tworząc struktury logiczne np. każdy czytnik może być powiązany z dowolnym wyjściem obsługi rygla, zarówno w kontrolerze jak i w terminalu czy którymś module rozszerzającym. Dzięki takiej elastyczności można np. skonfigurować wyjście, które jest sterowane przez cztery czytniki.

2.2 Czytniki i Terminale

Standardowo, w systemie bibi, wykorzystywane są czytniki i terminale RFID pracujące w dwóch standardach.

- Unique - częstotliwość pracy 125 kHz, modulacja amplitudy, tryb Manchester
- Mifare oraz I-Code - częstotliwość pracy 13,56 MHz, odczyt identyfikatora karty (UID)

2.2.1 Czytniki Unique

Czytniki i terminale podłączane są do magistrali bibiBUS (RS485) kontrolerów.

- **bibi-R40** - mały czytnik odporny na warunki atmosferyczne
- **bibi-R41** – elegancki czytnik z frontem szklanym (z dowolnym nadrukiem) przeznaczony do pracy wewnątrz pomieszczeń (głównie biurowych).
- **bibi-R42** - czytnik wyposażony w kolorowy ekran dotykowy, przeznaczony głównie do rejestracji czasu pracy. Może też pracować jako czytnik kontroli dostępu z klawiaturą PIN-kodów.
- **bibi-R43** - elegancki czytnik z klawiaturą na szklanym froncie (dowolnym wygląd klawiatury). Czytnik jest przeznaczony do pracy wewnątrz pomieszczeń (głównie biurowych).
- **bibi-R44** – czytnik bezprzewodowy – zasięg do 100 m od stacji bazowej **bibi-D54**
- **bibi-T40** – terminal zawierający oprócz czytnika R40 wyjście tranzystorowe do sterownia rygla i dwa wejścia (typowo: czujnik otwarcia drzwi i przycisk wyjścia)
- **bibi-T41** – terminal z frontem szklanym zawierający oprócz czytnika R41 wyjście tranzystorowe do sterownia rygla i dwa wejścia (typowo: czujnik otwarcia drzwi i przycisk wyjścia)

Oprócz ww. dostępne są czytniki Administratora Systemu podłączane bezpośrednio do terminala operatora. Ułatwiają wprowadzanie kart do systemu bibinet.

- **bibi-A40** - czytnik podłączany przez złącze USB.

2.2.2 Czytniki Mifare oraz I-Code

W tym standardzie RFID mamy dostępne następujące czytniki i terminale:

- **bibi-R50** - czytnik odporny na warunki atmosferyczne.
- **bibi-R51** – elegancki czytnik z frontem szklanym (z dowolnym nadrukiem) przeznaczony do pracy wewnątrz pomieszczeń (głównie biurowych)
- **bibi-R52** - czytnik wyposażony w kolorowy ekran dotykowy, przeznaczony głównie do rejestracji czasu pracy. Może też pracować jako czytnik kontroli dostępu z klawiaturą PIN-kodów.
- **bibi-R53** - elegancki czytnik z klawiaturą na szklanym froncie (dowolnym wygląd klawiatury). Czytnik jest przeznaczony do pracy wewnątrz pomieszczeń (głównie biurowych).
- **bibi-R54** - czytnik bezprzewodowy – zasięg do 100 m od stacji bazowej **bibi-D54**
- **bibi-T50** – terminal zawierający oprócz czytnika R40 wyjście tranzystorowe do sterownia rygla i dwa wejścia (typowo: czujnik otwarcia drzwi i przycisk wyjścia)
- **bibi-T51** – terminal z frontem szklanym zawierający oprócz czytnika R51 wyjście tranzystorowe do sterownia rygla i dwa wejścia (typowo: czujnik otwarcia drzwi i przycisk wyjścia)

oraz czytnik Administratora Systemu

- **bibi-A50** – podłączany do terminala operatora przez złącze USB.

2.2.3 Czytniki innych producentów

System bibinet może współpracować także z czytnikami innych producentów (np. HID, IDESCO, PROMAG, Roger ...). Mogą to być także czytniki biometryczne lub czytniki dalekiego zasięgu pracujące w paśmie UHF. Podłączenie tych czytników do magistrali bibiBUS odbywa się przy pomocy specjalnego terminala **bibi-T30**.

2.3 Rejestratory Czasu Pracy

Urządzeniami, które służą tylko do ewidencji czasu pracy (bez funkcji kontroli dostępu) są rejestratory RCP. Obecnie w ofercie są dwa rejestratory

- **bibi-C24** pracujący z identyfikatorami zbliżeniowymi Unique 125 kHz.
- **bibi-C25** pracujący z identyfikatorami zbliżeniowymi Mifare 13,56 MHz.

Wybór rodzaju rejestrowanego zdarzenia (wejście, wyjście, normalne, służbowe, przerwa itp.) odbywa się na kolorowym panelu dotykowym rejestratora.

Komunikacja z komputerem zarządzającym realizowana jest poprzez sieć Ethernet protokołem TCP/IP.

2.4 Moduły rozszerzeń

Do magistrali bibiBUS kontrolerów można dodatkowo podłączać urządzenia zwiększające ich możliwości. Są to moduły rozszerzeń:

- **bibi-D50** moduł pokazujący aktualny czas systemowy kontrolera
- **bibi-D51** moduł dodatkowych 3 wyjść przekaźnikowych i 6 wejść
- **bibi-D52** moduł dodatkowych 2 wyjść przekaźnikowych i 8 wejść
- **bibi-D53** moduł winda: dodatkowe 8 wyjść przekaźnikowych i 5 wejść
- **bibi-D54** moduł obsługi czytników bezprzewodowych

2.5 Akcesoria systemu kontroli dostępu

W ofercie posiadamy dedykowane do naszych urządzeń metalowe obudowy MM-OM1 z zasilaczami firmy MEAN WEEL produkowane wg naszego projektu przez firmę Pulsar. W obudowach można zamontować do 3 urządzeń systemu bibinet w obudowach DIN i maksymalnie 2 moduły bezpiecznikowe MM-F01, które służą do odseparowania zasilania czytników od zasilania rygli rewersyjnych i zwór elektromagnetycznych.

2.6 Autonomiczne zamki kontroli dostępu

Urządzenia autonomiczne nie są podłączane do sieci urządzeń systemu bibinet. Są one uzupełnieniem systemu w miejscach, gdzie trudno lub kosztownie jest doprowadzić okablowanie i do których dostęp ma zwykle ma mała liczba osób. Takim urządzeniem są elektroniczne zamki kontroli dostępu obsługiwane kartami MASTER:

- **Mm-Z40** – autonomiczny zamek sterowany kartami Unique 125 kHz
- **Mm-Z41** – autonomiczny zamek z frontem szklanym sterowany kartami Unique 125 kHz
- **Mm-Z50** - autonomiczny zamek sterowany kartami Mifare i I-Code 13,56 MHz
- **Mm-Z51** - autonomiczny zamek z frontem szklanym sterowany kartami Mifare i I-Code 13,56 MHz

3. Oprogramowanie

3.1 Dostępne licencje

Oprogramowanie jest licencjonowane. Licencja określa zakres działania programu co do ilości obsługiwanych osób, określa funkcje programu i aktywne opcje dodatkowe.

Producent przygotował do wyboru kilka licencji:

- **bibi.KD** – obsługa tylko funkcji kontroli dostępu, możliwość pracy tylko na jednym komputerze, obsługa urządzeń sieciowych (np. bibi-F22, bibi-K22, bibi-K25, bibi-C24, bibi-C25), maksymalnie 10 000 użytkowników, zawiera 2 klucze sprzętowe USB bibi.HAK do szyfrowania danych.
- **bibi.50** – obsługa funkcji kontroli dostępu i rejestracji czasu pracy, możliwość pracy tylko na jednym komputerze, obsługa urządzeń sieciowych, możliwe dokupienie opcji podglądu raportów pracowniczych przez przeglądarkę internetową, maksymalnie 50 użytkowników w systemie (50 kart), zawiera 2 klucze sprzętowe bibi-.HAK do szyfrowania danych.
- **bibi.150** – obsługa funkcji kontroli dostępu i rejestracji czasu pracy, możliwość pracy na 3 komputerach, obsługa urządzeń sieciowych, możliwe dokupienie opcji podglądu raportów pracowniczych przez przeglądarkę internetową, max. 150 użytkowników, zawiera 2 klucze sprzętowe bibi.HAK do szyfrowania danych.
- **bibi.500** – obsługa funkcji kontroli dostępu i rejestracji czasu pracy, możliwość pracy na 3 komputerach, obsługa urządzeń sieciowych, możliwe dokupienie opcji podglądu raportów pracowniczych przez przeglądarkę internetową, do 500 użytkowników, zawiera 2 klucze sprzętowe bibi.HAK do szyfrowania danych
- **bibi.XL** – obsługa funkcji kontroli dostępu i rejestracji czasu pracy, możliwość pracy na 6 komputerach, obsługa urządzeń sieciowych, możliwe dokupienie opcji podglądu raportów pracowniczych przez przeglądarkę internetową, do 10 000 użytkowników, zawiera 2 klucze sprzętowe bibi.HAK do szyfrowania danych
- **bibi.XXL** – obsługa funkcji kontroli dostępu i rejestracji czasu pracy, możliwość pracy na 8 komputerach, obsługa urządzeń sieciowych, możliwe dokupienie opcji podglądu raportów pracowniczych przez przeglądarkę internetową, do 15 000 użytkowników, zawiera 2 klucze sprzętowe bibi.HAK do szyfrowania danych. **Licencja nie może współpracować z systemami, w których wykorzystane są kontrolery bibi-K12 i starsze.**
- **bibi.EDU** – licencja specjalna dla szkół, obsługa funkcji kontroli dostępu i ewidencji czasu pracy, możliwość pracy na jednym komputerze, obsługa urządzeń sieciowych, do 10 000 użytkowników (uczniów + nauczycieli), zawiera 2 klucze bibi.HAK do szyfrowania danych

Powyższe licencje można rozszerzać o dodatkowe stanowiska komputerowe, dodatkowe opcje, dokupować klucze sprzętowe – w zależności od potrzeb.

Oprogramowanie udostępnia podgląd raportów pracowniczych przez przeglądarkę internetową. Jest to opcja dodatkowa **bibi.PDP** opłacana w postaci rocznego abonamentu. Podgląd jest zabezpieczony przy pomocy protokołu SSL.

3.2 Programy - klienci sieci bibi.net

Programy - klienci sieci bibi.net mogą być uruchamiani na dowolnym terminalu. Są to następujące programy:

- **bibi** – podstawowy program do konfiguracji urządzeń oraz do wytwarzania raportów kontroli dostępu i ewidencji czasu pracy
- **bibi szef** – program do raportowania on line aktualnej frekwencji pracowników na terenie obiektu
- **bibi bramka** – program do podglądu on line wybranego przejścia kontrolowanego (przeznaczony głównie dla służb ochrony.
- **bibi fakty** – program do bieżącej wizualizacji zdarzeń, które występują w systemie (poza rejestracjami) - zapis pracy operatorów, zdarzeń zgłaszanych przez urządzenia, przez system itp. Program ponadto umożliwia wydrukowanie (do plików formatu pdf) list obecnych w danych strefach lub obszarach pracowników (np. w celi ewakuacji.

Wszyscy klienci komunikują się z serwerem za pomocą prostych, standardowych funkcji zebranych w bibliotece bibi10.dll. Opis tych funkcji jest udostępniony przez firmę MicroMade. Dlatego, oprócz używania standardowych klientów sieci bibi.net, istnieje możliwość napisania własnych programów do obróbki danych zgromadzonych w serwerach bibinet.

3.3 Kodowanie transmisji – klucze sprzętowe

Jak już wspomniano, węzły sieci potrafią porozumiewać się ze sobą zarówno wewnątrz sieci lokalnej jak i poprzez routery i sieć Internet. Dla zapewnienia bezpieczeństwa przesyłanych danych, cała transmisja pomiędzy węzłami w sieci TCP/IP jest szyfrowana z siłą 3DES. Klucz do szyfrowania o wielkości 3 x 56 bitów jest losowany w każdej instalacji i przechowywany w kluczach sprzętowych bibi.HAK. Klucz sprzętowy uczestniczy w szyfrowaniu transmisji pomiędzy węzłami sieci - dlatego **do prawidłowej pracy niezbędny jest klucz sprzętowy** z danej instalacji **w każdym węźle sieci bibi.** Klucz ten szyfruje także transmisję pomiędzy węzłem sieci bibi.net a podłączonymi do niego urządzeniami sieciowymi systemu bibinet.

Klucze sprzętowe dodatkowo przechowują hasła operatorów systemu bibinet. W każdym kluczu można zapisać 32 takie hasła.

Do konfiguracji kluczy sprzętowych w systemie służy program narzędziowy bikeys.exe

Standardowo do każdej licencji dołącza się 2 klucze bibi.HAK

3.4 Programy narzędziowe

Razem z podstawowym oprogramowaniem dostarczany jest cały zestaw programów narzędziowych ułatwiających pracę instalatora i administratora systemu bibinet:

- biArchiver – program służący do zamykania starych okresów rozliczeniowych. Dzięki niemu baza danych podlegających edycji nie rozrasta się w nieskończoność. Program umożliwia też „czyszczenie” rekordów zajmowanych przez zwolnionych pracowników.
- biclient – program ustawiający sposób logowania do programu bibi, niezbędny przy instalacji terminali.
- bicomp – aplikacja odczytująca parametry identyfikacyjne komputera, przydatna przy deklaracji komputerów w sieci bibi.net
- biExport – program umożliwiający export rejestracji do innych programów kadrowo – płacowych
- bikeys – program do zarządzania kluczami sprzętowymi bibi.HAK
- bipnp – program przeznaczony do wyszukiwania urządzeń systemu bibinet podłączonych do sieci Ethernet
- bis2h – przepisuje hasła z klucza software'owego (licencja programowa) do kluczy sprzętowych
- biserver – program do konfiguracji serwera systemu bibinet
- bisetup – program do zakładania bazy danych
- biSprzet – program służący do aktualizowania oprogramowania w kontrolerach bibi-K12 podłączonych do komputera przez interfejs bibi-F21. Urządzenia podłączone przez sieć Ethernet (np przez interfejs bibi-F22 aktualizują się automatycznie)

Oprócz tych programów w osobnej kartotece na nośniku z instalatorem programu bibi jest dostępny także program biSprzetLAN.exe służący do wstępnej konfiguracji kontrolerów bibi-K22, bibi-K25 i kontrolera windy bibi-K28.

4. Instalacja oprogramowania 1.10.12.x

4.1 Reinstalacja z wersji wcześniejszych oprogramowania

Uwaga!

Bezpośrednie przejście do wersji 1.10.xx oprogramowania jest możliwe tylko z wersji 1.9.xx. Aby dokonać przejścia z wersji niższych, należy najpierw uaktualnić posiadaną wersję programu do wersji 1.9.xx. Program instalacyjny w wersji 1.9.xx można pobrać ze strony: http://pliki.micromade.pl/archiwum/bibinet_setup_19.zip Opis reinstalacji wersji starszych do wersji 1.9.xx opisany jest w instrukcji instalacji 1.9.0.0.

Uwaga!

Reinstalacja do wersji 1.10.xx jest możliwa pod warunkiem posiadania pliku licencji wystawionego nie wcześniej niż rok przed datą reinstalacji. Datę wystawienia pliku licencji można zmienić wykupując odpowiedni abonament. Informacje na ten temat są dostępne na https://micromade.pl/wsparcie/zdalna-pomoc-bibinet/

Uwaga!

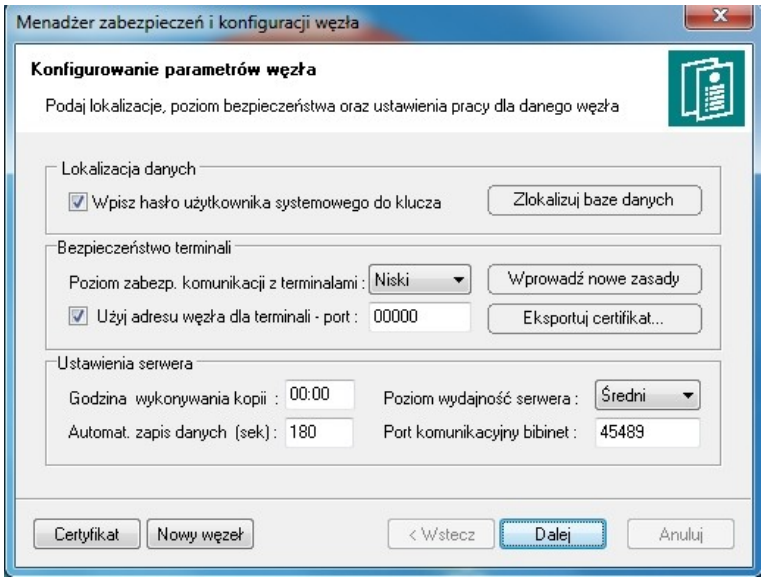
Jeżeli do systemu podpięte są kontrolery poprzez interfejs bibi-F21, po wykonaniu reinstalacji oprogramowania (opis poniżej) należy przeprowadzić aktualizację sprzętu przy pomocy programu narzędziowego biSprzęt. Jeżeli do systemu podpięte są kontrolery bibi-K12 przez interfejs ethernetowy bibi-F22 lub kontrolery bibi-K22 i bibi-K25 aktualizacja sprzętu wykona się automatycznie po uruchomieniu programu bibi w nowej zaktualizowanej wersji.

Wersja instalacyjna programu jest dostępna na:

https://micromade.pl/wsparcie/biblioteka-programow/programy-systemu-bibinet/

Instalator w wersji 1.10.x.x potrafi automatycznie uaktualnić poprzednią wersję systemu. W tym celu należy:

- Wyłączyć wszystkie aplikacje bibi
- Programem narzędziowym biserver,exe zatrzymać pracę serwera bibinet (wszystkich serwerów bibinet jeżeli w systemie jest więcej niż jeden bibinet serwer). W tym celu należy:
  - uruchomić program biserver.exe
  - zalogować się jako Administrator
  - ustawić *Poziom zabezpieczeń komunikacji z terminalami* na *Niski*
  - wcisnąć *Wprowadź nowe zasady*
  - nie trzeba restartować systemu Windows
  - zamknąć program biserver.exe



- Uruchomić program bibinet_setup.exe.
  - Zaakceptować umowę licencyjną

Program automatycznie uaktualni potrzebne pliki, zgodnie z poprzednio wybranym typem instalacji.

- Uruchomić program narzędziowy biserver.exe.
  - zalogować się jako Administrator
  - wcisnąć klawisz *Zlokalizuj bazę danych*
  - ustawić na nowo tryb pracy serwera (wysoki lub niski – taki jak był pierwotnie ustawiony)
  - wcisnąć *Wprowadź nowe zasady*
  - nie trzeba restartować systemu Windows
  - jeżeli do serwera podłączone są terminale należy dodatkowo wyeksportować nowy certyfikat węzła
- Zamknąć program biserver.exe

Po wykonaniu tych operacji system bibinet pracuje już w wersji 1.10.xx.x

Operację należy wykonać na wszystkich węzłach systemu bibinet.

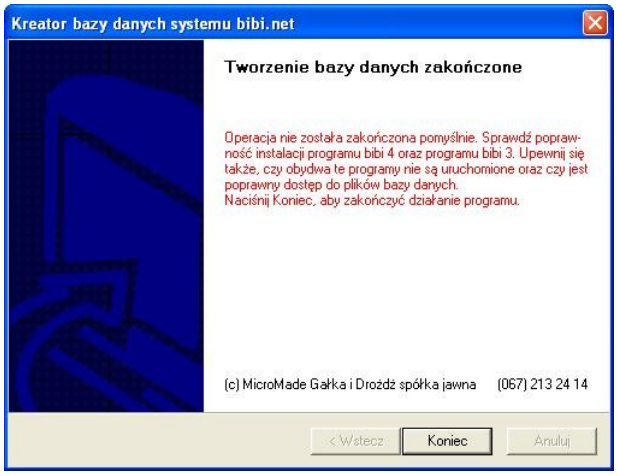
Jeżeli w systemie zadeklarowane są terminale należy na każdym z nich uruchomić instalator bibinet_setup.exe w celu uaktualnienia wersji oprogramowania na terminalu.

4.1.1 Możliwe problemy z reinstalacją

Jeżeli po uruchomieniu instalatora pojawi się informacja:

to należy przed następną próbą reinstalacji zamówić usługę bibi.WTU (prawo do upgrade oprogramowania i wsparcia technicznego przez rok). Po zajupie usługi zostanie przesłany e-mailem plik licencji z aktualną datą, który należy podmienić w katalogu (standardowo) C:\Program Files(x86)\MicroMade\bibinet\Server\Data.

Po zakończeniu konwersji danych program poinformuje o tym okienkiem końcowym. Jeżeli w trakcie przetwarzania danych wystąpiły jakieś błędy, okienko końcowe będzie wyglądało następująco:



W takim wypadku należy usunąć przyczyny błędów i ponownie uruchomić program bisetup.exe.

4.2 Instalacja oprogramowania w nowym systemie bibinet

Program bibi jest licencjonowany. Właścicielem licencji jest firma, która jest (będzie) użytkownikiem systemu bibinet. Każda licencja zawiera następujące elementy:

- Plik licencyjny license.dat podpisany cyfrowo zawierający zakres wykupionej licencji, nazwę i adres użytkownika oraz datę wydania licencji
- Dwa klucze USB bibi.HAK służące do przechowywania haseł operatorów i szyfrowania transmisji w systemie bibinet
- Certyfikat PDF niezbędny do podpisywania dokumentów w formacie *.pdf generowanych przez program.
- Certyfikat SSL (opcja) dostarczany jeżeli została wykupiona opcja oglądania raportów przez przeglądarkę internetową (bibi.PDP).

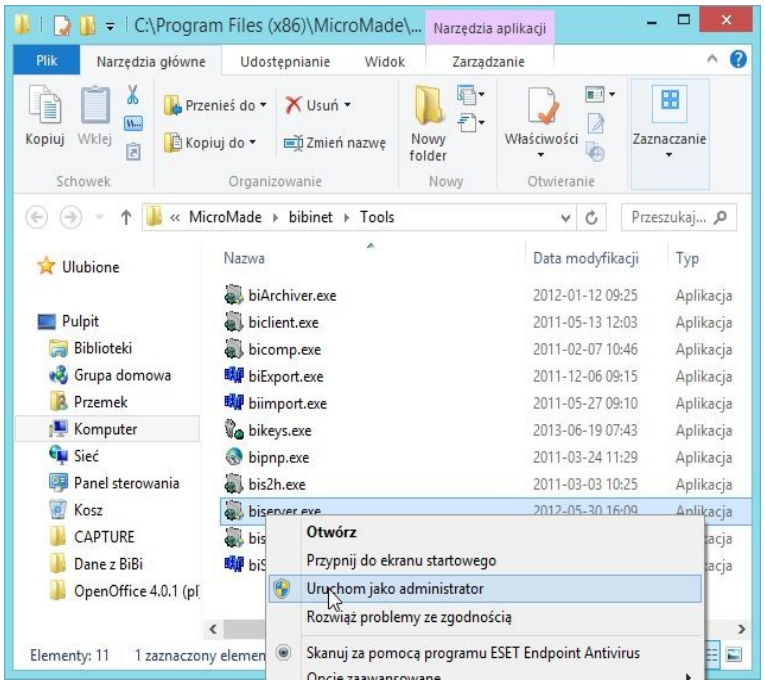
Dzięki tym elementom dane w systemie przechowywane i przesyłane są w bezpiecznym sposób. Skutkuje to jednak tym, że instalację takiego oprogramowania trzeba wykonać w kilku krokach:

- Instalacja programów bibi
- Wytworzenie bazy danych systemu i zainstalowanie certyfikatu PDF
- Konfiguracja kluczy szyfrujących bibi.HAK

Instalacja oprogramowanie powinna być przeprowadzona przez administratora sieci komputerowej użytkownika systemu lub pod jego nadzorem.

4.2.1 Przed instalacją

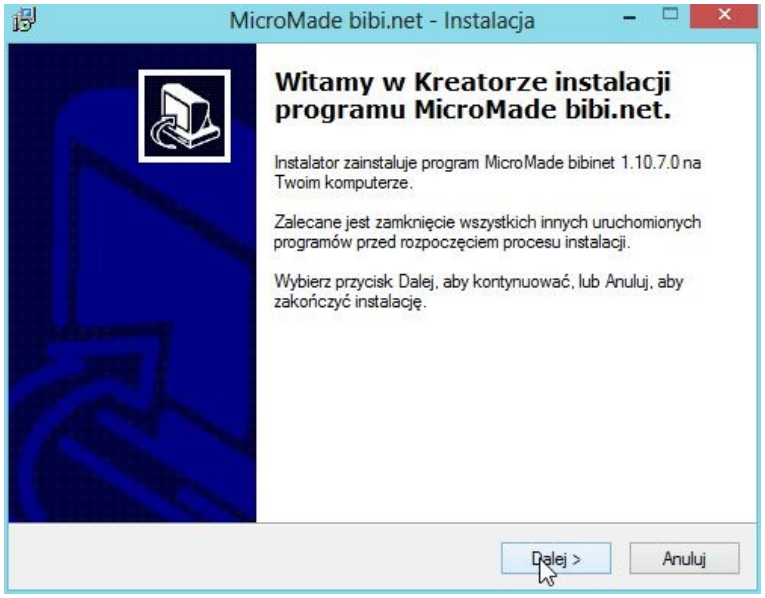
- Nie zalecamy instalacji węzła na systemach linii Windows Home (wyjątkiem jest instalacja jednostanowiskowa lub węzeł bez dodatkowych terminali).
- Instalację programu należy przeprowadzić na koncie Administratora komputera jeżeli instalujemy węzeł grupie roboczej Windows albo na koncie Administratora domeny jeżeli komputer jest podłączony do domeny. W systemach Windows 7/8/10 dodatkowo należy sprawdzić czy Administrator ma wyłączoną funkcję kontroli konta użytkownika. W tym celu trzeba otworzyć *Panel sterowania* i w sekcji *Konta użytkowników* przesunąć suwak (wybrać opcję) *Nie powiadamiaj nigdy*.
- Programy narzędziowe systemu bibinet znajdujące się w katalogu MicroMade/bibinet/Tools (skrót na Pulpicie: bibi - programy narzędziowe) należy uruchamiać będąc zalogowanym na koncie Administratora systemu Windows. Dodatkowo w systemie Windows 7/8/10 programy te należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”



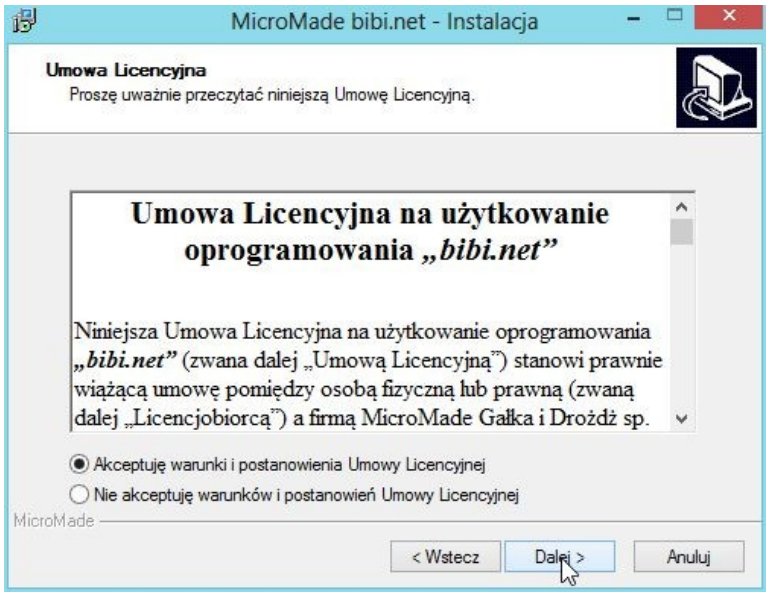
- Standardowo oprogramowanie Systemu Bibi instalowane jest w katalogu:
  - C:\Program Files(x86)\MicroMade\bibinet\ (dla systemów 64 bitowych)
  - C:\Program Files\MicroMade\bibinet\ (dla systemów 32bitowych).

4.2.2 Instalacja programów

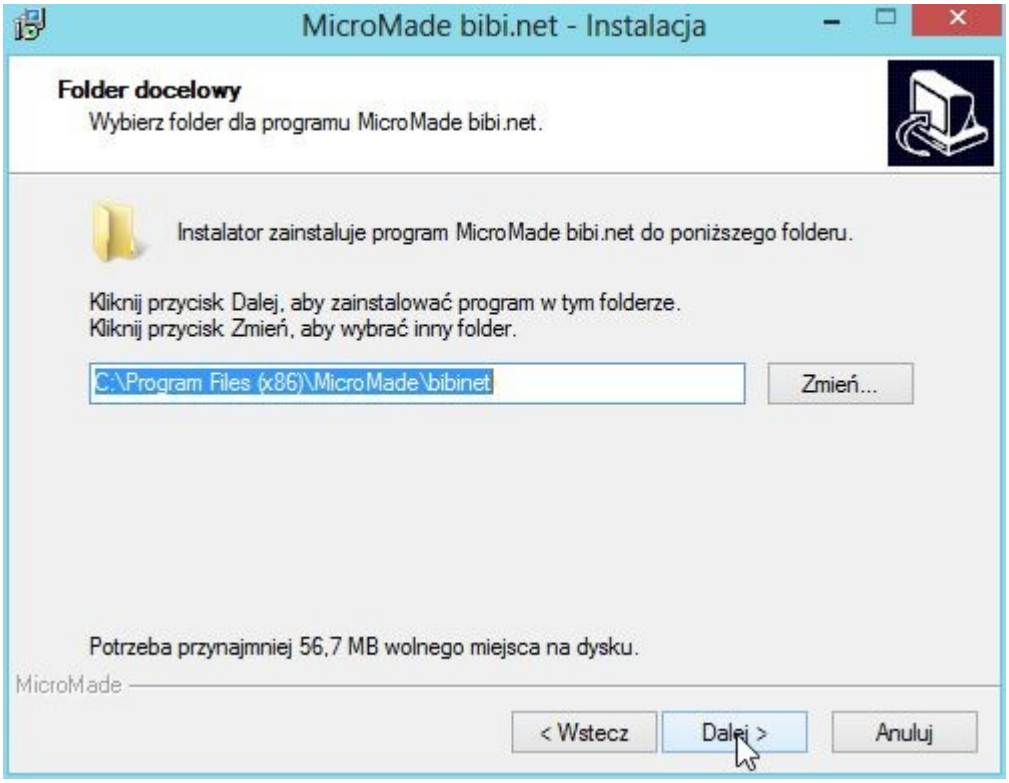
- Włożyć pendrive do złącza USB komputera. Wybrać z menu instalatora systemu bibinet "Instalacja bibinet" lub uruchomić program bibinet_setup.exe.



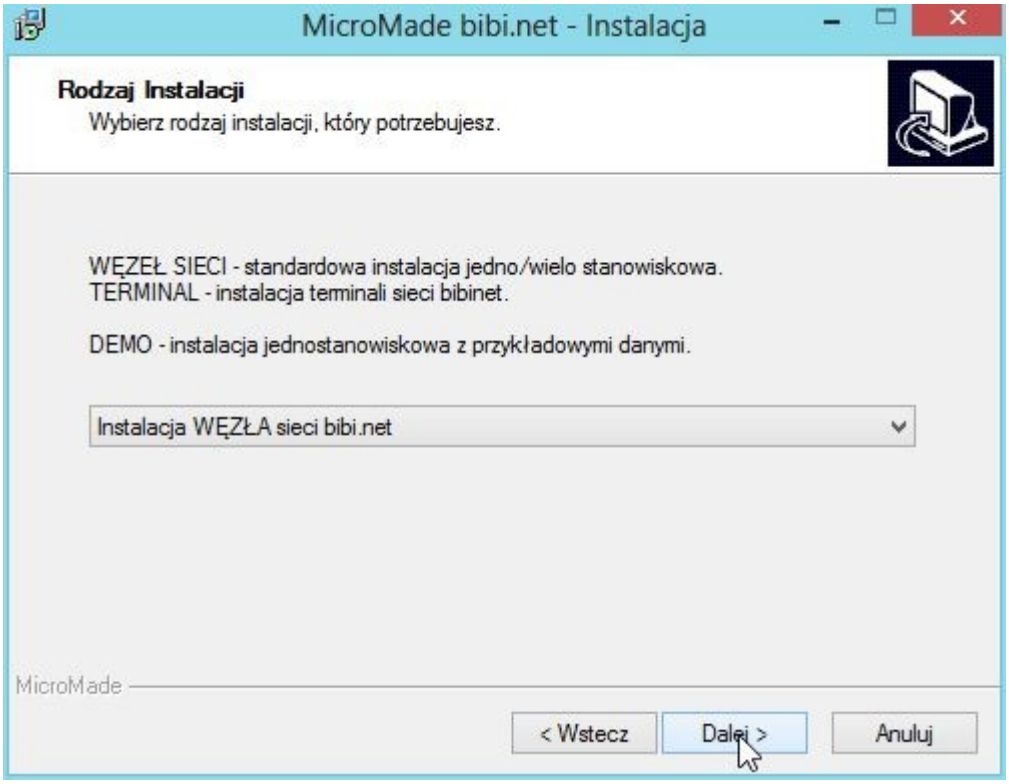
- Przeczytać i zaakceptować umowę licencyjną.



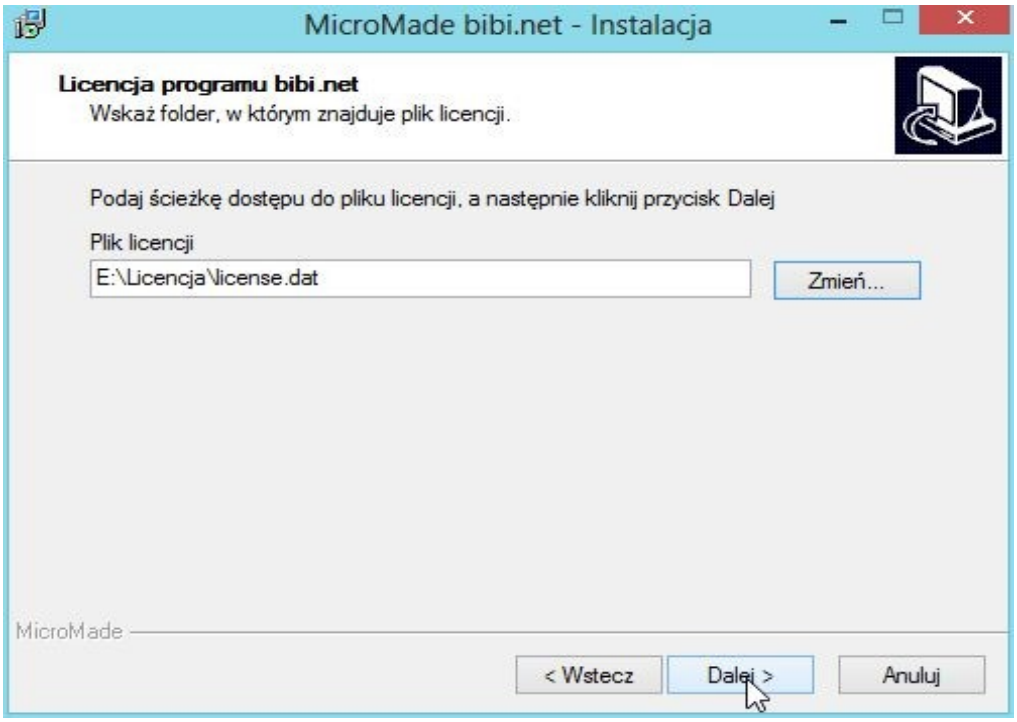
- Zaakceptować lub zmienić folder instalacji.



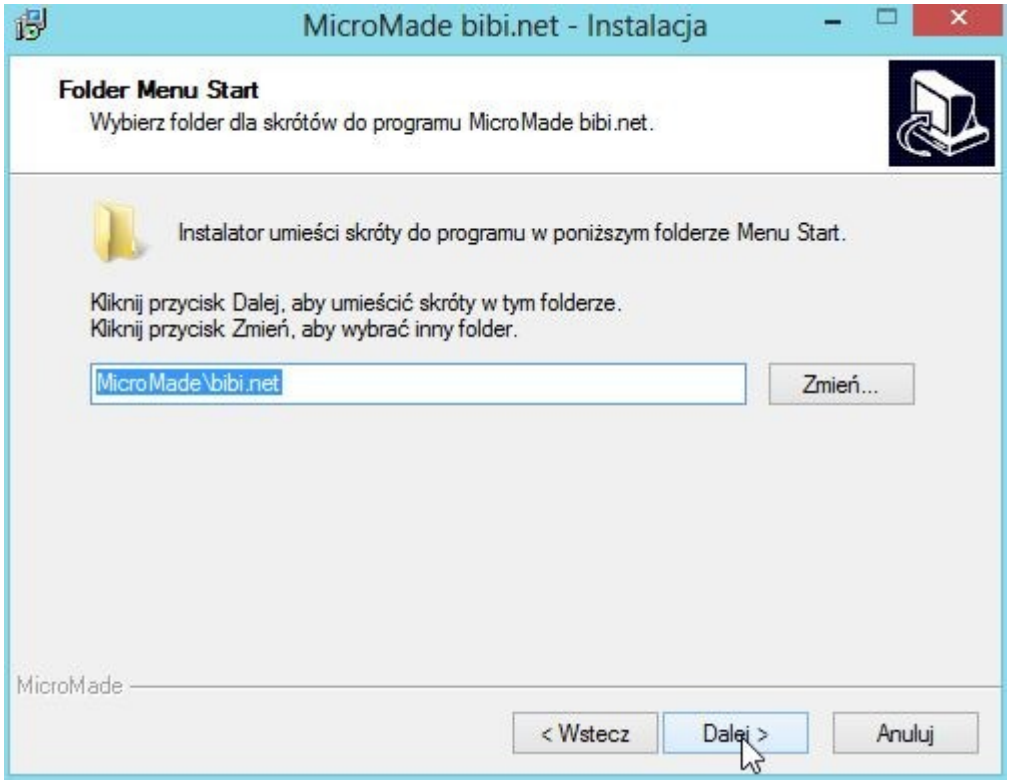
- Wybrać „Instalacja WĘZŁA sieci bibinet”.



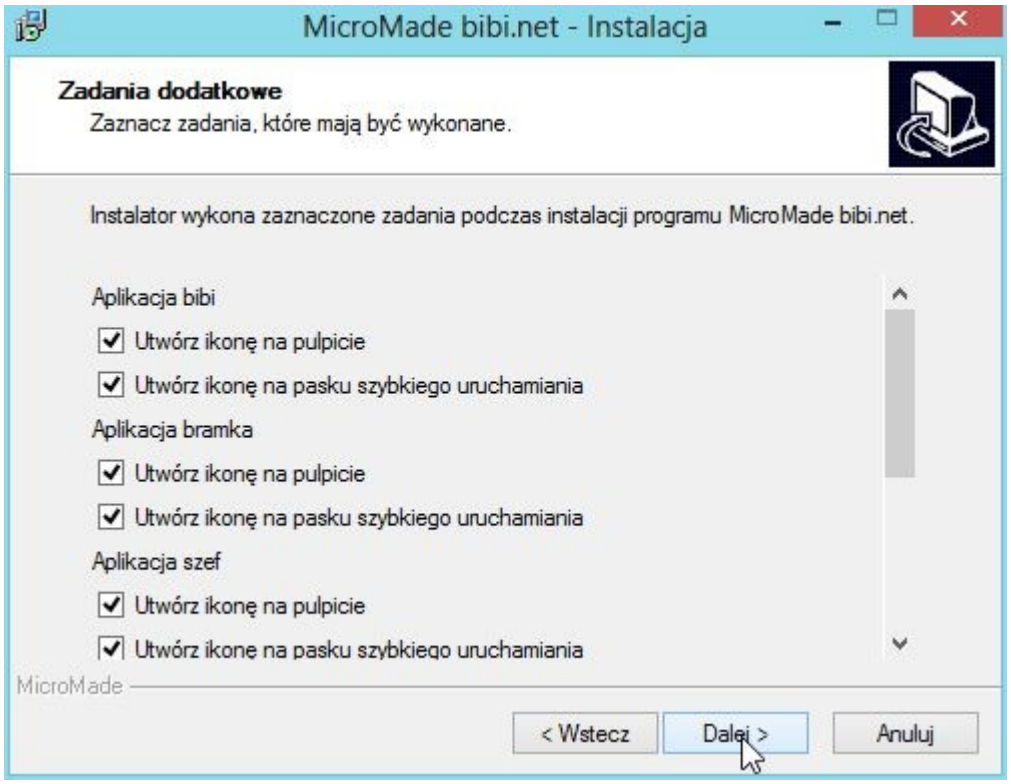
- Wskazać folder, w którym umieszczony jest plik licencji license.dat. Może on być na pendrive w folderze Licencja lub został przesłany pocztą elektroniczną.



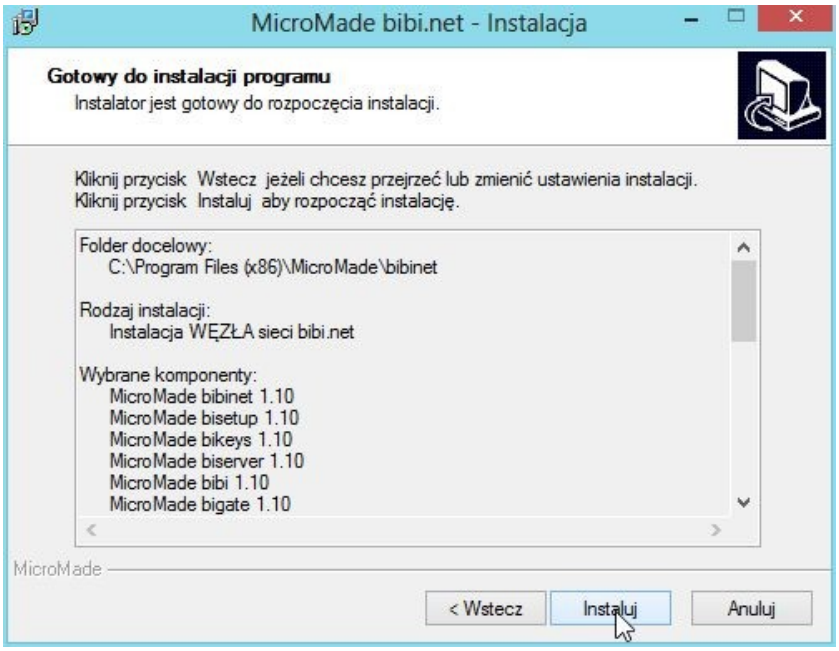
- Wybrać folder dla skrótów do programu.

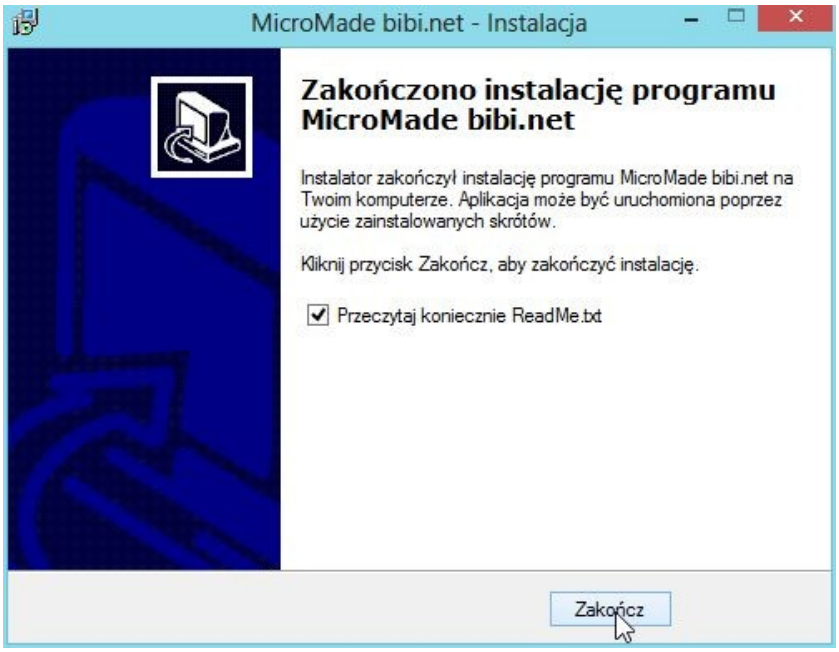


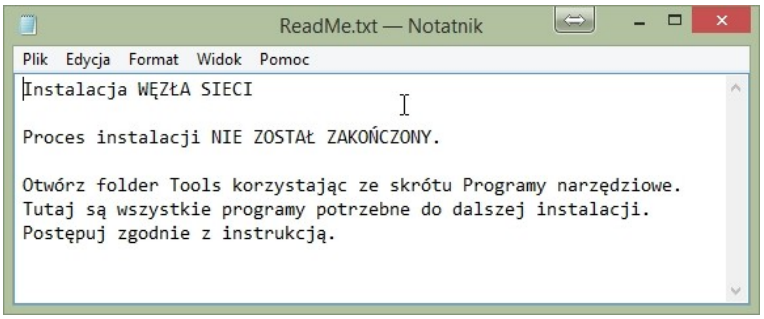
- Wybrać do jakich aplikacji systemu bibi mają być utworzone skróty i gdzie mają być umieszczone.



- Zakończyć proces instalacji klikając na klawisz Instaluj.







Programy użytkowe (bibi, bramka, szef) zostaną zainstalowane w folderze:

C:\Program Files(x86)\MicroMade\bibinet\

Programy narzędziowe zostaną zainstalowane w folderze:

C:\Program Files(x86)\MicroMade\bibinet\Tools\

Dokumentacje (tekst licencji i instrukcje) zostaną zainstalowane w folderze:

C:\Program Files(x86)\MicroMade\bibinet\Doc\

Baza danych systemu bibinet będzie tworzona w folderze:

C:\Program Files(x86)\MicroMade\bibinet\Server\Data

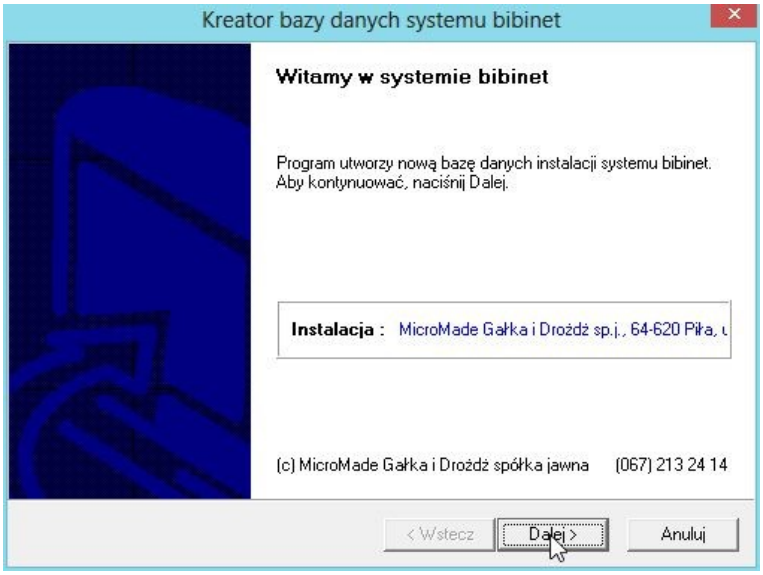
Wskazane powyżej foldery dotyczą standardowej instalacji w systemach Windows w wersji 64 bitowej. W systemach 32 bitowych pliki będą znajdowały się w odpowiednich folderach kartoteki C:\Program Files\

4.2.3 Wytworzenie bazy danych

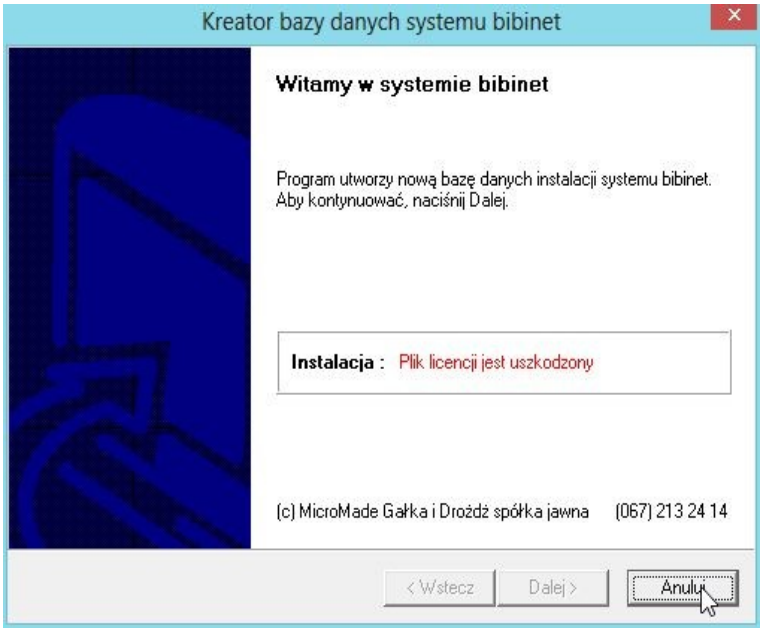
Po zainstalowaniu programów systemu bibinet należy wytworzyć bazę danych, w której będą gromadzone dane rejestrowane w systemie.

Do tego celu służy program narzędziowy bisetup.exe dostępny w katalogu C:\Program Files\MicroMade\bibinet\Tools\ lub w folderze bibi programy narzędziowe.

- Włożyć klucz bibi.HAK do złącza USB komputera
- Uruchomić program bisetup.exe (skrót: *bibi programy narzędziowe*), w systemie Windows 7/8/10 programy te należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”

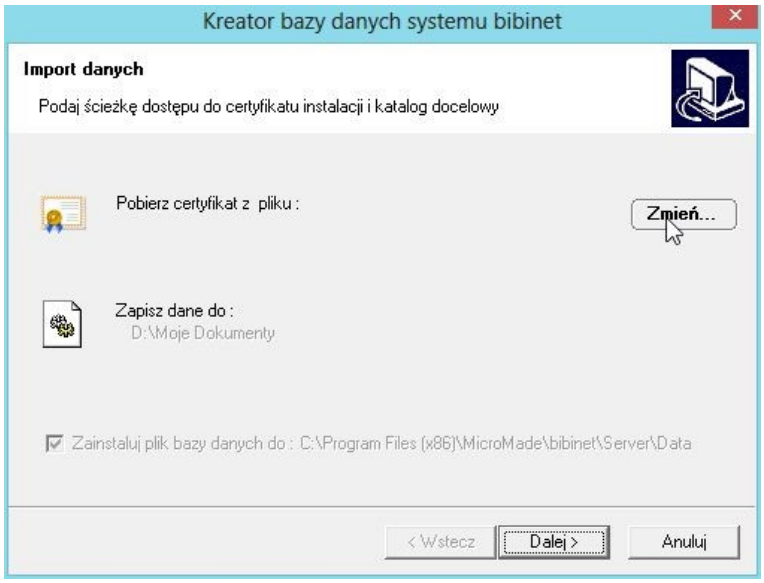


- Jeżeli program bisetup.exe zgłosi zastrzeżenie:



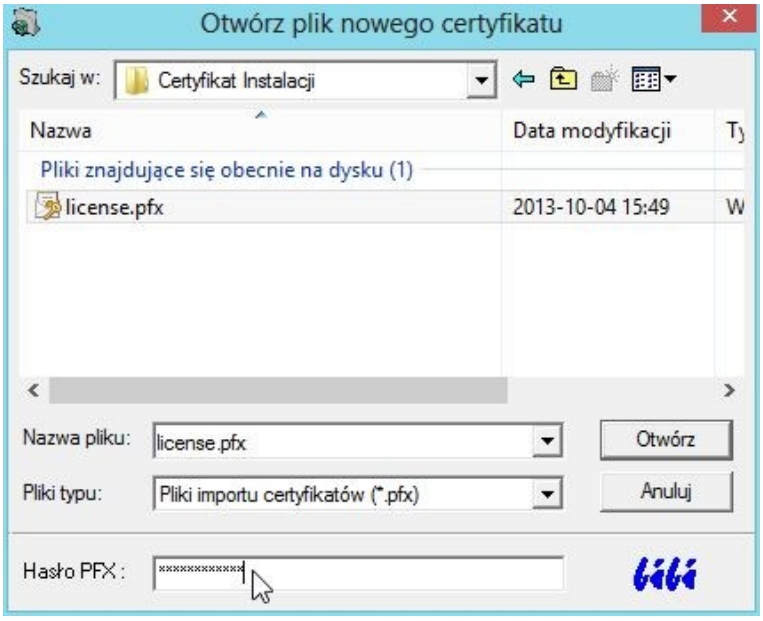
To oznacza, że nie został włożony do gniazda USB klucz bibi.HAK.

- Przejść Dalej do okna instalacji certyfikatu PDF



Klawiszem Zmień należy wskazać miejsce pliku license.pfx (certyfikatu klucza prywatnego do podpisywania dokumentów *.pdf). Jest on dostarczany z wersją instalacyjną programu na nośniku (pendrive) w katalogu Certyfikaty\ Certfikat Instalacji.

Certyfikat ten można też zainstalować później w programie narzędziowym biserver.exe w certyfikatach SSL węzła używając opcji "Dodaj certyfikat systemowy" (uruchamine z prawego klawisza myszy na polu Certyfikaty SSL węzła).



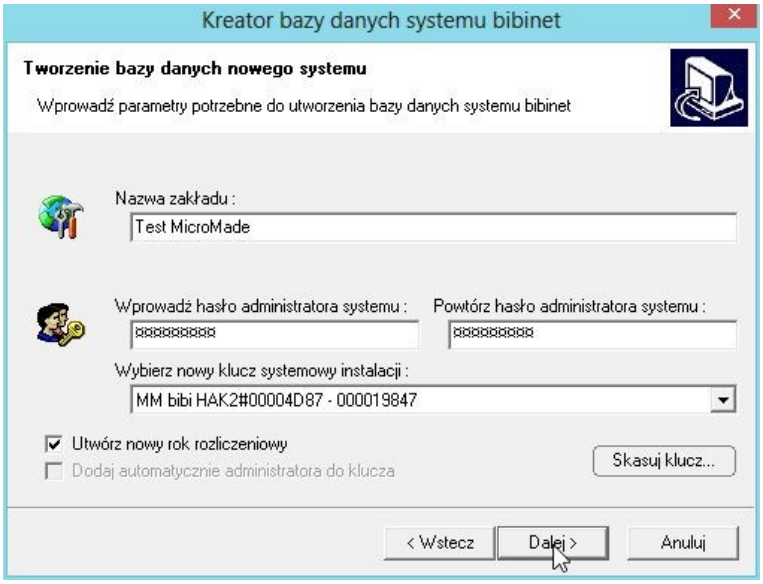
W oknie *Hasło PFX* wpisujemy hasło certyfikatu zapisane w pliku license.txt . **Zarówno hasło jak i plik certyfikatu powinny być przechowywane w bezpiecznym miejscu**.

Jeżeli po akceptacji klawiszem Otwórz na ekranie pojawi się ostrzeżenie

należy sprawdzić poprawność wprowadzonego hasła PFX i powtórzyć operację.

Uwaga: Instalację certyfikatu można pominąć. Nie jest on niezbędny do poprawnego działania programu bibi.

Po zainstalowaniu certyfikatu należy przejść do następnego okna w którym wpisujemy hasło **Administratora Systemu** bibinet (minimum 8 znaków) – ustalamy sami to hasło.



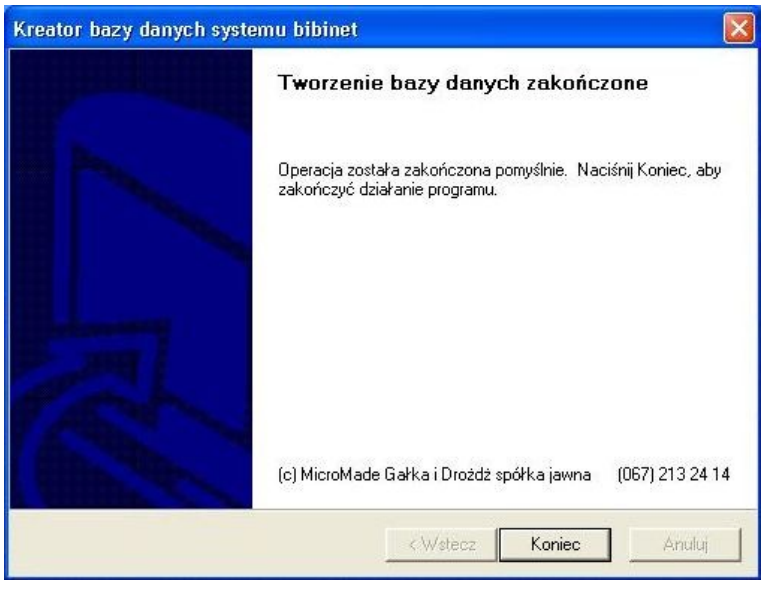
Jest to najważniejsze hasło w systemie bibinet i należy je przechowywać w bezpiecznym miejscu. Administrator Systemu ma władzę:

- Zarządzać kluczami sprzętowymi bibi.HAK
- Zmienić hasło Administratora programu bibi
- Zarządzać biblioteką certyfikatów w systemie bibinet

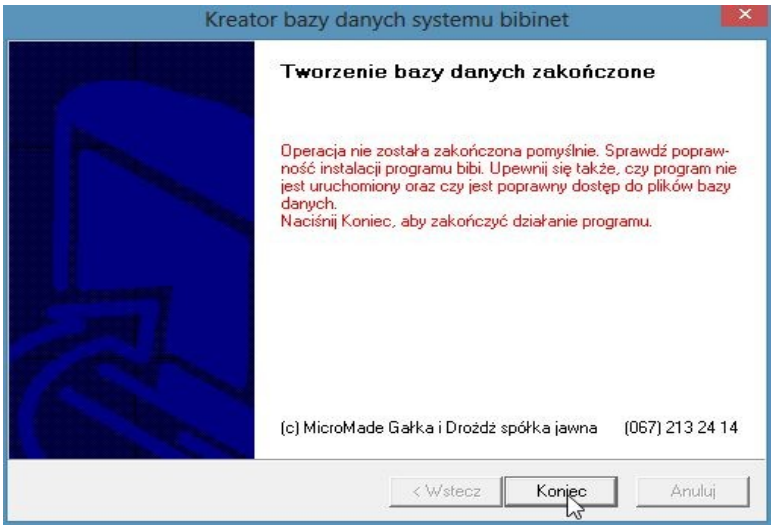
Następnie należy wybrać klucz systemowy instalacji. Wybrany klucz bibi.HAK będzie kluczem, z którego można pobierać hasło niezbędne do programowania innych kluczy bibi.HAK w systemie. Powinien być on przechowywany w bezpiecznym miejscu razem z hasłem Administratora Systemu.

Jeżeli klucz był wcześniej używany należy go skasować wciskając klawisz Skasuj klucz, następnie podając hasło kasujące. Hasło to dla każdego klucza bibi.HAK jest inne. Można je uzyskać pocztą elektroniczną z firmy MicroMade.

- Zakończyć tworzenie bazy danych systemu bibinet



- Podczas instalacji w systemach Windows 7/8/10 na niektórych komputerach może pojawić się następujące ostrzeżenie.



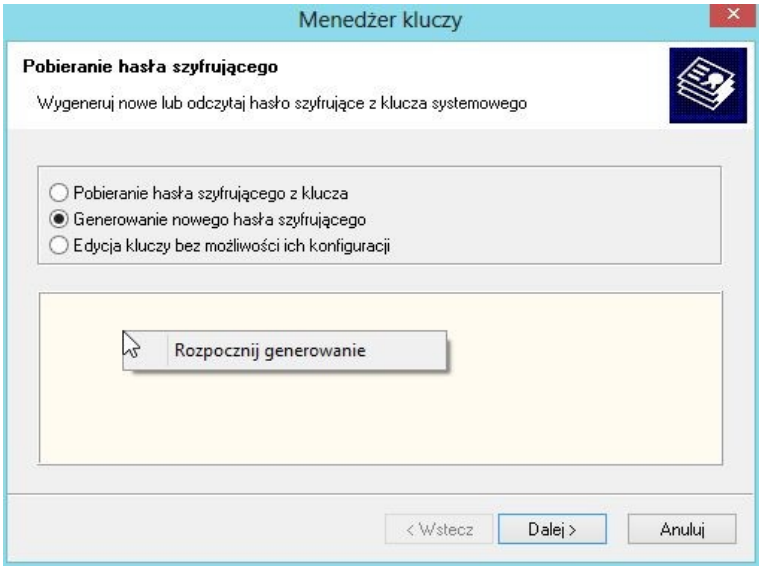
Nie znaczy ono jednak, że baza została źle zainstalowana. Najlepiej po zaprogramowaniu kluczy bibiHAK sprawdzić działanie programu.

4.2.4 Konfiguracja kluczy sprzętowych bibi.HAK

Do tego celu służy program narzędziowy bikeys.exe. W programie tym generowany jest algorytm szyfrujący transmisję w sieci urządzeń i komputerów bibi.net .

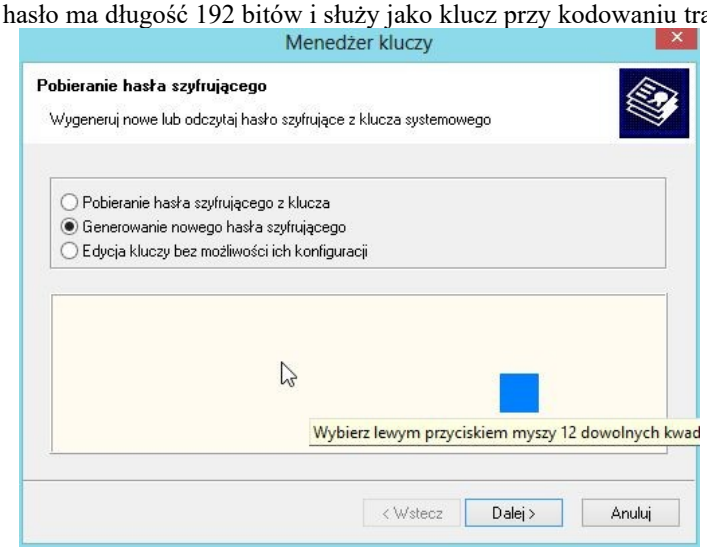
- Otworzyć program bikeys.exe (w systemie Windows 7 / 8 / 10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator") i zalogować się jako Administrator Systemu – hasło zadeklarowane przy tworzeniu bazy danych.

- Wybrać opcję Generowanie nowego hasła szyfrującego. **Ustawić kursor na białym polu poniżej**, wcisnąć prawy klawisz myszy i wciskając klawisz rozpocząć generowanie hasła. Generowanie polega na klikaniu lewym klawiszem myszy na pojawiające się na ekranie kwadraciki.

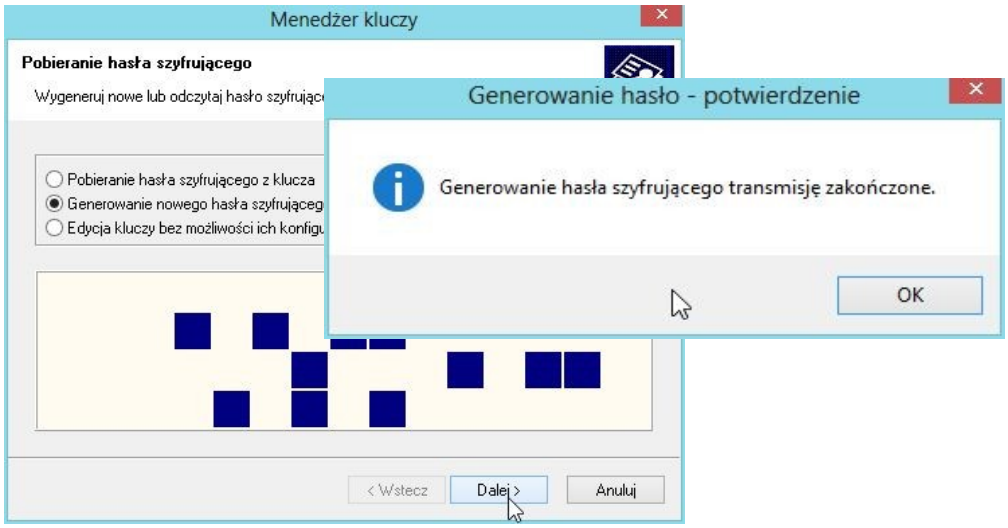


Po pojawieniu się takiego kwadratu należy najechać na niego myszką i kliknąć lewym klawiszem. Po trafieniu w 12 kwadratów (dowolne – nie muszą być kolejne) generowanie hasła jest zakończone.

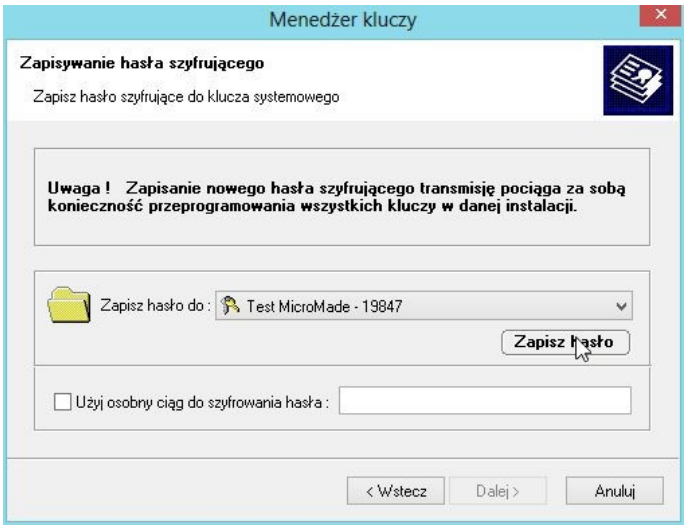
Tak wylosowane hasło ma długość 192 bitów i służy jako klucz przy kodowaniu transmisji algorytmem 3DES.

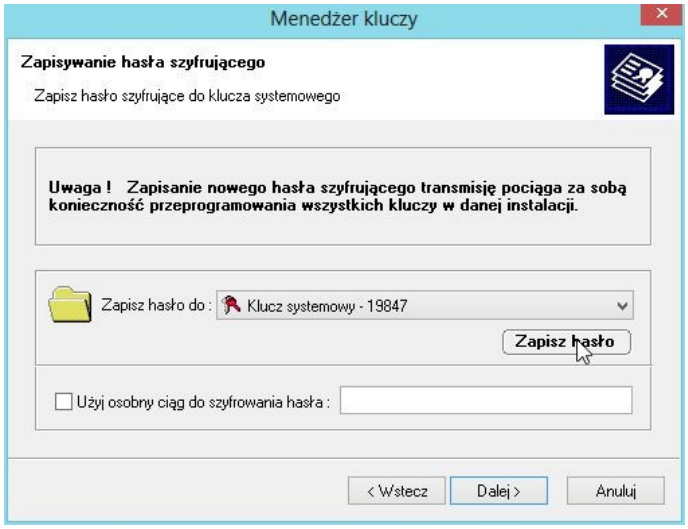


- Po wygenerowaniu hasła szyfrującego wcisnąć myszą przycisk *Dalej*

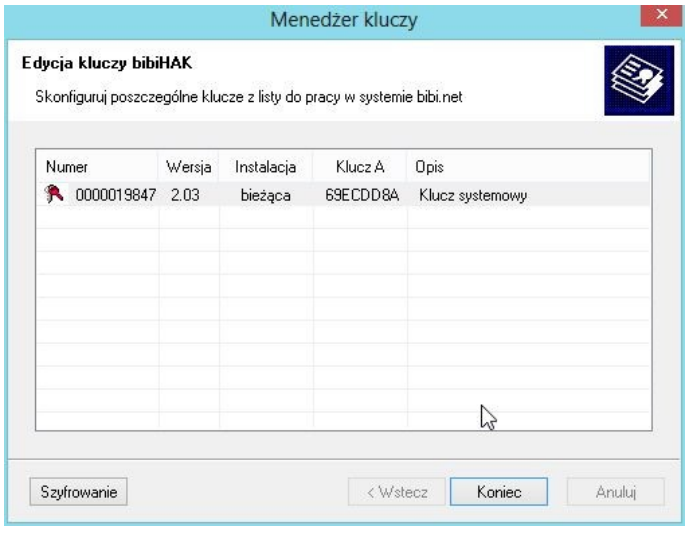


- W następnym oknie programu zapisać wygenerowane hasło szyfrujące do wybranego klucza. Ikona przy kluczu zmieni się na czerwony kolor i nazwa klucza zmieni się na „Klucz systemowy”

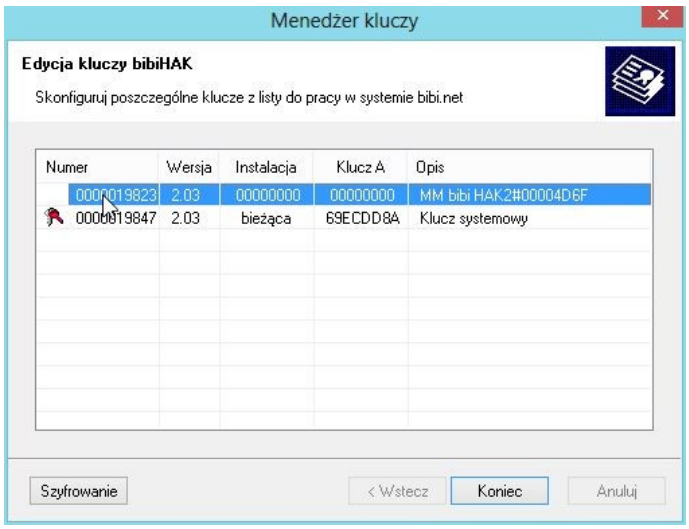


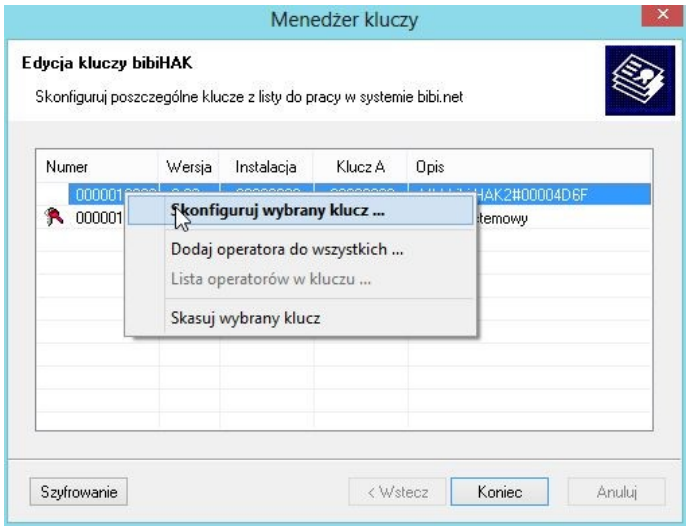


- **Klucz systemowy (wzorzec klucza instalacji) należy przechowywać w bezpiecznym miejscu razem z hasłem Administratora Systemu** ponieważ ten klucz umożliwia wytwarzanie kolejnych kluczy w przypadku rozbudowy systemu lub w przypadku awarii klucza używanego standardowo w systemie.

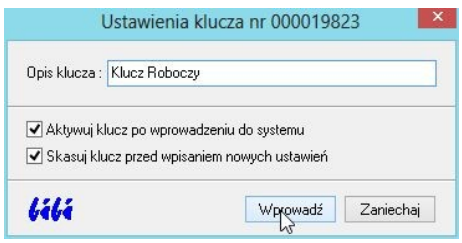


- Następnie (wcisnąć *Dalej*) przejść do tabeli kluczy. Klucz systemowy można już wyjąć. Włożyć drugi klucz do gniazda USB komputera. Pojawi się on w tabeli kluczy. Zaznaczyć go prawym klawiszem myszy. Z menu kontekstowego wybrać opcję *Skonfiguruj wybrany klucz*. Należy nadać mu unikalną nazwę tak, żeby łatwo można było go zidentyfikować np.:
  - klucz p. Marka
  - klucz Księgowej itp.

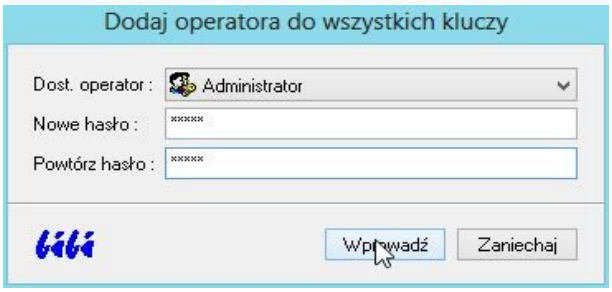




- Jeżeli klucz był już używany (inny system, próbna instalacja) należy najpierw wydać polecenie “skasuj wybrany klucz”. Do klucza zostanie przepisane hasło szyfrujące transmisję.

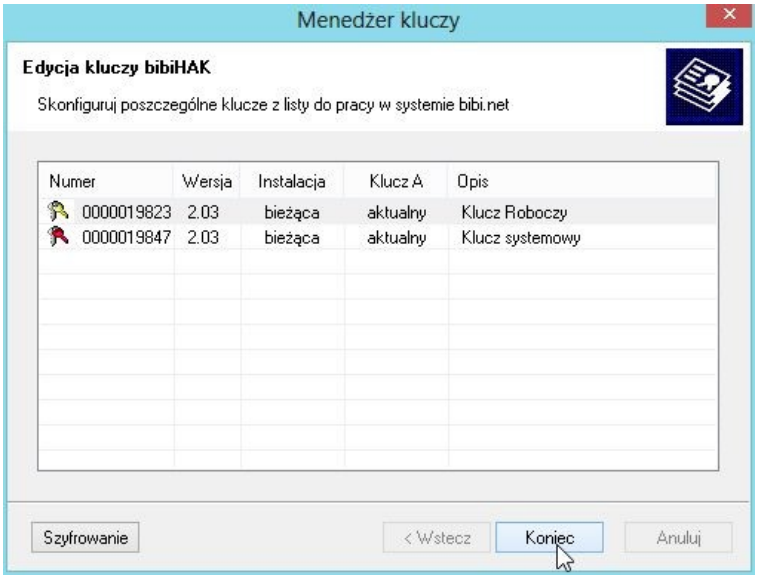


- Następnie z menu kontekstowego wybrać opcję *Dodaj operatora do wszystkich.* Wybrać z listy operatora *Administrator* i wprowadzić jego hasło do klucza (minimum 4 znaki).



W ten sposób należy skonfigurować klucze dostarczone wraz z licencją. **Klucz systemowy powinno się oznaczyć i umieścić w bezpiecznym miejscu razem z hasłem Administratora Systemu (lub hasło to zapamiętać)**. Drugi skonfigurowany klucz z wpisanym hasłem Administratora pozostaje w komputerze – węźle (serwerze) systemu bibinet. Wyjęcie tego klucza uniemożliwi działanie serwera bibinet.

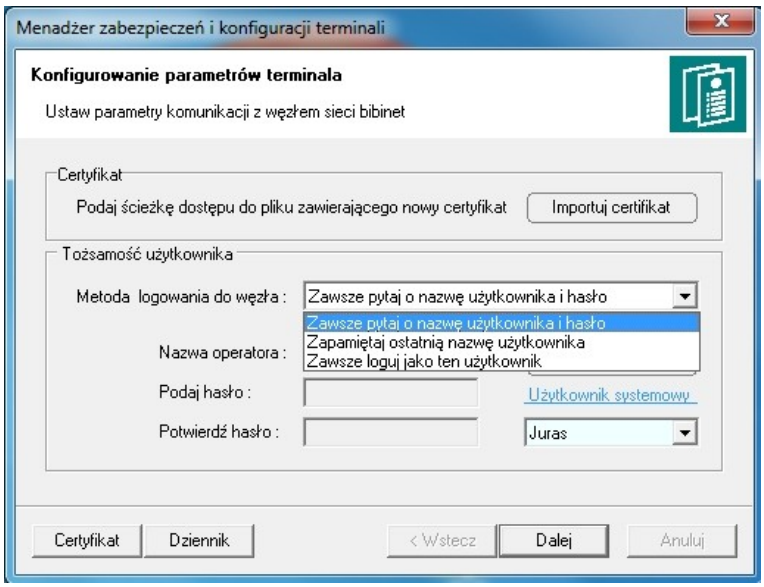
Administrator wpisany do klucza posiada największą władzę w programie podstawowym bibi. Pozwala zalogować się do programów narzędziowych biArchiver, biSprzęt, biServer, biKlient, bipnp. *Zalecamy dodanie operatora Administrator do klucza systemowego co umożliwia np. konfigurację terminali bez zatrzymywania pracy węzła (serwera) bibi.*



4.2.5 Zakończenie procesu instalacji

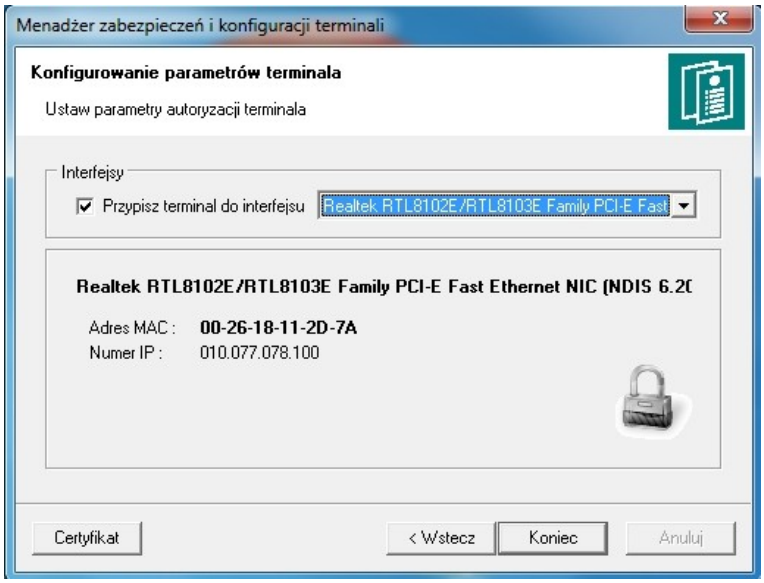
Po zakończeniu konfigurowania kluczy bibi.HAK należy uruchomić program narzędziowy biserver.exe znajdujący się w katalogu MicroMade/bibinet/Tools (skrót na Pulpicie: bibi - programy narzędziowe). **W systemie Windows 7/8/10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”**. Po zalogowaniu się jako Administrator należy ustawić poziom zabezpieczenia połączeń z terminalami na „Niski” (jest to najlepszy wariant ustawienia biserwera do pracy podczas uruchamiania systemu) , i nacisnąć „Wprowadź nowe zasady” a następnie zamknąć program biserver.

Ze względu na to, że obecnie komputery wyposażone są nawet w kilka interfejsów (kart) sieciowych, należy przypisać interfejs sieciowy do terminala. Robimy to za pomocą programu narzędziowego biclient. W systemie Windows 7/8/10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”. Po zalogowaniu otwiera się okno, w którym możemy ustawić sposób logowania się do programu bibi.



Wybór potwierdzamy przyciskiem „Zapisz zmiany”.

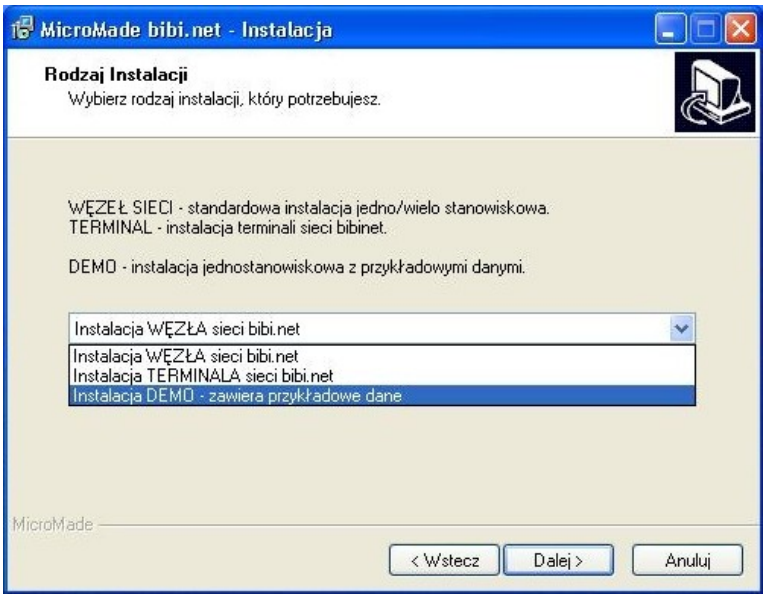
Następnie przechodzimy do kolejnej zakładki naciskając przycisk "Dalej". Zaznaczamy wybór "Przypisz terminal do interfejsu", i wybieramy interfejs sieciowy. Powinien to być interfejs, który zawsze jest włączony w systemie. Najlepiej wybrać kartę sieciową typu Ethernet (standardową). Po wybraniu zamknąć program przyciskiem „Koniec”.



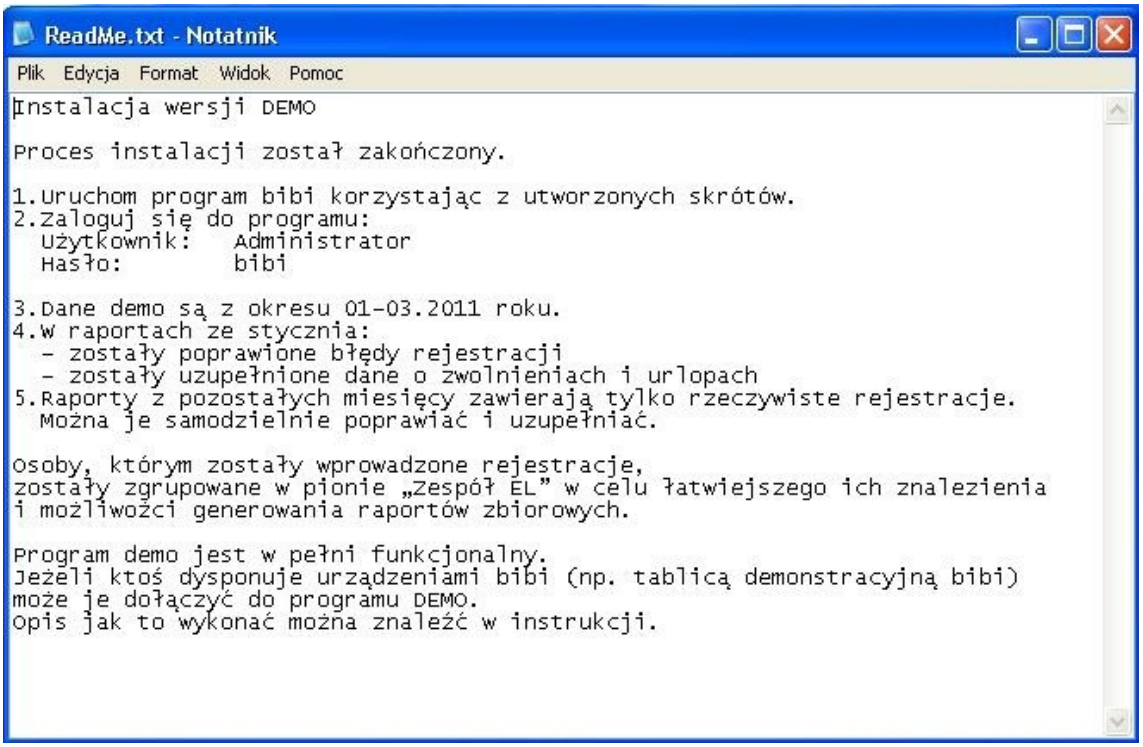
Teraz można zalogować się po raz pierwszy do programu bibi jako Administrator. W programie należy skonfigurować sieć urządzeń bibi (kontrolery, czytniki itp.), zadeklarować wydziały i grupy pracowników, strefy dostępu i obszary zabezpieczone oraz ustawić potrzebne funkcje.

4.3 Instalacja wersji DEMO

Aby zainstalować wersję demonstracyjną programu bibi należy po uruchomieniu instalatora programu (bibinet_setup.exe) wybrać z listy dostępnych instalacji, instalację DEMO.



Program zainstaluje się standardowo, dodatkowo tworząc na dysku bazę danych z przykładowymi danymi. Po zakończeniu instalacji należy przeczytać informację **Readme.txt zawierającą wskazówki jak korzystać z wersji demonstracyjnej programu**.



UWAGA

Przed zainstalowaniem użytkowej (licencjonowanej) wersji programu należy odinstalować program demonstracyjny poleceniem Windows „Dodaj/Usuń programy" a następnie usunąć cały katalog MicroMade z folderu Program Files lub Program Files (x86) (dla systemów 64 bitowych).

5. Konfiguracja urządzeń systemu bibinet

Po wykonaniu instalacji urządzeń (kontrolerów, czytników, terminali ...) i włączeniu zasilania należy je wstępnie skonfigurować programem biSprzetLAN.exe a następnie resztę ustawień wykonać w programie bibi.

UWAGA!!!

W trakcie pracy z programem bibi należy pamiętać, że wiele funkcji dostępnych jest za pomocą podręcznego menu wywoływanego prawym klawiszem myszy.

5.1 Deklaracje wstępne w programie bibi

Zanim przystąpi się do konfigurowania urządzeń należy zadeklarować w programie wydziały i grupy pracowników oraz strefy dostępu, a w nich obszary zabezpieczone.

Ikonką  otworzyć panel sterujący programu bibi. Panel sterujący to obszar z prawej strony ekranu. W górnej części panelu znajduje się okno z oznaczeniem okresu, za który program generować będzie raporty. W dolnej części panelu są 3 zakładki: Grupy, Piony, Obszary.

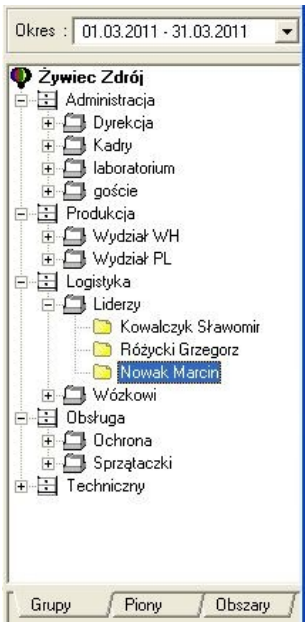
Zakładka grupy zawiera listę pracowników. Są oni podzieleni zgodnie ze strukturą zakładu na wydziały i grupy pracowników. Ten podział jest obowiązkowy w programie bibi.

Dodatkowo niektórzy pracownicy (np. kierownicy, brygadziści) mogą być dodatkowo pogrupowani. Ten podział ma odzwierciedlenie w zakładce Piony. Ten podział nie jest obowiązkowy.

Zakładka Obszary służy to podziału obiektu na strefy dostępu i obszary zabezpieczone. Strefa dostępu to zespół obszarów zabezpieczonych, do których ma dostęp ta sama grupa ludzi. Obszar zabezpieczony to nazwa pomieszczenia (pokoju), hala fabryczna, magazyn itp. Obiekt (zakład pracy) musi mieć zadeklarowaną chociaż jedną strefę dostępu a w niej chociaż jeden obszar zabezpieczony.

5.1.1 Deklaracja wydziałów i grup pracowników.

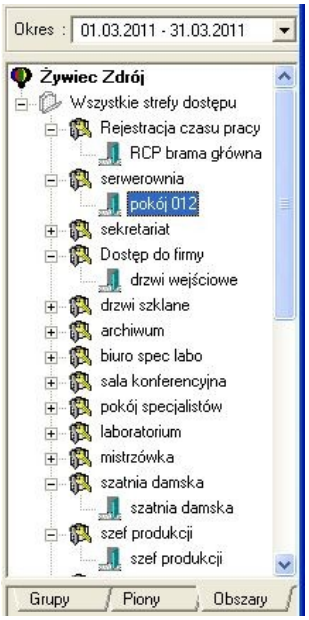
W zakładce Grupy ustawiamy się myszą na nazwie zakładu pracy i z menu kontekstowego (prawy klawisz myszy) wybieramy Dodaj nowy wydział. Ustawiając się na nazwie wydziału dodajemy w sposób analogiczny grupę pracowników. Do grupy dodajemy podobnie pracownika.



W podobny sposób (jeżeli potrzeba) można zdeklarować podział pionowy pracowników w zakładce Piony.

5.1.2 Deklaracja stref dostępu i obszarów zabezpieczonych.

W panelu sterującym wybieramy zakładkę Obszary. Ustawiamy się na napisie Wszystkie strefy dostępu i z menu kontekstowego wybieramy Dodaj nową strefę dostępu. Analogiczne ustawiając się na zadeklarowanej strefie dodajemy do niej obszary zabezpieczone.



Zadeklarowane obszary posłużą do opisania przejść dostępu w kontrolerach (Opcje systemu bibi). W zadeklarowanych strefach dostępu zostaną określone uprawnienia dostępu wydziałów lub grup pracowniczych.

5.1.3 Deklaracja uprawnień stałych kontroli dostępu

Aby wprowadzone do systemu karty mogły rejestrować zdarzenia ewidencji czasu pracy lub otwierać drzwi (kołowroty itp.) trzeba je przydzielić do choćby jednej strefy dostępu. W tym celu należy w zakładce *Obszary* panelu sterującego ustawić się na wybranej strefie dostępu i z menu kontekstowego wybrać *Uprawnienia stał*e. Następnie przejść do zakładki *Grupy* i chwytając wybrany Wydział, Grupę, Pion lub Pracownika przeciągnąć w otwarte okno uprawnień stałych i upuścić.

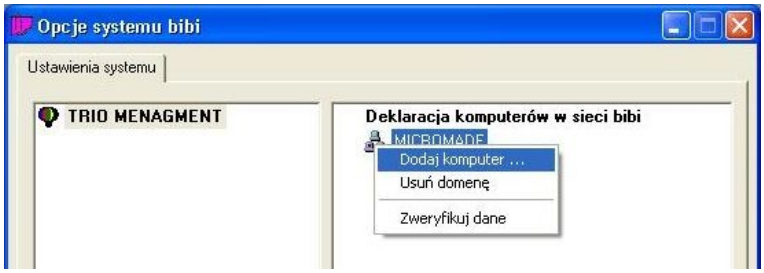
Standardowo przeciągnięta grupa otrzymuje dostęp zawsze. Jeżeli potrzebne są inne schematy czasowe można je zadeklarować wybierając z menu Edycja schematów czasowych.

Jeżeli zadeklarujemy dostęp dla Grupy, Wydziału czy całego Zakładu Pracy, to wówczas każda karta wydana do tej grupy nabiera automatycznie uprawnienia dostępu tej grupy. Jest to najwygodniejszy sposób deklarowania uprawnień dostępu.

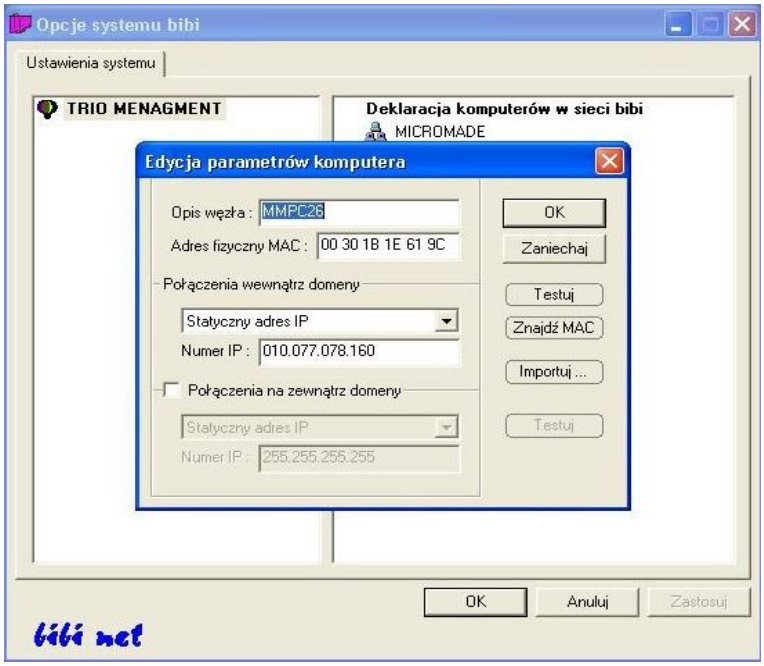
5.1.4 Deklaracja komputerów w systemie bibinet

System bibinet wymaga dokładnego zdefiniowania komputera (komputerów), na których zainstalowane jest oprogramowanie bibi.net. Podstawowym elementem tej deklaracji, jest zadeklarowanie komputera – węzła sieci bibi.net, do którego podłączone są urządzenia systemu. Należy pamiętać, że komputer ten powinien mieć stały numer IP lub mieć zdefiniowaną nazwę w serwerze DNS.

Ikonką  lub z menu Konfiguracja – Opcje systemu otworzyć okno Opcje systemu bibi. Ustawić się w prawej części okna na napisie Deklaracja komputerów w sieci bibi i z menu kontekstowego wybrać Dodaj domenę. Jeżeli komputer podłączony jest do lokalnej sieci komputerowej to nazwa domeny zostanie wstawiona automatycznie.



następnie ustawić się na ikonce domeny  i klikając prawym klawiszem myszy dodać komputer. Jego parametry powinny podstawić się automatycznie. Po zatwierdzeniu nazwa komputera powinna pokazać się pod nazwą domeny.



Do tak zdefiniowanego węzła można dodawać kontrolery bibi-K22 i bibi-K25 lub rejestratory czasu pracy.

Deklaracja komputerów – terminali i dodatkowych węzłów opisana jest w dalszej części instrukcji.

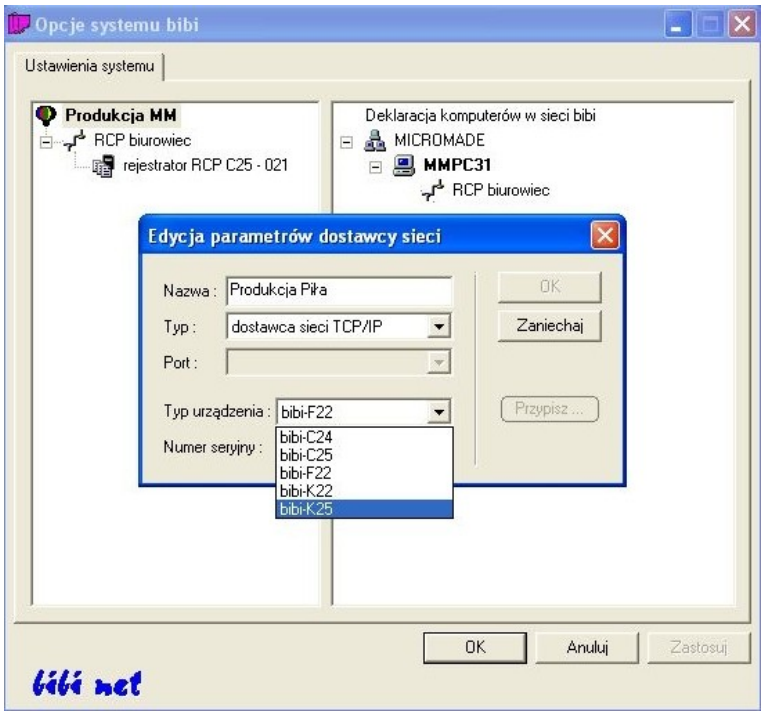
5.2 Konfiguracja kontrolerów bibi-K22 i bibi-K25

Kontrolery bibi-K22 i bibi-K25 powinny być wstępnie skonfigurowane przez instalatora montującego urządzenia na obiekcie przy pomocy programu **biSprzetLAN.exe** . Tak przygotowane kontrolery można dopiero przypisać do instalacji i skonfigurować programem bibi.

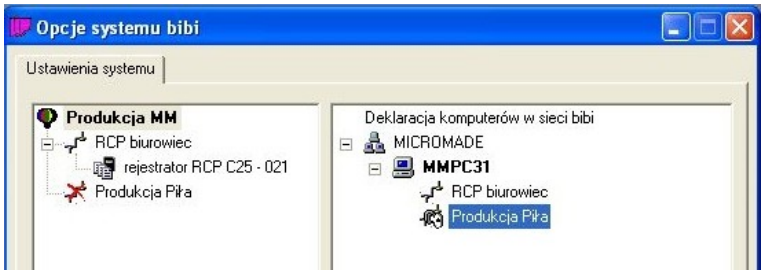
5.2.1 Przypisanie kontrolerów do instalacji

Kontrolery powinny mieć podłączone zasilanie i być połączony z siecią Ethernet z protokołem TCP/IP.

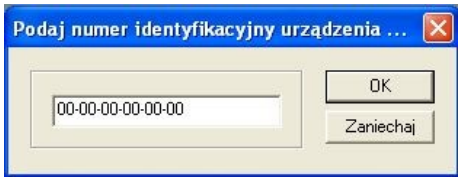
Przypisanie kontrolera do systemu odbywa się w prosty sposób w programie bibi. Po otwarciu okna Opcje systemu bibi klikamy prawym klawiszem myszy na nazwie komputera – węzła sieci bibinet i z menu wybieramy funkcję dodaj dostawcę.



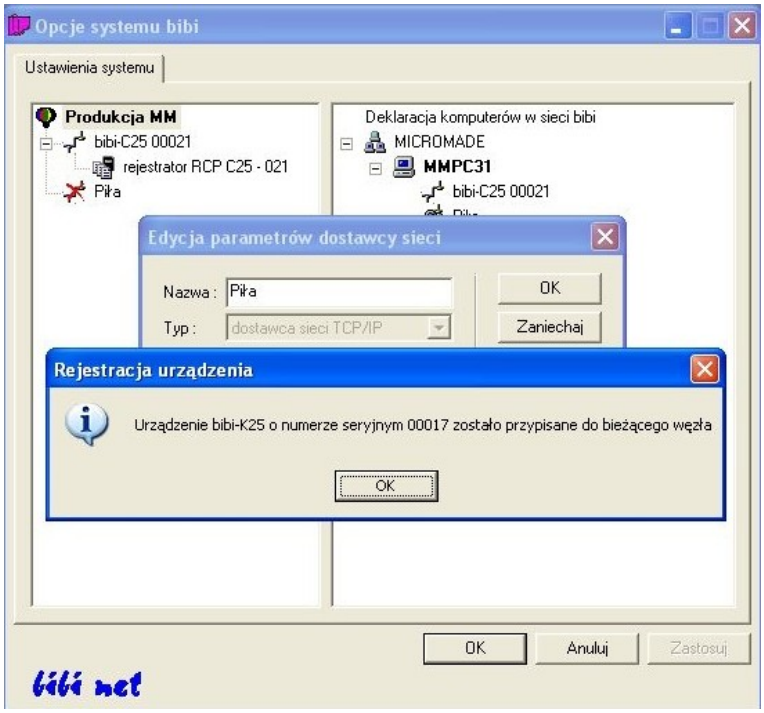
Wpisujemy nazwę (np. miejsce w którym jest umieszczony interfejs) i wybieramy typ dostawca sieci TCP/IP. Ustawiamy typie kontrolera i wpisujemy jego numer seryjny, a następnie wciskamy klawisz OK. Na liście Deklaracje komputerów w sieci bibi pojawi się pod wybranym węzłem zadeklarowana nazwa tego kontrolera.



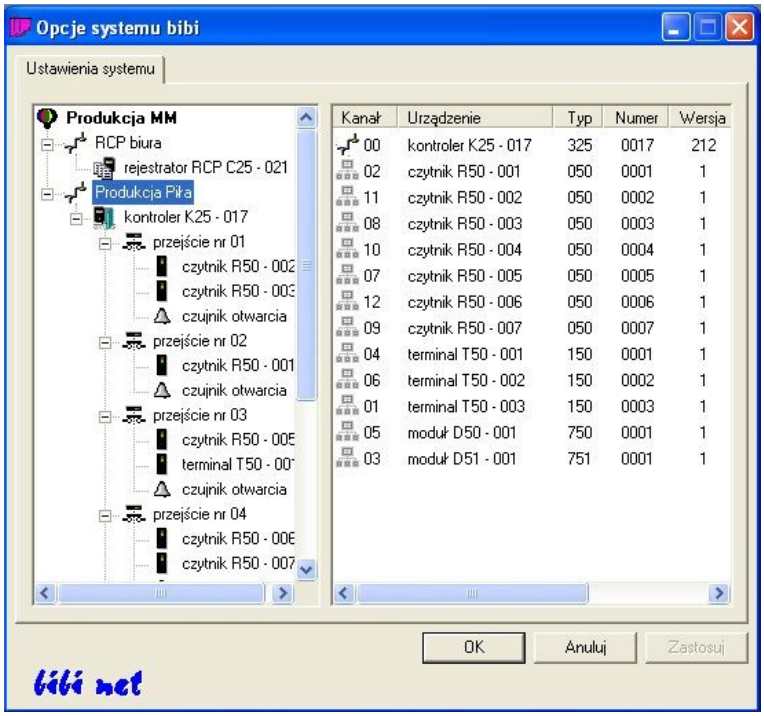
Należy jeszcze raz kliknąć na tej nazwie i w otwartym oknie Edycja parametrów dostawcy sieci wcisnąć klawisz Przypisz.



W otwartym oknie wpisujemy numer identyfikacyjny interfejsu. Numer ten można znaleźć na tylnej ściance obudowy kontrolera lub na naklejce przyklejonej do arkusza identyfikacyjnego znajdującego się wewnątrz opakowania kontrolera.



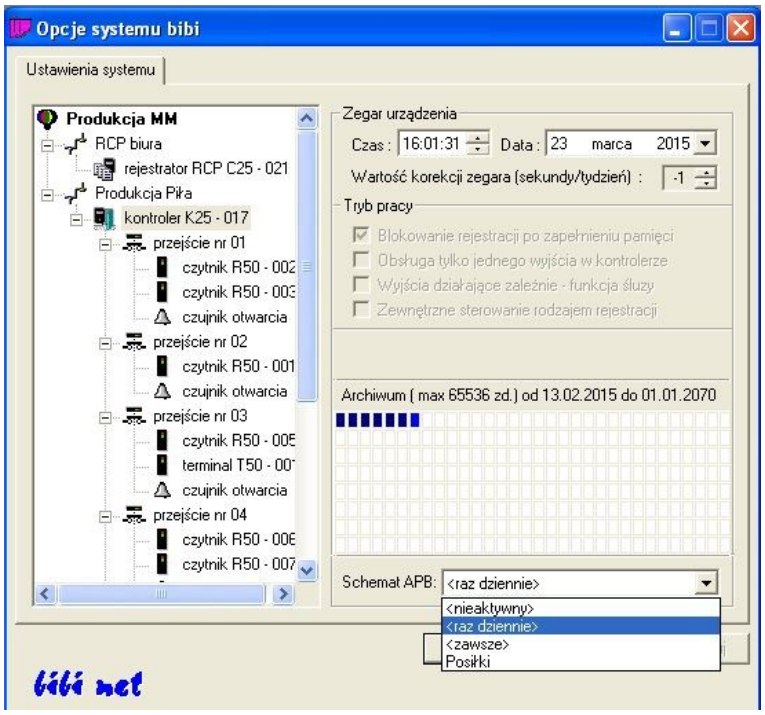
Po potwierdzeniu operacji program nawiąże komunikację z interfejsem samoczynnie. W lewej stronie okna Opcje systemu bibi pojawi się struktura drzewiasta urządzeń (kontrolerów, rejestratorów) i podłączonych do nich czytników i terminali zgodnie z deklaracją wykonaną przy pomocy programu biSprzetLAN.



Wszystkie opisane będą swoimi numerami fabrycznymi. Przy ich konfiguracji bardzo przydatne mogą okazać się wypełnione karty ewidencyjne kontrolerów. Poprawnie wypełnione zawierają informacje o miejscu zamontowania czytników i terminali.
Korzystając z tych informacji i z deklaracji poczynionych wcześniej szybko można skonfigurować podłączone do systemu kontrolery.

5.2.2 Ustawienie anty pass back'u

W otwartym oknie Opcje systemu bibi kliknąć na wybranym kontrolerze. Z prawej strony okna kontroler wyswietli swój aktualny czas i datę. Czas jest synchronizowany z internetowymi wzorcami czasu SNTP lub z lokalnym serwerem czasu ustawionym przez stronę www urządzenia. Jeżeli kontroler nie może zsynchronizować czasu z wzorcami czasu, wówczas pobiera go z komputera zarządzającego systemem (węzła systemu bibinet).



Jeżeli na przejściach podłączonych do kontrolera ma być wykorzystywana funkcja AntyPassBack'u to w oknie **Schemat APB** wybieramy schemat wg jakiego ma działać ta funkcja:

- <nieaktywny> - funkcja APB jest wyłączona (ustawienie standardowe)
- <raz dziennie> - blokada APB kasowana jest o północy
- <zawsze> - zawsze po wejściu możliwe będzie tylko wyjście z obszaru (nie można dwa pod rząd wejść do obszaru)
- Posiłki – przykładowy zdefiniowany schemat czasowy (np. wejście po posiłek na stołówkę tylko raz podczas swojej zmiany), blokada jest aktywna tylko wg zdefiniowanego schematu czasowego (max 4 razy w ciągu doby).

Wybór przejścia, na którym ma być aktywna funkcja AntyPassBack'u następuje podczas konfiguracji tego przejścia.

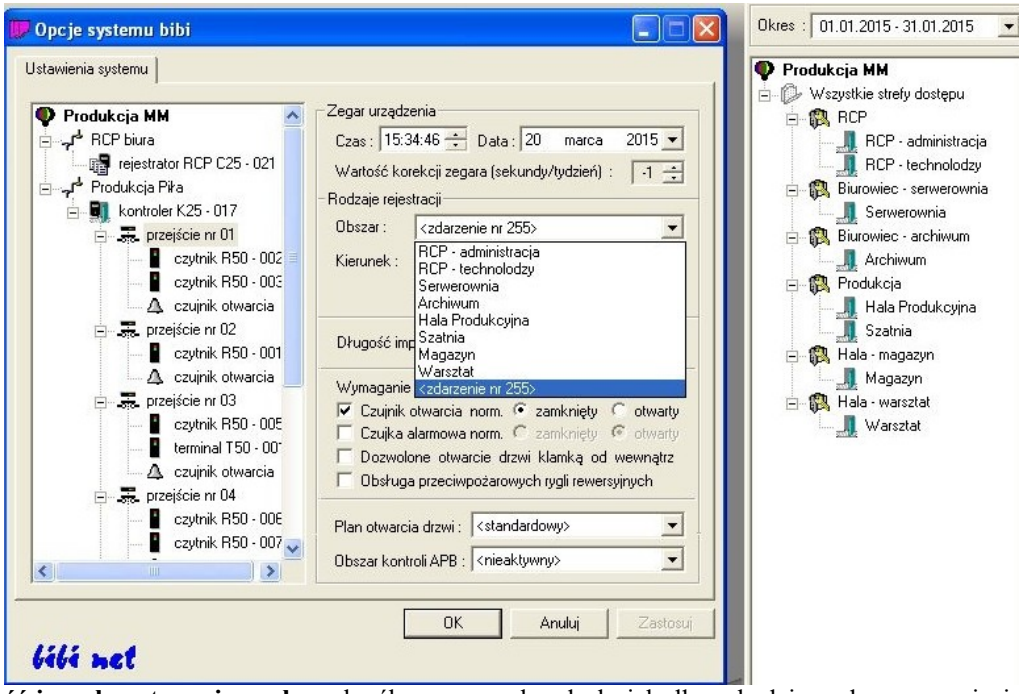
5.2.3 Konfiguracja przejścia zarządzanego przez kontroler

Kontroler zarządza przejściami przy pomocy własnych wyjść przekaźnikowych lub przy pomocy wyjść w podłączonych do niego terminalach lub modułach rozszerzeń (tylko w przypadku kontrolera **bibi-K25**). Wstępna konfiguracja tych urządzeń wykonywana jest za pomocą oprogramowania biSprzetLAN.

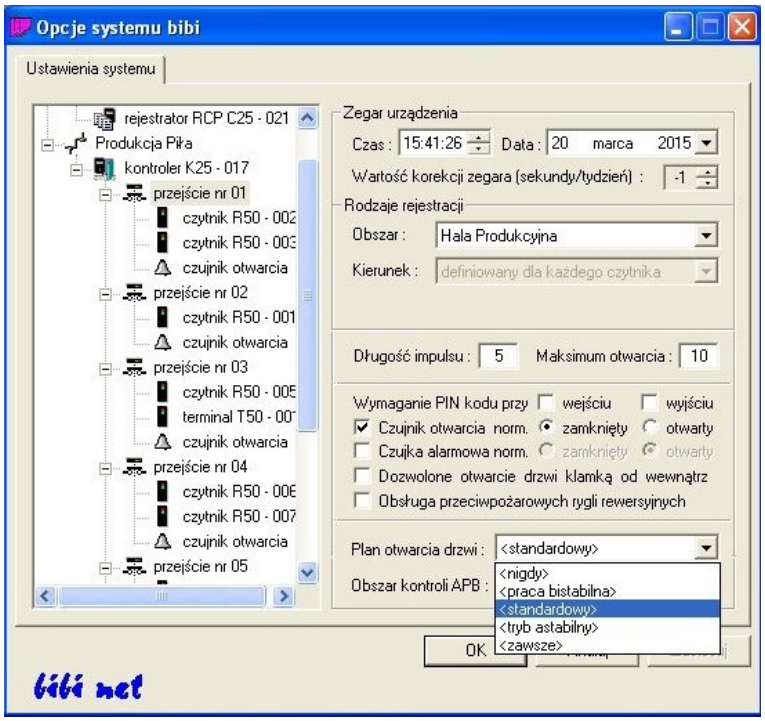
Ostateczną konfigurację wykonuje się w programie bibi w zakładce Opcje systemu bibi. Klikając prawym klawiszem myszy na **przejście nr...** pod nazwą kontrolera możemy zmienić opis przejścia (rygla) np. na „Pokój nr 325”.

Po prawej stronie okna możemy poza tym zdefiniować:

- **Obszar** - Należy wybrać obszar zabezpieczony, do którego prowadzi to przejście. Obszary muszą być wcześniej zdefiniowane w zakładce „Obszary” bocznego panelu sterującego. Obszar zabezpieczony to jedno lub kilka pomieszczeń, do którego prowadzą przejścia kontrolowane. W przypadku kontroli dostępu, obszar zabezpieczony jest przeważnie rzeczywistym obszarem - np. magazyn. Jeżeli przejście pełni tylko rolę rejestracji czasu pracy, obszar może być wirtualny - np. RCP.



- **Długość impulsu otwarcia rygla** - określa czas w sekundach, jak długo będzie podawane napięcie otwierające rygiel po zbliżeniu uprawnionej karty lub przyciśnięciu przycisku wyjścia. Można ustawić czas od 1 do 63 sekund. Napięcie będzie wyłączone po tym czasie, lub natychmiast po otwarciu drzwi jeżeli na przejściu zamontowany jest kontaktronowy czujnik otwarcia drzwi. Ustawienie czasu 0 spowoduje, że rygiel w ogóle nie będzie otwierany (typowe ustawienie dla RCP).
- **Dozwolony maksymalny czas otwarcia drzwi** - określa czas w sekundach, jak długo mogą być otwarte drzwi po uprawnionym otwarciu. Można ustawić czas od 1 do 63 sekund. Jeżeli drzwi nie zostaną w tym czasie zamknięte, zostanie zgłoszony alarm.
- **Czujnik otwarcia** - flagę tą należy zaznaczyć, jeżeli zamontowano czujnik otwarcia drzwi
  - **norm. zamknięty / otwarty** - należy określić, w jakim stanie pozostaje czujnik przy drzwiach zamkniętych. Typowo, przy czujnikach magnetycznych (kontaktronach), jest on normalnie zamknięty.
- **Czujka alarmowa** - flagę tą należy zaznaczyć, jeżeli podłączono czujkę alarmową do wejścia zdefiniowanego dla tego przejścia
  - **norm. zamknięty / otwarty** - należy określić, w jakim stanie pozostaje czujka w stanie nieaktywnym.
- **Dozwolone otwarcie drzwi klamką od wewnątrz** - tą flagę należy zaznaczyć, jeżeli wewnątrz pomieszczenia nie zamontowano czytnika kart ani przycisku wyjścia, a wyjście z pomieszczenia następuje poprzez normalne otwarcie drzwi klamką. Nie jest to zalecana konfiguracja, gdyż system nie może rozpoznać wyłamania drzwi od zewnątrz.
- **Obsługa przeciwpożarowych rygli rewersyjnych** – zaznaczenie tej flagi powoduje, że nie jest kasowany sygnał otwierający rygiel elektromagnetyczny po otwarciu drzwi. Stosuje się to zaznaczenie, jeżeli na tym przejściu zastosowano np. zworę elektromagnetyczną z wbudowanym czujnikiem otwarcia drzwi. Wówczas napięcie ze zwory zdejmowane jest na czas ustawiony w ramce *Długość impulsu*.
  W przypadku nie zaznaczenia tej flagi sygnał podawany na rygiel jest kasowany w momencie naruszenia czujnika otwarcia drzwi. To rozwiązanie stosuje się najczęściej przy sterowaniu ryglami w kołowrotach.
- **Plan otwarcia drzwi** - określa schemat czasowy, kiedy drzwi mają być otwarte na stałe. Jest to wykorzystywane w biurach, gdzie w ciągu dnia przychodzą interesanci - w uprawnionym czasie drzwi są wtedy otwarte. W pozostałych godzinach drzwi mogą otworzyć tylko uprawnione osoby. Można wybrać ze schematów określonych przez producenta, lub wstawić dowolny zdefiniowany schemat czasowy.
  - **<standardowy>** - ustawienie najbardziej typowe, otwarcie drzwi następuje tylko poprzez uprawnione karty lub przyciskiem wyjścia
  - **<nigdy>** - ten schemat zabrania otwarcia drzwi nawet przez osoby uprawnione (awaryjne zamknięcie obszaru chronionego), powoduje też brak rejestracji RCP.
  - **<praca bistabilna>** - przy tym schemacie kolejne użycie uprawnionej karty powoduje na przemian otwarcie/zamknięcie drzwi (włączenie/wyłączenie urządzenia)



- **<tryb astabilny>** - to jest schemat przeznaczony do sterowania urządzeń. Zbliżenie karty do czytnika powoduje aktywowanie wyjścia, zabranie karty wyłącza wyjście.
- **<zawsze>** - ten schemat otwiera drzwi na stałe
- **dni robocze 7-15** – (przykładowy schemat czasowy) ten lub dowolny inny zdefiniowany schemat czasowy spowoduje otwarcie drzwi na stałe w określonych dniach i godzinach. Poza tymi godzinami otwarcie drzwi może nastąpić uprawnionymi kartami.

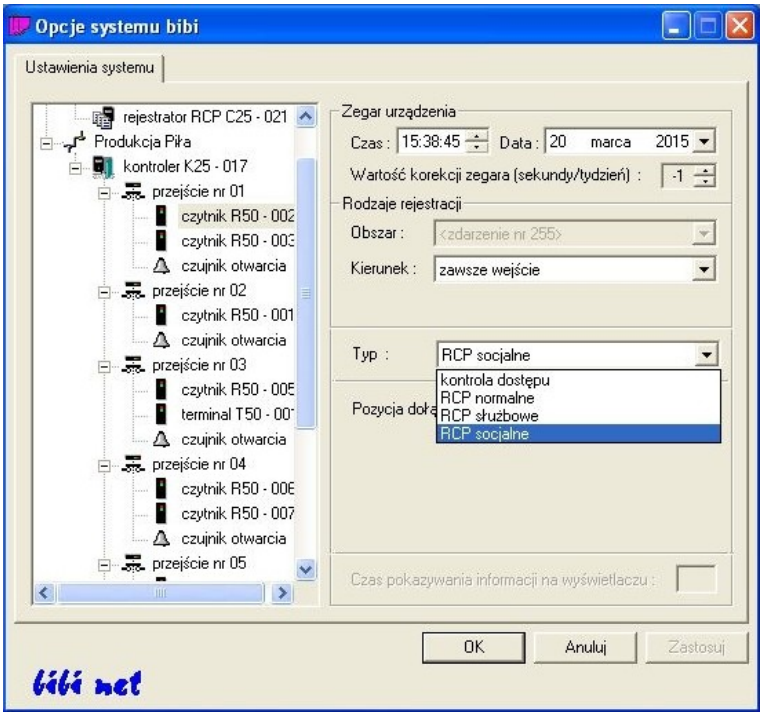
- **Obszar kontroli APB** - określa sposób działania AntyPassBacku.
  - **<nieaktywny>** - AntyPassBack na tym przejściu wyłączony
  - **<lokalny>** - AntyPassBack działa wspólnie na wszystkich przejściach które spełniają warunki:
    - przejścia są obsługiwane przez ten sam kontroler
    - przejścia mają ustawiony ten sam Obszar
    - przejścia mają włączony AntyPassBack - <lokalny>

5.3 Konfiguracja czytników i terminali RFID

Standardowo do każdego przejścia obsługiwanego przez kontroler podłączone są od jednego do czterech czytników lub terminali RFID.

Każdy z nich należy ustawić zgodnie ze swoją wiedzą i zgodnie z zaleceniami inwestora. Do tego celu najlepiej wykorzystać arkusz identyfikacyjny wypełniony podczas montowania czytników (terminali) w obiekcie. Powinien on zwierać informację który czytnik (numer fabryczny naklejony na spodzie obudowy) został powieszony na wejściu do obszaru zabezpieczonego, który na wyjściu. Jakie urządzenie steruje danym ryglem (kołowrotem, bramą itp.). Czy na wybranym przejściu jest podłączony czujnik otwarcia drzwi, przycisk wyjścia, sterowanie CCTV itp. Taki zbiór informacji znacznie ułatwia konfigurację urządzeń systemu, szczególnie w przypadku rozległych instalacji.

Czytniki i terminale (czytniki z tranzystorem otwierającym przejście) są konfigurowane w ten sam sposób w programie bibi. W oknie **Opcje systemu bibi** Należy myszką kliknąć na wybranej nazwie (symbol i numer fabryczny) czytnika/terminala i w prawej części okna dokonać odpowiednich ustawień.



- **Kierunek** - określa, czy rejestracja w czytniku dotyczy wejścia czy wyjścia z danego obszaru. W wypadku rejestracji czasu pracy określa to jednocześnie rozpoczęcie (wejście) lub zakończenie (wyjście) pracy.
- **Typ** - określa, typ rejestracji. Istnieją 4 typy rejestracji:
  - **kontrola dostępu** - rejestracje te nie będą analizowane przy rozliczaniu czasu pracy
  - **RCP normalne** - rejestracje te będą trafiały do rozliczenia czasu pracy, jako normalne wejścia do pracy i wyjścia z pracy
  - **RCP służbowe** - rejestracje z tego czytnika będą traktowane jak zdarzenia służbowe. Aby takie zdarzenie zarejestrować, trzeba mieć indywidualnie przyznane uprawnienie: „Wyjścia służbowe” (w „Edycji Danych Pracowniczych”). Osobom nie posiadające takich uprawnień drzwi nie będą otwarte i zostanie zarejestrowane zdarzenie „brak uprawnień RCP”.
  - **RCP socjalne** - rejestracje z tego czytnika będą traktowane jak wejścia i wyjścia na przerwę. Aby takie zdarzenie zarejestrować, trzeba mieć indywidualnie przyznane uprawnienie: „Wyjścia socjalne” (w „Edycji Danych Pracowniczych”). Osobom nie posiadające takich uprawnień drzwi będą otwarte i zostanie zarejestrowane zdarzenie kontroli dostępu.

5.4 Konfiguracja czytników z ekranem dotykowym LCD

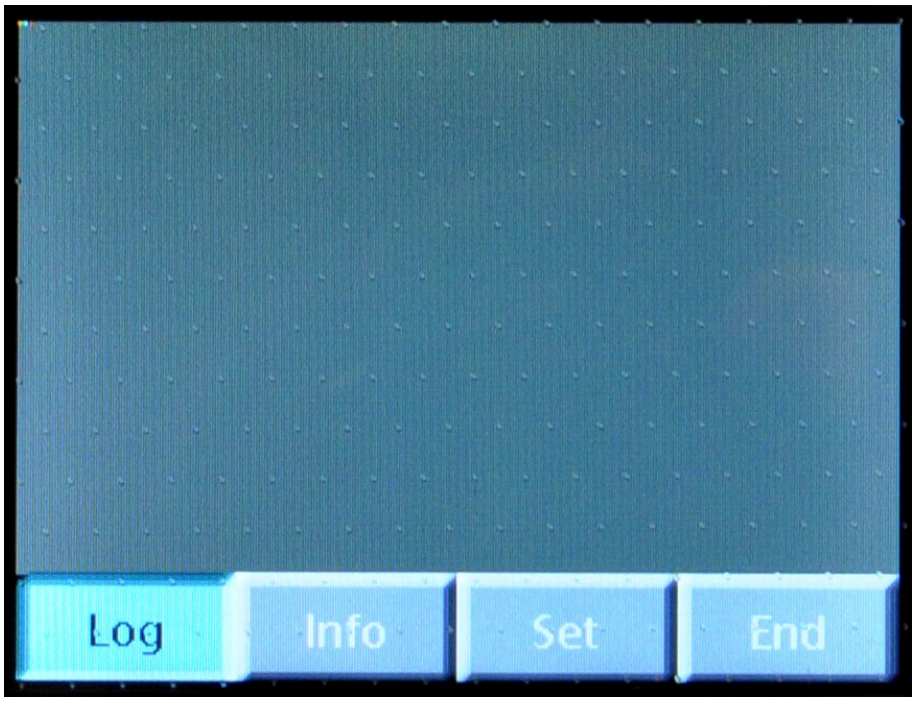
Czytniki z ekranem dotykowym LCD, powinny być, tak jak inne czytniki, przypisane do odpowiednich przejść kontrolera systemu bibinet przy pomocy programu biSprzetLAN.exe .

Pozostałe jego ustawienia:

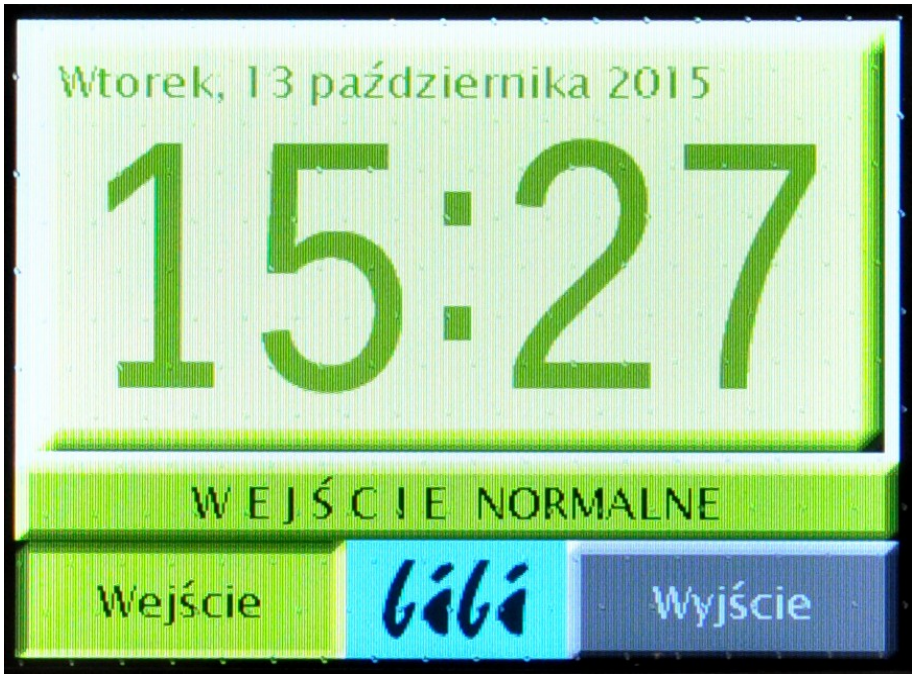
- domyślny rodzaj rejestrowanego zdarzenia
- aktywne klawisze wyboru zdarzenia
- język komend wyświetlanych na ekranie
- godzinę, o której czytnik może przełaczac się z rejestracji wejścia na rejestrację wyjścia
- itp.

wykonuje się przy pomocy menu instalatora na ekranie dotykowym czytnika.

Po pierwszym podłączeniu czytnika standardowo na ekranie LCD pojawi się ekran menu instalatora.

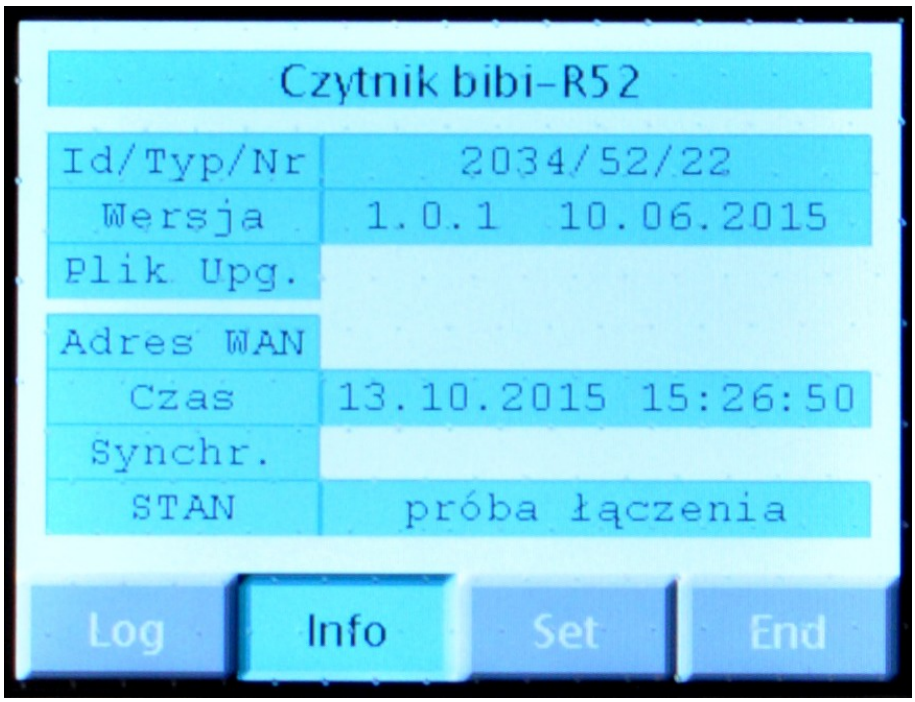


Jeżeli na ekranie wyświetlany jest standardowy obraz z zegarem czasu rzeczywistego

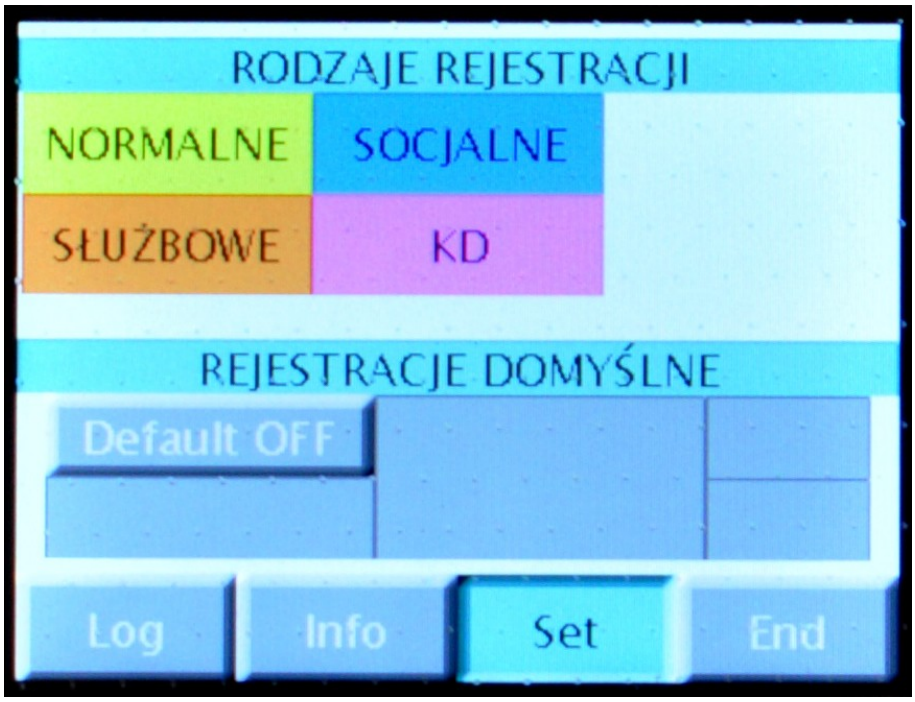


należy odłączyć zasilanie czytnika i po ponownym włączeniu w ciągu 10 sekund nacisnąć ekran dotykowy – na ekranie pojawi się ekran z menu instalatora.

Po włączeniu klawisz info pokaże się informacja o numerze czytnika i wersji jego oprogramowania.

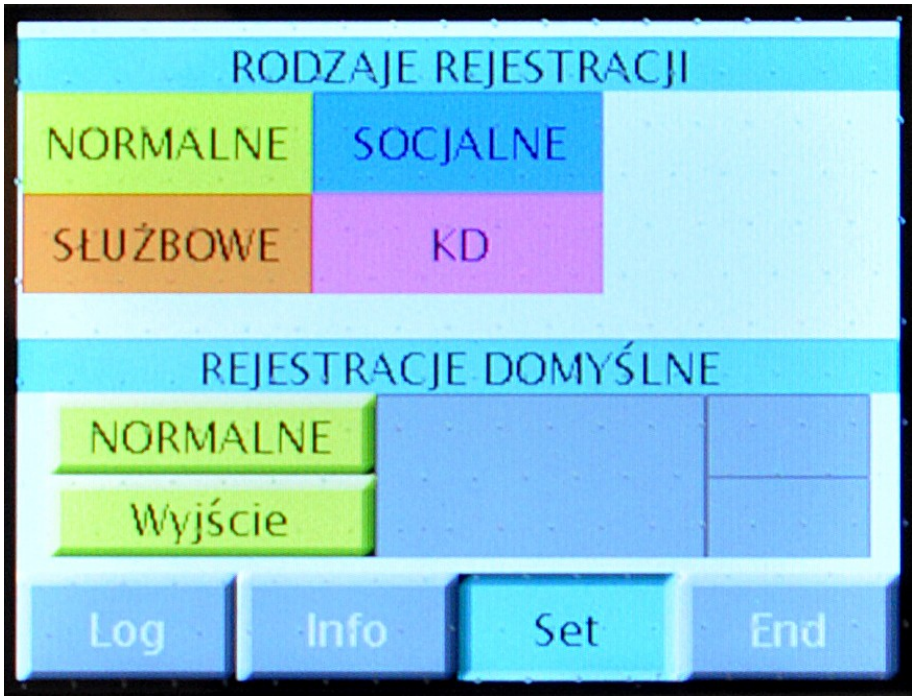


W zakładce **Set** możemy ustawić rodzaje zdarzeń, które ma rejestrować czytnik.. Aby wyłączyć rodzaj zdarzenia należy przycisnąć odpowiadający mu klawisz tak, aby zrobił się szary. Ponowne naciśnięcie uaktywnia go.

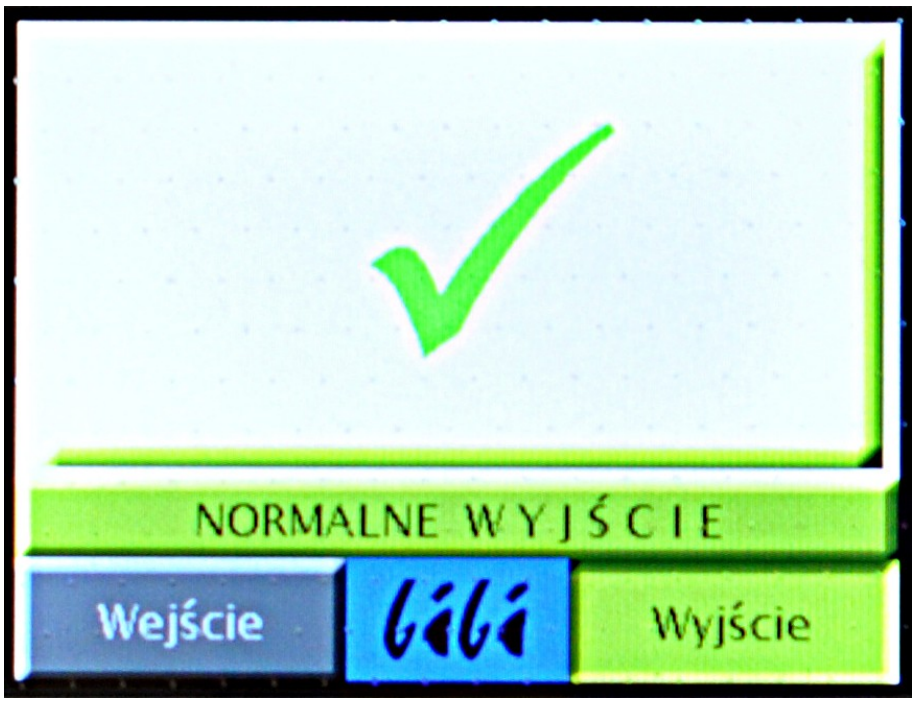


Ustawione jako aktywne klawisze rodzajów rejestracji będą dostępne podczas normalnej pracy czytnika pod klawiszem **bibi.**

W dolnej części zakładki Set ustawić można domyślny rodzaj zdarzenia, które ma rejestrować czytnik. Jeżeli cała dolna część jest szara (Deafult OFF), wówczas czytnik nie ma ustawionego żadnego domyślnego rodzaju rejestracji – wybiera się go przyciskami dostępnymi na ekranie dotykowym. Po przyciśnięciu klawisza Deafult OFF możliwe jest wybranie rodzaju i kierunku domyślnego zdarzenia jakie ma rejestrować czytnik.

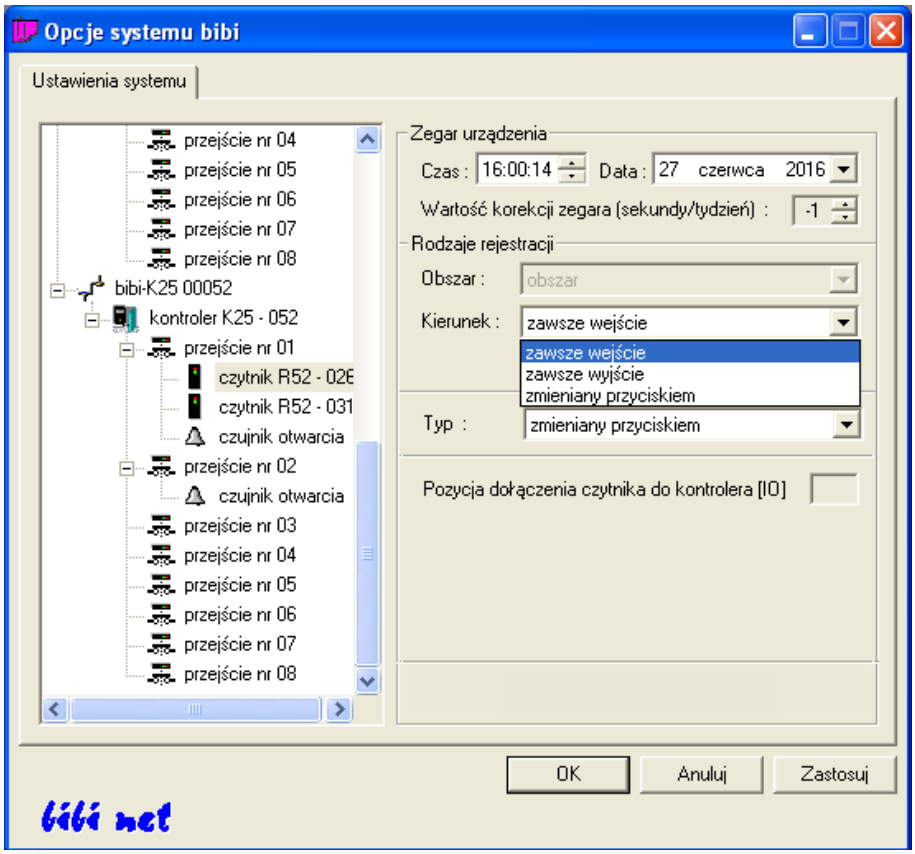


Np. takie ustawienie jak wyżej spowoduje, że czytnik będzie domyślnie rejestrował normalne wyjścia RCP (rejestracji czasu pracy).

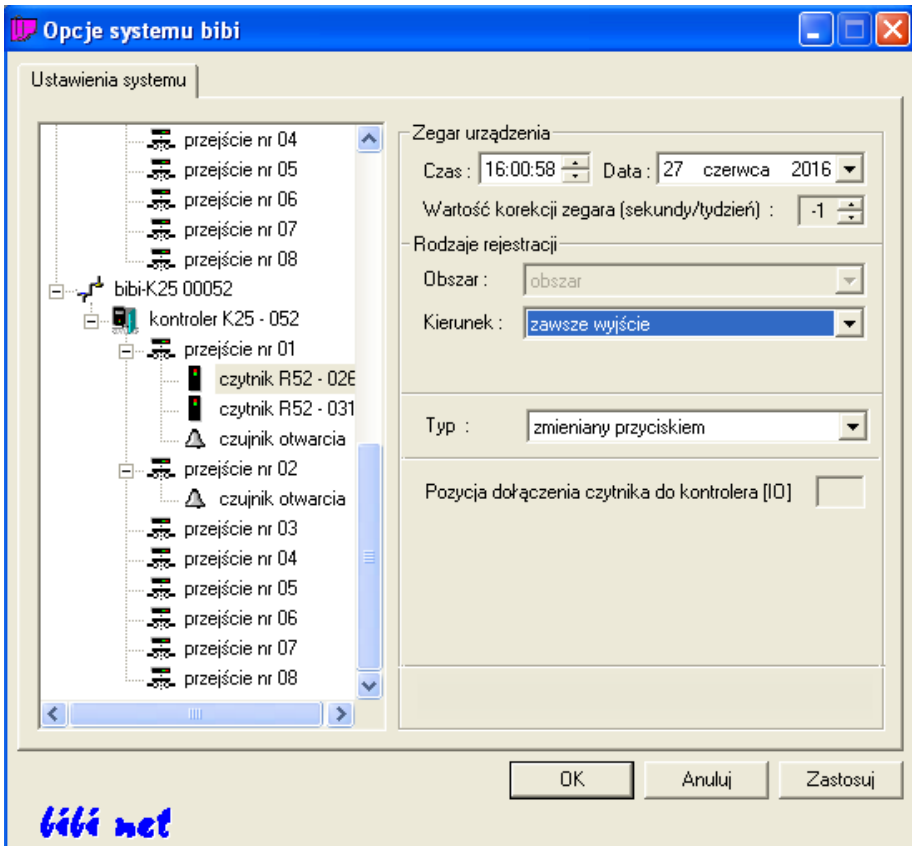


W dowolnym momencie użytkownik może zarejestrować inny rodzaj zdarzenia ale po takiej rejestracji czytnik zawsze wróci do ustawienia domyślnego.

Jeżeli chcemy, aby użytkownik nie miał możliwości zmiany kierunku rejestracji, to taka blokada możliwa jest tylko z poziomu programu komputerowego bibi.



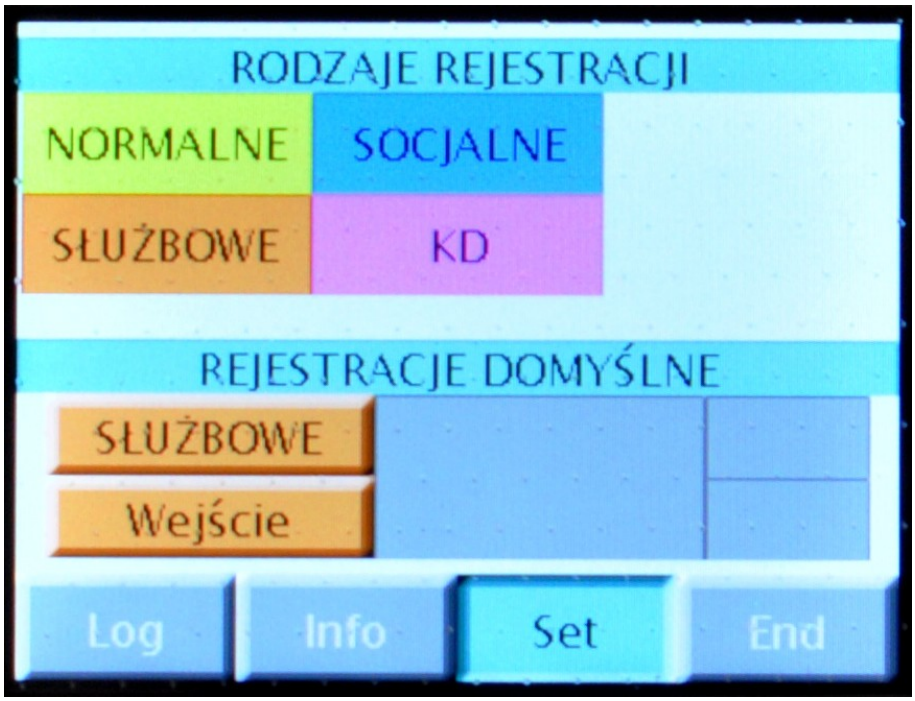
Standardowe ustawienie czytnika w programie bibi to pole kierunek usttawione na *zmieniany przyciskiem* oraz typ rejestracji na *zmieniany przyciskiem.* Jeżeli chcemy zablokować zmianę kierunku rejestracji wówczas musimy zmienić wybór w polu Kierunek.



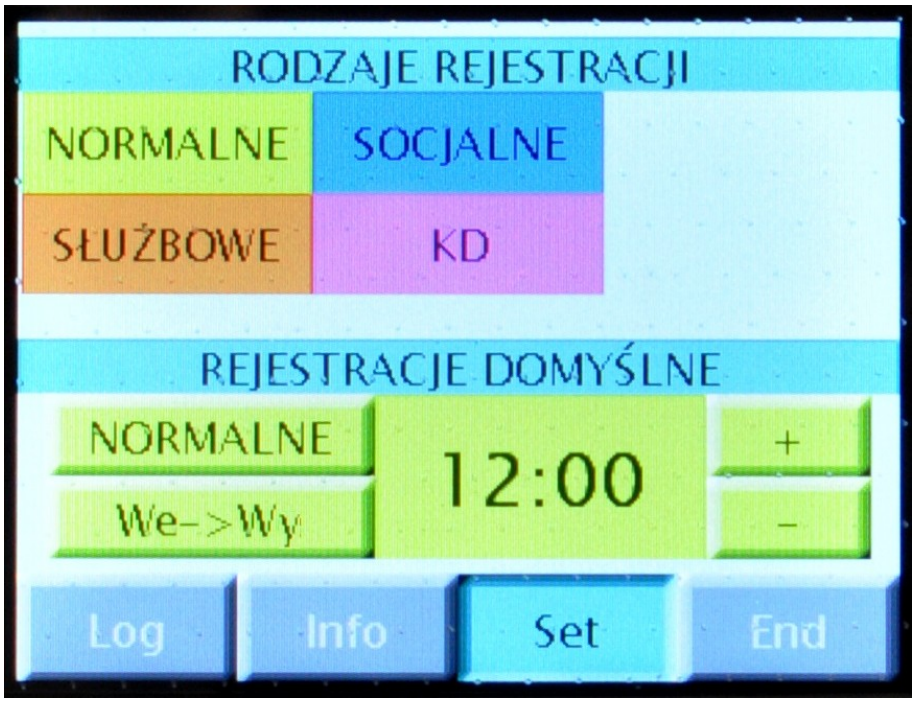
Ustawiając w programie bibi zamiast standardowego ustawienia kierunku: *zmieniany przyciskiem* na np. *tylko wyjście*, kalwisz *Wejście* na ekranie czytnika jest nieaktywny.

Jeżeli chcemy aby np. czytnik rejestrował tylko wejścia służbowe

To wówczas należy ustawić czytnik w następujący sposób:



Można też ustawić czytnik tak, aby o wyznaczonej godzinie sam przestawiał się z rejestracji wejść na rejestrację wyjść z pracy.



Godzinę przełączania ustawia się przyciskami „+” i „-”. Powrotna zmiana rejestracji następuje o północy.

Takie ustawienie czytnika przydatne jest w jednozmianowych systemach pracy (np. w urzędach, biurach, przedszkolach itp.)

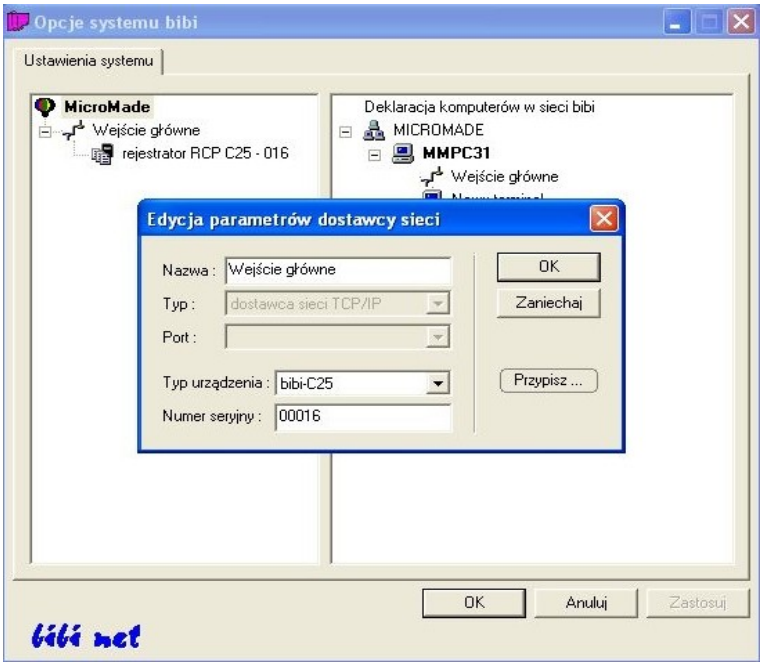
5.5 Konfiguracja rejestratorów czasu pracy

Rejestratory RCP najpierw podłączamy do sieci komputerowej Ethernet (dokładny opis znajduje się w instrukcji obsługi rejestratora) a następnie przystępujemy do ich konfiguracji w programie bibi.

5.5.1 Przypisanie rejestratora do instalacji

Powiązanie z instalacją wykonujemy poprzez przypisanie rejestratora do konkretnego węzła w instalacji. Należy wybrać taki węzeł, który będzie stosunkowo często włączony (najlepiej na stałe np. komputer w serwerowni), tak aby dane z rejestratora zawsze spływały on-line do systemu bibinet.

Po otwarciu okna *Opcje systemu bibi* klikamy prawym klawiszem myszy na nazwie komputera – węzła sieci bibinet i z menu wybieramy funkcję dodaj dostawcę.

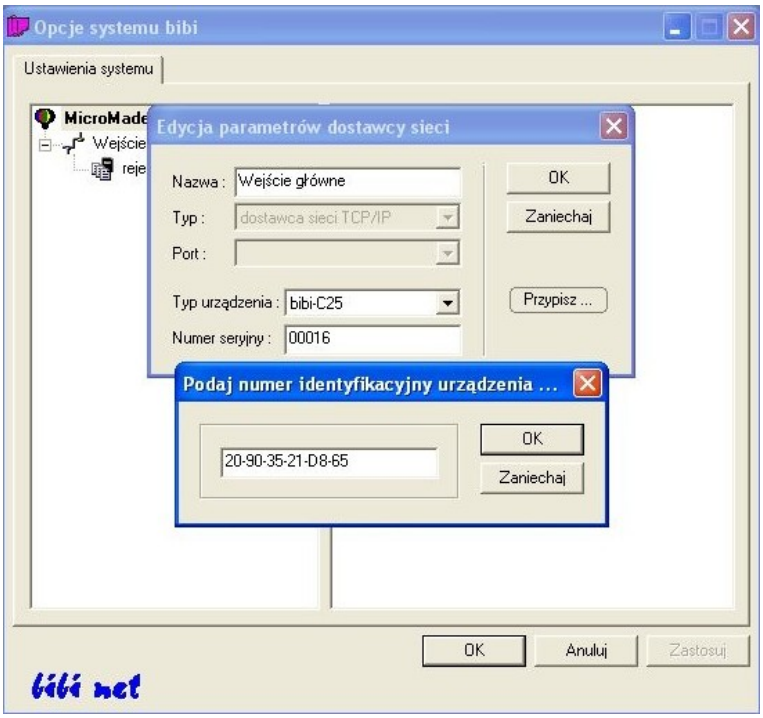


W otwartym okienku podajemy parametry:

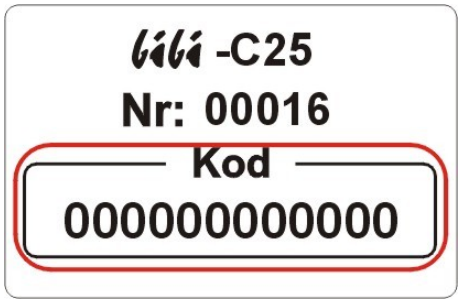
- Typ - dostawca sieci TCP/IP (wybieramy z listy)
- Typ urządzenia - **bibi-C25** (wybieramy z listy)
- Numer seryjny - numer ten można znaleźć na naklejce z tyłu urządzenia
- Nazwa - domyślna nazwa **bibi-C25 numer** zostanie automatycznie utworzona po podaniu numeru urządzenia. Nazwę możemy zmienić na dowolną, np. wskazującą na lokalizację tego rejestratora.

Po naciśnięciu klawisza [OK] urządzenie zostanie podpięte pod węzeł w oknie *Opcje systemu bibi*. Ponownie otwieramy okienko edycji parametrów dostawcy sieci poprzez kliknięcie na nazwie rejestratora.

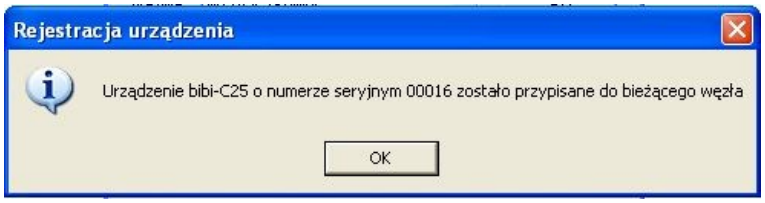
W otwartym okienku naciskamy klawisz *Przypisz...*. Otworzy się kolejne okienko, w którym należy wpisać numer identyfikacyjny czyli kod danego rejestratora.



Kod ten możemy znaleźć na naklejce umieszczonej wewnątrz urządzenia na tylnej ściance. Druga identyczna naklejka jest umieszczona na karcie gwarancyjnej rejestratora.



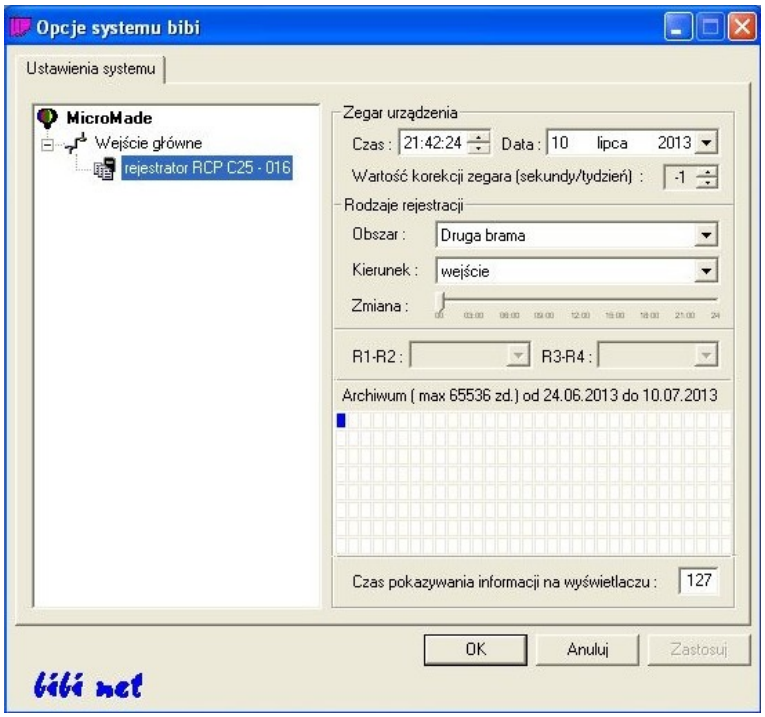
Wpisany kod należy zatwierdzić klawiszem [OK]. Jeżeli kod jest prawidłowy program zarejestruje urządzenie, co potwierdzi odpowiednim komunikatem.



Proces powiązania interfejsu do danej instalacji został zakończony.

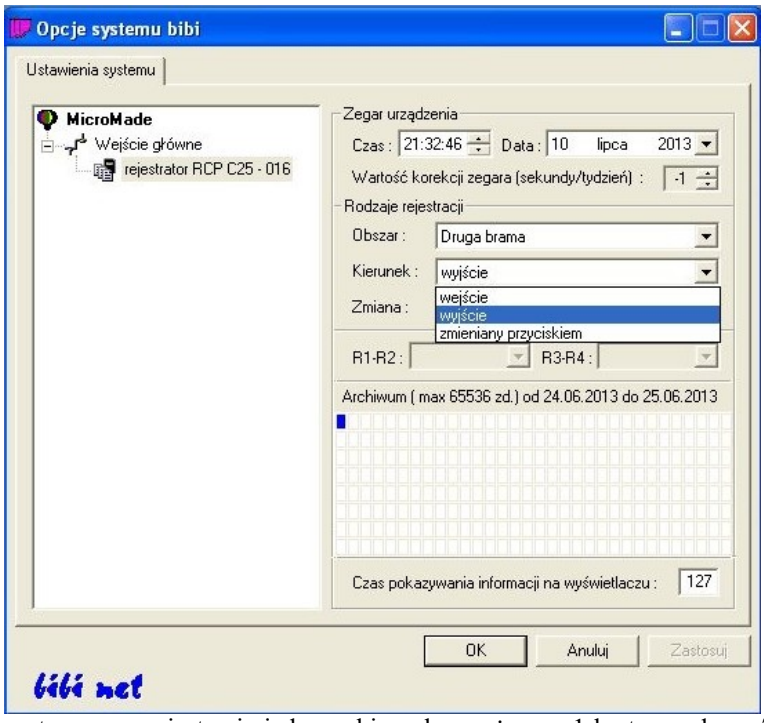
5.5.2 Ustawienie parametrów pracy rejestratora

Po przypisaniu rejestratora do instalacji należy ustawić jego sposób działania. W tym celu należy kliknąć myszką z lewej strony okna Opcje systemu bibi na wybranym rejestratorze.



Następnie wybrać wcześniej zadeklarowany w zakładce *Obszary Panela Sterującego* programu *Obszar***,** przy którym chcemy rejestrować czas pracy pracowników. Wówczas pracownicy, którzy mają uprawnienia dostępu do *Strefy dostępu* obejmującej ten obszar będą mogli rejestrować się na wybranym rejestratorze.

Ustalamy kierunek zdarzenia, które ma być rejestrowane standardowo na rejestratorze. Do rejestracji czasu pracy małej liczby osób można ustawić opcję *zmieniany przyciskiem*. Przy dużej liczbie pracowników lepiej powiesić dwa rejestratory na przejściu i ustawić tak, aby jeden rejestrował tylko wejścia a drugi tylko wyjścia. Zwiększy to znacznie przepustowość takiego przejścia.



Rejestrator ustawiony na sztywno na rejestrację jednego kierunku można na 1 kartę przełączyć w celu zarejestrowania przeciwnego kierunku zdarzenia. Jeżeli karta nie zostanie zbliżona w ciągu 10 sekund rejestrator wróci do poprzedniego ustawienia rejestracji.

Można też suwakiem *Zmiana* ustawić godzinę, w której rejestrator sam automatycznie będzie zmieniał kierunek rejestracji z wejścia na wyjście. Aby ustawienie suwaka nie miało wpływu na konfigurację rejestratora należy ustawić go w skrajne lewe położenie (godzina 0). Jest to szczególnie przydatne przy jednozmianowym charakterze pracy w biurach, szkołach, urzędach itp.

5.6 Instalacja i konfiguracja czytnika administratora systemu

Obecnie w ofercie są dostępne dwa czytniki administratora systemu bibinet:

- bibi-A40, przeznaczony do wprowadzania do systemu kart Unique 125kHz
- bibi-A50, przeznaczony do wprowadzania kart Mifare 13,56 MHz

Po instalacji programu bibi na serwerze (węźle systemu) lub na terminalu, wystarczy czytnik podłączyć do dowolnego gniazda USB komputera. Po zainstalowaniu się sterownika urządzenia czytnik jest gotowy do pracy (nie wymaga żadnej konfiguracji). Sterownik czytnika (WinUSB) jest wbudowany w system Windows (od 7 w zwyż).

Jeżeli system Windows nie znajdzie odpowiedniego sterownika należy zainstalować sterownik dostępny w katalogu: C:\Program Files (x86)\MicroMade\bibinet\drv\MmUsbDrv lub pobrac go ze strony producenta www.micromade.pl.

5.7 Wyświetlacze czasu systemowego

Na przejściach (szczególnie z ewidencją czasu pracy – RCP) zbudowanych w oparciu o czytniki bez wyświetlaczy (np. **bibi-R40**, **bibi-R50**) lub terminale (**bibi-T40**, **bibi-T50**) wskazane jest zastosowanie wyświetlaczy czasu rzeczywistego kontrolera. Wyświetlacze (np. **bibi-D50**) podłączane są do magistrali bibiBUS (RS485) kontrolerów. Wyświetlacze te nie wymagają żadnej dodatkowej konfiguracji w programie bibi.

6. Dodatki

6.1 Podgląd raportów pracowniczych przez przeglądarkę internetową

Podgląd raportów dla pracowników przez przeglądarkę internetową jest dostępny dla użytkowników systemu, których oprogramowanie oparte jest na licencji bibi.50, bibi.150, bibi.500 lub bibi.XL z wykupioną opcją dodatkową. Opłata za tą opcję jest pobierana w postaci rocznego abonamentu.

Przy zakupie tej opcji należy podać numer IP komputera – węzła sieci bibinet z którego pobierane będą dane do podglądu lub jego nazwę w sieci (np. www.micromade.pl/raporty). Na tej podstawie MicroMade przygotowuje i przesyła do zainteresowanej firmy 3 pliki niezbędne do zainstalowania bezpiecznego certyfikatu SSL zabezpieczającego poufność udostępnianych danych.

6.1.1 Konfiguracja serwera do podglądu danych przez przeglądarkę www

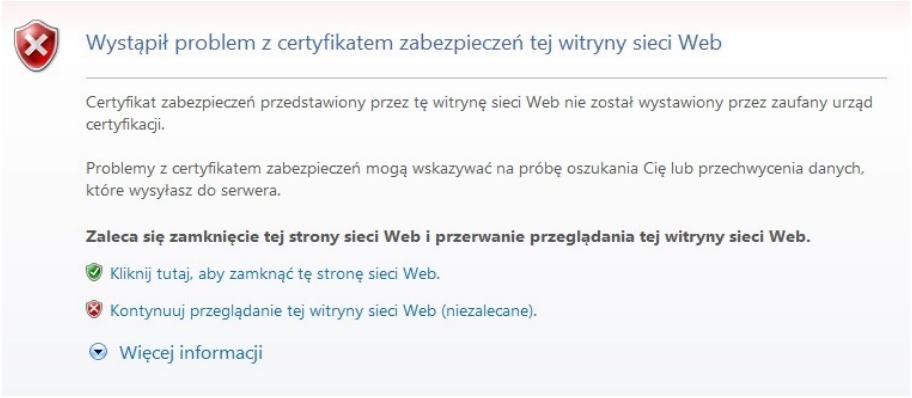
Aby skonfigurować serwer należy

- Zamknąć program bibi
- Uruchomić program narzędziowy biserver, zalogować się jako Administrator, ustawić poziom zabezpieczeń połączeń zewnętrznych na wysoki, wprowadź nowe zasady, nie restartować systemu Windows
- Przejść Dalej wciskając przycisk w dolnej części okna
- W okienku *Certyfikaty SSL* węzła z menu kontekstowego (prawy klawisz myszy) wybrać opcję *Dodaj nowy certyfikat*. Wskazać plik certificate.pfx otrzymany od MicroMade i w dolnym oknie *Hasło PFX*: wpisać kod przesłany w pliku certificate.txt. Potwierdź operację klawiszem Otwórz. Certyfikat SSL zostanie zainstalowany.
- Następnie w oknie *Usługi serwera* należy kliknąć prawym klawiszem myszy na usłudze *Dostęp pracowników do własnych raportów przez serwer WWW* i uruchomić usługę.

6.1.2 Korzystanie z podglądu raportów przez pracowników.

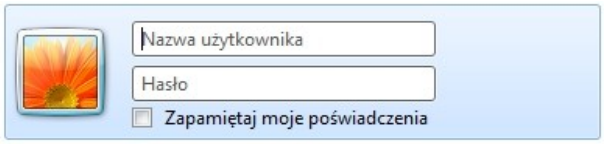
Pracownik wpisuje adres serwera w przeglądarce internetowej postaci: https://[nr IP serwera bibinet] (np.: https://215.177.278.194)

Jeżeli serwer oparty jest na darmowym certyfikacie SSL może pokazać się okno informujące o niepoprawności certyfikatu SSL. Aby to ostrzeżenie nie pokazywało się należy zakupić certyfikat SSL wydany przez zaufany urząd certyfikacji.

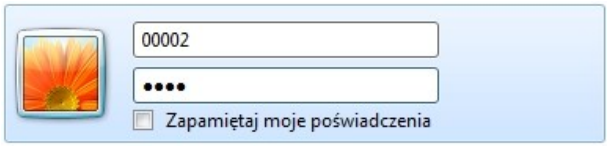


Jeżeli nie dysponujemy takim certyfikatem należy wybrać *Kontynuuj przeglądanie tej witryny sieci Web*. Wówczas pokaże się okno logowania do serwera systemu bibinet.

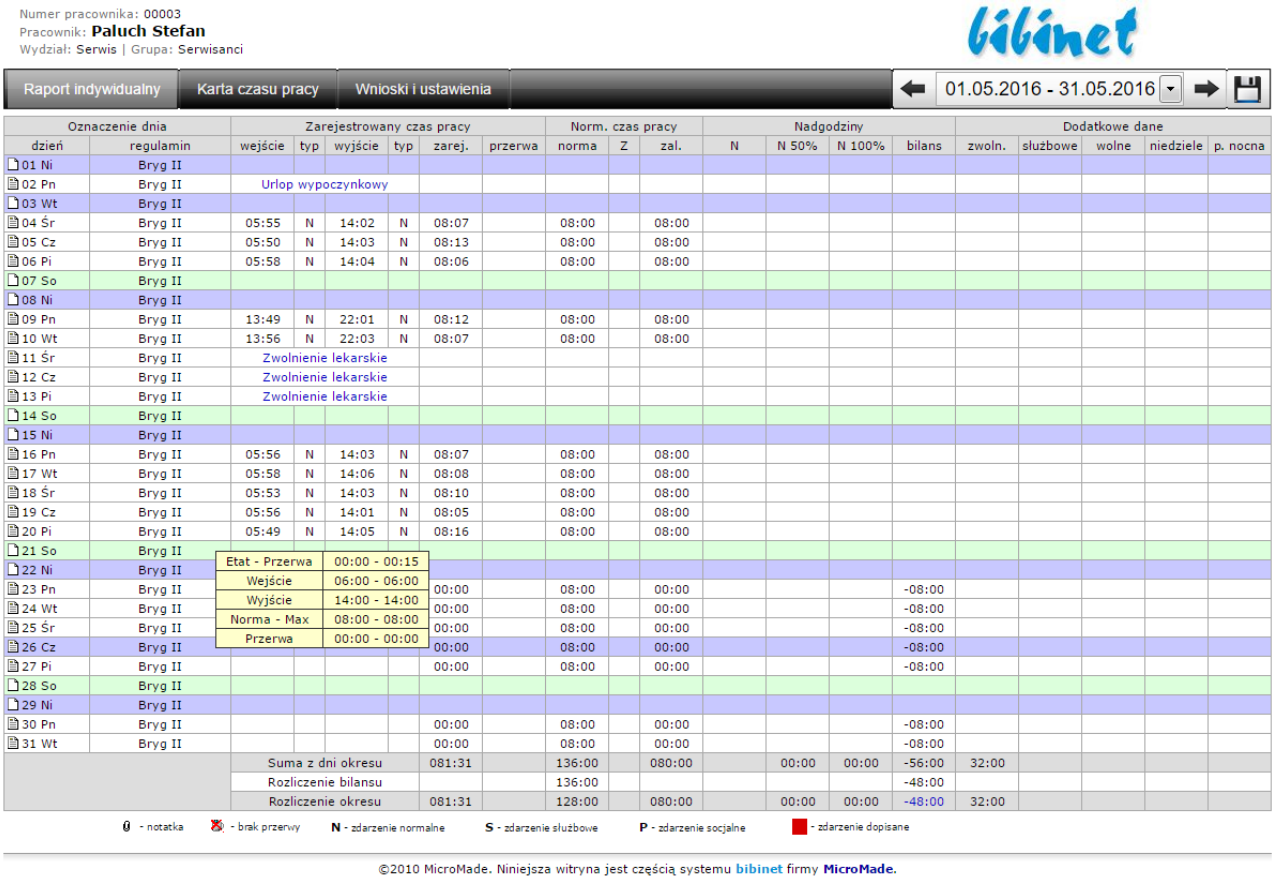
Certyfikat SSL wydaje firma MicroMade przy zakupie opcji podglądu (bibi.PDP).



Jako *Nazwę użytkownika* należy wpisać swój numer w systemie bibinet (5 cyfr) i hasło będące liczbą składającą się z 4-6 cyfr (pierwsza cyfra hasła nie może być zerem 0). Po zaakceptowaniu pokaże się raport indywidualny pracownika. Hasło początkowe ustawia się w programie bibi w *Edycji danych pracowniczych* (Indywidualny kod dostępu do pomieszczeń) – rozdział 2.1.2. Pracownik może zmienić to hasło z poziomu przeglądarki (zakładka Wnioski i ustawienia)..



Po zaakceptowaniu pokaże się raport indywidualny pracownika.



Numer pracownika: 00003
Pracownik: **Paluch Stefan**
Wydział: Serwis | Grupa: Serwisanci

bibinet

Raport indywidualny | Karta czasu pracy | Wnioski i ustawienia | 01.05.2016 - 31.05.2016

Oznaczenie dnia		Zarejestrowany czas pracy						Norm. czas pracy			Nadgodziny				Dodatkowe dane				
dzień	regulamin	wejście	typ	wyjście	typ	zarej.	przerwa	norma	Z	zal.	N	N 50%	N 100%	bilans	zwoln.	służbowe	wolne	niedziele	p. nocna
01 Ni	Bryg II																		
02 Pn	Bryg II	Urlop wypoczynkowy																	
03 Wt	Bryg II																		
04 Śr	Bryg II	05:55	N	14:02	N	08:07		08:00		08:00									
05 Cz	Bryg II	05:50	N	14:03	N	08:13		08:00		08:00									
06 Pi	Bryg II	05:58	N	14:04	N	08:06		08:00		08:00									
07 So	Bryg II																		
08 Ni	Bryg II																		
09 Pn	Bryg II	13:49	N	22:01	N	08:12		08:00		08:00									
10 Wt	Bryg II	13:56	N	22:03	N	08:07		08:00		08:00									
11 Śr	Bryg II	Zwolnienie lekarskie																	
12 Cz	Bryg II	Zwolnienie lekarskie																	
13 Pi	Bryg II	Zwolnienie lekarskie																	
14 So	Bryg II																		
15 Ni	Bryg II																		
16 Pn	Bryg II	05:56	N	14:03	N	08:07		08:00		08:00									
17 Wt	Bryg II	05:58	N	14:06	N	08:08		08:00		08:00									
18 Śr	Bryg II	05:53	N	14:03	N	08:10		08:00		08:00									
19 Cz	Bryg II	05:56	N	14:01	N	08:05		08:00		08:00									
20 Pi	Bryg II	05:49	N	14:05	N	08:16		08:00		08:00									
21 So	Bryg II																		
22 Ni	Bryg II																		
23 Pn	Bryg II					00:00		08:00		00:00				-08:00					
24 Wt	Bryg II					00:00		08:00		00:00				-08:00					
25 Śr	Bryg II					00:00		08:00		00:00				-08:00					
26 Cz	Bryg II					00:00		08:00		00:00				-08:00					
27 Pi	Bryg II					00:00		08:00		00:00				-08:00					
28 So	Bryg II																		
29 Ni	Bryg II																		
30 Pn	Bryg II					00:00		08:00		00:00				-08:00					
31 Wt	Bryg II					00:00		08:00		00:00				-08:00					
		Suma z dni okresu				081:31		136:00		080:00		00:00	00:00	-56:00	32:00				
		Rozliczenie bilansu						136:00						-48:00					
		Rozliczenie okresu				081:31		128:00		080:00		00:00	00:00	-48:00	32:00				

Etat - Przerwa	00:00 - 00:15
Wejście	06:00 - 06:00
Wyjście	14:00 - 14:00
Norma - Max	08:00 - 08:00
Przerwa	00:00 - 00:00

0 - notatka | - brak przerwy | **N** - zdarzenie normalne | **S** - zdarzenie służbowe | **P** - zdarzenie socjalne | - zdarzenie dopisane

6.1.3 Logo klienta w podglądzie raportów pracowniczych.

Logo to może zastąpić niebieskie logo bibinet w podglądzie raportów pracowniczych.

Na węźla sieci bibinet z którego pobierane są dane do podglądu, w katalogu dane (standardowo w lokalizacji: C:\Program Files\MicroMade\bibinet\Server\Data lub C:\Program Files (x86)\MicroMade\bibinet\Server\Data dla systemów

64 bitowych) należy umieścić plik o nazwie logo.jpg (wymiary 200 pikseli x 60 pikseli w formacie jpg). Po restarcie serwera bibinet (np. poprzez uruchomienie i zalogowanie się do programu narzędziowego biserver.exe), nowe logo będzie widoczne dla użytkowników systemu.

6.2 Instalacja terminali

Instalacje terminali musimy rozpocząć od skonfigurowania węzła, z którym mają się łączyć terminale.

Węzeł systemu bibinet i podłączone do niego terminale muszą pracować:

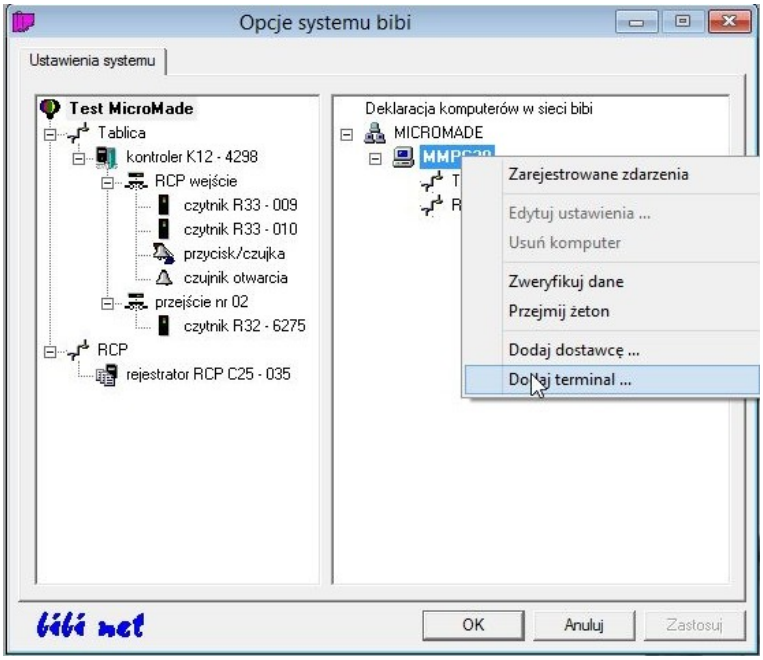
- w jednej domenie albo
- w grupie roboczej.

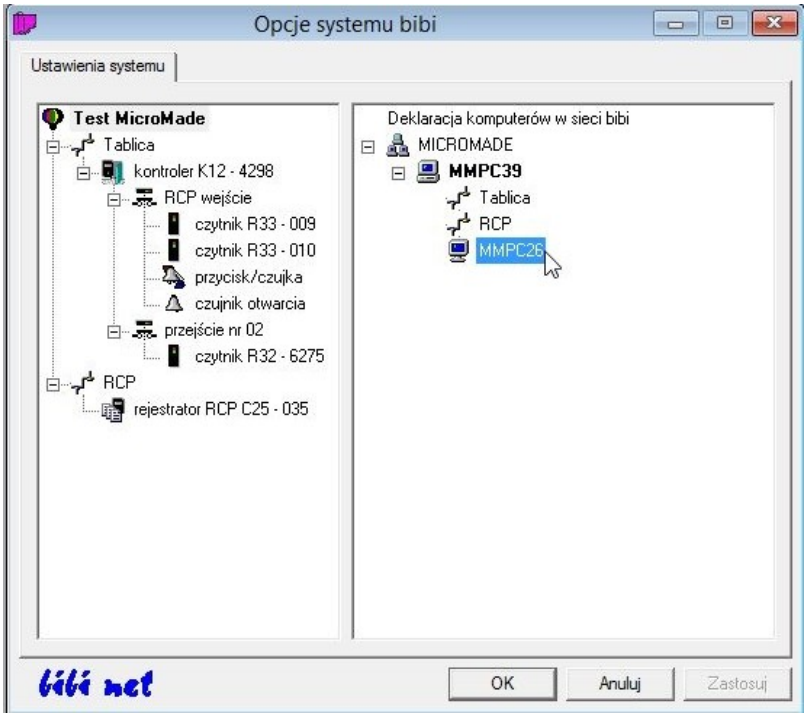
Nie można mieszać tych dwóch sposobów identyfikacji w ramach jednego węzła systemu bibinet.

6.2.1 Konfigurowanie węzła do podłączenia terminali

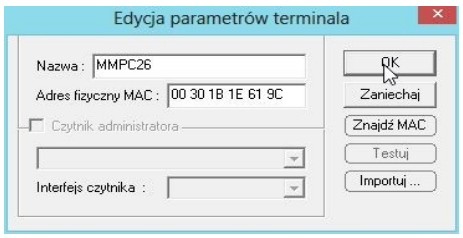
- Zadeklarować terminale na węźle.

Wykonać to można w sposób zbliżony do dodawania kolejnych komputerów. W okienku „Opcje systemu bibi" należy ustawić się na nazwie komputera (węzła systemu bibinet), do którego dołączane będą komputery-terminale i z podręcznego menu wydać polecenie: *Dodaj terminal*.





Przy dodawaniu terminali można skorzystać z danych wytworzonych przez program narzędziowy bicomp. Wystarczy nacisnąć klawisz *Importuj* i wybrać plik *.bix wytworzony programem bicomp na komputerze, który ma pełnić funkcję terminala sieci bibinet.

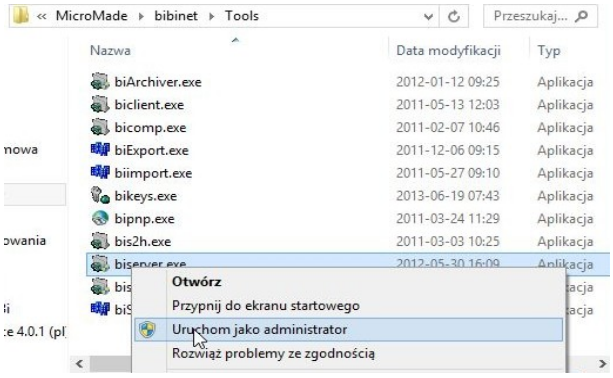


Jeżeli nie posiadamy pliku wytworzonego przez program bicomp, należy parametry komputera wpisać w okienko. Dla terminala należy podać adres fizyczny MAC (numer karty sieciowej). W tym celu można się posłużyć klawiszem Znajdź MAC, który poprosi o podanie numeru IP lub o nazwę komputera w sieci obsługiwanej przez DNS.

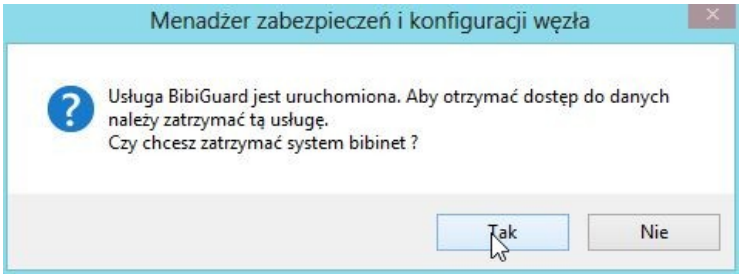
W ten sposób należy zadeklarować wszystkie terminale, które chcemy dołączyć do danego węzła.

- Uruchomić program narzędziowy biserver.exe w celu konfiguracji serwera do połączenia z terminalami

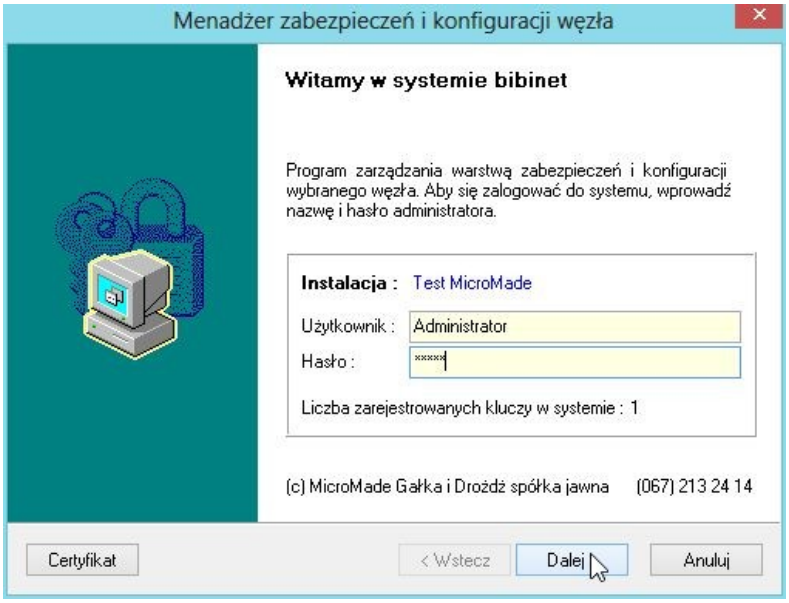
  (w systemie Windows 7/8/10 programy te należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator")



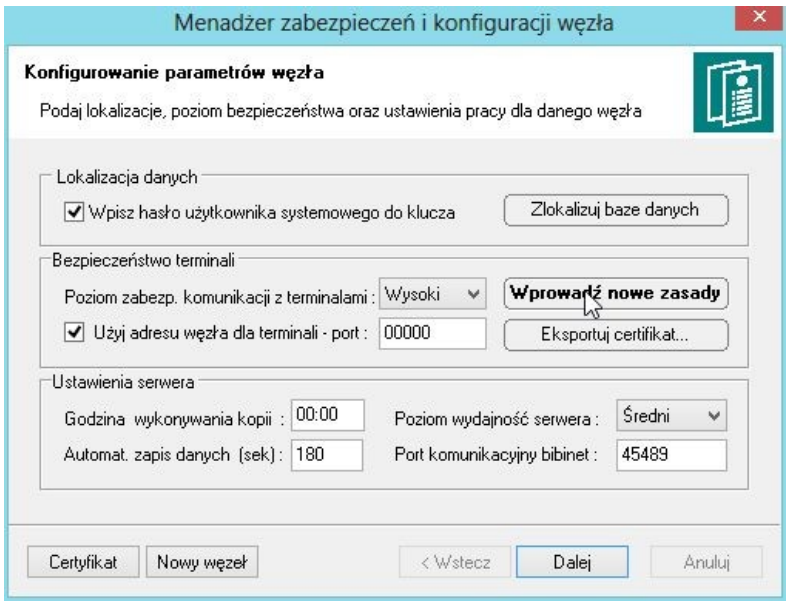
- Jeżeli pojawi się komunikat „Czy chcesz zatrzymać system bibinet ?" należy go potwierdzić.



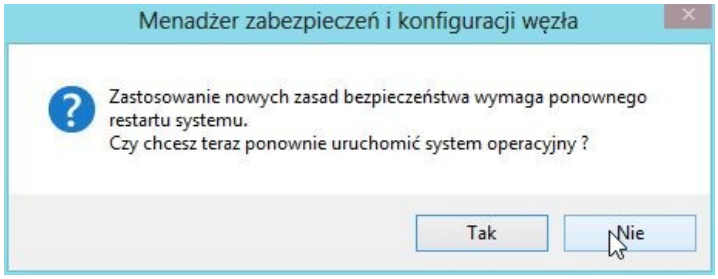
- Wpisać użytkownika Administrator i jego hasło



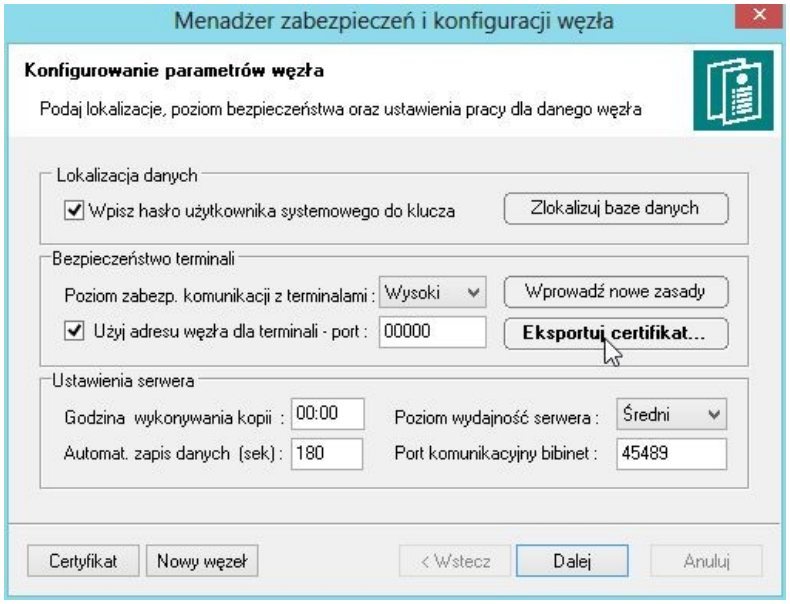
- Ustawić poziom zabezpieczeń komunikacji z terminalami na *Wysoki* i zatwierdzić klawiszem *Wprowadź nowe zasady.*

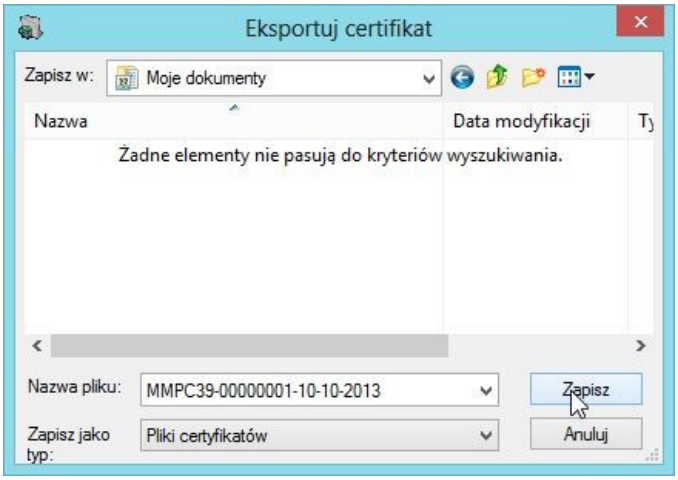


- Jeżeli na ekranie pojawi się informacja o konieczności restartu systemu Windows, można odpowiedzieć *NIE*, ponieważ nie jest to wymagane do wprowadzenia nowych zasad pracy serwera



- Wyeksportować certyfikat (klawiszem *Eksportuj certyfikat*) i zapisać go na dysku - będzie potrzebny przy instalacji terminali.

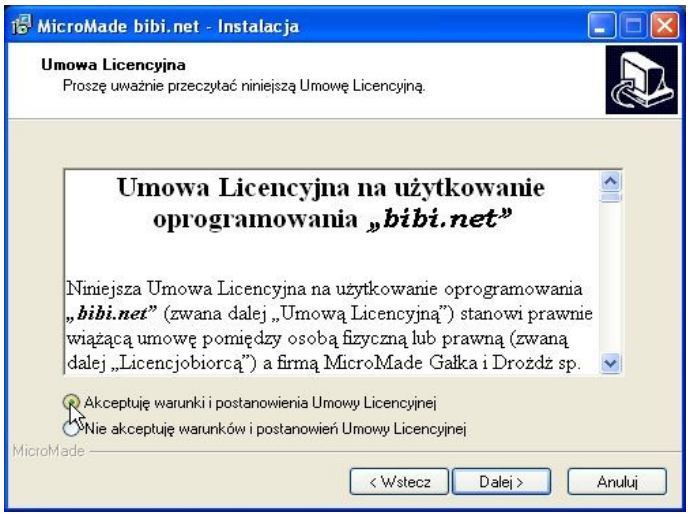




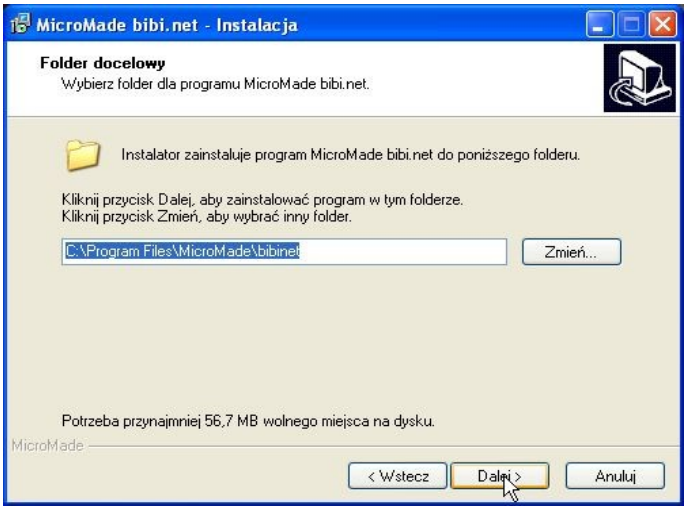
6.2.2 Instalacja program bibi.net na terminalu

Na terminalach należy zainstalować tą samą wersję programu, która jest na węźle systemu bibinet.

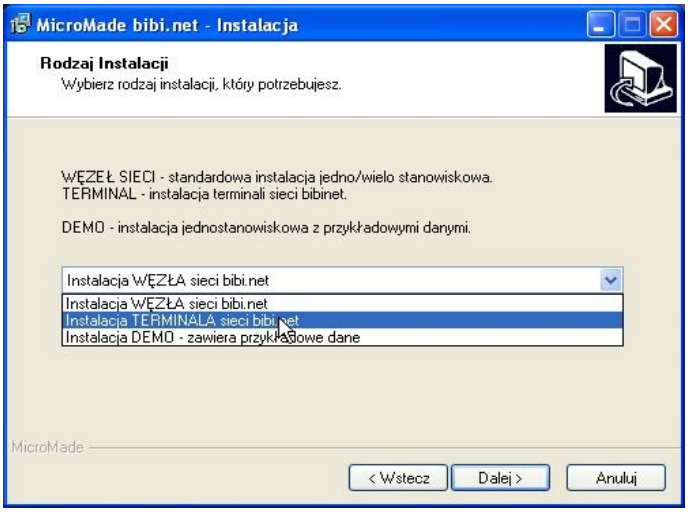
- Wybrać z menu instalatora systemu bibi.net "Instalacja bibi.net" lub uruchomić program bibinet_setup.exe.
- Przeczytać i zaakceptować umowę licencyjną.

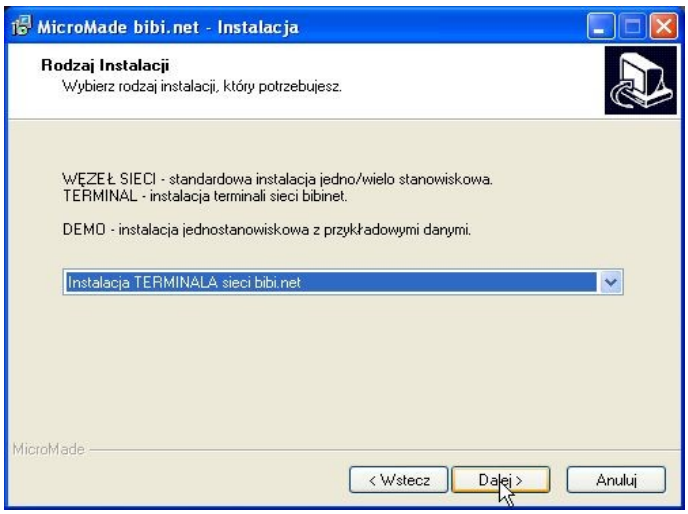


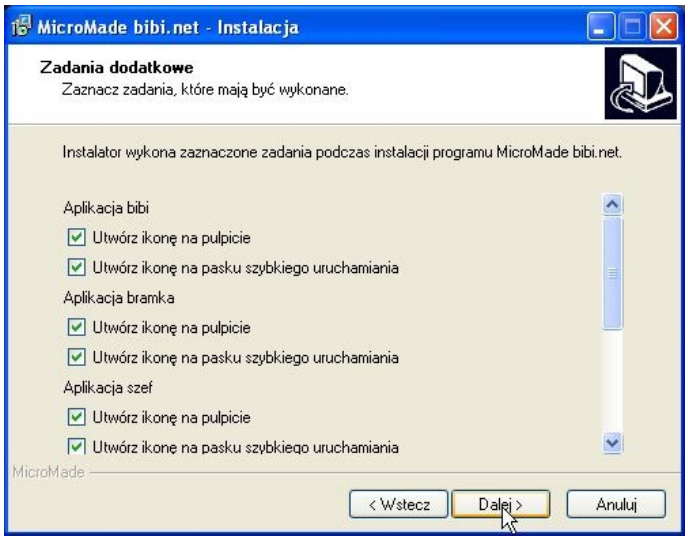
- Wybrać miejsce instalacji programu

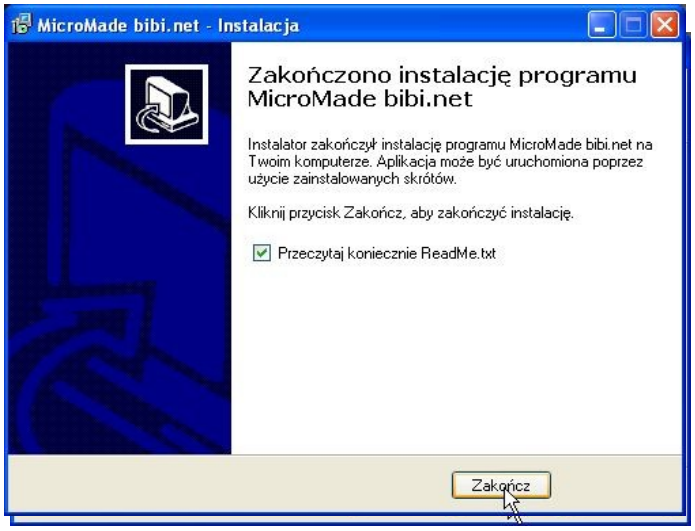


- Wybrać rodzaj instalacji: „Instalacja TERMINALA sieci bibi.net”



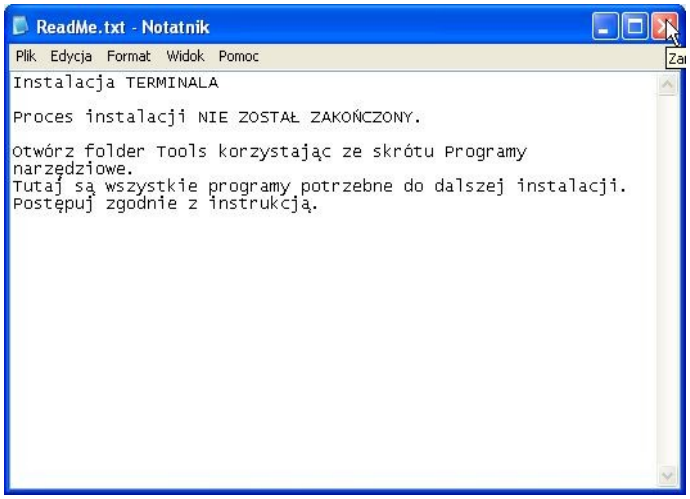






W wyniku tej instalacji na terminalu zostały zainstalowane aplikacje bibi, bramka, szef oraz program narzędziowy bic-lient.

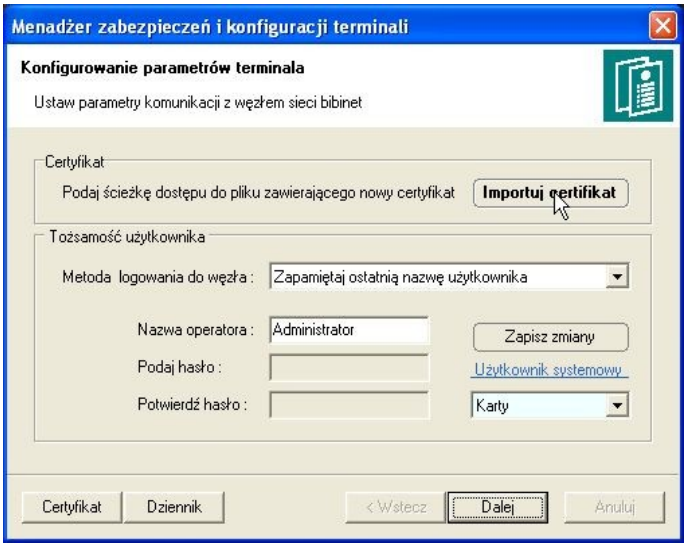
6.2.3 Dokończenie instalacji terminala



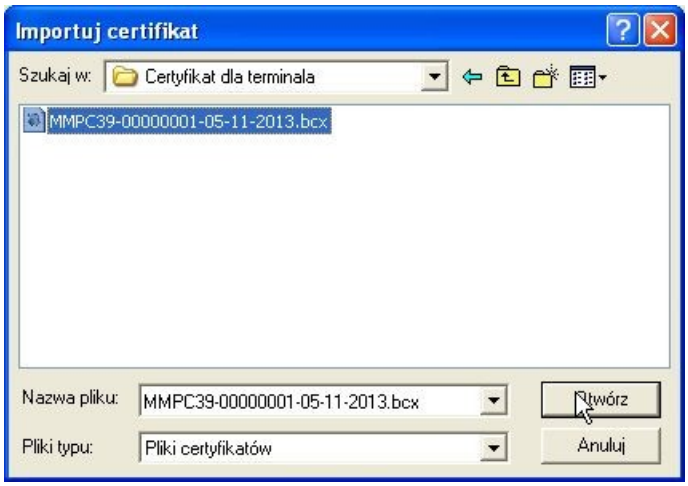
W tym celu potrzebny będzie tymczasowo klucz bibi.HAK. Może to być klucz z serwera lub dodatkowy Klucz systemowy - w terminalu będzie on potrzebny tylko w czasie instalacji.

- Udostępnić plik certyfikatu *.bcx w sieci lub skopiować na terminal.
- Włożyć klucz do portu USB w terminalu.
- Otworzyć program biclient.exe (w systemie Windows 7/8/10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”) i zalogować się jako Administrator.

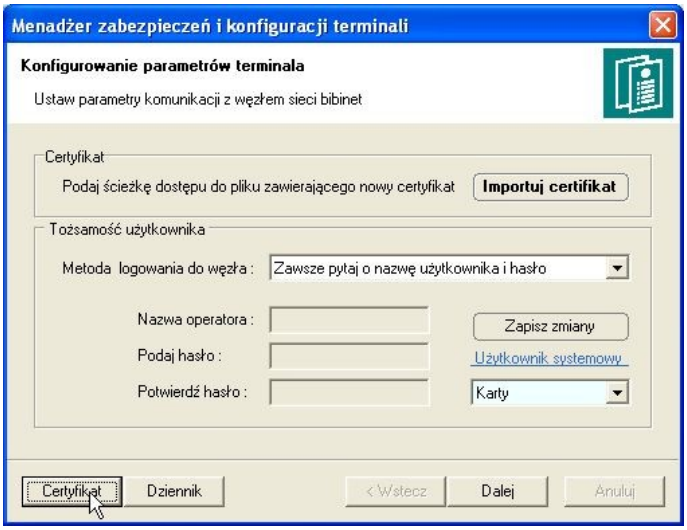
- Po zalogowaniu się naciśnij przycisk „Importuj certyfikat”.



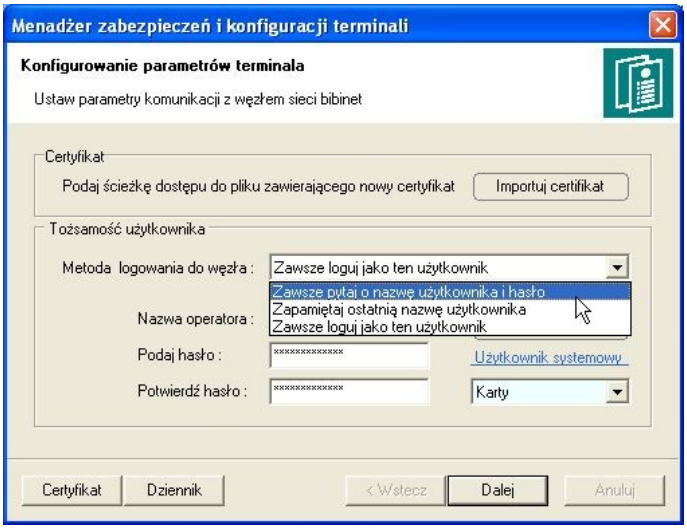
- Wskaż udostępniony certyfikat *.bcx a następnie kliknij na przycisk „Otwórz.”



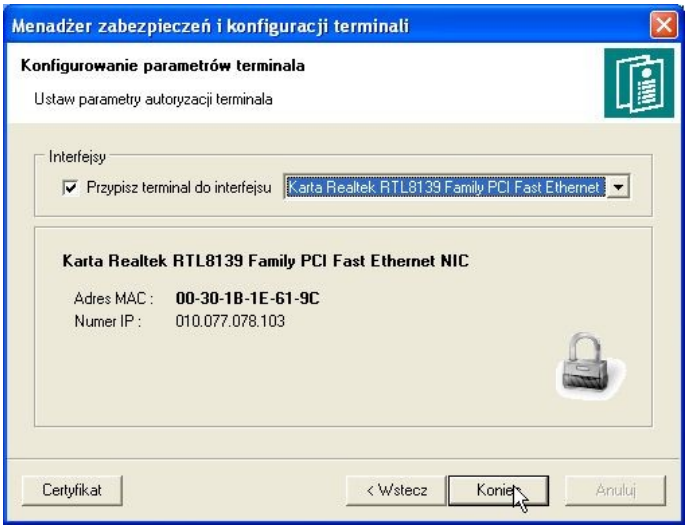
- certyfikat zostanie zainstalowany (można go podejrzeć wciskając klawisz Certyfikat)



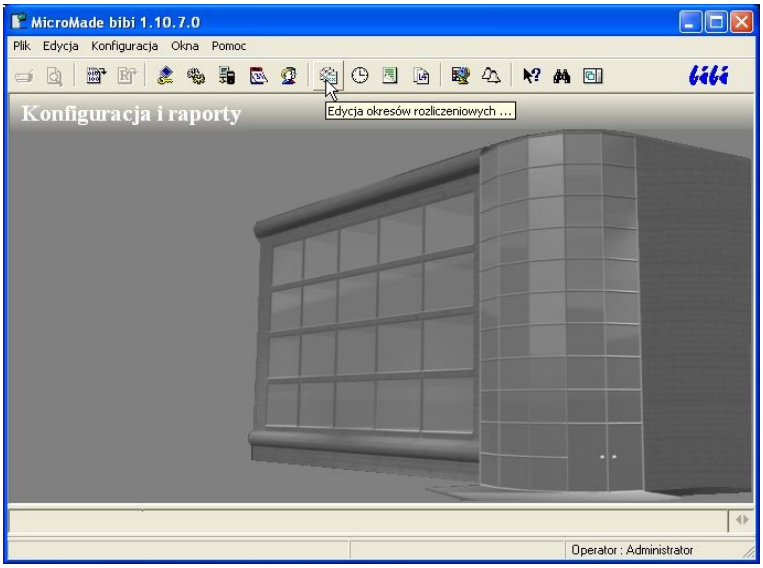
- Ustawić sposób logowania się operatorów na terminalu



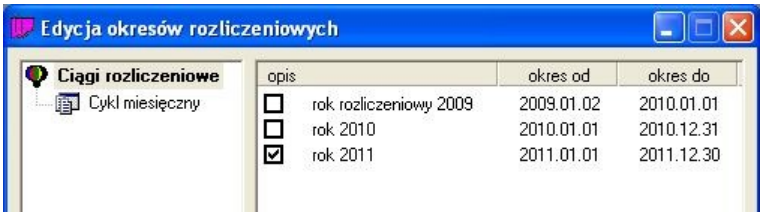
- Jeżeli komputer, który ma być terminalem posiada więcej niż jedną kartę sieciową należy klawiszem *Dalej* przejść do następnego okna i ustawić parametry autoryzacji terminala w sieci



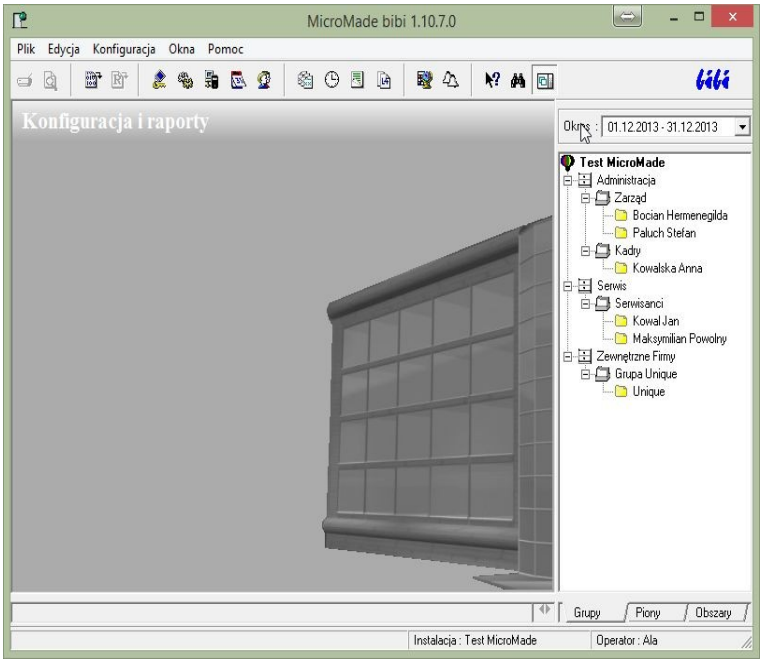
- Zamknąć program biclient.
- Jeżeli klucz na czas instalacji terminala został zabrany z węzła (serwera) to należy go z powrotem włożyć do portu USB serwera.
- Uruchomić program bibi

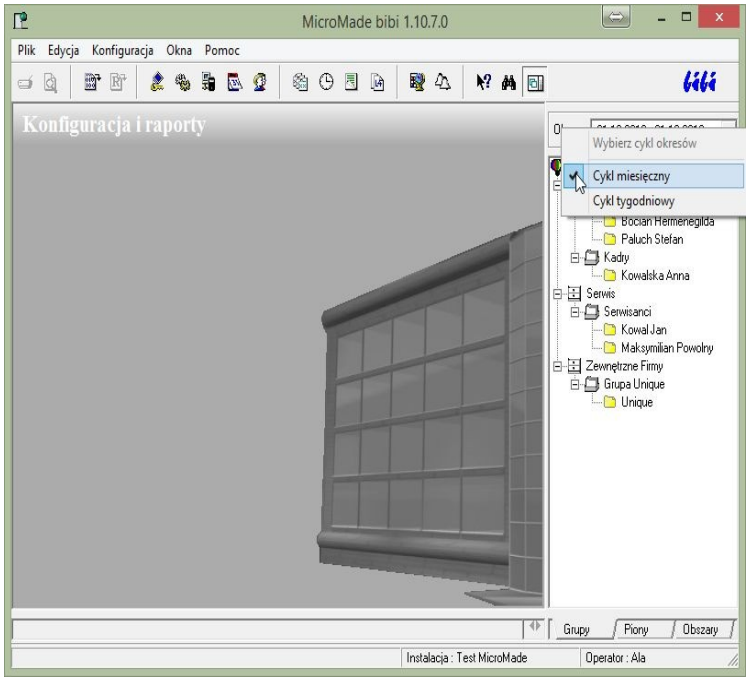


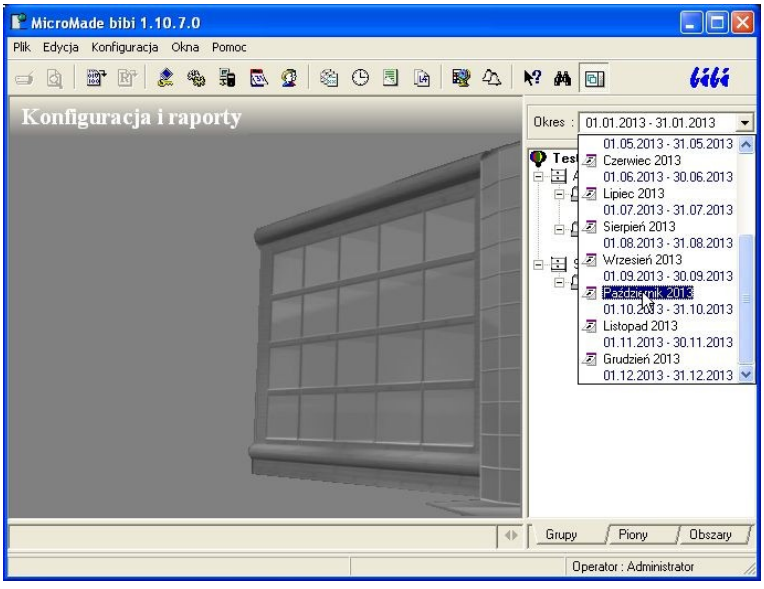
- Otworzyć okienko *Edycja okresów rozliczeniowych* i wybrać jeden z zadeklarowanych okresów rozliczeniowych



- Włączyć boczny panel, wskazać myszą napis **Okres** i w podręcznym menu wskazać jeden cykl (np. cykl miesięczny)







- Wybrać z listy okres, za który będą sporządzane raporty przez program bibi.
- można już pracować na terminalu

Opisane czynności powtórzyć na wszystkich terminalach.

6.3 Instalacja kolejnych węzłów

Dodatkowe węzły instaluje się głównie w rozległych instalacjach, gdzie w różnych oddalonych obiektach jest konieczność obsługi lokalnych części instalacji przez lokalnych operatorów np. sieć fabryk, zakładów pracujących pod wspólną marką, sieć dużych hurtowni itp.

6.3.1 Deklarowanie kolejnych komputerów na pierwszym węźle

Zadeklarować kolejne komputery na pierwszym węźle. W tym celu otworzyć okno Opcje systemu bibi. Ustawić się na ikonie domeny i dodać kolejny węzeł (węzły) pracujące w tej samej domenie lub ustawić się na napisie Deklaracja komputerów w sieci bibi i dodać nową domenę a w niej kolejne węzły.

Przy dodawaniu pierwszego komputera w instalacji program sam odczyta parametry komputera, na którym jest uruchomiony i wypełni odpowiednio dane w powyższym okienku. Wystarczy tylko je zaakceptować klawiszem „OK”.

Przy dodawaniu kolejnych komputerów można skorzystać z danych wytworzonych na innych węzłach przez program narzędziowy bicomp Wystarczy nacisnąć klawisz *Importuj* i wybrać plik *.bix wytworzony na komputerze, który ma być dodany.

Jeżeli nie posiadamy pliku wytworzonego przez program bicomp, należy parametry komputera wpisać w okienko używając klawiatury. Komputer węzeł w sieci bibi.net musi posiadać stały numer IP lub numer ten otrzymywać z serwera DNS. Wybieramy jeden z tych wariantów:

- dla stałego numeru IP podajemy ten numer
- dla numeru IP otrzymywanego z serwera DNS wpisujemy nazwę komputera dla serwera DNS

Następnie wciskamy klawisz „Znajdź MAC”, co umożliwia automatyczne wyszukanie adresu fizycznego MAC i wpisanie go do parametrów komputera.

Jeżeli dodawany komputer nie jest obecnie dostępny w sieci (lub dodajemy komputer spoza domeny), numer MAC może nie zostać automatycznie wyszukany. W takim wypadku należy go wpisać używając klawiatury bezpośrednio do okienka z parametrami komputera.

Zarówno numer IP jak i adres fizyczny MAC możemy odczytać z komputera. W tym celu należy otworzyć okienko DOS-owe poprzez:

- Start/Programy/Akcesoria/Wiersz polecenia lub
- Start/Uruchom i wpisanie komendy cmd.

W otwartym okienku należy wpisać rozkaz:

ipconfig /all

który spowoduje wypisanie na ekranie potrzebnych numerów.

- Zamknąć program bibi
- Uruchomić program narzędziowy biserver.exe .
  - Zalogować się jako Administrator.
  - Nacisnąć klawisz *Nowy węzeł*
  - Zapisać dane węzła do pliku NazwaZakładu.bnx
  - Zamknąć program biserver

6.3.2 Konfiguracja kluczy sprzętowych bibi.HAK

Na pierwszym węźle skonfigurować odpowiednią ilość kluczy bibi.HAK - minimum tyle ile ma być węzłów sieci plus jeden (klucz systemowy). Jeżeli nie były przygotowane od razu, to należy ponownie uruchomić program narzędziowy bikeys.exe. Przy czym, teraz nie należy generować nowego hasła, ale należy wybrać opcję *pobierz hasło z klucza,* włożyć klucz systemowy i pobrać z niego hasło szyfrujące. Przejść *Dalej* do tabeli z kluczami włożonymi do komputera i skonfigurować je do pracy w systemie bibinet.

6.3.3 Instalacja programów bibi.net na kolejnych węzłach

- Wybrać z menu instalatora systemu bibi.net "Instalacja bibi.net" lub uruchomić program bibinet_setup.exe.
- Przeczytać i zaakceptować umowę licencyjną.

- Wybrać *Instalacja WĘZŁA sieci bibi.net*
- Wskazać folder, w którym umieszczony jest plik licencji license.dat. Może on być na pendrive w folderze Licencja lub został przesłany pocztą elektroniczną. Plik ten znajduje się w katalogu: ..\MicroMade\bibinet\Server\Data

6.3.4 Dokończenie instalacji kolejnych węzłów

- Udostępnić plik NazwaZakładu.bnx w sieci lub skopiować na nowy węzeł.
- Włożyć skonfigurowany wcześniej klucz bibi.HAK do nowego węzła.
- Kliknąć myszą na pliku NazwaZakładu.bnx lub z podręcznego menu wydać komendę „Zainstaluj”
- Automatycznie uruchomi się program narzędziowy biserver.exe.
  - wydać polecenie *Zlokalizuj bazę danych*
  - ustawić *Poziom zabezpieczeń komunikacji z terminalami* - zalecany Wysoki
  - nacisnąć klawisz *Wprowadź nowe zasady*
  - nie restartować systemu Windows
  - zamknąć program biserver
- Powtórzyć te czynności na wszystkich węzłach
- Na wszystkich komputerach uruchomić program bibi.

W oknie *Opcje systemu bibi* na każdym węźle powinny być widoczne wszystkie komputery jako dostępne - nieprzekreślone.

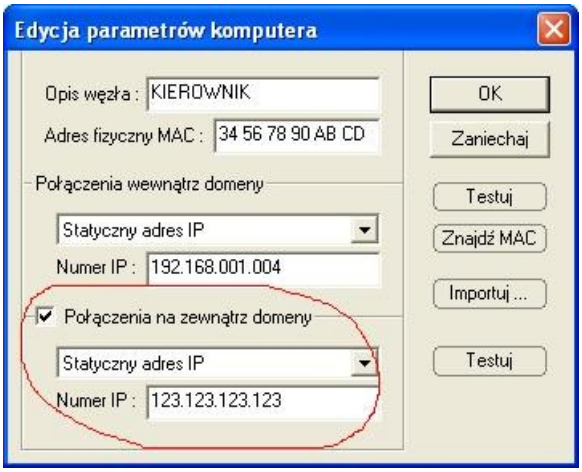
6.4 Budowanie rozległej sieci bibi.net

Taką sieć musimy zbudować, jeżeli firma mieści się w kilku lokalizacjach i w każdej z nich komputery pracują w sieci lokalnej, podłączonej do internetu poprzez routery.

Całą sieć definiujemy na jednym komputerze. Dla każdej lokalizacji należy zdefiniować oddzielną domenę bibi.net.

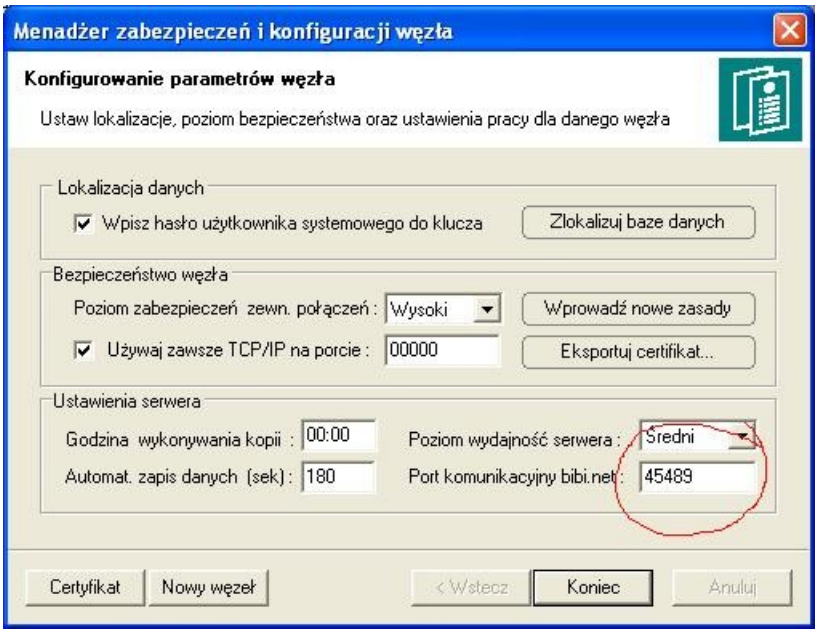
W tych domenach definiujemy komputery, które mają pracować jako węzły sieci bibi.net.

Wszystkie komputery w jednej domenie porozumiewają się ze sobą (każdy z każdym) w celu wymiany danych. Natomiast do połączenia pomiędzy domenami należy wyznaczyć jeden komputer w każdej domenie. Dla tych komputerów należy otworzyć okienko *Edycja parametrów komputera* i zaznaczyć flagę *Połączenia na zewnątrz domeny*. Jako numer IP podajemy zewnętrzny numer routera sieci lokalnej, pod jakim jest on widoczny w sieci internet.



Po zdefiniowaniu komputerów do połączenia pomiędzy domenami, będzie to zaznaczone w opcjach systemu bibi.

Wszystkie komputery pracujące w jednej sieci bibi.net muszą mieć jednakowo zdefiniowany port do komunikacji między sobą. Port ten można zdefiniować w programie biserver. Domyślnie jest przypisany port 45489 czyli 0xB1B1, ale można wybrać dowolny numer.



Należy zapewnić, aby port ten nie był używany przez inne programy oraz nie był blokowany przez programy typu firewall. Dodatkowo, w routerach należy przekierować transmisję przychodzącą na ten port, na komputer wybrany do połączenia między domenami.

Do tak zdefiniowanej sieci komputerów - węzłów sieci bibi.net, należy dodać jeszcze komputery, które będą terminalami w tej sieci. Terminale pracują tylko w sieci lokalnej, i będą pobierały dane z serwera, do którego zostały przypisane. Dodanie terminali kończy pierwszy etap budowy sieci bibi.net. W opcjach systemu bibi powinna być widoczna cała sieć bibi, choć część komputerów będzie poprzekreślana, jako obecnie niedostępna.

Po zdefiniowaniu całej sieci komputerów można przystąpić do instalacji programu bibi.net na pozostałych węzłach. W tym celu, korzystając z klawisza „Nowy węzeł” w programie biserver, tworzymy plik eksportu danych węzła *.bnx. Plik ten należy następnie zaimportować na wszystkich pozostałych węzłach.

Po uruchomieniu serwerów bibinet na wszystkich węzłach, wszystkie komputery w sieci bibinet powinne być widoczne jako nieprzekreślone.

Następnym etapem jest dołączenie urządzeń bibi, czyli dostawców sieci. Należy to wykonać na węzłach sieci, do których dołączone są sieci urządzeń bibi.

Podsumowanie:

Rozległą sieć deklarujemy na jednym węźle i bazę danych bidata.bdb kopiujemy na wszystkie pozostałe węzły (można w tym celu wykorzystać plik *.bnx)

6.5 Opis programów narzędziowych.

Programy narzędziowe systemu bibinet znajdujące się w katalogu MicroMade/bibinet/Tools (skrót na Pulpicie: bibi - programy narzędziowe) **należy uruchamiać będąc zalogowanym na koncie Administratora systemu Windows. Dodatkowo w systemie Windows 7/ 8/10 programy te należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”**

6.5.1 Program bicomp - odczyt danych komputera

W celu ułatwienia odczytu danych z komputera został stworzony program bicomp.exe. Po jego uruchomieniu na ekranie pojawi się okienko z wszystkimi potrzebnymi danymi.

Odczytane dane można skopiować (górna ikonka) poprzez schowek do np. notatnika i przesłać na komputer, na którym dodawane są kolejne węzły. Przy dodawaniu do sieci bibi.net kolejnego komputera, trzeba potrzebne dane przepisać.

Jeszcze prostszą metodą jest zapisanie tych danych do specjalnego pliku *.bix (dolna ikonka). Plik ten należy udostępnić w sieci, lub przesłać do komputera, na którym dodawane są kolejne węzły lub terminale sieci bibi.net. Przy dodawaniu kolejnego komputera lub terminala wystarczy nacisnąć klawisz *Importuj* i wskazać plik z odpowiedniego komputera.

6.5.2 Program biserver - konfigurowanie węzła sieci

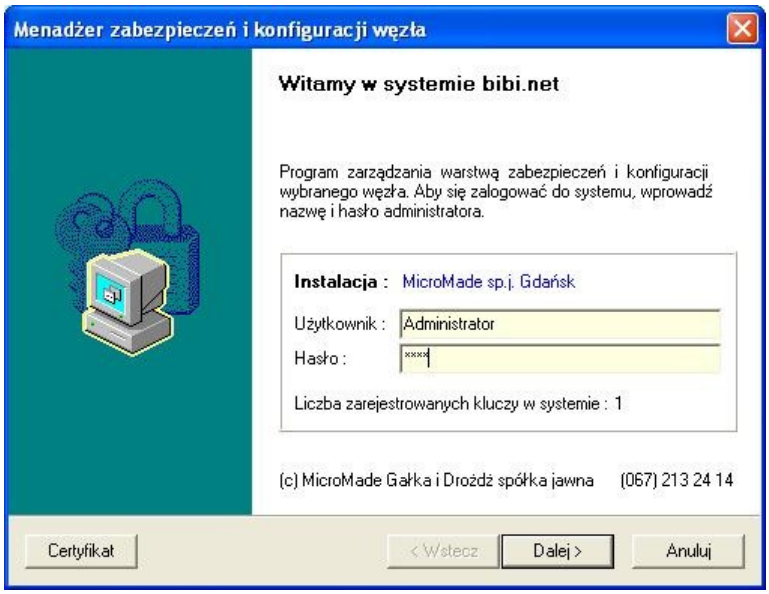
W systemie Windows 7/ 8/10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”.

Program biserver służy do konfigurowania węzła sieci. Użycie jego jest niezbędne na każdym węźle sieci dla prawidłowej pracy serwera bibinet. Jedynym wyjątkiem jest instalacja Demo, gdzie pewne ustawienia są wprowadzane razem z dostarczoną bazą danych.

Program biserver, jeżeli wybierzemy wysoki poziom zabezpieczeń komunikacji z terminalami, automatycznie rejestruje usługę biguard. Usługa ta automatycznie uruchamia serwer bibinet po uruchomieniu komputera. Program biserver można uruchomić tylko wtedy, kiedy nie działa serwer bibinet. Dlatego, przy kolejnych uruchomieniach programu biserver, może pojawić się następujący komunikat:

Należy wybrać klawisz *Tak*, który zatrzyma usługę BibiGuard, a tym samym zostanie zatrzymany serwer bibinet.exe. Dzięki temu program biserver będzie mógł komunikować się z bazą danych.

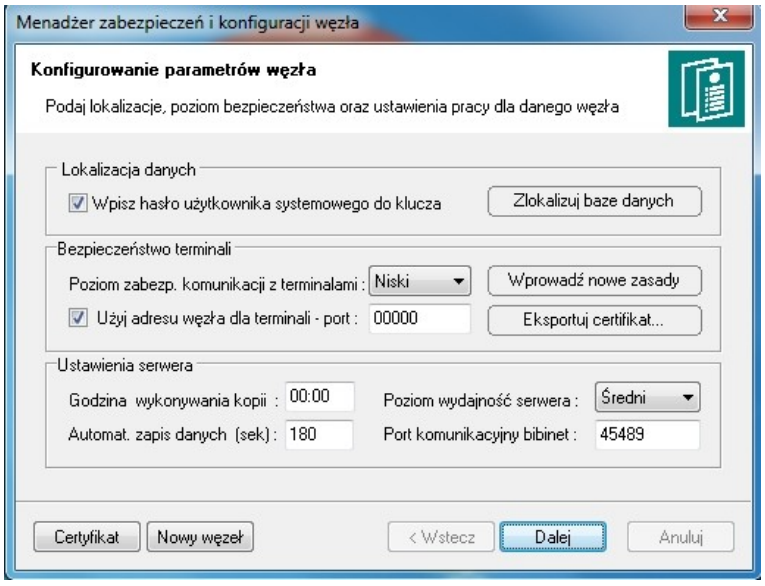
Po uruchomieniu programu biserver pojawia się okno logowania, w którym należy zalogować się jako Administrator.



Po zalogowaniu się otwiera się właściwe okno programu.

Konfiguracji serwera dokonuje się przełączając się między trzema oknami programu klawiszem Dalej.

W pierwszym oknie znajdują się trzy oddzielne ramki, odpowiedzialne za poszczególne zadania.



Lokalizacja danych

Jest to funkcja potrzebna przy tworzeniu kolejnego węzła sieci i przenoszeniu na niego bazy danych. Baza taka jest powiązana z komputerem, na którym jest tworzona. Aby mogła prawidłowo pracować na innym komputerze, musi nastąpić jej lokalizacja. Można to wykonać poprzez naciśnięcie klawisza „Zlokalizuj bazę danych".

Bezpieczeństwo węzła

Określa sposób pracy serwera bibinet oraz poziom zabezpieczeń przy połączeniu terminali z węzłem.

- Wysoki
  - rejestruje usługę biguard, która nadzoruje pracę serwera bibinet

- uruchamia serwer bibinet przy włączeniu komputera
- nadzoruje na bieżąco pracę serwera - w razie konieczności potrafi go na nowo uruchomić

- włącza szyfrowanie transmisji pomiędzy serwerem a terminalami
- konfiguruje serwer do bezpiecznego łączenia się terminali

- Niski
  - wyłącza usługę biguard
  - serwer jest uruchamiany na czas pracy aplikacji użytkowej (bibi, bramka) uruchamianej na tym komputerze (aplikacja uruchomiona na terminalu nie potrafi uruchomić serwera)
  - wyłączone szyfrowanie transmisji pomiędzy serwerem a terminalami
  - wyłączone jest uwierzytelnianie połączeń z terminala
- Użytkownika (nie zalecany)
  - usługa biguard i serwer bibinet jak w stanie niskim
  - administrator sieci może sam skonfigurować połączenie terminala z serwerem

Przy dołączeniu do serwera terminali, wymagany jest poziom zabezpieczeń „Wysoki".

W pozostałych wypadkach również zaleca się ustawienie poziomu zabezpieczeń „Wysoki".

Szczególnie ma to znaczenie na węzłach do których dołączone są urządzenia bibi - rejestracje zbierane są na bieżąco i dzięki temu dostępne na innych węzłach sieci.

Poziom „Niski" należy stosować w przypadku konieczności wyłączenia serwera i w instalacjach w których rzadko korzysta się z programu bibi.

Flaga „Używaj zawsze TCP/IP" powinna być zaznaczona, jeżeli w sieci posługujemy się stałymi adresami IP. Jeżeli komputery pracują w domenie, flagę „Używaj zawsze TCP/IP" możemy odznaczyć.

Numer portu poniżej 1024 oznacza, że system przydzieli automatycznie numer portu do komunikacji z terminalem. Ustawienie dowolnej wartości wyższej spowoduje, że komunikacja będzie odbywała się z wykorzystaniem tego ustawionego numeru portu. Port ten nie może być zablokowany przez filtrowanie TCP/IP.

Standardowo, flagę „Używaj zawsze TCP/IP" należy pozostawić zaznaczoną, a port pozostawić ustawiony na 0.

Po dokonaniu tych ustawień należy nacisnąć klawisz „Wprowadź nowe zasady". W tym momencie wyskoczy okienko:

Obecnie, już wszystkie zasady wprowadzane są prawidłowo bez restartu systemu, tak więc można odpowiedzieć Nie. Jeżeli jednak coś by nie działało prawidłowo prosimy zrestartować system później.

Wprowadzone w ten sposób zasady pracy węzła (serwera) zapisywane są w certyfikacie. Można go obejrzeć po naciśnięciu klawisza *Certyfikat*.

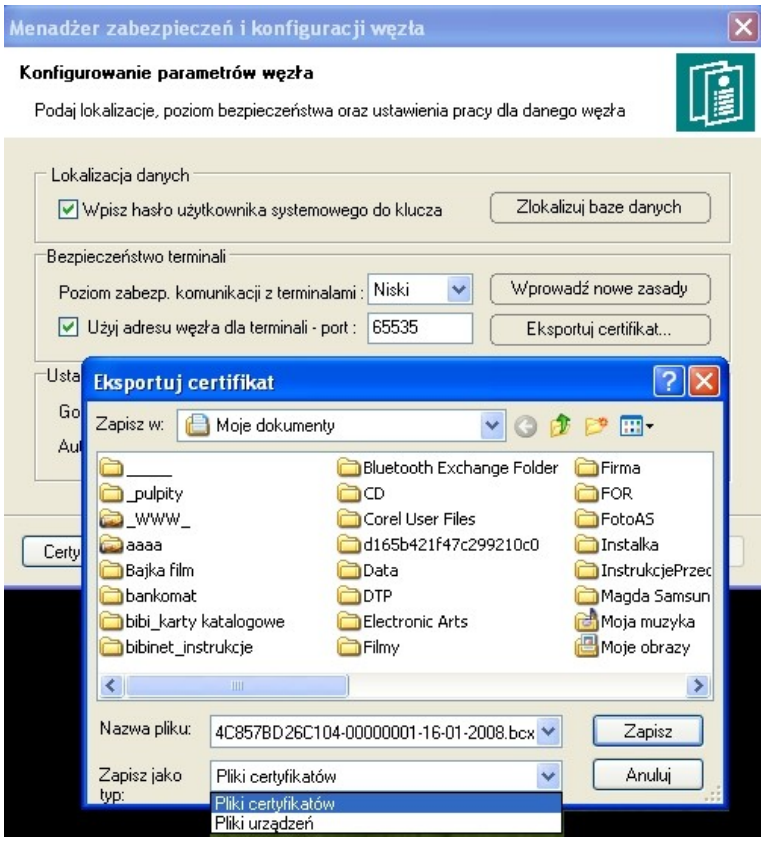
Eksport (zapisywanie) certyfikatu.

Certyfikat zawierający cechy i zasady pracy węzła (serwera) systemu bibinet służy do zapewnienia bezpiecznej transmisji z terminalami lub urządzeniami sieciowymi systemu.

Jeżeli do węzła chcemy podłączać dodatkowe komputery jako terminale systemu (ich ilość opisuje wykupiona przez użytkownika licencja), należy certyfikat wyeksportować do pliku wybierając opcję *Pliki certyfikatów*, który następnie pobrany będzie w procesie instalacji terminala programem narzędziowym biclient.

Jeżeli do węzła podłączane będą urządzenia sieciowe (np. interfejs bibi-F22), znajdujące się w innych podsieciach, konieczne będzie dostarczenie tym urządzeniom pliku certyfikatu przy pomocy programu narzędziowego urządzenia działającego przez przeglądarkę internetową. Taki certyfikat zapisujemy wybierając opcję *Pliki urządzeń*.

Wybór rodzaju eksportowanego certyfikatu wybieramy z menu rozwijanego po wciśnięciu klawisza *Eksportuj certyfikat*



Ustawienia serwera

Pozwala na zmianę innych ustawień w serwerze. Bez wyraźnej potrzeby nie należy tych ustawień zmieniać.

„Port komunikacyjny bibi.net" określa numer portu, który wykorzystywany jest w komunikacji pomiędzy serwerami. Standardowo jest on ustawiony na wartość 45489 (czyli w zapisie szesnastkowym 0xB1B1). Należy pamiętać, aby był on jednakowo ustawiony we wszystkich węzłach, i nie był blokowany przez filtrowanie TCP/IP.

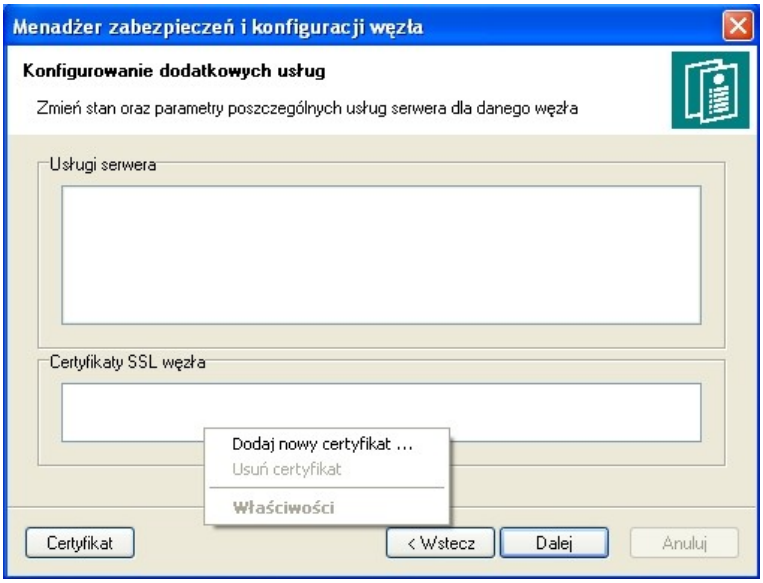
Nowy węzeł

Klawisz ten pozwala na wyeksportowanie danych węzła do pliku NazwaZakładu.bnx. Plik ten jest przydatny przy tworzeniu nowego węzła w sieci bibi.net.

Pobieranie certyfikatów na węzeł.

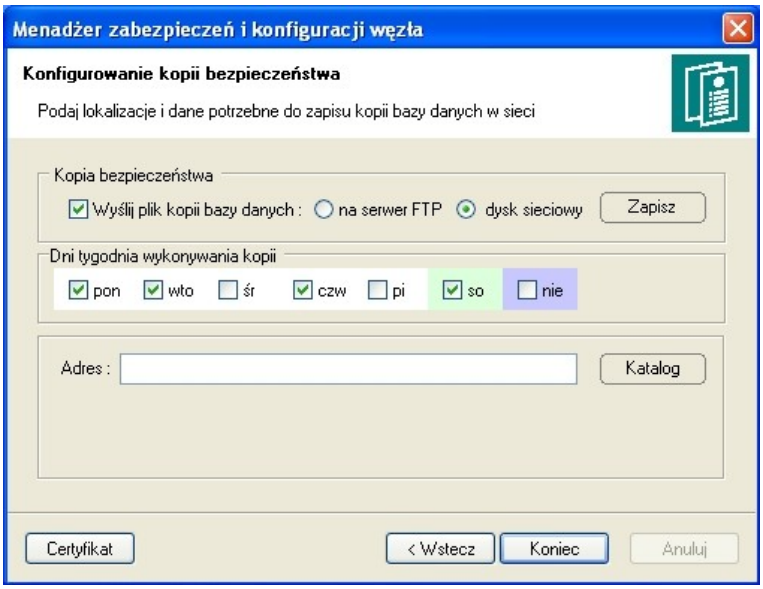
Wciskając klawisz Dalej, przechodzimy do następnego okna programu. W górnej części okna widać dostępne usługi dodatkowe serwera (np. usługa serwera www umożliwiającego podgląd raportów indywidualnych przez pracowników). Usługa ta jest dostępna, jeżeli została wykupiona odpowiednia licencja umożliwiająca podgląd raportów przez przeglądarkę internetową.

Na polu w dolnej części okna widoczne są certyfikaty SSL wykorzystywane przez węzeł. Klikając na tym polu prawym klawiszem myszy można dodawać nowe lub usuwać niepotrzebne certyfikaty.



Kopia bezpieczeństwa

Z okna opisującego dodatkowe usługi serwera można przejść do kolejnego okna służącego do ustawiania miejsca wykonywania kopii bezpieczeństwa danych.

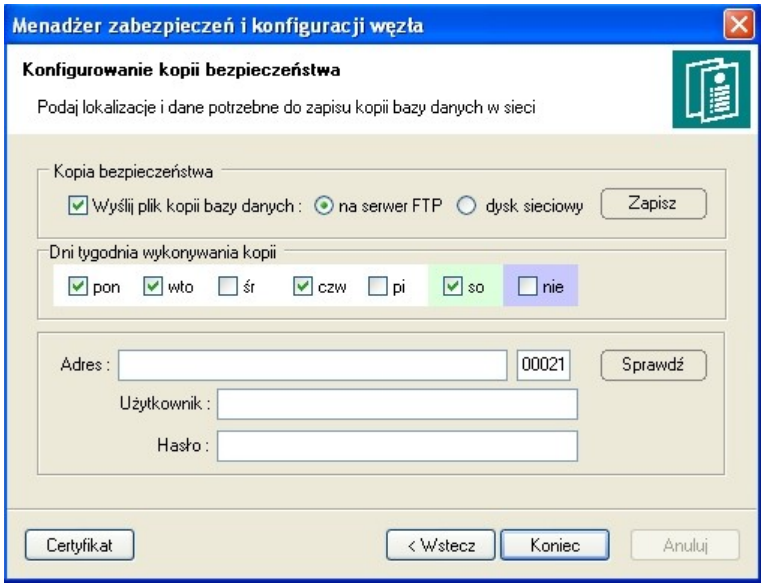


Jeżeli żadna opcja nie jest zaznaczona kopia bezpieczeństwa danych wykonywana jest w katalogu ..\MicroMade/bibinet/Server/Data/Archiwum. Oprócz tego do wyboru są dwie opcje:

kopia bezpieczeństwa wykonywana jest na dysku sieciowym w wyznaczone dni tygodnia

kopia bezpieczeństwa wykonywana jest na wybranym serwerze FTP

Dzięki powyższym ustawieniom uszkodzenie dysku twardego, na którym zainstalowany jest program nie przekreśla możliwości odtworzenia systemu po awarii komputera.



Usługa biguard

Usługa biguard uruchamia serwer bibinet zawsze, jak włączony jest komputer. Powinna być bezwzględnie uruchomiona na węźle sieci, do której są dołączone terminale. Umożliwia ona uruchomienie programów bibi.net na terminalach w dowolnej chwili - zawsze będą mogły połączyć się z serwerem bibinet i uzyskać potrzebne dane.

Usługa biguard powinna być sterowana wyłącznie przez program biserver. Jeżeli został wybrany wysoki poziom zabezpieczeń komunikacji z terminalami usługa jest automatycznie włączana. Jeżeli wybrany został inny poziom zabezpieczeń komunikacji z terminalami, usługa biguard jest automatycznie wyłączana, a tym samym wyłączany jest serwer bibinet. Może to wykorzystać przy konieczności zatrzymania serwera bibinet.

Wskazane jest uruchomienie usługi biguard na wszystkich węzłach sieci. Dzięki temu, zbierane będą wszystkie rejestracje z urządzeń i wymieniane dane między węzłami, nawet jeżeli nikt nie uruchomi programu bibi.

6.5.3 Program biclient - konfigurowanie terminali

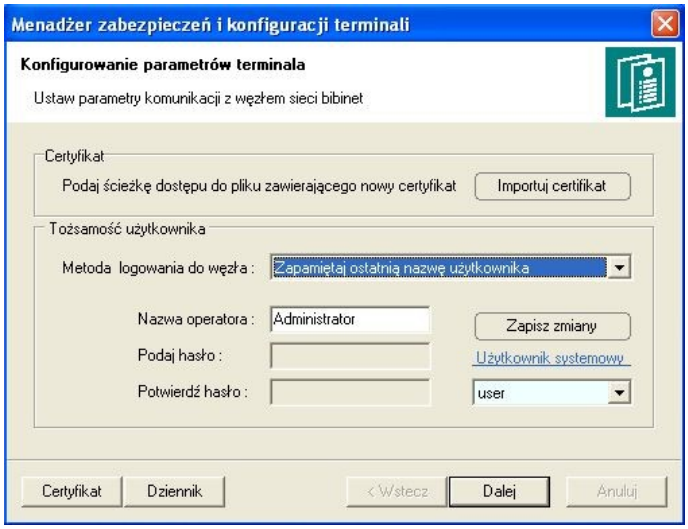
W systemie Windows 7/ 8/10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”.

Program biclient służy do konfigurowania komputerów, które mają pełnić rolę terminali w sieci bibi. Umożliwia on odnalezienie serwera programom uruchomionym na terminalu.

Dodatkowo program biclient ustawia sposób logowania się do programów. Dlatego może być celowe uruchomienie jego również na węźle sieci bibi.net.

Do zalogowania się do programu biclient potrzebny będzie tymczasowo klucz HAK2. Może on być wzięty z węzła sieci - później nie będzie on już potrzebny. W czasie normalnej pracy programów na terminalu wszystkie hasła sprawdzane są przez serwer. Tak więc osoby logujące się na terminalu muszą być wpisane do kluczy włożonych w serwerze.

Po zalogowaniu się włącza się główne okno programu biclient. W oknie tym znajdują się dwie oddzielne ramki, odpowiedzialne za poszczególne zadania.



Certyfikat

Należy nacisnąć klawisz *Importuj certyfikat* i wskazać lokalizację certyfikatu wygenerowanego na węźle. Zaimportowany certyfikat można obejrzeć - klawisz *Certyfikat*. Powinien on wyglądać dokładnie tak samo, jak certyfikat wygenerowany na węźle.

Tożsamość użytkownika

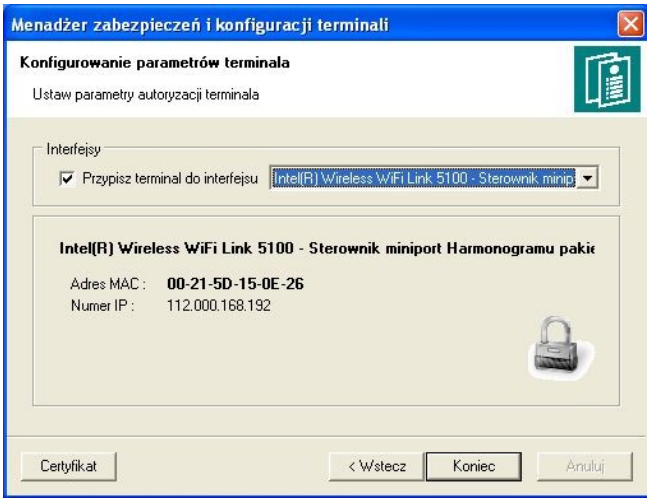
Można tutaj ustawić sposób logowania się do programu bibi. Można to zrobić niezależnie dla różnych osób.

- Wybrać użytkownika systemowego - czyli nazwę użytkownika logującego się do komputera.
- Wybrać metodę logowania się do węzła:
  - Zawsze pytaj o nazwę użytkownika i hasło
    Nazwę użytkownika i hasło trzeba zawsze wpisać przy logowaniu się
  - Zapamiętaj ostatnią nazwę użytkownika
    Program sam wpisze nazwę użytkownika, natomiast hasło trzeba będzie wpisać samodzielnie
  - Zawsze loguj jako ten użytkownik
    Okno logowania w ogóle nie pojawi się - program zaloguje użytkownika używając podanej tutaj nazwy i hasła
- W zależności od wybranej metody logowania się, wypełnić pola nazwa i hasło
- Nacisnąć klawisz *Zapisz zmiany*

Powtórzyć powyższą procedurę dla wszystkich osób, które będą logować się do programów bibi.net.

Interfejsy

Wciskając klawisz *Dalej* można przejść do następnego okna programu, w którym wybiera się kartę sieciową, która ma służyć do autoryzacji terminala w sieci bibinet. Dotyczy to głównie komputerów posiadających więcej niż jedną kartę sieciową.



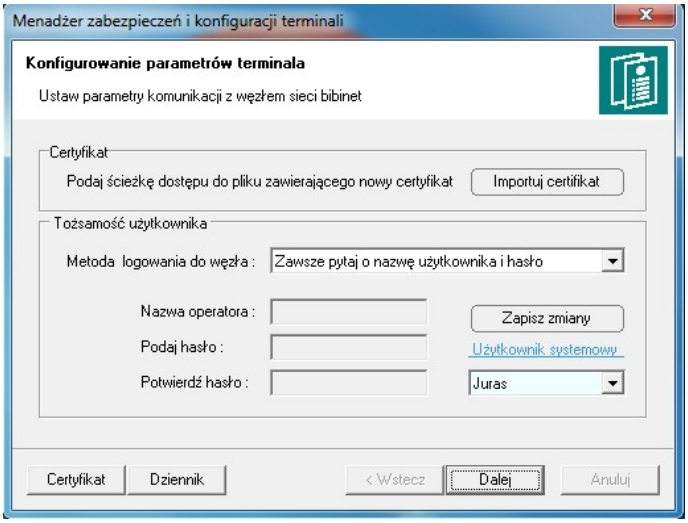
6.5.4 Program biclient - ustawienie sposobu logowania do programu

W systemie Windows 7/8/10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”.

Na węźle sieci może zachodzić potrzeba uruchomienia programu biclient w celu ustalenia sposobu logowania się użytkowników do aplikacji użytkowych. Program biclient nie może zostać uruchomiony, jeżeli pracuje serwer bibinet (nie będzie możliwości zalogowania się). Sytuacja taka ma miejsce, jeżeli w programie biserver został ustawiony wysoki poziom zabezpieczeń komunikacji z terminalami, a tym samym serwer bibinet pracuje cały czas.

W celu zatrzymania pracy serwera bibinet należy uruchomić program biserver i przełączyć poziom zabezpieczeń komunikacji z terminalami na niski. Następnie nacisnąć klawisz *Wprowadź nowe zasady* (nie restartować windows)i zamknąć program.

Teraz można już uruchomić program biclient i wprowadzić potrzebne ustawienia. Po zakończeniu pracy z programem biclient należy ponownie uruchomić program biserver i włączyć poprzednie ustawienia.



W następnej zakładce programu (przycisk Dalej) można ustawić numer karty sieciowej po której rozpoznawany będzie terminal (komputer) w systemie bibinet.

6.5.5 Program biSprzęt

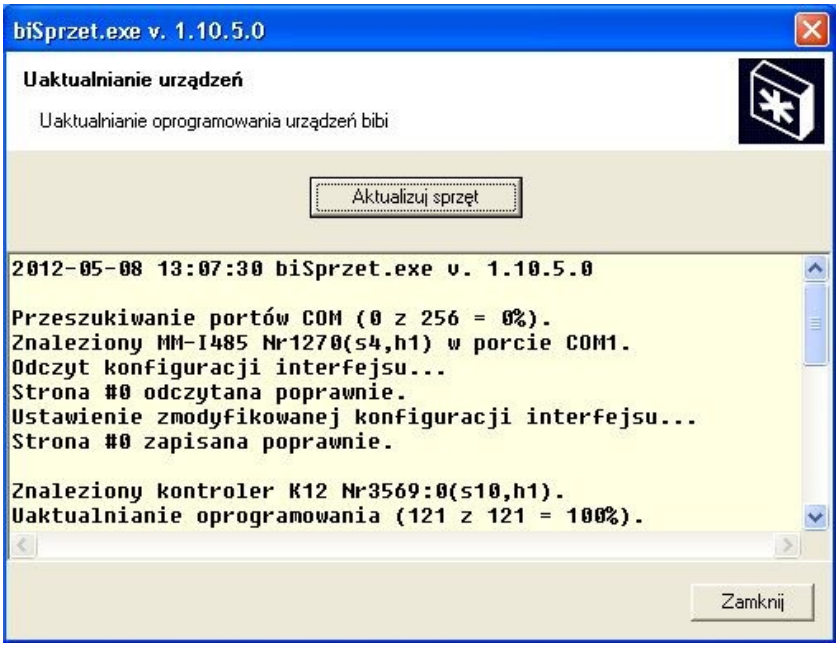
Program nie ma zastosowania do kontrolerów bibi-K22 i bibi-K25 oraz kontrolerów bibi-K12 podłączonych do węzła przez interfejs bibi-F22.

Program służy do aktualizacji oprogramowania w kontrolerach systemu bibinet podłączonych przez interfejs bibi-F21 do komputera zarządzającego. Przed uruchomieniem programu należy zamknąć wszystkie programy bibi uruchomione na komputerze.

Po otwarciu programu należy wcisnąć klawisz Aktualizuj sprzęt. Oprogramowanie w kontrolerach i interfejsach podłączonych do komputera zostanie zaktualizowane do wersji zbieżnej z używaną wersją programu bibi.

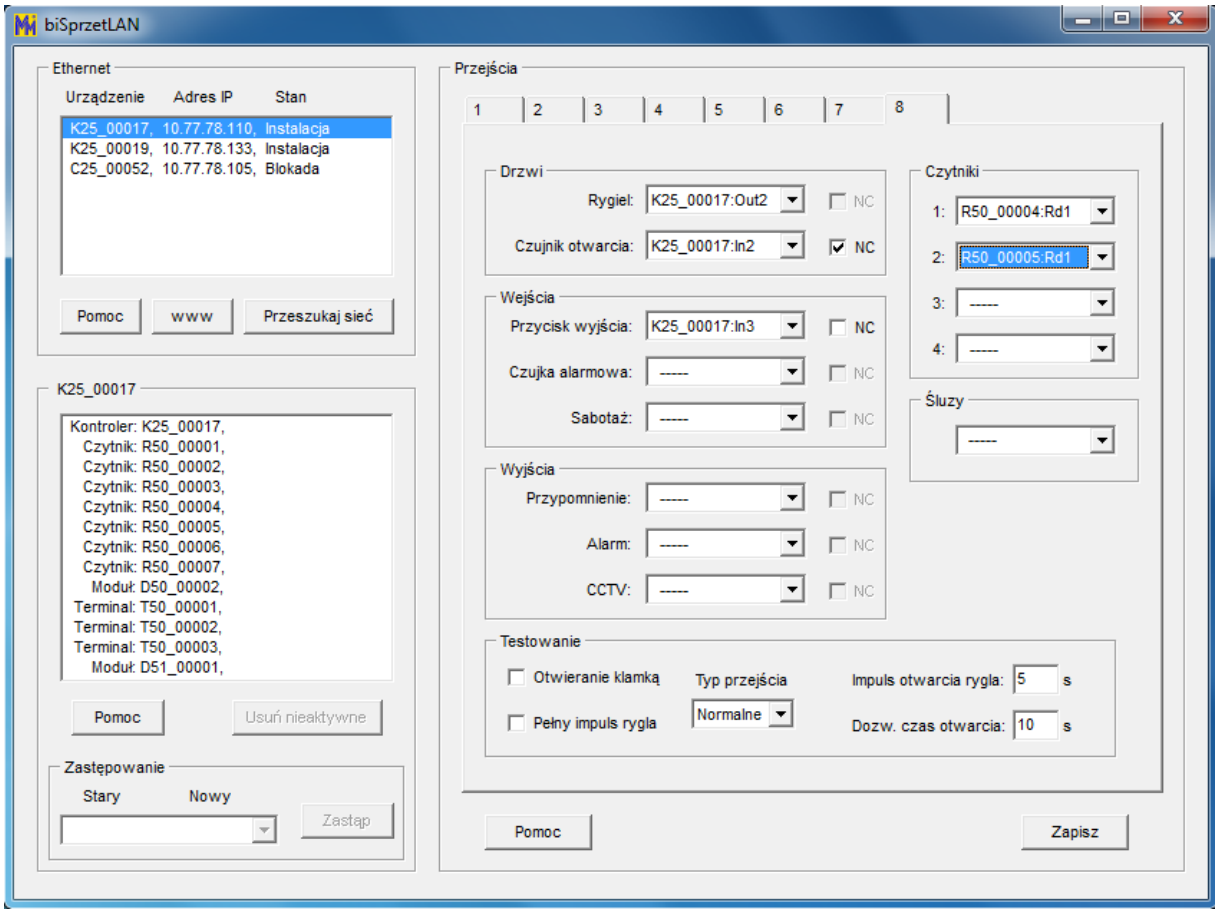
Log z tego upgrade zostanie zapisany na dysku w katalogu Tools.

Jeżeli program biSprzęt nie wykryje żadnego sprzętu podłączonego do komputera należy sprawdzić połączenia urządzeń (okablowanie) i ich zasilanie.

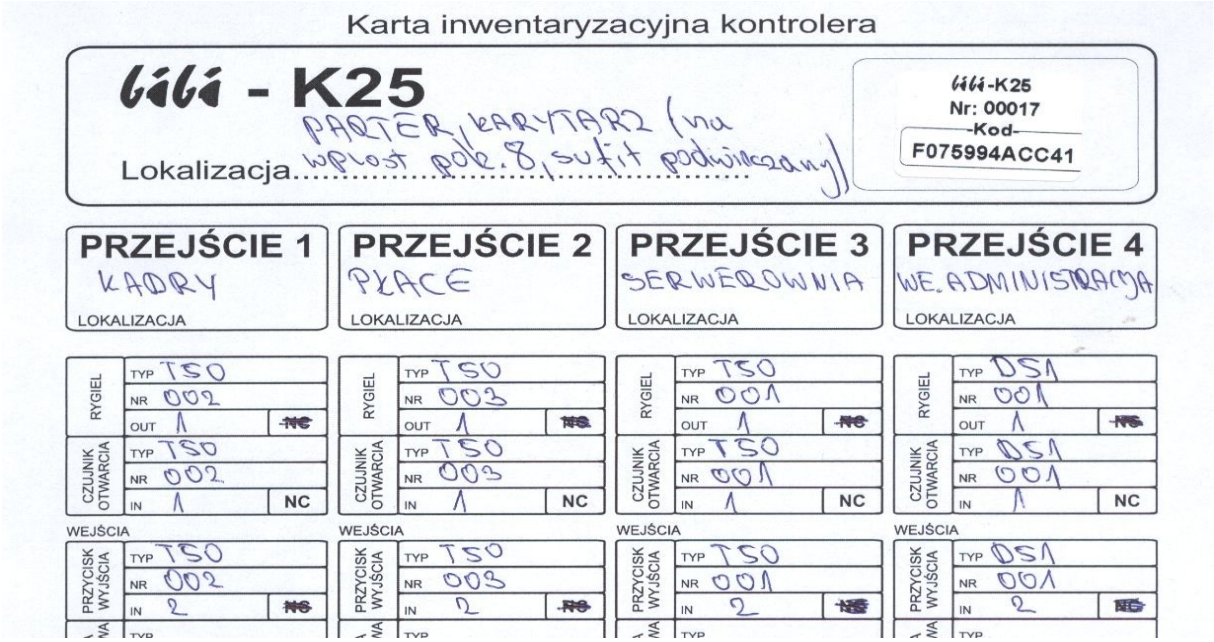


6.5.6 Program biSprzętLAN – wstępna konfiguracja kontrolerów bibi-K22 i bibi-K25

Program służy do wstępnej konfiguracji kontrolerów **bibi-K22** i **bibi-K25** oraz podłączonych do nich urządzeń: czytników, terminali, modułów rozszerzeń itp. Dzięki niemu można zaraz po zamontowaniu urządzeń przeprowadzić ich wstępną konfigurację i wykonać pierwsze testy poprawności działania. Wpisana do kontrolera konfiguracja jest zapisywana w jego pamięci. Po przypisaniu kontrolera do instalacji w programie bibi jest widoczna w oknie *Opcje systemu bibi*.



Bardzo przydatna do ustawienia konfiguracji jest **karta inwentaryzacyjna kontrolera**, którą wypełnia się podczas montażu poszczególnych elementów systemu.


Karta inwentaryzacyjna kontrolera

bibi - K25

Lokalizacja PARTER, KARYTARZ (na wprost pok. 8, sufit podwieszany)

bibi-K25 Nr: 00017 -Kod- F075994ACC41

PRZEJŚCIE 1	PRZEJŚCIE 2	PRZEJŚCIE 3	PRZEJŚCIE 4
KADRY	PŁACE	SERWEROWNIA	WE. ADMINISTRACJA
LOKALIZACJA	LOKALIZACJA	LOKALIZACJA	LOKALIZACJA
RYGIEL TYP TSO NR 002 OUT 1 NC	RYGIEL TYP TSO NR 003 OUT 1 NC	RYGIEL TYP TSO NR 001 OUT 1 NC	RYGIEL TYP DS1 NR 001 OUT 1 NC
CZUJNIK OTWARCIA TYP TSO NR 002 IN 1 NC	CZUJNIK OTWARCIA TYP TSO NR 003 IN 1 NC	CZUJNIK OTWARCIA TYP TSO NR 001 IN 1 NC	CZUJNIK OTWARCIA TYP DS1 NR 001 IN 1 NC
WEJŚCIA	WEJŚCIA	WEJŚCIA	WEJŚCIA
PRZYCISK WYJŚCIA TYP TSO NR 002 IN 2 NC	PRZYCISK WYJŚCIA TYP TSO NR 003 IN 2 NC	PRZYCISK WYJŚCIA TYP TSO NR 001 IN 2 NC	PRZYCISK WYJŚCIA TYP DS1 NR 001 IN 2 NC

W karcie wpisuje się miejsce zamontowania urządzenia (np. pokój nr 305), jego typ (np. czytnik bibi-R50), numer fabryczny SN (np. 0254) i funkcję, którą wykonuje (np wejście RCP). Dzięki tym informacją konfiguracja urządzeń programem **biSprzętLAN** i potem programem **bibi** jest bardzo łatwa.

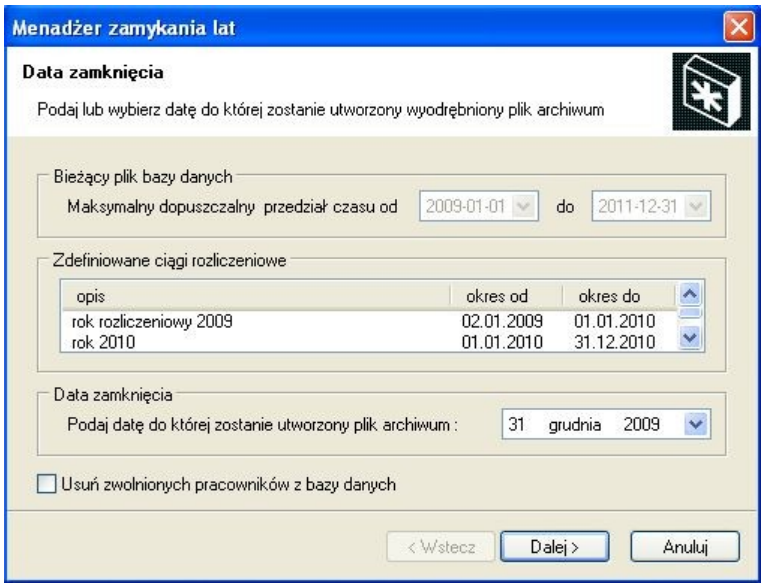
6.5.7 Archiwizacja starych okresów rozliczeniowych - program biArchiver

W systemie Windows 7/8/10 program należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator".

Jeżeli w edycji okresów rozliczeniowych opcja *Dodaj ciąg rozliczeniowy* jest nieaktywna to oznacza, że znaleźliśmy się poza zdefiniowanym przedziałem czasu dla naszego programu. Przedział ten może obejmować maksymalnie 3 lata danych, z których program oblicza raporty.

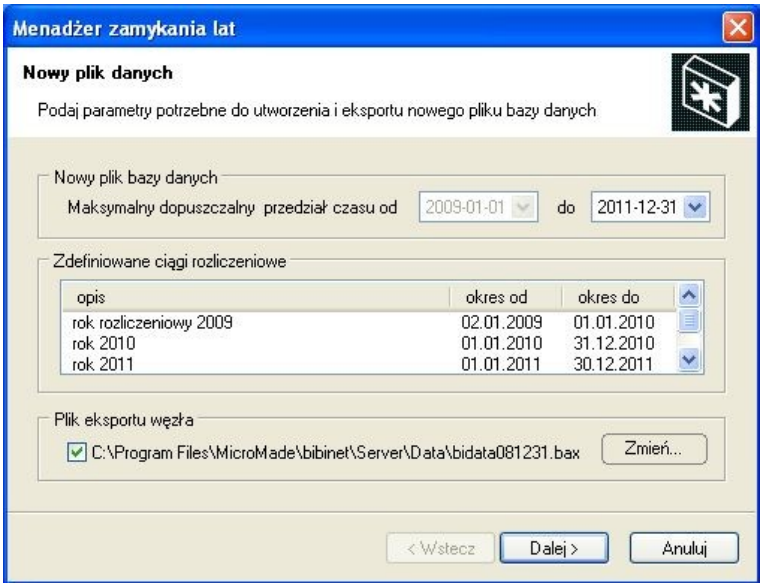
Załóżmy, że chcemy dodać okres rozliczeniowy, który jest rokiem kalendarzowym 2012.

W takim przypadku należy zamknąć program bibi, a następnie za pomocą programu narzędziowego biArchiver zarchiwizować rok 2009.



W programie tym należy wykonać 3 kroki:

1. Otworzyć program biArchiver (skrót na pulpicie "bibi - programy narzędziowe" lub katalog ..\MicroMade\bibinet\Tools). Zalogować się jako Administrator, w dolnej części ekranu ustawić datę do której będzie utworzony plik archiwum na 31 grudnia 2009r., wcisnąć przycisk *Dalej*. Program dokona podziału pliku bazy danych.
2. Po tej operacji odblokuje się *Maksymalny dopuszczalny przedział czasu* do daty 2012-12-31. Można ją zmienić na 2013-12-31 rozwijając strzałkę z prawej strony pola i wybierając odpowiednią datę w kalendarzu. Gdy mamy więcej niż jeden węzeł w systemie bibinet to należy dodatkowo zaznaczyć pole *Plik eksportu węzła*.



3. **Następnie wcisnąć przycisk *Dalej***. Program dokona poszerzenia aktualnej bazy danych do 2012-12-31. Gdy na ekranie pojawi się napis *Zamykanie lat zakończone* można zamknąć program.

Po wykonaniu operacji zamknięcia lat, w programie bibi dostępna będzie funkcja dodawania nowych okresów rozliczeniowych.

Jeżeli w systemie mamy więcej niż jeden węzeł to należy skopiować do niego Plik eksportu węzła. Na nowym węźle należy kliknąć na nazwę tego pliku prawym klawiszem myszy i wybrać funkcję Zainstaluj. Otworzy się program narzędziowy biserver, w którym należy wcisnąć klawisz Zlokalizuj bazę danych, ustawić poziom zabezpieczeń zew. połączeń na wysoki, kliknąć Wprowadź nowe zasady i zamknąć program.

Operację należy powtórzyć na wszystkich węzłach systemu bibinet.

6.6 Pomoc świadczona przez instalatora systemu

6.6.1 Dane teleadresowe instalatora/dealera systemu

Aby przy wywołaniu menu Pomoc/Instalator systemu otworzyło się okno z danymi instalatora /dealera systemu należy:

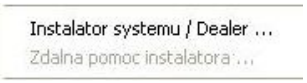
- odszukać w kartotece Doc (standardowo: Program Files\MicroMade\bibinet\Doc) plik dealer.dsc
- otworzyć go przy pomocy edytora tekstów np. WordPad
- wpisać nazwę, adres, telefon itp.
- zapisać pod taką samą nazwą

Po wykonaniu tych czynności w oknie Instalator będą widoczne dane niezbędne do kontaktu z instalatorem systemu .

6.6.2 Zdalna pomoc wykonywana przez instalatora

Aby uaktywnić funkcję zdalnej pomocy wykonywanej przez instalatora należy do katalogu Doc (standardowo: Program Files\MicroMade\bibinet\Doc) wgrać plik programu zdalnej pomocy (np. TeamViewer.exe lub podobny). Zmienić nazwę tego pliku na dealer.exe .

Funkcja *Zdalna pomoc instalatora* w programie bibi będzie aktywna



7. Rozwiązywanie problemów

7.1 Uszkodzenie lub wymiana komputera, na którym był zainstalowany program

7.1.1 Instalacja z jednym węzłem systemu bibinet

W takim przypadku należy:

Zainstalować na nowym komputerze węzeł systemu bibinet (bez wytwarzania nowej bazy danych)

Skopiować dane czyli zawartość całego katalogu Data (standardowo C:\Program Files\MicroMade\bibinet\Serwer\Data) ze starego komputera wgrać do katalogu Data, który powstał po instalacji programu na nowym komputerze.

uruchomić program narzędziowy biserver.exe

- zalogować się jako administrator
- wydać polecenie: zlokalizuj bazę danych (każda baza danych musi być przypisana do danego komputera)
- ustawić poziom zabezpieczeń komunikacji z terminalami najlepiej wysoki jeżeli podłączone są terminale, niski jeżeli rzadko używa się bibi
- wydać polecenie "wprowadź nowe zasady" - na pytanie o reset komputera można odpowiedzieć NIE
- zamknąć program biserver

Uruchomić program bibi

- otworzyć okienko Opcje systemu bibinet
- ustawić się w prawej części okienka na nazwie komputera (będzie przekreślona)
- kliknąć podwójnie myszą - otworzy się okienko Edycja parametrów komputera
- wprowadzić dane nowego komputera (adres MAC i nr IP)- zakończyć OK
- jeżeli urządzenia są podłączone do tego samego COMu (np.COM1) jak w starym komputerze, to powinny zostać znalezione.
- jeżeli są podłączone do innego COMu, to należy usunąć dostawcę, a następnie dodać nowego dostawcę z ustawionym odpowiednim COMem.

I to już koniec - wszystko powinno być jak na poprzednim komputerze

Taką samą procedurę należy wykonać przy zmianie karty sieciowej (płyty głównej) w komputerze

7.1.2 Instalacja z wieloma węzłami systemu bibinet

Wykorzystamy fakt, że na każdym węźle sieci bibinet jest taka sama baza danych programu:

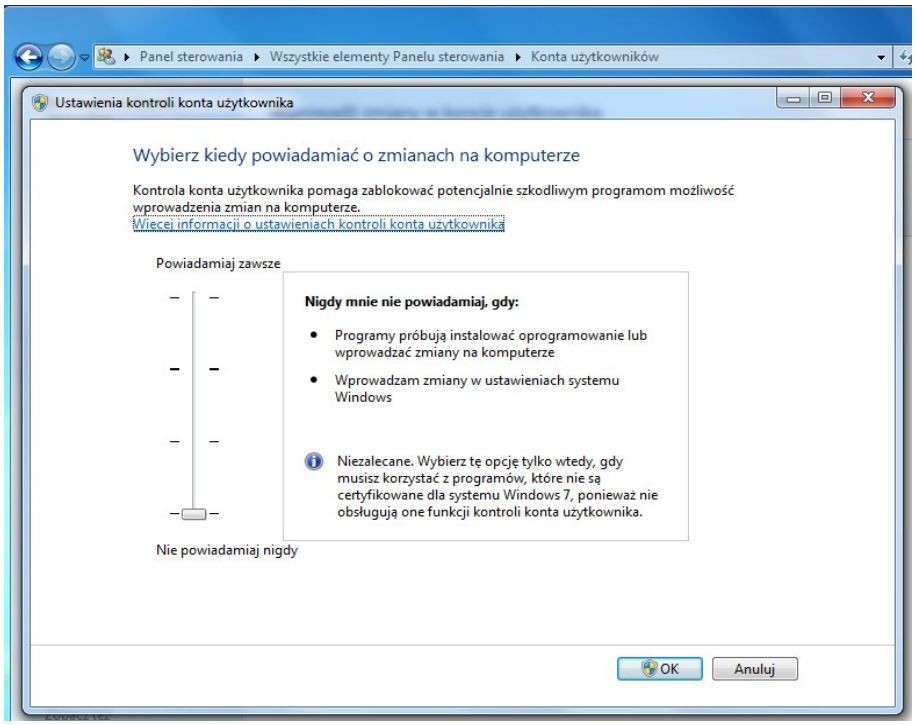
- otworzyć program bibi na jednym z działających węzłów
- w oknie opcje systemu bibi ustawić kursor na nazwie zakładu pracy
- w prawej części okna (Deklaracja komputerów w sieci bibi) znaleźć uszkodzony węzeł.
- usunąć podpięte do niego terminale
- następnie dwa razy klikając myszą na jego nazwie wejść w okno edycji węzła
- ustawić parametry (MAC, nr IP) nowego komputera, zatwierdzić
- dodać terminale
- zamknąć program bibi
- zamknąć wszystkie aplikacje bibi na komputerach
- na każdym węźle uruchomić program narzędziowy biserver i wybrać poziom zabezpieczeń komunikacji z terminalami na niski, wprowadź nowe zasady, nie restartować systemu Windows

- zainstalować na nowym komputerze węzeł systemu bibinet (bez wytwarzania nowej bazy danych)
- włożyć klucz bibi.HAK do złącza USB
- przekopiować bazę danych bidata.bdb (C:\Program Files\MicroMade\bibinet\Server\Data) na nowy komputer do analogicznego katalogu
- bazę danych (bidata.bdb) ze zmienionym komputerem przegrać na pozostałe węzły
- na każdym węźle uruchomić program narzędziowy biserver i wybrać poziom zabezpieczeń komunikacji z terminalami na wysoki, wprowadź nowe zasady, nie restartować systemu Windows

Instalacja z nowych węzłem powinna działać poprawnie. Jeżeli do nowego węzła mają być podpięte terminale to należy dodatkowo w programie narzędziowym biserver wyeksportować certyfikat i zaimportować go programem narzędziowym biclient na terminalach.

7.2 Kłopot z instalacją bazy danych pod Windows 7/8/10.

Należy pamiętać, że instalację programu należy przeprowadzić na koncie Administratora komputera. Dodatkowo należy sprawdzić czy Administrator ma wyłączoną funkcję kontroli konta użytkownika. W tym celu trzeba otworzyć *Panel sterowania* i w sekcji *Konta użytkowników* przesunąć suwak (wybrać opcję) *Nie powiadamiaj nigdy*.

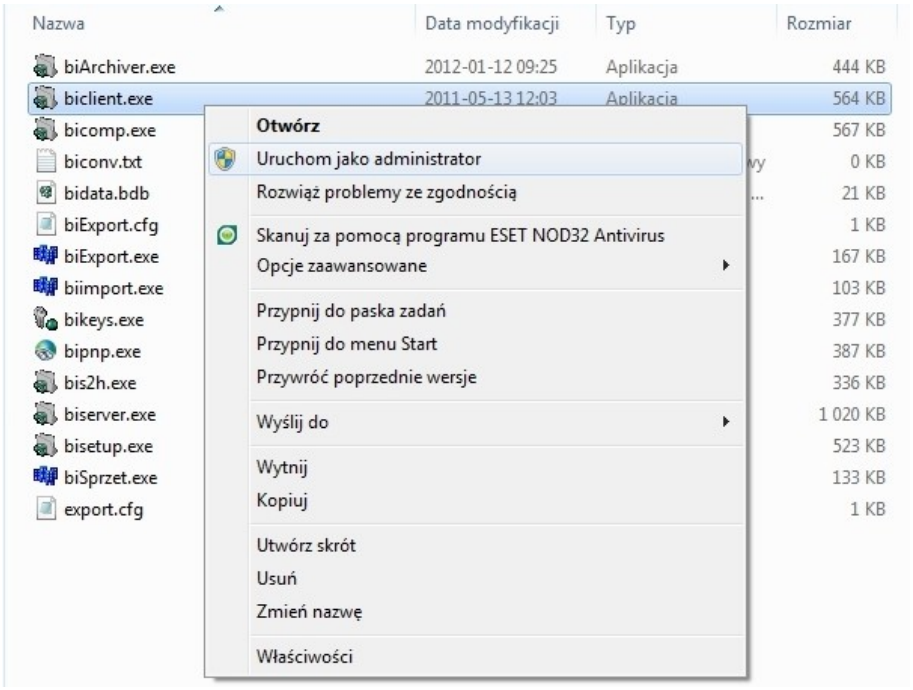


W ten sposób wyłączamy blokadę instalacji programów nie posiadających certyfikatu zgodności z Windows 7. Jeżeli nie wyłączymy tej opcji to w drugim kroku instalacji przy wytwarzaniu bazy danych (rozdział 4.2.2) system zgłosi błąd niepoprawnego wytworzenia bazy danych.

7.3 Uruchamianie programów narzędziowych pod systemem Windows 7/8/10

Programy narzędziowe systemu bibinet znajdujące się w katalogu MicroMade/bibinet/Tools (skrót na Pulpicie: bibi - programy narzędziowe) należy uruchamiać będąc zalogowanym na koncie Administratora systemu Windows. Dodat-

kowo w systemie Windows 7 programy te należy uruchamiać z menu kontekstowego (prawy klawisz myszy) wybierając opcję „Uruchom jako administrator”



Przy standardowym uruchamianiu niektóre funkcje programu mogą być niedostępne. Na przykład w programie narzędziowym biclient.exe funkcja „Importuj certyfikat” może być nieaktywna.

7.4 Kłopot z uruchomieniem programu bibi.exe pod systemami Windows 2003/2008/2012/2016/2019 Server

Aby uruchomić program bibi.exe pod systemami Windows 2003/2008/2012 Server należy :

- Zalogować się do systemu Windows jako Administrator
- Uruchomić shella – cmd.exe (menu Start - Uruchom)
- Wydać polecenie: "bcdedit.exe /set {current} nx OptIn",
  lub ewentualnie: "bcdedit.exe /set {current} nx AlwaysOff"
- Zrestartować system

Operacja ta włącza funkcje DEP tylko dla aplikacji systemowych i usług (ewentualnie wyłącza funkcje DEP dla całego systemu - AlwaysOff), co pozwala na pracę programu bibi.exe.

W Windows 2003 Server funkcja ta jest standardowo wyłączona, zaś w systemie Windows 2008/2012 Server włączona.

Ustawienia funkcji DEP można zmienić też w inny sposób w Panel sterowania wybierając: Wszystkie elementy Panelu sterowania →System→Zaawansowane ustawienia systemu→Wydajność → ustawienia. Następnie wybrać:

"Zapobieganie wykonywaniu danych" i należy zaznaczyć "Włącz funkcję DEP tylko dla istotnych programów i usług systemu Windows" (wymaga restartu serwera) albo dodać program bibi.exe do wyjątków (nie wymaga restartu) i kliknąć "Zastosuj".

7.5 Nie można dodać nowego okresu rozliczeniowego (nowego roku rozliczeniowego) w programie bibi

Jeżeli w edycji okresów rozliczeniowych opcja Dodaj ciąg rozliczeniowy jest nieaktywna to oznacza, że znaleźliśmy się poza zdefiniowanym przedziałem czasu dla naszego programu. Przedział ten może obejmować maksymalnie 3 lata danych, z których program oblicza raporty.

Załóżmy, że chcemy dodać okres rozliczeniowy, który jest rokiem kalendarzowym 2016.

W takim przypadku należy zamknąć program bibi, a następnie za pomocą programu narzędziowego biArchiver zarchiwizować rok 2014.

W programie tym należy wykonać 2 kroki:

Otworzyć program biArchiver (skrót na pulpicie "bibi - programy narzędziowe" lub katalog ..\MicroMade\bibinet\Tools), zalogować się jako Administrator, w dolnej części ekranu ustawić datę do której będzie utworzony plik archiwum na 31 grudnia 2014r., wcisnąć przycisk Dalej. Program dokona podziału pliku bazy danych.

Po tej operacji odblokuje się Maksymalny dopuszczalny przedział czasu do daty 2016-12-31. Można ją zmienić na 2017-12-31 rozwijając strzałkę z prawej strony pola i wybierając odpowiednią datę w kalendarzu. Gdy mamy więcej niż jeden węzeł w systemie bibinet to należy dodatkowo zaznaczyć pole "Plik eksportu węzła". **Następnie wcisnąć przycisk Dalej**. Program dokona poszerzenia aktualnej bazy danych do 2015-12-31. Gdy na ekranie pojawi się napis "Zamykanie lat zakończone" można zamknąć program.

Opis programu biArchiver znajduje się w instrukcji obsługi programu.

Po wykonaniu operacji zamknięcia lat, w programie bibi dostępna będzie funkcja dodawania nowych okresów rozliczeniowych.

7.6 Komputer nie podłączony do sieci komputerowej

Warunkiem poprawnej pracy programu bibi.net jest dostęp programu do adresu MAC karty sieciowej. W tym celu należy w „Panelu sterowania" otworzyć okienko „Połączenia sieciowe" i sprawdzić stan „Połączenia lokalnego". Jeżeli jest wyłączony, to należy go włączyć. Ponieważ komputer jest odłączony od sieci, więc zamiast stanu „włączony" będzie napisane „Kabel sieciowy odłączony" - to nie przeszkadza w pracy systemu bibi.net.

Przy dodawaniu komputera w okienku „Opcje systemu bibi" należy wpisać właściwy Adres fizyczny MAC, natomiast jako numer IP należy podać 127.000.000.001 (jest to adres zarezerwowany i oznacza lokalny komputer).

7.7 Węzły bibinet w domenach połączonych poprzez Neostradę.

W neostradzie nie ma na stałe przydzielonych numerów IP. Każdą domenę połączoną do internetu przez neostradę trzeba zarejestrować w dynamicznym serwerze DNS. Można to na przykład zrobić w serwerze DynDNS.org .

7.8 Kłopot z podłączeniem terminala do węzła postawionego na Windows Home

W Windows serii Home są ograniczenia w stosunku do serii Professional mimo, że ustawienia sieci można w obu programach wykonać identycznie (stały adres IP, DNSy, itd.).

Ograniczenie dotyczy tylko dołączania terminali do serwera postawionego na wersji Home. W wersjach Home ustawiona jest na stałe flaga „loguj z zewnątrz jako gość". Nie pozwala to na bezpieczne logowanie z zewnątrz do serwera bibinet. Dlatego nie można na Windows Home skonfigurować węzła do którego podłączone są terminale.

7.9 Kłopot z reinstalacją programu do wersji 1.10

Reinstalacja do wersji 1.10 jest możliwa **tylko z wersji 1.9** . Jeżeli konieczna jest reinstalacja z wersji wcześniejszej (numer wersji znajduje się w prawym górnym rogu głównego okna programu bibi) to należy najpierw pobrać ze strony http://pliki.micromade.pl/archiwum/bibinet_setup_19.zip wersję 1.9 programu.

- Rozpakować i uruchomić instalator, który dokona uaktualnienia programu.
- Następnie uruchomić program narzędziowy bisprzęt i zaktualizować kontrolery do wersji 1.9.
- Uruchomić program bibi w wersji 1.9 w celu przepisania ustawień kontrolerów.
- Zamknąć program bibi.
- Uruchomić instalator wersji 1.10

Uwaga!

Operacje powyższe są dostępne tylko dla użytkowników posiadających aktualną licencję (nie starszą niż rok) lub mają wykupiony abonament na pomoc techniczną.

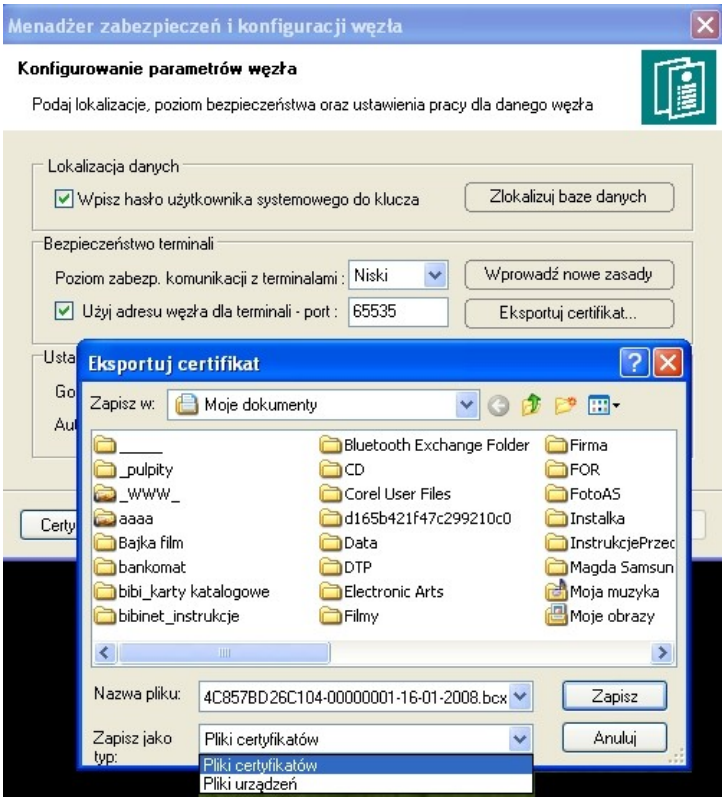
Przy reinstalacji postępować zgodnie z opisem zamieszczonym w rozdziale 4.1

7.10 Kłopot z przypisaniem urządzenia sieciowego do instalacji

Standardowo urządzenia sieciowe (np. interfejs bibi-F22, rejestrator bibi-C25, kontrolery bibi-K22 i bibi-K25) otrzymują certyfikat opisujący połączenie z węzłem sieci bibinet poprzez powiadomienia rozsyłane przez serwer w sieci lokalnej (tzw.broadcast'y). Jeżeli połączenie następuje poprzez sieć internet, urządzenie łączy się z domeną techniczną bibi.pl, z której pobiera odpowiedni certyfikat.

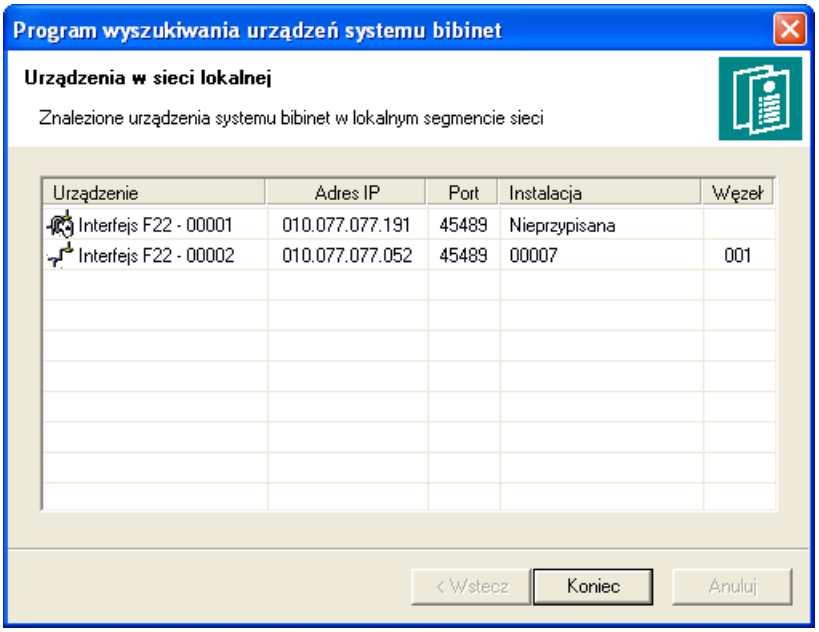
Jeżeli urządzenie podłączone jest w innej podsieci, do której nie docierają powiadomienia (np. są blokowane przez routery) konieczne jest „ręczne" dostarczenie certyfikatu do urządzenia.

W tym celu należy wyłączyć wszystkie aplikacje bibi korzystające z usług bibinet serwera, a następnie uruchomić program narzędziowy biServer. Wybrać opcję *Eksportuj certyfikat*, rozwinąć opcję *Zapisz jako typ*: Pliki urządzeń.



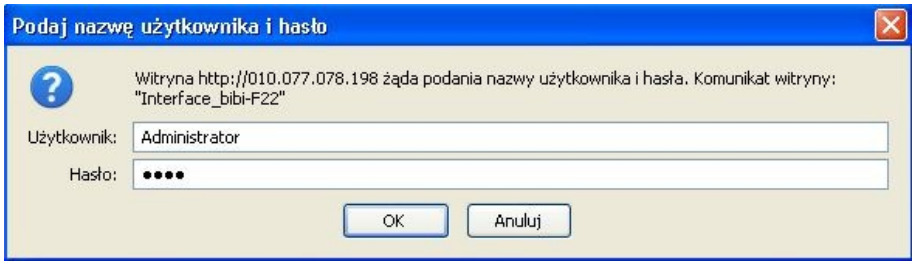
Następnie należy połączyć się z serwerem www urządzenia sieciowego. Można to uzyskać poprzez wpisanie jego adresu w przeglądarce internetowej (np.192.168.1.1xx). Możliwa jest sytuacja, że nie znamy tego numeru - na przykład jeżeli numer IP został nadany przez serwer DHCP. Do wyszukania wszystkich urządzeń sieciowych systemu bibi zainstalowanych w sieci lokalnej służy program bipnp.exe. Program ten znajduje się w katalogu Tools instalacji bibinet. Po uruchomieniu programu zobaczymy okienko ze wszystkimi zainstalowanymi interfejsami.

Program ten może być uruchomiony z dowolnego komputera w sieci LAN - nie musi być na nim instalowany program bibinet. Jednak do uruchomienia programu, w celu zalogowania się do niego, trzeba będzie na chwilę włożyć klucz bibi.HAK z instalacji.



Uwaga!
Program bipnp.exe uruchomiony na tym samym komputerze co węzeł bibinet może utrudnić komunikację interfejs - węzeł. Po wyszukaniu interfejsów program bipnp.exe należy wyłączyć.

Kliknięcie na wybranym interfejsie spowoduje otwarcie strony www interfejsu. Do serwera www należy zalogować się poprzez login: Administrator i hasło: bibi lub hasło zmienione (nadane) przez Administratora.



Pobranie do urządzenia certyfikatu wykonuje się w zakładce Certyfikat. Plik certyfikatu należy wskazać w okienku *Załaduj plik certyfikatu*.
Po operacji Wyślij plik do urządzenia można odświeżyć okno przeglądarki i sprawdzić poprawność załadowanego certyfikatu.

Tak przygotowane urządzenie powinno w ciągu kilku minut pokazać się w oknie Opcje systemu bibi w programie bibi jako aktywne.


MicroMade
bibi-F22
Interfejs Ethernet - RS485 do systemu bibinet
Urządzenie | LAN | Czas | Certyfikat | Dziennik | Hasło | Blokuj | Wyloguj
Urządzenie nieprzypisane do instalacji.
Certyfikat
Informacje o certyfikacie
Ważny od : Brak certyfikatu
Wydany przez :
Sygnatura kodu dostępu :
Instalacja / Domena / Węzeł :
Adres lokalny węzła :
Adres zewnętrzny węzła :
Załaduj plik certyfikatu
Plik certyfikatu
Przeglądaj...
Wyślij plik
© MicroMade. Konfiguracja urządzenia bibi-F22 - interfejs Ethernet-RS485 do systemu bibinet.


MicroMade
bibi-F22
Interfejs Ethernet - RS485 do systemu bibinet
Urządzenie | LAN | Czas | Certyfikat | Dziennik | Hasło | Blokuj | Wyloguj
Możliwość edycji ustawień została zablokowana.
Urządzenie skojarzone z instalacją 39 z węzłem MMPC26.
Certyfikat
Informacje o certyfikacie
Ważny od : 08.05.2012
Wydany przez : MMPC26
Sygnatura kodu dostępu : 1 / 07.02.2106
Instalacja / Domena / Węzeł : 39 / 1 / 1
Adres lokalny węzła : 10.77.78.160 : 45489
Adres zewnętrzny węzła : 255.255.255.255 : 45489
© MicroMade. Konfiguracja urządzenia bibi-F22 - interfejs Ethernet-RS485 do systemu bibinet.

Jeżeli kłopoty z przyłączeniem interfejsu lub rejestratora występują nadal można stan urządzenia zapisać do pliku tekstowego. Można to zrobić w zakładce *Urządzenie* klikając klawisz *Zapisz plik na dysku*.

Taki plik można przeanalizować lub przesłać na adres mm@micromade.pl z prośbą o pomoc w rozwiązaniu problemu.

7.11 Rozbudowa systemu przy braku klucza systemowego

Rozbudowa systemu o nowe serwery bibinet wymaga wytworzenia kolejnych kluczy bibi.HAK zaprogramowanych do danej instalacji. Do tej operacji konieczny jest klucz systemowy, w którym przechowywane jest główne hasło danej instalacji bibinet.

Przy braku klucza systemowego główne hasło tej instalacji musi być powtórnie wygenerowane i zapisane we wszystkich kluczach. Dlatego konieczne jest zebranie wszystkich kluczy bibi.HAK z danej instalacji. Jednocześnie z generowaniem hasła zostanie wytworzony nowy klucz systemowy.

- Zebrać wszystkie klucze z instalacji
- Wyłączyć wszystkie serwery
  - Przełączyć wszystkie serwery w stan niski (programem biServer)
- Zebrać klucze bibi.HAK z serwerów
- Wybrać klucz, który ma być nowym kluczem systemowym - włożyć go do komputera
- Uruchomić program bikeys i postępować podobnie, jak przy pierwszym konfigurowaniu kluczy (opis w rozdziale 4.2.3).
  - zalogować się jako Administrator Systemu
  - wybrać opcję: Generowanie nowego hasła systemowego
  - ustawić się na polu poniżej i z menu kontekstowego wydać komendę: Rozpocząć generowanie
  - po zakończeniu generowania: OK - Dalej - Zapisz hasło - w ten sposób został wytworzony nowy klucz systemowy

- po kolejnej komendzie Dalej widać tabelkę z kluczami
- włożyć do komputera pozostałe klucze (zarówno używane poprzednio w tej instalacji jak i nowe) (jeżeli brakuje złącz USB to można je wkładać kolejno)
- kolejno dla każdego klucza wydać polecenie:
  - Skonfiguruj wybrany klucz...
  - wprowadzić nazwę dla klucza
  - zatwierdzić poprzez Wprowadź

- wydać polecenie Dodaj operatora do wszystkich ...
  - wybrać Administratora i wpisać hasło dla niego
- do poszczególnych kluczy można również dodać innych operatorów
- zakończyć program bikeys

- Skopiować bazę danych na pozostałe serwery bibinet
- Włożyć do serwerów klucze bibi.HAK
- Uruchomić serwery poprzez przełączenie zabezpieczeń komunikacji z terminalami w stan wysoki (program biServer)

Po wykonaniu tych operacji wszystkie serwery powinny się ze sobą komunikować wykorzystując już nowe hasło do kodowania transmisji. Korzystając z nowych kluczy bibi.HAK zaprogramowanych do danej instalacji, można rozbudować system o kolejne serwery.

Nowy klucz systemowy przechować w bezpiecznym miejscu (razem z hasłem Administratora Systemu).

7.12 Brak komunikacji między terminalami a serwerem systemu bibinet

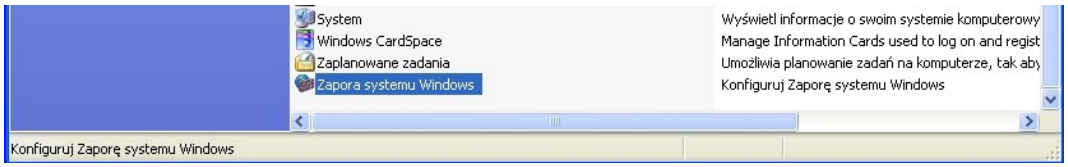
Często po zainstalowaniu terminala systemu bibinet przy otwieraniu programu bibi na tym terminalu nie otwiera się okno logowania . Przyczyną tego jest brak komunikacji między terminalem bibinet a serwerem systemu. Taki stan wynika najczęściej z :

- braku lub niepoprawnego zdefiniowanie terminala w programie bibi na serwerze systemu (opcje systemu bibi / deklaracja komputerów w sieci bibi)
- braku zarejestrowania certyfikatu serwera na terminalu przy pomocy programu biclient
- źle ustawionej zapory systemu Windows lub źle skonfigurowanego programu antywirusowego
- blokady portu RPC

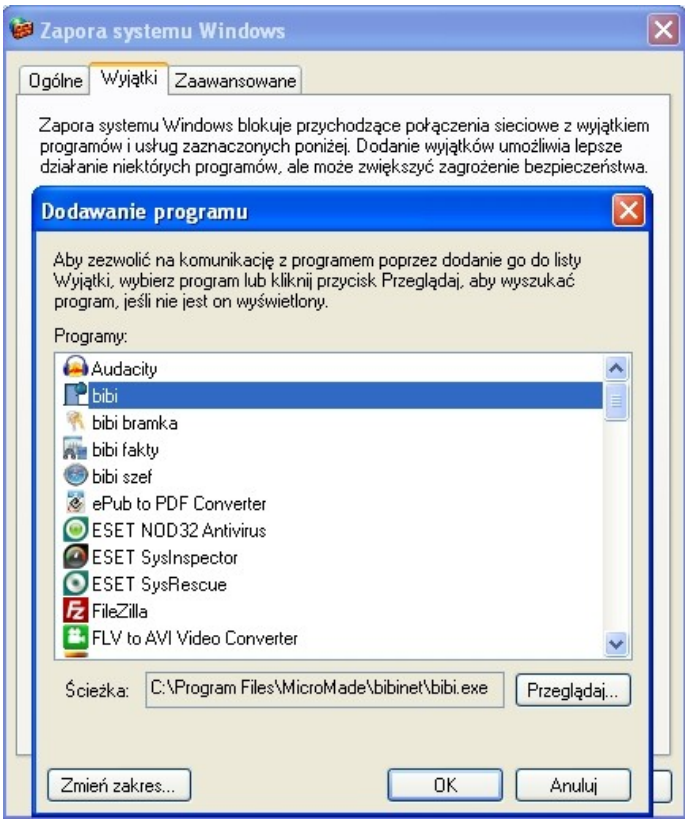
Opis pierwszych dwóch punktów znajduje się w rozdziale 6.2 niniejszej instrukcji. Problemy zawarte w trzecim i czwartym punkcie **powinien rozwiązać administrator lokalnej sieci komputerowej.**

7.12.1 Ustawienie zapory systemu Windows

Ustawienie wyjątku dla aplikacji bibi w zaporze systemu Windows należy rozpocząć od wybrania z menu Start opcji Panel sterowania i dalej Zapora systemu Windows.



Następnie należy dodać aplikację bibi do wyjątków, które nie będą filtrowane przez zaporę systemu Windows.

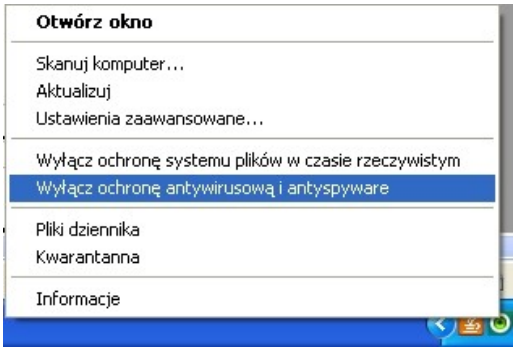


7.12.2 Ustawienie programu antywirusowego

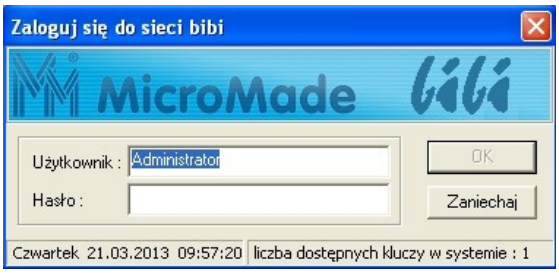
Obecnie najczęściej nad bezpieczeństwem komunikacji w systemie Windows czuwa program antywirusowy.

Poniżej została opisana przykładowa konfiguracja programu antywirusowego NOD32 firmy ESET. Ustawienia innych programów antywirusowych wykonuje się w podobny sposób.

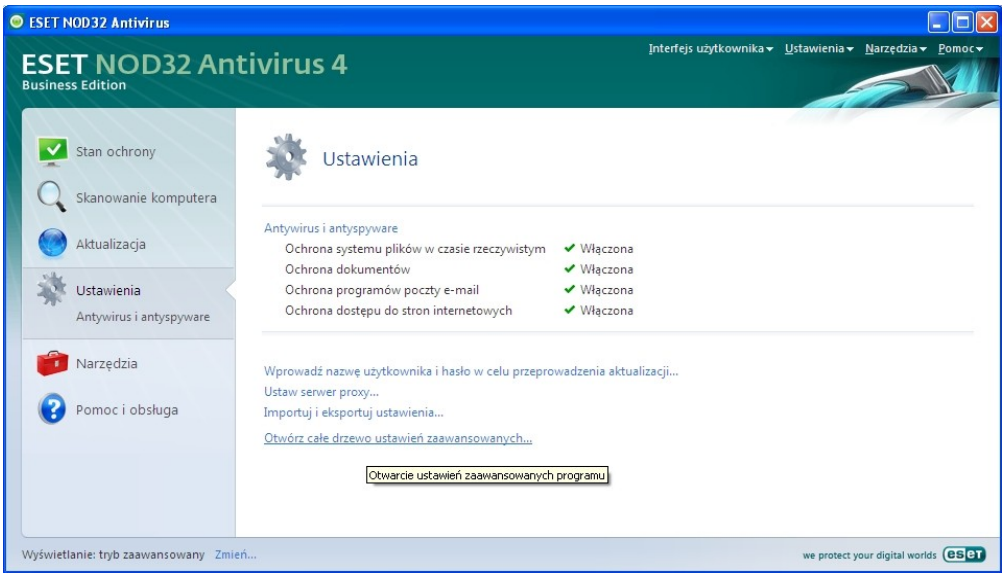
- Aby zdiagnozować wpływ ustawień programu antywirusowego na komunikację terminala z serwerem należy na chwilę wyłączyć program antywirusowy na terminalu i serwerze.



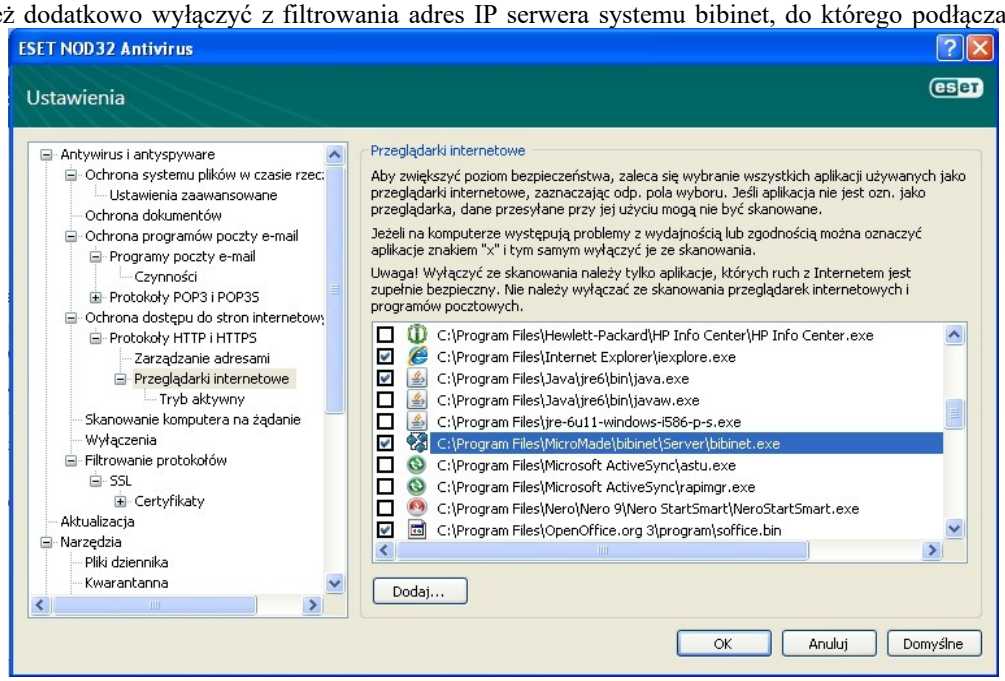
- Następnie należy uruchomić program bibi na terminalu i sprawdzić czy teraz otworzy się okno logowania



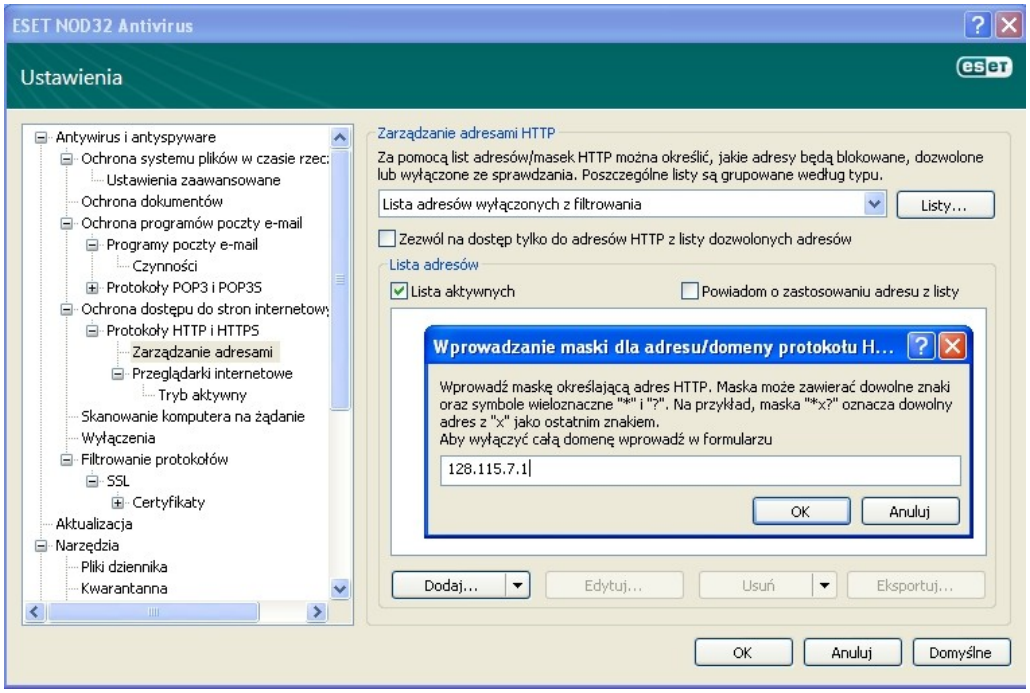
- Jeżeli operacja się powiodła, to oznacza , że program antywirusowy blokuje (filtruje) komunikację między tymi komputerami. Należy ponownie włączyć działanie programu antywirusowego.
- Następnie należy odpowiednio skonfigurować program antywirusowy. W tym celu należy wejść w ustawienia zaawansowane programu antywirusowego. Następnie należy wyłączyć z filtrowania przez program antywirusowy aplikację bibinet.exe na serwerze i aplikację bibi.exe na terminalu.



- Można też dodatkowo wyłączyć z filtrowania adres IP serwera systemu bibinet, do którego podłączamy terminale.



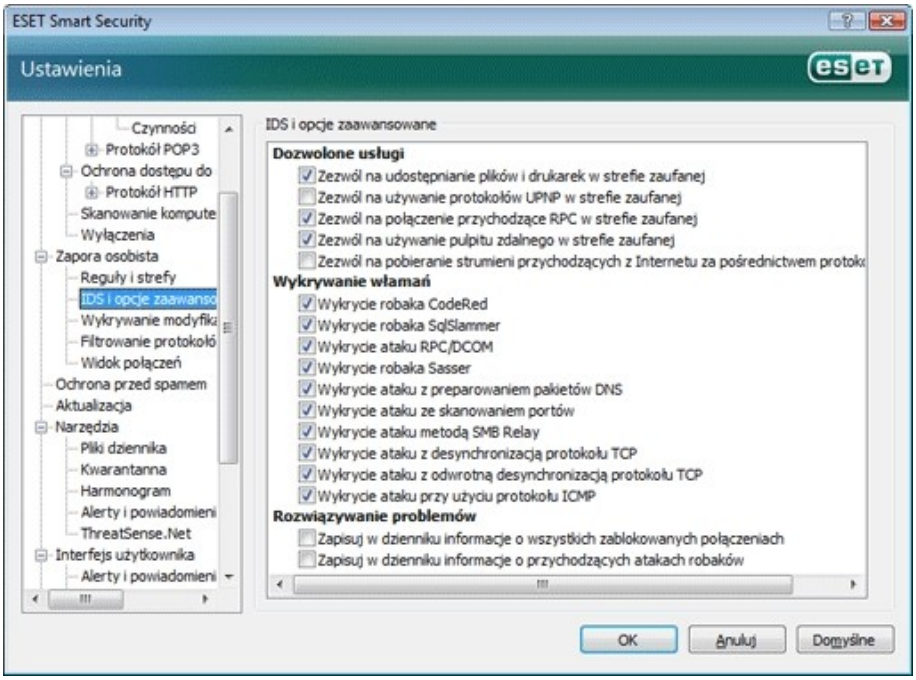
nale.



7.12.3 Odblokowanie portu RPC

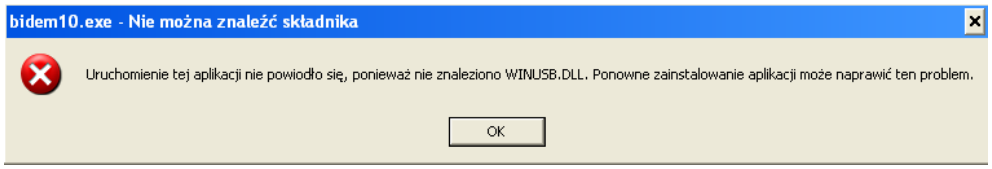
Do poprawnej komunikacji serwera bibinet z terminalami czasami konieczne jest odblokowanie portu zdalnego przydzielania procedur (RPC lub port nr 135). Odblokowanie to należy zrobić po obu stronach komunikacji czyli zarówno na serwerze jak i na terminalu.

Jeżeli komputery zabezpieczone są standardową zaporą systemu Windows to instalacja oprogramowania bibi udrażnia ten port do komunikacji między terminalem a serwerem systemu bibinet. Jeżeli jednak zaporą zarządzają dodatkowe programy antywirusowe często zachodzi konieczność odpowiedniego ich skonfigurowania tak, aby nie filtrowaly portu RPC. Na przykład w programie antywirusowym NOD Smart Security firmy ESET wybranie opcji *Zezwól na połączenie przychodzące żądania RPC w strefie zaufanej* — umożliwia korzystanie w strefie zaufanej z połączeń realizowanych za pośrednictwem mechanizmu RPC DCOM firmy Microsoft i tym samym udrażnia port 135 (RPC) do komunikacji między serwerem bibinet a terminalem.



7.13 Problem z (re)instalacją programu w systemie Windows XP i Windows Server 2003

Przy instalacji lub reinstalacji programu na komputerach z systemem Windows XP lub Windows Server 2003 może zostać zgłoszony błąd:



Wówczas należy zainstalować poprawkę Microsoft KB971286 uruchamiając program WINUSB_UPDATE_XP-SRV03.exe dostępny na pendrive w katalogu:

- XP poprawka\WinXP_USB_KB971286\x86 dla systemów 32 bitowych
- XP poprawka\WinXP_USB_KB971286\amd64 dla systemów 64 bitowych

Po zakończeniu instalacji poprawki (re)instalację programu bibi należy powtórzyć.

8. Archiwalia

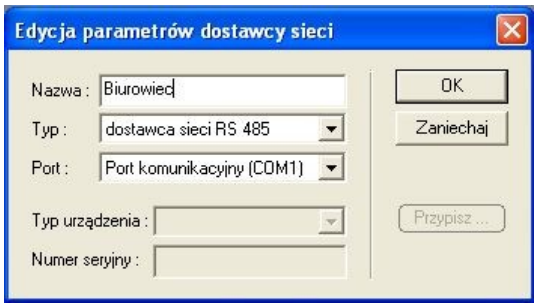
8.1 Konfiguracja interfejsów (dostawców urządzeń)

Dostawcami sprzętu w starszych wersjach systemu bibinet były interfejsy: interfejs bibi-F21 lub interfejs bibi-F22. Były to urządzenia, które łączyły siec kontrolerów bibi-K12 z komputerem zarządzającym systemem.

8.1.1 Konfiguracja interfejsu bibi-F21 (RS232 – RS485)

Interfejs bibi-F21 umożliwia podłączenie do 100 kontrolerów bibi-K12 podwieszonych do magistrali RS485 do jednego złącza RS232 (COM) komputera. COM może być także wytworzony przez adaptor USB-RS232. Interfejs może otwierać magistralę RS485 lub znajdować się w dowolnym miejscu tej magistrali. Dokładne warunki techniczne podłączania kontrolerów do magistrali opisuje instrukcja obsługi interfejsu lub instrukcja obsługi kontrolera.

Aby dodać interfejs i podłączone do niego urządzenia do systemu bibinet należy w programie bibi w oknie Opcje systemu bibi ustawić się na nazwie komputera, do którego podłączony jest interfejs i z menu kontekstowego wybrać Dodaj dostawcę.



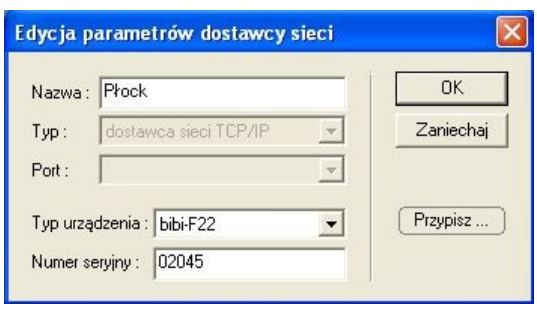
Należy wpisać nazwę , wybrać dostawca sieci RS 485 i wybrać COM do którego podłączony jest interfejs. Jeżeli instalacja urządzeń wykonana jest poprawnie to po zatwierdzeniu klawiszem OK, w lewej stronie okna pojawi się struktura drzewiasta urządzeń (kontrolerów i czytników) podłączonych do interfejsu. Aby sprawdzić do którego portu COM podłączony jest interfejs można użyć programu biSprzęt.exe znajdującego się w katalogu ..\MicroMade\bibinet\Tools.

8.1.2 Konfiguracja interfejsu bibi-F22 (Ethernet – RS485)

W systemie bibinet urządzenia (kontrolery) można podłączać zarówno przez port szeregowy komputera przy pomocy interfejsu bibi-F21, jak i przez sieć Ethernet przy pomocy interfejsu bibi-F22. Ten interfejs od strony magistrali RS485 ma takie same właściwości jak bibi-F21: umożliwia podłączenie do 100 kontrolerów bibi-K12, zapewnia też izolację galwaniczną pomiędzy urządzeniami.

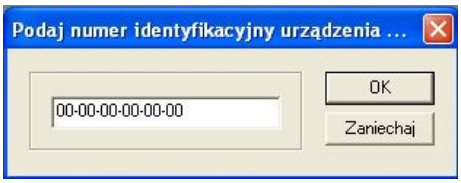
Interfejs F22 umożliwia podłączenie kontrolera lub kontrolerów bibi-K12 do najbliższego gniazdka sieci Ethernet, co znacznie upraszcza budowanie systemów kontroli dostępu i ewidencji czasu pracy. Możliwe jest też podłączanie go do routera internetowego. Można w ten sposób obsługiwać odległe lokalizacje, nie angażując do celu tego dodatkowych komputerów.

Podłączanie interfejsu do systemu odbywa się w prosty sposób w programie bibi. Po otwarciu okna Opcje systemu bibi klikamy prawym klawiszem myszy na nazwie komputera – węzła sieci bibinet i z menu wybieramy funkcję dodaj dostawcę.

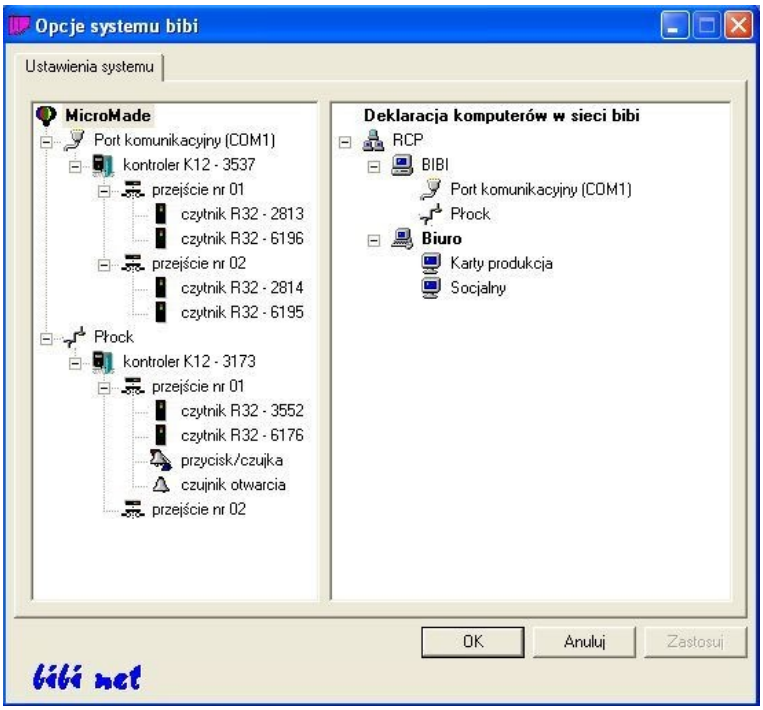


Wpisujemy nazwę (np. miejsce w którym jest umieszczony interfejs) i wybieramy typ dostawca sieci TCP/IP. Ustawiamy typ urządzenia na bibi-F22 i wpisujemy jego numer seryjny, a następnie wciskamy klawisz OK. Na liście Deklaracje komputerów w sieci bibi pojawi się pod wybranym węzłem zadeklarowana nazwa tego interfejsu.

Należy jeszcze raz kliknąć na tej nazwie i w otwartym oknie Edycja parametrów dostawcy sieci wcisnąć klawisz Przypisz.



W otwartym oknie wpisujemy numer identyfikacyjny interfejsu. Numer ten można znaleźć na tylnej ściance obudowy interfejsu lub na naklejce przyklejonej do arkusza identyfikacyjnego znajdującego się wewnątrz opakowania interfejsu. Po potwierdzeniu operacji program nawiąże komunikację z interfejsem samoczynnie. W lewej stronie okna Opcje systemu bibi pojawi się struktura drzewiasta urządzeń (kontrolerów i czytników) podłączonych do zadeklarowanego interfejsu bibi-F22.



W ten sposób należy skonfigurować wszystkie interfejsy bibi-F22 z danej instalacji. Dokładny opis ustawień i montażu interfejsu bibi-F22 opisany jest w instrukcji instalacji dołączanej do każdego zakupionego egzemplarza tego urządzenia.

Jeżeli przy przypisaniu interfejsu występują kłopoty należy zajrzeć do rozdziału 7.10 *Kłopot z przypisaniem urządzenia sieciowego do instalacji*

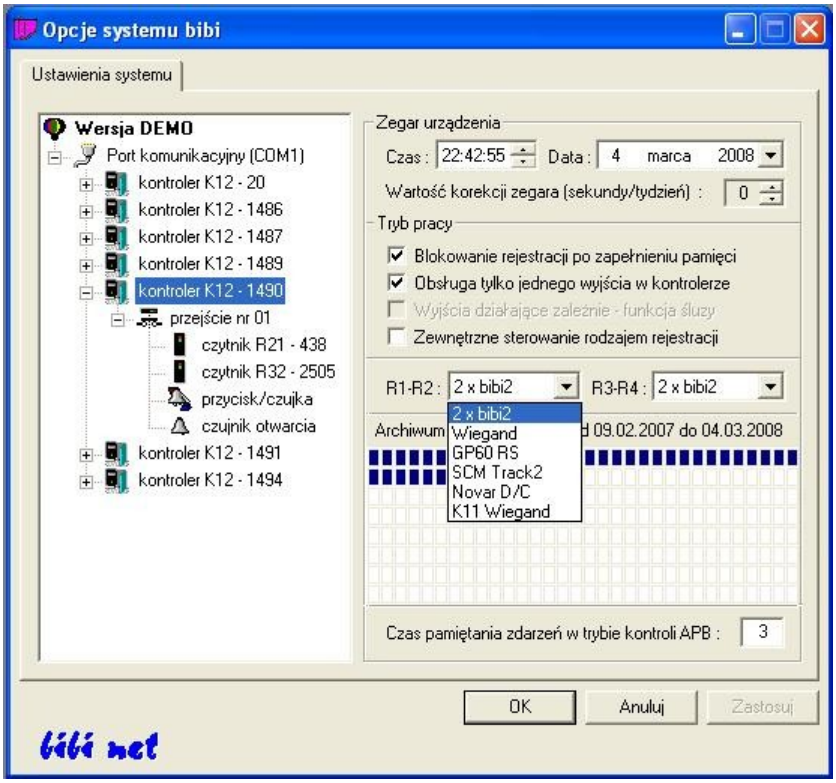
8.2 Konfiguracja kontrolerów bibi-K12

Po poprawnym skonfigurowaniu interfejsów wszystkie podłączone do systemu kontrolery bibi-K12powinny pojawić się w prawej części okna Opcje systemu bibi. Wszystkie opisane będą swoimi numerami fabrycznymi. Przy ich konfiguracji bardzo przydatne mogą okazać się wypełnione karty ewidencyjne interfejsów. Poprawnie wypełnione zawierają informacje o miejscu zamontowania kontrolerów i rozmieszczeniu podłączonych do nich czytników (wejście – wyjście).

Korzystając z tych informacji i z deklaracji poczynionych wcześniej szybko można skonfigurować podłączone do systemu kontrolery.

8.2.1 Konfiguracja ogólna kontrolera bibi-K12

W otwartym oknie Opcje systemu bibi kliknąć na wybranym kontrolerze i ustawić wszystkie parametry stosownie do swoich potrzeb.



- **Blokowanie rejestracji po zapełnieniu pamięci** – zaznaczenie tej flagi zabezpiecza przed utratą zarejestrowanych zdarzeń, jeżeli kontroler jest rzadko łączony z komputerem. Kontroler przestanie rejestrować kolejne zdarzenia, jeżeli cała pamięć będzie zapełniona rejestracjami nie zebranymi przez komputer.
  Jeżeli kontroler jest na stałe połączony z komputerem to ustawienie tej flagi nie ma znaczenia.
- **Obsługa tylko jednego wyjścia w kontrolerze** – zaznaczenie tej flagi powoduje, że kontroler obsługuje tylko jedno przejście. Wszystkie czytniki są wtedy przełączone na to wyjście.
- **Wyjścia działające zależnie – funkcja śluzy** – (flaga aktywna przy obsłudze dwóch wyjść przez kontroler). Zaznaczenie tej flagi powoduje, że kontroler realizuje funkcję śluzy. Otwarcie jednych drzwi może nastąpić tylko wtedy, jeżeli drugie drzwi są zamknięte.
- **Zewnętrzne sterowanie rodzajem rejestracji** – (flaga aktywna przy obsłudze jednego wyjścia przez kontroler). Zaznaczenie tej flagi zmienia działanie wejść In3 i In4 oraz wyjść Out3 i Out4 w kontrolerze. Wejście In3 steruje rodzajem rejestracji na czytniku dołączonym do interfejsu R1-R2 (lub R1 dla R32), a wyjście Out3 sygnalizuje ten rodzaj rejestracji. Wejście In4 i wyjście Out4 działa analogicznie dla interfejsu R3-R4 (lub R3 dla czytników R32). Rodzaje rejestracji (zmiana kierunku bądź typu rejestracji) ustawiane są w konfiguracji czytników. To ustawienie ma znaczenie szczególnie jeżeli do kontrolera podłączmy czytniki innych producentów lub czytniki biometryczne.
- **Interfejsy do czytników R1-R2 i R3-R4** – te pozycje pozwalają na wybranie odpowiednich interfejsów, w zależności jakie czytniki będą podłączone do kontrolera.

Jeżeli wybierzemy interfejs bibi2, to po podłączeniu czytników bibi zostaną one automatycznie zgłoszone do komputera i pojawią się na liście urządzeń z podaniem typu i numeru fabrycznego.

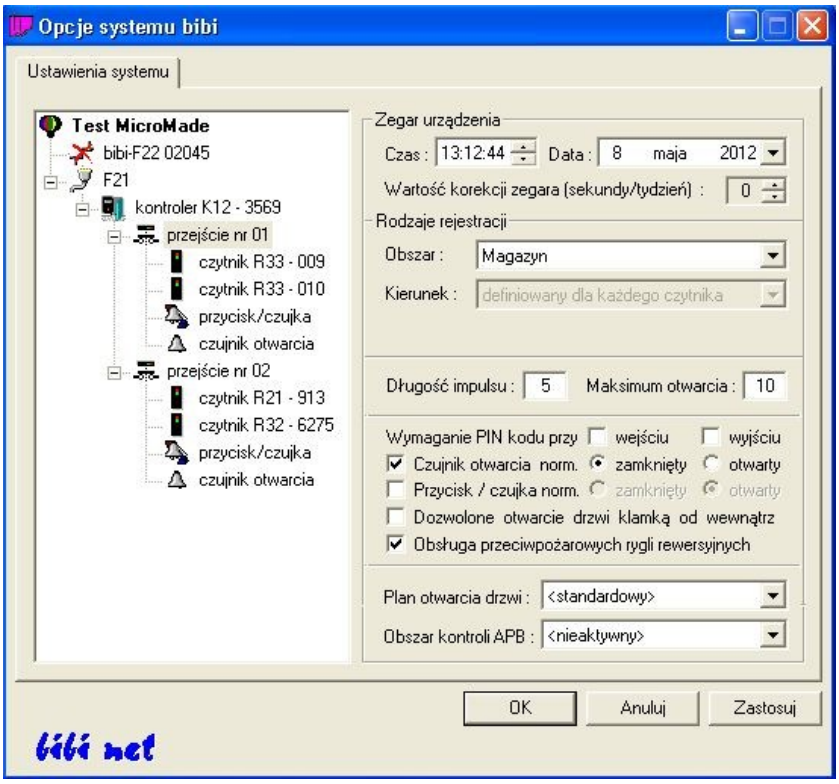
Czytniki pracujące z innym interfejsem (Wiegand,Track2) nie mogą same zgłaszać się do kontrolera. Dlatego też, po wybraniu określonego interfejsu, kontroler natychmiast zgłasza do programu obecność takich czytników, bez względu na to, czy są w rzeczywistości podłączone.

Czytniki z interfejsem Track 2 zgłaszane są do programu jako czytniki R40, natomiast czytniki z interfejsem Wieganda jako R41. Numer czytnika tworzony jest z numeru kontrolera oraz pozycji podłączenia czytnika (nie jest to numer fabryczny czytnika).

- **Czas pamiętania zdarzeń w trybie kontroli APB** – jest to czas wyrażony w minutach blokowania kolejnej takiej samej rejestracji w trybie AntyPassBacku (jeżeli tryb ten będzie włączony dla któregoś przejścia). Ustawie-

nie wartości 0 blokuje odblokowywanie rejestracji po czasie, czyli zawsze po wejściu możliwe będzie tylko wyjście.

8.2.2 Konfiguracja przejścia w kontrolerze bibi-K12

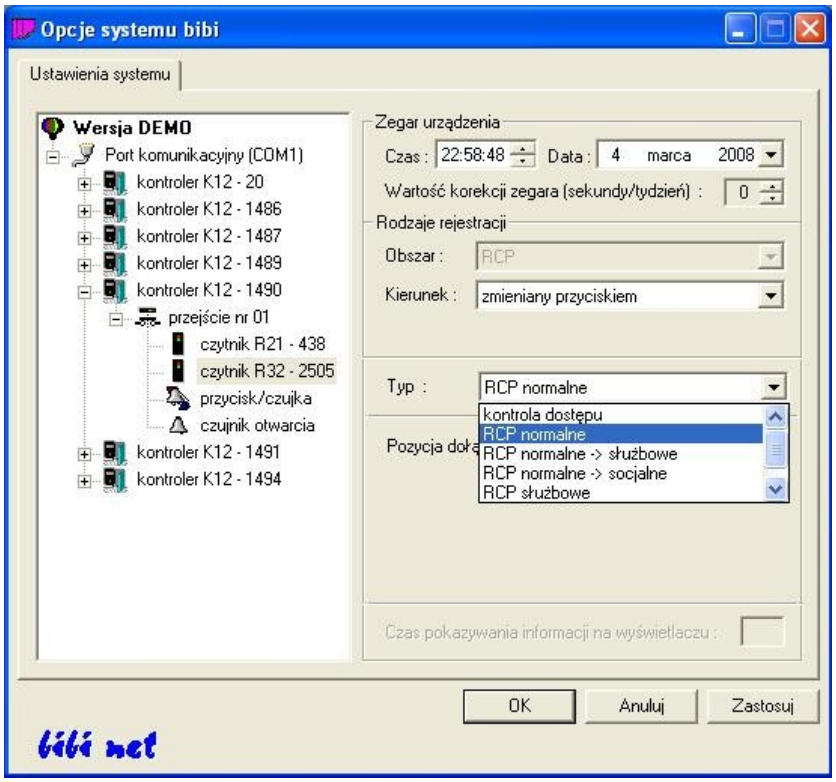


- **Obszar** - Należy wybrać obszar zabezpieczony, do którego prowadzi to przejście. Obszary muszą być wcześniej zdefiniowane w zakładce „Obszary" bocznego panelu sterującego. Obszar zabezpieczony to jedno lub kilka pomieszczeń, do którego prowadzą przejścia kontrolowane. W przypadku kontroli dostępu, obszar zabezpieczony jest przeważnie rzeczywistym obszarem - np. magazyn. Jeżeli przejście pełni tylko rolę rejestracji czasu pracy, obszar może być wirtualny - np. RCP.
- **Długość impulsu otwarcia rygla** - określa czas w sekundach, jak długo będzie podawane napięcie otwierające rygiel po zbliżeniu uprawnionej karty lub przyciśnięciu przycisku wyjścia. Można ustawić czas od 1 do 63 sekund. Napięcie będzie wyłączone po tym czasie, lub natychmiast po otwarciu drzwi jeżeli na przejściu zamontowany jest kontaktronowy czujnik otwarcia drzwi. Ustawienie czasu 0 spowoduje, że rygiel w ogóle nie będzie otwierany (typowe ustawienie dla RCP).
- **Dozwolony maksymalny czas otwarcia drzwi** - określa czas w sekundach, jak długo mogą być otwarte drzwi po uprawnionym otwarciu. Można ustawić czas od 1 do 63 sekund. Jeżeli drzwi nie zostaną w tym czasie zamknięte, zostanie zgłoszony alarm.
- **Czujnik otwarcia** - flagę tą należy zaznaczyć, jeżeli zamontowano czujnik otwarcia drzwi
  - **norm. zamknięty / otwarty** - należy określić, w jakim stanie pozostaje czujnik przy drzwiach zamkniętych. Typowo, przy czujnikach magnetycznych (kontaktronach), jest on normalnie zamknięty.
- **Przycisk / czujka** - flagę tą należy zaznaczyć, jeżeli podłączono przycisk wyjścia lub czujkę alarmową do wejścia IN1 (IN3 dla przejścia 2). Wybór, które z tych dwóch urządzeń jest faktycznie podłączone, należy dokonać konfigurując pozycję „przycisk/czujka" widoczną w lewej stronie okna.
  - **norm. zamknięty / otwarty** - należy określić, w jakim stanie pozostaje przycisk/czujka w stanie nieaktywnym. Typowo, przycisk wyjścia jest normalnie otwarty.
  - Przycisku otwarcia nie należy mylić z przeciwpożarowym przyciskiem ewakuacyjnym, który włączany jest bezpośrednio w obwód rygla. Ten przycisk nie jest definiowany w systemie bibinet.

- **Dozwolone otwarcie drzwi klamką od wewnątrz** - tą flagę należy zaznaczyć, jeżeli wewnątrz pomieszczenia nie zamontowano czytnika kart ani przycisku wyjścia, a wyjście z pomieszczenia następuje poprzez normalne otwarcie drzwi klamką. Nie jest to zalecana konfiguracja, gdyż system nie może rozpoznać wyłamania drzwi od zewnątrz.
- **Obsługa przeciwpożarowych rygli rewersyjnych** – zaznaczenie tej flagi powoduje, że nie jest kasowany sygnał otwierający rygiel elektromagnetyczny po otwarciu drzwi. Stosuje się to zaznaczenie, jeżeli na tym przejściu zastosowano np. zworę elektromagnetyczną z wbudowanym czujnikiem otwarcia drzwi. Wówczas napięcie ze zwory zdejmowane jest na czas ustawiony w ramce *Długość impulsu*.
  W przypadku nie zaznaczenia tej flagi sygnał podawany na rygiel jest kasowany w momencie naruszenia czujnika otwarcia drzwi. To rozwiązanie stosuje się najczęściej przy sterowaniu ryglami w kołowrotach.
- **Plan otwarcia drzwi** - określa schemat czasowy, kiedy drzwi mają być otwarte na stałe. Jest to wykorzystywane w biurach, gdzie w ciągu dnia przychodzą interesanci - w uprawnionym czasie drzwi są wtedy otwarte. W pozostałych godzinach drzwi mogą otworzyć tylko uprawnione osoby. Można wybrać ze schematów określonych przez producenta, lub wstawić dowolny zdefiniowany schemat czasowy.
  - **<standardowy>** - ustawienie najbardziej typowe, otwarcie drzwi następuje tylko poprzez uprawnione karty lub przyciskiem wyjścia
  - **<nigdy>** - ten schemat zabrania otwarcia drzwi nawet przez osoby uprawnione (awaryjne zamknięcie obszaru chronionego), powoduje też brak rejestracji RCP.
  - **<praca bistabilna>** - przy tym schemacie kolejne użycie uprawnionej karty powoduje na przemian otwarcie/zamknięcie drzwi (włączenie/wyłączenie urządzenia)
  - **<tryb astabilny>** - to jest schemat przeznaczony do sterowania urządzeń. Zbliżenie karty do czytnika powoduje aktywowanie wyjścia, zabranie karty wyłącza wyjście. Tryb ten poprawnie działa tylko z czytnikami firmy MicroMade sprzedawanymi od kwietnia 2008r.
  - **<zawsze>** - ten schemat otwiera drzwi na stałe
  - **dni robocze 7-15** – (przykładowy schemat czasowy) ten lub dowolny inny zdefiniowany schemat czasowy spowoduje otwarcie drzwi na stałe w określonych dniach i godzinach. Poza tymi godzinami otwarcie drzwi może nastąpić uprawnionymi kartami.
- **Obszar kontroli APB** - określa sposób działania AntyPassBacku.
  - **<nieaktywny>** - AntyPassBack na tym przejściu wyłączony
  - **<lokalny>** - AntyPassBack działa wspólnie na wszystkich przejściach które spełniają warunki:
    - kontrolery są dołączone do tego samego interfejsu bibi-F21 lub bibi-F22
    - przejścia mają ustawiony tez sam Obszar
    - przejścia mają włączony AntyPassBack - <lokalny>

8.3 Konfiguracja czytników RFID bibi-R32 i bibi-R33

Standardowo do każdego przejścia obsługiwanego przez kontroler podłączone są od jednego do 4 czytników RFID. Każdy z nich należy ustawić zgodnie ze swoją wiedzą i zgodnie z zaleceniami inwestora.



- **Kierunek** - określa, czy rejestracja w czytniku dotyczy wejścia czy wyjścia z danego obszaru. W wypadku rejestracji czasu pracy określa to jednocześnie rozpoczęcie (wejście) lub zakończenie (wyjście) pracy.
  - **zmieniany przyciskiem** - taka pozycja pojawi się dodatkowo dla czytników bibi-R21 oraz przy zaznaczeniu flagi w kontrolerze: „Zewnętrzne sterowanie rodzajem rejestracji". Oznacza ona, że rodzaj rejestracji z tego czytnika będzie można wybrać w momencie rejestracji.
- **Typ** - określa, typ rejestracji. Istnieją 4 typy rejestracji:
  - **kontrola dostępu** - rejestracje te nie będą analizowane przy rozliczaniu czasu pracy
  - **RCP normalne** - rejestracje te będą trafiały do rozliczenia czasu pracy, jako normalne wejścia do pracy i wyjścia z pracy
  - **RCP służbowe** - rejestracje z tego czytnika będą traktowane jak zdarzenia służbowe. Aby takie zdarzenie zarejestrować, trzeba mieć indywidualnie przyznane uprawnienie: „Wyjścia służbowe" (w „Edycji Danych Pracowniczych"). Osobom nie posiadające takich uprawnień drzwi nie będą otwarte i zostanie zarejestrowane zdarzenie „brak uprawnień RCP".
  - **RCP socjalne** - rejestracje z tego czytnika będą traktowane jak wejścia i wyjścia na przerwę. Aby takie zdarzenie zarejestrować, trzeba mieć indywidualnie przyznane uprawnienie: „Wyjścia socjalne" (w „Edycji Danych Pracowniczych"). Osobom nie posiadające takich uprawnień drzwi będą otwarte i zostanie zarejestrowane zdarzenie kontroli dostępu.
  - **RCP normalne -> służbowe** - typ rejestracji zmieniany przyciskiem (czytnik R21 lub zaznaczona flaga w kontrolerze: „Zewnętrzne sterowanie rodzajem rejestracji")
  - **RCP normalne -> socjalne** - typ rejestracji zmieniany przyciskiem (czytnik R21 lub zaznaczona flaga w kontrolerze: „Zewnętrzne sterowanie rodzajem rejestracji"). Jeżeli osoba nie posiada uprawnień do rejestracji socjalnych, przy próbie zarejestrowania takiego zdarzenia drzwi nie będą otwarte i zostanie zarejestrowane zdarzenie „brak uprawnień RCP".
- **Pozycja dołączenia czytnika do kontrolera** - informuje, do którego interfejsu w kontrolerze został dołączony czytnik. Ma to ułatwić identyfikację poszczególnych dołączonych czytników.

8.4 Zmiana licencji programowej na sprzętową

W przypadku rozbudowy systemu może zajść konieczność zmiany instalacji jednostanowiskowej programowej na instalację oparta o sprzętowe klucze bibi.HAK. W celu wymiany klucza programowego na sprzętowe należy:

- Przygotować zakupioną licencję sprzętową (plik license.dat) oraz klucze sprzętowe bibi.HAK
- Uruchomić program narzędziowy biserver
  - ustawić „Poziom zabezpieczeń zewn. połączeń” - Niski
  - nacisnąć klawisz „Wprowadź nowe zasady”
  - NIE restartować systemu Windows
- włożyć klucz bibi.HAK do złącza USB komputera
- uruchomić program narzędziowy bis2h.exe
  - zalogować się jako Administrator Systemu (w prostej instalacji opartej na licencji bibi.baza jest to hasło identyczne z hasłem Administratora programu bibi)
  - wskazać położenie pliku nowej licencji (sprzętowej)
  - nacisnąć *Dalej* - dane z klucza programowego zostaną przeniesione do klucza bibi.HAK
- uruchomić program narzędziowy bikeys.exe
  - zalogować się jako Administrator Systemu
  - wybrać opcję: *Generowanie nowego hasła szyfrującego*
  - ustawić się na białym polu poniżej wybranej opcji i prawym klawiszem myszy uruchomić funkcję *Rozpocznij generowanie*
  - po zakończeniu generowania należy hasło wpisać do wybranego klucza bibi.HAK – stanie się on kluczem systemowym instalacji (można będzie z niego pobierać hasło szyfrujące konieczne do konfiguracji pozostałych kluczy)
  - po przejściu Dalej do tabeli z kluczami wybrać klucz systemowy i prawym klawiszem myszy dodać do niego Administratora programu bibi
  - włożyć pozostałe klucze bibi.HAK do złącz USB komputera. Pojawią się one w tabeli kluczy. Wskazując myszą przy pomocy menu kontekstowego skonfigurować je do pracy w instalacji bibinet.

W ten sposób powstanie pierwszy węzeł działający w oparciu o klucze sprzętowe. Aby dodać terminale do tego węzła skorzystać z opisu w następnym rozdziale W celu dodania kolejnych węzłów należy postępować zgodnie z opisem zawartym w rozdziale **Instalacja kolejnych węzłów**.

8.5 Instalacja - licencja bibi.baza

Właścicielem licencji jest firma lub osoba fizyczna, która jest (będzie) użytkownikiem systemu bibinet. Do instalacji bibi.baza wydawana jest licencja, niewymagająca kluczy sprzętowych USB bibi.HAK. Dla tej licencji klucze takie symulowane są w serwerze bibinet. Mimo braku fizycznej obecności kluczy, wszystkie programy (narzędziowe i użytkowe) pracują tak, jakby one istniały.

Obecnie takie licencje programowe nie maja zastosowania w systemie bibinet. Funkcjonowały do 2011 r.

Licencja ta pozwała na pełną funkcjonalność programu w zakresie kontroli dostępu i rejestracji czasu pracy w małej firmie (instytucji) – baza danych może zawierać maksymalnie 30 rekordów (użytkowników).

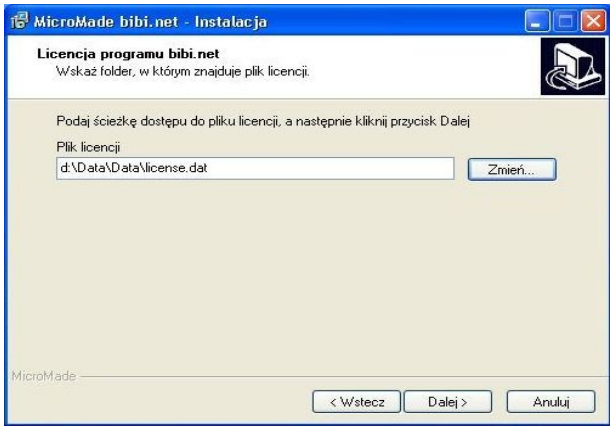
Licencja nie umożliwiała obsługi urządzeń sieciowych (brak kluczy sprzętowych szyfrujących komunikację z tymi urządzeniami), oraz nie pozwalała na uruchomienie podglądu raportów przez przeglądarkę internetową.

8.5.1 Instalacja programów systemu bibinet

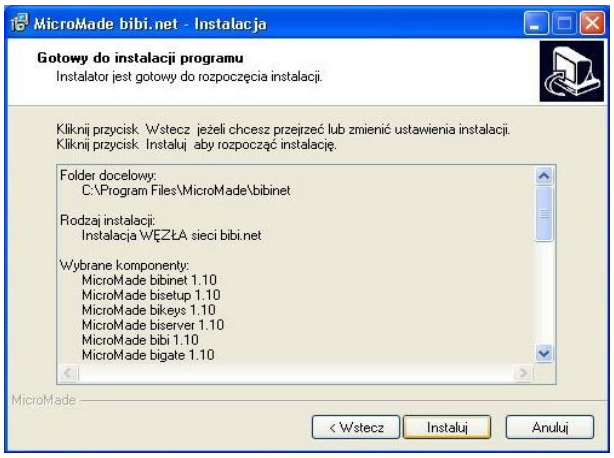
- Włożyć pendrive do złącza USB komputera. Wybrać z menu instalatora systemu bibinet "Instalacja bibinet" lub uruchomić program bibinet_setup.exe.

  Przeczytać i zaakceptować umowę licencyjną.

- Wybrać „Instalacja WĘZŁA sieci bibinet”.
- Wskazać folder, w którym umieszczony jest plik licencji license.dat. Może on być na pendrive w folderze Licencja lub został przesłany pocztą elektroniczną.



Przechodząc przez kolejne okna instalatora zakończyć proces instalacji.



Programy użytkowe (bibi, bramka, szef) zostaną zainstalowane w folderze:

C:\Program Files\MicroMade\bibinet\

Programy narzędziowe zostaną zainstalowane w folderze:

C:\Program Files\MicroMade\bibinet\Tools\

Dokumentacje (tekst licencji i instrukcje) zostaną zainstalowane w folderze:

C:\Program Files\MicroMade\bibinet\Doc\

Baza danych systemu bibi.net będzie tworzona w folderze:

C:\Program Files\MicroMade\bibinet\Server\Data

Do programów użytkowych, do katalogu z programami narzędziowymi, oraz do instrukcji zostaną umieszczone skróty w menu start:

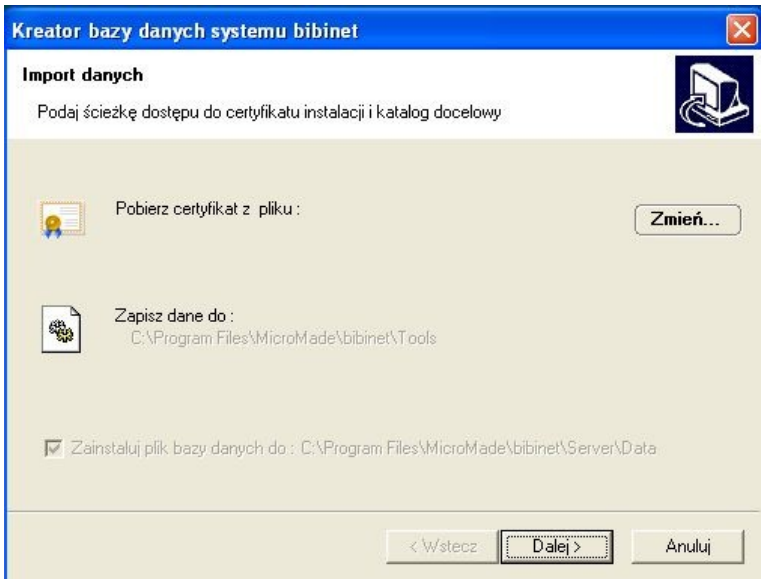
Start\Programy\MicroMade\bibinet\

8.5.2 Wytworzenie bazy danych

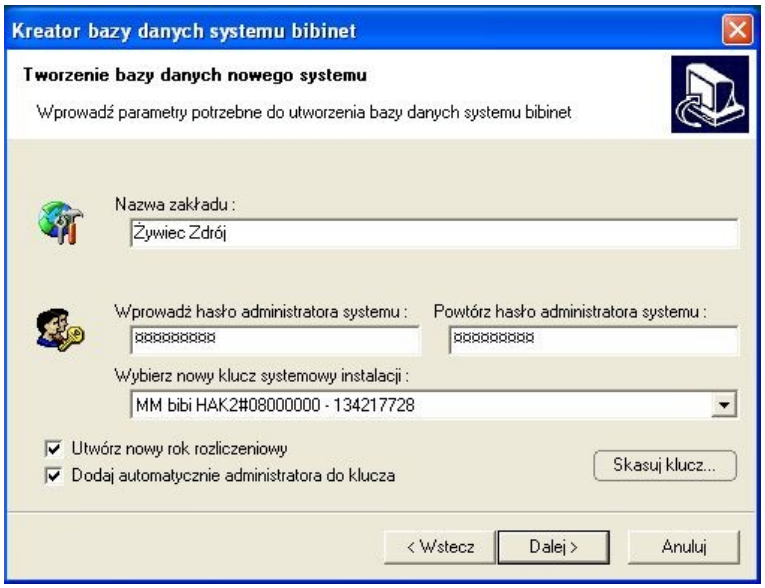
Po zainstalowaniu programów systemu bibinet należy wytworzyć bazę danych do której będą zapisywane rejestracje występujące w systemie.

Do tego celu służy program narzędziowy bisetup.exe dostępny w katalogu C:\Program Files\MicroMade\bibinet\Tools\ lub w folderze bibi programy narzędziowe

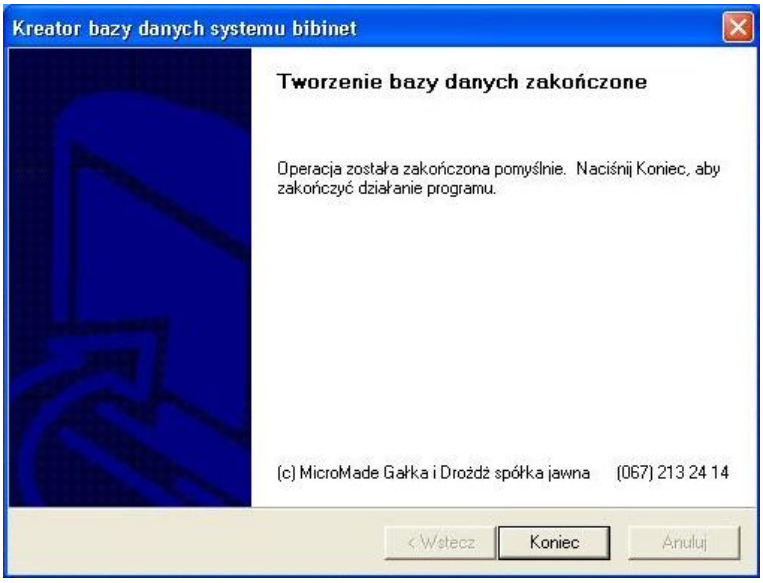
Po uruchomieniu programu w oknie jak niżej wciskamy klawisz *Dalej* przechodząc do następnego okna.



Tutaj wpisujemy hasło Administratora Systemu – minimum 8 znaków, które jest równoznaczne z hasłem Administratora programu bibi.



Przechodząc dalej kończymy proces wytworzenia bazy danych.



Po tej operacji można otworzyć program bibi

i przystąpić do konfiguracji systemu (rozdział 5).

Umowa Licencyjna na użytkowanie oprogramowania systemu KD i RCP bibinet

Niniejsza Umowa Licencyjna na użytkowanie oprogramowania ***„bibi.net”*** (zwana dalej „Umową Licencyjną”) stanowi prawnie wiążącą umowę pomiędzy osobą fizyczną lub prawną (zwaną dalej „Licencjobiorcą”) a firmą MicroMade Gałka i Drożdż sp. j. (zwaną dalej „Licencjodawcą”), której przedmiotem jest oprogramowanie systemu ***bibinet*** (zwane dalej „Oprogramowaniem”).
Poprzez instalację Oprogramowania Licencjobiorca zgadza się przestrzegać postanowień niniejszej Umowy Licencyjnej.

§ 1. PRZEDMIOT UMOWY- UDZIELENIE LICENCJI

1. Przedmiotem niniejszej umowy jest podstawowy pakiet oprogramowania systemu kontroli dostępu i rejestracji czasu pracy ***bibinet*** zawierający:
   A. serwer ***bibinet***
   B. programy ***bibi, bibi szef, bibi bramka, bibi fakty.***
2. Licencjodawca udziela Licencjobiorcy niewyłącznej licencji na korzystanie z oprogramowania na czas nieoznaczony. Licencjobiorca korzystać będzie z oprogramowania wyłącznie na własne potrzeby związane z prowadzoną działalnością gospodarczą.
3. Warunkiem przyznania licencji, o której mowa powyżej, jest wniesienie opłaty licencyjnej zgodnie z cennikiem MicroMade.
4. Licencja o której mowa powyżej obejmuje:
   A. prawo do korzystania z oprogramowania na określonej liczbie komputerów
   B. sporządzenie kopii zapasowej oprogramowania.
5. Licencja obejmuje również roczny abonament liczony od daty zawarcia umowy licencyjnej. W ramach abonamentu Licencjobiorca ma prawo do:
   A. zainstalowania aktualnej wersji oprogramowania udostępnionej przez Licencjodawcę pod adresem *www.micromade.pl*
   B. korzystania z opcji podglądu raportów przez przeglądarkę internetową (jeżeli ta opcja została wykupiona)
   C. korzystania z pomocy technicznej udzielanej drogą elektroniczną lub przez telefon.
6. Potwierdzeniem przyznania licencji jest plik aktywacyjny oprogramowania, zawierający:
   A. dane Licencjobiorcy
   B. zakres licencji (wykupione opcje, maksymalne parametry itp.)
   C. datę zawarcia Umowy Licencyjnej.
7. Licencjobiorca może rozszerzyć posiadaną licencję na kolejne stanowiska pod warunkiem wniesienia uzupełniającej opłaty licencyjnej zgodnie z cennikiem MicroMade aktualnym w dniu rozszerzenia.
8. Po upływie roku Licencjobiorca może wykupić abonament na kolejny rok poprzez wniesienie opłaty abonamentowej zgodnie z cennikiem MicroMade aktualnym w dniu zakupu abonamentu. Abonament przedłuża prawo do:
   A. aktualizacji oprogramowania i pomocy technicznej, o których mowa w pkt. 5
   B. korzystanie z opcji podglądu raportów przez przeglądarkę internetową (przy zakupie tej opcji)

   na kolejny rok licząc od daty wygaśnięcia poprzedniego abonamentu.

§ 2. OGRANICZENIA

Licencjobiorca, z zastrzeżeniem przepisów o prawie autorskim i prawach pokrewnych (DZ.U.z 1994 r. nr 24 poz.83 ze zm.) nie może:

1. odtwarzać, dekompilować lub deasemblować Oprogramowania z wyjątkiem sytuacji, gdy niezależnie od niniejszego ograniczenia działania takie są dozwolone przez prawo właściwe i tylko w zakresie takiego zezwolenia.
2. rozpowszechniać, wprowadzać do obrotu oprogramowania (lub też kopii), oddawać w najem lub dzierżawę (a także w żaden sposób obciążać prawami osób trzecich).

§ 3. ODPOWIEDZIALNOŚĆ

1. Licencjobiorca zobowiązany jest do korzystania z Oprogramowania w sposób zgodny z niniejszą licencją, przeznaczeniem oprogramowania i instrukcją obsługi.
2. Odpowiedzialność za wszystkie skutki funkcjonowania oprogramowania (w tym także niemożności użytkowania oprogramowania) oraz decyzje podjęte na tej podstawie ponosi wyłącznie Licencjobiorca.
3. Licencjodawca nie ponosi odpowiedzialności za ewentualne powstałe szkody w wyniku korzystania (lub niemożności korzystania) z oprogramowania przez Licencjobiorcę
4. Licencjodawca nie ponosi odpowiedzialności za usterki innego programu komputerowego funkcjonującego jednocześnie z Oprogramowaniem.
5. Licencjodawca nie ponosi odpowiedzialności za wadliwe działanie Oprogramowania wynikające z wadliwego funkcjonowania sieci komputerowej Licencjobiorcy lub sieci globalnej (internet).

§ 4. CZAS OBOWIĄZYWANIA

1. Umowa obowiązuje od daty zawartej w pliku aktywacyjnym.
2. Niniejsza umowa licencyjna zostaje zawarta na czas nieoznaczony.
3. Licencjodawca może rozwiązać niniejszą umowę bez wypowiedzenia ze skutkiem natychmiastowym gdy Licencjobiorca rażąco narusza postanowienia niniejszej umowy. W takiej sytuacji Licencjobiorca jest zobowiązany zniszczyć wszystkie kopie oprogramowania.

§ 5. GWARANCJA

1. Licencjodawca udziela 12 miesięcznej gwarancji, że oprogramowanie będzie wykonywało funkcje kontroli dostępu i rejestracji czasu pracy określone w ofercie.
2. Licencjodawca (jako gwarant) zapewnia że dołożył należytej staranności przy opracowywaniu oprogramowania, jednakże nie przejmuje odpowiedzialności za niewłaściwe działanie oprogramowania, w szczególności przerwanie pracy oprogramowania lub innych błędów (o podobnym charakterze).
3. Niniejszym wyłącza się rękojmię wynikającą z przepisów kodeksu cywilnego.

§6. POSTANOWIENIA KOŃCOWE

1. Wszelkie zmiany niniejszej umowy, winny być dokonywane w formie pisemnej.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy kodeksu cywilnego, ustawa o prawie Autorskim i prawach pokrewnych
3. Do rozstrzygania sporów wynikłych na tle stosowania niniejszej umowy właściwym będzie Sąd dla siedziby firmy MicroMade Gałka i Drożdż sp.j.

LICENCJODAWCA