Oprogramowanie Target CI wer. 1.5

PRZEWODNIK PO CYBERBEZPIECZEŃSTWIE

Polski

Zaktualizowano: wrzesień 2025

A Sonova Brand

Spis treści

1. WPROWADZENIE

W niniejszym dokumencie zawarto informacje dotyczące bezpieczeństwa technicznego i prywatności oprogramowania Target CI wer. 1.5 firmy Advanced Bionics, zwanego dalej „oprogramowaniem dopasowującym”. Oprogramowanie dopasowujące jest przeznaczone dla wykwalifikowanych audiologów (HCP) w celu konfiguracji (tj. dopasowania) aparatów słuchowych u pacjentów, którym wszczepiono implanty ślimakowe firmy Advanced Bionics.

W dokumencie tym skoncentrowano się na zagadnieniach cyberbezpieczeństwa i prywatności, które mają znaczenie w kontekście korzystania z oprogramowania dopasowującego. Obejmuje ona ocenę kontroli bezpieczeństwa i prywatności, które są obecnie zintegrowane z oprogramowaniem, a także tych, które mają być stosowane i konfigurowane w środowisku informatycznym, w którym produkt będzie używany zgodnie z przeznaczeniem.

Niniejszy dokument nie zawiera informacji technicznych na temat bezpieczeństwa i prywatności w następujących kwestiach:

- Poprzednie wersje oprogramowania dopasowującego AB
- Oprogramowanie AB inne niż Target CI wer. 1.5
- Strony internetowe AB
- Aplikacja mobilna AB Remote
- Urządzenia słuchowe AB

1.1 SKRÓTY I DEFINICJE:

Akronim	Termin
FSW	Oprogramowanie dopasowujące
HCP	Audiolog
SaMD	Oprogramowanie jako urządzenie medyczne
AB	Advanced Bionics
IFU	Instrukcja obsługi

2. INNE ZASOBY

2.1 OBSŁUGA KLIENTA

Dla użytkowników na terenie Stanów Zjednoczonych i Kanady firma Advanced Bionics udostępnia bezpłatny numer linii telefonicznej pomocy technicznej (877-271-6727), pod którym dostępne jest profesjonalne wsparcie od poniedziałku do piątku w godzinach od 5:00 do 17:00 czasu pacyficznego.

W przypadku użytkowników spoza USA i Kanady pomoc techniczna jest świadczona regionalnie. W przypadku pytań dotyczących oprogramowania dopasowującego, sprzętu lub innych kwestii związanych z programowaniem, należy skontaktować się z lokalnym przedstawicielem firmy AB.

2.2 PORTAL AB PRO

Oprogramowanie dopasowujące i powiązaną dokumentację można pobrać ze strony https://www.abproportal.com lub klienta internetowego Sonova. Wymagane jest zalogowanie się na konto. Zasób ten może nie być dostępny na wszystkich rynkach. Aby uzyskać więcej informacji, skontaktować się z przedstawicielem AB.

2.3 PODRĘCZNIK INSTALACJI ZAAWANSOWANEJ

Podręcznik instalacji zaawansowanej Target CI wer. 1.5 jest dostępny na żądanie. W podręczniku zamieszczono informacje techniczne dotyczące instalatora oprogramowania, w tym opcje wiersza poleceń dla instalacji cichej i automatycznej.

2.4 MDS2

Oświadczenie producenta dotyczące bezpieczeństwa urządzeń medycznych (MDS2) to standardowy formularz branżowy zawierający odpowiedzi na pytania dotyczące bezpieczeństwa i prywatności dotyczące oprogramowania do montażu urządzeń medycznych AB. Formularz jest dostępny na żądanie.

2.5 INSTRUKCJA OBSŁUGI

Instrukcja obsługi zostanie dostarczona wraz z nośnikiem instalacyjnym oprogramowania. W przypadku niektórych rynków elektroniczną wersję instrukcji obsługi można pobrać ze strony: www.advancedbionics.com/ifu

Poniższe sekcje IFU mogą być istotne dla profesjonalistów IT:

- Opis produktu
- Minimalne wymagania systemowe i charakterystyka pracy
- Wytyczne bezpieczeństwa IT
- Instrukcja instalacji
- Pomoc techniczna

2.6 HIMSA

HIMSA to niezależny dostawca oprogramowania, który produkuje Noah System 4, system programowy przeznaczony dla branży opieki słuchowej, który zapewnia specjalistom ds. opieki słuchowej niezależny od dostawcy system do wykonywania zadań związanych z obsługą klienta.

Oprogramowanie dopasowujące można opcjonalnie skonfigurować tak, aby do przechowywania danych wykorzystywało system Noah System 4, a nie lokalną bazę danych.

Na stronie internetowej HIMSA poświęconej bezpieczeństwu znajdują się odpowiedzi na najczęstsze pytania dotyczące bezpieczeństwa IT w systemie Noah System 4.

https://www.himsa.com/support/noah-enterprise-support/security-questionnaire-support/

https://www.himsa.com/support/noah-enterprise-support/security-considerations/

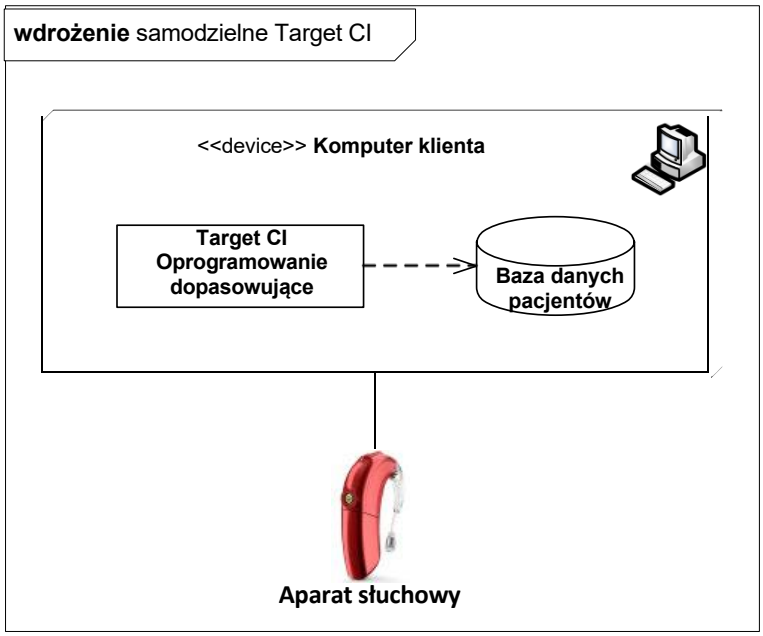
Dodatkowe informacje na temat bezpieczeństwa znajdziesz w sekcji Bezpieczeństwo w Centrum szkoleniowym HIMSA: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

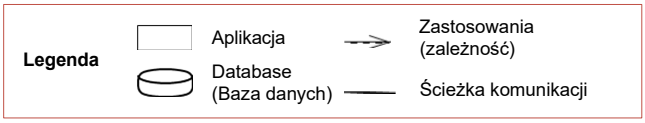
3. DIAGRAMY SIECIOWE I KONTEKSTOWE

Obsługiwane są dwa modele wdrażania oprogramowania dopasowującego, które jest aplikacją kliencką (SaMD) instalowaną na komercyjnie dostępnym komputerze z systemem Microsoft Windows. Oprogramowanie nie zawiera żadnego sprzętu ani systemu operacyjnego.

3.1 MODEL WDROŻENIA 1: SAMODZIELNY

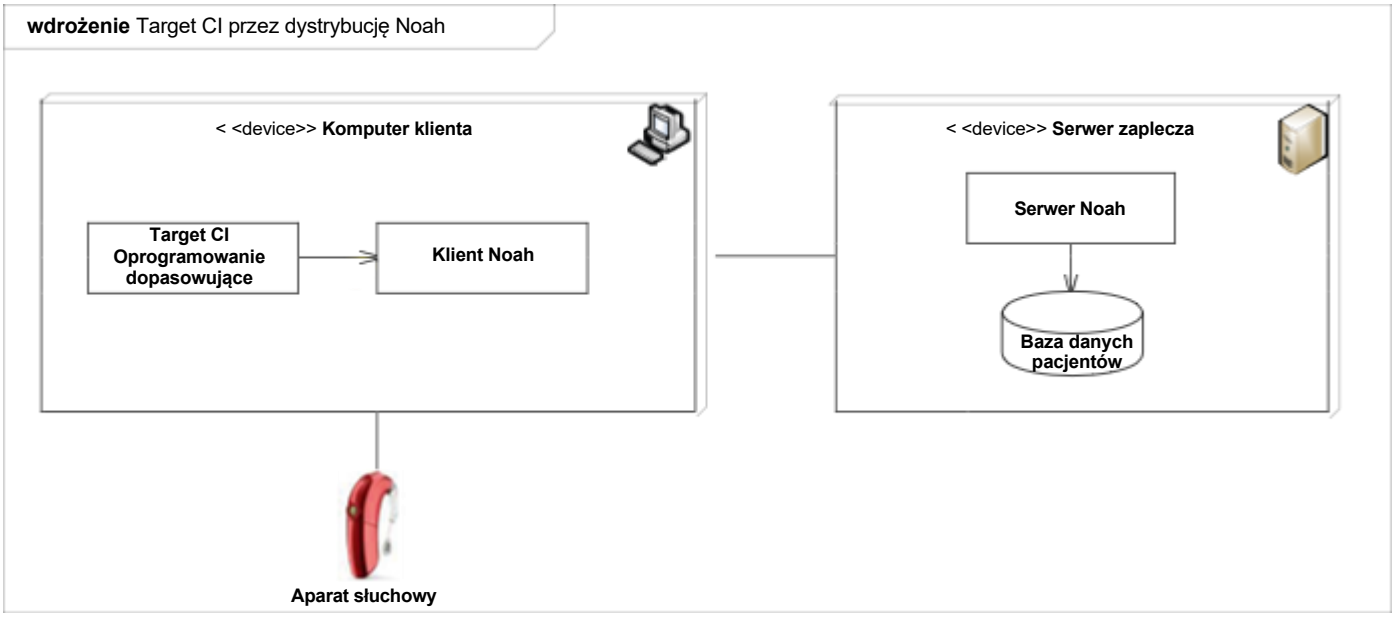
W modelu wdrożenia samodzielnym oprogramowanie dopasowujące jest instalowane na komputerze klienckim. Baza danych pacjentów przechowywana jest na tym samym komputerze i instalowana razem z oprogramowaniem dopasowującym.

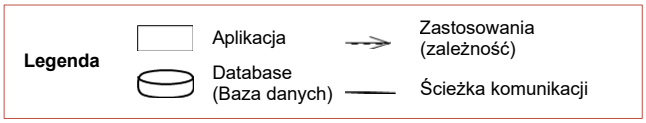




3.2 MODEL WDROŻENIA 2: DYSTRYBUCJA NOAH

W modelu wdrażania przez dystrybucję Noah oprogramowanie dopasowujące jest wdrażane na jednym lub większej liczbie komputerów klienckich. Noah, zewnętrzny system zarządzania pacjentami, jest wdrożony na wewnętrznym serwerze, do którego dostęp mają komputery klienckie. Baza danych pacjentów przechowywana jest na serwerze Noah i dostęp do niej można uzyskać za pośrednictwem sieci z jednego lub większej liczby komputerów klienckich.



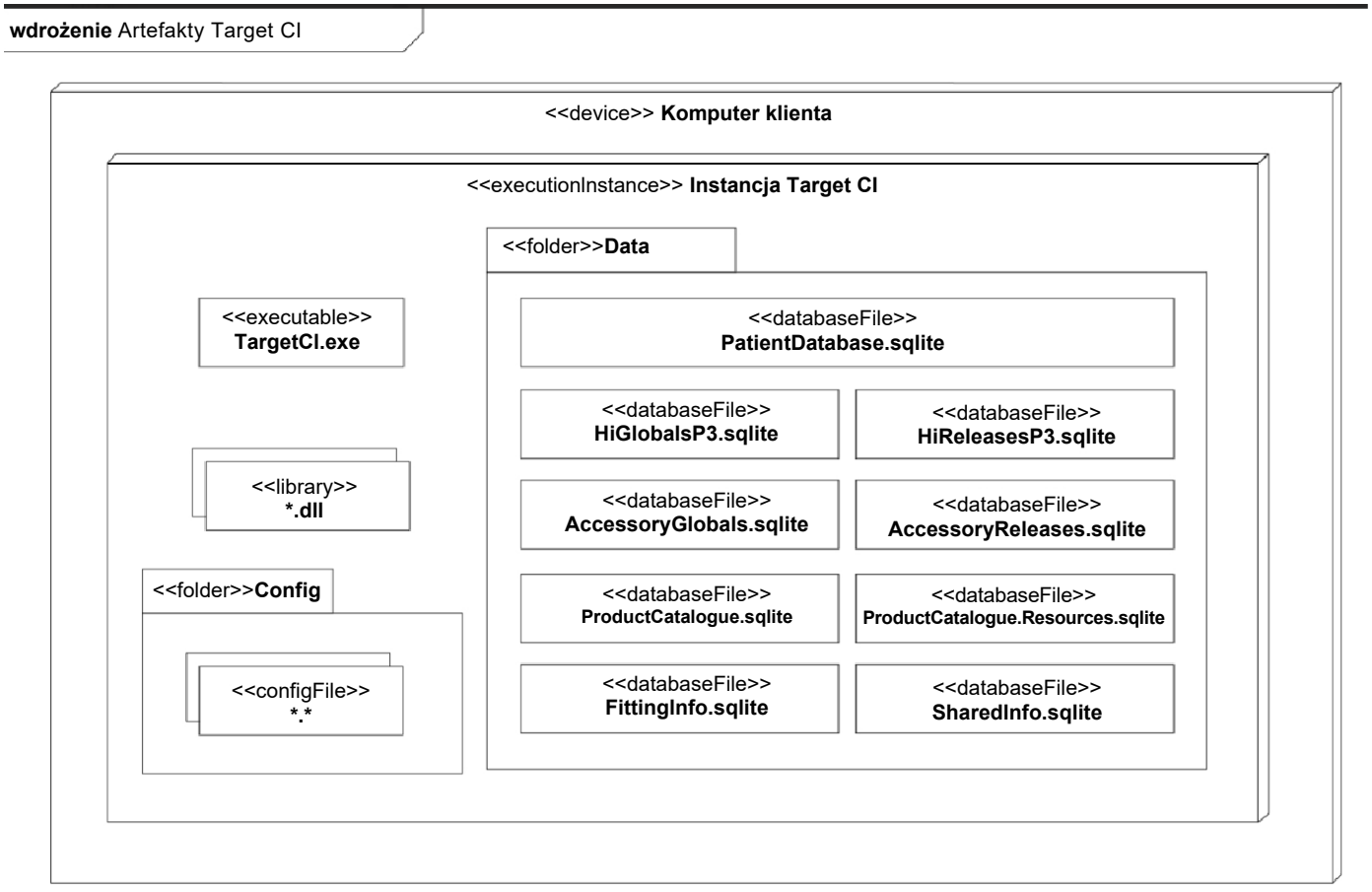


3.3 ARTEFAKTY WDROŻENIA

Oprogramowanie dopasowujące instaluje się z plikiem wykonywalnym i zestawem powiązanych plików, obejmujących biblioteki DLL komponentów, pliki konfiguracyjne i pliki bazy danych SQLite. Pliki konfiguracyjne są instalowane w folderze „%ProgramData%\ Advanced Bionics\Target CI\Target CI\Config" a pliki bazy danych są instalowane w folderze „%ProgramData%\Advanced Bionics\Target CI\Target CI\Data." Folder Data zawiera pojedynczy plik bazy danych transakcyjnych i kilka plików bazy danych informacyjnych.

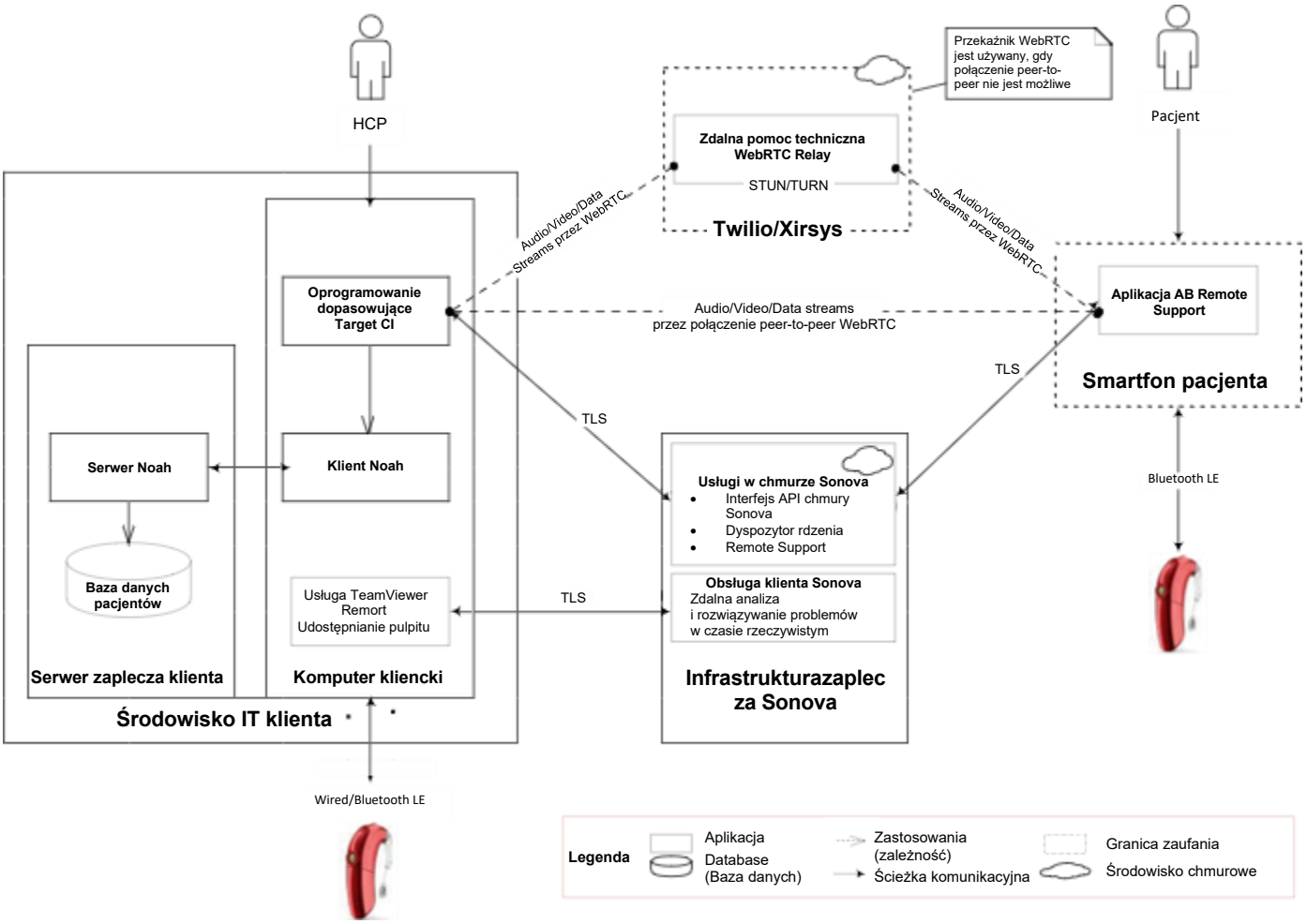
Baza danych transakcyjnych PatientDatabase.sqlite przechowuje dane demograficzne i dane dotyczące dopasowania pacjenta. Zostanie ona zainstalowana tylko wtedy, gdy oprogramowanie dopasowujące zostanie wdrożone w trybie samodzielnym.

Gdy oprogramowanie dopasowywujące jest wdrożone jako moduł Noah, system Noah dostarcza wymagane usługi trwałości danych pacjenta do oprogramowania dopasowującego. Pozostałe pliki sqlite są integralną częścią oprogramowania dopasowującego i są wymagane we wszystkich modelach wdrożeniowych.



3.4 POŁĄCZENIA SYSTEMOWE

Poniższy schemat i tabela ilustrują podstawowe połączenia systemowe. Zazwyczaj wykorzystywana jest tylko część dostępnych połączeń.



Źródło / Miejsce docelowe	Usługa	Protokół	Port	Opis
Aparaty słuchowe	Komunikacja za pomocą aparatu słuchowego	Połączenie przewodowe / Bluetooth® Low Energy	Nie dotyczy	Służy do komunikacji z aparatami słuchowymi w celu sterowania, konfiguracji i sprawdzania statusu i celów odczytu danych
Noah	Noah 4 ModuleAPI	Zdalna obsługa .NET	Nie dotyczy	Podstawowy interfejs modułu służącego do dostępu do oprogramowania Noah (tylko w modelu wdrażania przez dystrybucję Noah)
Usługi w chmurze Sonova	Sonova Cloud API, Core dispatcher, Remote support	SOAP, REST	443	Usługi Sonova hostowane w centrum danych Microsoft Azure służą do: • pobierania danych konfiguracji klienta oprogramowania

Źródło / Miejsce docelowe	Usługa	Protokół	Port	Opis
				dopasowującego z pamięci masowej zaplecza Sonova • rejestrowania transferów i danych analitycznych • ustanawiania zdalnej sesji dopasowania w czasie rzeczywistym
Twilio/Xirsys, Aplikacja mobilna AB Remote Support	Remote Support	WebRTC	Lista portów dostępna na żądanie	Usługi komunikacji w chmurze firmy Twilio są hostowane na platformach chmurowych innych firm, w szczególności Amazon Web Services (AWS) i Google Cloud Platform (GCP). Usługi te wykorzystywane są wyłącznie przez funkcję zdalnego wsparcia oprogramowania dopasowującego, która umożliwia sygnalizację WebRTC i przeprowadzanie sesji dopasowania w czasie rzeczywistym.
Obsługa klienta AB	Udostępnianie pulpitu	Protokół zastrzeżony TeamViewer	5938, 443, 80 Zobacz TeamViewerPorts	Służy do przeprowadzania zdalnej analizy w czasie rzeczywistym i rozwiązywania problemów związanych z instalacją oprogramowania dopasowującego. Więcej informacji można znaleźć w rozdziale 6.6 OBSŁUGA ZDALNA.

4. Wymagania systemowe

System operacyjny	Windows 10, Pro/Enterprise
Środowisko .NET Framework	Wersja 4.8
Procesor	Procesor Intel® Core™ i5 lub równoważny o równej lub lepszej wydajności
Pamięć RAM	4 GB lub więcej
Przestrzeń na dysku twardym	3 GB lub więcej
Minimalne wymagania dotyczące wyświetlacza	• Rozdzielczość 1280 x 1024 (maksymalne skalowanie 125%) • 24-bitowy kolor
Sterowniki urządzeń	• Sterownik sieci bezprzewodowej Noahlink (w przypadku korzystania z interfejsu programowania sieci bezprzewodowej Noahlink innej firmy podłączonego przez USB wymagana jest najnowsza wersja udostępniana przez HIMSA). • Sterownik CPI-3 (wymagany w przypadku korzystania z interfejsu programowania CPI-3 podłączonego przez USB).

Database (Baza danych)	SQLite lub Noah System 4 (wersja 4.14 lub nowsza)
Połączenie internetowe	Do zdalnego wsparcia i rejestrowania analiz wymagane jest połączenie z Internetem, patrz sekcja 4.4 Połączenia systemowe; w przypadku korzystania z sieciowego systemu Noah 4 wymagany jest intranet.
Porty sieciowe	Zobacz sekcję 3.4 Połączenia systemowe; zobacz sekcję 3. Inne zasoby — HIMSA, aby sprawdzić porty używane przez system Noah 4.

5. WYMAGANIA

5.1 INSTALACJI

Aby zainstalować odpowiednie oprogramowanie, wymagane jest konto administratora. Po zainstalowaniu oprogramowania można je uruchamiać bez uprawnień administracyjnych lub podwyższonego poziomu uprawnień.

Informacje na temat sprawdzania integralności oprogramowania przed instalacją można znaleźć w rozdziale 8, Integralność oprogramowania.

Przed instalacją administratorom systemu zaleca się upewnienie się, że:

• instalowana jest najnowsza dostępna wersja oprogramowania.

• system operacyjny jest aktualny.

5.2 TYPY INSTALATORÓW

Do instalacji oprogramowania montażowego dostępne są dwa instalatory:

• Standardowy instalator

• Instalator dla profesjonalistów IT

Instalator dla profesjonalistów IT jest pojedynczym plikiem MSI i nie zawiera wymaganych komponentów, ale poza tym jest równoważny instalatorowi standardowemu.

Do wymaganych komponentów należą Microsoft .NET Framework w wersji 4.8 i pakiety redystrybuowalne Microsoft Visual C++

Oba instalatory obsługują zaawansowane scenariusze instalacji, w tym instalację cichą.

Instalatora dla profesjonalistów IT należy używać wyłącznie wtedy, gdy organizacja wymaga, aby instalowała i zarządzała niezbędnymi komponentami sama, a nie przez odpowiedniego instalatora oprogramowania. W pozostałych przypadkach należy używać Instalatora standardowego.

Instalator dla profesjonalistów IT można uzyskać od przedstawiciela klinicznego AB. Instalatora dla profesjonalistów IT nie można używać do naprawy, ponownej instalacji ani odinstalowywania instalacji wykonanych przy użyciu instalatora standardowego. Instalatora standardowego nie można używać do naprawy, ponownej instalacji ani odinstalowywania instalacji wykonanych przez Instalator dla profesjonalistów IT.

6. KONTROLA BEZPIECZEŃSTWA

Oprogramowanie dopasowujące jest aplikacją kliencką instalowaną na komercyjnym komputerze PC z systemem Microsoft Windows. Oprogramowanie dopasowujące można zainstalować jako samodzielną aplikację lub jako moduł Noah.

6.1 UWIERZYTELNIANIE – WDROŻENIE SAMODZIELNE

Gdy oprogramowanie dopasowujące jest zainstalowane jako samodzielna aplikacja, korzysta z mechanizmów kontroli dostępu udostępnianych przez system operacyjny hosta. System operacyjny hosta może zostać skonfigurowany przez personel IT klienta w celu zarządzania uwierzytelnianiem. Oprogramowanie dopasowujące nie posiada takiej integralnej funkcji. Advanced Bionics zaleca, aby każdy użytkownik logował się do systemu operacyjnego hosta przy użyciu unikalnego konta użytkownika.

6.2 UWIERZYTELNIANIE – WDROŻENIE NOAH

Po zainstalowaniu oprogramowania dopasowującego jako modułu Noah, kontrolę dostępu zapewnia Noah System 4. Informacje na temat kontroli audytu stosowanych przez Noah System 4 można znaleźć na stronie www.HIMSA.com.

6.3 UWIERZYTELNIANIE

Oprogramowanie dopasowujące nie ogranicza dostępu do swoich funkcji na podstawie ról poszczególnych użytkowników. Oprogramowanie spełnia jedną główną funkcję: dopasowywanie aparatów słuchowych pacjentom oraz rolę profesjonalnego dopasowującego. Kontrola dostępu oparta na rolach nie ma zastosowania.

6.4 AUDYT – WDROŻENIE SAMODZIELNE

Gdy oprogramowanie dopasowujące jest instalowane jako samodzielna aplikacja, korzysta z mechanizmów audytu udostępnianych przez system operacyjny hosta. Oprogramowanie dopasowujące nie posiada takiej zintegrowanej funkcji. System operacyjny hosta może zostać skonfigurowany przez personel IT klienta w celu rejestrowania wywołań odpowiedniego oprogramowania i loginów użytkowników. Advanced Bionics zaleca, aby każdy użytkownik logował się do systemu operacyjnego hosta przy użyciu unikalnego konta użytkownika, aby ułatwić audyt.

6.5 AUDYT – WDROŻENIE NOAH

Po zainstalowaniu oprogramowania dopasowującego jako modułu Noah, system Noah dostarcza dzienniki audytu. Zobacz kontrolę audytu https://www.himsa.com/ do stosowaną przez Noah System 4.

6.6 ZDALNY DOSTĘP

Funkcja udostępniania pulpitu umożliwia zdalną analizę w czasie rzeczywistym i rozwiązywanie problemów dotyczących instalacji odpowiedniego oprogramowania. Funkcja ta oparta jest na narzędziu innej firmy o nazwie TeamViewer QuickSupport (wdrażanym domyślnie wraz z odpowiednim oprogramowaniem) i umożliwia pracownikom pomocy technicznej AB zdalne połączenie się z komputerem pracownika pomocy technicznej i uzyskanie pełnej kontroli nad nim, łącznie z dostępem do systemu operacyjnego i plików.

Aby nawiązać sesję udostępniania pulpitu, wymagana jest interakcja z pracownikiem służby zdrowia. HCP musi najpierw uruchomić narzędzie TeamViewer QuickSupport (np. za pośrednictwem oprogramowania dopasowującego Target CI) i przekazać swoje dane uwierzytelniające TeamViewer zespołowi wsparcia AB za pośrednictwem kanału komunikacji poza pasmem (np. rozmowy telefonicznej).

Imię i nazwisko członka zespołu wsparcia AB oraz jego identyfikator TeamViewer są domyślnie wyświetlane na monitorze komputera pracownika służby zdrowia podczas każdej aktywnej sesji udostępniania pulpitu.

Cały ruch sieciowy w ramach udostępniania pulpitu jest zabezpieczony zgodnie ze standardami protokołów kryptograficznych i algorytmów (RSA) lub je przewyższającymi public/private wymiana kluczy i szyfrowanie sesji AES 256-bit).

TeamViewer QuickSupport można usunąć ręcznie bez wpływu na inne funkcje Target FSW. Program instalacyjny Target FSW obsługuje parametry instalacji z poziomu wiersza poleceń, co pozwala na instalację Target FSW z poziomu wiersza poleceń bez konieczności dołączania narzędzia TeamViewer QuickSupport.

7. OCHRONA INFORMACJI

7.1 POLITYKA PRYWATNOŚCI ADVANCED BIONICS

Politykę prywatności opisującą sposób gromadzenia, przesyłania, przechowywania i wykorzystywania danych osobowych przez firmę Advanced Bionics można pobrać ze strony: AdvancedBionics.com/privacy.

Firma Advanced Bionics nie hostuje, nie przechowuje, nie tworzy kopii zapasowych ani nie ma dostępu do żadnych danych przechowywanych w oprogramowaniu do dopasowania ani w bazach danych Noah, chyba że dane te zostaną wyraźnie przesłane do firmy Advanced Bionics.

7.2 FEDERALNE STANDARDY PRZETWARZANIA INFORMACJI (FIPS)

Target CI wer. 1.5 jest zgodny ze standardami szyfrowania FIPS 140-2.

7.3 BEZPIECZEŃSTWO W TRANSPORCIE

Bezpieczeństwo komunikacji jest zapewnione i włączone we wszystkich przychodzących i wychodzących komunikatach sieciowych oprogramowania montażowego. Z wyjątkiem funkcji Zdalnego Wsparcia (wykorzystującej protokół WebRTC) i komunikacji Bluetooth z aparatami słuchowymi & Akcesoria, wszystkie pozostałe połączenia chronione są protokołem Transport Layer Security (TLS), który zapewnia poufność, integralność i autentyczność.

TLS

Konfiguracja protokołu TLS jest zgodna z aktualnymi najlepszymi praktykami i zaleceniami dotyczącymi bezpieczeństwa udokumentowanymi w dokumencie BCP 195 – Rekomendacje dotyczące bezpiecznego korzystania z protokołów TLS i DTLS, BCP195, obejmującymi:

- Brak obsługi wersji SSL i TLS starszych niż 1.2
- Brak obsługi zestawów szyfrów wykorzystujących algorytmy kryptograficzne oferujące mniej niż 128 bitów bezpieczeństwa
- Obsługa zalecanych rozszerzeń TLS protokołu BCP 195
- Brak obsługi niebezpiecznych rozszerzeń BCP 195

DTLS

Szyfrowanie jest obowiązkową funkcją WebRTC i jest stosowane we wszystkich strumieniach multimedialnych przesyłanych przez WebRTC. Stosowany protokół szyfrowania zależy od typu kanału. Strumienie danych są szyfrowane przy użyciu protokołu DTLS, a strumienie multimedialne przy użyciu protokołu SRTP (Secure Real-time Transport Protocol), ponieważ jest to lżejsza opcja niż DTLS.

Aby uzyskać bardziej szczegółowe informacje na temat konfiguracji zabezpieczeń usługi Remote Support WebRTC, zapoznaj się z poniższym linkiem:

https://developer.liveswitch.io/liveswitch-server/server/security.html

BLE

Bezprzewodowa komunikacja Bluetooth Low Energy z aparatami słuchowymi i akcesoriami jest domyślnie szyfrowana, a jej integralność jest chroniona (z wyjątkiem przypadków identyfikacji i wykrywania). Ponadto czas trwania trybu parowania Bluetooth aparatu słuchowego jest ograniczony czasowo. Bardziej szczegółowy opis bezpieczeństwa kanału komunikacji Bluetooth można znaleźć w dokumentacji danego aparatu słuchowego.

7.4 BEZPIECZEŃSTWO W SPOCZYNKU

Baza danych pacjentów – model wdrożenia samodzielnego

Jeżeli oprogramowanie dopasowujące jest zainstalowane jako samodzielna aplikacja, baza danych pacjentów jest przechowywana lokalnie w: C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

Te rekordy nie są domyślnie szyfrowane w stanie spoczynku. Chronione informacje dotyczące zdrowia (PHI) i dane osobowe (PII) są przechowywane w bazie danych wewnętrznej oprogramowania dopasowującego i nie są przesyłane przez sieć.

W niektórych jurysdykcjach przepisy mogą wymagać szyfrowania wszystkich danych pacjentów w celu uniknięcia potencjalnej odpowiedzialności w przypadku utraty lub kradzieży danych. Włączyć funkcję BitLocker lub równoważne pełne szyfrowanie dysku (na poziomie systemu operacyjnego lub sprzętowe), aby zabezpieczyć dane przed nieautoryzowanym dostępem lub kopiowaniem, gdy dane nie są używane.

BitLocker to wbudowana funkcja systemu Windows, która szyfruje cały dysk i wymaga uwierzytelnienia, aby uzyskać do niego dostęp. Przed włączeniem funkcji BitLocker należy zawsze zapoznać się z oficjalnymi wytycznymi firmy Microsoft oraz polityką bezpieczeństwa IT obowiązującą w organizacji.

Jak włączyć funkcję BitLocker

Do zarządzania funkcją BitLocker wymagane są uprawnienia administratora.

1. Wyszukać opcję „Zarządzaj funkcją BitLocker”

   Otwórz menu Start, wpisać „Zarządzaj funkcją BitLocker” i wybrać ją z wyników wyszukiwania.

2. Wybrać dysk systemowy

   Wybrać dysk, na którym zainstalowany jest system Windows, aby skonfigurować ustawienia szyfrowania.

3. Wybrać metodę odblokowania

   Można wybrać jedną z poniższych opcji:

   - Tylko TPM
   - TPM + PIN
   - TPM + Klucz USB

   Wybierając metodę odblokowania, postępować zgodnie z najlepszymi praktykami firmy Microsoft i polityką bezpieczeństwa IT swojej organizacji.

4. Utworzyć kopię zapasową klucza odzyskiwania

Utworzyć kopię zapasową klucza odzyskiwania, korzystając z bezpiecznych metod zatwierdzonych przez przedsiębiorstwo. Zalecane opcje obejmują:

- Przechowywanie w Microsoft Entra ID (dawniej Azure AD) lub Active Directory dla urządzeń przyłączonych do domeny

- Zapisywanie w bezpiecznej lokalizacji sieciowej z kontrolą dostępu, szyfrowaniem i rejestrowaniem audytu

- Korzystanie z rozwiązania do zarządzania depozytem kluczy zatwierdzonego przez organizację

Unikać zapisywania klucza na dyskach lokalnych, nośnikach USB ani drukowania go, chyba że zasady wyraźnie na to zezwalają. Klucze odzyskiwania muszą być chronione z taką samą starannością jak inne poufne dane uwierzytelniające i natychmiast wymieniane w przypadku ich ujawnienia.

5. Rozpoczynanie szyfrowania

Wybrać:

- Cały dysk – zalecane w większości scenariuszy korporacyjnych. Szyfruje wszystkie sektory, łącznie z niewykorzystaną przestrzenią, aby zapobiec ponownemu gromadzeniu się danych.

Baza danych pacjentów – moduł dystrybucji Noah

Po zainstalowaniu oprogramowania dopasowującego jako modułu Noah, dane osobowe są przechowywane w bazie danych pacjentów hostowanej w Noah. Baza danych pacjentów hostowana w Noah może znajdować się na innym komputerze. Dane osobowe i inne dane pacjenta przechowywane są przez oprogramowanie Noah, a szyfrowanie danych pacjenta w stanie spoczynku jest zapewnione przez system Noah. Oprogramowanie dopasowujące może przekazywać/odbierać dane osobowe za pośrednictwem przewodowego lub bezprzewodowego połączenia sieciowego, gdy baza danych Noah jest skonfigurowana do dostępu sieciowego.

Informacje PII przechowywane w sieciowej bazie danych Noah będą widoczne dla innych użytkowników urządzeń na różnych komputerach, którzy mają uprawnienia do tej samej sieciowej bazy danych. Bazę danych Noah można również skonfigurować tak, aby nie wymagała dostępu przez sieć i zainstalować ją na tym samym komputerze, co oprogramowanie dopasowujące.

Noah uniemożliwia oprogramowaniu dopasowującemu dostęp do bazy danych dokumentacji medycznej pacjenta. Gdy użytkownik otwiera dane pacjenta w oprogramowaniu dopasowującym za pośrednictwem klienta Noah, oprogramowanie może jedynie odczytywać i zapisywać dane w aktualnie otwartej dokumentacji pacjenta, nie ma natomiast dostępu do innych dokumentacji pacjentów w bazie danych Noah.

Zobacz stronę www.HIMSA.com, aby zapoznać się ze standardami szyfrowania używanymi przez Noah System 4.

Pliki eksportowe RMA

Oprogramowanie dopasowujące pozwala na eksport informacji o kliencie do pliku. Plik RMA można wysłać do firmy Advanced Bionics w celu rozwiązania problemu RMA lub związanego z nim wsparcia.

Plik RMA jest szyfrowany asymetrycznie algorytmem RSA przy użyciu klucza o długości 512 bitów. Oprogramowanie dopasowujące nie posiada funkcji odszyfrowywania pliku RMA.

Anonimizowane pliki eksportowe

Oprogramowanie dopasowujące pozwala na eksport danych pacjenta do anonimowego pliku. Dane osobowe pacjenta, takie jak data urodzenia i imię, zostają zastąpione wartościami ogólnymi. Plik nie jest szyfrowany i można go zaimportować do tej samej lub innej instancji oprogramowania dopasowującego.

Standardowe pliki eksportowe

Oprogramowanie dopasowujące pozwala na eksport informacji o kliencie do standardowego pliku eksportowego. Plik używa zastrzeżonego formatu binarnego i nie jest szyfrowany. Plik można zaimportować do tego samego lub innego oprogramowania dopasowującego. Korzystając z tej funkcji, użytkownicy oprogramowania dopasowującego muszą upewnić się, że standardowe pliki eksportowe są obsługiwane zgodnie z lokalnymi zasadami IT dotyczącymi zarządzania niezaszyfrowanymi danymi osobowymi.

Aparat słuchowy

Oprogramowanie dopasowujące aparatów słuchowych zapisuje informacje o pacjencie na jego aparacie słuchowym. Dane osobowe, takie jak imię i nazwisko czy data urodzenia, nie są przechowywane na aparacie słuchowym. Pozostałe informacje nieosobowe są przechowywane przy użyciu szyfrowania PBKDF2 z kluczem 128-bitowym.

Oprogramowanie dopasowujące może wysyłać/odbierać informacje o kliencie niebędące danymi osobowymi do/z aparatu słuchowego za pośrednictwem przewodowego urządzenia firmowego (np. CPI-3), aplikacji mobilnej AB Remote Support lub urządzenia bezprzewodowego Noahlink. Urządzenie bezprzewodowe Noahlink łączy się z aparatem słuchowym za pomocą technologii Bluetooth Low Energy (BLE) za pośrednictwem standardowego kanału BLE z szyfrowaniem AES 128-bitowym.

8. INTEGRALNOŚĆ OPROGRAMOWANIA

8.1 WERYFIKACJA POBRANYCH NOŚNIKÓW INSTALACYJNYCH

Oprogramowanie do instalacji modułu Target CI można pobrać w niektórych regionach z portalu Pro Portal firmy Advanced Bionics lub klienta Sonova Web Client. Pobrany nośnik instalacyjny można uwierzytelnić przy użyciu dowolnego zaufanego narzędzia do haszowania SHA-256.

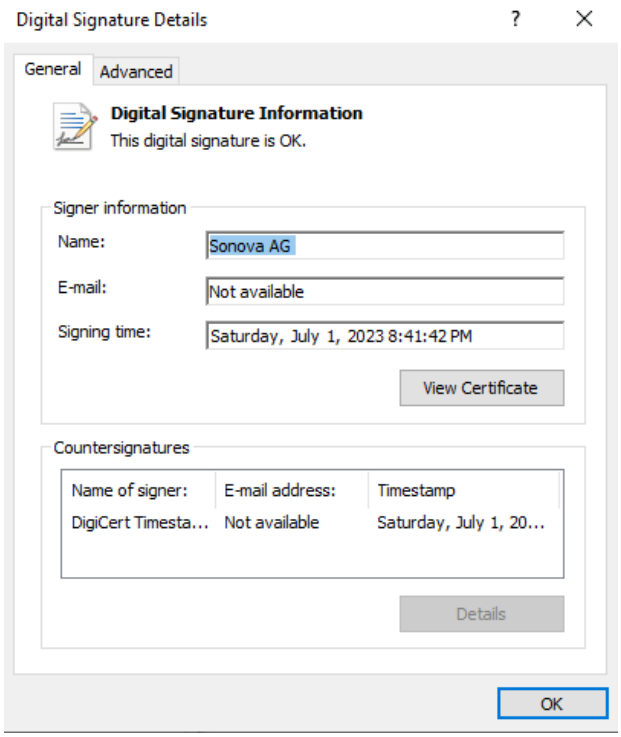
Skrót SHA256 dla standardowego pliku instalacyjnego ZIP to:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

Skrót SHA256 dla pliku zip instalacyjnego oprogramowania dla profesjonalistów IT to:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 RĘCZNA WERYFIKACJA OPROGRAMOWANIA DOPASOWUJĄCEGO PRZED INSTALACJĄ

Aby sprawdzić integralność i autentyczność oprogramowania dopasowującego przed instalacją, użytkownicy mogą wykonać następujące czynności:

1. Otworzyć Eksplorator Windows i przejść do folderu głównego nośnika instalacyjnego oprogramowania. Jeśli nośnikiem instalacyjnym jest pendrive, włożyć go do portu USB i przejść do jego katalogu głównego. Jeśli nośnik instalacyjny jest plikiem zip, rozpakować go do folderu i przejść do niego.
2. Kliknąć prawym przyciskiem myszy SonovaVerify.exe i wybrać Właściwości z menu kontekstowego.
3. Wybrać kartę Podpisy cyfrowe.
4. Kliknąć dwukrotnie podpis SHA256 „Sonova AG”.
5. Sprawdzić, czy elementy podpisu są prawidłowe. Sprawdzić w szczególności, czy komunikat „The digital signature is OK.” (Podpis cyfrowy jest prawidłowy) pojawia się w górnej części ekranu i czy imię i nazwisko osoby podpisującej oraz czas złożenia podpisu odpowiadają poniższemu obrazkowi:



1. Zamknąć okna dialogowe i kliknąć dwukrotnie plik SonovaVerify.exe.
2. Sprawdzić, czy wyświetla się komunikat „NO ERRORS DETECTED.” (NIE WYKRYTO BŁĘDÓW), jak pokazano na poniższym obrazku:

Na obrazku widać, że SonovaVerify uwierzytelnił i zweryfikował podpisy cyfrowe wszystkich plików na nośniku instalacyjnym, łącznie z instalatorem. Pozwala to sprawdzić, czy nośnik instalacyjny nie został zmodyfikowany, uszkodzony lub w inny sposób naruszony. SonovaVerify wyświetli ostrzeżenia lub komunikaty o błędach, jeśli brakuje plików lub folderów albo jeśli do nośnika instalacyjnego dodano nieoczekiwane pliki lub foldery.

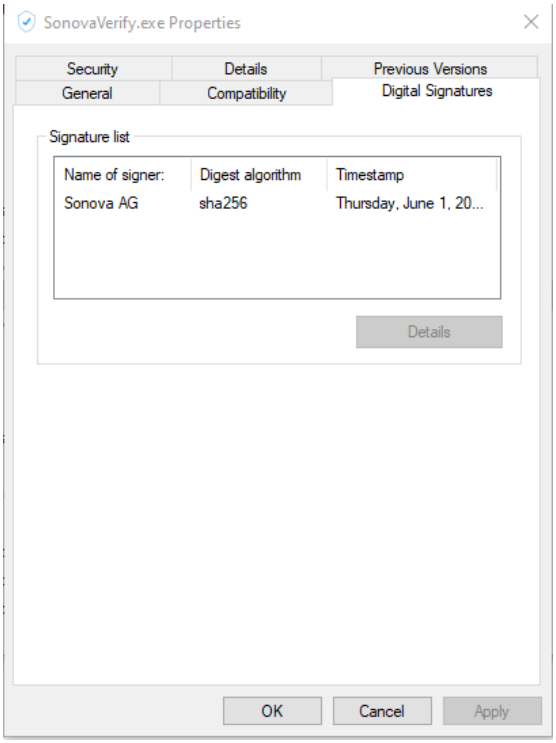
8.3 AUTOMATYCZNA WERYFIKACJA INTEGRALNOŚCI ZAINSTALOWANEGO OPROGRAMOWANIA DO INSTALACJI

Narzędzie SonovaVerify jest zintegrowane z oprogramowaniem dopasowującym i uruchamia się przy każdym uruchomieniu aplikacji, aby sprawdzić integralność plików programowych oprogramowania dopasowującego. Pliki programów są podpisywane cyfrowo przy użyciu standardowych praktyk branżowych i certyfikatów wydanych przez zaufany urząd certyfikacji. Oprogramowanie powiadamia użytkownika za pomocą komunikatów ostrzegawczych, jeśli którykolwiek z plików programu zostanie naruszony.

8.4 RĘCZNA WERYFIKACJA INTEGRALNOŚCI ZAINSTALOWANEGO OPROGRAMOWANIA DO INSTALACJI

Użytkownicy mogą w dowolnym momencie, bez konieczności uruchamiania oprogramowania, wykonać poniższe czynności w celu sprawdzenia integralności i autentyczności zainstalowanego oprogramowania dopasowującego:

1. Otworzyć Eksplorator Windows i przejść do folderu wykonywalnego odpowiedniego oprogramowania, który zwykle znajduje się w: C:\Program Akta (x86)\Advanced Bionics\Target CI\
2. Kliknąć prawym przyciskiem myszy SonovaVerify.exe i wybrać Właściwości z menu kontekstowego.
3. Wybrać kartę Podpisy cyfrowe.
4. Kliknąć dwukrotnie podpis SHA256 „Sonova AG”.
5. Sprawdzić, czy wszystkie elementy podpisu są prawidłowe, w szczególności czy w górnej części pojawia się komunikat „The digital signature is OK.” (Podpis cyfrowy jest prawidłowy) oraz czy imię i nazwisko osoby podpisującej oraz czas złożenia podpisu odpowiadają poniższemu obrazkowi:



1. Zamknąć okna dialogowe i kliknąć dwukrotnie plik SonovaVerify.exe.
2. Sprawdzić, czy wyświetla się komunikat „NO ERRORS DETECTED.” (NIE WYKRYTO BŁĘDÓW), jak pokazano na poniższym obrazku:

Na obrazku widać, że SonovaVerify uwierzytelnił i zweryfikował podpisy cyfrowe wszystkich zainstalowanych plików programu. Potwierdza to, że oprogramowanie dopasowujące nie zostało zmodyfikowane, uszkodzone lub w inny sposób naruszone. SonovaVerify wyświetli ostrzeżenia lub komunikaty o błędach, jeśli brakuje plików lub folderów albo jeśli do folderu plików programu dodano nieoczekiwane pliki lub foldery.

9. POPRAWKI I AKTUALIZACJE OPROGRAMOWANIA

Automatyczne aktualizacje nie są obsługiwane.

10. ZARZĄDZANIE DANYMI

10.1 BAZY DANYCH

Oprogramowanie dopasowujące wykorzystuje transakcyjną bazę danych do przechowywania danych pacjenta oraz zestaw baz danych informacyjnych, które zapewniają konfiguracje metadanych wymagane przez aplikację.

Szczegółową listę wszystkich baz danych wdrożonych przez oprogramowanie dopasowujące można znaleźć w sekcji 3. Diagramy sieciowe i kontekstowe — Artefakty wdrożenia.

Jeśli oprogramowanie dopasowujące jest zainstalowane jako samodzielna aplikacja, baza danych pacjentów staje się wewnętrzna w oprogramowaniu dopasowującym. Baza danych pacjentów, zapisana w pliku PatientDatabase.sqlite, znajduje się na tym samym komputerze co oprogramowanie dopasowujące i stanowi miejsce przechowywania danych pacjentów. Aby wykonać kopię zapasową danych aplikacji, gdy Target CI jest wdrażany jako samodzielna aplikacja, utworzyć kopię zapasową całego folderu znajdującego się w folderze %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Chronić kopie zapasowe danych nie tylko przed utratą danych, ale również przed kradzieżą. Po zainstalowaniu oprogramowania dopasowującego jako modułu Noah, dane pacjenta są zapisywane w bazie danych udostępnianej przez system Noah. Bazę danych Noah można skonfigurować tak, aby umożliwiała dostęp sieciowy. Bazę danych Noah można również skonfigurować tak, aby nie wymagała dostępu przez sieć i zainstalować ją na tym samym komputerze, co oprogramowanie dopasowujące. Skonfigurować szyfrowanie bazy danych Noah, aby chronić dane (zapoznać się z dokumentacją HIMSA).

W przypadku trybu wdrażania przez dystrybucję Noah, instrukcje dotyczące tworzenia kopii zapasowej i przywracania bazy danych pacjentów Noah można znaleźć pod poniższym linkiem:

https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/

10.2 MIGRACJA DANYCH

Oprogramowanie dopasowujące aparatów słuchowych umożliwia użytkownikom migrację dokumentacji pacjentów z poprzedniego oprogramowania dopasowującego aparatów słuchowych firmy AB, SoundWave 3.2. Aby można było przeprowadzić migrację, dokumentacja medyczna musi być dostępna z poziomu instalacji SoundWave 3.2 na tym samym komputerze, na którym znajduje się Target CI.

10.3 KONFIGURACJE APARATÓW SŁUCHOWYCH

Oprogramowanie dopasowujące umożliwia eksportowanie i importowanie konfiguracji i ustawień urządzenia.

10.4 UTYLIZACJA

Instrukcje dotyczące usuwania danych można znaleźć w instrukcji obsługi (IFU) lub na następującej stronie w przypadku wdrożeń Noah: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

11. ŚRODOWISKO BEZPIECZEŃSTWA – WSPÓLNA ODPOWIEDZIALNOŚĆ

Oprogramowanie dopasowujące aparatów słuchowych zostało zaprojektowane do użytku, w którym zarządzanie ryzykiem cyberbezpieczeństwa jest uważane za wspólną odpowiedzialność interesariuszy w całym ekosystemie opieki słuchowej, w tym między innymi użytkowników aparatów słuchowych, rodziców lub opiekunów prawnych dzieci korzystających z aparatów słuchowych, pracowników służby zdrowia, administratorów IT, placówek i dostawców opieki słuchowej, dostawców aparatów słuchowych i sprzętu programującego.

Poniżej znajduje się lista rekomendacji dotyczących najlepszych praktyk i kontroli bezpieczeństwa dla środowiska, w którym będzie używane oprogramowanie dopasowujące:

Poziom systemu operacyjnego

- Zastosować kontrolę dostępu na poziomie systemu operacyjnego, np.:
  - Należy usunąć wszystkie konta typu Gość
  - Aktywować logowanie użytkownika Windows
  - Prowadzić listę autoryzowanych operatorów, aby kontrolować dostęp do systemu
  - Ustawić niestandardowych użytkowników i role
  - Stosować silne hasła i utrzymywać poufność danych uwierzytelniających
- Zastosować kontrole audytu na poziomie systemu operacyjnego
- Utrzymywać system operacyjny w aktualnym stanie.
- Utrzymywać aktualną wersję zainstalowanego oprogramowania.
- Włączyć aktualną ochronę przed złośliwym oprogramowaniem i oprogramowaniem antywirusowym
- Włączyć białą listę aplikacji

Ochrona danych

- Szyfrować dane pacjentów za pomocą narzędzi lub elementów sterujących innych firm na poziomie systemu operacyjnego, np. stosując szyfrowanie dysku (np. darmowy program Microsoft BitLocker), aby chronić wszystkie dane. W przypadku pracy w systemie Noah należy rozważyć szyfrowanie bazy danych Noah.
- Nośniki zewnętrzne zawierające dane eksportowane z oprogramowania dopasowującego, łącznie z raportami i dziennikami, powinny być zabezpieczone. Po zaprzestaniu użytkowania dane należy bezpiecznie usunąć i/lub zniszczyć ich nośniki.
- Używać nośników pamięci USB z wbudowaną funkcjonalnością zabezpieczającą, np. szyfrowanych dysków USB ze zintegrowaną klawiaturą.
- Pamiętać, aby zawsze dbać o bezpieczeństwo danych:
  - Przesyłając dane przez niebezpieczne kanały, należy albo wysyłać dane anonimowe, albo je szyfrować.
  - Chronić kopie zapasowe danych nie tylko przed utratą danych, ale również przed kradzieżą.
  - Usunąć z nośników danych wszystkie dane, które nie są już używane lub zostaną wyrzucone.

- Użytkownicy powinni stosować zatwierdzone procedury i narzędzia do bezpiecznego usuwania danych przechowywanych na nośnikach wymiennych, zgodnie z obowiązującymi przepisami i wytycznymi dotyczącymi postępowania z informacjami o pacjentach. / dane osobowe (PII) / chronione informacje zdrowotne (PHI)

Infrastruktura informatyczna

Korzystać z odpowiedniego oprogramowania w bezpiecznym środowisku sieciowym chronionym przed nieautoryzowanym dostępem. Istnieje wiele skutecznych technik izolowania i ochrony systemów informatycznych w medycynie, w tym wdrażanie zabezpieczeń w postaci zapór sieciowych, stref zdemilitaryzowanych (DMZ), wirtualnych sieci lokalnych (VLAN) i enklaw sieciowych. Aby otrzymywać aktualizacje systemu operacyjnego, utrzymywać aktywne połączenie sieciowe.

Poziom fizyczny

- Stanowisko pracy, na którym instalowane jest oprogramowanie dopasowujące, powinno być zabezpieczone fizycznie w sposób uniemożliwiający jego używanie przez nieupoważnionych użytkowników.
- Upewnić się, że osoby nieupoważnione nie będą manipulować systemem.
- Dostęp do drukarek podłączonych do stacji roboczej powinien być kontrolowany.
- Monitor stanowiska pracy, na którym zainstalowano oprogramowanie montażowe, należy umieścić w sposób ograniczający widoczność zawartości ekranu wyłącznie dla użytkownika.

Poziom organizacyjny

- Do obsługi tego systemu upoważnieni są wyłącznie profesjonalnie przeszkoleni, w pełni wykwalifikowani pracownicy. Przed udzieleniem komukolwiek upoważnienia do obsługi systemu należy sprawdzić, czy dana osoba przeczytała i w pełni rozumie instrukcję obsługi dostarczoną wraz z oprogramowaniem.
- Jeśli zauważy się jakąkolwiek podejrzaną aktywność na kontach oprogramowania dopasowującego lub nieoczekiwaną operację, skontaktuj się z firmą Advanced Bionics. Więcej informacji znajduje się w rozdziale 2.1.

Aby uzyskać więcej informacji na temat współodpowiedzialności i bardziej szczegółową listę zaleceń dotyczących najlepszych praktyk i kontroli bezpieczeństwa dla środowiska dopasowującego, w którym oprogramowanie dopasowujące będzie stosowane na różnych poziomach, zapoznać się z dokumentem dokumetem:

- Biała księga EHIMA „Najlepsze praktyki bezpiecznego dopasowywania aparatów słuchowych”, EHIMAWhitePaper

12. PROCES PRODUKCJI I ROZWOJU OPROGRAMOWANIA

Kwestia cyberbezpieczeństwa jest brana pod uwagę na każdym etapie procesu tworzenia oprogramowania. Oprogramowanie dopasowujące zostało opracowane zgodnie z normami IEC 62304 i IEC 82304.

Oprogramowanie dopasowujące jest skanowane w celu wykrycia wirusów i złośliwego oprogramowania w ramach procesu produkcyjnego.

Luki w zabezpieczeniach komponentów innych firm, wymienione w Krajowej Bazie Danych Podatności (NVD) NIST, są oceniane i łagodzone w trakcie procesu tworzenia oprogramowania oraz monitorowane po wprowadzeniu odpowiedniego oprogramowania na rynek.

13. SKŁADNIKI OPROGRAMOWANIA I LISTA MATERIAŁÓW

Oprogramowanie dopasowujące zawiera pewne gotowe, komercyjne komponenty oprogramowania.

Poniższa tabela zawiera listę wszystkich SOUP-ów (oprogramowania o nieznanym pochodzeniu) dystrybuowanych wraz z oprogramowaniem dopasowującym.

SOUP ITEM	OPIS FUNKCJONALNOŚCI	PRODUCENT	WERSJA
(ii) Korzystanie ze składnika System.Runtime.CompilerServices.Unsafe	Provides the System.Runtime. Klasa CompilerServices.Unsafe zapewniająca ogólną, niskopoziomową funkcjonalność do manipulowania wskaźnikami.	24rogramma, dotnetframework	5,0
(s) Korzystanie ze składnika Destructurama.Attributed	Używane przez biblioteki Nephele.	Współtwórcy Serilog	3.0
API SharpBITS	SharpBITS.NET to wrapper .NET dla interfejsu API BITS oraz niewielka aplikacja interfejsu użytkownika systemu Windows ułatwiająca dostęp do pobierania i wysyłania danych do usługi BITS.	perpetualKid	2.1.0.0
CredentialManagement	Pakiet zarządzania poświadczeniami to wrapper dla interfejsu API zarządzania poświadczeniami systemu Windows	iLya Lozovyy	1.0.2
CSharpAnalytics	Używane do Google Analytics.	Wzór ataku	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78
DirectShow 2005	Umożliwia dostęp do funkcjonalności DirectShow firmy Microsoft z poziomu aplikacji .NET.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	National Centre for Audiology, Kanada	4.2
DSL5	DSL 5 Fitting formula library	National Centre for Audiology, Kanada	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical przepakowany dla Sonova	GNOtometria	2.0.1.9
IceLink	Używane do WebRTC audio/video integracja konferencyjna	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect i Biblioteka klienta OAuth 2.0 używana przez komponent Kona.CommonServices.Authentication do uwierzytelniania OAuth 2.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Biblioteka interfejsu komunikacyjnego międzymodułowego Noah	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Używane przez biblioteki pochodzące z Sonova do komunikacji z Git	Współtwórcy LibGit2Sharp	0.26.1
Mapster	Służy do mapowania obiektów w kodzie	chaowlert,eric_swann	7.2.0.0
MathNet.Numerics	Służy do dopasowywania algorytmów (ścieżka sygnału, dopasowanie docelowe itp.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael i współpracownicy	4.11.0
Microsoft Visual C++ 2010 x86, redystrybuowalne	Microsoft Visual C++ 2010, redystrybuowalne	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012, redystrybuowalne	Microsoft Visual C++ 2012, redystrybuowalne	Microsoft	11.0.61030.0

SOUP ITEM	OPIS FUNKCJONALNOŚCI	PRODUCENT	WERSJA
Microsoft Visual C++ 2017, redystrybuowalne (x86)	Microsoft Visual C++ 2017, redystrybuowalne	Microsoft	14.16.27024.1
Microsoft.Bcl.AsyncInterfaces	Zapewnia IAsyncEnumerable <T> oraz interfejsy IAsyncDisposable i typy pomocnicze dla .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Używane przez biblioteki pochodzące z Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Używane przez biblioteki pochodzące z Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.Identity.Client	Biblioteka MSAL dla platformy .NET jest częścią platformy tożsamości Microsoft dla programistów (dawniej Azure AD) w wersji 2.0. Umożliwia ona pozyskiwanie tokenów bezpieczeństwa w celu wywoływania chronionych interfejsów API. Wykorzystuje standardy branżowe OAuth2 i OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions. Msal	Bezpieczna międzyplatformowa pamięć podręczna tokenów dla publicznych aplikacji klienckich MSAL.	Microsoft	2.19.3.0
Microsoft.IdentityModel. JsonWebTokens	Obejmuje typy zapewniające obsługę tworzenia, serializacji i walidacji Tokeny internetowe JSON. Używane przez komponenty komunikujące się z usługami zaplecza, które wykorzystują tokeny JSON Web Token do uwierzytelniania.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	Zależne od Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Zależne od SOAP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Używane jako narzędzie do tworzenia kopii zapasowych FSW (automatyczne tworzenie kopii zapasowych).	Dawid Hall	2.5.11.0
Microsoft.XAML.Behaviors.Wpf	XAML Behaviors to łatwy w użyciu sposób umożliwiający dodawanie typowych i wielokrotnego użytku funkcji interaktywnych do aplikacji WPF przy minimalnej ilości kodu.	xamlexperiencesteam, Microsoft	1.0.1
MS-VisualC++, biblioteki wykonawcze 7.1	Microsoft Visual C++, biblioteki wykonawcze	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1 Fitting formula library	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting formula library	Australian Hearing	2.0.11
NAudio.dll	Służy do regulacji głośności i odtwarzania plików dźwiękowych.	Open Source	1.9

SOUP ITEM	OPIS FUNKCJONALNOŚCI	PRODUCENT	WERSJA
Newtonsoft.Json	Służy do serializacji i deserializacji JSON.	James Newton-King	12.0.3
Nibelung	Biblioteki dopasowania bezprzewodowego NoahLink	GN ReSound	1.3.16.1
Nlog	Jest to zależność od HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	4.4.0
NoahLink	Sterownik urządzenia montażowego NoahLink	HIMSA	1.55.6.166
Noahlink Wireless	Sterownik Noahlink Wireless	HIMSA	2.0.0.68
Oszczędność	Służy do definiowania protokołu łącza zdalnego	Apache	0.13.0.0
Otometrics.HiPro2	Biblioteki komunikacyjne HiPro	GNOtometria	2.0.0.4
Otometrics.REMaccess	Warstwa abstrakcji Otometrics powyżej biblioteki interfejsu komunikacyjnego międzymodułowego Noah	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	Ten C# Biblioteka PDF umożliwiająca tworzenie i edycję dokumentów PDF w aplikacjach .Net.	Patagames.com	4.54.2704.0
Polly	Biblioteka umożliwiająca programistom płynne i bezpieczne dla wątków wyrażanie zasad odporności i obsługi błędów przejściowych, takich jak ponawianie próby, wyłącznik obwodu, izolacja grodzi i powrót do poprzedniego stanu.	App vNext	7.2.1
Polly.Contrib.WaitAndRetry	Biblioteka dla Polly zawierająca metody pomocnicze dla różnych strategii czekania i ponawiania próby.	Grant Dickinson, aplikacja vNext	1.1.1
Polly.Extensions.Http	Biblioteka zawierająca wygodne metody konfiguracji zasad Polly umożliwiające obsługę przejściowych błędów typowych dla wywołań przez HttpClient.	App vNext	3.0
protobuf-net.dll	Struktura serializacji używana dla blobu RC.	Open Source	2.0.0.668
Przenośny.Dmuchany Zamek	To zależność od HIMSA Nibelung.CPD (Noahlink Wirlesss)	BouncyCastle.Crypto	1.8.10.0
Renderowanie XPS do PDF (NiXPS)	Konwertuje pliki XPS 25grammatically do formatu PDF; używane w raportach aplikacji dopasowujących.	NiXPS	2.6.7.0
Security.Cryptography	Rozszerzenia interfejsów API zabezpieczeń dostarczanych wraz z platformą .NET Framework	Microsoft	1.7.2
Serilog	Komponent rejestrujący używany w całej aplikacji Chinook.	Współtwórcy Serilog	2.10.0
Serilog.Enrichers.Thread	Wzbogać zdarzenia Serilog o właściwości z bieżącego wątku	Współtwórcy Serilog	3.1

SOUP ITEM	OPIS FUNKCJONALNOŚCI	PRODUCENT	WERSJA
Serilog.Expressions	Filtrowanie zdarzeń oparte na wyrażeniach dla Serilog.	Współtwórcy Serilog	2.0
Serilog.Settings.AppSettings	Konfiguracja XML (Konfiguracja systemu < appSettings>) wsparcie dla Serilog.	Współtwórcy Serilog	2.2.2
Serilog.Sinks.Console	Serilog, który zapisuje zdarzenia dziennika do console/terminal.	Współtwórcy Serilog	4.0.0.0
Serilog.Sinks.Debug	Serilog, który zapisuje zdarzenia dziennika w oknie wyjściowym debugowania.	Współtwórcy Serilog	2.0
Serilog.Sinks.File	Zapisywanie zdarzeń Serilog do plików tekstowych w formacie zwykłym lub JSON.	Współtwórcy Serilog	4.1
Serilog.Sinks.Trace	Diagnostyczny ślad dla Serilog.	Współtwórcy Serilog	2.1
SharpZipLib	#ziplib (SharpZipLib, dawniej NzipLib) to biblioteka Zip, Gzip, Tar i Bzip2 napisana w całości w C# dla platformy .NET. Ta biblioteka udostępnia funkcjonalność kompresji (zip, unzip, kompresja strumieniowa itp.). Używamy go w aplikacji Aktualizacja oprogramowania sprzętowego.	Open Source	1.1.0.145
SM VC++ 2008 Redystrybuowalne	Microsoft Visual C++ 2008, redystrybuowalne	Microsoft	9.0.30729.6161
SQLite.Interop	SQLite to biblioteka oprogramowania zapewniająca system zarządzania relacyjnymi bazami danych. Słowo „lite” w języku SQLite oznacza lekkość pod względem konfiguracji, administrowania bazą danych i wymaganych zasobów. SQLite ma następujące zauważalne cechy: jest autonomiczny, bezserwerowy, nie wymaga konfiguracji, transakcyjny. Jest to baza danych (SQLite 3.32.1) służąca do przechowywania informacji o pacjencie (w trybie autonomicznym), zasobów naszego katalogu produktów oraz metadanych dotyczących dopasowania, akcesoriów i HI.	Zespół programistów SQLite	1.0.113
Sterownik klucza sprzętowego WAP BT	Sterownik klucza sprzętowego WAP BT (dopasowanie klucza sprzętowego)	Rozwiązania iAnywhere	3.0.0.6095
Superpower	Biblioteka kombinatoryczna parsera dla C#	Datalust,Superpower Contributors,Sprache Contributors	2.3
Symulator ubytku słuchu ciAD	Biblioteka symulatorów ubytku słuchu dla odtwarzacza multimedialnego	ciAD (Jurg Haubold)	1.0.0.1
System.Buffers	Umożliwia łączenie zasobów dowolnego typu w aplikacjach, w których wydajność jest krytyczna, a obiekty są często przydzielane i zwalniane.	23rogramma,dotnetframework	4.5.1

SOUP ITEM	OPIS FUNKCJONALNOŚCI	PRODUCENT	WERSJA
System.Collections.Immutable	Używane przez biblioteki pochodzące z Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5,0
System.ComponentModel. Annotations	Zawiera atrybuty służące do definiowania metadanych dla obiektów wykorzystywanych jako źródła danych.	23rogramma,dotnetframe work	4.7
System.Configuration.Configuration Manager	Dostarcza typy obsługujące pliki konfiguracyjne.	Microsoft	5,0
System.Data.SQLite.Core	Używane przez biblioteki pochodzące z Sonova.HardwareAbstraction. Palio.Trafo	Zespół programistów SQLite	1.0.113.7
System.Drawing.Common	Zapewnia dostęp do funkcjonalności graficznej GDI+.	Microsoft	5.0.1
System.IdentityModel.Tokens.Jwt	Zawiera typy zapewniające obsługę tworzenia, serializacji i walidacji tokenów internetowych JSON. Używane przez komponenty komunikujące się z usługami zaplecza, które wykorzystują tokeny JSON Web Token do uwierzytelniania.	Microsoft	6.8.0
System.IO.Abstractions	Zbiór abstrakcji umożliwiający testowanie interakcji systemu plików.	Tatham Oddie i przyjaciele	12.0.10
System.Memory	Zawiera typy umożliwiające efektywną reprezentację i łączenie zarządzanych, stosowych i natywnych segmentów pamięci oraz sekwencji takich segmentów, a także prymitywy do analizy i formatowania zakodowanego tekstu UTF-8 przechowywanego w tych segmentach pamięci.	24rogramma,dotn etfra me work	4.5.4
System.Numerics.Vectors	Zapewnia przyspieszane sprzętowo typy numeryczne, odpowiednie do zastosowań wymagających wysokiej wydajności przetwarzania i grafiki.	24rogramma,dotn etfra me work	4,5
System.Reactive. Interfejsy	Reaktywne rozszerzenia (Rx) dla .NET	.NET Foundation	3.1.1
System.Reactive.Core	Reaktywne rozszerzenia (Rx) dla .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Reaktywne rozszerzenia (Rx) dla .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Reaktywne rozszerzenia (Rx) dla .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Reaktywne rozszerzenia (Rx) dla .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Udostępnia klasę umożliwiającą dynamiczne tworzenie typów proxy implementujących określony interfejs i dziedziczących po określonym typie DispatchProxy. Wywołania metod na wygenerowanej instancji proxy są wysyłane do typu bazowego DispatchProxy.	Microsoft	4.7.1

SOUP ITEM	OPIS FUNKCJONALNOŚCI	PRODUCENT	WERSJA
System.Reflection.Metadane	Ten pakiet zapewnia niskopoziomowy czytnik i zapis metadanych .NET (ECMA-335). Jest nastawiony na wydajność i stanowi idealny wybór do tworzenia bibliotek wyższego poziomu, które mają udostępniać własny model obiektowy, np. kompilatory.	Microsoft	5,0
System.Security.AccessControl	Udostępnia klasy bazowe umożliwiające zarządzanie listami kontroli dostępu i audytu w obiektach podlegających zabezpieczeniu.	Microsoft	5,0
System.Security.Permissions	Dostarcza typy obsługujące zabezpieczenia dostępu do kodu (CAS).	Microsoft	5,0
System.Security.Principal.Windows	Udostępnia klasy umożliwiające pobranie bieżącego użytkownika systemu Windows i interakcję z użytkownikami i grupami systemu Windows.	Microsoft	5,0
System.Text.Encoding.CodePages	Zapewnia obsługę kodowania opartego na stronie kodowej, w tym Windows-1252, Shift-JIS i GB2312.	Microsoft	5,0
System.Text.Encodings.Web	Dostarcza typy do kodowania i eskapowania ciągów znaków do użytku w JavaScript, HyperText Markup Language (HTML) i jednorodnych lokalizatorach zasobów (URL). Jest zależnością SOUP IdentityModel	24rogramma,dotn etfra me work	5,0
System.Text.Json	Zapewnia wydajne i wymagające niewielkiej alokacji typy, które serializują obiekty do tekstu JavaScript Object Notation (JSON) i deserializują tekst JSON do obiektów, ze wbudowaną obsługą UTF-8. Dostarcza również typy do odczytu i zapisu tekstu JSON zakodowanego jako UTF-8 oraz do tworzenia modelu obiektów dokumentu (DOM) w pamięci, który jest tylko do odczytu, w celu losowego dostępu do elementów JSON w ramach ustrukturyzowanego widoku danych.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Udostępnia dodatkowe typy, które upraszczają pisanie kodu współbieżnego i asynchronicznego.	25rogramma,dotnetfra mework	4.5.4
System.ValueTuple	Dostarcza struktury System.ValueTuple, które implementują podstawowe typy krotek w C# i Visual Basic. Dodaje obsługę krotek wartości, ponieważ są one uwzględniane dopiero w późniejszych wersjach .NET Framework.	25rogramma,dotnetfra mework	4.5.0
Środowisko .NET Framework	Czas działania środowiska .NET Framework	Microsoft	4.8.3928.0
Unity	Unity Container (Unity) to w pełni funkcjonalny, rozszerzalny kontener do wstrzykiwania zależności.	Unity Container Project	5.8.13
WebSync	Służy do integracji dopasowanego kanału danych	FM (Frozen Mountain)	4.9.32.0

14. PIŚMIENNICTWO

Tytuł	Strona internetowa
Instrukcja obsługi (elektronika)	https://ifu.advancedbionics.com/
Globalna polityka prywatności firmy Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
System Noaha 4	https://www.himsa.com/products/all-about-noah-system-4/
Tworzenie kopii zapasowej i przywracanie danych w bazie danych Noah	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Osiągnięto maksymalną pojemność bazy danych systemu Noah.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer – lista używanych portów	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Dokumentacja zabezpieczeń serwera LiveSwitch	https://developer.liveswitch.io/liveswitch-server/server/security.html
Najlepsze praktyki dotyczące bezpiecznego dopasowania aparatów słuchowych – dokument informacyjny EHIMA	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA Cyberbezpieczeństwo-FSW-Security-Whitepaper v1-Sep2021 .pdf

CE 0123

Advanced Bionics LLC
28515 Westinghouse Place
Valencia, CA 91355, United States
T: +1.661.362.1400

info.us@advancedbionics.com

EU REP Advanced Bionics GmbH
Feodor-Lynen-Strasse 35
D-30625 Hannover

info.switzerland@advancedbionics.com

Informacje o oddziałach firmy AB w innych krajach są dostępne na stronie *advancedbionics.com/contact*

AB – A Sonova brand

W sprawie dopuszczania do sprzedaży i dostępności w danym regionie należy skontaktować się z lokalnym przedstawicielem firmy AB.

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S396-16 Rev A 2025-09-15