# Target CI Version 1.5

## LEITFADEN ZUR CYBERSICHERHEIT

*Deutsch*

Aktualisiert: September 2025


A Sonova Brand

# Inhalt

# 1. EINFÜHRUNG

Das vorliegende Dokument enthält technische Sicherheits- und Datenschutzinformationen zum Softwaresystem Target CI v1.5 von Advanced Bionics, im Folgenden „Anpasssoftware“ genannt. Die Anpasssoftware ist für die Verwendung durch qualifizierte Audiologen und Hörakustiker zum Konfigurieren (d. h. Anpassen) von Hörsystemen für Patienten konzipiert, die Cochlea-Implantate von Advanced Bionics tragen.

Das vorliegende Dokument widmet sich schwerpunktmäßig Aspekten der Cybersicherheit und des Datenschutzes, soweit sie für die Verwendung der Anpasssoftware relevant sind. Dies umfasst eine Bewertung der Sicherheits- und Datenschutzkontrollen, die derzeit in die Software integriert sind, sowie solcher, die voraussichtlich in der IT-Umgebung eingesetzt und konfiguriert werden, in der das Produkt für den vorgesehenen Zweck genutzt wird.

Das vorliegende Dokument enthält keine technischen Sicherheits- und Datenschutzinformationen zu Folgendem:

- Frühere Versionen der AB Anpasssoftware
- Andere AB Software als Target CI v1.5
- AB Websites
- AB App-Anwendungen
- AB Hörsysteme

## 1.1 ABKÜRZUNGEN UND BEGRIFFSBESTIMMUNGEN:

| Akronym | Begriff |
|---|---|
| FSW | Anpasssoftware |
| HCP | Audiologe oder Hörakustiker |
| SaMD | Software as a Medical Device (Software als Medizinprodukt) |
| AB | Advanced Bionics |
| IFU | Gebrauchsanweisung |

# 2. WEITERE RESSOURCEN

## 2.1 KUNDENSERVICE

Für Kunden in den USA und Kanada bietet Advanced Bionics eine gebührenfreie Technik-Hotline an (877-271-6727). Unter dieser Hotline sind von Montag bis Freitag von 5:00 bis 17:00 Uhr (Pacific Time) kompetente und professionelle Servicemitarbeiter erreichbar.

Außerhalb der USA und Kanada erhalten Sie technische Unterstützung in Ihrer jeweiligen Region. Sollten Sie Fragen zur Anpasssoftware oder zur Hardware oder andere Anliegen in Zusammenhang mit der Programmierung haben, kontaktieren Sie bitte Ihre AB Vertretung vor Ort.

## 2.2 AB PRO PORTAL

Die Anpasssoftware und die dazugehörige Dokumentation können heruntergeladen werden unter https://www.abproportal.com oder aus dem Sonova Web Client. Hierfür ist ein Konto-Login erforderlich. Diese Ressource ist möglicherweise nicht in allen Märkten verfügbar. Wenden Sie sich für weitere Informationen an Ihren AB Vertreter.

## 2.3 ERWEITERTE INSTALLATIONSANLEITUNG

Die erweiterte Installationsanleitung für Target CI v1.5 ist auf Anfrage erhältlich. Die Anleitung enthält technische Informationen zum Installationsprogramm für die Anpasssoftware, einschließlich Befehlszeilenoptionen für unbeaufsichtigte und automatisierte Installationen.

## 2.4 MDS2

MDS2 (Manufacturer Disclosure Statement for Medical Device Security) ist ein branchenübliches Standardformblatt, das Antworten zu Sicherheits- und Datenschutzfragen bezüglich der Anpasssoftware von AB enthält. Das Formblatt ist auf Anfrage erhältlich.

## 2.5 GEBRAUCHSANWEISUNG

Die Gebrauchsanweisung wird mit dem Softwareinstallationsmedium ausgeliefert. Für einige Märkte steht die elektronische Gebrauchsanweisung unter www.advancedbionics.com/ifu zum Download bereit.

Die folgenden Abschnitte der Gebrauchsanweisung können für IT-Fachleute relevant sein:

- Produktbeschreibung
- Mindestanforderungen an das System und Leistungsmerkmale
- Richtlinien für IT-Sicherheit
- Installationsanweisungen
- Technischer Dienst

## 2.6 HIMSA

HIMSA ist ein Drittanbieter von Software, der Noah System 4 herstellt. Dies ist eine für die Hörsystembranche entwickelte Software, die Audiologen und Hörakustikern ein herstellerunabhängiges System zur Durchführung kundenbezogener Aufgaben bereitstellt.

Die Anpasssoftware kann optional so konfiguriert werden, dass sie zur Datenspeicherung statt einer lokalen Datenbank Noah System 4 verwendet.

Auf der Sicherheitswebseite von HIMSA finden Sie Antworten auf häufige Fragen zur IT-Sicherheit von Noah System 4.

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

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

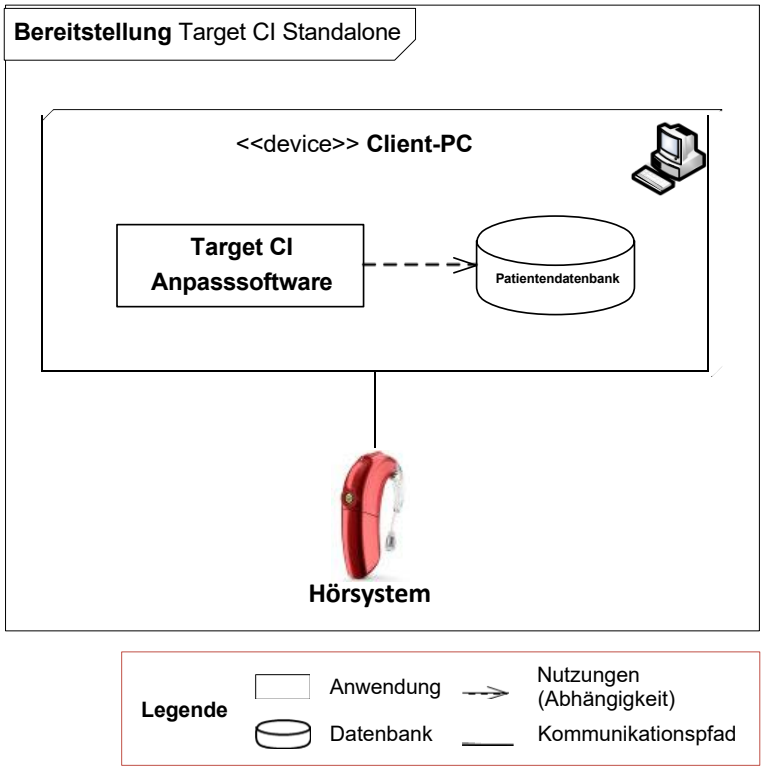
Weitere Sicherheitsinformationen finden Sie im Abschnitt „Sicherheit“ des HIMSA Trainingscenter:
https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

# 3. NETZWERK- UND KONTEXTDIAGRAMME

Für die Anpasssoftware, bei der es sich um eine Client-Anwendung (SaMD) handelt, die auf einem handelsüblichen Microsoft Windows-PC installiert wird, werden zwei Bereitstellungsmodelle unterstützt. Die Software beinhaltet weder die Hardware noch das Betriebssystem.

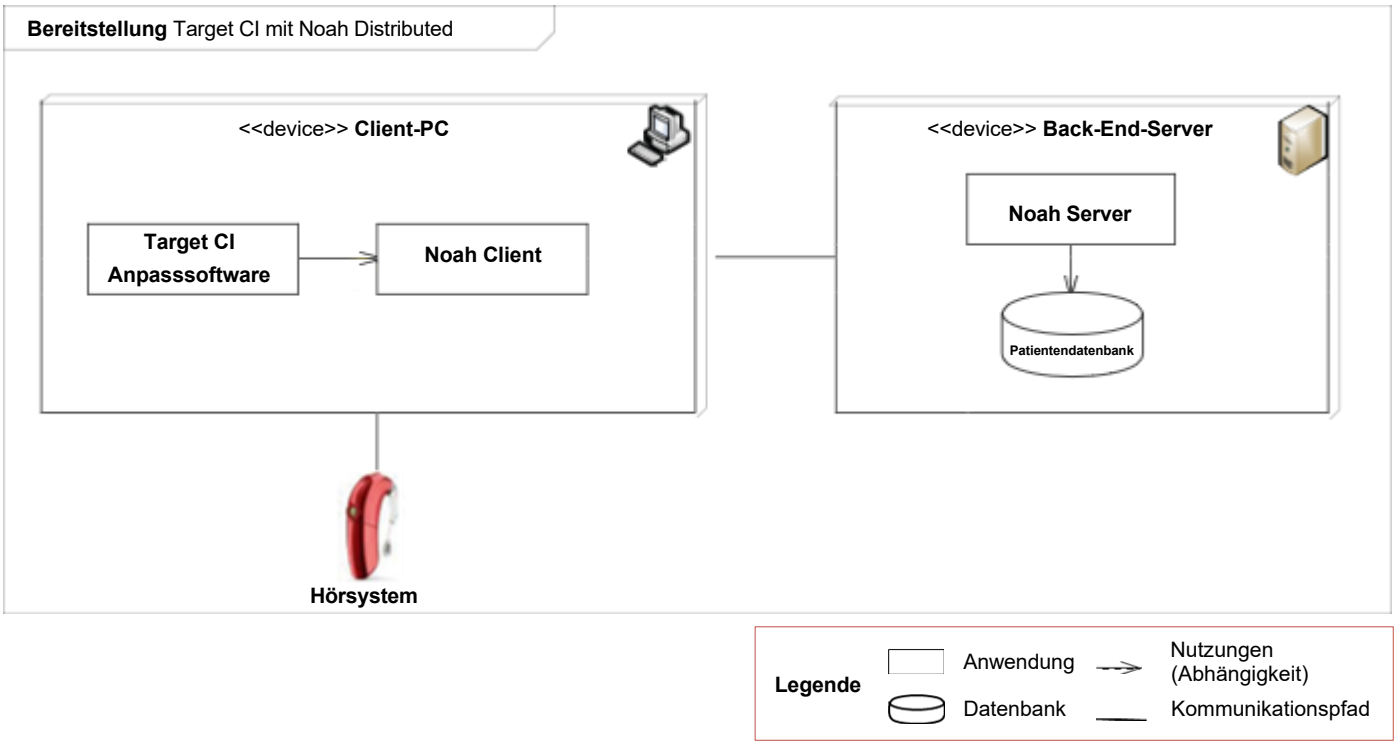
## 3.1 BEREITSTELLUNGSMODELL 1: STANDALONE

Beim Standalone-Bereitstellungsmodell wird die Anpasssoftware auf einem Client-PC bereitgestellt. Die Patientendatenbank wird auf demselben PC gespeichert und zusammen mit der Anpasssoftware installiert.




## 3.2 BEREITSTELLUNGSMODELL 2: NOAH DISTRIBUTED

Im Bereitstellungsmodell Noah Distributed wird die Anpasssoftware auf einem oder mehreren Client-PCs bereitgestellt. Noah ist der Name des Patientenverwaltungssystems eines Drittanbieters. Dieses wird auf einem internen Server bereitgestellt, auf den die Client-PCs zugreifen können. Die Patientendatenbank wird auf dem Noah Server gespeichert und über das Netzwerk von einem oder mehreren Client-PCs abgerufen.

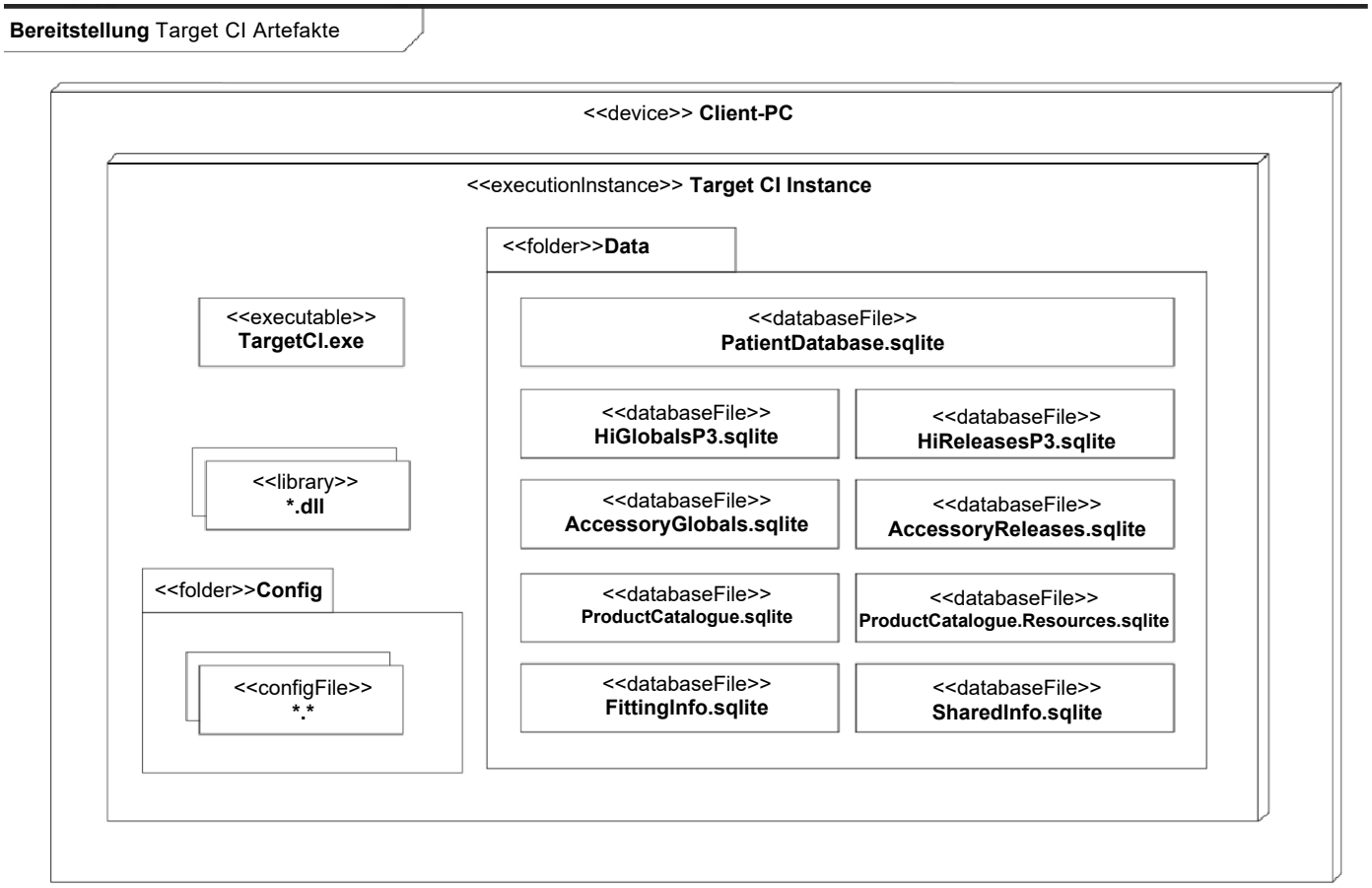


## 3.3 BEREITSTELLUNGSARTEFAKTE

Die Anpasssoftware wird mit einer ausführbaren Datei und einer Reihe zugehöriger Dateien installiert, darunter DLL-Komponenten, Konfigurationsdateien und SQLite-Datenbankdateien. Die Konfigurationsdateien werden im Ordner „%ProgramData%\Advanced Bionics\Target CI\Target CI\Config“ installiert, die Datenbankdateien im Ordner „%ProgramData%\Advanced Bionics\Target CI\Target CI\Data“. Der Ordner „Data“ enthält eine einzelne Transaktionsdatenbankdatei und mehrere Infodatenbankdateien.

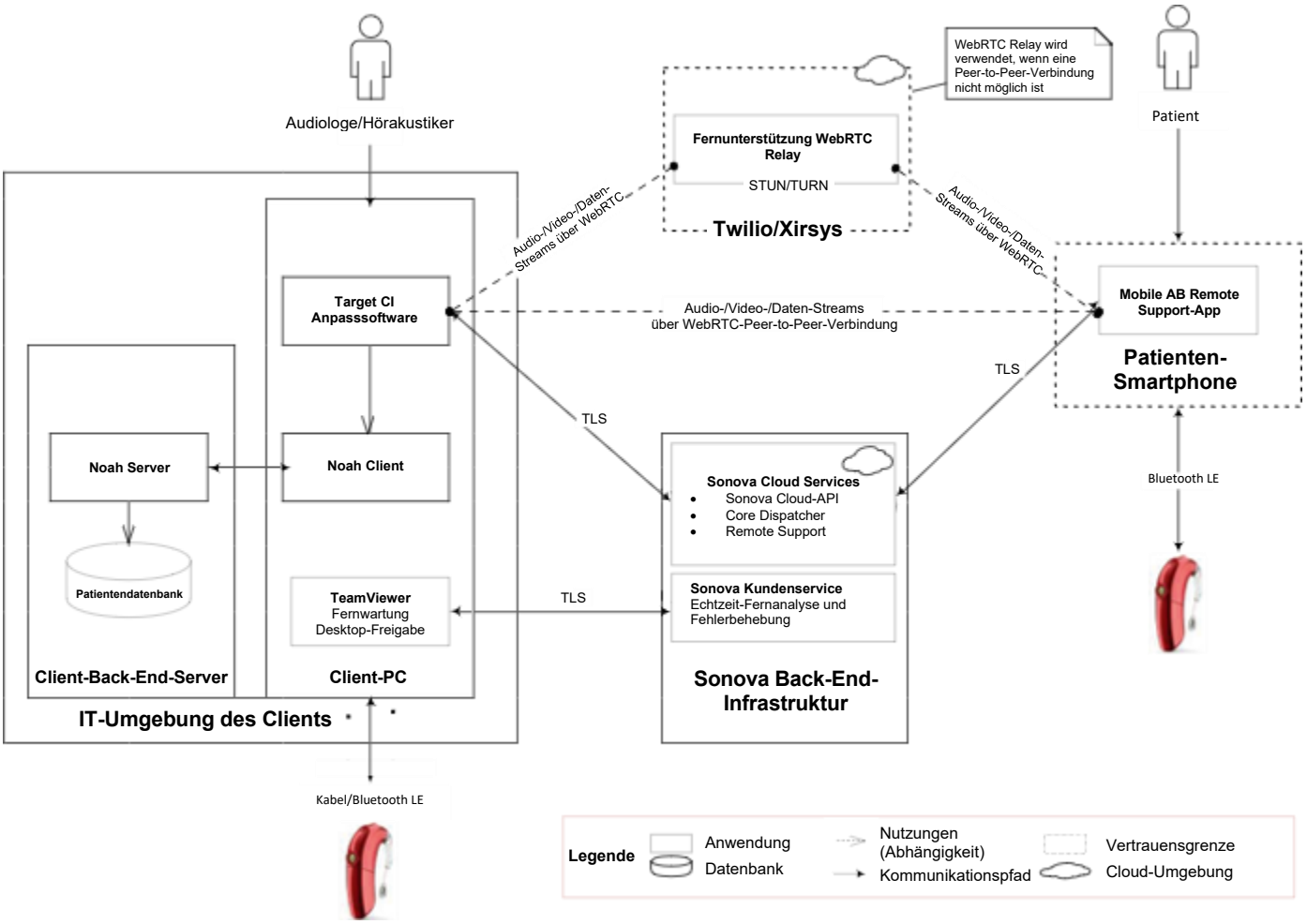
Die Transaktionsdatenbank „PatientDatabase.sqlite“ speichert demografische Daten und Anpassdaten des Patienten und wird nur installiert, wenn die Anpasssoftware im Standalone-Modus bereitgestellt wird.

Wenn die Anpasssoftware als Noah Modul bereitgestellt wird, stellt das Noah System der Anpasssoftware die erforderlichen Dienste zur dauerhaften Speicherung der Patientendaten bereit. Die verbleibenden SQLite-Dateien sind wesentlicher Bestandteil der Anpasssoftware und bei allen Bereitstellungsmodellen erforderlich.



## 3.4 SYSTEMVERBINDUNGEN

Das Diagramm und die Tabelle unten veranschaulichen die primären Systemverbindungen. Normalerweise wird nur ein Teil der angegebenen Verbindungen genutzt.




| Quelle/Ziel | Service | Protokoll | Port | Beschreibung |
|---|---|---|---|---|
| Hörsysteme | Hörsystemkom-munikation | Kabelverbindung/ Bluetooth® Low Energy | k. A. | Dient zur Kommunikation mit Hörsystemen zur Steuerung und Konfiguration sowie zum Auslesen von Status und Daten |
| Noah | Noah 4 ModuleAPI | .NET Remoting | k. A. | Primäre Schnittstelle für das Modul, das für den Zugriff auf die Noah Software verwendet wird (nur beim Bereitstellungsmodell Noah Distributed) |
| Sonova Cloud Services | Sonova Cloud-API, Core Dispatcher, Remote Support | SOAP, REST | 443 | Sonova-Dienste, die in einem Microsoft Azure Data Center gehostet werden, werden zu folgenden Zwecken verwendet: |

| Quelle/Ziel | Service | Protokoll | Port | Beschreibung |
|---|---|---|---|---|
| | | | | • Abrufen der Client-Konfigurationsdaten der Anpasssoftware aus dem Sonova Back-End-Speicher<br>• Übertragungsprotokollierung und Analysedaten<br>• Einrichten von Echtzeit-Fernanpasssitzungen |
| Twilio/Xirsys, Mobile AB Remote Support-App | Remote Support | WebRTC | Liste der Ports auf Anfrage erhältlich | Die Cloud-Kommunikationsdienste von Twilio werden auf Cloud-Plattformen von Drittanbietern und konkret bei Amazon Web Services (AWS) und Google Cloud Platform (GCP) gehostet. Diese Dienste werden ausschließlich von der Remote Support-Funktion der Anpasssoftware genutzt, die WebRTC-Signalisierung und Echtzeit-Fernanpasssitzungen ermöglicht. |
| AB Kundenservice | Desktop-Freigabe | Proprietäres TeamViewer-Protokoll | 5938, 443, 80<br><br>Siehe TeamViewer-Ports | Wird verwendet, um Echtzeit-Fernanalysen und Fehlerbehebungen durchzuführen, welche die Installation der Anpasssoftware beeinträchtigen. Weitere Informationen finden Sie in Abschnitt 6.6 FERNWARTUNG. |

## 4. SYSTEMANFORDERUNGEN

| | |
|---|---|
| Betriebssystem | Windows 10 Pro/Enterprise (64-Bit) |
| .NET Framework | Version 4.8 |
| CPU | Intel® Core™ i5 oder gleichwertig mit gleicher oder besserer Leistung |
| RAM | 4 GB min. |
| Freier Festplattenspeicher | 3 GB min. |
| Displaymindestanforderungen | • Auflösung 1280 × 1024 Bildpunkte (maximale Skalierung 125 %)<br>• 24-Bit-Farben |
| Gerätetreiber | • NoahLink Wireless-Treiber (bei Verwendung einer über USB verbundenen NoahLink Wireless-Programmierschnittstelle eines Drittanbieters ist die neueste Version erforderlich, die bei HIMSA bezogen werden kann)<br>• CPI-3-Treiber (erforderlich bei Verwendung einer über USB verbundenen CPI-3-Programmierschnittstelle) |
| Datenbank | SQLite oder Noah System 4 (Version 4.14 oder höher) |
| Internetverbindung | Für Fernunterstützung und Analyseprotokollierung ist eine Internetverbindung erforderlich (vgl. Abschnitt 4.4 „Systemverbindungen“); bei Verwendung eines vernetzten Noah System 4 wird ein Intranet benötigt. |
| Netzwerkports | Informationen hierzu finden Sie in Abschnitt 3.4 „Systemverbindungen“ sowie in Abschnitt 3 „Weitere Ressourcen – HIMSA“ zu den von Noah System 4 verwendeten Ports. |

## 5. INSTALLATION

### 5.1 ANFORDERUNGEN

Für die Installation der Anpasssoftware ist ein Administratorkonto erforderlich. Nach Abschluss der Installation kann die Software ohne Administratorrechte oder erhöhte Berechtigungen ausgeführt werden.

Informationen zur Validierung der Software-Integrität vor der Installation finden Sie in Abschnitt 8 „Software-Integrität“.

Vor der Installation wird Systemadministratoren empfohlen, Folgendes sicherzustellen:

• Die zu installierende Version der Anpasssoftware ist die aktuellste verfügbare Version.

• Das zugrunde liegende Betriebssystem ist auf dem neuesten Stand.

### 5.2 INSTALLATIONSPROGRAMME

Zum Installieren der Anpasssoftware sind zwei Installationsprogramme verfügbar:

• Standardinstallationsprogramm

• IT Professional-Installationsprogramm

Das IT Professional-Installationsprogramm ist eine einzelne MSI-Datei und schließt erforderliche Komponenten aus, ist ansonsten jedoch mit dem Standardinstallationsprogramm identisch.

Zu den erforderlichen Komponenten gehören Microsoft .NET Framework v4.8 und die Microsoft Visual C++ Redistributable-Pakete.

Beide Installationsprogramme unterstützen erweiterte Installationsszenarien, einschließlich der unbeaufsichtigten Installation.

Das IT Professional-Installationsprogramm sollte nur verwendet werden, falls in Ihrem Unternehmen die Installation und Verwaltung der erforderlichen Komponenten durch das Unternehmen selbst vorgeschrieben ist und daher nicht durch das Installationsprogramm der Anpasssoftware durchgeführt werden kann. In allen anderen Fällen sollte das Standardinstallationsprogramm verwendet werden.

Das IT Professional-Installationsprogramm kann über einen AB-Vertreter bezogen werden. Das IT Professional-Installationsprogramm kann nicht zum Reparieren, Neuinstallieren oder Deinstallieren von Installationen mit dem Standardinstallationsprogramm verwendet werden. Ebenso kann das Standardinstallationsprogramm nicht zum Reparieren, Neuinstallieren oder Deinstallieren von Installationen mit dem IT Professional-Installationsprogramm verwendet werden.

## 6. SICHERHEITSKONTROLLEN

Bei der Anpasssoftware handelt es sich um eine Client-Anwendung, die auf einem handelsüblichen Microsoft Windows-PC installiert wird. Die Anpasssoftware kann als eigenständige Anwendung („Standalone“) oder als Noah Modul installiert werden.

### 6.1 AUTHENTIFIZIERUNG BEI STANDALONE-BEREITSTELLUNG

Wenn die Anpasssoftware als Standalone-Anwendung installiert wird, nutzt sie die Zugriffskontrollmechanismen des Host-Betriebssystems. Die Authentifizierungsverwaltung kann vom IT-Personal des Kunden im Host-Betriebssystem konfiguriert werden. Die Anpasssoftware selbst verfügt über keine solche integrierte Funktion. Advanced Bionics empfiehlt, dass sich jeder Benutzer mit einem eigenen Benutzerkonto beim Host-Betriebssystem anmeldet.

### 6.2 AUTHENTIFIZIERUNG BEI NOAH BEREITSTELLUNG

Wenn die Anpasssoftware als Noah Modul installiert ist, erfolgt die Zugriffskontrolle durch Noah System 4. Informationen zu den von Noah System 4 verwendeten Auditkontrollen finden Sie unter www.HIMSA.com.

### 6.3 AUTORISIERUNG

Die Anpasssoftware schränkt den Zugriff auf ihre Funktionen nicht auf Grundlage der Rollen einzelner Benutzer ein. Die Software unterstützt eine einzige Hauptfunktion, nämlich die Anpassung von Hörsystemen an Patienten, und eine einzige Rolle als Anpassfachkraft. Rollenbasierte Zugriffskontrollen sind nicht anwendbar.

### 6.4 AUDIT BEI STANDALONE-BEREITSTELLUNG

Wenn die Anpasssoftware als Standalone-Anwendung installiert wird, nutzt sie die Auditmechanismen des Host-Betriebssystems. Die Anpasssoftware selbst verfügt über keine solche integrierte Funktion. Das Host-Betriebssystem kann vom IT-Personal des Kunden so konfiguriert werden, dass es Starts der Anpasssoftware und Benutzeranmeldungen protokolliert. Zum Zweck der Durchführung von Audits empfiehlt Advanced Bionics, dass sich jeder Benutzer mit einem eigenen Benutzerkonto beim Host-Betriebssystem anmeldet.

### 6.5 AUDIT BEI NOAH BEREITSTELLUNG

Wenn die Anpasssoftware als Noah Modul installiert wird, werden durch das Noah System Auditprotokolle implementiert. Informationen zu den von Noah System 4 verwendeten Auditkontrollen finden Sie unter https://www.himsa.com/.

## 6.6 FERNZUGRIFF

Die Funktion zur Desktop-Freigabe ermöglicht eine Echtzeit-Fernanalyse sowie die Fehlerbehebung bei Problemen mit der Anpasssoftware-Installation. Diese Funktion beruht auf dem Drittanbietertool TeamViewer QuickSupport (das standardmäßig zusammen mit der Anpasssoftware bereitgestellt wird) und ermöglicht es Kundendienstmitarbeitern von AB, eine Fernverbindung mit dem Computer des Audiologen oder Hörakustikers herzustellen und dessen Desktop uneingeschränkt (auch mit Zugriff auf das zugrunde liegende Betriebs- und Dateisystem) zu steuern.

Zum Einrichten einer Desktop-Freigabesitzung ist die Interaktion des Audiologen bzw. Hörakustikers erforderlich. Der Adiologen bzw. Hörakustiker muss zunächst das QuickSupport-Tool von TeamViewer ausführen (z. B. durch Aufruf über die Target CI-Anpasssoftware) und seine TeamViewer-ID-Zugangsdaten über einen separaten Kommunikationskanal (z. B. telefonisch) an das AB Supportteam übermitteln.

Der Name des AB Supportmitarbeiters sowie seine TeamViewer-ID werden bei jeder aktiven Desktop-Freigabesitzung standardmäßig auf dem Computermonitor des Audiologen bzw. Hörakustikers angezeigt.

Der gesamte bei einer Desktop-Freigabesitzung ausgetauschte Netzwerkverkehr ist abgesichert und erfüllt oder übertrifft die geltenden Standards für Verschlüsselungsprotokolle und -algorithmen (Austausch öffentlicher und privater Schlüssel nach RSA-Verfahren, AES-256-Bit-Sitzungsverschlüsselung).

TeamViewer QuickSupport kann manuell entfernt werden, ohne dass sonstige Funktionen der Target Anpasssoftware beeinträchtigt werden. Das Installationsprogramm für die Target Anpasssoftware unterstützt einen Installationsparameter für die Kommandozeile. Auf diese Weise soll eine Installation der Target Anpasssoftware über die Kommandozeile ohne Einbeziehung des QuickSupport-Tools von TeamViewer ermöglicht werden.

# 7. DATENSCHUTZ

## 7.1 ADVANCED BIONICS DATENSCHUTZRICHTLINIE

Die Datenschutzrichtlinie, die beschreibt, wie Advanced Bionics personenbezogene Daten erhebt, überträgt, speichert und nutzt, kann hier heruntergeladen werden: AdvancedBionics.com/privacy.

Weder hostet, speichert oder sichert Advanced Bionics Daten, die in der Anpasssoftware oder den Noah Datenbanken gespeichert sind, noch hat Advanced Bionics Zugriff auf diese Daten, sofern diese nicht ausdrücklich an Advanced Bionics gesendet werden.

## 7.2 US-BUNDESSTANDARDS FÜR DIE INFORMATIONSVERARBEITUNG (FIPS)

Target CI v1.5 entspricht den Verschlüsselungsstandards nach FIPS 140-2.

## 7.3 SICHERHEIT BEI DER ÜBERTRAGUNG

Kommunikationssicherheit ist bei allen eingehenden und ausgehenden Netzwerkkommunikationen der Anpasssoftware gewährleistet und aktiviert. Mit Ausnahme der Remote Support-Funktion (die das WebRTC-Protokoll verwendet) und der Bluetooth-Kommunikation mit Hörsystemen und Zubehör sind alle Verbindungen durch das TLS-Protokoll (Transport Layer Security) geschützt, das Vertraulichkeit, Integrität und Authentizität gewährleistet.

### TLS

Die TLS-Konfiguration entspricht geltenden Best Practices und Sicherheitsempfehlungen, die in BCP 195 („Recommendations for Secure Use of TLS and DTLS“) dokumentiert sind, darunter:

- Keine Unterstützung für SSL- und TLS-Versionen vor 1.2

- Keine Unterstützung für Cipher Suites, die kryptografische Algorithmen verwenden, die weniger als 128-Bit-Sicherheit bieten
- Unterstützung in BCP 195 empfohlener TLS-Erweiterungen
- Keine Unterstützung von in BCP 195 als unsicher eingestuften Erweiterungen

#### DTLS

Verschlüsselung ist eine obligatorische Funktion von WebRTC und wird für alle über WebRTC gesendeten Medien-Streams erzwungen. Das verwendete Verschlüsselungsprotokoll hängt vom Kanaltyp ab. Daten-Streams werden mit DTLS verschlüsselt, Medien-Streams hingegen mit dem Secure Real-time Transport Protocol (SRTP), da es eine im Vergleich zu DTLS schlankere Option ist.

Ausführlichere Informationen zur Sicherheitskonfiguration von Remote Support WebRTC finden Sie unter folgendem Link:

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

#### BLE

Die drahtlose Bluetooth Low Energy-Kommunikation mit Hörsystemen und Zubehör ist standardmäßig verschlüsselt und ihre Integrität geschützt (außer bei Anwendungsfällen zur Identifizierung und Erkennung). Darüber hinaus ist die Dauer des Bluetooth-Kopplungsmodus beim Hörsystem zeitlich begrenzt. Eine ausführlichere Beschreibung der Sicherheit des Bluetooth-Kommunikationskanals finden Sie in der Dokumentation zum Hörsystem.

### 7.4 SICHERHEIT IM RUHEZUSTAND

#### Patientendatenbank bei Standalone-Bereitstellung

Wenn die Anpasssoftware als Standalone-Anwendung installiert ist, wird die Patientendatenbank lokal unter „C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data“ gespeichert.

Diese ruhenden Datenbestände werden standardmäßig nicht verschlüsselt. Geschützte Gesundheitsinformationen und personenbezogene Daten werden in einer internen Datenbank der Anpasssoftware gespeichert und nicht über das Netzwerk übertragen.

In manchen Rechtsordnungen kann die Verschlüsselung aller Patientendaten vorgeschrieben sein, um eine mögliche Haftung im Falle von Datenverlust oder -diebstahl zu vermeiden. Aktivieren Sie BitLocker oder eine gleichwertige vollständige Festplattenverschlüsselung (auf Betriebssystemebene oder hardwarebasiert), um ruhende Daten vor unbefugtem Zugriff oder Kopieren zu schützen.

BitLocker ist eine in Windows integrierte Funktion, die das gesamte Laufwerk verschlüsselt und für den Zugriff eine Authentifizierung verlangt. Ziehen Sie vor der Aktivierung von BitLocker immer die offiziellen Empfehlungen von Microsoft und die IT-Sicherheitsrichtlinien Ihres Unternehmens zurate.

**So aktivieren Sie BitLocker**

Zum Verwalten von BitLocker sind Administratorrechte erforderlich.

1. Nach „BitLocker verwalten“ suchen

Öffnen Sie das Startmenü, geben Sie „BitLocker verwalten“ ein und wählen Sie den entsprechenden Eintrag in den Suchergebnissen aus.

2. Systemlaufwerk auswählen

Wählen Sie das Laufwerk aus, auf dem Windows installiert ist, um die Verschlüsselungseinstellungen zu konfigurieren.

3. Entsperrmethode wählen

Wählen Sie eine der folgenden Optionen:

- Nur TPM

- TPM + PIN

- TPM + USB-Schlüssel

Befolgen Sie beim Auswählen der Entsperrmethode die von Microsoft empfohlenen Best Practices sowie die IT-Sicherheitsrichtlinien Ihres Unternehmens.

4. Wiederherstellungsschlüssel sichern

Erstellen Sie eine Sicherungskopie des Wiederherstellungsschlüssels mithilfe sicherer, unternehmensweit zugelassener Methoden. Zu den empfohlenen Optionen gehören:

- Speichern in Microsoft Entra ID (vormals Azure AD) oder Active Directory für Geräte, die einer Domäne beigetreten sind

- Speichern an einem sicheren, zugriffskontrollierten Netzwerkspeicherort mit Verschlüsselung und Prüfprotokollierung

- Nutzen einer von Ihrer Organisation genehmigten verwalteten Lösung zum Hinterlegen von Schlüsseln

Speichern Sie den Schlüssel nicht auf lokalen Laufwerken oder USB-Sticks und drucken Sie ihn nicht aus, sofern dies nicht ausdrücklich durch eine Richtlinie erlaubt ist. Wiederherstellungsschlüssel müssen mit der gleichen Sorgfalt wie andere vertrauliche Zugangsdaten geschützt und bei Offenlegung sofort ausgetauscht werden.

5. Verschlüsselung starten

Ihnen stehen folgende Optionen zur Verfügung:

- „Gesamtes Laufwerk“: empfohlen für die meisten Unternehmensszenarien. Verschlüsselt alle Sektoren, einschließlich ungenutztem Speicherplatz, um Datenremanenz zu verhindern.

## Patientendatenbank – Noah Distributed-Bereitstellungsmodul

Wenn die Anpasssoftware als Noah Modul installiert wird, werden personenbezogene Daten in der von Noah gehosteten Patientendatenbank gespeichert. Die von Noah gehostete Patientendatenbank kann sich auf einem anderen Computer befinden. Personenbezogene Daten und andere Patientendaten werden von der Noah Software verwaltet, und die Verschlüsselung der ruhenden Patientendaten wird durch das Noah System sichergestellt. Die Anpasssoftware kann personenbezogene Daten über eine kabelgebundene oder kabellose Netzwerkverbindung senden/empfangen, wenn der Netzwerkzugriff für eine Noah Datenbank konfiguriert ist.

In der vernetzten Noah Datenbank gespeicherte personenbezogene Daten sind für andere Gerätebenutzer auf anderen PCs sichtbar, die über Berechtigungen für diese vernetzte Datenbank verfügen. Die Noah Datenbank kann auch ohne Netzwerkzugriff konfiguriert und dann auf demselben PC wie die Anpasssoftware installiert werden.

Noah verhindert, dass die Anpasssoftware auf die Datenbank mit den Patientendaten zugreift. Wenn ein Benutzer im Noah Client einen Patienten in der Anpasssoftware öffnet, kann die Anpasssoftware nur den aktuell geöffneten Patientendatensatz lesen und bearbeiten, hat jedoch keinen Zugriff auf andere Patientendatensätze in der Noah Datenbank.

Informationen zu den von Noah System 4 verwendeten Verschlüsselungsstandards finden Sie im entsprechenden Abschnitt auf www.HIMSA.com.

#### RMA-Exportdateien

Die Anpasssoftware ermöglicht den Export von Kundendaten in eine Datei. Die RMA-Datei kann an Advanced Bionics gesendet werden, um RMA- oder damit verbundene Supportprobleme zu lösen.

Die RMA-Datei ist asymmetrisch RSA-verschlüsselt und verwendet eine Schlüssellänge von 512 Bit. Die Anpasssoftware verfügt nicht über die Möglichkeit, eine RMA-Datei zu entschlüsseln.

#### Anonymisierte Exportdateien

Die Anpasssoftware ermöglicht den Export von Kundendaten in eine anonymisierte Kundendatei. Die personenbezogenen Daten des Kunden, wie etwa Geburtsdatum und Name, werden durch generische Werte ersetzt. Die Datei ist nicht verschlüsselt und kann in dieselbe oder eine andere Instanz der Anpasssoftware importiert werden.

#### Standardexportdateien

Die Anpasssoftware ermöglicht den Export von Kundendaten in eine Standardexportdatei. Diese Datei verwendet ein proprietäres Binärformat und ist nicht verschlüsselt. Die Datei kann in dieselbe oder eine andere Instanz der Anpasssoftware importiert werden. Bei Verwendung dieser Funktion müssen Benutzer der Anpasssoftware sicherstellen, dass Standardexportdateien gemäß den jeweils geltenden lokalen IT-Richtlinien für die Verwaltung unverschlüsselter personenbezogener Daten verarbeitet werden.

#### Hörsystem

Die Anpasssoftware speichert Kundeninformationen auf dem Hörsystem des Kunden. Personenbezogene Daten wie Name und Geburtsdatum des Kunden werden auf dem Hörsystem nicht gespeichert. Andere nicht personenbezogene Daten werden mithilfe der PBKDF2-Verschlüsselung unter Verwendung eines 128-Bit-Schlüssels gespeichert.

Die Anpasssoftware kann nicht personenbezogene Kundendaten über ein proprietäres kabelgebundenes Gerät (z. B. CPI-3), die mobile AB Remote Support-Anwendung oder ein NoahLink Wireless Gerät an ein Hörsystem übertragen bzw. von diesem empfangen. Das NoahLink Wireless Gerät verbindet sich per Bluetooth Low Energy (BLE) über einen mit 128 Bit AES-verschlüsselten BLE-Standardkanal mit dem Hörsystem.

## 8. SOFTWARE-INTEGRITÄT

### 8.1 ÜBERPRÜFEN DER HERUNTERGELADENEN INSTALLATIONSMEDIEN

Das Installationsmedium für die Target CI-Anpasssoftware kann in einigen Regionen vom Pro Portal oder Sonova Web Client von Advanced Bionics heruntergeladen werden. Das heruntergeladene Installationsmedium kann mit jedem vertrauenswürdigen SHA-256-Hashing-Tool authentifiziert werden.

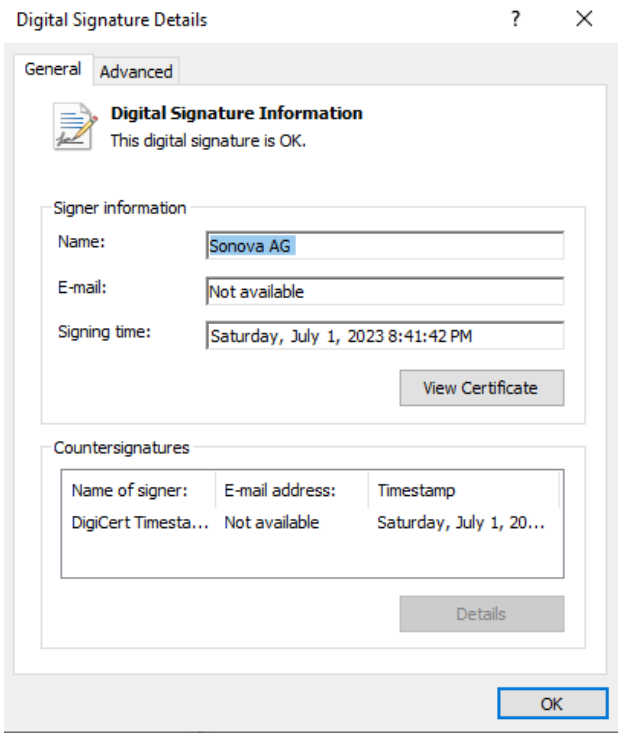
Der SHA256-Hash für die ZIP-Datei des Standardinstallationsprogramms lautet:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

Der SHA256-Hash für die ZIP-Datei des IT Professional-Installationsprogramms lautet:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

## 8.2 MANUELLES ÜBERPRÜFEN DER ANPASSSOFTWARE VOR DER INSTALLATION

Benutzer können die folgenden Schritte ausführen, um die Integrität und Echtheit der Anpasssoftware vor der Installation zu überprüfen:

1. Öffnen Sie den Windows Explorer und navigieren Sie zum Stammordner des Installationsmediums der Anpasssoftware. Wenn es sich bei Ihrem Installationsmedium um einen USB-Stick handelt, stecken Sie ihn in einen USB-Anschluss und navigieren Sie zu seinem Stammverzeichnis. Wenn Ihr Installationsmedium eine ZIP-Datei ist, entpacken Sie diese in einen Ordner und navigieren Sie dann dorthin.
2. Klicken Sie mit der rechten Maustaste auf „SonovaVerify.exe“ und wählen Sie „Eigenschaften“ im Kontextmenü aus.
3. Wählen Sie die Registerkarte „Digitale Signaturen“ aus.
4. Doppelklicken Sie auf die SHA256-Signatur „Sonova AG“.
5. Überprüfen Sie, ob die Elemente der Signatur gültig sind. Überprüfen Sie insbesondere, ob oben die Meldung „The digital signature is OK.“ (Die digitale Signatur ist gültig) angezeigt wird und Name des Signaturgebers und Uhrzeit der Signatur mit dem folgenden Bild übereinstimmen:




1. Schließen Sie die Popup-Dialoge und doppelklicken Sie auf „SonovaVerify.exe“.
2. Überprüfen Sie, ob, wie im folgenden Bild dargestellt, „NO ERRORS DETECTED“ (KEINE FEHLER ERKANNT) angezeigt wird:

Das Bild zeigt, dass SonovaVerify die digitalen Signaturen aller Dateien auf dem Installationsmedium, einschließlich des Installationsprogramms, authentifiziert und verifiziert hat. Dadurch ist sichergestellt, dass das Installationsmedium nicht manipuliert, beschädigt oder anderweitig beeinträchtigt wurde. SonovaVerify zeigt Warnungen oder Fehlermeldungen an, wenn Dateien oder Ordner fehlen oder dem Installationsmedium unerwartete Dateien oder Ordner hinzugefügt wurden.

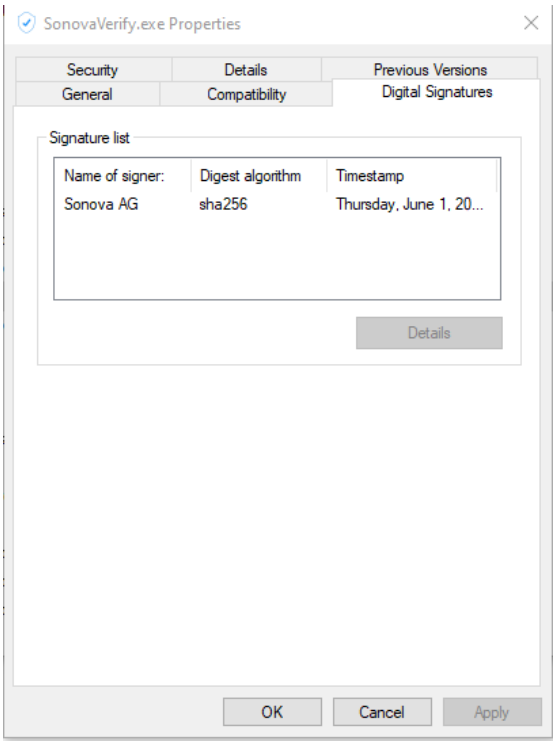
## 8.3 AUTOMATISCHES ÜBERPRÜFEN DER INTEGRITÄT DER INSTALLIERTEN ANPASSSOFTWARE

SonovaVerify ist in die Anpasssoftware integriert und wird bei jedem Start der Anwendung ausgeführt, um die Integrität der Programmdateien der Anpasssoftware zu überprüfen. Programmdateien werden mithilfe branchenüblicher Verfahren und Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden, digital signiert. Die Software informiert den Benutzer in Form von Warnmeldungen, wenn Programmdateien beschädigt sind.

## 8.4 MANUELLES ÜBERPRÜFEN DER INTEGRITÄT DER INSTALLIERTEN ANPASSSOFTWARE

Benutzer können die folgenden Schritte ausführen, um jederzeit die Integrität und Echtheit der installierten Anpasssoftware zu überprüfen, ohne die Anpasssoftware starten zu müssen:

1. Öffnen Sie den Windows Explorer und navigieren Sie zum Ordner mit der ausführbaren Datei der Anpasssoftware, der sich normalerweise hier befindet: C:\Programmdateien (x86)\Advanced Bionics\Target CI\
2. Klicken Sie mit der rechten Maustaste auf „SonovaVerify.exe“ und wählen Sie „Eigenschaften“ im Kontextmenü aus.
3. Wählen Sie die Registerkarte „Digitale Signaturen“ aus.
4. Doppelklicken Sie auf die SHA256-Signatur „Sonova AG“.
5. Überprüfen Sie, ob die Elemente der Signatur gültig sind, und insbesondere, ob oben die Meldung „The digital signature is OK.“ (Die digitale Signatur ist gültig) angezeigt wird und Name des Signaturgebers und Uhrzeit der Signatur mit dem folgenden Bild übereinstimmen:



1. Schließen Sie die Popup-Dialoge und doppelklicken Sie auf „SonovaVerify.exe“.
2. Überprüfen Sie, ob, wie im folgenden Bild dargestellt, „NO ERRORS DETECTED“ (KEINE FEHLER ERKANNT) angezeigt wird:


Das Bild zeigt, dass SonovaVerify die digitalen Signaturen aller installierten Programmdateien authentifiziert und verifiziert hat. Dadurch ist sichergestellt, dass die Anpasssoftware nicht manipuliert, beschädigt oder anderweitig beeinträchtigt wurde. SonovaVerify zeigt Warnungen oder Fehlermeldungen an, wenn Dateien oder Ordner fehlen oder dem Ordner mit den Programmdateien unerwartete Dateien oder Ordner hinzugefügt wurden.

## 9. SOFTWARE-PATCHES UND UPDATES

Automatische Updates werden nicht unterstützt.

## 10. DATENVERWALTUNG

### 10.1 DATENBANKEN

Die Anpasssoftware verwendet eine transaktionale Datenbank zum Speichern von Patientendaten sowie eine Reihe von Infodatenbanken, welche die von der Anwendung benötigten Metadatenkonfigurationen bereitstellen.

Eine detaillierte Liste aller von der Anpasssoftware implementierten Datenbanken finden Sie in Abschnitt 3 „Netzwerk- und Kontextdiagramme“ unter „Bereitstellungsartefakte“.

Wenn die Anpasssoftware als Standalone-Anwendung installiert wird, befindet sich die Patientendatenbank intern in der Anpasssoftware. Die in der Datei „PatientDatabase.sqlite“ gespeicherte Patientendatenbank befindet sich auf demselben Computer wie die Anpasssoftware und ermöglicht das Speichern von Patientendaten. Zum Sichern der Anwendungsdaten können Sie, wenn Target CI als Standalone-Anwendung bereitgestellt ist, eine Sicherungskopie des gesamten Ordners „%ProgramData%\Advanced Bionics\Target CI\Target CI\Data“ erstellen. Schützen Sie Datensicherungen nicht nur vor Datenverlust, sondern auch vor Diebstahl. Wenn die Anpasssoftware als Noah Modul installiert ist, werden die Patientendaten in der vom Noah System bereitgestellten Datenbank gespeichert. Für die Noah Datenbank kann der Netzwerkzugriff konfiguriert werden. Die Noah Datenbank kann auch ohne Netzwerkzugriff konfiguriert und dann auf demselben PC wie die Anpasssoftware installiert werden. Konfigurieren Sie die Noah Datenbankverschlüsselung, um die Daten zu schützen (siehe Dokumentation von HIMSA).

Informationen zum Noah Distributed-Bereitstellungsmodus finden Sie unter dem folgenden Link, über den Sie Anleitungen zum Sichern und Wiederherstellen der Noah Patientendatenbank aufrufen können:

https://www.himsa.com/de/support-2/noah-4-knowledgebase-german/trainingscenter/backup-und-wiederherstellung-der-daten-in-ihrer-noah-datenbank/

## 10.2 DATENMIGRATION

Die Anpasssoftware ermöglicht es Benutzern, Patientendatensätze der vorherigen AB Anpasssoftware (SoundWave 3.2) zu migrieren. Damit die Patientendaten migriert werden können, muss der Zugriff auf diese Daten von einer SoundWave 3.2-Installation auf demselben Computer wie Target CI möglich sein.

## 10.3 HÖRSYSTEMKONFIGURATIONEN

Die Anpasssoftware ermöglicht das Exportieren und Importieren von Gerätekonfigurationen und -einstellungen.

## 10.4 DATENENTSORGUNG

Anweisungen zur Datenentsorgung finden Sie in der Gebrauchsanweisung oder auf der folgenden Website für Noah Bereitstellungen: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

# 11. SICHERHEITSUMGEBUNG – GEMEINSAME VERANTWORTUNG

Die Anpasssoftware wurde für einen Verwendungszweck entwickelt, bei dem davon ausgegangen wird, dass die Steuerung von Cybersicherheitsrisiken in der gemeinsamen Verantwortung aller Beteiligten im gesamten Ökosystem für Hörsysteme liegt. Hierzu gehören insbesondere Hörsystemträger, Eltern oder Erziehungsberechtigte von Kindern, die Hörsysteme tragen, Audiologen und Hörakustiker, IT-Administratoren, Hörversorgungseinrichtungen und -anbieter sowie Anbieter von Hörsystemen und Programmiergeräten.

Die folgende Liste enthält Empfehlungen zu bewährten Vorgehensweisen und Sicherheitskontrollen für die Anpassungsumgebung, in der die Anpasssoftware verwendet wird:

### Betriebssystemebene

- Wenden Sie Zugriffskontrollen auf Betriebssystemebene an, z. B. durch:
  - Entfernen von Gästekonten
  - Aktivieren der Windows-Benutzeranmeldung
  - Führen einer Liste autorisierter Bediener, um den Zugriff auf das System zu kontrollieren
  - Festlegen angepasster Benutzer und Rollen
  - Festlegen von Anforderungen für sichere Passwörter und Geheimhalten von Zugangsdaten
- Wenden Sie Auditkontrollen auf Betriebssystemebene an.
- Halten Sie das Betriebssystem aktuell.
- Halten Sie die installierte Anpasssoftwareversion aktuell.
- Aktivieren Sie aktuelle Versionen von Malware- und Virenschutz.
- Aktivieren Sie Positivlisten für Anwendungen.

### Datenschutz

- Verschlüsseln Sie Patientendaten mithilfe von Drittanbieter-Tools oder -kontrollen auf Betriebssystemebene, z. B. durch Verwendung einer Laufwerkverschlüsselung (wie das kostenlose Microsoft BitLocker), um alle Daten zu schützen. Bei Noah Bereitstellungen sollten Sie die Nutzung der Noah Datenbankverschlüsselung in Betracht ziehen.
- Sorgen Sie für den Schutz externer Medien mit aus der Anpasssoftware exportierten Daten, insbesondere Berichten und Protokollen. Wenn die Daten nicht mehr benötigt werden, sollten sie und/oder die betreffenden Medien sicher gelöscht werden.
- Verwenden Sie USB-Speichermedien mit integrierter Sicherheitsfunktion, beispielsweise verschlüsselte USB-Laufwerke mit integriertem Tastenfeld.
- Sorgen Sie dafür, dass Ihre Daten stets sicher sind:
  - Senden Sie beim Übertragen von Daten über unsichere Kanäle entweder anonyme Daten oder verschlüsseln Sie sie.
  - Schützen Sie Datensicherungen nicht nur vor Datenverlust, sondern auch vor Diebstahl.
  - Entfernen Sie alle Daten von Medien, die nicht mehr verwendet werden oder zur Entsorgung bestimmt sind.

- Benutzer sollten gemäß geltenden Vorschriften und Richtlinien für den Umgang mit Patienteninformationen/personenbezogenen Daten/geschützten Gesundheitsinformationen zugelassene Verfahren und Tools zum sicheren Entfernen von auf Wechselmedien gespeicherten Daten nutzen.

### IT-Infrastruktur

Betreiben Sie die Anpasssoftware in einer sicheren Netzwerkumgebung, die vor unbefugtem Zugriff geschützt ist. Es gibt viele wirksame Techniken zum Isolieren und Schützen medizinischer Informationssysteme, insbesondere die Implementierung von Firewall-Schutz, demilitarisierten Zonen (DMZ), virtuellen lokalen Netzen (VLAN) und Netzwerkenklaven. Halten Sie eine aktive Netzwerkverbindung aufrecht, um Betriebssystemupdates zu beziehen.

### Physische Ebene

- Der Arbeitsplatz, auf der die Anpasssoftware installiert ist, muss physisch so abgesichert sein, dass er für unbefugte Benutzer nicht zugänglich ist.
- Schützen Sie das System vor Manipulation durch unbefugte Mitarbeitende.
- Der Zugriff auf an den Arbeitsplatz angeschlossene Drucker sollte kontrolliert werden.
- Der Monitor des Arbeitsplatzes, auf dem die Anpasssoftware installiert ist, sollte so aufgestellt werden, dass nur der Benutzer den Bildschirminhalt einsehen kann.

### Organisationsebene

- Nur professionell geschultes und qualifiziertes Personal ist zur Bedienung des Systems befugt. Bevor einer Person die Befugnis zur Bedienung des Systems gegeben wird, ist sicherzustellen, dass sie die mit der Anpasssoftware gelieferte Bedienungsanleitung gelesen und vollständig verstanden hat.
- Wenn Sie verdächtige Aktivitäten auf Ihren Anpasssoftware-Konten oder unerwartete Vorgänge bemerken, wenden Sie sich an Advanced Bionics. Weitere Informationen finden Sie in Abschnitt 2.1.

Weitere Informationen zur gemeinsamen Verantwortung und eine ausführlichere Liste von bewährten Verfahren und Sicherheitskontrollen für die Anpassumgebung, in der die Anpasssoftware auf verschiedenen Ebenen eingesetzt wird, finden Sie im:

- EHIMA-Whitepaper „Best Practices for Secure Fitting of Hearing Devices“ (Best Practices für die sichere Hörsystemanpassung) hier

## 12. HERSTELLUNG UND SOFTWARE-ENTWICKLUNG

Die Cybersicherheit spielt während der gesamten Software-Entwicklung eine zentrale Rolle. Die Anpasssoftware wird in Übereinstimmung mit den Normen IEC 62304 und IEC 82304 entwickelt.

Die Anpasssoftware wird im Rahmen des Herstellungsprozesses auf Viren und Malware geprüft.

Sicherheitslücken in Komponenten von Drittanbietern, die in der National Vulnerability Database (NVD) des National Institute of Standards and Technology (NIST) aufgeführt sind, werden während des Entwicklungsprozesses bewertet und behoben. Nach dem Inverkehrbringen der Software wird diese weiterhin auf Auftreten der dort aufgeführten Sicherheitslücken überwacht.

## 13. SOFTWAREKOMPONENTEN UND STÜCKLISTE

Die Anpasssoftware umfasst bestimmte COTS-Softwarekomponenten (Commercial Off-the-Shelf, d. h. gewerbliche Standardsoftware).

In der folgenden Tabelle sind alle SOUP (Software of Unknown Provenance, also Software unsicherer Herkunft) aufgeführt, die mit der Anpasssoftware vertrieben werden.

| SOUP | FUNKTIONSBESCHREIBUNG | HERSTELLER | VERSION |
|---|---|---|---|
| ciAD Hearingloss Simulator | Hörverlustsimulatorbibliothek für Mediaplayer | ciAD (Jörg Haubold) | 1.0.0.1 |
| CredentialManagement | Das Credential Management-Paket ist ein Wrapper für die Credential Management-API von Windows. | iLya Lozovyy | 1.0.2 |
| CSharpAnalytics | Wird für Google Analytics verwendet | Attack Pattern | 1.6.1 |
| Dapper | ORM | Sam Saffron, Marc Gravell, Nick Craver | 2.0.78 |
| Destructurama.Attributed | Wird von Nephele-Bibliotheken verwendet | Serilog-Mitwirkende | 3.0 |
| DirectShow 2005 | Ermöglicht von .NET-Anwendungen aus den Zugriff auf die Microsoft DirectShow-Funktionalität | 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 | GNOtmetrics.Aurical, neu gepackt für Sonova | GNOtometrics | 2.0.1.9 |
| IceLink | Wird für die Integration von WebRTC-Audio-/Videokonferenzen verwendet | FM (Frozen Mountain) | 3.8.0.22151 |
| IdentityModel | OpenID Connect & OAuth 2.0-Client-Bibliothek, die von der Komponente Kona.CommonServices.Authentication für die OAuth 2-Authentifizierung verwendet wird | Dominick Baier, Brock Allen | 5.0.1 |
| IMCInterfaces | Schnittstellenbibliothek für die Kommunikation zwischen Noah Modulen | HIMSA II K/S | 4.4.0.2266 |
| LibGit2Sharp | Wird von Bibliotheken von Sonova zur Kommunikation mit Git verwendet | LibGit2Sharp-Mitwirkende | 0.26.1 |
| Mapster | Wird für das Objekt-Mapping in Code verwendet | chaowlert, eric_swann | 7.2.0.0 |
| MathNet.Numerics | Wird für Anpassalgorithmen (Signalpfad, Zielabgleich usw.) genutzt | Christoph Rüegg, Marcus Cuda, Jurgen van Gael und Mitwirkende | 4.11.0 |
| Microsoft.Bcl.AsyncInterfaces | Stellt die Schnittstellen IAsyncEnumerable<T> und IAsyncDisposable sowie Hilfstypen für .NET Standard 2.0 bereit | Microsoft | 5.0.0 |
| Microsoft.CodeAnalysis.Common | Wird von den Bibliotheken in Sonova.HardwareAbstraction verwendet Palio.Trafo | Microsoft | 3.9 |
| Microsoft.CodeAnalysis.CSharp | Wird von den Bibliotheken in Sonova.HardwareAbstraction verwendet Palio.Trafo | Microsoft | 3.9 |

| SOUP | FUNKTIONSBESCHREIBUNG | HERSTELLER | VERSION |
|---|---|---|---|
| Microsoft.Identity.Client | Die MSAL-Bibliothek für .NET ist Teil der Microsoft Identity Platform für Entwickler v2.0 (vormals Azure AD). Sie ermöglicht das Abrufen von Sicherheits-Token für den Aufruf geschützter APIs. Sie verwendet den Branchenstandard OAuth2 und OpenID Connect. | Microsoft | 4.38.0.0 |
| Microsoft.Identity.Client.Extensions.Msal | Sicherer plattformübergreifender Token-Cache für öffentliche MSAL-Client-Apps | Microsoft | 2.19.3.0 |
| Microsoft.IdentityModel.JsonWebTokens | Umfasst Typen, die Unterstützung für das Erstellen, Serialisieren und Validieren von JSON Web Token bieten<br><br>Wird von Komponenten verwendet, die mit Back-End-Diensten kommunizieren, die JSON Web Token zur Authentifizierung verwenden | Microsoft | 6.8.0 |
| Microsoft.IdentityModel.Logging | Abhängigkeit von Microsoft.IdentityModel.Tokens | Microsoft | 6.8.0 |
| Microsoft.IdentityModel.Tokens | Abhängigkeit von SOUP Microsoft.IdentityModel.JsonWebTokens | Microsoft | 6.8.0 |
| Microsoft.Win32.TaskScheduler.dll | Wird für das Backup-Tool der Anpasssoftware (d. h. für automatisierte Backups) verwendet | David Hall | 2.5.11.0 |
| Microsoft.Xaml.Behaviors.Wpf | XAML Behaviors ist eine benutzerfreundliche Möglichkeit, WPF-Anwendungen mit minimalem Programmieraufwand allgemeine und wiederverwendbare Interaktivität hinzuzufügen. | xamlexperiencesteam, Microsoft | 1.0.1 |
| MS VC++ 2008 Redistributable | Microsoft Visual C++ 2008 Redistributable | Microsoft | 9.0.30729.6161 |
| Microsoft Visual C++ 2010 x86 Redistributable | Microsoft Visual C++ 2010 Redistributable | Microsoft | 10.0.40219.325 |
| Microsoft Visual C++ 2012 Redistributable | Microsoft Visual C++ 2012 Redistributable | Microsoft | 11.0.61030.0 |
| Microsoft Visual C++ 2017 Redistributable (x86) | Microsoft Visual C++ 2017 Redistributable | Microsoft | 14.16.27024.1 |
| MS-VisualC++ 7.1 Laufzeitbibliotheken | Laufzeitbibliotheken für Microsoft Visual C++ | 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 | Wird zum Anpassen von Lautstärken und zum Wiedergeben von Audiodateien verwendet | Open Source | 1.9 |
| .NET Framework | .NET-Laufzeit-Framework | Microsoft | 4.8.3928.0 |

| SOUP | FUNKTIONSBESCHREIBUNG | HERSTELLER | VERSION |
|---|---|---|---|
| Newtonsoft.Json | Wird für die JSON-Serialisierung und -Deserialisierung verwendet | James Newton-King | 12.0.3 |
| Nibelung | NoahLink Wireless-Anpassbibliotheken | GN ReSound | 1.3.16.1 |
| Nlog | Abhängigkeit der HIMSA Nibelung.CPD (NoahLink Wireless) | Kim Christensen | 4.4.0 |
| NoahLink | NoahLink Anpassgerätetreiber | HIMSA | 1.55.6.166 |
| NoahLink Wireless | NoahLink Wireless-Anpassgerätetreiber | HIMSA | 2.0.0.68 |
| Otometrics.HiPro2 | HiPro-Kommunikationsbibliotheken | GNOtometrics | 2.0.0.4 |
| Otometrics.REMaccess | Otometrics-Abstraktionsschicht oberhalb der Schnittstellenbibliothek für die Kommunikation zwischen Noah Modulen | GN Otometrics | 1.0.0.10 |
| Pdfium.Net.SDK | C#-PDF-Bibliothek zum Erstellen und Bearbeiten von PDF-Dokumenten in .NET-Anwendungen. | Patagames.com | 4.54.2704.0 |
| Polly | Bibliothek, mit der Entwickler Resilienz- und Fehlerbehandlungsrichtlinien für verschiedene Aspekte wie Wiederholungen (Retry), Überlastungsschutz durch Trennschalter (Circuit Breaker), Schottisolierung (Bulkhead Isolation) und Rückfall (Fallback) auf flüssige und Thread-sichere Weise ausdrücken können | App vNext | 7.2.1 |
| Polly.Extensions.Http | Bibliothek mit vordefinierten Komfortmethoden zum Konfigurieren von Polly-Richtlinien zur Behandlung transienter Fehler, wie sie für Aufrufe über HttpClient typisch sind | App vNext | 3.0 |
| Polly.Contrib.WaitAndRetry | Bibliothek für Polly, die Hilfsmethoden für verschiedene Wait-and-Retry-Strategien enthält | Grant Dickinson, App vNext | 1.1.1 |
| Portable.BouncyCastle | Abhängigkeit der HIMSA Nibelung.CPD (NoahLink Wireless) | BouncyCastle.Crypto | 1.8.10.0 |
| protobuf-net.dll | Für RC-Blob verwendetes Serialisierungs-Framework. | Open Source | 2.0.0.668 |
| Serilog | Protokollierungskomponente, die für die gesamte Chinook-Anwendung verwendet wird | Serilog-Mitwirkende | 2.10.0 |
| Serilog.Enrichers.Thread | Erweitert Serilog-Ereignisse um Eigenschaften aus dem aktuellen Thread | Serilog-Mitwirkende | 3.1 |
| Serilog.Expressions | Ausdrucksbasierte Ereignisfilterung für Serilog | Serilog-Mitwirkende | 2.0 |
| Serilog.Sinks.Console | Serilog-Senke, die Protokollereignisse in die Konsole/das Terminal schreibt | Serilog-Mitwirkende | 4.0.0.0 |

| SOUP | FUNKTIONSBESCHREIBUNG | HERSTELLER | VERSION |
|---|---|---|---|
| Serilog.Sinks.Debug | Serilog-Senke, die Protokollereignisse in das Debug-Ausgabefenster schreibt | Serilog-Mitwirkende | 2.0 |
| Serilog.Sinks.File | Schreibt Serilog-Ereignisse in Textdateien im Plain-Text- oder JSON-Format | Serilog-Mitwirkende | 4.1 |
| Serilog.Sinks.Trace | Serilog-Senke für Diagnose-Traces | Serilog-Mitwirkende | 2.1 |
| Serilog.Settings.AppSettings | XML-Konfiguration (System.Configuration.< appSettings>)-Unterstützung für Serilog | Serilog-Mitwirkende | 2.2.2 |
| Security.Cryptography | Erweiterungen der mit .NET Framework ausgelieferten Sicherheits-APIs | Microsoft | 1.7.2 |
| SharpBITS API | SharpBITS.NET ist ein .NET-Wrapper der BITS-API sowie eine schlanke Windows-UI-Anwendung für einfacheren Zugriff auf BITS-Uploads und -Downloads. | perpetualKid | 2.1.0.0 |
| SharpZipLib | #ziplib (SharpZipLib, vormals NzipLib) ist eine Zip-, Gzip-, Tar- und Bzip2-Bibliothek, die vollständig in C# für die .NET-Plattform geschrieben ist. Diese Bibliothek bietet Komprimierungsfunktionen (Zip, Unzip, Stream-Komprimierung usw.). Wir nutzen sie innerhalb der Firmware-Update-App. | Open Source | 1.1.0.145 |
| Superpower | Parser-Kombinator-Bibliothek für C# | Datalust, Superpower-Mitwirkende, Sprache-Mitwirkende | 2.3 |
| SQLite.Interop | SQLite ist eine Softwarebibliothek, die ein relationales Datenbankverwaltungssystem bereitstellt. Das „Lite“ in SQLite bezieht sich darauf, dass es sich in Bezug auf Einrichtung, Datenbankverwaltung und erforderliche Ressourcen um eine ausgesprochen schlanke Komponente handelt. SQLite hat die folgenden markanten Eigenschaften: Es ist in sich geschlossen, serverlos, konfigurationsfrei und transaktionsfähig. Es handelt sich um eine Datenbank (SQLite 3.32.1) zum Speichern von Patientendaten (im Standalone-Modus), unseren Produktkatalogressourcen und den Metadaten für Anpassung, Zubehör und Hörsysteme. | SQLite-Entwicklungsteam | 1.0.113 |
| System.Buffers | Stellt Ressourcen-Pooling aller Art für leistungskritische Anwendungen bereit, die häufig Objekte zuweisen und freigeben | 23rogramma,dotnetframework | 4.5.1 |
| System.Collections.Immutable | Wird von den Bibliotheken in Sonova.HardwareAbstraction verwendet Palio.Trafo | Microsoft | 5.0 |
| System.ComponentModel.Annotations | Implementiert Attribute, die zum Definieren von Metadaten für Objekte verwendet werden, die als Datenquellen dienen | 23rogramma,dotnetframework | 4.7 |

| SOUP | FUNKTIONSBESCHREIBUNG | HERSTELLER | VERSION |
|---|---|---|---|
| System.Configuration.Configuration Manager | Implementiert Typen, welche die Verwendung von Konfigurationsdateien unterstützen. | Microsoft | 5.0 |
| System.Data.SQLite.Core | Wird von den Bibliotheken in Sonova.HardwareAbstraction verwendet Palio.Trafo | SQLite-Entwicklungsteam | 1.0.113.7 |
| System.Drawing.Common | Bietet Zugriff auf die GDI+-Grafikfunktionalität. | Microsoft | 5.0.1 |
| System.IdentityModel.Tokens.Jwt | Umfasst Typen, die Unterstützung für das Erstellen, Serialisieren und Validieren von JSON Web Token bieten<br>Wird von Komponenten verwendet, die mit Back-End-Diensten kommunizieren, die JSON Web Token zur Authentifizierung verwenden | Microsoft | 6.8.0 |
| System.IO.Abstractions | Satz von Abstraktionen, die dabei helfen, Dateisysteminteraktionen testbar zu machen | Tatham Oddie & Friends | 12.0.10 |
| System.Numerics.Vectors | Implementiert hardwarebeschleunigte numerische Typen, die für Hochleistungsverarbeitungs- und Grafikanwendungen geeignet sind | 24rogramma,dotnetframework | 4.5 |
| System.Memory | Implementiert Typen für die effiziente Darstellung und Zusammenführung verwalteter, gestapelter und nativer Speichersegmente und Abfolgen solcher Segmente sowie Primitive zum Parsen und Formatieren UTF-8-codierten Texts, der in diesen Speichersegmenten gespeichert ist | 24rogramma,dotnetframework | 4.5.4 |
| System.Reactive.Core | Reactive Extensions (Rx) für .NET | .NET Foundation | 3.1.1 |
| System.Reactive. Interfaces | Reactive Extensions (Rx) für .NET | .NET Foundation | 3.1.1 |
| System.Reactive.Linq | Reactive Extensions (Rx) für .NET | .NET Foundation | 3.1.1 |
| System.Reactive.PlatformServices | Reactive Extensions (Rx) für .NET | .NET Foundation | 3.1.1 |
| System.Reactive.Windows.Threading | Reactive Extensions (Rx) für .NET | .NET Foundation | 3.1.1 |
| System.Reflection.DispatchProxy | Stellt eine Klasse zum dynamischen Erstellen von Proxytypen bereit, die eine angegebene Schnittstelle implementieren und von einem angegebenen DispatchProxy-Typ abgeleitet sind. Methodenaufrufe der generierten Proxyinstanz leiten an diesen DispatchProxy-Basistyp weiter. | Microsoft | 4.7.1 |

| SOUP | FUNKTIONSBESCHREIBUNG | HERSTELLER | VERSION |
|---|---|---|---|
| System.Reflection.Metadata | Dieses Paket implementiert maschinennahe Lese- und Schreibfunktionen für .NET-Metadaten (ECMA-335). Es ist leistungsoptimiert und die ideale Wahl zum Erstellen komplexerer Bibliotheken, die ein eigenes Objektmodell bereitstellen sollen, wie z. B. Compiler. | Microsoft | 5.0 |
| System.Runtime.CompilerServices.Unsafe | Implementiert die System.Runtime.CompilerServices.Unsafe-Klasse, die generische, maschinennahe Funktionen zur Manipulation von Zeigern bietet | 24rogramma,dotnetframework | 5.0 |
| System.Security.AccessControl | Implementiert Basisklassen, welche die Verwaltung von Zugriffs- und Auditkontrolllisten für sicherungsfähige Objekte ermöglichen | Microsoft | 5.0 |
| System.Security.Permissions | Implementiert Typen, die Code Access Security (CAS) unterstützen | Microsoft | 5.0 |
| System.Security.Principal.Windows | Implementiert Klassen zum Abrufen des aktuellen Windows-Benutzers und zur Interaktion mit Windows-Benutzern und -Gruppen | Microsoft | 5.0 |
| System.Text.Encoding.CodePages | Bietet Unterstützung für Codepage-basierte Verschlüsselungen, einschließlich Windows-1252, Shift-JIS und GB2312 | Microsoft | 5.0 |
| System.Text.Encodings.Web | Implementiert Typen zum Kodieren und Escape-Maskieren von Zeichenfolgen zur Verwendung in JavaScript, HyperText Markup Language (HTML) und Uniform Resource Locators (URLs). Ist eine Abhängigkeit von SOUP IdentityModel. | 24rogramma, dotnetframework | 5.0 |
| System.Text.Json | Implementiert leistungsstarke und ressourcenschonende Typen, die Objekte in JSON-Text (JavaScript Object Notation) serialisieren und JSON-Text in Objekte deserialisieren, einschließlich UTF-8-Unterstützung. Implementiert ferner Typen zum Lesen und Schreiben von UTF-8-codiertem JSON-Text und zum Erstellen eines schreibgeschützten In-Memory-Dokumentobjektmodells (DOM) für den wahlfreien Zugriff auf die JSON-Elemente in einer strukturierten Datenansicht. | Microsoft | 5.0.1 |
| System.Threading.Tasks.Extensions | Implementiert zusätzliche Typen, die das Schreiben von nebenläufigem und asynchronem Code vereinfachen | 25rogramma, dotnetframework | 4.5.4 |
| System.ValueTuple | Stellt die System.ValueTuple-Strukturen bereit, welche die zugrunde liegenden Typen für Tupel in C# und Visual Basic implementieren<br>Ergänzt Unterstützung für Werttupel, da diese erst in späteren Versionen von .NET Framework enthalten sind | 25rogramma, dotnetframework | 4.5.0 |

| SOUP | FUNKTIONSBESCHREIBUNG | HERSTELLER | VERSION |
|---|---|---|---|
| Thrift | Wird für die Remotelink-Protokolldefinition verwendet | Apache | 0.13.0.0 |
| Unity | Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container. | Unity Container Project | 5.8.13 |
| WAP BT Dongle-Treiber | Treiber für WAP BT-Dongle (Anpass-Dongle) | iAnywhere Solutions | 3.0.0.6095 |
| WebSync | Wird zur Integration des Anpassdatenkanals verwendet | FM (Frozen Mountain) | 4.9.32.0 |
| XPS-PDF-Rendering (NiXPS) | Konvertiert programmgesteuert erstellte XPS-Dateien in das PDF-Format; wird für Berichtsfunktionen in der Anpass-App verwendet | NiXPS | 2.6.7.0 |

## 14. REFERENZEN

| Titel | URL |
|---|---|
| Gebrauchsanweisung (in elektronischer Form) | https://ifu.advancedbionics.com/ |
| Advanced Bionics Datenschutzrichtlinie | https://advancedbionics.com/privacy |
| HIMSA | https://www.himsa.com/ |
| Noah System 4 | https://www.himsa.com/de/produkte/noah-system-4/ |
| Backup und Wiederherstellung der Daten in Ihrer Noah Datenbank | https://www.himsa.com/de/support-2/noah-4-knowledgebase-german/trainingscenter/backup-und-wiederherstellung-der-daten-in-ihrer-noah-datenbank/ |
| Kapazität der Noah System Datenbank ist erreicht | https://www.himsa.com/de/support-2/noah-4-knowledgebase-german/trainingscenter/kapazitat-der-noah-system-datenbank-ist-erreicht/ |
| Welche Ports verwendet TeamViewer? | https://www.teamviewer.com/de/global/support/knowledge-base/teamviewer-remote/troubleshooting/ports-used-by-teamviewer/? |
| BCP 195 | https://www.rfc-editor.org/info/bcp195 |
| LiveSwitch Server Security Documentation (Sicherheitsdokumentation zum LiveSwitch-Server) | https://developer.liveswitch.io/liveswitch-server/server/security.html |
| EHIMA-Whitepaper „Best Practices for Secure Fitting of Hearing Devices“ (Best Practices für die sichere Hörsystemanpassung) | https://www.ehima.com/wp-content/uploads/2021/09/EHIMA Cybersecurity-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

Informationen über weitere AB Standorte finden Sie unter: *AdvancedBionics.com/contact*

AB – A Sonova brand

Informieren Sie sich bitte bei Ihrem lokalen Vertreter von AB über die Zulassung und Verfügbarkeit in Ihrer Region.



ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S396-01 Rev A 2025-09-15