Target CI v1.5

CYBERSECURITY GUIDE

English

Updated: September 2025

A Sonova Brand

Contents

1. INTRODUCTION

This document provides technical security and privacy information about the Target CI v1.5 software system from Advanced Bionics, hereinafter “fitting software.” The fitting software is designed for use by qualified hearing care professionals (HCP) to configure (i.e., fit) hearing devices for patients who have received cochlear implants from Advanced Bionics.

This document specifically focuses on the cybersecurity and privacy considerations that are relevant to the use of the fitting software. It includes an evaluation of the security and privacy controls that are currently integrated into the software, as well as those that are anticipated to be applied and configured within the IT environment where the product will be used for its intended purpose.

This document does not provide technical security and privacy information about:

- Previous versions of AB fitting software
- AB software other than Target CI v1.5
- AB websites
- AB mobile applications
- AB hearing devices

1.1 ABBREVIATIONS AND DEFINITIONS:

Acronym	Term
FSW	Fitting software
HCP	Hearing Care Professional
SaMD	Software as a Medical Device
AB	Advanced Bionics
IFU	Instructions For Use

2. OTHER RESOURCES

2.1 CUSTOMER SUPPORT

For those located inside the United States and Canada, Advanced Bionics offers a toll-free technical hotline phone number (877-271-6727) where dedicated professional support is available Monday through Friday from 5:00am to 5:00pm Pacific Time.

For those located outside the US and Canada, technical support is provided regionally. If you have questions about the fitting software, related hardware, or other programming concerns, please contact your local AB representative.

2.2 AB PRO PORTAL

The fitting software and related documentation may be downloaded from https://www.abproportal.com or the Sonova Web Client. An account login is required. This resource may not be available in all markets; contact your AB representative for more information.

2.3 ADVANCED INSTALLATION GUIDE

The Target CI v1.5 Advanced Installation Guide is available upon request. The guide provides technical information about the fitting software installer, including command-line options for silent and automated installations.

2.4 MDS2

The Manufacturer Disclosure Statement for Medical Device Security (MDS2) is an industry-standard form containing security and privacy answers about the AB's fitting software. The form is available upon request.

2.5 INSTRUCTIONS FOR USE (IFU)

The IFU will ship with the software installation media. For some markets, the electronic IFU is available for download at www.advancedbionics.com/ifu

The following sections in the IFU may be relevant to IT professionals:

- Product Description
- System Minimum Requirements & Performance Characteristics
- Guidelines for IT Security
- Installation Instructions
- Technical Support

2.6 HIMSA

HIMSA is a third-party software vendor that produces Noah System 4, a software system designed for the hearing care industry that provides hearing care professionals with a vendor-agnostic system for performing client-related tasks.

The fitting software may optionally be configured to use Noah System 4 for data storage rather than a local database.

HIMSA's security web page provides answers to common IT security questions about the Noah System 4.

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

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

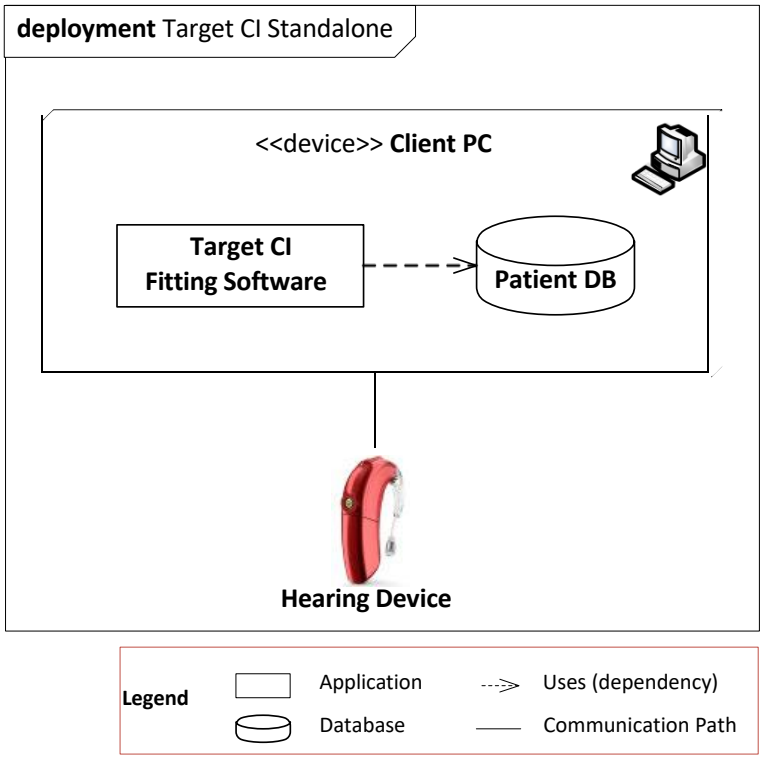
See the Security section of the HIMSA Learning Center for additional security information:
https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

3. NETWORK AND CONTEXT DIAGRAMS

There are two deployment models supported for the fitting software, which is a client application (SaMD) installed on a commercially available off-the-shelf Microsoft Windows PC. The software does not include any hardware or operating system.

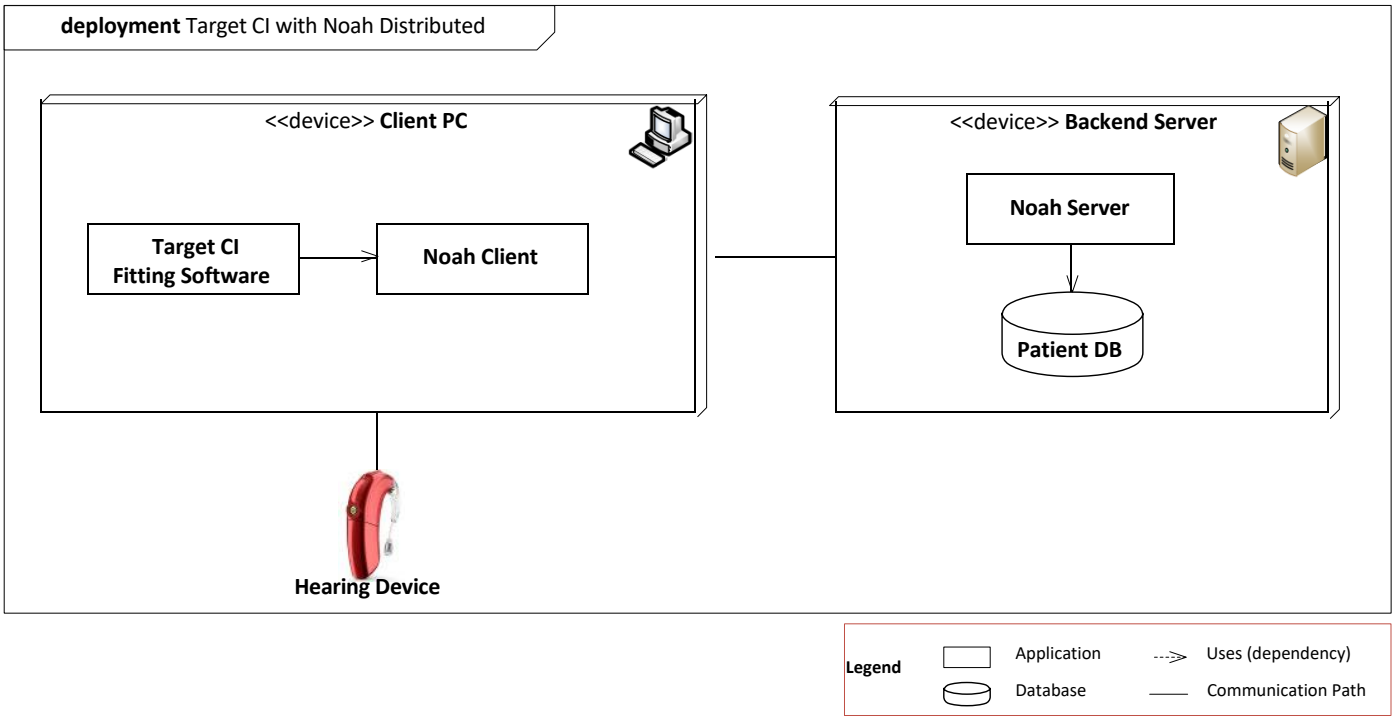
3.1 DEPLOYMENT MODEL 1: STANDALONE

In the standalone deployment model, the fitting software is deployed to a client PC. The patient database is stored on the same PC and installed together with the fitting software.



3.2 DEPLOYMENT MODEL 2: NOAH DISTRIBUTED

In the Noah Distributed deployment model, the fitting software is deployed to one or more client PCs. Noah, a third-party patient management system, is deployed to an internal server accessible to the client PCs. The patient database is stored on the Noah server and accessed over the network by one or more client PCs.

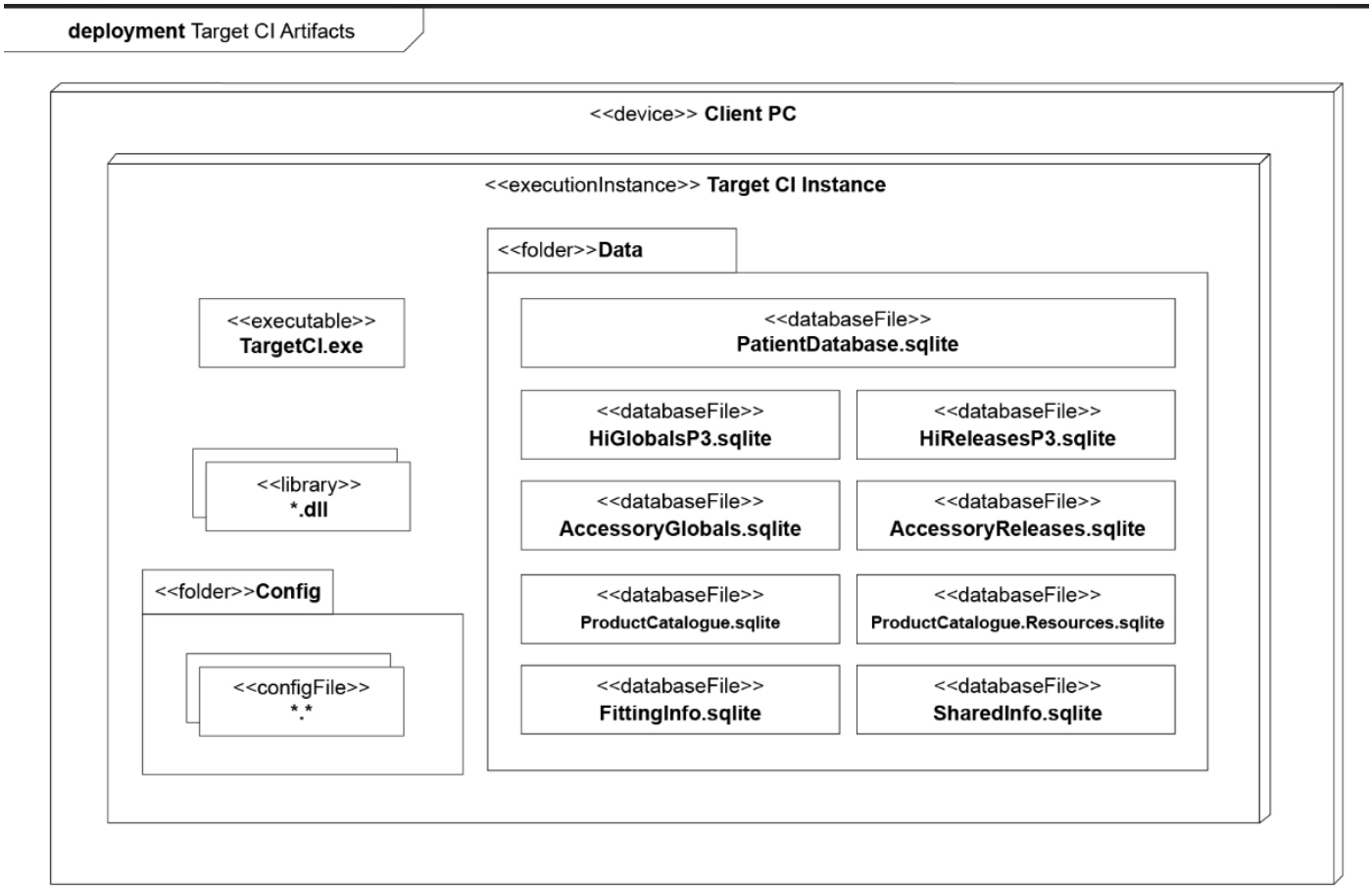


3.3 DEPLOYMENT ARTIFACTS

The fitting software installs with an executable file and a set of associated files including component DLLs, configuration files, and SQLite database files. The configuration files are installed in folder “%ProgramData%\Advanced Bionics\Target CI\Target CI\Config” and database files are installed in folder “%ProgramData%\Advanced Bionics\Target CI\Target CI\Data.” The Data folder holds a single transactional database file and several info database files.

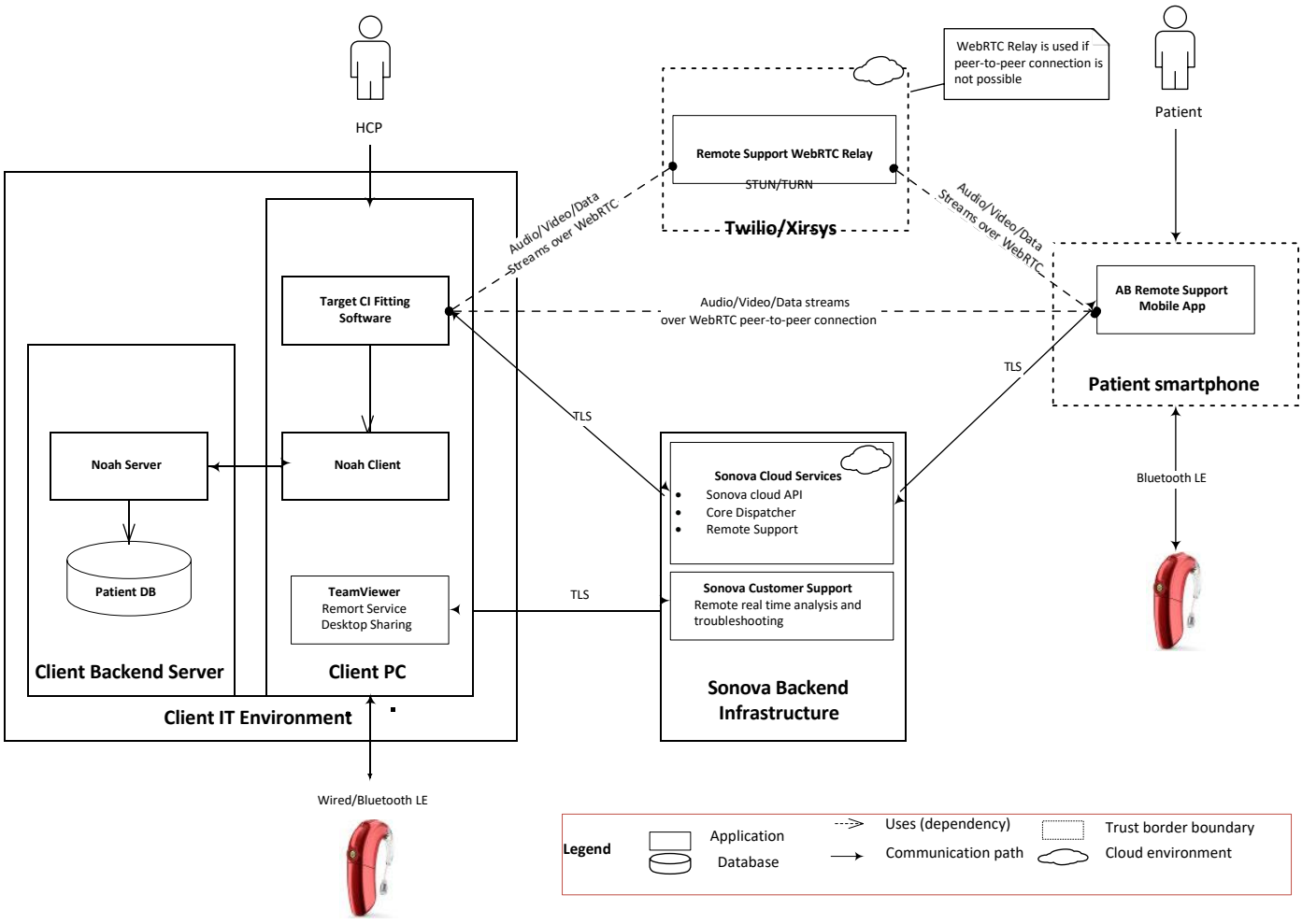
The transactional database, PatientDatabase.sqlite, stores the demographics and fitting data of the patient and will be installed only when the fitting software is deployed in standalone mode.

When the fitting software is deployed as a Noah module, the Noah system supplies the required patient data persistence services to the fitting software. The remaining sqlite files are integral to the fitting software and required for all deployment models.



3.4 SYSTEM INTERCONNECTIONS

The diagram and table below illustrate the primary system interconnections. Typically, only a portion of the available interconnections are utilized.



Source / Destination	Service	Protocol	Port	Description
Hearing devices	Hearing device communication	Wired connection / Bluetooth® Low Energy	N/A	Used to communicate with hearing devices for control, configuration and status & data readout purposes
Noah	Noah 4 ModuleAPI	.NET Remoting	N/A	Primary interface for the module used to access the Noah software (in Noah distributed deployment model only)
Sonova Cloud Services	Sonova Cloud API, Core dispatcher, Remote support	SOAP, REST	443	Sonova services hosted in a Microsoft Azure Data Center are used to: • fetch fitting software client configuration data from Sonova backend storage • transfer logging and analytics data

Source / Destination	Service	Protocol	Port	Description
				• establish real time remote fitting sessions
Twilio/Xirsys, AB Remote Support Mobile App	Remote Support	WebRTC	List of ports available upon request	Twilio's cloud communication services are hosted on third-party cloud platforms, specifically Amazon Web Services (AWS) and Google Cloud Platform (GCP). These services are utilized exclusively by the remote support feature of the fitting software, which enables WebRTC signaling and real-time remote fitting sessions to take place.
AB Customer Support	Desktop sharing	TeamViewer proprietary protocol	5938, 443, 80 Refer to TeamViewerPorts	Used to perform remote real time analysis and troubleshooting of issues affecting fitting software installations. Refer to section 6.6 REMOTE SERVICE for more information.

4. SYSTEM REQUIREMENTS

Operating System	64-bit Windows 10 Pro/Enterprise
.NET Framework	Version 4.8
CPU	Intel® Core™ i5 or equivalent with equal or better performance
RAM	4GB or more
Hard Disk Space	3GB or more
Minimum Display Requirements	• 1280 x 1024 resolution (maximum scaling 125%) • 24-bit color
Device Drivers	• Noahlink Wireless driver (latest version available from HIMSA is required if using third-party USB-connected Noahlink Wireless programming interface). • CPI-3 driver (required if using a USB-connected CPI-3 programming interface).
Database	SQLite or Noah System 4 (version 4.14 or higher)
Internet Connection	Internet connection required for remote support and analytics logging, see section 4.4 System Interconnections; intranet required when using networked Noah System 4.
Network Ports	See section 3.4 System Interconnections; see section 3. Other Resources — HIMSA for ports used by Noah System 4.

5. INSTALLATION

5.1 REQUIREMENTS

An Administrator account is required to install the fitting software. Once the software is installed, it can be run without administrative or elevated permissions.

See section 8, Software Integrity, for information on validating the integrity of the software prior to installation.

Prior to installation, system administrators are recommended to make sure that:

• the fitting software product version to be installed is the latest available.

• the underlying operating system is up-to-date.

5.2 INSTALLER TYPES

Two installers are available for installing the fitting software:

• Standard Installer

• IT Professional Installer

The IT Professional installer is a single MSI file and excludes prerequisite components but is otherwise equivalent to the Standard installer.

Prerequisite components include the Microsoft .NET Framework v4.8, and the Microsoft Visual C++ Redistributable packages.

Both installers support advanced installation scenarios, including silent installation.

The IT Professional Installer should only be used if your organization requires prerequisite components to be installed and managed by your organization and not by the fitting software installer. The Standard Installer should be used in all other cases.

The IT Professional Installer may be obtained from AB clinical representative. The IT Professional installer cannot be used to repair, reinstall, or uninstall installations by the Standard installer. The Standard installer cannot be used to repair, reinstall, or uninstall installations by the IT Professional installer.

6. SECURITY CONTROLS

The fitting software is a client application installed on a commercial Microsoft Windows off-the-shelf PC. The fitting software can be installed as standalone application or as a Noah module.

6.1 AUTHENTICATION – STANDALONE DEPLOYMENT

When the fitting software is installed as a standalone application, it relies on the access control mechanisms provided by the host operating system. The host operating system may be configured by the customer's IT personnel to manage authentication. The fitting software does not have any such integral facility. Advanced Bionics recommends that each user login to the host OS with a unique per-user account.

6.2 AUTHENTICATION – NOAH DEPLOYMENT

When the fitting software is installed as a Noah module, access control is provided by Noah System 4.
See www.HIMSA.com for audit controls used by Noah System 4.

6.3 AUTHORIZATION

The fitting software does not restrict access to its features based on the roles of individual users. The software supports a single major function of fitting patient's hearing devices and a single role of fitting professional. Role- based access controls are not applicable.

6.4 AUDIT – STANDALONE DEPLOYMENT

When the fitting software is installed as a standalone application, it relies on the audit mechanisms provided by the host operating system. The fitting software does not have any such integrated facility. The host operating system may be configured by the customer's IT personnel to log launches/executions of the fitting software and user logins. Advanced Bionics recommends that each user login to the host OS with a unique per-user account to facilitate auditing.

6.5 AUDIT – NOAH DEPLOYMENT

When the fitting software is installed as a Noah module, audit logs are provided by Noah system. See https://www.himsa.com/ for audit controls used by Noah System 4.

6.6 REMOTE ACCESS

The Desktop Sharing feature allows for remote real time analysis and troubleshooting of issues affecting fitting software installations. This feature is based on the TeamViewer QuickSupport 3rd-party tool (deployed by default together with fitting software) and allows AB customer support professionals to remotely connect to the HCP's computer and gain full desktop control of it, including access to the underlying operating and file system.

To establish a Desktop Sharing session, HCP interaction is required. HCP shall first execute the TeamViewer QuickSupport tool (e.g., through the Target CI fitting software) and communicate their TeamViewer ID credentials to the AB Support team through an out-of-band communication channel (e.g., phone call).

The AB support team member's name and their TeamViewer ID are by default displayed on the HCP's computer monitor during each active Desktop Sharing session.

All Desktop Sharing network traffic is secured meeting or exceeding cryptographic protocols and algorithms standards (RSA public/private key exchange and AES 256-bit session encryption).

TeamViewer QuickSupport can be manually removed without affecting other Target FSW functionalities. The Target FSW installation program supports a command line installation parameter to allow a Target FSW command line installation without including the TeamViewer QuickSupport tool.

7. INFORMATION PROTECTION

7.1 ADVANCED BIONICS PRIVACY POLICY

The privacy policy describing how Advanced Bionics collects, transfers, stores, and uses personal data, can be downloaded from: AdvancedBionics.com/privacy.

Advanced Bionics does not host, store, backup, or have access to any data stored within the fitting software or Noah databases, unless the data is expressly sent to Advanced Bionics.

7.2 FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

Target CI v1.5 is compliant with FIPS 140-2 encryption standards.

7.3 SECURITY IN TRANSIT

Communication security is ensured and enabled in all inbound and outbound fitting software network communications. Except for the Remote Support feature (which uses the WebRTC protocol) and Bluetooth communication with hearing devices & accessories, all other connections are protected by the Transport Layer Security (TLS) protocol which provides confidentiality, integrity, and authenticity.

TLS

TLS configuration is compliant to current best practices and security recommendations documented in BCP 195 – Recommendations for Secure Use of TLS and DTLS, BCP195 including:

- Not supporting SSL and TLS versions prior to 1.2
- Not supporting cipher suites that use cryptographic algorithms offering less than 128 bits of security
- Supporting recommended TLS extensions of BCP 195
- Not supporting insecure extensions of BCP 195

DTLS

Encryption is a mandatory feature of WebRTC and is enforced on all media streams sent over WebRTC. The encryption protocol used depends on the channel type; data streams are encrypted using DTLS and media streams are encrypted using Secure Real-time Transport Protocol (SRTP) used because it is a lighter-weight option than DTLS.

Refer to the following link for more detailed information about security configuration of Remote Support WebRTC:

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

BLE

Bluetooth Low Energy wireless communication with hearing devices and accessories is encrypted and integrity protected by default (except for identification and detection use cases). In addition to that, the duration of the hearing device's Bluetooth pairing mode is limited in time. Refer to available hearing device documentation for more detailed description about security of Bluetooth communication channel.

7.4 SECURITY AT REST

Patient database – Standalone Deployment model

If the fitting software is installed as a standalone application, the patient database is stored locally at: C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

These records are not encrypted at rest by default. Protected Health Information (PHI) and Personally identifiable information (PII) is stored in a database that is internal to the fitting software and is not transmitted over the network.

In some jurisdictions, regulations may require encrypting all patient data to avoid potential liability in case of data loss or theft. Enable BitLocker or equivalent full-disk encryption (OS-level or hardware-based) to safeguard the data from unauthorized access or copying while the data is at rest.

BitLocker is a built-in Windows feature that encrypts the entire drive and requires authentication to access. Always consult Microsoft's official guidance and your organization's IT security policy before enabling BitLocker.

How to Enable BitLocker

Administrator privileges are required to manage BitLocker.

1.Search “Manage BitLocker”

Open the Start menu, type “Manage BitLocker,” and select it from the search results.

2. Select the System Drive

Choose the drive where Windows is installed to configure encryption settings.

3. Choose an Unlock Method

Select one of the following options:

- TPM only

- TPM + PIN

- TPM + USB key

Follow Microsoft’s best practice guidance and your organization’s IT security policy when selecting the unlock method.

4. Back Up the Recovery Key

Back up the recovery key using secure, enterprise-approved methods. Recommended options include:

- Storing in Microsoft Entra ID (formerly Azure AD) or Active Directory for domain-joined devices

- Saving to a secure, access-controlled network location with encryption and audit logging

- Using a managed key escrow solution approved by your organization

Avoid saving the key to local drives, USBs, or printing it unless explicitly permitted by policy. Recovery keys must be protected with the same rigor as other sensitive credentials and rotated immediately if exposed.

5. Start Encryption

Choose:

- Entire drive – recommended for most enterprise scenarios. Encrypts all sectors, including unused space, to prevent data remanence.

Patient database – Noah Distributed Deployment module

When the fitting software is installed as a Noah module, PII is stored within the patient database hosted by Noah. The patient database hosted by Noah may reside on another machine. PII and other patient data is maintained by Noah software and the encryption of the patient’s data-at-rest is ensured by the Noah System. The fitting software may transmit/receive PII via a wired or wireless network connection when a Noah database is configured for network access.

PII stored on networked Noah database will be visible to other device users on different PCs that have permissions to the same networked database. The Noah database may also be configured for non-network access and installed on the same PC as the fitting software.

Noah prevents the fitting software from accessing the patient-record database. When a user opens a patient in the fitting software via the Noah Client, the fitting software is only able to read from and write to the currently opened patient record and is not able to access other patient records in the Noah database.

See section www.HIMSA.com for encryption standards used by Noah System 4.

RMA Export Files

The fitting software allows client information to be exported to a file. The RMA file can be sent to Advanced Bionics to resolve RMA or related support issues.

The RMA file is asymmetrically RSA encrypted using a 512-bit key length. The fitting software does not have any facility to decrypt an RMA file.

Anonymized Export Files

The fitting software allows client information to be exported to a client-anonymized file. The client's personally identifiable information, such as birthdate and name, are replaced with generic values. The file is not encrypted and can be imported into the same instance or a different instance of the fitting software.

Standard Export Files

The fitting software allows client information to be exported to a standard export file. The file uses a proprietary binary format and is not encrypted. The file can be imported into the same or a different instance of the fitting software. When using this feature, fitting software users must ensure that standard export files are handled according to their local IT policies for managing unencrypted PII.

Hearing Device

The fitting software stores client information on the client's hearing device. Personally identifiable information such as the client's name and birthdate are not stored on the hearing device. Other non-PII information is stored using PBKDF2 encryption with a 128-bit key.

The fitting software may transmit/receive non-PII client information to/from a hearing instrument via a proprietary wired device (i.e., CPI-3), AB Remote Support mobile application, or Noahlink Wireless device. The Noahlink Wireless device connects with the hearing device using Bluetooth Low Energy (BLE) via a standard BLE 128-bit AES encrypted channel.

8. SOFTWARE INTEGRITY

8.1 VERIFICATION OF DOWNLOADED INSTALLATION MEDIA

The Target CI fitting software installation media may be downloaded in some regions from Advanced Bionics' Pro Portal or Sonova Web Client. The downloaded installation media can be authenticated using any trusted SHA-256 hashing tool.

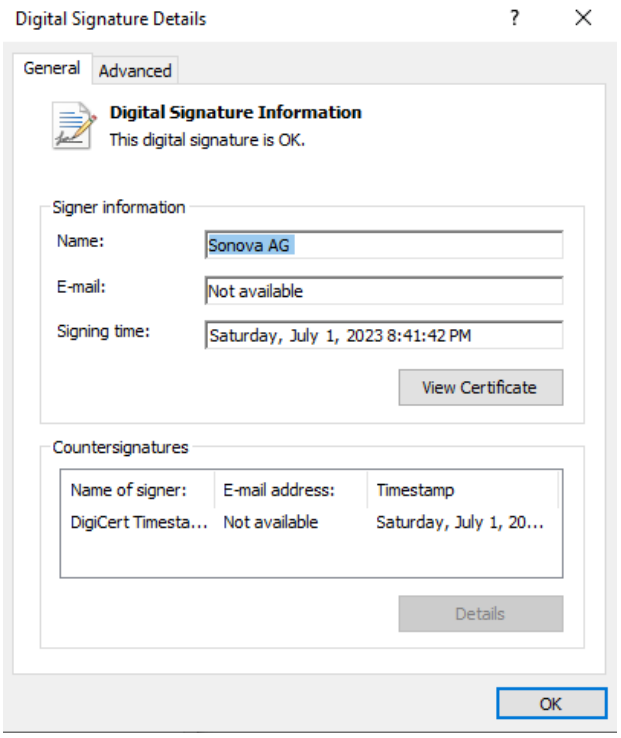
The SHA256 hash for the standard installation zip file is:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

The SHA256 hash for the IT Professional installation zip file is:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 MANUAL VERIFICATION OF FITTING SOFTWARE PRIOR TO INSTALLATION

Users may perform the following steps to verify the fitting software's integrity and authenticity prior to installation:

1. Open Windows Explorer and navigate to the root folder of the fitting software's installation media. If your installation media is a thumb drive, insert it into a USB port and navigate to its root. If your installation media is a zip file, unzip it to a folder and navigate to that folder.
2. Right click on SonovaVerify.exe and select Properties from the context menu.
3. Select the Digital Signatures tab.
4. Double click the SHA256 "Sonova AG" signature.
5. Verify the elements of the signature are valid. In particular, verify that the message "The digital signature is OK." appears near the top and that the signer's name and signing time match the following image:



1. Close the popup dialogs and double click SonovaVerify.exe.
2. Verify that "NO ERRORS DETECTED." is displayed as shown in the following image:

```
   FILES PROCESSED: 79

   IGNORED FILES: 1
       .\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

The image shows that SonovaVerify has authenticated and verified digital signatures of all files on the installation media, including the installer. This verifies that the installation media has not been tampered with, corrupted, or otherwise compromised. SonovaVerify will display warnings or error messages if files or folders are missing, or unexpected files or folders have been added to the installation media.

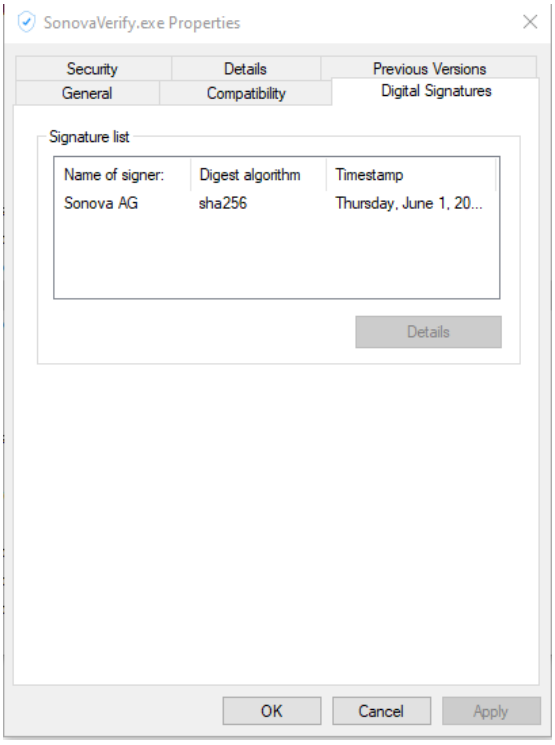
8.3 AUTOMATIC VERIFICATION OF INSTALLED FITTING SOFTWARE INTEGRITY

SonovaVerify is integrated with the fitting software and runs each time the application is launched to verify the integrity of the fitting software's program files. Program files are digitally signed using industry-standard practices and certificates issued by a trusted certificate authority. The software notifies the user via warning messages if any program files are compromised.

8.4 MANUAL VERIFICATION OF INSTALLED FITTING SOFTWARE INTEGRITY

Users may perform the following steps to verify the installed fitting software's integrity and authenticity at any time without the need to launch the fitting software:

1. Open Windows Explorer and navigate to the fitting software's executable folder, usually located in: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Right click on SonovaVerify.exe and select Properties from the context menu.
3. Select the Digital Signatures tab.
4. Double click the SHA256 "Sonova AG" signature.
5. Verify the elements of the signature are valid, in particular that the message "The digital signature is OK." appears near the top and that the signer's name and signing time match the following image:



1. Close the popup dialogs and double click SonovaVerify.exe.
2. Verify that “NO ERRORS DETECTED.” is displayed as shown in the following image:

The image shows that SonovaVerify has authenticated and verified digital signatures of all installed program files. This verifies that the fitting software has not been tampered with, corrupted, or otherwise compromised. SonovaVerify will display warnings or error messages if files or folders are missing, or unexpected files or folders have been added to the program files folder.

9. SOFTWARE PATCHES AND UPDATES

Auto-updates are not supported.

10. DATA MANAGEMENT

10.1 DATABASES

The fitting software uses a transactional database for storing patient data and a set of info databases that provide metadata configurations required by the application.

See Section 3. Network and Context Diagrams - Deployment Artifacts for a detailed list of all databases deployed by the fitting software.

When the fitting software is installed as a standalone application, the patient database is internal to the fitting software. The patient database, stored in file PatientDatabase.sqlite, resides on the same machine as the fitting software and provides the storage for patient data. To back up application data when Target CI is deployed as a standalone application, create a backup copy of the entire folder located at %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Protect data backups not only from data loss but also from theft. When the fitting software is installed as a Noah module, patient data is stored in the database provided by the Noah System. The Noah database may be configured for network access. The Noah database may also be configured for non-network access and installed on the same PC as the fitting software. Configure Noah database encryption to protect data (refer to HIMSA documentation.

For the Noah distributed deployment mode, refer to the following link for instructions about backup and restore of the Noah patient database:

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 DATA MIGRATION

The fitting software allows users to migrate patient records from AB's previous fitting software, SoundWave 3.2. Patient records must be accessible from a SoundWave 3.2 installation on the same computer as Target CI in order to be migrated.

10.3 HEARING DEVICE CONFIGURATIONS

The fitting software provides for exporting and importing device configuration and settings.

10.4 DATA DISPOSAL

Instructions for data disposal can be found in the IFU (Instructions For Use) or on the following site for Noah deployments: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

11. SECURITY ENVIRONMENT – SHARED RESPONSIBILITY

The fitting software has been designed for an intended use in which cybersecurity risk management is considered a shared responsibility among stakeholders across the entire hearing care ecosystem which include, but are not limited to, hearing device users, parents or legal guardians of children who are hearing device users, HCPs, IT administrators, hearing care facilities and providers, vendors of hearing devices and programming equipment.

Here follows a list of best common practice recommendations and security controls for the fitting environment where the fitting software will be used:

OS level

- Apply access controls at OS level, e.g.:

    - Eliminate guest accounts
    - Activate the Windows user login
    - Maintain a list of authorized operators to control access to the system
    - Set customized users and roles
    - Apply strong passwords requirements and keep credentials secret
- Apply audit controls at OS level
- Keep the operating system up-to-date.
- Keep the installed fitting software version up-to-date.
- Enable up-to-date malware and antivirus protection
- Enable application whitelisting

Data protection

- Encrypt patient data using 3rd party tools or controls at OS level e.g., by using drive encryption (e.g., the free Microsoft BitLocker) to protect all data. For Noah deployments, consider using the Noah database encryption.
- External media containing data exported from fitting software including reports and logs should be secured. When no longer used, the data should be securely erased and/or the media should be securely deleted.
- Use USB storage media with built in security functionality, like encrypted USB drives with integrated keypad.
- Make sure to always keep data safe:
    - When transferring data through unsafe channels, either send anonymous data or encrypt it.
    - Protect data backups not only from data loss but also from theft.
    - Remove all data from data medium which are no longer used or will be disposed.
- Approved procedures and tools should be used by users for secure removal of data stored on removable media, according to applicable regulations and guidelines for handling patient information / personally identifiable information (PII) / protected health information (PHI)

IT infrastructure

Operate fitting software in a secure network environment protected from unauthorized intrusion. There are many effective techniques for isolating and protecting medical information systems, including implementing firewall protection, demilitarized zones (DMZs), Virtual Local Area Networks (VLANs) and network enclaves. Maintain an active network connection to receive operating system updates.

Physical level

- The workstation where fitting software is installed should be physically secured in a way that it is not accessible for unintended users.
- Ensure that unauthorized personnel do not tamper with the system.
- Access to printers connected to the workstation should be controlled.
- The monitor of the workstation where fitting software is installed should be placed in a way limiting the visibility of the screen content to the user only.

Organizational level

- Only professionally trained, fully qualified personnel are authorized to operate the system. Before authorizing anyone to operate the system, it should be verified that the person has read, and fully understands, the operating instructions provided with the fitting software.
- If you notice any suspicious activity on your fitting software accounts or any unexpected operation, contact Advanced Bionics. Refer to section 2.1 for more information.

For more information about shared responsibility and for a more detailed list of best practice recommendations and security controls for the fitting environment where the fitting software will be used to be applied at various levels refer to:

- the EHIMA Whitepaper “Best Practices for Secure Fitting of Hearing Devices,” EHIMAWhitePaper

12. MANUFACTURING AND SOFTWARE DEVELOPMENT PROCESS

Cybersecurity is considered throughout the entire software development process. The fitting software is developed in compliance with IEC 62304 and IEC 82304 standards.

The fitting software is scanned for viruses and malware as part of the manufacturing process.

Vulnerabilities in third-party components listed in NIST’s National Vulnerability Database (NVD), are assessed, and mitigated during the development process and monitored once the fitting software has been released to the market.

13. SOFTWARE COMPONENTS AND BILL OF MATERIALS

The fitting software incorporates certain commercial off-the-shelf software components.

The following table enumerates all SOUP (Software of Unknown Provenance) distributed with the fitting software.

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
ciAD Hearingloss Simulator	Hearing loss simulator library for media player	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	Credential Management package is a wrapper for the Windows Credential Management API	iLya Lozovyy	1.0.2
CSharpAnalytics	Used for Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron,Marc Gravell,Nick Craver	2.0.78
Destructurama.Attributed	Used by Nephele libraries.	Serilog Contributors	3.0
DirectShow 2005	Allows access to Microsoft's DirectShow functionality from within .NET applications.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	National Centre for Audiology, Canada	4.2
DSL5	DSL 5 Fitting formula library	National Centre for Audiology, Canada	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical repacked for Sonova	GNOtometrics	2.0.1.9
IceLink	Used for WebRTC audio/video conference integration	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect & OAuth 2.0 client library used by the Kona.CommonServices.Authentication component for OAuth 2 authentication.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Noah Inter-Module Communication Interface Library	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Used by libraries coming from Sonova to communicate with Git	LibGit2Sharp contributors	0.26.1
Mapster	Used for mapping objects in code	chaowlert,eric_swann	7.2.0.0
MathNet.Numerics	Used for fitting algorithms (signal path, target matcher etc)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael and contributors	4.11.0
Microsoft.Bcl.AsyncInterfaces	Provides the IAsyncEnumerable<T> and IAsyncDisposable interfaces and helper types for .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Used by the libraries coming from Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Used by the libraries coming from Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	3.9
Microsoft.Identity.Client	The MSAL library for .NET is part of the Microsoft identity platform for developers (formerly named Azure AD) v2.0. It enables you to acquire security tokens to call protected APIs. It uses industry standard OAuth2 and OpenID Connect.	Microsoft	4.38.0.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Microsoft.Identity.Client.Extensions.Msal	Secure cross-platform token cache for MSAL public client apps.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Includes types that provide support for creating, serializing and validating JSON Web Tokens. Used by components that communicate with back-end services that use JSON Web Tokens for authentication.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	Dependecy of Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Dependency of the SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Used for FSW backup tool (automated backups).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors is an easy-to-use means of adding common and reusable interactivity to your WPF applications with minimal code.	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 runtime libraries	Microsoft Visual C++ runtime libraries	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	Used to adjust volumes and play soundfiles.	Open Source	1.9
.NET Framework	.NET runtime framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Used for JSON serialization and de-serialization.	James Newton-King	12.0.3
Nibelung	NoahLink Wireless fitting libraries	GN ReSound	1.3.16.1
Nlog	This a dependency of the HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	4.4.0
NoahLink	NoahLink fitting device driver	HIMSA	1.55.6.166

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
NoahLink Wireless	NoahLink Wireless fitting device driver	HIMSA	2.0.0.68
Otometrics.HiPro2	HiPro communication libraries	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Otometrics' abstraction Layer above the Noah Inter-Module Communication Interface Library	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	The C# PDF Library to Create and Edit PDF documents in .Net applications.	Patagames.com	4.54.2704.0
Polly	Library that allows developers to express resilience and transient fault handling policies such as Retry, Circuit Breaker, Bulkhead Isolation and Fallback in a fluent and thread-safe manner	App vNext	7.2.1
Polly.Extensions.Http	A library containing opinionated convenience methods for configuring Polly policies to handle transient faults typical of calls through HttpClient.	App vNext	3.0
Polly.Contrib.WaitAndRetry	A library for Polly containing helper methods for a variety of wait-and-retry strategies.	Grant Dickinson, App vNext	1.1.1
Portable.BouncyCastle	This a dependency of the HIMSA Nibelung.CPD (Noahlink Wirlesss)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Serialization framework used for RC blob.	Open Source	2.0.0.668
Serilog	The logging component which is used for the whole Chinook application.	Serilog Contributors	2.10.0
Serilog.Enrichers.Thread	Enrich Serilog events with properties from the current thread	Serilog Contributors	3.1
Serilog.Expressions	Expression-based event filtering for Serilog.	Serilog Contributors	2.0
Serilog.Sinks.Console	A Serilog sink that writes log events to the console/terminal.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	A Serilog sink that writes log events to the debug output window.	Serilog Contributors	2.0
Serilog.Sinks.File	Write Serilog events to text files in plain or JSON format.	Serilog Contributors	4.1
Serilog.Sinks.Trace	The diagnostic trace sink for Serilog.	Serilog Contributors	2.1
Serilog.Settings.AppSettings	XML configuration (System.Configuration <appSettings>) support for Serilog.	Serilog Contributors	2.2.2

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Security.Cryptography	Extensions to the security APIs shipped with the .NET framework	Microsoft	1.7.2
SharpBITS API	SharpBITS.NET is a .NET wrapper of the BITS API and a little Windows UI application for easier access to BITS up- and downloads.	perpetualKid	2.1.0.0
SharpZipLib	#ziplib (SharpZipLib, formerly NzipLib) is a Zip, Gzip, Tar and Bzip2 library written entirely in C# for the .NET platform. This library provides compression functionality (zip, unzip, stream compression, etc.). We use it in the Firmware Update app.	Open Source	1.1.0.145
Superpower	A parser combinator library for C#	Datalust,Superpower Contributors,Sprache Contributors	2.3
SQLite.Interop	SQLite is a software library that provides a relational database management system. The lite in SQLite means light weight in terms of setup, database administration, and required resource. SQLite has the following noticeable features: self-contained, serverless, zero-configuration, transactional. It is a database (SQLite 3.32.1) to store information about patient (in standalone mode), our product catalog resources and the metadata for fitting, accessories and His.	SQLite Development Team	1.0.113
System.Buffers	Provides resource pooling of any type for performance-critical applications that allocate and deallocate objects frequently.	23rogramma,dotnetframework	4.5.1
System.Collections.Immutable	Used by the libraries coming from Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	5.0
System.ComponentModel.Annotations	Provides attributes that are used to define metadata for objects used as data sources.	23rogramma,dotnetframework	4.7
System.Configuration.ConfigurationManager	Provides types that support using configuration files.	Microsoft	5.0
System.Data.SQLite.Core	Used by the libraries coming from Sonova.HardwareAbstraction.Palio.Trafo	SQLite Development Team	1.0.113.7
System.Drawing.Common	Provides access to GDI+ graphics functionality.	Microsoft	5.0.1
System.IdentityModel.Tokens.Jwt	Includes types that provide support for creating, serializing and validating JSON Web Tokens. Used by components that communicate with back-end services that use JSON Web Tokens for authentication.	Microsoft	6.8.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System.IO.Abstractions	A set of abstractions to help make file system interactions testable.	Tatham Oddie & friends	12.0.10
System.Numerics.Vectors	Provides hardware-accelerated numeric types, suitable for high-performance processing and graphics applications.	24rogramma,dotnetframework	4.5
System.Memory	Provides types for efficient representation and pooling of managed, stack, and native memory segments and sequences of such segments, along with primitives to parse and format UTF-8 encoded text stored in those memory segments.	24rogramma,dotnetframework	4.5.4
System.Reactive.Core	Reactive Extensions (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.Interfaces	Reactive Extensions (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Reactive Extensions (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Reactive Extensions (Rx) for .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Reactive Extensions (Rx) for .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Provides a class to dynamically create proxy types that implement a specified interface and derive from a specified DispatchProxy type. Method invocations on the generated proxyinstance are dispatched to that DispatchProxy base type.	Microsoft	4.7.1
System.Reflection.Metadata	This package provides a low-level .NET (ECMA-335) metadata reader and writer. It is geared for performance and is the ideal choice for building higher-level libraries that intend to provide their own object model, such as compilers.	Microsoft	5.0
System.Runtime.CompilerServices.Unsafe	Provides the System.Runtime. CompilerServices.Unsafe class, which provides generic, low-level functionality for manipulating pointers.	24rogramma, dotnetframework	5.0
System.Security.AccessControl	Provides base classes that enable managing access and audit control lists on securable objects.	Microsoft	5.0
System.Security.Permissions	Provides types supporting Code Access Security (CAS).	Microsoft	5.0
System.Security.Principal.Windows	Provides classes for retrieving the current Windows user and for interacting with Windows users and groups.	Microsoft	5.0
System.Text.Encoding.CodePages	Provides support for code-page based encodings, including Windows-1252, Shift-JIS, and GB2312.	Microsoft	5.0
System.Text.Encodings.Web	Provides types for encoding and escaping strings for use in JavaScript, HyperText Markup Language (HTML), and uniform resource locators (URL). Is a dependency of SOUP IdentityModel	24rogramma,dotnetframework	5.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System.Text.Json	Provides high-performance and low-allocating types that serialize objects to JavaScript Object Notation (JSON) text and deserialize JSON text to objects, with UTF-8 support built-in. Also provides types to read and write JSON text encoded as UTF-8, and to create an in-memory document object model (DOM), that is read- only, for random access of the JSON elements within a structured view of the data.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Provides additional types that simplify the work of writing concurrent and asynchronous code.	25rogramma,dotnetframework	4.5.4
System.ValueTuple	Provides the System.ValueTuple structs, which implement the underlying types for tuples in C# and Visual Basic. Adds value tuples support since they are only included in later .NET framework versions.	25rogramma,dotnetframework	4.5.0
Thrift	Used for remotelink protocol definition	Apache	0.13.0.0
Unity	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	5.8.13
WAP BT Dongle Driver	WAP BT Dongle Driver (Fitting Dongle)	iAnywhere Solutions	3.0.0.6095
WebSync	Used for integration of fitting data channel	FM (Frozen Mountain)	4.9.32.0
Xps to Pdf render (NiXPS)	Convert 25rogrammatically xps files to pdf; used in fitting app reports.	NiXPS	2.6.7.0

14. REFERENCES

Title	Website
Instructions for Use (Electronic)	https://ifu.advancedbionics.com/
Advanced Bionics Global Privacy Policy	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Backing up and restoring the data in your Noah database	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Noah System Database Capacity has been Reached.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer - List of used ports	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
LiveSwitch Server Security Documentation	https://developer.liveswitch.io/liveswitch-server/server/security.html
Best Practices for Secure Fitting of Hearing Devices EHIMA whitepaper	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

For information on additional AB locations, please visit
advancedbionics.com/contact

AB – A Sonova brand

Please contact your local AB representative for regulatory approval and availability in your region.

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S396-02 Rev A 2025-09-15