

Target CI v1.6

GUIDA ALLA SICUREZZA INFORMATICA

Italiano

Aggiornato: luglio 2026



Sommario

1. INTRODUZIONE.....	3
1.1 ABBREVIAZIONI E DEFINIZIONI:.....	3
2. ALTRE RISORSE	4
2.1 ASSISTENZA CLIENTI	4
2.2 AB PRO PORTAL	4
2.3 GUIDA AVANZATA ALL'INSTALLAZIONE	4
2.4 CONFIGURAZIONE DEL FIREWALL DI TARGET CI	4
2.5 MDS2	4
2.6 ISTRUZIONI PER L'USO (IFU)	5
2.7 HIMSA.....	5
3. DIAGRAMMI DI CONTESTO E RETE.....	6
3.1 MODELLO DI DISTRIBUZIONE 1: AUTONOMO.....	6
3.2 MODELLO DI DISTRIBUZIONE 2: DISTRIBUITO CON NOAH	7
3.3 ARTEFATTI DI DISTRIBUZIONE	8
3.4 INTERCONNESSIONI DI SISTEMA.....	9
4. REQUISITI DI SISTEMA.....	11
5. SICUREZZA INFORMATICA NEL CICLO DI VITA DEL PRODOTTO	12
5.1 DISTRIBUZIONE	12
5.2 INSTALLAZIONE	12
5.3 CONFIGURAZIONE E FUNZIONAMENTO	13
5.4 RIMOZIONE E DISMISSIONE	14
6. CONTROLLI DI SICUREZZA	16
6.1 CONTROLLI DI ACCESSO	16
6.2 REGISTRAZIONE DEGLI AUDIT E CONTROLLI DI RESPONSABILITÀ	17
6.3 ACCESSO REMOTO	17
7. PROTEZIONE DELLE INFORMAZIONI	18
7.1 INFORMATIVA SULLA PRIVACY DI ADVANCED BIONICS	18
7.2 STANDARD FEDERALI PER IL TRATTAMENTO DELLE INFORMAZIONI (FIPS)	18
7.3 PII/PHI TRATTATE DAL PRODOTTO	18
7.4 SICUREZZA DURANTE IL TRASFERIMENTO	19
7.5 SICUREZZA A RIPOSO	20

8. INTEGRITÀ DEL SOFTWARE	23
8.1 VERIFICA DEL SUPPORTO DI INSTALLAZIONE SCARICATO	23
8.2 VERIFICA MANUALE DEL SOFTWARE DI FITTING PRIMA DELL'INSTALLAZIONE.....	24
8.3 VERIFICA AUTOMATICA DELL'INTEGRITÀ DEL SOFTWARE DI FITTING INSTALLATO	25
8.4 VERIFICA MANUALE DELL'INTEGRITÀ DEL SOFTWARE DI FITTING INSTALLATO	26
9. PATCH E AGGIORNAMENTI DEL SOFTWARE.....	28
10. GESTIONE DEI DATI.....	28
10.1 DATABASE	28
10.2 MIGRAZIONE DEI DATI	28
10.3 CONFIGURAZIONI DEL DISPOSITIVO ACUSTICO	28
10.4 SMALTIMENTO DEI DATI.....	29
11. AMBIENTE DI SICUREZZA – RESPONSABILITÀ CONDIVISA	29
12. PRODUZIONE, SVILUPPO SOFTWARE E GESTIONE DELLA SICUREZZA	32
13. COMPONENTI SOFTWARE E LISTA DEI MATERIALI.....	33
14. BIBLIOGRAFIA.....	52

1. INTRODUZIONE

Il presente documento fornisce informazioni tecniche sulla sicurezza e sulla privacy relative al sistema software Target CI v1.6 di Advanced Bionics, di seguito denominato “software di fitting”. Il software di fitting è progettato per essere utilizzato da audioprotesisti (HCP) qualificati per la configurazione (ovvero il fitting) di dispositivi acustici per i pazienti che hanno ricevuto impianti cocleari da Advanced Bionics.

Il presente documento si concentra in particolare sulle considerazioni relative alla sicurezza informatica e alla privacy rilevanti per l'utilizzo del software di fitting. Include una valutazione dei controlli di sicurezza e privacy attualmente integrati nel software, nonché di quelli che si prevede saranno applicati e configurati nell'ambiente IT in cui il prodotto verrà utilizzato per lo scopo previsto.

Il presente documento non fornisce informazioni tecniche sulla sicurezza e sulla privacy in merito a:

- Versioni precedenti del software di fitting AB
- Software AB diverso da Target CI v1.6
- Siti web di AB
- Applicazioni mobili di AB
- Dispositivi acustici AB

1.1 ABBREVIAZIONI E DEFINIZIONI:

Acronimo	Significato
FSW	Software di fitting
SaMD	Software as a Medical Device (software come dispositivo medico)
Noah	Un sistema di gestione dei pazienti di terze parti di HIMSA utilizzato per archiviare e gestire i dati demografici dei pazienti e i dati di fitting
TeamViewer	Uno strumento multiplatforma per l'accesso remoto e la condivisione del desktop
SOUP	Software of Unknown Provenance (software di provenienza sconosciuta)
HCP	Audioprotesista
SaMD	Software as a Medical Device (software come dispositivo medico)
AB	Advanced Bionics
Sonova	Advanced Bionics è una società interamente controllata da Sonova e opera come entità a pieno titolo all'interno del Gruppo Sonova.
IFU	Instructions for Use (istruzioni per l'uso)
PHI	Protected Health Information (informazioni sanitarie protette)
PII	Personally Identifiable Information (informazioni di identificazione personale)
SBOM	Software Bill of Material (distinta base del software)

2. ALTRE RISORSE

2.1 ASSISTENZA CLIENTI

Per chi si trova negli Stati Uniti e in Canada, Advanced Bionics mette a disposizione un numero verde per l'assistenza tecnica (877-271-6727), a cui rispondono dei professionisti dedicati, disponibili dal lunedì al venerdì, dalle ore 5:00 alle ore 17:00 (fuso orario del Pacifico).

Per chi si trova fuori dagli Stati Uniti e dal Canada, l'assistenza tecnica viene fornita a livello locale. In caso di domande sul software di fitting, sul relativo hardware o su altre questioni di programmazione, invitiamo a contattare il rappresentante AB locale.

2.2 AB PRO PORTAL

Il software di fitting e la relativa documentazione possono essere scaricati da <https://www.abproportal.com> o dal Sonova Web Client. È necessario effettuare l'accesso all'account. Questa risorsa potrebbe non essere disponibile in tutti i mercati; per ulteriori informazioni, contattare il proprio rappresentante AB.

2.3 GUIDA AVANZATA ALL'INSTALLAZIONE

La Guida avanzata all'installazione di Target CI v1.6 è disponibile su richiesta. La guida fornisce informazioni tecniche sul programma di installazione del software di fitting, comprese le opzioni della riga di comando per installazioni silenziose e automatizzate.

2.4 CONFIGURAZIONE DEL FIREWALL DI TARGET CI

Il documento di configurazione del firewall è disponibile su richiesta. Questo documento fornisce indicazioni di natura informatica al fine di garantire il corretto funzionamento di Target CI 1.6 dietro un firewall aziendale, specificando l'accesso HTTP/HTTPS necessario e i nomi host principali. Tratta la connettività WebRTC tramite Twilio e Xirsys, descrivendo le porte TURN e di peer-relay e sottolinea che molti indirizzi IP sono dinamici, pertanto, ove possibile, è consigliabile utilizzare regole basate sul nome host.

2.5 MDS2

La dichiarazione informativa del produttore per la sicurezza dei dispositivi medici (MDS2) è un modulo standard del settore contenente informazioni in materia di sicurezza e privacy relative al software di fitting AB. Il presente modulo è disponibile su richiesta.

2.6 ISTRUZIONI PER L'USO (IFU)

Le IFU verranno fornite insieme al materiale di installazione del software.

Per alcuni mercati, le IFU elettroniche sono disponibili per il download all'indirizzo www.advancedbionics.com/ifu

Le seguenti sezioni delle IFU possono essere rilevanti per i professionisti IT:

- Descrizione del prodotto
- Requisiti minimi di sistema e caratteristiche di performance
- Linee guida per la sicurezza informatica
- Istruzioni per l'uso
- Smaltimento e materiali pericolosi
- Assistenza tecnica

2.7 HIMSA

Hearing Instrument Manufacturer's Software Association (HIMSA) è un fornitore di software di terze parti che produce Noah System 4, un sistema software progettato per il settore dell'assistenza all'udito che fornisce agli audioprotesisti un sistema indipendente dal fornitore per l'esecuzione di attività correlate al cliente.

Il software di fitting può essere facoltativamente configurato per utilizzare Noah System 4 al posto di un database locale per la conservazione dei dati.

La pagina web sulla sicurezza di HIMSA fornisce risposte alle domande più comuni sulla sicurezza informatica relative a Noah System 4.

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

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

Per ulteriori informazioni sulla sicurezza, consultare la sezione dedicata alla sicurezza di HIMSA Learning Center:

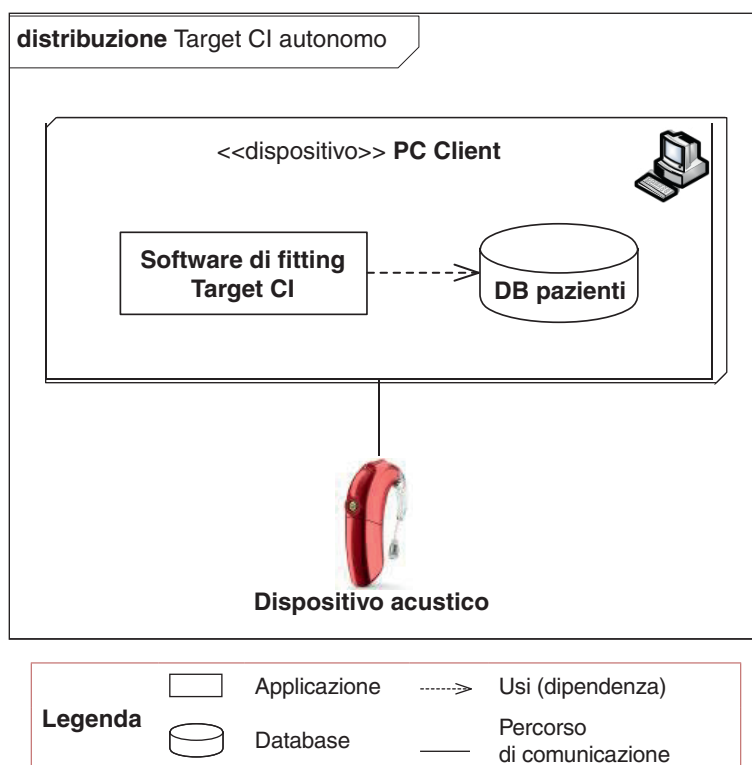
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. DIAGRAMMI DI CONTESTO E RETE

Il software di fitting, un'applicazione client (SaMD) installata su un PC Microsoft Windows disponibile in commercio, supporta due modelli di distribuzione. Il software non include alcun hardware o sistema operativo.

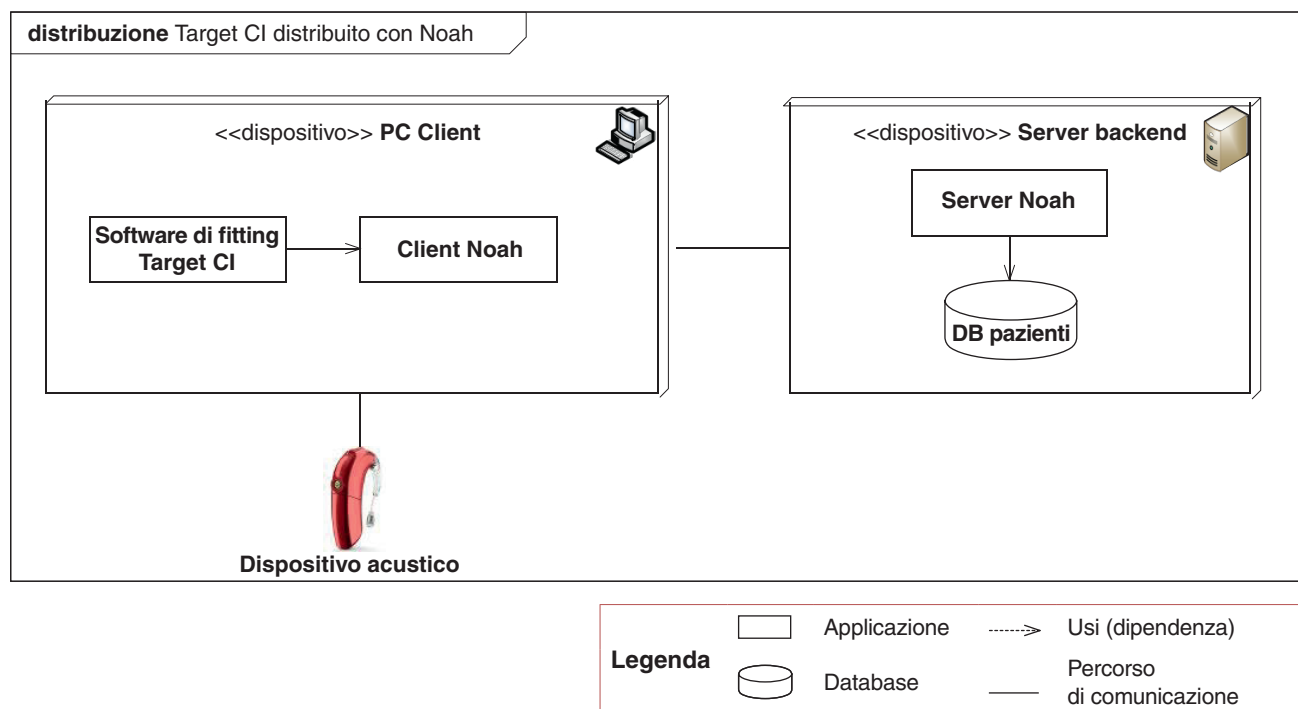
3.1 MODELLO DI DISTRIBUZIONE 1: AUTONOMO

Nel modello di distribuzione autonomo, il software di fitting viene distribuito su un PC client. Il database dei pazienti viene memorizzato sullo stesso PC e installato insieme al software di fitting.



3.2 MODELLO DI DISTRIBUZIONE 2: DISTRIBUITO CON NOAH

Nel modello di distribuzione con Noah, il software di fitting viene distribuito su uno o più PC client su cui è installato Noah. Noah, un sistema di gestione dei pazienti di terze parti, viene distribuito su un server interno accessibile ai PC client. Il database dei pazienti viene conservato sul server Noah e vi si può accedere in rete tramite uno o più PC client.

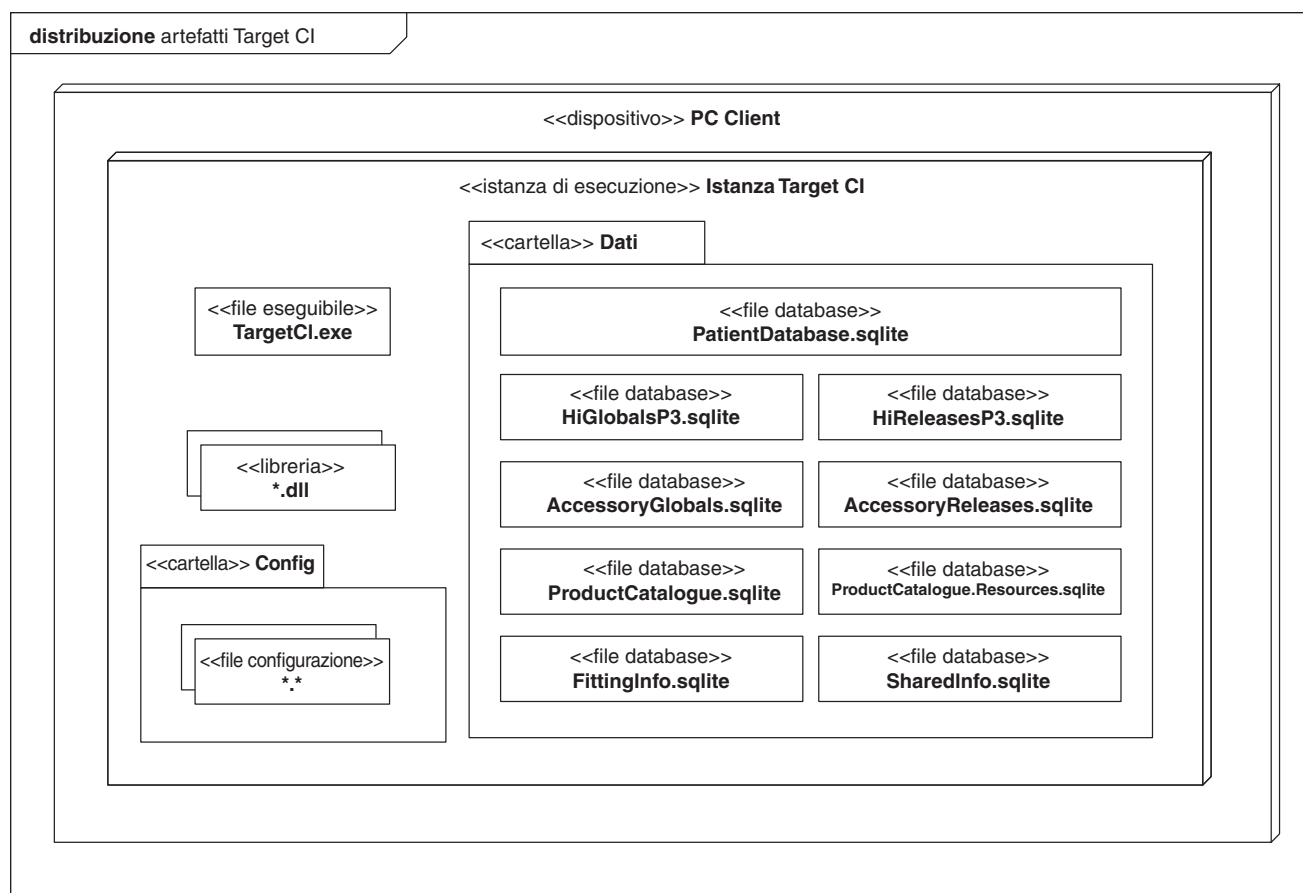


3.3 ARTEFATTI DI DISTRIBUZIONE

Il software di fitting viene installato con un file eseguibile e una serie di file associati, tra cui DLL dei componenti, file di configurazione e file del database SQLite. I file di configurazione vengono installati nella cartella “%ProgramData%\Advanced Bionics\Target CI\Target CI\Config” e file di database vengono installati nella cartella “%ProgramData%\Advanced Bionics\Target CI\Target CI\Data”. La cartella dei dati contiene un singolo file di database transazionale e diversi file di database informativi.

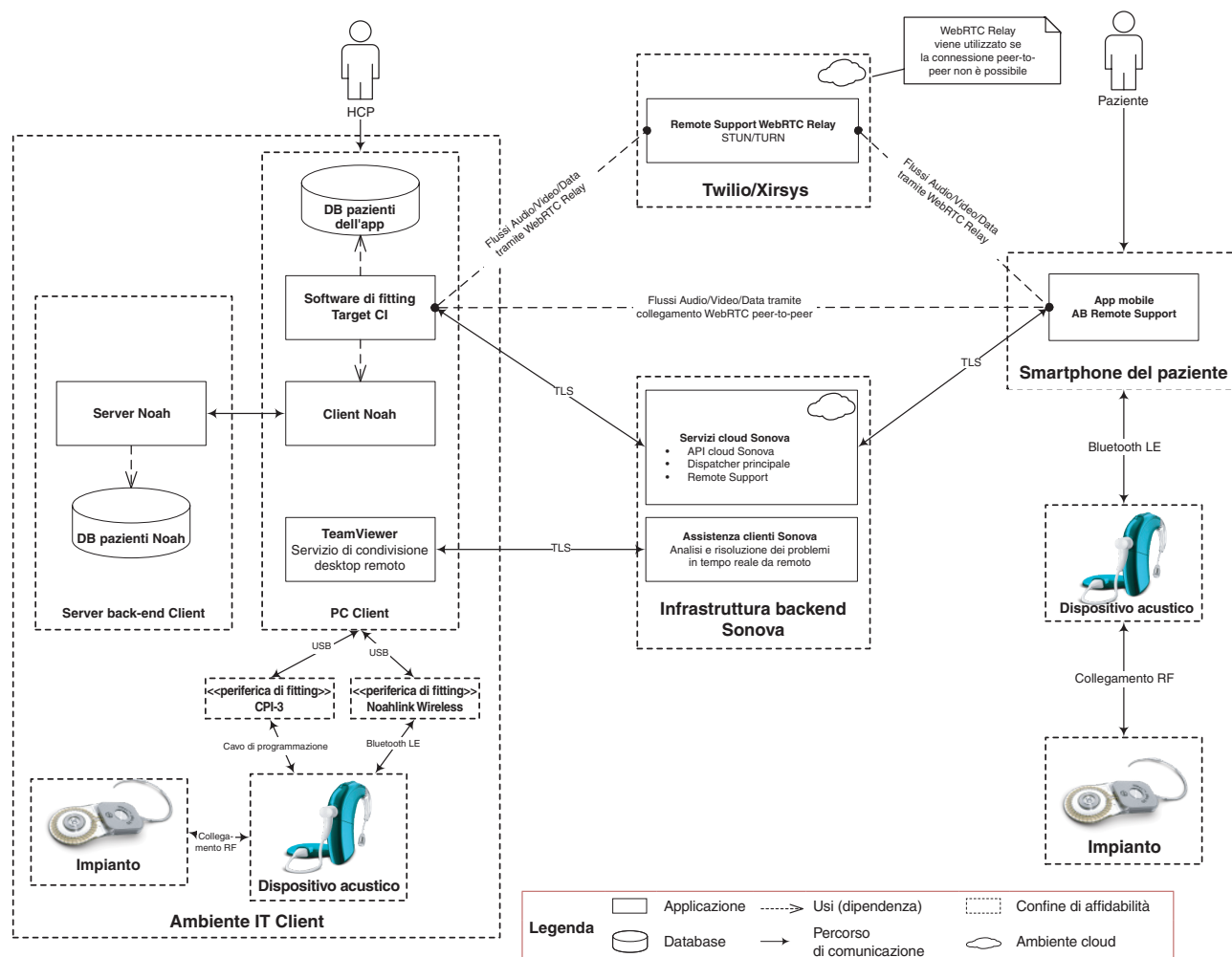
Il database transazionale PatientDatabase.sqlite memorizza i dati anagrafici e di fitting dei pazienti e verrà installato solo quando il software di fitting verrà distribuito in modalità autonoma.

Quando il software di fitting viene distribuito come modulo Noah, il sistema Noah fornisce al software di fitting i servizi di archiviazione dei dati del paziente richiesti. I restanti file sqlite sono parte integrante del software di fitting e necessari per tutti i modelli di distribuzione.



3.4 INTERCONNESSIONI DI SISTEMA

Il diagramma e la tabella sottostanti illustrano le principali interconnessioni del sistema. Solitamente viene utilizzata solo una parte delle interconnessioni disponibili.



Fonte / Destinazione	Servizio	Protocollo	Porta	Descrizione
Dispositivo acustico	Comunicazione tramite dispositivo acustico	Connessione con cavo / Bluetooth® Low Energy	N/D	Utilizzato per comunicare con i dispositivi acustici per finalità di controllo, configurazione, stato e lettura dei dati

Fonte / Destinazione	Servizio	Protocollo	Porta	Descrizione
Noah	API modulo Noah 4	.NET Remoting	N/D	Interfaccia primaria per il modulo utilizzata per accedere al software Noah (solo nel modello di distribuzione con Noah)
Servizi cloud Sonova	Sonova Cloud API, dispatcher principale, Remote Support	SOAP, REST	443	I servizi Sonova ospitati in un data center Microsoft Azure vengono utilizzati per: - recuperare i dati di configurazione del client del software di fitting dall'archiviazione back-end di Sonova - trasferire dati di registro e analisi - stabilire il fitting remoto in tempo reale
Twilio/Xirsys, AB Remote Support e AB Remote Support + app mobili	Remote Support	WebRTC	Reperibile nel documento di configurazione del firewall di Target CI	Utilizzato dalla funzione di supporto remoto per eseguire la segnalazione WebRTC e condurre sessioni di fitting remoto in tempo reale
Assistenza clienti AB	Condivisione del desktop	Protocollo proprietario di TeamViewer	5938, 443, 80 Fare riferimento a TeamViewerPorts	Utilizzato per eseguire analisi in tempo reale e la risoluzione dei problemi relativi alle installazioni del software di fitting. Per ulteriori informazioni, fare riferimento alla sezione 6.3 ACCESSO REMOTO .

4. REQUISITI DI SISTEMA

Sistema operativo	Windows 10,11, Pro/Enterprise
.NET Framework	Versione 4.8
CPU	Intel® Core™ i5 o equivalente con prestazioni uguali o migliori
RAM	4 GB o più
Spazio su disco rigido	3 GB o più
Requisiti minimi del display	• Risoluzione 1280 x 1024 (ridimensionamento massimo 125%) • Colore a 24 bit
Driver del dispositivo	• Driver Noahlink Wireless (se si utilizza l'interfaccia di programmazione Noahlink Wireless di terze parti collegata tramite USB, è richiesta la versione più recente disponibile da HIMSA). • Driver CPI-3 (necessario se si utilizza un'interfaccia di programmazione CPI-3 collegata tramite USB).
Database	SQLite oppure Noah System 4 (versione 4.16 o superiore)
Connessione Internet	Connessione Internet richiesta per il supporto remoto e il registro di analisi, vedere la sezione 3.4 Interconnessioni di sistema; intranet richiesta quando si utilizza Noah System 4 in rete.
Porte di rete	Vedere la sezione 3.4 Interconnessioni di sistema; vedere la sezione 2. Altre risorse — HIMSA per le porte utilizzate da Noah System 4.

5. SICUREZZA INFORMATICA NEL CICLO DI VITA DEL PRODOTTO

5.1 DISTRIBUZIONE

Metodi di distribuzione approvati:

1. Scaricare dal Sonova Web Client (SFTP) all'indirizzo <https://webclient.sonova.com> oppure dal portale AB Pro all'indirizzo <https://www.abproportal.com>
2. Installare da una chiavetta USB ufficiale di Advanced Bionics.

Prima dell'installazione, verificare la firma digitale del programma di installazione ed eseguire una scansione del file con un software antivirus aggiornato. Per istruzioni dettagliate sulla verifica dell'integrità, fare riferimento alla sezione 8. Durante la fase di distribuzione, applicare i controlli di sicurezza IT standard per il settore sanitario, tra cui la protezione degli endpoint e le restrizioni di rete.

Quando si utilizza una chiavetta USB:

- Utilizzare esclusivamente chiavette USB ufficiali fornite da Advanced Bionics.
- Conservare la chiavetta USB in un luogo sicuro e non modificarne il contenuto.
- Eseguire una scansione dell'unità USB e dell'ambiente di installazione con un antivirus aggiornato e con le whitelist delle applicazioni abilitate.
- Advanced Bionics declina ogni responsabilità per i dati non autorizzati memorizzati su chiavette USB contenenti il pacchetto di installazione.

5.2 INSTALLAZIONE

Per installare il software di fitting è necessario un account amministratore. Una volta installato, il software può essere eseguito senza autorizzazioni amministrative o di livello elevato.

Per informazioni sulla verifica dell'integrità del software prima dell'installazione, vedere la sezione 8, Integrità del software.

Prima dell'installazione, si consiglia agli amministratori del sistema di accertarsi che:

- la versione del software di fitting da installare sia l'ultima disponibile.
- il sistema operativo sottostante sia aggiornato.
- venga verificata l'integrità e l'autenticità dei dati del programma di installazione del software di fitting. Per informazioni sulla convalida dell'integrità del software prima dell'installazione, vedere la sezione 8

Per installare il software di fitting sono disponibili due programmi di installazione:

- Programma di installazione Standard
- Programma di installazione IT Professional

Il programma di installazione IT Professional è un singolo file MSI ed esclude i componenti prerequisiti, ma è altrimenti equivalente al programma di installazione Standard.

I componenti prerequisiti includono Microsoft .NET Framework v4.8 e i pacchetti ridistribuibili Microsoft Visual C++.

Entrambi i programmi di installazione supportano scenari di installazione avanzati, tra cui l'installazione silenziosa.

Il programma di installazione IT Professional deve essere utilizzato solo se la propria organizzazione richiede che i componenti prerequisiti siano installati e gestiti dalla propria organizzazione e non dal programma di installazione del software di fitting. In tutti gli altri casi si deve utilizzare il programma di installazione Standard.

È possibile ottenere il programma di installazione IT Professional da un rappresentante clinico AB. Il programma di installazione IT Professional non può essere utilizzato per riparare, reinstallare o disinstallare le installazioni eseguite dal programma di installazione Standard. Il programma di installazione Standard non può essere utilizzato per riparare, reinstallare o disinstallare le installazioni eseguite dal programma di installazione IT Professional.

Per scenari di installazione avanzati, seguire le istruzioni contenute nella Guida avanzata all'installazione del software di fitting (vedere la sezione 2.3). Per gli scenari di installazione standard, fare riferimento alla sezione 2.5 di questo documento, che include un collegamento alle Istruzioni per l'uso (IFU) del software di fitting.

5.3 CONFIGURAZIONE E FUNZIONAMENTO

Il software di fitting supporta una serie di controlli e funzionalità per la privacy e la sicurezza. Alcune funzionalità per la privacy e la sicurezza del software di fitting sono abilitate di default, altre sono configurabili al momento dell'installazione e dipendono dal modello di implementazione selezionato, mentre altre ancora sono configurabili durante il normale utilizzo tramite l'interfaccia grafica dell'applicazione.

Fare riferimento a:

- La sezione 6 elenca i controlli di sicurezza che migliorano la protezione del sistema dell'applicazione del software di fitting
- La sezione 7 elenca i controlli di sicurezza che migliorano la protezione dei dati elaborati dall'applicazione del software di fitting

Ulteriori controlli di privacy e sicurezza (non supportati dal software di fitting a livello di applicazione) dovranno essere abilitati e configurati dagli utenti (ad esempio, operatori sanitari, amministratori di sistema, personale IT) a livello di sistema operativo e/o a livello di infrastruttura IT. Fare riferimento alla sezione 11 del presente documento per un elenco delle migliori pratiche e dei controlli di sicurezza per l'ambiente di fitting in cui verrà utilizzato il software di fitting.

Firewall

Il software di fitting non è dotato di un firewall interno.

Nel caso in cui sia abilitato un firewall esterno (ad esempio a livello di sistema operativo), potrebbe essere necessario aggiornarne la configurazione per consentire il traffico in entrata e in uscita richiesto (ad esempio, flussi audio/video/dati WebRTC durante una sessione Remote Support). Consultare il documento di configurazione del firewall del software di fitting, che contiene l'elenco degli indirizzi di rete e delle porte utilizzate dal software stesso.

Impostazioni del proxy

Il software di fitting è dotato di un proxy locale. Tramite l'apposita interfaccia grafica del software di fitting è possibile modificare le impostazioni di tale proxy:

- Nessun proxy
- Rilevamento automatico delle impostazioni del proxy
- Configurazione manuale del proxy. Selezionando questa opzione, è possibile configurare le seguenti impostazioni:
 - Indirizzo
 - Porta
 - Abilitare/disabilitare l'autenticazione proxy (nome utente, password, dominio)

5.4 RIMOZIONE E DISMISSIONE

Per istruzioni dettagliate sulla disinstallazione del software di fitting, fare riferimento al documento IFU (Istruzioni per l'uso) del programma in questione.

Il programma di disinstallazione non rimuove le categorie di dati elencate nella tabella seguente. Salvo diversa indicazione nella colonna “Note” della tabella, tali dati devono essere rimossi manualmente dai sistemi dagli amministratori di sistema; ad esempio, eliminando manualmente i file o cancellando in modo sicuro il disco di sistema utilizzato per l'archiviazione dei dati.

Categoria dati	Posizione predefinita	Note
Dati dell'applicazione	C:\ProgramData\ Advanced Bionics\Target CI\Target CI	Include i seguenti tipi di dati: • Dati analitici • Dati di configurazione • Registri delle applicazioni • File temporanei
Dati personali	C:\ProgramData\ Advanced Bionics\Target CI\Target CI\Data	Database dei pazienti (rilevante solo per il modello di distribuzione autonomo)

Categoria dati	Posizione predefinita	Note
Strumento di accesso remoto	C:\Program Files (x86)\Common Files\Advanced Bionics\TeamViewer	Utilizzato per eseguire analisi in tempo reale e la risoluzione dei problemi relativi al software di fitting, compresi quelli che si verificano durante l'installazione e la disinstallazione. Per ulteriori informazioni, fare riferimento alla sezione 6.3.

Quando si disinstalla il software di fitting dal computer/portatile destinato alla dismissione o allo smaltimento, assicurarsi che tutti i dati sensibili (ad esempio, PHI, PII) vengano cancellati.

Per le distribuzioni di Noah, fare riferimento alle istruzioni dettagliate per lo smaltimento dei dati relative alle distribuzioni di Noah, reperibili al seguente indirizzo:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

I supporti esterni contenenti dati esportati dal software di fitting, inclusi report e registri, devono essere protetti. Quando non vengono più utilizzati, i dati devono essere cancellati in modo sicuro e/o il supporto deve essere cancellato o distrutto in modo sicuro.

È necessario utilizzare procedure e strumenti approvati per la rimozione sicura dei dati memorizzati su supporti rimovibili, in conformità alle normative e alle linee guida vigenti per la gestione di informazioni sui pazienti / informazioni di identificazione personale (PII) / informazioni sanitarie protette (PHI).

6. CONTROLLI DI SICUREZZA

Il software di fitting è un'applicazione client installata su un PC Microsoft Windows comunemente reperibile in commercio. Il software di fitting può essere installato come applicazione autonoma o come modulo Noah.

6.1 CONTROLLI DI ACCESSO

Il software di fitting non limita l'accesso alle sue funzionalità in base ai requisiti di login e ai ruoli dei singoli utenti. I controlli di accesso basati sui ruoli non sono supportati.

Accesso locale degli utenti

Quando il software di fitting viene installato come applicazione autonoma, dipende dai meccanismi di controllo degli accessi del sistema operativo ospitante. Il personale IT del cliente può configurare il sistema operativo ospitante per gestire l'autenticazione degli utenti e assegnare diritti o privilegi di accesso. Si raccomanda vivamente a ciascun utente di accedere con un account univoco e personale.

Ulteriori controlli compensativi sono descritti nella sezione 11 del presente documento e nella sezione Linee guida per la sicurezza informatica delle Istruzioni per l'uso.

Quando il software di fitting viene installato come modulo Noah, il controllo degli accessi viene gestito tramite Noah System 4.

Per maggiori dettagli sulle funzionalità di controllo accessi implementate da Noah System 4, consultare la documentazione disponibile sul sito www.HIMSA.com.

Accesso al servizio

I tecnici dell'assistenza in loco possono accedere al software di fitting tenendo conto dei controlli di accesso configurati dal personale IT del cliente per la gestione dell'autenticazione.

I tecnici dell'assistenza AB possono accedere al software di fitting utilizzando la funzione di condivisione del desktop supportata dal software stesso. Per informazioni dettagliate sui controlli di sicurezza abilitati per questa funzionalità, fare riferimento alla sezione 6.3.

6.2 REGISTRAZIONE DEGLI AUDIT E CONTROLLI DI RESPONSABILITÀ

Il software di fitting non genera registri di audit o report aggiuntivi rispetto a quelli forniti dal sistema operativo sottostante.

Modello di distribuzione autonomo

Quando il software di fitting viene installato come applicazione autonoma, si basa sui meccanismi di controllo forniti dal sistema operativo ospitante. Il software di fitting non dispone di alcuna funzione integrata di questo tipo. Il sistema operativo ospitante può essere configurato dal personale IT del cliente in modo da registrare determinati eventi, come gli avvii/le esecuzioni del software di fitting. Si consiglia a ciascun utente di accedere al sistema operativo ospitante con un account univoco per agevolare l'attività di audit.

Modello di distribuzione distribuito con Noah

Quando il software di fitting viene installato come modulo Noah, i registri di audit vengono gestiti da Noah System (Noah Activity Log). Per maggiori dettagli sui controlli degli audit disponibili in Noah System 4, consultare la documentazione disponibile all'indirizzo www.himsa.com

6.3 ACCESSO REMOTO

La funzionalità di condivisione del desktop consente di eseguire da remoto, in tempo reale, l'analisi e la risoluzione dei problemi relativi alle installazioni del software di fitting. Questa funzionalità si basa sullo strumento di terze parti TeamViewer QuickSupport (distribuito per impostazione predefinita insieme al software di fitting) e consente ai professionisti dell'assistenza clienti di AB di connettersi in remoto al computer dell'audioprotesista e di ottenerne il controllo completo, incluso l'accesso al sistema operativo e ai file system sottostanti.

Per stabilire una sessione di condivisione desktop è necessaria l'interazione dell'audioprotesista. L'audioprotesista dovrà innanzitutto eseguire lo strumento TeamViewer QuickSupport (ad esempio, tramite il software di fitting Target CI) e comunicare le proprie credenziali ID di TeamViewer al team di assistenza di AB tramite un canale di comunicazione fuori banda (ad esempio, una telefonata).

Il nome del collaboratore dell'assistenza di AB e il suo ID di TeamViewer vengono visualizzati per impostazione predefinita sul monitor del computer dell'audioprotesista durante ogni sessione attiva di condivisione desktop.

Tutto il traffico di rete di condivisione desktop è protetto utilizzando protocolli e algoritmi crittografici considerati sicuri secondo gli standard attuali (scambio di chiavi pubbliche/private RSA e crittografia di sessione AES a 256 bit).

Lo strumento di accesso remoto può essere rimosso manualmente senza compromettere le altre funzionalità del software di fitting Target. Il programma di installazione del software di fitting Target supporta un parametro di installazione da riga di comando per consentire un'installazione da riga di comando del software di fitting Target senza includere lo strumento di accesso remoto.

7. PROTEZIONE DELLE INFORMAZIONI

7.1 INFORMATIVA SULLA PRIVACY DI ADVANCED BIONICS

L'informativa sulla privacy che descrive come Advanced Bionics raccoglie, trasferisce, conserva e utilizza i dati personali può essere scaricata da: AdvancedBionics.com/privacy.

Advanced Bionics non ospita dati, non li conserva, non ne esegue il backup, né ha accesso ai dati memorizzati nel software di fitting o nei database Noah, a meno che i dati non vengano espressamente inviati ad Advanced Bionics.

7.2 STANDARD FEDERALI PER IL TRATTAMENTO DELLE INFORMAZIONI (FIPS)

Target CI v1.6 è conforme agli standard di crittografia FIPS 140-2.

7.3 PII/PHI TRATTATE DAL PRODOTTO

Il software di fitting elabora le informazioni personali e sanitarie del paziente.

Le informazioni sul paziente vengono inserite manualmente dall'utente del software di fitting oppure vengono ricevute dall'applicazione tramite uno o più dei suoi flussi di dati.

Nei flussi di dati principali del software di fitting vengono elaborati i seguenti tipi di informazioni:

	Servizi cloud Sonova (dispatcher principale, Remote Support)	Dispo- sitivo acustico	App mobili	DB pazienti (locale/ Noah)	Accesso remoto
Nome				X	X(2)
Indirizzo				X	X(2)
Data di nascita	X(1)		X	X	X(2)
Numero di telefono				X	X(2)
Indirizzo e-mail				X	X(2)
Numeri di cartella clinica				X	X(2)
Identificativi del dispositivo e numeri di serie	X(1)	X	X	X	X(2)
Indirizzo IP	X(1)				
Audiogrammi, RECD, REUG	X(1)	X	X	X	X(2)
Dati relativi al fitting		X	X	X	X(2)
Dati sull'utilizzo dei dispositivi acustici	X(1)	X	X	X	
Dati di utilizzo del software di fitting	X(1)				

(1) Pseudonimizzate prima dell'arrivo nel datalake di Sonova.

(2) Durante una sessione di condivisione del desktop in tempo reale, i tecnici dell'assistenza clienti di AB ottengono il pieno controllo del desktop dell'HCP, compreso l'accesso al sistema operativo e al file system sottostanti e ai dati in esso memorizzati. Per ulteriori informazioni, fare riferimento alla sezione 6.3.

Per informazioni più dettagliate sulla raccolta e il trattamento dei dati, contattare il proprio referente dell'assistenza locale.

7.4 SICUREZZA DURANTE IL TRASFERIMENTO

La sicurezza delle comunicazioni è garantita e abilitata in tutte le comunicazioni di rete in entrata e in uscita del software di fitting. Ad eccezione della funzione di Remote Support (che utilizza il protocollo WebRTC) e della comunicazione Bluetooth con i dispositivi acustici e gli accessori, tutte le altre connessioni sono protette dal protocollo Transport Layer Security (TLS) che garantisce riservatezza, integrità e autenticità.

TLS

La configurazione TLS è conforme alle attuali migliori pratiche e alle raccomandazioni di sicurezza documentate in BCP 195 – Raccomandazioni per l'uso sicuro di TLS e DTLS [8], tra cui:

- Nessun supporto alle versioni SSL e TLS precedenti alla 1.2
- Nessun supporto alle suite di cifratura che utilizzano algoritmi crittografici che offrono meno di 128 bit di sicurezza
- Supporto alle estensioni TLS consigliate di BCP 195
- Nessun supporto alle estensioni non sicure di BCP 195

DTLS

La crittografia è una funzionalità obbligatoria di WebRTC e viene applicata a tutti i flussi multimediali inviati tramite WebRTC. Il protocollo di crittografia utilizzato dipende dal tipo di canale; i flussi di dati vengono crittografati tramite DTLS 1.2, mentre i flussi multimediali vengono crittografati tramite Secure Real-time Transport Protocol (SRTP), utilizzato perché è un'opzione più leggera rispetto a DTLS.

Per informazioni più dettagliate sulla configurazione di sicurezza di Remote Support WebRTC, fare riferimento al seguente collegamento:

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

BLE

La comunicazione wireless Bluetooth Low Energy con dispositivi acustici e accessori è crittografata e protetta per impostazione predefinita (ad eccezione dei casi di utilizzo per l'identificazione e il rilevamento). Oltre a ciò, la durata della modalità di accoppiamento Bluetooth del dispositivo acustico è limitata nel tempo. Per una descrizione più dettagliata sulla sicurezza del canale di comunicazione Bluetooth, fare riferimento alla documentazione disponibile sul dispositivo acustico.

7.5 SICUREZZA A RIPOSO

Dati dell'applicazione

I dati dell'applicazione risiedono sullo stesso computer, nella directory predefinita:
C:\ProgramData\Advanced Bionics\Target CI\Target CI

Il diritto di accesso viene ereditato dalla cartella principale ed è limitato agli utenti connessi al sistema locale (gruppo utenti INTERACTIVE integrato¹) durante l'installazione del software.

Gli utenti autorizzati dispongono di diritti di lettura e scrittura sulla directory.

¹ <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-special-identities-groups#interactive>

Per ridurre il rischio di accesso non autorizzato ai dati dell'applicazione tramite la rete, assicurarsi che nessuna delle cartelle o dei file contenenti i dati sia condiviso in rete. Le posizioni predefinite dei dati dell'applicazione sono elencate nella sezione 5.4.

Database dei pazienti – Modello di distribuzione autonomo

Quando il software di fitting viene installato come applicazione autonoma, il database dei pazienti risiede sullo stesso computer e i record di dati dei pazienti non vengono crittografati a riposo. Le PII non vengono trasmesse tramite la rete dall'applicazione.

Qualsiasi utente in grado di accedere al computer con il software di fitting installato avrà pieno accesso a tutti i dati dell'applicazione, compreso il database dei pazienti. Si prega di consultare la sezione Protezione dati per indicazioni sulle misure di protezione dei dati raccomandate.

In alcune giurisdizioni, le normative potrebbero richiedere la crittografia di tutti i dati dei pazienti per evitare potenziali responsabilità in caso di perdita o furto dei dati. Abilitare BitLocker o una crittografia completa del disco equivalente (a livello di sistema operativo o basata su hardware) per proteggere i dati da accessi o copie non autorizzati mentre sono a riposo.

BitLocker è una funzionalità integrata di Windows che crittografa l'intera unità e richiede l'autenticazione per l'accesso. Prima di abilitare BitLocker, consultare sempre le linee guida ufficiali di Microsoft e i criteri di sicurezza IT della propria organizzazione.

Come abilitare BitLocker

Per gestire BitLocker sono necessari privilegi di amministratore.

1. Cercare “Gestisci BitLocker”
Aprire il menu Avvio, digitare “Gestisci BitLocker” e selezionarlo dai risultati della ricerca.
2. Selezionare l'unità di sistema
Selezionare l'unità in cui è installato Windows per configurare le impostazioni di crittografia.
3. Scegliere un metodo di sblocco
Selezionare una delle seguenti opzioni:
 - Solo TPM
 - TPM + PIN
 - TPM + chiave USBQuando si seleziona il metodo di sblocco, seguire le indicazioni sulle migliori pratiche di Microsoft e i criteri di sicurezza IT della propria organizzazione.
4. Eseguire il backup della chiave di ripristino
Eseguire il backup della chiave di ripristino utilizzando metodi sicuri e approvati dall'azienda. Le opzioni consigliate includono:
 - Archiviazione in Microsoft Entra ID (in precedenza Azure AD) o Active Directory per i dispositivi aggiunti al dominio

- Salvataggio in una posizione di rete sicura e con accesso controllato, crittografia e registrazione degli audit
- Utilizzo di una soluzione di key escrow gestita e approvata dalla propria organizzazione

Evitare di salvare la chiave su unità locali, USB o di stamparla, a meno che non sia esplicitamente consentito dalla policy. Le chiavi di ripristino devono essere protette con lo stesso rigore delle altre credenziali sensibili e sostituite immediatamente se divulgate.

5. Avviare la crittografia

Scegliere:

- Unità intera: consigliato per la maggior parte degli scenari aziendali. Vengono crittografati tutti i settori, incluso lo spazio non utilizzato, per impedire la persistenza dei dati.

Database dei pazienti – Modulo di distribuzione con Noah

Quando il software di fitting viene installato come modulo Noah, le PII vengono memorizzate nel database pazienti ospitato da Noah. Il database dei pazienti ospitato da Noah potrebbe risiedere su un altro computer. Le PII e gli altri dati dei pazienti vengono gestiti dal software Noah e la crittografia dei dati a riposo dei pazienti è garantita da Noah System. Il software di fitting può trasmettere/ricevere PII tramite una connessione di rete cablata o wireless quando un database Noah è configurato per l'accesso alla rete.

Le PII memorizzate nel database Noah in rete saranno accessibili agli altri utenti su altri PC che dispongono delle autorizzazioni per lo stesso database in rete. Il database Noah può anche essere configurato per l'accesso non in rete e installato sullo stesso PC del software di fitting.

Noah impedisce al software di fitting di accedere al database delle cartelle cliniche dei pazienti. Quando un utente apre la scheda di un paziente nel software di fitting tramite il client Noah, il software di fitting è in grado solo di leggere e scrivere sulla cartella clinica del paziente attualmente aperta e non è in grado di accedere ad altre cartelle cliniche di pazienti nel database Noah.

Per ulteriori informazioni sugli standard di crittografia utilizzati da Noah System, consultare il seguente link:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/patient-database-encryption/>

File di esportazione RMA

Il software di fitting consente di esportare le informazioni dei clienti in un file. Il file RMA può essere inviato ad Advanced Bionics per risolvere l'RMA o problemi di supporto correlati.

Il file RMA è crittografato in modo asimmetrico con RSA utilizzando una chiave di 2048 bit. Il software di fitting non dispone di alcuna funzionalità per decifrare un file RMA.

File di esportazione resi anonimi

Il software di fitting consente di esportare le informazioni dei clienti in un file reso anonimo. Le informazioni personali identificabili del cliente, come la data di nascita e il nome, vengono sostituite con valori generici. Il file non è crittografato e può essere importato nella stessa istanza o in un'istanza diversa del software di fitting.

File di esportazione standard

Il software di fitting consente di esportare le informazioni dei clienti in un file di esportazione standard. Il file utilizza un formato binario proprietario e non è crittografato. Il file può essere importato nella stessa istanza o in un'istanza diversa del software di fitting. Quando si utilizza questa funzionalità, gli utenti del software di fitting devono assicurarsi che i file di esportazione standard vengano gestiti in base alle proprie politiche IT locali per la gestione delle PII non crittografate.

Dispositivo acustico

Il software di fitting memorizza le informazioni del cliente sul suo dispositivo acustico. Le informazioni personali identificabili, come il nome e la data di nascita del cliente, non vengono memorizzate sul dispositivo acustico. Le altre informazioni che non fanno parte delle PII vengono memorizzate utilizzando la crittografia PBKDF2 con una chiave a 128 bit.

Il software di fitting può trasmettere/ricevere informazioni del cliente che non fanno parte delle PII verso/da un apparecchio acustico tramite un dispositivo cablato proprietario (ad esempio, CPI-3), AB Remote Support e AB Remote Support + app mobili o il dispositivo Noahlink Wireless. Il dispositivo Noahlink Wireless si connette al dispositivo acustico utilizzando la tecnologia Bluetooth Low Energy (BLE) tramite un canale standard BLE crittografato con AES a 128 bit.

8. INTEGRITÀ DEL SOFTWARE

8.1 VERIFICA DEL SUPPORTO DI INSTALLAZIONE SCARICATO

In alcune regioni geografiche, il supporto di installazione del software di fitting Target CI può essere scaricato dal Pro Portal di Advanced Bionics o dal Sonova Web Client. Il supporto di installazione scaricato può essere autenticato utilizzando qualsiasi strumento di hashing SHA-256 attendibile.

L'hash SHA256 per il file zip di installazione standard è:

A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

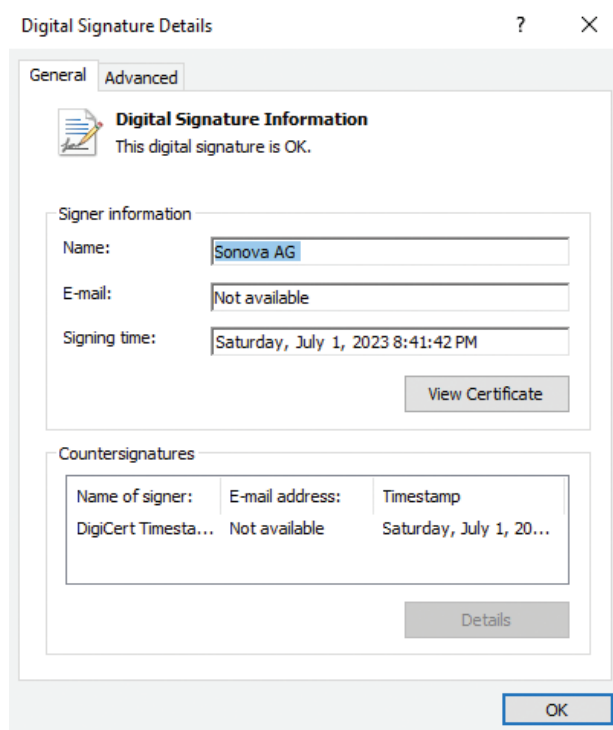
L'hash SHA256 per il file zip di installazione di IT Professional è:

DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 VERIFICA MANUALE DEL SOFTWARE DI FITTING PRIMA DELL'INSTALLAZIONE

Gli utenti possono eseguire i seguenti passaggi per verificare l'integrità e l'autenticità del software di fitting prima dell'installazione:

1. Aprire Esplora file su Windows e andare alla cartella principale del supporto di installazione del software di fitting. Se il supporto di installazione è una chiavetta USB, inserirla in una porta USB e andare alla sua cartella principale. Se il supporto di installazione è un file zip, decomprimerlo e salvarlo in una cartella, quindi aprirla.
2. Fare clic con il pulsante destro del mouse su SonovaVerify.exe e selezionare "Properties" (Proprietà) dal menu contestuale.
3. Selezionare la scheda "Digital Signatures" (Firme digitali).
4. Fare doppio clic sulla firma SHA256 "Sonova AG".
5. Verificare che gli elementi della firma siano validi. In particolare, verificare che in alto appaia il messaggio "The digital signature is OK." (La firma digitale è corretta.) e che il nome del firmatario e l'ora della firma corrispondano all'immagine seguente:



6. Fare clic sul pulsante “View Certificate” (“Visualizza certificato”) e sulla scheda “Details” (“Dettagli”) e verificare che il valore del campo “Thumbprint” (“Impronta digitale”) corrisponda a questa stringa:
db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Chiudere le finestre di dialogo popup e fare doppio clic su SonovaVerify.exe
8. Verificare che venga visualizzato “NO ERRORS DETECTED” (NESSUN ERRORE RILEVATO) come mostrato nell'immagine seguente:

```

SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

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

```

L'output “NO ERRORS DETECTED” (“NESSUN ERRORE RILEVATO”) corrisponde a una verifica di integrità e autenticità del contenuto del supporto di installazione del software di fitting, eseguita con successo. Ciò significa che SonovaVerify.exe ha autenticato e verificato l'integrità di tutti i file e le cartelle. In questo modo si verifica che i contenuti del software di fitting non siano stati manomessi, danneggiati o altrimenti compromessi.

SonovaVerify.exe visualizzerà avvisi o messaggi di errore se mancano file o cartelle oppure se al supporto di installazione sono stati aggiunti file o cartelle inaspettati. Qualora vengano visualizzati messaggi di avviso o di errore, la verifica dell'integrità e dell'autenticità del contenuto del supporto di installazione del software di fitting risulta non riuscita e si consiglia di:

- non procedere con l'installazione
- non aprire né eseguire alcun file contenuto nell'immagine di installazione del software per il fitting; segnalare il problema all'assistenza di Advanced Bionics (fare riferimento alla sezione 2.1)

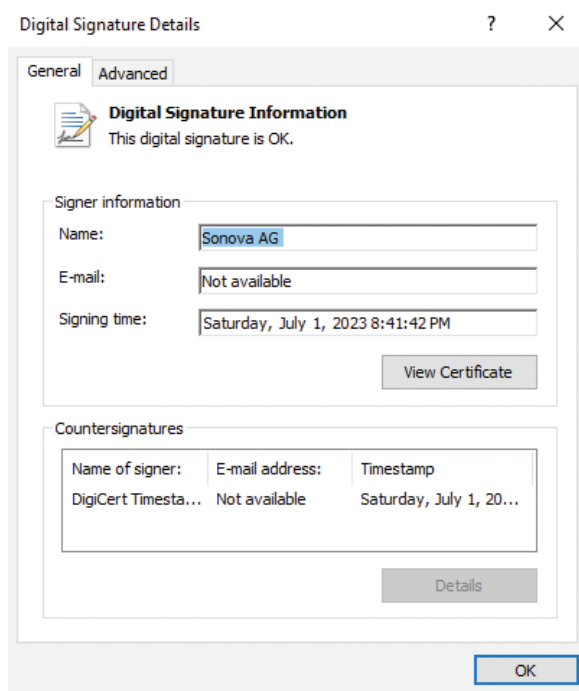
8.3 VERIFICA AUTOMATICA DELL'INTEGRITÀ DEL SOFTWARE DI FITTING INSTALLATO

SonovaVerify è integrato con il software di fitting e viene eseguito ogni volta che l'applicazione viene avviata per verificare l'integrità dei file di programma del software di fitting. I file di programma sono firmati digitalmente utilizzando le pratiche standard del settore e certificati rilasciati da un'autorità di certificazione attendibile. Il software avvisa l'utente tramite messaggi di avviso se uno qualsiasi dei file di programma risulta compromesso.

8.4 VERIFICA MANUALE DELL'INTEGRITÀ DEL SOFTWARE DI FITTING INSTALLATO

Gli utenti possono eseguire i seguenti passaggi per verificare l'integrità e l'autenticità del software di fitting installato in qualsiasi momento, senza che questo venga avviato:

1. Aprire Esplora file su Windows e andare alla cartella dell'eseguibile del software di fitting, solitamente situata in: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Fare clic con il pulsante destro del mouse su SonovaVerify.exe e selezionare "Properties" (Proprietà) dal menu contestuale.
3. Selezionare la scheda "Digital Signatures" (Firme digitali).
4. Fare doppio clic sulla firma SHA256 "Sonova AG".
5. Verificare che gli elementi della firma siano validi, in particolare che in alto appaia il messaggio "The digital signature is OK." (La firma digitale è corretta.) e che il nome del firmatario e l'ora della firma corrispondano all'immagine seguente:



6. Fare clic sul pulsante “View Certificate” (“Visualizza certificato”) e sulla scheda “Details” (“Dettagli”) e verificare che il valore del campo “Thumbprint” (“Impronta digitale”) corrisponda a questa stringa:
db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Chiudere le finestre di dialogo popup e fare doppio clic su SonovaVerify.exe
8. Verificare che venga visualizzato “NO ERRORS DETECTED” (NESSUN ERRORE RILEVATO) come mostrato nell'immagine seguente:

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

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

L'output “NO ERRORS DETECTED” (“NESSUN ERRORE RILEVATO”) corrisponde a una verifica di integrità e autenticità del contenuto del supporto di installazione del software di fitting, eseguita con successo. Ciò significa che SonovaVerify.exe ha autenticato e verificato l'integrità di tutti i file e le cartelle. In questo modo si verifica che i contenuti del software di fitting non siano stati manomessi, danneggiati o altrimenti compromessi.

SonovaVerify.exe visualizzerà avvisi o messaggi di errore se mancano file o cartelle oppure se al supporto di installazione sono stati aggiunti file o cartelle inaspettati. Qualora vengano visualizzati messaggi di avviso o di errore, la verifica dell'integrità e dell'autenticità del contenuto del supporto di installazione del software di fitting risulta non riuscita e si consiglia di:

- non procedere con l'installazione
- non aprire né eseguire alcun file contenuto nell'immagine di installazione del software per il fitting; segnalare il problema all'assistenza di Advanced Bionics (fare riferimento alla sezione 2.1)

9. PATCH E AGGIORNAMENTI DEL SOFTWARE

Gli aggiornamenti automatici non sono supportati. Per ulteriori informazioni, fare riferimento alla sezione 12.

10. GESTIONE DEI DATI

10.1 DATABASE

Il software di fitting utilizza un database transazionale per l'archiviazione dei dati dei pazienti e un set di database informativi che forniscono le configurazioni dei metadati richieste dall'applicazione.

Vedere la Sezione 3. Diagrammi di contesto e rete - Artefatti di distribuzione per un elenco dettagliato di tutti i database distribuiti dal software di fitting.

Quando il software di fitting viene installato come applicazione standalone, il database dei pazienti è interno al software di fitting. Il database dei pazienti, memorizzato nel file PatientDatabase.sqlite, risiede sullo stesso computer del software di fitting e fornisce l'archiviazione dei dati dei pazienti. Per eseguire il backup dei dati dell'applicazione quando Target CI viene distribuito come applicazione autonoma, creare una copia di backup dell'intera cartella situata in %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Proteggere i backup dei dati non solo dalla perdita, ma anche dal furto. Quando il software di fitting viene installato come modulo Noah, i dati dei pazienti vengono memorizzati nel database fornito da Noah System. Il database Noah può essere configurato per l'accesso in rete. Il database Noah può anche essere configurato per l'accesso non in rete e installato sullo stesso PC del software di fitting. Configurare la crittografia del database Noah per proteggere i dati (fare riferimento alla documentazione HIMSA).

Per la modalità di distribuzione distribuita di Noah, fare riferimento al seguente collegamento per istruzioni sul backup e sul ripristino del database dei pazienti di Noah:

<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 MIGRAZIONE DEI DATI

Il software di fitting consente agli utenti di migrare le cartelle cliniche dei pazienti dal precedente software di fitting di AB, SoundWave 3.2. Per poter effettuare la migrazione, le cartelle cliniche dei pazienti devono essere accessibili da un'installazione SoundWave 3.2 sullo stesso computer di Target CI.

10.3 CONFIGURAZIONI DEL DISPOSITIVO ACUSTICO

Il software di fitting consente di esportare e importare le configurazioni e le impostazioni del dispositivo.

10.4 SMALTIMENTO DEI DATI

Per indicazioni sullo smaltimento dei dati, fare riferimento alla sezione 5.4, Rimozione e dismissione, del presente documento e alla sezione Smaltimento e materiali pericolosi delle Istruzioni per l'uso. Per le distribuzioni di Noah, le istruzioni dettagliate per l'eliminazione delle cartelle cliniche dei pazienti sono disponibili al seguente indirizzo: <https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

11. AMBIENTE DI SICUREZZA – RESPONSABILITÀ CONDIVISA

Il software di fitting è stato progettato per un utilizzo previsto in cui la gestione del rischio di sicurezza informatica è considerata una responsabilità condivisa tra le parti interessate nell'intero ecosistema dell'assistenza uditiva. Tra queste vi sono, a titolo esemplificativo ma non esaustivo, utenti di dispositivi acustici, genitori o tutori legali di bambini che utilizzano dispositivi acustici, operatori sanitari, amministratori IT, strutture e fornitori di assistenza uditiva, venditori di dispositivi acustici e apparecchiature di programmazione.

Di seguito è riportato un elenco delle migliori pratiche comuni e dei controlli di sicurezza per l'ambiente di fitting in cui verrà utilizzato il software di fitting:

Livello sistema operativo

- Applicare controlli di accesso a livello di sistema operativo, ad esempio:
 - eliminare gli account guest
 - attivare l'accesso utente di Windows
 - mantenere un elenco degli operatori autorizzati, per controllare l'accesso al sistema
 - impostare utenti e ruoli personalizzati
 - applicare requisiti di password complesse e mantenere segrete le credenziali
 - abilitare il timeout di inattività della sessione
- applicare controlli di audit a livello di sistema operativo
- assicurarsi che il sistema operativo sia aggiornato
- assicurarsi che la versione del software di fitting installato sia aggiornata
- utilizzare una protezione antivirus e antimalware adeguata e aggiornata
- assicurarsi di disattivare le funzioni AutoRun e AutoPlay
- abilitare l'inserimento delle applicazioni nella whitelist

Protezione dati

- Assicurarsi che nessuna cartella e nessun file contenente i dati dell'applicazione sia condiviso in rete. Le posizioni predefinite dei dati dell'applicazione sono elencate nella tabella della sezione 5.4. Per verificare la presenza di condivisioni di rete esposte da un computer, accedere a “Gestione computer -> Cartelle condivise -> Condivisioni” nello strumento Gestione computer di Microsoft oppure eseguire il comando PowerShell `Get-WmiObject -class Win32_Share`.
- Durante l'installazione, le autorizzazioni sulla cartella dei dati dell'applicazione vengono impostate secondo quanto descritto nella sezione 6.1. Le cartelle dei dati dell'applicazione ereditano le autorizzazioni di accesso dalla cartella principale. La gestione dei permessi sulla cartella principale è responsabilità dell'operatore del software.
- Crittografare i dati dei pazienti utilizzando strumenti o controlli di terze parti a livello di sistema operativo utilizzando la crittografia dell'unità (ad esempio, il software gratuito Microsoft BitLocker) per proteggere tutti i dati. Per le distribuzioni con Noah, prendere in considerazione l'uso della crittografia del database Noah.
- I supporti esterni contenenti dati esportati dal software di fitting, inclusi report e registri, devono essere protetti. Quando non vengono più utilizzati, i dati devono essere cancellati in modo sicuro e/o il supporto deve essere eliminato in modo sicuro.
- Utilizzare supporti di archiviazione USB con funzionalità di sicurezza integrate, come unità USB crittografate con tastiera integrata.
- Garantire sempre la sicurezza dei dati seguendo queste pratiche:
 - Quando si trasmettono dati su canali non protetti, è necessario anonimizzare o crittografare i dati.
 - Proteggere i backup dei dati non solo dalla perdita, ma anche dal furto.
 - Rimuovere dal supporto dati tutti i dati che non vengono più utilizzati o che devono essere smaltiti.
- Gli utenti devono applicare procedure e strumenti approvati per la rimozione sicura dei dati memorizzati su supporti rimovibili, in conformità alle normative e alle linee guida vigenti per la gestione di informazioni sui pazienti / informazioni di identificazione personale (PII) / informazioni sanitarie protette (PHI)

Infrastruttura IT

Utilizzare il software di fitting in un ambiente di rete sicuro, protetto da intrusioni non autorizzate. Esistono numerose tecniche efficaci per isolare e proteggere i sistemi informatici medici, tra cui l'implementazione di firewall di protezione, zone demilitarizzate (DMZ), reti locali virtuali (VLAN) ed enclavi di rete. Mantenere una connessione di rete attiva per ricevere gli aggiornamenti del sistema operativo.

Livello fisico

- La postazione di lavoro in cui è installato il software di fitting deve essere fisicamente protetta in modo tale da non essere accessibile a personale non autorizzato né da poter essere manomessa da quest'ultimo.
- L'accesso alle stampanti collegate alla postazione di lavoro deve essere controllato.
- Il monitor della postazione di lavoro in cui è installato il software di fitting deve essere posizionato in modo da garantire la visibilità del contenuto della schermata solo all'utente.

Livello organizzativo

- Solo il personale professionalmente formato e pienamente qualificato è autorizzato a utilizzare il sistema. Prima di autorizzare chiunque a utilizzare il sistema, è necessario verificare che la persona abbia letto e compreso appieno le istruzioni operative fornite con il software di fitting.
- Solo il personale autorizzato alla manutenzione e al funzionamento del software di fitting deve essere dotato di un account per il computer su cui è installato il software. Gli account del computer e del dominio, nonché i relativi diritti di accesso, devono essere periodicamente rivisti e disattivati qualora l'accesso al computer non sia più richiesto.
- Se si notano attività sospette sui propri account del software di fitting oppure operazioni inaspettate, contattare Advanced Bionics. Per ulteriori informazioni, fare riferimento alla sezione 2.1.

Per maggiori informazioni sulla responsabilità condivisa e per un elenco più dettagliato delle raccomandazioni sulle migliori pratiche e sui controlli di sicurezza per l'ambiente di fitting in cui verrà utilizzato il software di fitting da applicare a vari livelli, fare riferimento a:

- documento informativo EHIMA “Best Practices for Secure Fitting of Hearing Devices”, [EHIMAWhitePaper](#)

12. PRODUZIONE, SVILUPPO SOFTWARE E GESTIONE DELLA SICUREZZA

La sicurezza informatica viene presa in considerazione durante l'intero processo di sviluppo del software. Il software di fitting è sviluppato in conformità agli standard IEC 62304 e IEC 82304.

Durante il processo di produzione, il software di fitting viene sottoposto a scansione per rilevare virus e malware.

Le vulnerabilità nei componenti di terze parti elencate nel National Vulnerability Database (NVD) del NIST vengono valutate e mitigate durante il processo di sviluppo e monitorate una volta che il software di fitting è stato rilasciato sul mercato.

Gestione della configurazione

AB sviluppa internamente, documenta e mantiene sotto controllo di configurazione la configurazione di riferimento di ogni versione rilasciata del software di fitting.

Tutti i componenti software di terze parti utilizzati dall'applicazione software di fitting sono identificati e documentati nella distinta base del software (SBOM). SBOM viene utilizzato da AB nella gestione del rischio di sicurezza informatica per valutare e monitorare l'esposizione alle minacce informatiche e alle vulnerabilità divulgate, avvalendosi di strumenti di scansione delle vulnerabilità aggiornati.

Aggiornamenti di sicurezza

AB monitora costantemente le vulnerabilità di sicurezza che interessano il software di fitting. Ciò include vulnerabilità nel software di fitting e nei componenti di terze parti utilizzati dall'applicazione del software di fitting.

Le vulnerabilità annunciate vengono valutate in base alla configurazione e all'utilizzo del software di fitting.

Se necessario, le vulnerabilità di sicurezza possono essere corrette mediante una versione del software di fitting più ampia che implementi patch per specifici componenti software all'interno del pacchetto software.

Divulgazione delle vulnerabilità

Ci impegniamo a divulgare le vulnerabilità e a migliorare la sicurezza dei nostri prodotti e servizi.

Si incoraggia la segnalazione di presunte vulnerabilità o problemi di sicurezza relativi ai nostri prodotti o al software/all'infrastruttura sottostante.

Si prega di leggere la nostra politica sulla divulgazione delle vulnerabilità pubblicata all'indirizzo <https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy> e di seguire le istruzioni per inviare una segnalazione.

13. COMPONENTI SOFTWARE E LISTA DEI MATERIALI

Il software di fitting incorpora alcuni componenti software commerciali già pronti all'uso.

La tabella seguente elenca tutti i SOUP (Software di provenienza sconosciuta) distribuiti con il software di fitting.

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
AForge.NET	Libreria matematica e multimediale AForge.NET, parte integrante e necessaria di IceLink e LiveSwitch.	AForge.NET	2.2.5.0
Amplifon. Programmer	Componente della suite software di Amplifon	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Componente della suite software di Amplifon	Amplifon	1.0.4.0
AutoMapper	Automatizza la mappatura da oggetto a oggetto	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	Libreria per il benchmarking, che fornisce strumenti per misurare e confrontare le prestazioni del codice	BenchmarkDotNet Community	0.13.0.0
Castle.Core	Una libreria fondamentale del progetto Castle, che offre componenti come la generazione dinamica di proxy e contenitori di inversione del controllo per le applicazioni .NET.	Castle Project	4.4.1
Chessie	Una libreria funzionale per la gestione degli errori in F#	Open Source	0.6.0.0
ciAD Hearingloss Simulator	Libreria di simulatori della perdita dell'udito per lettore multimediale	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Semplifica la lettura, la manipolazione e la scrittura di file Excel senza richiedere l'installazione di Excel	ClosedXML Community	0.95.4.0
CommandLine Parser	Fornisce un'API pulita e concisa per il parsing degli argomenti della riga di comando	CommandLineParser Community	2.4.3
Common.Logging	Un'astrazione di logging portatile per applicazioni .NET	Common.Logging Community	3.4.1.0

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
CommonService Locator	Fornisce un'interfaccia comune per la localizzazione dei servizi, consentendo alle applicazioni di svincolarsi da specifici contenitori IoC.	Microsoft	2.0.5.0
Credential Management	Il pacchetto Credential Management è un wrapper per l'API di gestione delle credenziali di Windows	iLya Lozovyy	1.0.2
CSharpAnalytics	Utilizzato per Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78.45418
Deconstructurama. Attributed	Utilizzato dalle librerie Nephele.	Contributori Serilog	3.1.0.0
Developer Express Suite	Una suite completa di controlli e librerie per l'interfaccia utente, pensata per gli sviluppatori .NET, che offre strumenti per la creazione di applicazioni ricche di funzionalità.	Developer Express Inc	20.2.10.0
DirectShow 2005	Consente l'accesso alle funzionalità DirectShow di Microsoft dall'interno delle applicazioni .NET.	Microsoft	2.0
DSL4	Fitting formula library DSL 4	National Centre for Audiology, Canada	4.2
DSL5	Fitting formula library DSL 5	National Centre for Audiology, Canada	5.0.34
ExcelNumberFormat	Fornisce funzionalità per l'analisi e la formattazione dei formati numerici di Excel	Open Source	1.1.0.0
FM.dll	Parte integrante dei loro framework di comunicazione in tempo reale come LiveSwitch e IceLink	FM (Frozen Mountain)	2.9.32
FSharp.Core	La libreria principale per il linguaggio di programmazione F#	Microsoft	6.0.322.10402
FTDI Chip	Un pacchetto di driver di Future Technology Devices International (FTDI) che facilita la comunicazione tra dispositivi USB e applicazioni software.	FTDI	3.02.07
GNOtometrics. Aurical	GNOtometrics.Aurical ridistribuito per Sonova	Natus Medical Incorporated	2.0.1.9

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
SharedUtilities.dll	Fornisce funzioni di utilità comuni e risorse condivise tra le applicazioni Natus.	Natus Medical Incorporated	1.0.0.0
Hardware.Info	Un componente che raccoglie e fornisce informazioni dettagliate sulla configurazione hardware di un sistema	Open Source	11.1.0.1
Himsa.NLWSMAPI.dll	Una libreria associata al software Noah di HIMSA	HIMSA	2.0.3.0
natus.otometrics.hipro2	Librerie di comunicazione HiPro	Natus Medical Incorporated	2.0.0.4
Iced.dll	Facilita le comunicazioni in tempo reale consentendo lo streaming di audio, video e dati	FM (Frozen Mountain)	1.12.0.0
IceLink	Utilizzato per l'integrazione della conferenza audio/video WebRTC	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	Offre supporto Unicode e per la globalizzazione delle applicazioni software	FM (Frozen Mountain)	54.1.0.0
IdentityModel	Libreria client OpenID Connect e OAuth 2.0 utilizzata dal componente Kona.CommonServices.Authentication per l'autenticazione OAuth 2.	Dominick Baier, Brock Allen	6.2.0.0
IMCInterfaces	Libreria di interfaccia di comunicazione inter-modulo Noah	HIMSA II K/S	4.4.0.2266
iText 7	Libreria PDF per creare, modificare e ispezionare documenti PDF a livello di programmazione.	iText Software	7.1.16.0
JetBrains.dotMemory	Uno strumento di profilazione della memoria per rilevare perdite di memoria e ottimizzare l'utilizzo della memoria nelle applicazioni .NET	JetBrains	111.0.0.0
JsonDiffPatch DotNet.dll	Fornisce funzionalità per confrontare e modificare oggetti JSON	Open Source	1.0.1.0
LibGit2Sharp	Utilizzato dalle librerie provenienti da Sonova per comunicare con Git	Contributori LibGit2Sharp	0.26.1.93

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
LiveSwitch	Utilizzato per l'integrazione della conferenza audio/video WebRTC.	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	Framework di logging per .NET	Apache	4.7.0.3189
Mapster	Utilizzato per mappare gli oggetti nel codice	chaowlert,eric_swann	7.2.0.0
Mapster.Core	Utilizzato per mappare gli oggetti nel codice	chaowlert,eric_swann	1.2.0.0
MathNet.Numerics	Utilizzato per algoritmi di fitting (percorso del segnale, target matcher ecc.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael e contributori	4.11.0
Microsoft.Bcl.AsyncInterfaces	Fornisce le interfacce <code>IAsyncEnumerable<T></code> e <code>IAsyncDisposable</code> e tipi di supporto per .NET Standard 2.0.	Microsoft	6.0.21.52210
Microsoft.CodeAnalysis.Common	Utilizzato dalle librerie provenienti da Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft.CodeAnalysis.CSharp	Utilizzato dalle librerie provenienti da Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Fornisce funzionalità di compilazione e generazione di codice utilizzando C#	Microsoft	4.700.19.56404
Microsoft.Diagnostics.FastSerialization.dll	Utilizzato per la serializzazione e deserializzazione efficiente dei dati diagnostici	Microsoft	1.0.0.0
Microsoft.Diagnostics.NETCore.Client.dll	Una libreria gestita che consente l'interazione con il runtime .NET Core per varie attività diagnostiche, come la tracciatura e la richiesta di dump.	Microsoft	0.2.4.27602
Microsoft.Diagnostics.Runtime.dll	Fornisce API per l'ispezione dei processi attivi e dei dump di arresto anomalo, consentendo agli sviluppatori di creare strumenti per eseguire il debug e la diagnostica.	Microsoft	2.0.4.26801
Microsoft.Diagnostics.Tracing.TraceEvent.dll	Una libreria per l'analisi e l'elaborazione degli eventi di Event Tracing for Windows (ETW)	Microsoft	2.0.70

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
Microsoft. DotNet.Platform Abstractions.dll	Fornisce API per accedere alle informazioni sulla piattaforma .NET	Microsoft	3.100.620.31604
Microsoft. Extensions. Dependency Injection. Abstractions	Definisce le astrazioni per l'inserimento di dipendenze nelle applicazioni .NET	Microsoft	6.0.21.52210
Microsoft. Extensions.Logging	Facilita la registrazione strutturata degli eventi nelle applicazioni .NET.	Microsoft	6.0.21.52210
Microsoft. Extensions.Options	Supporta la configurazione delle opzioni nelle applicazioni .NET	Microsoft	6.0.21.52210
Microsoft. Extensions. Primitives	Fornisce interfacce e classi per il tracciamento delle modifiche e i token di annullamento, facilitando la gestione dei dati mutabili e la pulizia delle risorse.	Microsoft	6.0.21.52210
Microsoft.Identity. Client	La libreria MSAL per .NET fa parte della piattaforma di identità Microsoft per sviluppatori (precedentemente denominata Azure AD) v2.0. Consente di acquisire token di sicurezza per chiamare API protette. Utilizza gli standard di settore OAuth2 e OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity. Client.Extensions. Msal	Cache di token multiplatforma sicura per app client pubbliche MSAL.	Microsoft	2.19.3.0
Microsoft. IdentityModel. JsonWebTokens	Include tipi che forniscono supporto per la creazione, la serializzazione e la convalida di token web JSON. Utilizzato dai componenti che comunicano con i servizi back-end che utilizzano token web JSON per l'autenticazione.	Microsoft	6.8.0.11012
Microsoft. IdentityModel. Logging	Dipendenza di Microsoft.IdentityModel.Tokens	Microsoft	6.8.0.11012
Microsoft. IdentityModel. Tokens	Dipendenza del SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0.11012

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
Microsoft. ML.OnnxRuntime	Un motore di inferenza per l'esecuzione di modelli di apprendimento automatico nel formato ONNX (Open Neural Network Exchange)	Microsoft	1.12.1
Microsoft. ML.OnnxRuntime. Managed	Il wrapper .NET gestito per ONNX Runtime	Microsoft	1.12.1
Microsoft.Office. Interop.Excel.dll	Questa DLL, parte degli assembly di interoperabilità di Office, consente alle applicazioni .NET di interagire con Microsoft Excel	Microsoft	14.0.4733.1000
Microsoft. VisualStudio. TextTemplating.10.0	Offre funzionalità di creazione di modelli di testo all'interno di Visual Studio, consentendo agli sviluppatori di generare codice e altri artefatti testuali utilizzando i modelli T4.	Microsoft	10.0.40219.1
Microsoft.Win32. Registry.dll	Consente l'accesso al registro di sistema di Windows	Microsoft	5.0.20.51904
Microsoft.Win32. SystemEvents.dll	Supporta la gestione degli eventi di sistema nelle applicazioni .NET	Microsoft	8.0.23.53103
Microsoft.Win32. TaskScheduler.dll	Utilizzato per lo strumento di backup del FSW (backup automatici).	David Hall	2.5.11.0
Microsoft.Xaml. Behaviors.Wpf	XAML Behaviors è un mezzo semplice da usare per aggiungere interattività comune e riutilizzabile alle applicazioni WPF con un codice minimo.	xamlexperienceteam, Microsoft	1.0.1.0
Microsoft DIA SDK	Fornisce API per lavorare con le informazioni di debug nei file PDB	Microsoft	2.0.0.0
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	11.0.51106.1

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
Mono.Cecil	Utilizzato per ispezionare, modificare e creare assembly .NET	Microsoft	0.11.3.0
Moq.dll	Libreria .NET open-source per la creazione di oggetti mock durante i test di unità	Moq Community (Open Source)	4.16.1.0
Librerie di runtime MS-VisualC++ 7.1	Librerie di runtime Microsoft Visual C++	Microsoft	7.10.6030.0
NAL-NL1	Fitting formula library NAL-NL1	Australian Hearing	1.1.0.0
NAL-NL2	Fitting formula library NAL-NL2	Australian Hearing	2.0.11
NAudio.dll	Utilizzato per regolare i volumi e riprodurre file audio.	Open Source	1.9.0.0
.NET Framework	Runtime .NET Framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Utilizzato per la serializzazione e la deserializzazione JSON.	James Newton-King	13.0.3.27908
Newtonsoft.Json.Schema.dll	Una libreria per la validazione dello schema dei dati JSON	James Newton-King	3.0.14.25421
Nibelung	Librerie di fitting NoahLink Wireless	HIMSA	1.3.16.1
Nibelung2.CPD	Librerie di fitting NoahLink Wireless	HIMSA	2.0.3.0
Nlog	Dipendenza di HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	5.0.4.1331
Noahlink	Driver del dispositivo di fitting Noahlink	HIMSA	1.55.6.166
Driver Noahlink Wireless	Driver del dispositivo di fitting Noahlink Wireless	HIMSA	1.1.0.0
Noahlink Wireless Upgrader	Strumento di aggiornamento del firmware Noahlink Wireless	HIMSA	3.1.0.82
ModuleAPI.dll (Noah System)	Un componente di Noah System di HIMSA, che fornisce API per l'integrazione e la gestione dei dati audiologici	HIMSA	4.13.0.5404
NiXPS SDK	Fornisce funzionalità per la gestione di documenti XPS (XML Paper Specification)	NiXPS NV	2.6.0.0

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
NPOI	Una libreria open-source che facilita la lettura e la scrittura di documenti Microsoft Office nelle applicazioni .NET	NPOI comuni	2.4.1.0
NuGet Package Manager	Uno strumento per la gestione di librerie e pacchetti .NET	Microsoft	6.3.0.131
Nunit	Un framework per i test di unità delle applicazioni .NET	NUnit Project	3.12.0.0
ONNX Runtime	Motore per modelli Open Neural Network Exchange (ONNX)	Microsoft	1.12.20220803.2.7048164
Open XML SDK	Fornisce strumenti per lavorare con i documenti Office Open XML	Microsoft	2.7.2
OSExtensions.dll	Libreria che offre estensioni per le funzionalità del sistema operativo	Microsoft	1.0.0.0
Otometrics.REMaccess	Livello di astrazione di Otometrics sopra la libreria dell'interfaccia di comunicazione inter-modulo Noah	GN Otometrics	1.0.0.10
Paket.Core.dll	Un gestore di dipendenze open source per progetti .NET e Mono	Paket Community (Open Source)	7.1.5.0
Patagames.Pdf	La libreria C# PDF per creare e modificare documenti PDF nelle applicazioni .Net.	patagames.com	8.57.30.48
Patagames.Pdf.Wpf	La libreria C# PDF per creare e modificare documenti PDF nelle applicazioni .Net.	Patagames.com	4.19.18.48

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
Polly	Libreria che consente agli sviluppatori di esprimere politiche di resilienza e gestione degli errori transitori come Retry, Circuit Breaker, Bulkhead Isolation e Fallback in modo fluido e thread-safe	App vNext	7.2.3.0
Portable.BouncyCastle	Dipendenza di HIMS A Nibelung.CPD (Noahlink Wireless)	The Legion of the Bouncy Castle Inc	1.8.15362.1
Portable.BouncyCastle.Crypto	Dipendenza di HIMS A Nibelung.CPD (Noahlink Wireless)	The Legion of the Bouncy Castle Inc	1.9.0.1
protobuf-net.dll	Framework di serializzazione utilizzato per RC blob.	Open Source	2.3.2.0
Google.Protobuf	La libreria ufficiale Protocol Buffers di Google per .NET, che facilita la serializzazione e la deserializzazione dei dati strutturati.	Google Inc	3.19.3.0
Perfolizer.dll	Una libreria open-source per l'analisi delle prestazioni	Open Source	0.2.1.0
Rhino.Mocks.dll	Un framework dinamico per oggetti mock per .NET	Rhino Mocks Community	3.6.0.0
Security.Cryptography.NetCore.dll	Fornisce funzionalità crittografiche per le applicazioni .NET Core	HardDev	1.0.1.0
Serilog	Componente di registrazione utilizzato per l'intera applicazione Chinook.	Contributori Serilog	3.0.1.0
Serilog.Enrichers.Thread	Arricchisce gli eventi Serilog con le proprietà del thread corrente	Contributori Serilog	3.1.0.0

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
Serilog. Extensions. Logging	Integra Serilog con le astrazioni di logging di Microsoft	Contributori Serilog	3.1.0.0
Serilog. Expressions	Filtraggio degli eventi basato sulle espressioni per Serilog.	Contributori Serilog	2.0.0.0
Serilog.Sinks. Console	Un sink Serilog che scrive gli eventi di registro nella console/nel terminale.	Contributori Serilog	4.0.0.0
Serilog.Sinks. Debug	Un sink Serilog che scrive gli eventi di registro nella finestra di output di debug.	Contributori Serilog	2.0.0.0
Serilog.Sinks.File	Scrive gli eventi Serilog in file di testo in formato semplice o JSON.	Contributori Serilog	4.1.0.0
Serilog.Sinks. NUnit.dll	Si integra con NUnit, indirizzando gli eventi di log all'output dei test di NUnit e facilitando la diagnostica dei test.	Contributori Serilog	1.0.3.0
Serilog.Sinks. Trace	Il sink di traccia diagnostica per Serilog.	Contributori Serilog	2.1.0.0
Serilog.Settings. AppSettings	Supporto della configurazione XML (System.Configuration <appSettings>) per Serilog.	Contributori Serilog	2.2.2.0
Security. Cryptography. NetCore.dll	Estensioni alle API di sicurezza fornite con il framework .NET	Microsoft	1.0.1.0
SharpBITS API	SharpBITS.NET è un wrapper .NET dell'API BITS e una piccola applicazione per l'interfaccia utente di Windows per un accesso più semplice al caricamento e al download di BITS.	perpetualKid	2.1.0.0

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
SharpZipLib	#ziplib (SharpZipLib, precedentemente NzipLib) è una libreria Zip, Gzip, Tar e Bzip2 scritta interamente in C# per la piattaforma .NET. Questa libreria fornisce funzionalità di compressione (zip, unzip, compressione di flussi, ecc.). Viene utilizzata nell'app di aggiornamento del firmware.	Open Source	1.3.3.11
SharpDX	Utilizzato da LiveSwitch: SharpDX.Direct3D11, SharpDX.Direct2D1, SharpDX.Mathematics	Alexandre Mutel	4.0.1
SocketIOClient	Fornisce un client per Socket.IO, consentendo la comunicazione bidirezionale in tempo reale basata su eventi nelle applicazioni .NET	HeroWong	2.2.4.0
Superpower	Una libreria di combinatori di parser per C#	Datalust, contributori Superpower, contributori Sprache	2.3.0.0
SQLite.Interop	Libreria di interoperabilità nativa per SQLite 3.36.0. SQLite è il database in-process utilizzato per memorizzare informazioni sui pazienti (in modalità autonoma), il nostro catalogo di prodotti, le relative risorse e i metadati per il fitting, gli accessori e gli apparecchi acustici. SQLite è di dominio pubblico.	Team di sviluppo SQLite	1.0.115

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
System.Buffers	Fornisce il raggruppamento delle risorse di qualsiasi tipo per applicazioni critiche in termini di prestazioni che assegnano ed eliminano oggetti frequentemente.	microsoft, dotnetframework	4.6.28619.01
System.Collections.Immutable	Utilizzato dalle librerie provenienti da Sonova. HardwareAbstraction. Palio.Trafo	Microsoft	7.0.22.51805
System.ComponentModel.Annotations	Fornisce attributi utilizzati per definire i metadati per gli oggetti utilizzati come origini dati.	microsoft, dotnetframework	4.6.26515.06
System.Configuration.ConfigurationManager	Fornisce tipi che supportano l'utilizzo di file di configurazione.	Microsoft	5.0.20.51904
System.CodeDom.dll	Fornisce classi per la generazione e la compilazione del codice sorgente in file eseguibili o assembly	Microsoft	8.0.23.53103
System.Data.SQLite	Utilizzato dalle librerie provenienti da Sonova. HardwareAbstraction. Palio.Trafo	Team di sviluppo SQLite	1.0.115.0
System.Diagnostics.DiagnosticSource	Una libreria di logging che consente agli sviluppatori di tracciare e monitorare i dati diagnostici	Microsoft	6.0.21.52210
System.Diagnostics.PerformanceCounter	Fornisce API per interagire con i contatori delle prestazioni di Windows	Microsoft	7.0.22.51805
System.Drawing.Common	Fornisce l'accesso alle funzionalità grafiche GDI+.	Microsoft	8.0.324.11603

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
System.Formats.Asn1.dll	Supporta la codifica e la decodifica dei dati in formato Abstract Syntax Notation One (ASN.1)	Microsoft	6.0.21.52210
System.IdentityModel.Tokens.Jwt	Include tipi che forniscono supporto per la creazione, la serializzazione e la convalida di token web JSON. Utilizzato dai componenti che comunicano con i servizi back-end che utilizzano token web JSON per l'autenticazione.	Microsoft	6.8.0.11012
System.IO.Abstractions	Un insieme di astrazioni che aiutano a rendere testabili le interazioni con il file system.	Tatham Oddie & friends	12.0.10.46693
System.IO.Hashing.dll	Fornisce funzionalità di hashing all'interno di .NET, inclusi algoritmi per il calcolo di checksum e hash crittografici.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Consente la lettura e la scrittura dei file di pacchetto	Microsoft	6.0.21.52210
System.IO.Ports.dll	Fornisce classi per la comunicazione tramite porta seriale, consentendo alle applicazioni .NET di interagire con l'hardware collegato tramite porte seriali.	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	Un gestore HTTP specializzato per Windows	Microsoft	6.0.422.16404

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
System.Numerics.Vectors	Fornisce tipi numerici accelerati tramite hardware, adatti per applicazioni grafiche ed elaborazione ad alte prestazioni.	microsoft, dotnetframework	4.6.26515.06
System.Memory	Fornisce tipi per una rappresentazione e un raggruppamento efficienti dei segmenti di memoria gestiti, dello stack e nativi e delle sequenze di tali segmenti, insieme a funzioni primitive per analizzare e formattare il testo codificato in UTF-8 memorizzato in tali segmenti di memoria.	microsoft, dotnetframework	4.6.31308.01
System.Reactive.dll		Open Source	5.0.0.1
System.Reflection.DispatchProxy	Fornisce una classe per creare dinamicamente tipi proxy che implementano un'interfaccia specifica e derivano da un tipo DispatchProxy specifico. Le invocazioni dei metodi sull'istanza proxy generata vengono inviate al tipo base DispatchProxy.	Microsoft	4.700.20.21406

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
System.Reflection.Metadata	Questo pacchetto fornisce un lettore e uno scrittore di metadati .NET (ECMA-335) di basso livello. È progettato per le prestazioni ed è la scelta ideale per creare librerie di livello superiore che intendono fornire il proprio modello di oggetti, come i compilatori.	Microsoft	5.0.20.51904
System.Reflection.TypeExtensions	Fornisce metodi di estensione per l'API reflection	Microsoft	4.700.19.56404
System.Runtime.CompilerServices.Unsafe	Fornisce System.Runtime.CompilerServices.Unsafe. Classe Unsafe, che fornisce funzionalità generiche di basso livello per la manipolazione dei puntatori.	microsoft, dotnetframework	6.0.21.52210
System.Security.AccessControl	Fornisce classi di base che consentono di gestire gli elenchi di controllo degli accessi e degli audit sugli oggetti proteggibili.	Microsoft	6.0.21.52210
System.Security.Permissions	Fornisce tipi che supportano Code Access Security (CAS).	Microsoft	5.0.20.51904
System.Security.Principal.Windows	Fornisce classi per recuperare l'utente Windows corrente e per interagire con utenti e gruppi Windows.	Microsoft	5.0.20.51904
System.Security.Cryptography.Cng.dll	Fornisce funzionalità crittografiche utilizzando le API Cryptography Next Generation (CNG)	Microsoft	5.0.20.51904

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
System.Security.Cryptography.Pkcs.dll	Offre classi per la gestione degli standard di crittografia a chiave pubblica (PKCS), inclusi i dati firmati e i dati incapsulati (enveloped)	Microsoft	6.0.1923.31806
System.Security.Cryptography.ProtectedData.dll	Fornisce metodi per proteggere e rimuovere la protezione dei dati, utilizzando Windows Data Protection API (DPAPI) per l'archiviazione sicura dei dati.	Microsoft	6.0.21.52210
System.Security.Cryptography.Xml.dll	Consente la crittografia XML e le firme digitali, supportando la gestione sicura dei dati XML nelle applicazioni .NET.	Microsoft	6.0.822.36306
System.ServiceModel.Http.dll	Fornisce funzionalità di comunicazione basate su HTTP per i servizi di Windows Communication Foundation (WCF).	Microsoft	4.700.19.56502
System.ServiceModel.Primitives.dll	Contiene le classi fondamentali per i servizi WCF, incluse le classi base e le interfacce per i contratti di servizio e i canali.	Microsoft	4.700.19.56502
System.Text.Encoding.CodePages	Fornisce supporto per le codifiche basate sulla tabella codici, tra cui Windows-1252, Shift-JIS e GB2312.	Microsoft	5.0.20.51904

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
System.Text.Encodings.Web	Fornisce tipi per la codifica e l'escape di stringhe da utilizzare in JavaScript, HyperText Markup Language (HTML) e Uniform Resource Locator (URL). Dipendenza del SOUP IdentityModel	microsoft, dotnetframework	6.0.21.52210
System.Text.Json	Fornisce tipi ad alte prestazioni e bassa allocazione che serializzano gli oggetti in testo JavaScript Object Notation (JSON) e deserializzano il testo JSON in oggetti, con supporto UTF-8 integrato. Fornisce inoltre tipi per leggere e scrivere testo JSON codificato come UTF-8 e per creare un modello di oggetto documento (DOM) in memoria, di sola lettura, per l'accesso casuale degli elementi JSON all'interno di una vista strutturata dei dati.	Microsoft	6.0.222.6406
System.Threading.Tasks.Extensions	Fornisce tipi aggiuntivi che semplificano il lavoro di scrittura di codice simultaneo e asincrono.	microsoft, dotnetframework	4.6.28619.01
System.Threading.Channels	Fornisce un insieme di strutture dati di sincronizzazione per il trasferimento di dati tra produttori e consumatori, supportando la programmazione parallela ad alte prestazioni.	Microsoft	6.0.21.52210

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
System.ValueTuple	Fornisce le strutture System.ValueTuple, che implementano i tipi sottostanti per tuple in C# e Visual Basic. Aggiunge il supporto per le tuple di valori poiché sono incluse solo nelle versioni successive di .NET Framework.	microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy.dll	Un framework di Behavior-Driven Development (BDD) per .NET	TestStack Community	4.3.2.0
Thrift	Utilizzato per la definizione del protocollo remotelink	Apache	0.13.0.0
Unity.Container	Unity Container (Unity) è un contenitore di inserimento di dipendenze completo ed estensibile.	Unity Container Project	5.8.13.0
Unity.Configuration	Unity Container (Unity) è un contenitore di inserimento di dipendenze completo ed estensibile.	Unity Container Project	5.2.5.0
Unity.Abstractions	Unity Container (Unity) è un contenitore di inserimento di dipendenze completo ed estensibile.	Unity Container Project	3.3.1.0
Unity.Interception.Configuration	Unity Container (Unity) è un contenitore di inserimento di dipendenze completo ed estensibile.	Unity Container Project	5.1.7.0

ELEMENTO SOUP	DESCRIZIONE DELLA FUNZIONALITÀ	PRODUTTORE	VERSIONE
Unity. Interception	Unity Container (Unity) è un contenitore di inserimento di dipendenze completo ed estensibile.	Unity Container Project	5.5.5.0
Unity. Registration ByConvention	Unity Container (Unity) è un contenitore di inserimento di dipendenze completo ed estensibile.	Unity Container Project	2.1.9.0
Unity. ServiceLocation	Unity Container (Unity) è un contenitore di inserimento di dipendenze completo ed estensibile.	Unity Container Project	2.1.2.0
WAP BT Dongle Driver	WAP BT Dongle Driver (chiavetta di fitting)	iAnywhere Solutions	3.0.0.6095
WebSync	Utilizzato per l'integrazione del canale dati di fitting	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor.dll	Un controllo editor esadecimale per applicazioni WPF	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	Una libreria di utilità per applicazioni WPF che fornisce informazioni su schermo e monitor	FM (Frozen Mountain)	2.1.0.0
Xceed Extended WPF Toolkit	Una raccolta di controlli e utilità WPF che arricchiscono le applicazioni WPF con componenti aggiuntivi dell'interfaccia utente.	Xceed	3.5.0.0
xmlunit-core.dll	Una libreria per testare e confrontare l'output XML.	XMLUnit Community	2.9.0.205
Xps to Pdf render (NiXPS)	Converte a livello di programmazione i file XPS in PDF; utilizzato nei report dell'app di fitting.	NiXPS	2.6.7.0

14. BIBLIOGRAFIA

Titolo	Sito web
Istruzioni per l'uso (formato elettronico)	https://ifu.advancedbionics.com/
Informativa sulla privacy globale di Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Backup e ripristino dei dati nel database Noah	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
È stata raggiunta la capacità massima del database del sistema Noah.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer – Elenco delle porte utilizzate	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Documentazione sulla sicurezza del server LiveSwitch	https://developer.liveswitch.io/liveswitch-server/server/security.html
Documento informativo EHIMA “Best Practices for Secure Fitting of Hearing Devices”	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA_Cybersecurity-FSW-Security-Whitepaper_v1-Sep2021.pdf

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

info.us@advancedbionics.com

 Advanced Bionics
Logistic Services GmbH
Rheinmetallstraße 18A
99610 Sömmerda, Germany

info.switzerland@advancedbionics.com

Per informazioni sulle altre sedi AB, visitare il sito
advancedbionics.com/contact

AB – A Sonova brand

Si prega di contattare il rappresentante locale AB per informazioni
sull'approvazione normativa e sulla disponibilità nella propria area geografica.

Il marchio denominativo e i loghi Bluetooth® sono marchi registrati di proprietà
di Bluetooth SIG, Inc. e qualsiasi uso di tali marchi da parte di Sonova AG
è concesso in licenza.



029-S398-05