

Target CI v1.6

CYBERSÄKERHETSGUIDE

Svenska

Uppdaterad: juli 2026



Innehåll

1. INLEDNING	3
1.1 FÖRKORTNINGAR OCH DEFINITIONER:	3
2. ANDRA RESURSER	4
2.1 KUNDSUPPORT	4
2.2 AB PRO PORTAL	4
2.3 AVANCERAD INSTALLATIONSGUIDE	4
2.4 BRANDVÄGGSKONFIGURATION FÖR TARGET CI	4
2.5 MDS2	4
2.6 BRUKSANVISNING (IFU)	5
2.7 HIMSA	5
3. NÄTVERKS- OCH KONTEXTDIAGRAM	6
3.1 DISTRIBUTIONSMODELL 1: FRISTÅENDE	6
3.2 DISTRIBUTIONSMODELL 2: NOAH DISTRIBUTED	7
3.3 DISTRIBUTIONSARTEFAKTER	8
3.4 SYSTEMSAMMANKOPPLINGAR	9
4. SYSTEMKRAV	11
5. CYBERSÄKERHET UNDER PRODUKTENS LIVSCYKEL	12
5.1 DISTRIBUTION	12
5.2 INSTALLATION	12
5.3 KONFIGURATION OCH ANVÄNDNING	13
5.4 BORTTAGNING OCH AVVECKLING	14
6. SÄKERHETSKONTROLLER	16
6.1 ÅTKOMSTKONTROLLER	16
6.2 REVISIONSLOGGNING OCH KONTROLLER FÖR ANSVARSSKYLDIGHET	16
6.3 FJÄRRÅTKOMST	17
7. INFORMATIONSSKYDD	18
7.1 INTEGRITETSPOLICY FÖR ADVANCED BIONICS	18
7.2 FEDERALA STANDARDER FÖR INFORMATIONSBEARBETNING (FIPS)	18
7.3 PII/PHI SOM BEHANDLAS AV PRODUKTEN	18
7.4 SÄKERHET VID ÖVERFÖRING	19
7.5 SÄKERHET FÖR LAGRADE DATA	20
8. PROGRAMVARUINTEGRITET	23
8.1 VERIFIERING AV NEDLADDAD INSTALLATIONSMEDIER	23
8.2 MANUELL VERIFIERING AV ANPASSNINGSPROGRAMVARAN FÖRE INSTALLATION	24
8.3 AUTOMATISK VERIFIERING AV DEN INSTALLERADE ANPASSNINGSPROGRAMVARANS INTEGRITET	25

8.4	MANUELL VERIFIERING AV DEN INSTALLERADE ANPASSNINGSPROGRAMVARANS INTEGRITET	26
9.	PROGRAMVARUKORRIGERINGAR OCH UPPDATERINGAR	27
10.	DATAHANTERING	28
10.1	DATABASER	28
10.2	DATAMIGRERING	28
10.3	HÖRAPPARATSKONFIGURATIONER.....	28
10.4	RADERING AV DATA	28
11.	SÄKERHETSMILJÖ – DELAT ANSVAR	29
12.	TILLVERKNING, PROGRAMVARUUTVECKLING OCH SÄKERHETSHANTERING.....	31
13.	PROGRAMVARUKOMPONENTER OCH MATERIALFÖRTECKNING	32
14.	REFERENSER	47

1. INLEDNING

Detta dokument innehåller teknisk information om säkerhet och integritet för programvarusystemet Target CI v1.6 från Advanced Bionics, nedan kallat "anpassningsprogramvaran". Anpassningsprogramvaran är utformad för att användas av kvalificerade audionomer för att konfigurera (dvs. anpassa) hörapparater för patienter som har fått cochleaimplantat från Advanced Bionics.

Detta dokument fokuserar specifikt på de cybersäkerhets- och integritetsaspekter som är relevanta vid användning av anpassningsprogramvaran. Det inkluderar en utvärdering av de säkerhets- och sekretesskontroller som för närvarande är integrerade i programvaran samt de som förväntas tillämpas och konfigureras i IT-miljön där produkten kommer att användas för sitt avsedda ändamål.

Detta dokument innehåller inte teknisk information om säkerhet och integritet för:

- Tidigare versioner av AB:s anpassningsprogramvara
- Annan AB-programvara än Target CI v1.6
- AB-webbplatser
- AB-mobilapplikationer
- AB-hörapparater

1.1 FÖRKORTNINGAR OCH DEFINITIONER:

Akronym	Term
FSW (Fitting software)	Anpassningsprogramvara
SaMD	Programvara som medicinteknisk produkt
Noah	Ett patienthanteringssystem från tredje part från HIMSA som används för att lagra och hantera patientuppgifter och anpassningsdata
TeamViewer	Ett plattformsoberoende verktyg för fjärråtkomst och skrivbordsdelning
SOUP	Programvara med okänt ursprung
HCP	Audionom
SaMD	Programvara som medicinteknisk produkt
AB	Advanced Bionics
Sonova	Advanced Bionics är ett helägt dotterbolag till Sonova och utgör en integrerad del av Sonova-koncernen.
IFU	Bruksanvisning
PHI	Skyddade hälsouppgifter
PII	Personligt identifierbar information
SBOM	Programvaruförteckning

2. ANDRA RESURSER

2.1 KUNDSUPPORT

För användare i USA och Kanada erbjuder Advanced Bionics ett avgiftsfritt telefonnummer för teknisk support (877-271-6727), där professionell support finns tillgänglig måndag till fredag kl. 5.00–17.00, Stillahavstid.

För användare utanför USA och Kanada tillhandahålls teknisk support regionalt. Om du har frågor om anpassningsprogramvaran, tillhörande maskinvara eller andra programmeringsproblem, kontakta din lokala AB-representant.

2.2 AB PRO PORTAL

Anpassningsprogramvaran och tillhörande dokumentation kan laddas ner från <https://www.abproportal.com> eller Sonova Web Client. En kontoinloggning krävs. Denna resurs kanske inte är tillgänglig på alla marknader; kontakta din AB-representant för mer information.

2.3 AVANCERAD INSTALLATIONSGUIDE

Den avancerade installationsguiden för Target CI v1.6 är tillgänglig på begäran. Guiden innehåller teknisk information om installationsprogrammet för anpassningsprogramvaran, inklusive kommandoradsalternativ för tysta och automatiserade installationer.

2.4 BRANDVÄGGSKONFIGURATION FÖR TARGET CI

Dokumentet om brandväggskonfiguration finns tillgängligt på begäran. Detta dokument innehåller IT-inriktad vägledning för att säkerställa att Target CI 1.6 fungerar bakom en företagsbrandvägg och beskriver den HTTP/HTTPS-åtkomst som krävs samt de viktigaste värnnamnen. Det omfattar WebRTC-anslutning via Twilio och Xirsys och beskriver TURN-portar och portar för peer-relaying. Det anges även att många IP-adresser är dynamiska och att värnnamnsbaserade regler därför bör användas där det är möjligt.

2.5 MDS2

Manufacturer Disclosure Statement for Medical Device Security (MDS2) är ett branschstandardformulär som innehåller information om säkerhet och integritet för AB:s anpassningsprogramvara. Formuläret finns tillgängligt på begäran.

2.6 BRUKSANVISNING (IFU)

Bruksanvisningen levereras med installationsmediet för programvaran. För vissa marknader finns den elektroniska bruksanvisningen tillgänglig för nedladdning på www.advancedbionics.com/ifu

Följande avsnitt i bruksanvisningen kan vara relevanta för IT-specialister:

- Produktbeskrivning
- Systemets minimikrav och prestandaegenskaper
- Riktlinjer för IT-säkerhet
- Användningsinstruktioner
- Kassering och farligt material
- Teknisk support

2.7 HIMSA

Hearing Instrument Manufacturer's Software Association (HIMSA) är en tredjepartsleverantör av programvara som utvecklar Noah System 4, ett programvarusystem för hörselvården som ger audionomer ett leverantörsoberoende system för att utföra klientrelaterade uppgifter.

Anpassningsprogramvaran kan som tillval konfigureras för att använda Noah System 4 för datalagring i stället för en lokal databas.

HIMSAs säkerhetswebbsida ger svar på vanliga IT-säkerhetsfrågor om Noah System 4.

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

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

Se säkerhetsavsnittet i HIMSA Learning Center för ytterligare säkerhetsinformation:

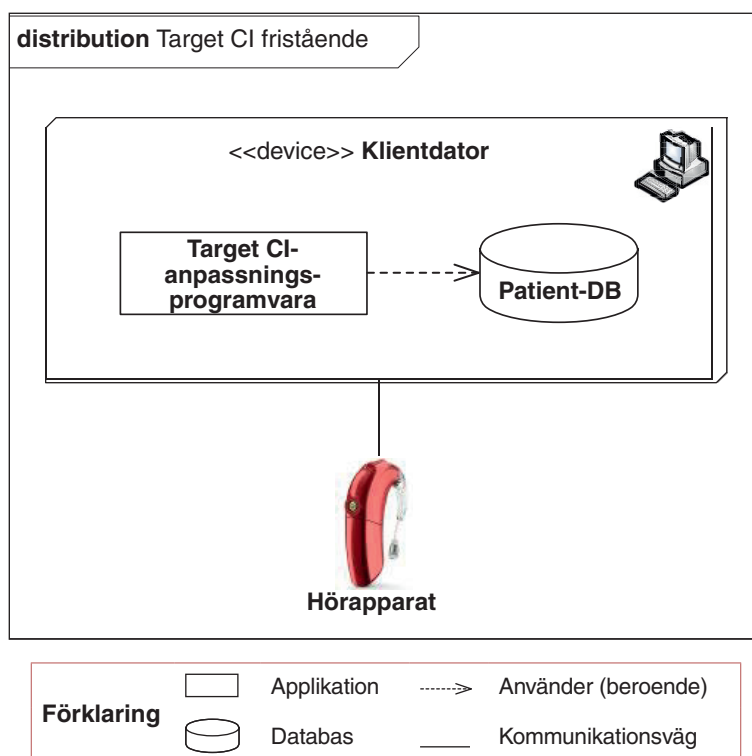
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. NÄTVERKS- OCH KONTEXTDIAGRAM

Det finns två distributionsmodeller som stöds för anpassningsprogramvaran, vilket är en klientapplikation (SaMD) installerad på en kommersiellt tillgänglig standard-Microsoft Windows-dator. Programvaran inkluderar ingen hårdvara eller något operativsystem.

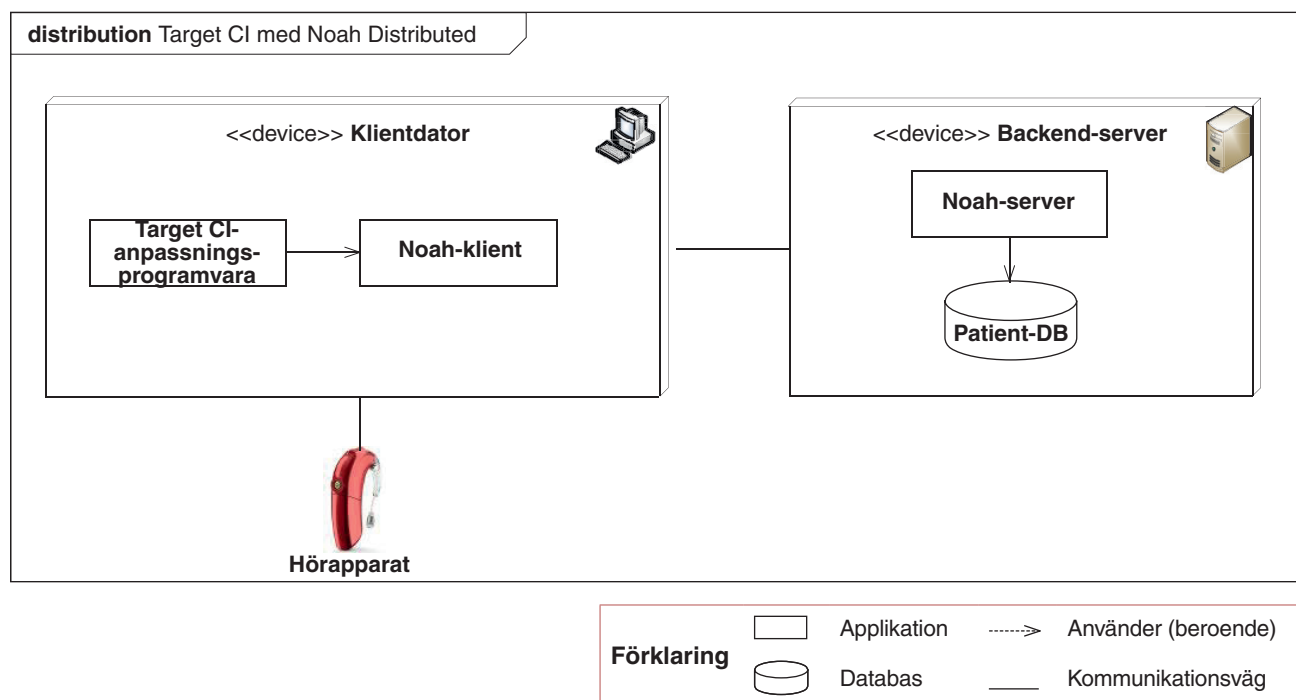
3.1 DISTRIBUTIONSMODELL 1: FRISTÅENDE

I den fristående distributionsmodellen distribueras anpassningsprogramvaran till en klientdator. Patientdatabasen lagras på samma dator och installeras tillsammans med anpassningsprogramvaran.



3.2 DISTRIBUTIONSMODELL 2: NOAH DISTRIBUTED

I distributionsmodellen Noah Distributed distribueras anpassningsprogramvaran till en eller flera klientdatorer där Noah är installerat. Noah, ett patienthanteringssystem från tredje part, distribueras till en intern server som är tillgänglig för klientdatorerna. Patientdatabasen lagras på Noah-servern och nås via nätverket från en eller flera klientdatorer.



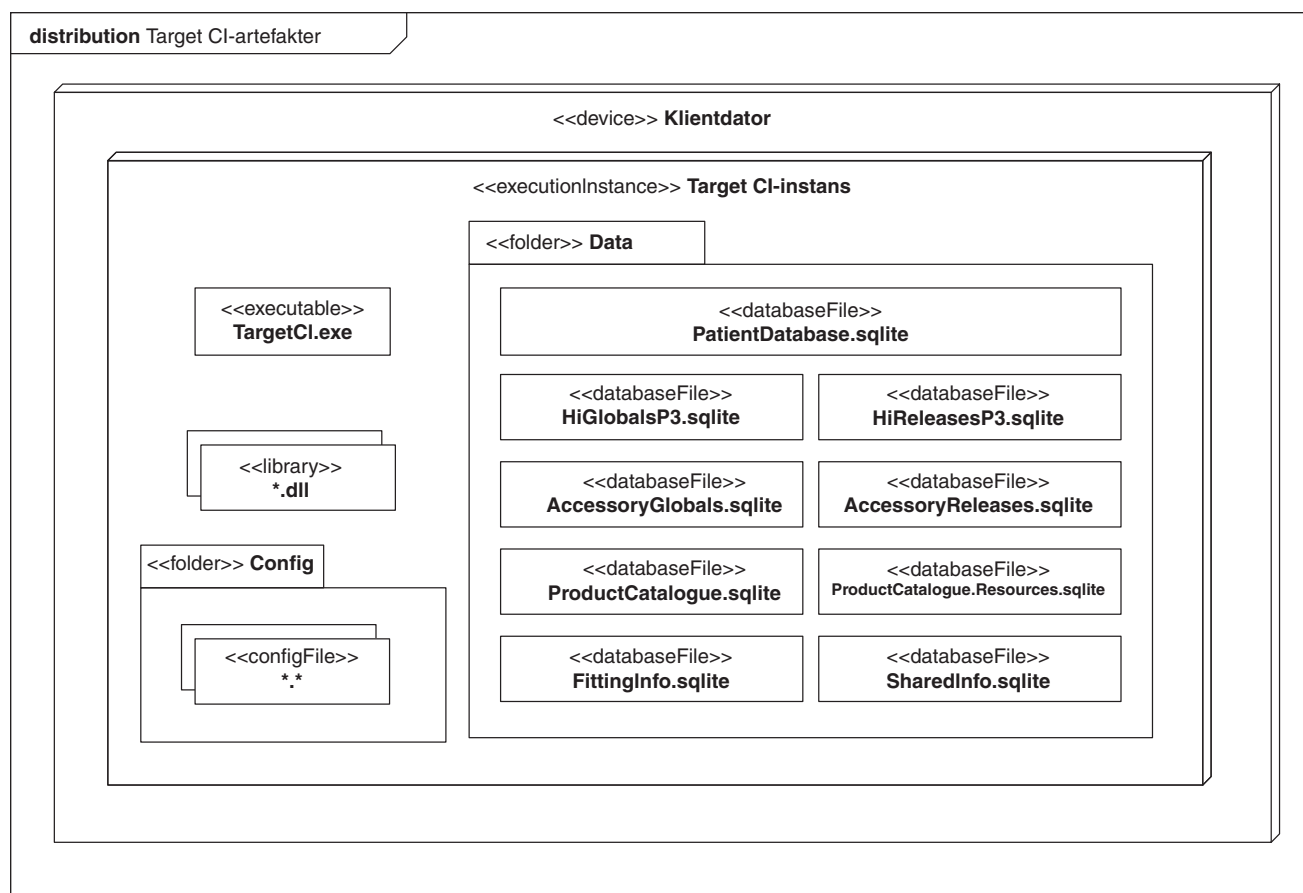
3.3 DISTRIBUTIONSARTEFAKTER

Anpassningsprogramvaran installeras med en körbar fil och en uppsättning tillhörande filer, inklusive komponent-DLL:er, konfigurationsfiler och SQLite-databasfiler.

Konfigurationsfilerna installeras i mappen "%ProgramData%\Advanced Bionics\Target CI\Target CI\Config" och databasfilerna installeras i mappen "%ProgramData%\Advanced Bionics\Target CI\Target CI\Data". Mappen Data innehåller en enda transaktionsdatabasfil och flera informationsdatabasfiler.

Transaktionsdatabasen PatientDatabase.sqlite lagrar patientens demografiska uppgifter och anpassningsdata och installeras endast när anpassningsprogramvaran distribueras i fristående läge.

När anpassningsprogramvaran distribueras som en Noah-modul tillhandahåller Noah-systemet de nödvändiga tjänsterna för beständig datalagring till anpassningsprogramvaran. De återstående SQLite-filerna är en integrerad del av anpassningsprogramvaran och krävs för alla distributionsmodeller.



Källa/ Destination	Tjänst	Protokoll	Port	Beskrivning
Noah	Noah 4 ModuleAPI	.NET Remoting	N/A	Primärt gränssnitt för modulen som används för att komma åt Noah- programvaran (endast i distributionsmodellen Noah Distributed)
Sonova Cloud Services	Sonova Cloud API, Core dispatcher, Remote support	SOAP, REST	443	Sonova-tjänster som finns i ett Microsoft Azure-datacenter används för att: • hämta anpassnings- programvarans klient- konfigurationsdata från Sonovas backend-lagring • överföra logg- och analysdata • upprätta fjärranpassnings- sessioner i realtid
Twilio/Xirsys, AB Remote Support och AB Remote Support + Mobile Apps	Remote Support	WebRTC	Finns i dokumentet Brandväggs- konfiguration för Target CI	Används av fjärrsupportfunktionen för WebRTC- signalering och fjärranpassnings- sessioner i realtid
AB:s kundsupport	Skrivbords- delning	TeamViewers proprietära protokoll	5938, 443, 80 Se TeamViewerPorts	Används för fjärranalys och felsökning i realtid av problem som påverkar installationer av anpassnings- programvaran. Se avsnitt 6.3 FJÄRRÅTKOMST för mer information.

4. SYSTEMKRAV

Operativsystem	Windows 10, 11, Pro/Enterprise
.NET Framework	Version 4.8
CPU	Intel® Core™ i5 eller motsvarande med likvärdig eller bättre prestanda
RAM	4 GB eller mer
Hårddiskutrymme	3 GB eller mer
Minimikrav för visning	• 1280 x 1024-upplösning (maximal skalning 125 %) • 24-bitars färg
Drivrutiner	• Noahlink Wireless-drivrutin (den senaste versionen från HIMSA krävs om du använder ett USB-anslutet Noahlink Wireless-programmeringsgränssnitt från tredje part). • CPI-3-drivrutin (krävs om ett USB-anslutet CPI-3-programmeringsgränssnitt används).
Databas	SQLite eller Noah System 4 (version 4.16 eller senare)
Internetanslutning	Internetanslutning krävs för fjärrsupport och analysloggning, se avsnitt 3.4 Systemsammankopplingar; intranät krävs vid användning av nätverksanslutet Noah System 4.
Nätverksportar	Se avsnitt 3.4 Systemsammankopplingar; se avsnitt 2. Andra resurser – HIMSA för portar som används av Noah System 4.

5. CYBERSÄKERHET UNDER PRODUKTENS LIVSCYKEL

5.1 DISTRIBUTION

Godkända distributionsmetoder:

1. Ladda ner från Sonova Web Client (SFTP) på <https://webclient.sonova.com>, eller från AB Pro Portal på <https://www.abproportal.com>
2. Installera från ett officiellt USB-minne från Advanced Bionics.

Verifiera installationsprogrammets digitala signatur före installationen och skanna filen med ett uppdaterat antivirusprogram. Se avsnitt 8 för detaljerade instruktioner om integritetsverifiering. Tillämpa sedvanliga IT-säkerhetskontroller för hälso- och sjukvården under distributionen, inklusive slutpunktsskydd och nätverksbegränsningar.

Vid användning av ett USB-minne:

- Använd endast officiella USB-minnen som tillhandahålls av Advanced Bionics.
- Förvara USB-minnet på en fysiskt säker plats och ändra inte dess innehåll.
- Skanna USB-minnet och installationsmiljön med ett uppdaterat antivirusprogram och vitlistning av applikationer.
- Advanced Bionics ansvarar inte för obehöriga data som lagras på USB-minnen som innehåller installationspaketet.

5.2 INSTALLATION

Ett administratörskonto krävs för att installera anpassningsprogramvaran. När programvaran har installerats kan den köras utan administratörsbehörighet eller utökade behörigheter.

Se avsnitt 8, Programvaruintegritet, för information om hur programvarans integritet verifieras före installation.

Före installationen rekommenderas systemadministratörer att säkerställa att:

- den version av anpassningsprogramvaran som ska installeras är den senaste tillgängliga.
- det underliggande operativsystemet är uppdaterat.
- integriteten och äktheten hos anpassningsprogramvarans installationsdata verifieras. Se avsnitt 8 för information om hur programvarans integritet verifieras före installation.

Det finns två installationsprogram för installation av anpassningsprogramvaran:

- Standardinstallationsprogram
- IT Professional-installationsprogram

IT Professional-installationsprogrammet är en enda MSI-fil och exkluderar nödvändiga komponenter men är i övrigt likvärdigt med standardinstallationsprogrammet.

Nödvändiga komponenter inkluderar Microsoft .NET Framework v4.8 och Microsoft Visual C++ Redistributable-paketet.

Båda installationsprogrammen stöder avancerade installationsscenarier, inklusive tyst installation.

IT Professional-installationsprogrammet bör endast användas om din organisation kräver att nödvändiga komponenter installeras och hanteras av just din organisation och inte av anpassningsprogramvarans installationsprogram. Standardinstallationsprogrammet bör användas i alla andra fall.

IT Professional-installationsprogrammet kan erhållas från en klinisk AB-representant. IT Professional-installationsprogrammet kan inte användas för att reparera, ominstallera eller avinstallera installationer som gjorts med standardinstallationsprogrammet. Standardinstallationsprogrammet kan inte användas för att reparera, ominstallera eller avinstallera installationer som gjorts med IT Professional-installationsprogrammet.

För avancerade installationsscenarier följer du instruktionerna i den avancerade installationsguiden för anpassningsprogramvaran (se avsnitt 2.3). För standardinstallationsscenarier, se avsnitt 2.5 i detta dokument, som innehåller en länk till bruksanvisningen (IFU) för anpassningsprogramvaran.

5.3 KONFIGURATION OCH ANVÄNDNING

Anpassningsprogramvaran stöder en uppsättning integritets- och säkerhetskontroller och funktioner. Vissa integritets- och säkerhetsfunktioner i anpassningsprogramvaran är aktiverade som standard, vissa kan konfigureras vid installationen och beror på den valda distributionsmodellen, medan andra kan konfigureras under normal användning via applikationens grafiska användargränssnitt.

Se:

- Avsnitt 6 för en lista över säkerhetskontroller som förbättrar skyddet av anpassningsprogramvarans applikationssystem
- Avsnitt 7 för en lista över säkerhetskontroller som förbättrar skyddet av data som behandlas av anpassningsprogrammet

Ytterligare integritets- och säkerhetskontroller (som inte stöds av anpassningsprogramvaran på applikationsnivå) förväntas aktiveras och konfigureras av användare (t.ex. audionomer, systemadministratörer och IT-personal) på operativsystemnivå och/eller IT-infrastrukturnivå. Se avsnitt 11 i detta dokument för en detaljerad lista över rekommendationer för bästa praxis och säkerhetskontroller för den anpassningsmiljö där anpassningsprogramvaran kommer att användas.

Brandvägg

Anpassningsprogramvaran är inte försedd med en intern brandvägg.

Om en extern brandvägg är aktiverad (t.ex. på operativsystemnivå) kan dess konfiguration behöva uppdateras för att tillåta nödvändig inkommande och utgående trafik (t.ex. WebRTC-ljud-, video- och dataströmmar under en Remote Support-session). Se dokumentet om brandväggskonfiguration för anpassningsprogramvaran, som innehåller en lista över nätverksadresser och portar som används av anpassningsprogramvaran.

Proxyinställningar

Anpassningsprogramvaran är försedd med en lokal proxy. Via anpassningsprogramvarans grafiska användargränssnitt går det att ändra inställningarna för proxyn:

- Ingen proxy
- Identifiera proxyinställningar automatiskt
- Manuell proxykonfiguration. Om det här alternativet väljs kan följande inställningar konfigureras:
 - Adress
 - Port
 - Aktivera/inaktivera proxyautentisering (användarnamn, lösenord, domän)

5.4 BORTTAGNING OCH AVVECKLING

Se bruksanvisningen (IFU) för anpassningsprogramvaran för detaljerad information om hur programvaran avinstalleras.

Avinstallationsprogrammet tar inte bort de datakategorier som anges i följande tabell. Om inget annat anges i kolumnen "Anmärkningar" i tabellen måste sådana data tas bort manuellt från systemen av systemadministratörer, t.ex. genom att filerna tas bort manuellt eller genom att systemdisken som används för datalagring raderas.

Datakategori	Standardplats	Anmärkningar
Applikationsdata	C:\ProgramData\ Advanced Bionics\Target CI\Target CI	Inkluderar följande typer av data: • Analysdata • Konfigurationsdata • Applikationsloggar • Tillfälliga filer
Personuppgifter	C:\ProgramData\ Advanced Bionics\Target CI\Target CI\Data	Patientdatabas (endast relevant för den fristående distributionsmodellen)
Fjärråtkomstverktyg	C:\Program Files (x86)\Common Files\ Advanced Bionics\ TeamViewer	Används för analys och felsökning i realtid av problem som påverkar anpassningsprogramvaran, inklusive problem som uppstår under installation och avinstallation. Se avsnitt 6.3 för mer information.

När du avinstallerar anpassningsprogramvaran från en stationär/bärbar dator som ska avvecklas eller kasseras ska du säkerställa att samtliga känsliga data (t.ex. PHI, PII) raderas.

För Noah-distributioner finns detaljerade instruktioner om radering av data på:

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

Externa medier som innehåller data som exporterats från anpassningsprogramvaran, inklusive rapporter och loggar, bör skyddas. När data inte längre används bör de raderas på ett säkert sätt och/eller mediet raderas på ett säkert sätt eller förstöras.

Godkända procedurer och verktyg bör användas för säker borttagning av data som lagras på flyttbara medier, i enlighet med tillämpliga föreskrifter och riktlinjer för hantering av patientinformation/personligt identifierbar information (PII)/skyddade hälsouppgifter (PHI).

6. SÄKERHETSKONTROLLER

Anpassningsprogramvaran är ett klientprogram som installeras på en kommersiell Microsoft Windows-dator. Anpassningsprogramvaran kan installeras som en fristående applikation eller som en Noah-modul.

6.1 ÅTKOMSTKONTROLLER

Anpassningsprogramvaran begränsar inte åtkomsten till sina funktioner baserat på inloggningskrav och enskilda användares roller. Rollbaserade åtkomstkontroller stöds inte.

Lokal användaråtkomst

När anpassningsprogramvaran installeras som en fristående applikation är den beroende av värdoperativsystemets mekanismer för åtkomstkontroll. Kundens IT-personal kan konfigurera värdoperativsystemet för att hantera användarautentisering och tilldela åtkomsträttigheter eller behörigheter. Det rekommenderas starkt att varje användare loggar in med ett unikt, individuellt konto.

Ytterligare kompenserande kontroller beskrivs i avsnitt 11 i detta dokument och i avsnittet Riktlinjer för IT-säkerhet i bruksanvisningen.

När anpassningsprogramvaran installeras som en Noah-modul hanteras åtkomstkontrollen via Noah System 4.

Mer information om de åtkomstkontrollfunktioner som implementeras av Noah System 4 finns i dokumentationen på www.HIMSA.com.

Serviceåtkomst

Servicetekniker på plats kan få åtkomst till anpassningsprogramvaran med hänsyn till de åtkomstkontroller som kundens IT-personal har konfigurerat för hantering av autentisering.

AB:s supporttekniker kan få åtkomst till anpassningsprogramvaran via funktionen för skrivbordsdelning som stöds av anpassningsprogramvaran. Se avsnitt 6.3 för detaljerad information om de säkerhetskontroller som är aktiverade för den här funktionen.

6.2 REVISIONSLOGGNING OCH KONTROLLER FÖR ANSVARSSKYLDIGHET

Anpassningsprogramvaran genererar inga ytterligare revisionsloggar eller rapporter utöver de som tillhandahålls av det underliggande operativsystemet.

Fristående distributionsmodell

När anpassningsprogramvaran installeras som en fristående applikation förlitar den sig på de revisionsmekanismer som tillhandahålls av värdoperativsystemet. Anpassningsprogramvaran har ingen sådan integrerad funktion. Vårdoperativsystemet kan konfigureras av kundens IT-personal för att logga vissa händelser, såsom start/körning av anpassningsprogramvaran. Det rekommenderas att varje användare loggar in på värdoperativsystemet med ett unikt individuellt användarkonto för att underlätta revision.

Distributionsmodellen Noah Distributed

När anpassningsprogramvaran installeras som en Noah-modul hanteras revisionsloggningen av Noah System (Noah Activity Log). Mer information om de revisionskontroller som finns i Noah System 4 finns i dokumentationen på www.himsa.com

6.3 FJÄRRÅTKOMST

Funktionen för skrivbordsdelning möjliggör fjärranalys i realtid och felsökning av problem som påverkar installationer av anpassningsprogramvaran. Den här funktionen är baserad på tredjepartsverktyget TeamViewer QuickSupport (distribueras som standard tillsammans med anpassningsprogramvaran) och gör det möjligt för AB:s kundsupportpersonal att fjärransluta till vårdgivarens dator och få fullständig kontroll över den från skrivbordet, inklusive åtkomst till det underliggande operativsystemet och filsystemet.

För att upprätta en skrivbordsdelningssession krävs interaktion med audionomen. Audionomen ska först köra TeamViewer QuickSupport-verktyget (t.ex. via anpassningsprogramvaran Target CI) och överföra sina TeamViewer ID-uppgifter till AB Support-teamet via en separat kommunikationskanal (t.ex. ett telefonsamtal).

Namnet och TeamViewer-ID:t för personen i AB Support-teamet visas som standard på audionomens datorskärm under varje aktiv skrivbordsdelningssession.

All nätverkstrafik för skrivbordsdelning skyddas med kryptografiska protokoll och algoritmer som anses säkra enligt dagens standarder (utbyte av offentliga/privata RSA-nycklar och AES 256-bitars sessionskryptering).

Fjärråtkomstverktyget kan tas bort manuellt utan att det påverkar andra funktioner i Target FSW. Installationsprogrammet för Target FSW stöder en kommandoradsparameter som möjliggör installation av Target FSW via kommandoraden utan att fjärråtkomstverktyget inkluderas.

7. INFORMATIONSSKYDD

7.1 INTEGRITETSPOLICY FÖR ADVANCED BIONICS

Integritetspolicyn som beskriver hur Advanced Bionics samlar in, överför, lagrar och använder personuppgifter kan laddas ner från AdvancedBionics.com/privacy.

Advanced Bionics är inte värd för, lagrar eller säkerhetskopierar och har inte heller åtkomst till några data som lagras i anpassningsprogramvarans eller Noahs databaser, såvida inte dessa data uttryckligen skickas till Advanced Bionics.

7.2 FEDERALA STANDARDER FÖR INFORMATIONSBEARBETNING (FIPS)

Target CI v1.6 uppfyller krypteringsstandarden FIPS 140-2.

7.3 PII/PHI SOM BEHANDLAS AV PRODUKTEN

Anpassningsprogramvaran behandlar patientens personuppgifter och hälsouppgifter.

Patientinformationen matas antingen in manuellt av användaren av anpassningsprogramvaran eller tas emot av applikationen via ett eller flera av dess dataflöden.

Följande typer av information behandlas i anpassningsprogramvarans huvudsakliga dataflöden:

	Sonova Cloud Services (Core dispatcher, Remote Support)	Hörapparat	Mobilapp	Patientdatabas (lokal/Noah)	Fjärråtkomst
Namn				X	X(2)
Adress				X	X(2)
Födelsedatum	X(1)		X	X	X(2)
Telefonnummer				X	X(2)
E-postadress				X	X(2)
Journalnummer				X	X(2)
Enhetsidentifierare och serienummer	X(1)	X	X	X	X(2)
IP-adress	X(1)				
Audiogram, RECD och REUG	X(1)	X	X	X	X(2)
Anpassningsdata		X	X	X	X(2)
Användningsdata för hörapparater	X(1)	X	X	X	
Användningsdata för anpassningsprogram	X(1)				

(1) Pseudonymiseras innan data överförs till Sonovas datasjö.

(2) Under en skrivbordsdelningssession i realtid får AB:s kundsupporttekniker fullständig kontroll över audionomens skrivbord, inklusive åtkomst till det underliggande operativsystemet och filsystemet samt data som lagras där. Se avsnitt 6.3 för mer information.

Kontakta din lokala supportrepresentant för mer detaljerad information om insamling och behandling av data.

7.4 SÄKERHET VID ÖVERFÖRING

Kommunikationssäkerhet säkerställs och aktiveras i all inkommande och utgående nätverkskommunikation för anpassningsprogramvaran. Förutom funktionen Remote Support (som använder WebRTC-protokollet) och Bluetooth-kommunikation med hörapparater och tillbehör skyddas alla andra anslutningar av TLS-protokollet (Transport Layer Security) som ger konfidentialitet, integritet och autenticitet.

TLS

TLS-konfigurationen följer aktuell bästa praxis och de säkerhetsrekommendationer som dokumenteras i BCP 195 – Recommendations for Secure Use of TLS and DTLS [8], inklusive:

- Stöder inte SSL- och TLS-versioner före 1.2
- Stöder inte chiffersviter som använder kryptografiska algoritmer med mindre än 128 bitars säkerhet
- Stöder rekommenderade TLS-tillägg enligt BCP 195
- Stöder inte osäkra tillägg enligt BCP 195

DTLS

Kryptering är en obligatorisk funktion i WebRTC och tillämpas på alla medieströmmar som skickas via WebRTC. Vilket krypteringsprotokoll som används beror på kanaltypen. Dataströmmar krypteras med DTLS 1.2 och medieströmmar krypteras med Secure Real-time Transport Protocol (SRTP), eftersom det är ett resurssnålare alternativ än DTLS.

Se följande länk för mer detaljerad information om säkerhetskongfigurationen för Remote Support WebRTC:

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

BLE

Trådlös Bluetooth Low Energy-kommunikation med hörapparater och tillbehör är krypterad och integritetsskyddad som standard (förutom för identifierings- och detekteringsanvändningsfall). Dessutom är hörapparaternas Bluetooth-parkopplingsläge tidsbegränsat. Se tillgänglig dokumentation för hörapparater för en mer detaljerad beskrivning av säkerheten för Bluetooth-kommunikationskanalen.

7.5 SÄKERHET FÖR LAGRADE DATA

Applikationsdata

Applikationsdata finns på samma maskin, under standardkatalogen:

C:\ProgramData\Advanced Bionics\Target CI\Target CI

Åtkomsträttigheten ärvs från den överordnade mappen och är begränsad till användare som är inloggade på det lokala systemet (den inbyggda användargruppen INTERACTIVE1¹) under installationen av programvaran.

Behöriga användare har läs- och skrivåtkomst till katalogen.

För att minska risken för obehörig åtkomst till applikationsdata via nätverket ska du säkerställa att inga mappar eller filer som innehåller dessa data delas i nätverket. Standardplatserna för applikationsdata anges i avsnitt 5.4.

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

Patientdatabas – fristående distributionsmodell

När anpassningsprogramvaran installeras som en fristående applikation finns patientdatabasen på samma dator och patientposterna är inte krypterade när de lagras. PII överförs inte via nätverket av applikationen.

Alla användare som kan logga in på datorn där anpassningsprogramvaran är installerad har fullständig åtkomst till alla applikationsdata, inklusive patientdatabasen. Se avsnittet Dataskydd för vägledning om rekommenderade dataskyddsåtgärder.

I vissa jurisdiktioner kan föreskrifter kräva att alla patientdata krypteras för att undvika potentiellt ansvar vid dataförlust eller stöld. Aktivera BitLocker eller motsvarande fullständig hårddiskkryptering (på operativsystemnivå eller hårdvarubaserad) för att skydda data från obehörig åtkomst eller kopiering medan data är i viloläge.

BitLocker är en inbyggd Windows-funktion som krypterar hela enheten och kräver autentisering för åtkomst. Läs alltid Microsofts officiella riktlinjer och din organisations IT-säkerhetspolicy innan du aktiverar BitLocker.

Så här aktiverar du BitLocker

Administratörsbehörighet krävs för att hantera BitLocker.

1. Sök efter "Hantera BitLocker"
Öppna Start-menyn, skriv "Hantera BitLocker" och välj det från sökresultaten.
2. Välj systemenheten
Välj den enhet där Windows är installerat för att konfigurera krypteringsinställningar.
3. Välj en upplåsningsmetod
Välj ett av följande alternativ:
 - Endast TPM
 - TPM + PIN
 - TPM + USB-nyckelFölj Microsofts riktlinjer för bästa praxis och din organisations IT-säkerhetspolicy när du väljer upplåsningsmetod.
4. Säkerhetskopiera återställningsnyckeln
Säkerhetskopiera återställningsnyckeln med säkra metoder som godkänts av organisationen. Rekommenderade alternativ inkluderar:
 - Lagring i Microsoft Entra ID (tidigare Azure AD) eller Active Directory för domänanslutna enheter
 - Lagring på en säker, åtkomstkontrollerad nätverksplats med kryptering och revisionsloggning
 - Användning av en hanterad nyckeldepositionslösning som godkänts av din organisationUndvik att spara nyckeln på lokala enheter, USB-minnen eller skriva ut den om det inte uttryckligen är tillåtet enligt policyn. Återställningsnycklar måste skyddas lika rigoröst som andra känsliga autentiseringsuppgifter och bytas ut omedelbart om de exponeras.

5. Starta kryptering

Välj:

- Hela enheten – rekommenderas i de flesta företagsmiljöer. Krypterar alla sektorer, inklusive oanvänt utrymme, för att förhindra kvarstående data.

Patientdatabas – Noah-distributionsmodul

När anpassningsprogramvaran installeras som en Noah-modul lagras personliga uppgifter i patientdatabasen som Noah hanterar. Patientdatabasen som Noah lagrar kan finnas på en annan dator. PII och andra patientdata hanteras av Noah-programvaran, och Noah System säkerställer krypteringen av patientens lagrade data. Anpassningsprogramvaran kan skicka/ta emot PII via en trådbunden eller trådlös nätverksanslutning när en Noah-databas konfigureras för nätverksåtkomst.

PII som lagras i en nätverksansluten Noah-databas är åtkomlig för andra användare på andra datorer som har behörighet till samma nätverksanslutna databas. Noah-databasen kan också konfigureras för lokal åtkomst och installeras på samma dator som anpassningsprogramvaran.

Noah förhindrar att anpassningsprogramvaran får åtkomst till patientjournaldatabasen. När en användare öppnar en patient i anpassningsprogramvaran via Noah Client kan anpassningsprogramvaran endast läsa från och skriva till den patientjournal som för närvarande är öppen och har inte åtkomst till andra patientjournaler i Noah-databasen.

Se följande länk för mer information om krypteringsstandarder som används av Noah System:

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

RMA-exportfiler

Anpassningsprogramvaran gör det möjligt att exportera klientinformation till en fil. RMA-filen kan skickas till Advanced Bionics för att lösa RMA-ärenden eller relaterade supportärenden.

RMA-filen är asymmetriskt RSA-krypterad med en nyckellängd på 2048 bitar. Anpassningsprogramvaran har ingen funktion för att dekryptera en RMA-fil.

Anonymiserade exportfiler

Anpassningsprogramvaran gör det möjligt att exportera klientinformation till en klientanonymiserad fil. Klientens personligt identifierbara information, såsom födelsedatum och namn, ersätts med generiska värden. Filen är inte krypterad och kan importeras till samma instans eller en annan instans av anpassningsprogramvaran.

Standardexportfiler

Anpassningsprogramvaran gör det möjligt att exportera klientinformation till en standardexportfil. Filen använder ett eget binärt format och är inte krypterad. Filen kan importeras till samma eller en annan instans av anpassningsprogramvaran. När den här funktionen används måste användare av anpassningsprogramvaran se till att standardexportfiler hanteras enligt deras lokala IT-policyer för hantering av okrypterad personlig information.

Hörapparat

Anpassningsprogramvaran lagrar klientinformation på klientens hörselanordning. Personligt identifierbar information som klientens namn och födelsedatum lagras inte i hörapparaten. Annan information som inte utgör PII lagras med PBKDF2-kryptering med en 128-bitars nyckel.

Anpassningsprogramvaran kan skicka/ta emot klientinformation som inte utgör PII till/från en hörselenhet via en proprietär trådbunden enhet (dvs. CPI-3), mobilapparna AB Remote Support och AB Remote Support+ eller en Noahlink Wireless-enhet. Noahlink Wireless-enheten ansluter till hörselenheten med Bluetooth Low Energy (BLE) via en standardiserad BLE-kanal med 128-bitars AES-kryptering.

8. PROGRAMVARUINTEGRITET

8.1 VERIFIERING AV NEDLADDADA INSTALLATIONSMEDIER

Installationsmedier för anpassningsprogramvaran Target CI kan i vissa regioner laddas ner från Advanced Bionics Pro Portal eller Sonova Web Client. De nedladdade installationsmediernas autenticitet kan verifieras med valfritt betrott SHA-256-hashverktyg.

SHA256-hashen för standardinstallationens zip-fil är:

A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

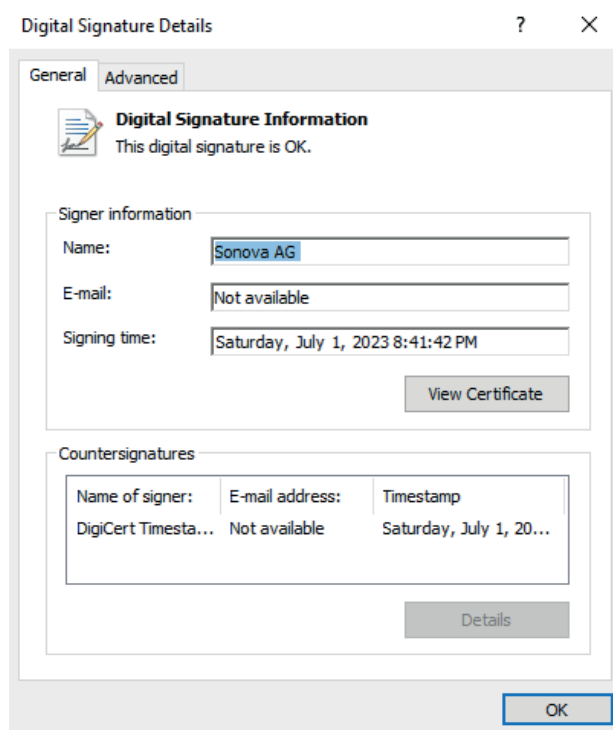
SHA256-hashen för IT Professional-installationens zip-fil är:

DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 MANUELL VERIFIERING AV ANPASSNINGSPROGRAMVARAN FÖRE INSTALLATION

Användare kan utföra följande steg för att verifiera anpassningsprogramvarans integritet och äkthet före installation:

1. Öppna Utforskaren i Windows och navigera till rotmappen för anpassningsprogramvarans installationsmedium. Om ditt installationsmedium är ett USB-minne, sätt in det i en USB-port och navigera till dess rotmapp. Om installationsmediet är en zip-fil packar du upp den till en mapp och navigerar till den mappen.
2. Högerklicka på SonovaVerify.exe och välj Egenskaper på snabbmenyn.
3. Välj fliken Digitala signaturer.
4. Dubbelklicka på SHA256-signaturen "Sonova AG".
5. Kontrollera att signaturens delar är giltiga. Kontrollera särskilt att meddelandet "Den digitala signaturen är OK." visas nära överkanten och att undertecknarens namn och signeringstid överensstämmer med följande bild:



6. Klicka på knappen "Visa certifikat" och sedan på fliken "Detaljer" och kontrollera att värdet i fältet "Tumavtryck" överensstämmer med följande:
db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Stäng popup-dialogrutorna och dubbelklicka på SonovaVerify.exe
8. Kontrollera att "NO ERRORS DETECTED." visas enligt följande bild:

```
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 . . .
```

Utdata "NO ERRORS DETECTED" innebär att verifieringen av integriteten och äktheten hos innehållet på anpassningsprogramvarans installationsmedium har slutförts utan fel. Detta innebär att SonovaVerify.exe har autentiserat alla filer och mappar och verifierat deras integritet. Detta verifierar att innehållet på anpassningsprogramvarans installationsmedium inte har manipulerats, skadats eller på annat sätt äventyrats.

SonovaVerify.exe visar varningar eller felmeddelanden om filer eller mappar saknas eller om oväntade filer eller mappar har lagts till på installationsmediet. Om varningar eller felmeddelanden visas har verifieringen av integriteten och äktheten hos innehållet på anpassningsprogramvarans installationsmedium misslyckats och du rekommenderas att:

- inte fortsätta med installationen
- inte öppna eller köra några filer som finns i anpassningsprogramvarans installationsavbildning och rapportera problemet till Advanced Bionics support (se avsnitt 2.1)

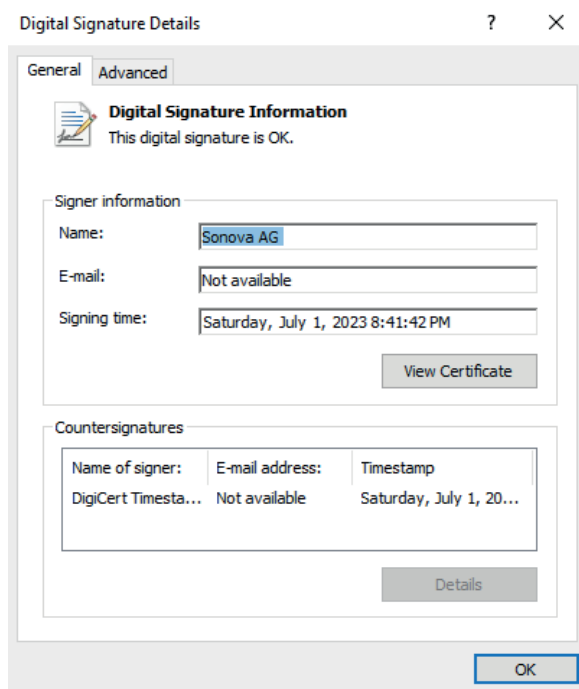
8.3 AUTOMATISK VERIFIERING AV DEN INSTALLERADE ANPASSNINGSPROGRAMVARANS INTEGRITET

SonovaVerify är integrerat med anpassningsprogramvaran och körs varje gång applikationen startas för att verifiera integriteten hos anpassningsprogramvarans programfiler. Programfiler signeras digitalt med hjälp av branschstandardpraxis och certifikat utfärdade av en betrodd certifikatutfärdare. Programvaran meddelar användaren via varningsmeddelanden om några programfiler har komprometterats.

8.4 MANUELL VERIFIERING AV DEN INSTALLERADE ANPASSNINGSPROGRAMVARANS INTEGRITET

Användare kan när som helst utföra följande steg för att verifiera den installerade anpassningsprogramvarans integritet och äkthet utan att behöva starta anpassningsprogramvaran:

1. Öppna Utforskaren i Windows och navigera till mappen med anpassningsprogramvarans körbara filer, som vanligtvis finns här: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Högerklicka på SonovaVerify.exe och välj Egenskaper på snabbmenyn.
3. Välj fliken Digitala signaturer.
4. Dubbelklicka på SHA256-signaturen "Sonova AG".
5. Kontrollera att signaturens delar är giltiga, särskilt att meddelandet "Den digitala signaturen är OK." visas nära överkanten och att undertecknarens namn och signeringstid överensstämmer med följande bild:



6. Klicka på knappen "Visa certifikat" och sedan på fliken "Detaljer" och kontrollera att värdet i fältet "Tumavtryck" överensstämmer med följande:
db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Stäng popup-dialogrutorna och dubbelklicka på SonovaVerify.exe
8. Kontrollera att "NO ERRORS DETECTED." visas enligt följande bild:

```
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 . . .
```

Utdata "NO ERRORS DETECTED" innebär att verifieringen av integriteten och äktheten hos innehållet på anpassningsprogramvarans installationsmedium har slutförts utan fel. Detta innebär att SonovaVerify.exe har autentiserat alla filer och mappar och verifierat deras integritet. Detta verifierar att innehållet på anpassningsprogramvarans installationsmedium inte har manipulerats, skadats eller på annat sätt äventyrats.

SonovaVerify.exe visar varningar eller felmeddelanden om filer eller mappar saknas eller om oväntade filer eller mappar har lagts till på installationsmediet. Om varningar eller felmeddelanden visas har verifieringen av integriteten och äktheten hos innehållet på anpassningsprogramvarans installationsmedium misslyckats och du rekommenderas att:

- inte fortsätta med installationen
- inte öppna eller köra någon fil som finns i anpassningsprogramvarans installationsavbildning och rapportera problemet till Advanced Bionics support (se avsnitt 2.1)

9. PROGRAMVARUKORRIGERINGAR OCH UPPDATERINGAR

Automatiska uppdateringar stöds inte. Se avsnitt 12 för mer information.

10. DATAHANTERING

10.1 DATABASES

Anpassningsprogramvaran använder en transaktionsdatabas för att lagra patientdata och en uppsättning informationsdatabaser som tillhandahåller de metadatakonfigurationer som krävs av applikationen.

Se avsnitt 3. Nätverks- och kontextdiagram - Distributionsartefakter för en detaljerad lista över alla databaser som distribuerats av anpassningsprogramvaran.

När anpassningsprogramvaran installeras som ett fristående program finns patientdatabasen i anpassningsprogramvaran. Patientdatabasen, som lagras i filen PatientDatabase.sqlite, finns på samma dator som anpassningsprogramvaran och används för lagring av patientdata. För att säkerhetskopiera applikationsdata när Target CI distribueras som en fristående applikation skapar du en säkerhetskopia av hela mappen på %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Skydda säkerhetskopior av data inte bara mot dataförlust utan även mot stöld. När anpassningsprogramvaran installeras som en Noah-modul lagras patientdata i databasen som tillhandahålls av Noah-systemet. Noah-databasen kan konfigureras för nätverksåtkomst. Noah-databasen kan också konfigureras för lokal åtkomst och installeras på samma dator som anpassningsprogramvaran. Konfigurera kryptering av Noah-databasen för att skydda data (se HIMSA-dokumentationen).

För distributionsläget Noah Distributed finns instruktioner om säkerhetskopiering och återställning av Noah-patientdatabasen på följande länk:

<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 DATAMIGRERING

Anpassningsprogramvaran låter användare migrera patientjournaler från AB:s tidigare anpassningsprogramvara, SoundWave 3.2. Patientjournaler måste vara tillgängliga från en SoundWave 3.2-installation på samma dator som Target CI för att kunna migreras.

10.3 HÖRAPPARATSKONFIGURATIONER

Anpassningsprogramvaran möjliggör export och import av enhetskonfigurationer och inställningar.

10.4 RADERING AV DATA

Se avsnitt 5.4, Borttagning och avveckling, i detta dokument och avsnittet Kassering och farligt material i bruksanvisningen (IFU) för vägledning om radering av data. För Noah-distributioner finns detaljerade instruktioner om radering av patientjournaler på:

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

11. SÄKERHETSMILJÖ – DELAT ANSVAR

Anpassningsprogramvaran har utformats för en avsedd användning där hantering av cybersäkerhetsrisker betraktas som ett delat ansvar mellan intressenter i hela hörselvårdssystemet, inklusive, men inte begränsat till, användare av hörselenheter, föräldrar eller vårdnadshavare till barn som använder hörapparater, audionomer, IT-administratörer, hörselvårdsinrättningar och vårdgivare samt leverantörer av hörselenheter och programmeringsutrustning.

Här följer en lista över rekommendationer för vedertagen bästa praxis och säkerhetskontroller för den anpassningsmiljö där anpassningsprogramvaran kommer att användas:

OS-nivå

- Tillämpa åtkomstkontroller på operativsystemnivå, t.ex.:
 - Ta bort gästkonton
 - Aktivera Windows-användarinloggningen
 - Upprätthåll en lista över behöriga operatörer för att kontrollera åtkomst till systemet
 - Konfigurera anpassade användare och roller
 - Tillämpa krav på starka lösenord och håll autentiseringsuppgifterna hemliga
 - Aktivera tidsgräns för inaktiva sessioner
- Tillämpa revisionskontroller på operativsystemnivå
- Se till att operativsystemet är uppdaterat
- Se till att den installerade versionen av anpassningsprogramvaran är uppdaterad
- Använd ett adekvat och uppdaterat skydd mot skadlig kod och virus
- Se till att funktionerna AutoRun och AutoPlay är inaktiverade
- Aktivera vitlistning av applikationer

Dataskydd

- Säkerställ att inga mappar eller filer som innehåller applikationsdata delas i nätverket. Standardplatserna för applikationsdata anges i tabellen i avsnitt 5.4. För att kontrollera vilka nätverksresurser som delas ut av en dator navigerar du till "Datorhantering -> Delade mappar -> Resurser" i Microsofts verktyg Datorhantering eller kör PowerShell-kommandot `Get-WmiObject -class Win32_Share`.
- Under installationen ställs behörigheten för mappen med applikationsdata in enligt avsnitt 6.1. Mappar med applikationsdata ärver åtkomstbehörigheter från den överordnade mappen. Hanteringen av behörigheter för den överordnade mappen är programvaruoperatörens ansvar.
- Kryptera patientdata med hjälp av tredjepartsverktyg eller kontroller på operativsystemnivå genom att använda enhetskryptering (t.ex. kostnadsfria Microsoft BitLocker) för att skydda alla data. För Noah-distributioner bör du överväga att använda kryptering av Noah-databasen.
- Externa medier som innehåller data som exporterats från anpassningsprogramvaran, inklusive rapporter och loggar, bör skyddas. När informationen inte längre används bör den raderas på ett säkert sätt och/eller mediet bör raderas på ett säkert sätt.

- Använd USB-lagringsmedier med inbyggda säkerhetsfunktioner, såsom krypterade USB-enheter med integrerad knappsats.
- Säkerställ alltid datasäkerheten genom att följa dessa rutiner:
 - När data överförs via osäkra kanaler ska de antingen anonymiseras eller krypteras.
 - Skydda säkerhetskopior av data inte bara mot dataförlust utan även mot stöld.
 - Ta bort alla data från datamedier som inte längre används eller som kommer att kasseras.
- Godkända procedurer och verktyg bör användas för säker borttagning av data som lagras på flyttbara medier, i enlighet med tillämpliga föreskrifter och riktlinjer för hantering av patientinformation/personligt identifierbar information (PII)/skyddade hälsouppgifter (PHI)

IT-infrastruktur

Använd anpassningsprogramvaran i en säker nätverksmiljö skyddad från obehörigt intrång. Det finns många effektiva tekniker för att isolera och skydda medicinska informationssystem, inklusive implementering av brandväggsskydd, demilitariserade zoner (DMZ), virtuella lokala nätverk (VLAN) och nätverksenklaver. Upprätthåll en aktiv nätverksanslutning för att ta emot operativsystemuppdateringar.

Fysisk nivå

- Arbetsstationen där anpassningsprogramvaran är installerad bör vara fysiskt säkrad så att obehörig personal varken kan få åtkomst till eller manipulera den.
- Åtkomst till skrivare som är anslutna till arbetsstationen bör kontrolleras.
- Bildskärmen på arbetsstationen där anpassningsprogramvaran är installerad bör placeras så att endast användaren kan se innehållet på skärmen.

Organisationsnivå

- Endast yrkesmässigt utbildad och fullt kvalificerad personal är behörig att använda systemet. Innan någon får behörighet att använda systemet bör det verifieras att personen har läst och till fullo förstår användningsinstruktionerna som medföljer anpassningsprogramvaran.
- Endast personal som är behörig att underhålla och använda anpassningsprogramvaran får tilldelas konton på den dator där programvaran är installerad. Dator- och domänkonton samt tillhörande åtkomsträttigheter bör granskas regelbundet och inaktiveras om åtkomst till datorn inte längre behövs.
- Om du upptäcker misstänkt aktivitet på dina konton för anpassningsprogramvaran eller oväntade åtgärder ska du kontakta Advanced Bionics. Se avsnitt 2.1 för mer information.

För mer information om delat ansvar och en mer detaljerad lista över rekommendationer för bästa praxis och säkerhetskontroller som ska tillämpas på olika nivåer i den anpassningsmiljö där anpassningsprogramvaran används, se:

- EHIMA:s [vitbok](#) "Best Practices for Secure Fitting of Hearing Devices"

12. TILLVERKNING, PROGRAMVARUUTVECKLING OCH SÄKERHETSHANTERING

Cybersäkerhet beaktas genom hela programvaruutvecklingsprocessen.

Anpassningsprogramvaran är utvecklad i enlighet med standarderna IEC 62304 och IEC 82304.

Anpassningsprogramvaran skannas efter virus och skadlig programvara som en del av tillverkningsprocessen.

Sårbarheter i tredjepartskomponenter som listas i NIST:s National Vulnerability Database (NVD) bedöms och åtgärdas under utvecklingsprocessen och övervakas efter att anpassningsprogramvaran har släppts på marknaden.

Konfigurationshantering

AB utvecklar, dokumenterar och underhåller internt baskonfigurationen för varje utgiven version av anpassningsprogramvaran under konfigurationskontroll.

Alla programvarukomponenter från tredje part som används av anpassningsprogramvaran identifieras och dokumenteras i programvarukomponentförteckningen (SBOM). SBOM används av AB vid hantering av cybersäkerhetsrisker för att bedöma och övervaka exponeringen för cybersäkerhetshot och offentliggjorda sårbarheter med hjälp av uppdaterade verktyg för sårbarhetsskanning.

Säkerhetsuppdateringar

AB övervakar kontinuerligt säkerhetssårbarheter som påverkar anpassningsprogramvaran. Detta inkluderar sårbarheter i anpassningsprogramvaran och i tredjepartskomponenter som används av anpassningsprogramvaran.

Offentliggjorda sårbarheter bedöms utifrån anpassningsprogramvarans konfiguration och användning.

Vid behov kan säkerhetssårbarheter åtgärdas genom en större version av anpassningsprogramvaran som innehåller korrigeringar för specifika programvarukomponenter i programvaruuppsättningen.

Sårbarhetsrapportering

Vi arbetar aktivt med sårbarhetsrapportering och med att förbättra säkerheten för våra produkter och tjänster.

Vi uppmuntrar rapportering av misstänkta sårbarheter eller säkerhetsproblem som rör våra produkter eller underliggande programvara/infrastruktur.

Läs vår policy för sårbarhetsrapportering som publicerats på <https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy> och följ instruktionerna för att skicka in en rapport.

13. PROGRAMVARUKOMPONENTER OCH MATERIALFÖRTECKNING

Anpassningsprogramvaran innehåller vissa kommersiella standardprogramvarukomponenter.

Följande tabell listar all SOUP (programvara av okänd härkomst) som distribueras med anpassningsprogramvaran.

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
AForge.NET	AForge.NET-bibliotek för matematik och media, som ingår i och krävs av IceLink och LiveSwitch.	AForge.NET	2.2.5.0
Amplifon. Programmer	Komponent i Amplifons programvarupaket	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Komponent i Amplifons programvarupaket	Amplifon	1.0.4.0
AutoMapper	Automatiserar mappning mellan objekt	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	Bibliotek för prestandamätning som tillhandahåller verktyg för att mäta och jämföra kodprestanda	BenchmarkDotNet Community	0.13.0.0
Castle.Core	Ett kärnbibliotek i Castle Project som erbjuder komponenter såsom dynamisk proxygenerering och IoC-containrar (Inversion of Control) för .NET-applikationer.	Castle Project	4.4.1
Chessie	Ett bibliotek för funktionell felhantering i F#	Open Source	0.6.0.0
ciAD Hearingloss Simulator	Bibliotek för simulering av hörselnedsättning för mediespelare	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Förenklar läsning, bearbetning och skrivning av Excel-filer utan att Excel behöver vara installerat	ClosedXML Community	0.95.4.0
CommandLine Parser	Tillhandahåller ett tydligt och koncist API för parsning av kommandoradsargument	CommandLineParser Community	2.4.3
Common.Logging	En portabel loggningsabstraktion för .NET-applikationer	Common.Logging Community	3.4.1.0
CommonService Locator	Tillhandahåller ett gemensamt gränssnitt för tjänstelokalisering, vilket gör det möjligt att frikoppla applikationer från specifika IoC-containrar.	Microsoft	2.0.5.0

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Credential Management	Credential Management-paketet är en wrapper för Windows Credential Management API	iLya Lozovyy	1.0.2
CSharpAnalytics	Används för Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78.45418
Deconstructurama.Attributed	Används av Nephele-bibliotek.	Serilog Contributors	3.1.0.0
Developer Express Suite	En omfattande uppsättning UI-kontroller och bibliotek för .NET-utvecklare med verktyg för att skapa funktionsrika applikationer.	Developer Express Inc	20.2.10.0
DirectShow 2005	Ger åtkomst till Microsofts DirectShow-funktion inifrån .NET-applikationer.	Microsoft	2.0
DSL4	DSL 4-anpassningsformelbibliotek	National Centre for Audiology, Kanada	4.2
DSL5	DSL 5-anpassningsformelbibliotek	National Centre for Audiology, Kanada	5.0.34
ExcelNumberFormat	Tillhandahåller funktioner för parsning och formatering av Excel-talformat	Open Source	1.1.0.0
FM.dll	En integrerad del av deras ramverk för realtidskommunikation, såsom LiveSwitch och IceLink	FM (Frozen Mountain)	2.9.32
FSharp.Core	Kärnbiblioteket för programmeringsspråket F#	Microsoft	6.0.322.10402
FTDI Chip	Ett drivrutinspaket från Future Technology Devices International (FTDI) som möjliggör kommunikation mellan USB-enheter och programvaruapplikationer.	FTDI	3.02.07
GNOtometrics.Aurical	GNOtometrics.Aurical ompaketerat för Sonova	Natus Medical Incorporated	2.0.1.9
SharedUtilities.dll	Tillhandahåller gemensamma hjälpfunktioner och delade resurser för Natus-applikationer.	Natus Medical Incorporated	1.0.0.0
Hardware.Info	En komponent som samlar in och tillhandahåller detaljerad information om ett systems maskinvarukonfiguration	Open Source	11.1.0.1

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Himsa.NLWSMAPI.dll	Ett bibliotek som är kopplat till HIMSA's Noah-programvara	HIMSA	2.0.3.0
natus.otometrics.hipro2	HiPro-kommunikationsbibliotek	Natus Medical Incorporated	2.0.0.4
Iced.dll	Möjliggör realtidskommunikation genom strömning av ljud, video och data	FM (Frozen Mountain)	1.12.0.0
IceLink	Används för WebRTC-audio/video-konferensintegration	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	Tillhandahåller stöd för Unicode och globalisering för programvaruapplikationer	FM (Frozen Mountain)	54.1.0.0
IdentityModel	OpenID Connect- och OAuth 2.0-klientbibliotek som används av komponenten Kona. CommonsServices.Authentication för OAuth 2-autentisering.	Dominick Baier, Brock Allen	6.2.0.0
IMCInterfaces	Noah Inter-Module Communication Interface Library	HIMSA II K/S	4.4.0.2266
iText 7	PDF-bibliotek för att skapa, modifiera och granska PDF-dokument programmatiskt.	iText Software	7.1.16.0
JetBrains.dotMemory	Ett minnesprofileringsverktyg för att upptäcka minnesläckor och optimera minnesanvändningen i .NET-applikationer	JetBrains	111.0.0.0
JsonDiffPatch DotNet.dll	Tillhandahåller funktioner för att jämföra och patcha JSON-objekt	Open Source	1.0.1.0
LibGit2Sharp	Används av bibliotek från Sonova för att kommunicera med Git	LibGit2Sharp contributors	0.26.1.93
LiveSwitch	Används för integrering av WebRTC-ljud-/videokonferenser	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	Loggningsramverk för .NET	Apache	4.7.0.3189
Mapster	Används för att mappa objekt i kod	chaowlert,eric_swann	7.2.0.0
Mapster.Core	Används för att mappa objekt i kod	chaowlert,eric_swann	1.2.0.0
MathNet.Numerics	Används för anpassningsalgoritmer (signalväg, målmatchning etc.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael och bidragsgivare	4.11.0

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Microsoft.Bcl.AsyncInterfaces	Tillhandahåller <code>IAsyncEnumerable< T></code> och <code>IAsyncDisposable</code> -gränssnitt och hjälptyper för .NET Standard 2.0.	Microsoft	6.0.21.52210
Microsoft.CodeAnalysis.Common	Används av biblioteken från Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	3.900.21.12420
Microsoft.CodeAnalysis.CSharp	Används av biblioteken från Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Tillhandahåller kompilering och kodgenerering med C#	Microsoft	4.700.19.56404
Microsoft.Diagnostics.FastSerialization.dll	Används för effektiv serialisering och deserialisering av diagnostikdata	Microsoft	1.0.0.0
Microsoft.Diagnostics.NETCore.Client.dll	Ett hanterat bibliotek som möjliggör interaktion med .NET Core-körningsmiljön för olika diagnostikuppgifter, såsom spårning och begäran av dumpar.	Microsoft	0.2.4.27602
Microsoft.Diagnostics.Runtime.dll	tillhandahåller API:er för att inspektera aktiva processer och kraschdumpar, vilket gör det möjligt för utvecklare att skapa felsöknings- och diagnostikverktyg.	Microsoft	2.0.4.26801
Microsoft.Diagnostics.Tracing.TraceEvent.dll	Ett bibliotek för parsning och bearbetning av Event Tracing for Windows-händelser (ETW)	Microsoft	2.0.70
Microsoft.DotNet.PlatformAbstractions.dll	Tillhandahåller API:er för åtkomst till information om .NET-plattformen	Microsoft	3.100.620.31604
Microsoft.Extensions.DependencyInjection.Abstractions	Definierar abstraktionerna för beroendeinjektion i .NET-applikationer	Microsoft	6.0.21.52210
Microsoft.Extensions.Logging	Underlättar strukturerad loggning i .NET-applikationer.	Microsoft	6.0.21.52210
Microsoft.Extensions.Options	Stöder konfiguration av alternativ i .NET-applikationer	Microsoft	6.0.21.52210

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Microsoft.Extensions.Primitives	Tillhandahåller gränssnitt och klasser för ändringsspårning och annulleringstoken, vilket underlättar hanteringen av föränderliga data och frigörandet av resurser.	Microsoft	6.0.21.52210
Microsoft.Identity.Client	MSAL-biblioteket för .NET är en del av Microsofts identitetsplattform för utvecklare (tidigare kallad Azure AD) v2.0. Det gör att du kan hämta säkerhetstokens för att anropa skyddade API:er. Det använder branschstandarden OAuth2 och OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Säker plattformsoberoende token-cache för offentliga MSAL-klientappar.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Innehåller typer som ger stöd för att skapa, serialisera och validera JSON Web Tokens. Används av komponenter som kommunicerar med backend-tjänster som använder JSON Web Tokens för autentisering.	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Logging	Beroende för Microsoft.IdentityModel.Tokens	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Tokens	Beroende för SOUP-komponenten Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0.11012
Microsoft.ML.OnnxRuntime	En inferensmotor för att köra maskininlärningsmodeller i ONNX-formatet (Open Neural Network Exchange)	Microsoft	1.12.1
Microsoft.ML.OnnxRuntime.Managed	Den hanterade .NET-wrappern för ONNX Runtime	Microsoft	1.12.1
Microsoft.Office.Interop.Excel.dll	Denna DLL-fil är en del av Office Interop-assemblierna och gör det möjligt för .NET-applikationer att interagera med Microsoft Excel	Microsoft	14.0.4733.1000
Microsoft.VisualStudio.TextTemplating.10.0	Tillhandahåller funktioner för textmallar i Visual Studio, vilket gör det möjligt för utvecklare att generera kod och andra textbaserade artefakter med hjälp av T4-mallar.	Microsoft	10.0.40219.1

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Microsoft.Win32.Registry.dll	Ger åtkomst till Windows-registret	Microsoft	5.0.20.51904
Microsoft.Win32.SystemEvents.dll	Stöder hantering av systemhändelser i .NET-applikationer	Microsoft	8.0.23.53103
Microsoft.Win32.TaskScheduler.dll	Används för FSW-säkerhetskopieringsverktyget (automatiska säkerhetskopior).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors är ett lättanvänt sätt att lägga till vanlig och återanvändbar interaktivitet i WPF-applikationer med minimal kod.	xamlexperienceteam, Microsoft	1.0.1.0
Microsoft DIA SDK	Tillhandahåller API:er för att arbeta med felsökningsinformation i PDB-filer	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
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
Mono.Cecil	Används för att inspektera, modifiera och skapa .NET-assemblyer	Microsoft	0.11.3.0
Moq.dll	.NET-bibliotek med öppen källkod för att skapa mockobjekt vid enhetstestning	Moq Community (Open Source)	4.16.1.0
MS-VisualC++ 7.1 runtime-bibliotek	Microsoft Visual C++ runtime-bibliotek	Microsoft	7.10.6030.0
NAL-NL1	Bibliotek för NAL-NL1-anpassningsformler	Australian Hearing	1.1.0.0
NAL-NL2	Bibliotek för NAL-NL2-anpassningsformler	Australian Hearing	2.0.11
NAudio.dll	Används för att justera volymen och spela upp ljudfiler.	Open Source	1.9.0.0
.NET Framework	.NET-miljö	Microsoft	4.8.3928.0
Newtonsoft.Json	Används för JSON-serialisering och deserialisering.	James Newton-King	13.0.3.27908

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Newtonsoft.Json.Schema.dll	Ett bibliotek för schemavalidering av JSON-data	James Newton-King	3.0.14.25421
Nibelung	NoahLink Wireless-anpassningsbibliotek	HIMSA	1.3.16.1
Nibelung2.CPD	NoahLink Wireless-anpassningsbibliotek	HIMSA	2.0.3.0
Nlog	Detta är ett beroende för HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	5.0.4.1331
NoahLink	Drivrutin för Noahlink-anpassningsenhet	HIMSA	1.55.6.166
Drivrutin för Noahlink Wireless	Drivrutin för Noahlink Wireless-anpassningsenhet	HIMSA	1.1.0.0
Noahlink Wireless Upgrader	Uppgraderingsverktyg för fast programvara i Noahlink Wireless	HIMSA	3.1.0.82
ModuleAPI.dll (Noah System)	En komponent i HIMSA's Noah System som tillhandahåller API:er för integrering och hantering av audiologiska data	HIMSA	4.13.0.5404
NiXPS SDK	Tillhandahåller funktioner för hantering av XPS-dokument (XML Paper Specification)	NiXPS NV	2.6.0.0
NPOI	Ett bibliotek med öppen källkod som underlättar läsning och skrivning av Microsoft Office-dokument i .NET-applikationer	NPOI communi	2.4.1.0
NuGet Package Manager	Ett verktyg för att hantera .NET-bibliotek och -paket	Microsoft	6.3.0.131
Nunit	Ett ramverk för enhetstestning av .NET-applikationer	NUnit Project	3.12.0.0
ONNX Runtime	Motor för modeller i formatet Open Neural Network Exchange (ONNX)	Microsoft	1.12.20220803.2.7048164
Open XML SDK	Tillhandahåller verktyg för att arbeta med Office Open XML-dokument	Microsoft	2.7.2
OSExtensions.dll	Bibliotek som tillhandahåller tillägg för operativsystemfunktioner	Microsoft	1.0.0.0
Otometrics.REMaccess	Otometrics abstraktionslager ovanpå Noah Inter-Module Communication Interface Library	GN Otometrics	1.0.0.10
Paket.Core.dll	En beroendehanterare med öppen källkod för .NET- och Mono-projekt	Paket Community (Open Source)	7.1.5.0

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Patagames.Pdf	C#-PDF-bibliotek för att skapa och redigera PDF-dokument i .NET-applikationer.	patagames.com	8.57.30.48
Patagames.Pdf.Wpf	C#-PDF-bibliotek för att skapa och redigera PDF-dokument i .NET-applikationer.	Patagames.com	4.19.18.48
Polly	Bibliotek som låter utvecklare uttrycka resiliens och hanteringsprinciper för transienta fel, såsom återförsök, kretsbytare, skottisolering och reservfunktion, på ett flytande och trådsäkert sätt.	App vNext	7.2.3.0
Portable.BouncyCastle	Detta är ett beroende för HIMSA Nibelung.CPD (Noahlink Wireless)	The Legion of the Bouncy Castle Inc	1.8.15362.1
Portable.BouncyCastle.Crypto	Detta är ett beroende för HIMSA Nibelung.CPD (Noahlink Wireless)	The Legion of the Bouncy Castle Inc	1.9.0.1
protobuf-net.dll	Serialiseringsramverk som används för RC-blob.	Open Source	2.3.2.0
Google.Protobuf	Googles officiella Protocol Buffers-bibliotek för .NET, som underlättar serialisering och deserialisering av strukturerade data.	Google Inc	3.19.3.0
Perfolizer.dll	Ett bibliotek med öppen källkod för prestandaanalys	Open Source	0.2.1.0
Rhino.Mocks.dll	Ett dynamiskt ramverk för mockobjekt i .NET	Rhino Mocks Community	3.6.0.0
Security.Cryptography.NetCore.dll	tillhandahåller kryptografiska funktioner för .NET Core-applikationer	HardDev	1.0.1.0
Serilog	Loggningskomponenten som används för hela Chinook-applikationen.	Serilog Contributors	3.0.1.0
Serilog.Enrichers.Thread	Berika Serilog-händelser med egenskaper från aktuell tråd	Serilog Contributors	3.1.0.0
Serilog.Extensions.Logging	Integrerar Serilog med Microsofts loggningsabstraktioner	Serilog Contributors	3.1.0.0
Serilog.Expressions	Uttrycksbaserad händelsefiltrering för Serilog.	Serilog Contributors	2.0.0.0
Serilog.Sinks.Console	En Serilog-sink som skriver logghändelser till konsolen/terminalen.	Serilog Contributors	4.0.0.0

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Serilog.Sinks.Debug	Serilog sink som skriver logghändelser till felsökningsfönstret.	Serilog Contributors	2.0.0.0
Serilog.Sinks.File	Skriv Serilog-händelser till textfiler i vanligt format eller JSON-format.	Serilog Contributors	4.1.0.0
Serilog.Sinks.NUnit.dll	Integreras med NUnit och dirigerar logghändelser till NUnits testutdata, vilket underlättar testdiagnostik.	Serilog Contributors	1.0.3.0
Serilog.Sinks.Trace	Serilog sink för diagnostisk spårning.	Serilog Contributors	2.1.0.0
Serilog.Settings.AppSettings	Stöd för XML-konfiguration (System.Configuration <appSettings>) i Serilog.	Serilog Contributors	2.2.2.0
Security.Cryptography.NetCore.dll	Utökningar av säkerhets-API:erna som medföljer .NET Framework	Microsoft	1.0.1.0
SharpBITS API	SharpBITS.NET är en .NET-wrapper för BITS API och en liten Windows UI-applikation för enklare åtkomst till BITS-uppladdningar och -nedladdningar.	perpetualKid	2.1.0.0
SharpZipLib	#ziplib (SharpZipLib, tidigare NzipLib) är ett Zip-, Gzip-, Tar- och Bzip2-bibliotek skrivet helt i C# för .NET-plattformen. Detta bibliotek tillhandahåller komprimeringsfunktioner (zip, unzip, stream compression, etc.). Vi använder det i appen Firmware Update.	Open Source	1.3.3.11
SharpDX	Används av LiveSwitch: SharpDX.Direct3D11, SharpDX.Direct2D1, SharpDX.Mathematics	Alexandre Mutel	4.0.1
SocketIOClient	Tillhandahåller en klient för Socket.IO som möjliggör dubbelriktad händelsebaserad kommunikation i realtid i .NET-applikationer	HeroWong	2.2.4.0
Superpower	Ett parserkombinatorbibliotek för C#	Datalust, Superpower Contributors, Sprache Contributors	2.3.0.0

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
SQLite.Interop	SQLite 3.36.0 Native Interop-bibliotek. SQLite är den databas som körs i processen och används för att lagra information om patienten (i fristående läge), vår produktkatalog och dess resurser samt metadata för anpassning, tillhör och His. SQLite är public domain.	SQLite Development Team	1.0.115
System Buffers	Tillhandahåller resurspoolning av valfri typ för prestandakritiska applikationer som ofta allokerar och avallokerar objekt.	Microsoft, dotnetframework	4.6.28619.01
System.Collections.Immutable	Används av biblioteken från Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	7.0.22.51805
System.ComponentModel.Annotations	Tillhandahåller attribut som används för att definiera metadata för objekt som används som datakällor.	Microsoft, dotnetframework	4.6.26515.06
System.Configuration.ConfigurationManager	Tillhandahåller typer som stöder användning av konfigurationsfiler.	Microsoft	5.0.20.51904
System.CodeDom.dll	Tillhandahåller klasser för att generera och kompilera källkod till körbara filer eller assemblyer	Microsoft	8.0.23.53103
System.Data.SQLite	Används av biblioteken från Sonova.HardwareAbstraction.Palio.Trafo	SQLite Development Team	1.0.115.0
System.Diagnostics.DiagnosticSource	Ett loggningsbibliotek som gör det möjligt för utvecklare att spåra och övervaka diagnostikdata	Microsoft	6.0.21.52210
System.Diagnostics.PerformanceCounter	Tillhandahåller API:er för interaktion med Windows prestandaräknare	Microsoft	7.0.22.51805
System.Drawing.Common	Ger åtkomst till GDI+-grafikfunktioner.	Microsoft	8.0.324.11603
System.Formats.Asn1.dll	Stöder kodning och avkodning av data i Abstract Syntax Notation One-format (ASN.1)	Microsoft	6.0.21.52210

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
System.IdentityModel.Tokens.Jwt	Innehåller typer som ger stöd för att skapa, serialisera och validera JSON Web Tokens. Används av komponenter som kommunicerar med backend-tjänster som använder JSON Web Tokens för autentisering.	Microsoft	6.8.0.11012
System.IO.Abstractions	En uppsättning abstraktioner som gör filsysteminteraktioner testbara.	Tatham Oddie & friends	12.0.10.46693
System.IO.Hashing.dll	Tillhandahåller hashfunktioner inom .NET, inklusive algoritmer för att beräkna kontrollsummor och kryptografiska hashvärden.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Möjliggör läsning och skrivning av paketfiler	Microsoft	6.0.21.52210
System.IO.Ports.dll	Tillhandahåller klasser för serieportskommunikation, vilket gör det möjligt för .NET-applikationer att interagera med maskinvara som är ansluten via serieportar.	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	En specialiserad HTTP-hanterare för Windows	Microsoft	6.0.422.16404
System.Numerics.Vectors	Tillhandahåller maskinvaruaccelererade numeriska typer som lämpar sig för högpresterande bearbetning och grafikapplikationer.	Microsoft, dotnetframework	4.6.26515.06
System.Memory	Tillhandahåller typer för effektiv representation och pooling av hanterade minnessegment, stackminnessegment och interna minnessegment samt sekvenser av sådana segment, tillsammans med primitiver för parsning och formatering av UTF-8-kodad text som lagras i dessa minnessegment.	Microsoft, dotnetframework	4.6.31308.01
System.Reactive.dll		Open Source	5.0.0.1
System.Reflection.DispatchProxy	Tillhandahåller en klass för att dynamiskt skapa proxytyper som implementerar ett angivet gränssnitt och härleds från en angiven DispatchProxy-typ. Metodanrop på den genererade proxyinstansen skickas till den DispatchProxy-bastypen.	Microsoft	4.700.20.21406

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
System.Reflection.Metadata	Det här paketet tillhandahåller en lågnivåläsare och -skrivare för .NET-metadata (ECMA-335). Det är optimerat för prestanda och är ett lämpligt val för att bygga bibliotek på högre nivå som ska tillhandahålla sina egna objektmodeller, exempelvis kompilatorer.	Microsoft	5.0.20.51904
System.Reflection.TypeExtensions	Tillhandahåller tilläggsmetoder för reflektions-API:et	Microsoft	4.700.19.56404
System.Runtime.CompilerServices.Unsafe	Tillhandahåller System.Runtime.CompilerServices.Unsafe-klassen, som tillhandahåller generisk lågnivåfunktionalitet för manipulering av pekare.	Microsoft, dotnetframework	6.0.21.52210
System.Security.AccessControl	Tillhandahåller basklasser som möjliggör hantering av åtkomst- och granskningskontrollistor för skyddsvärda objekt.	Microsoft	6.0.21.52210
System.Security.Permissions	Tillhandahåller typer som stöder Code Access Security (CAS).	Microsoft	5.0.20.51904
System.Security.Principal.Windows	Tillhandahåller klasser för att hämta den aktuella Windows-användaren och för att interagera med Windows-användare och grupper.	Microsoft	5.0.20.51904
System.Security.Cryptography.Cng.dll	Tillhandahåller kryptografisk funktionalitet med hjälp av API:er för Cryptography Next Generation (CNG)	Microsoft	5.0.20.51904
System.Security.Cryptography.Pkcs.dll	Tillhandahåller klasser för hantering av Public Key Cryptography Standards (PKCS), inklusive signerade och inkapslade data	Microsoft	6.0.1923.31806
System.Security.Cryptography.ProtectedData.dll	Tillhandahåller metoder för att skydda och ta bort skyddet från data med hjälp av Windows Data Protection API (DPAPI) för säker datalagring.	Microsoft	6.0.21.52210
System.Security.Cryptography.Xml.dll	Möjliggör XML-kryptering och digitala signaturer och stöder säker hantering av XML-data i .NET-applikationer.	Microsoft	6.0.822.36306

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
System.ServiceModel.Http.dll	Tillhandahåller HTTP-baserad kommunikationsfunktionalitet för Windows Communication Foundation-tjänster (WCF)	Microsoft	4.700.19.56502
System.ServiceModel.Primitives.dll	Innehåller grundläggande klasser för WCF-tjänster, inklusive basklasser och gränssnitt för tjänstekontrakt och kanaler.	Microsoft	4.700.19.56502
System.Text.Encoding.CodePages	Ger stöd för kodsidesbaserade kodningar, inklusive Windows-1252, Shift-JIS och GB2312.	Microsoft	5.0.20.51904
System.Text.Encodings.Web	Tillhandahåller typer för kodning och escape-strängar för användning i JavaScript, HyperText Markup Language (HTML) och URL (Uniform Resource Locators). Är ett beroende för SOUP-komponenten IdentityModel	Microsoft, dotnetframework	6.0.21.52210
System.Text.Json	Tillhandahåller högpresterande typer med låg allokering som serialiserar objekt till JavaScript Object Notation-text (JSON) och deserialiserar JSON-text till objekt, med inbyggt stöd för UTF-8. Tillhandahåller även typer för att läsa och skriva JSON-text kodad som UTF-8 samt för att skapa en skrivskyddad dokumentobjektmodell (DOM) i minnet för direktåtkomst till JSON-elementen i en strukturerad vy av data.	Microsoft	6.0.222.6406
System.Threading.Tasks.Extensions	Tillhandahåller ytterligare typer som förenklar arbetet med att skriva samtidig och asynkron kod.	Microsoft, dotnetframework	4.6.28619.01
System.Threading.Channels	Tillhandahåller en uppsättning datastrukturer för synkronisering och överföring av data mellan producenter och konsumenter, med stöd för högpresterande parallell programmering.	Microsoft	6.0.21.52210

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
System.ValueTuple	Tillhandahåller System.ValueTuple-strukturerna, som implementerar de underliggande typerna för tupler i C# och Visual Basic. Läger till stöd för värdetupler eftersom de endast ingår i senare versioner av .NET Framework.	Microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy.dll	Ett ramverk för beteendedriven utveckling (BDD) för .NET	TestStack Community	4.3.2.0
Thrift	Används för definition av fjärrlänkprotokoll	Apache	0.13.0.0
Unity.Container	Unity Container (Unity) är en fullfjädrad, utökningsbar container för beroendeinjektion.	Unity Container Project	5.8.13.0
Unity.Configuration	Unity Container (Unity) är en fullfjädrad, utökningsbar container för beroendeinjektion.	Unity Container Project	5.2.5.0
Unity.Abstractions	Unity Container (Unity) är en fullfjädrad, utökningsbar container för beroendeinjektion.	Unity Container Project	3.3.1.0
Unity.Interception.Configuration	Unity Container (Unity) är en fullfjädrad, utökningsbar container för beroendeinjektion.	Unity Container Project	5.1.7.0
Unity.Interception	Unity Container (Unity) är en fullfjädrad, utökningsbar container för beroendeinjektion.	Unity Container Project	5.5.5.0
Unity.Registration.ByConvention	Unity Container (Unity) är en fullfjädrad, utökningsbar container för beroendeinjektion.	Unity Container Project	2.1.9.0
Unity.ServiceLocation	Unity Container (Unity) är en fullfjädrad, utökningsbar container för beroendeinjektion.	Unity Container Project	2.1.2.0
WAP BT Dongle Driver	WAP BT-dongeldrivrutin (anpassningsdongel)	iAnywhere Solutions	3.0.0.6095
WebSync	Används för integration av anpassningsdatakanaler	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor.dll	En hexadecimal redigeringskontroll för WPF-applikationer	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	Ett verktygsbibliotek för WPF-applikationer som tillhandahåller information om skärmar och bildskärmar	FM (Frozen Mountain)	2.1.0.0

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Xceed Extended WPF Toolkit	En samling WPF-kontroller och verktyg som utökar WPF-applikationer med ytterligare UI-komponenter.	Xceed	3.5.0.0
xmlunit-core.dll	Ett bibliotek för att testa och jämföra XML-utdata.	XMLUnit Community	2.9.0.205
Xps to Pdf render (NiXPS)	Konverterar XPS-filer programmatiskt till PDF; används i rapporter från anpassningsapplikationen.	NiXPS	2.6.7.0

14. REFERENSER

Titel	Webbplats
Bruksanvisning (elektronisk)	https://ifu.advancedbionics.com/
Advanced Bionics globala integritetspolicy	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

 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

Du hittar fler kontaktuppgifter på
advancedbionics.com/contact

AB – A Sonova brand

Kontakta din lokala AB-representant för regulatoriskt godkännande och
tillgänglighet i din region.

Bluetooth®-ordmärket och logotyperna är registrerade varumärken som ägs av
Bluetooth SIG, Inc. All användning av sådana märken av Sonova AG sker under
licens.



029-S398-09