Target CI v1.5

CYBERSÄKERHETSGUIDE

Svenska

Uppdaterad: september 2025

A Sonova Brand

Innehåll

1. INLEDNING

Detta dokument innehåller teknisk säkerhets- och sekretessinformation om programvarusystemet Target CI v1.5 från Advanced Bionics, nedan kallat “anpassningsprogramvara”. 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 integritetsöverväganden som är relevanta vid användningen av anpassningsprogramvaran. Den 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 säkerhets- och sekretessinformation om:

- Tidigare versioner av AB-anpassningsprogramvara
- Annan AB-programvara än Target CI v1.5
- AB-webbplatser
- AB-mobilapplikationer
- AB-hörapparater

1.1 FÖRKORTNINGAR OCH DEFINITIONER:

Akronym	Term
FSW (Fitting software)	Anpassningsprogramvara
Audionom	Audionom
SaMD (Software as a Medical Device)	Programvara som medicinteknisk produkt
AB	Advanced Bionics
IFU (Instructions For Use)	Bruksanvisning

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 dedikerad professionell support är tillgänglig måndag till fredag från kl. 5.00 till kl. 17.00 Stillahavstid.

För den som befinner sig utanför USA och Kanada finns det regional teknisk support. 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 v1.5 är tillgänglig på begäran. Guiden ger teknisk information om installationsprogrammet för anpassningsprogramvaran, inklusive kommandoradsalternativ för tysta och automatiserade installationer.

2.4 MDS2

Tillverkarens uttalande om säkerhet inom medicinteknisk utrustning (MDS2) är ett branschstandardformulär som innehåller svar om säkerhet och integritet gällande AB:s anpassningsprogramvara. Blanketten finns tillgänglig på begäran.

2.5 BRUKSANVISNING

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
- Installationsanvisningar
- Teknisk support

2.6 HIMSA

HIMSA är en tredjepartsleverantör av mjukvara som producerar Noah System 4, ett mjukvarusystem utformat för hörselvårdsbranschen. Systemet förser audionomer med ett leverantörsoberoende system för att utföra klientrelaterade uppgifter.

Anpassningsprogramvaran kan valfritt konfigureras för att använda Noah System 4 för datalagring istället 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/

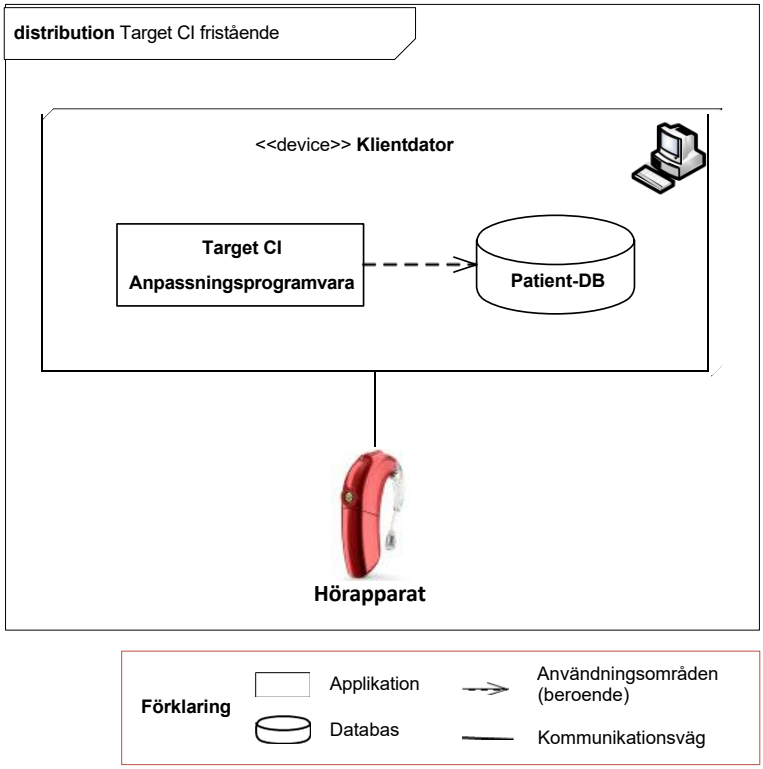
Se säkerhetsavsnittet i HIMSA Learning Center för ytterligare säkerhetsinformation: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

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 operativsystem.

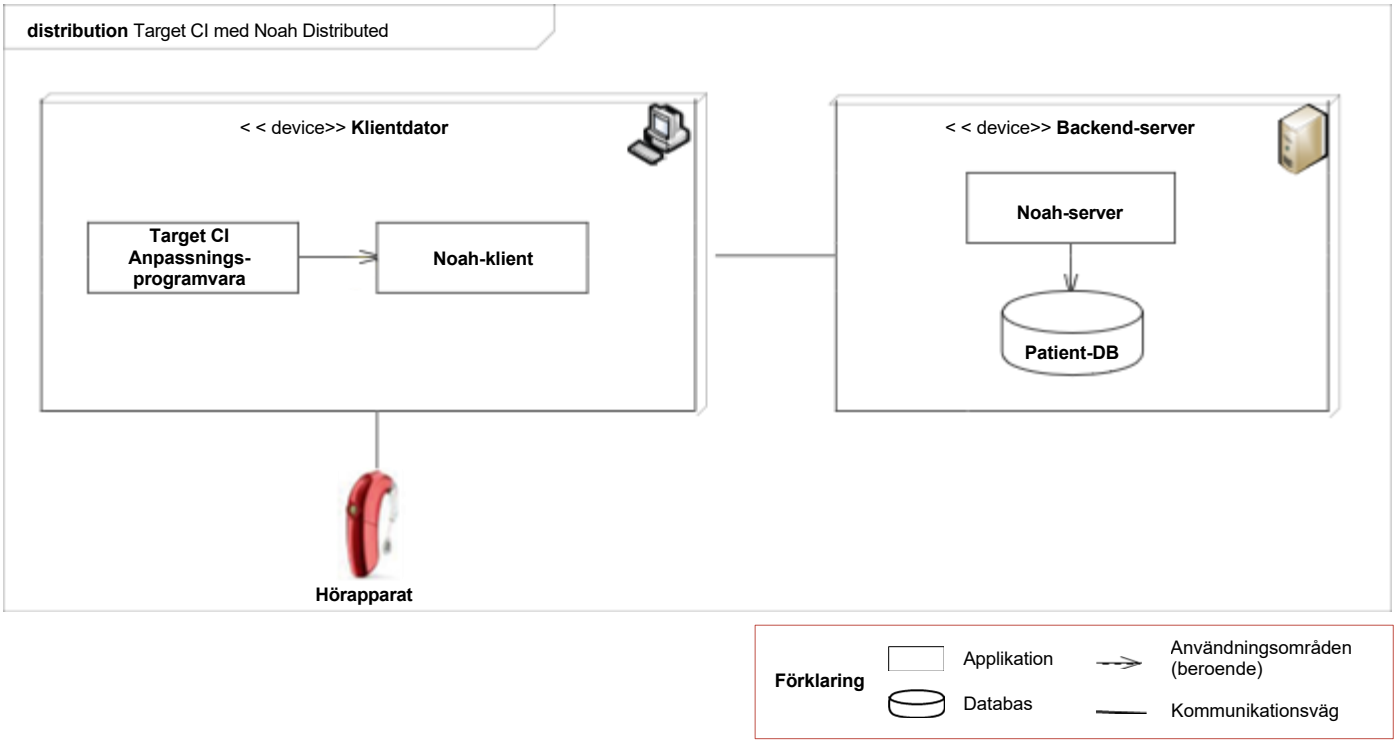
3.1 DISTRIBUTIONSMODELL 1: FRISTÅENDE

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



3.2 DISTRIBUTIONSMODELL 2: NOAH-DISTRIBUERAD

Med Noah Distributed-distributionsmodellen distribueras anpassningsprogramvaran till en eller flera klientdatorer. 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.

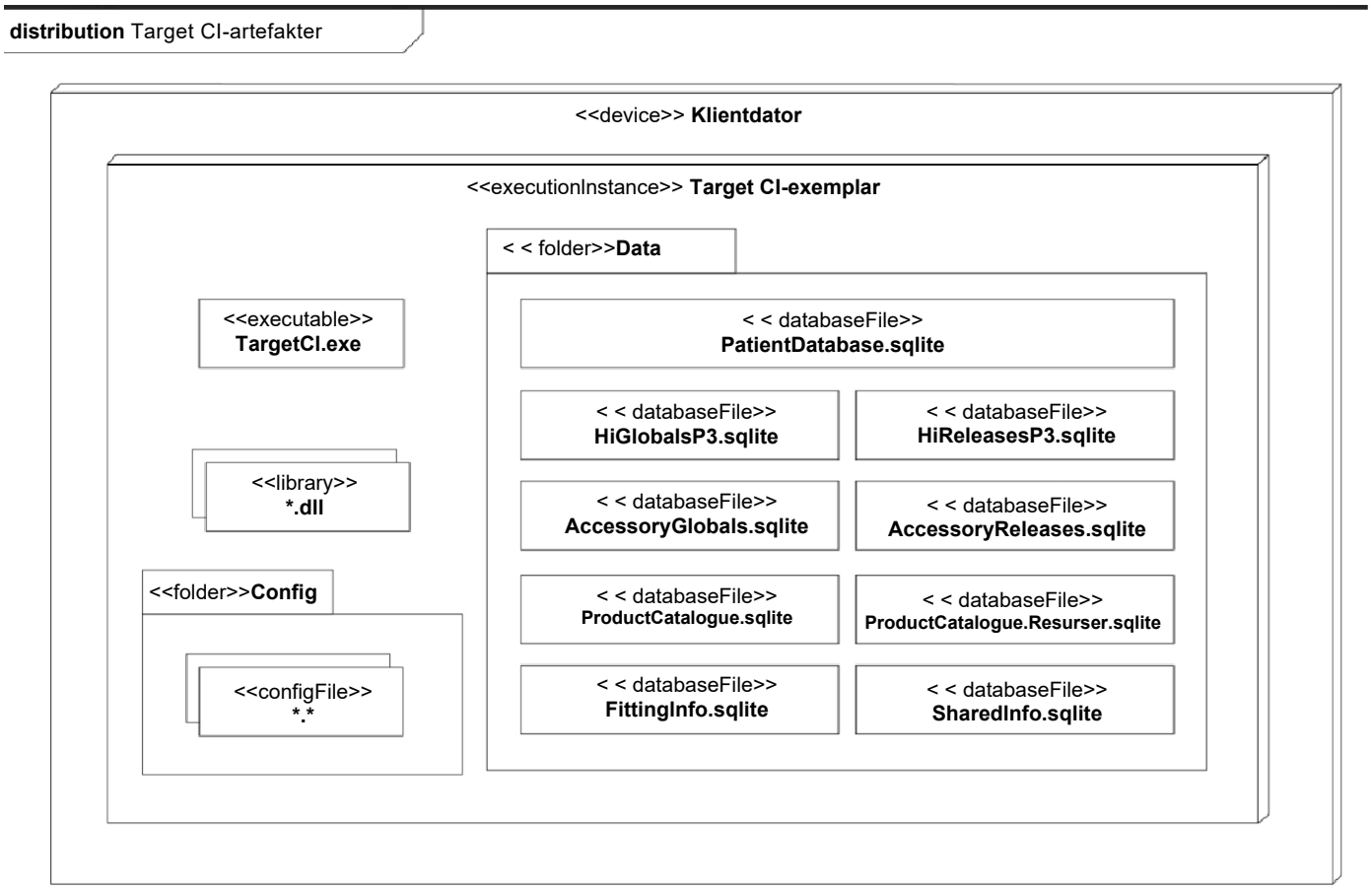


3.3 DISTRIBUTIONSARTEFAKTER

Anpassningsprogramvaran installeras med en körbar fil och en uppsättning associerade 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.” Datamappen innehåller en enda transaktionsdatabasfil och flera informationsdatabasfiler.

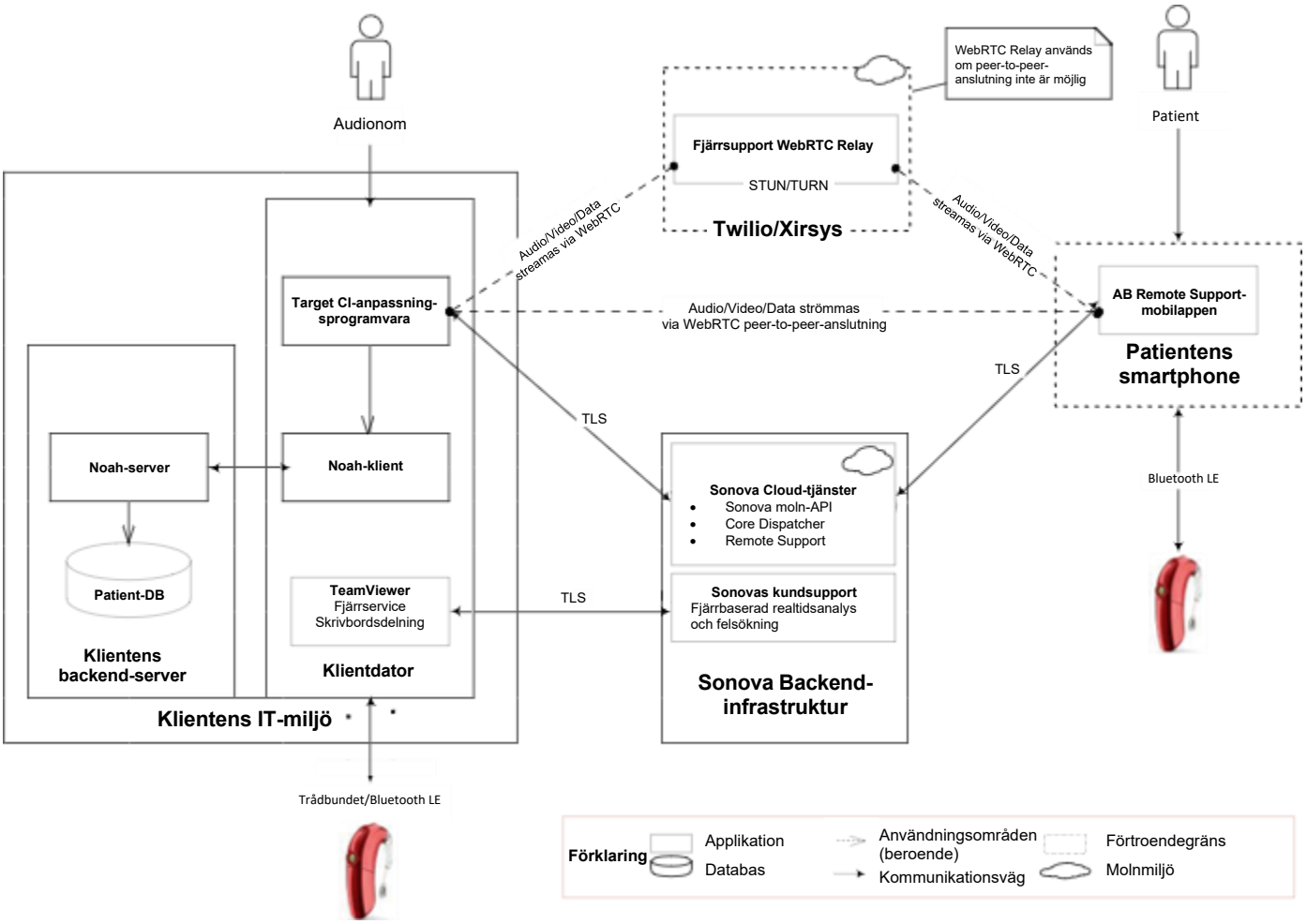
Transaktionsdatabasen PatientDatabase.sqlite lagrar patientens demografiska uppgifter och anpassningsdata och installeras endast när anpassningsprogramvaran distribueras i fristående läge.

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.



3.4 SYSTEMSAMMANKOPPLINGAR

Diagrammet och tabellen nedan illustrerar de primära systemsammankopplingarna. Vanligtvis utnyttjas endast en del av de tillgängliga sammankopplingarna.



Källa/ Destination	Tjänst	Protokoll	Port	Beskrivning
Hörapparater	Hörapparats-kommunikation	Trådbunden anslutning / Bluetooth® lågenergi	Ej tillämpligt	Används för att kommunicera med hörapparater för kontroll, konfiguration samt status- och dataavläsningsändamål
Noah	Noah 4 ModuleAPI	.NET Remoting	Ej tillämpligt	Primärt gränssnitt för modulen som används för att komma åt Noah-programvaran (endast i Noah distributed distributionsmodell)
Sonova Cloud-tjänster	Sonova Cloud API, Core dispatcher, Remote support	SOAP, REST	443	Sonova-tjänster som finns i ett Microsoft Azure-datacenter används för att: • hämta anpassningsprogramvarans klientkonfigurationsdata från Sonovas backend-lagring

Källa/ Destination	Tjänst	Protokoll	Port	Beskrivning
				• överföringsloggning och analysdata • upprätta fjärranpassningssessioner i realtid
Twilio/Xirsys, AB Remote Support mobilapp	Remote Support	WebRTC	Lista över portar tillgängliga på begäran	Twilios molnkommunikationstjänster finns på tredjeparts-molnplattformar, närmare bestämt Amazon Web Services (AWS) och Google Cloud Platform (GCP). Dessa tjänster används uteslutande av fjärrsupportfunktionen i anpassningsprogramvaran, vilket möjliggör WebRTC-signalering och fjärranpassningssessioner i realtid.
AB:s kundsupport	Skrivbordsdelning	TeamViewer proprietärt protokoll	5938, 443, 80 Se TeamViewerPorts	Används för att utföra realtidsanalys och felsökning av problem som påverkar installationer av anpassningsprogramvara. Se avsnitt 6.6 FJÄRRSERVICE för merinformation.

4. SYSTEMKRAV

Operativsystem	64-bitars Windows 10 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 4.14 eller senare)
Internetanslutning	Internetanslutning krävs för fjärrsupport och analysloggning, se avsnitt 4.4 Systemanslutningar; intranät krävs vid användning av nätverksanslutet Noah System 4.
Nätverksportar	Se avsnitt 3.4 Systemsammankopplingar; se avsnitt 3. Andra resurser — HIMSA för portar som används av Noah System 4.

5. INSTALLATION

5.1 KRAV

Ett administratörskonto krävs för att installera anpassningsprogramvaran. När programvaran är installerad kan den köras utan administratörsbehörighet eller förhöjda behörigheter.

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

Innan installationen rekommenderas systemadministratörer att säkerställa att:

• Den version av anpassningsprogramvaran som ska installeras är den senaste tillgängliga.

• Det underliggande operativsystemet är uppdaterat.

5.2 TYPER AV INSTALLATIONSPROGRAM

Det finns två installationsprogram för att installera anpassningsprogramvaran:

• Standardinstallationsprogrammet

• IT Professional-installationsprogrammet

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-paketen.

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 AB:s kliniska representant. IT Professional-installationsprogrammet kan inte användas för att reparera, ominstallera eller avinstallera installationer av standardinstallationsprogrammet. Standardinstallationsprogrammet kan inte användas för att reparera, ominstallera eller avinstallera installationer av IT Professional-installationsprogrammet.

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 AUTENTISERING – FRISTÅENDE DISTRIBUTION

När anpassningsprogramvaran installeras som en fristående applikation förlitar den sig på de åtkomstkontrollmekanismer som tillhandahålls av värddatorns operativsystem. Värddatorns operativsystem kan konfigureras av kundens IT-personal för att hantera autentisering. Anpassningsprogramvaran har ingen sådan integrerad funktion. Advanced Bionics rekommenderar att varje användare loggar in på värddatorns operativsystem med ett unikt konto per användare.

6.2 AUTENTISERING – NOAH-DISTRIBUTION

När anpassningsprogramvaran installeras som en Noah-modul tillhandahålls åtkomstkontroll av Noah System 4. Se www.HIMSA.com för granskningskontroller som används av Noah System 4.

6.3 AUTENTISERING

Anpassningsprogramvaran begränsar inte åtkomsten till sina funktioner baserat på enskilda användares roller. Programvaran stöder en enda huvudfunktion för att anpassa patienters hörapparater och en enda roll som anpassande audionom. Rollbaserade åtkomstkontroller är inte tillämpliga.

6.4 GRANSKNING – FRISTÅENDE DISTRIBUTION

När anpassningsprogramvaran installeras som en fristående applikation förlitar den sig på de granskningsmekanismer som tillhandahålls av värddatorns operativsystem. Anpassningsprogramvaran har ingen sådan integrerad funktion. Värddatorns operativsystem kan konfigureras av kundens IT-personal för att logga start/användning av anpassningsprogramvaran och användarinloggningar. Advanced Bionics rekommenderar att varje användare loggar in på värddatorns operativsystem med ett unikt konto per användare för att underlätta granskning.

6.5 GRANSKNING – NOAH-DISTRIBUTION

När anpassningsprogramvaran installeras som en Noah-modul tillhandahålls granskningsloggar av Noah-systemet. Se https://www.himsa.com/ för granskningskontroller som används av Noah System 4.

6.6 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 kommunicera sina TeamViewer ID-inloggningsuppgifter till AB Support-teamet via en extern kommunikationskanal (t.ex. telefonsamtal).

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

All nätverkstrafik för skrivbordsdelning är säkrad och uppfyller eller överträffar kryptografiska protokoll och algoritmstandarder (utbyte av öppna/privata RSA-nycklar och AES 256-bitars sessionskryptering).

TeamViewer QuickSupport kan tas bort manuellt utan att det påverkar andra funktioner i Target FSW. Installationsprogrammet för Target FSW stöder en kommandoradsparameter för att tillåta en kommandoradsinstallation av Target FSW utan att inkludera TeamViewer QuickSupport-verktyget.

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 varken lagrar, säkerhetskopierar eller har åtkomst till data som lagras i anpassningsprogramvaran eller Noah-databaserna, såvida inte informationen uttryckligen skickas till Advanced Bionics.

7.2 FEDERALA STANDARDER FÖR INFORMATIONSBEARBETNING (FIPS)

Target CI v1.5 är kompatibel med FIPS 140-2 krypteringsstandarder.

7.3 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 säkerhetsrekommendationer som dokumenterats i BCP 195 – Rekommendationer för säker användning av TLS och DTLS, BCP195 inklusive:

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

DTLS

Kryptering är en obligatorisk funktion i WebRTC och tillämpas på alla mediestreams som skickas via WebRTC. Vilket krypteringsprotokoll som används beror på kanaltypen; datastreams krypteras med DTLS och mediastreams krypteras med SRTP (Secure Real-time Transport Protocol) eftersom det är ett lättare alternativ än DTLS.

Se följande länk för mer detaljerad information om säkerhetskonfiguration av 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 hörapparatens Bluetooth-parkopplingsläge tidsbegränsat. Se tillgänglig dokumentation för hörapparater för en mer detaljerad beskrivning av säkerheten för Bluetooth-kommunikationskanalen.

7.4 SÄKERHET I VILOLÄGE

Patientdatabas – Fristående distributionsmodell

Om anpassningsprogramvaran installeras som ett fristående program lagras patientdatabasen lokalt på: C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

Dessa poster krypteras inte som standard i viloläge. Skyddad hälsoinformation (PHI) och personligt identifierbar information (PII) lagras i en databas som är intern i anpassningsprogramvaran och överförs inte via nätverket.

I vissa jurisdiktioner kan föreskrifter kräva att all 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 hårddisken och kräver autentisering för åtkomst. Konsultera alltid Microsofts officiella riktlinjer och din organisations IT-säkerhetspolicy innan du aktiverar BitLocker.

Hur man aktiverar 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-nyckel

   Följ Microsofts riktlinjer för bästa praxis och din organisations IT-säkerhetspolicy när du väljer upplåsningsmetod.

4. Säkerhetskopiera återställningsnyckeln

   Säkerhetskopiera återställningsnyckeln med säkra, företagsgodkända metoder. Rekommenderade alternativ inkluderar:

   - Lagring i Microsoft Entra ID (tidigare Azure AD) eller Active Directory för domänanslutna enheter

   - Spara till en säker, åtkomstkontrollerad nätverksplats med kryptering och granskningsloggning

   - Använda en hanterad nyckeldepositionslösning som godkänts av din organisation

   Undvik att spara nyckeln på lokala enheter, USB-minnen eller skriva ut den om det inte uttryckligen är tillåtet enligt policyn. Återställningsnycklar måste skyddas med samma rigorösa egenskaper som andra känsliga inloggningsuppgifter och omedelbart roteras om de exponeras.

5. Starta kryptering

   Välj:

   - Hela hårddisken – rekommenderas för de flesta företag. 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. Personlig information och andra patientdata hanteras av Noah-programvaran och krypteringen av patientens vilande data säkerställs av Noah-systemet. Anpassningsprogramvaran kan skicka/ta emot PII via en trådbunden eller trådlös nätverksanslutning när en Noah-databas konfigureras för nätverksåtkomst.

Personlig information som lagras i den nätverksanslutna Noah-databasen kommer att vara synlig för andra enhetsanvändare på olika datorer som har behörighet till samma nätverksanslutna databas. Noah-databasen kan också konfigureras för åtkomst utanför nätverket och installeras på samma dator som anpassningsprogramvaran.

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

Se avsnittet www.HIMSA.com för krypteringsstandarder som används av Noah System 4.

RMA-exportfiler

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

RMA-filen är asymmetriskt RSA-krypterad med en nyckellängd på 512 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 är personlig lagras med PBKDF2-kryptering med en 128-bitars nyckel.

Anpassningsprogramvaran kan skicka/ta emot opersonlig klientinformation till/från en hörapparat via en egenutvecklad trådbunden enhet (t.ex. CPI-3), AB Remote Support mobilapplikation eller NoahLink Wireless-enhet. Den trådlösa Noahlink -enheten ansluter till hörapparaten med Bluetooth Low Energy (BLE) via en standard BLE 128-bitars AES-krypterad kanal.

8. PROGRAMVARANS INTEGRITET

8.1 VERIFIERING AV NEDLADDADE INSTALLATIONSMEDIA

Installationsmedia för Target CI-anpassningsprogramvaran kan i vissa regioner laddas ner från Advanced Bionics Pro Portal eller Sonova Web Client. Nedladdade installationsmedia kan autentiseras med hjälp av valfritt betrott SHA-256-hashverktyg.

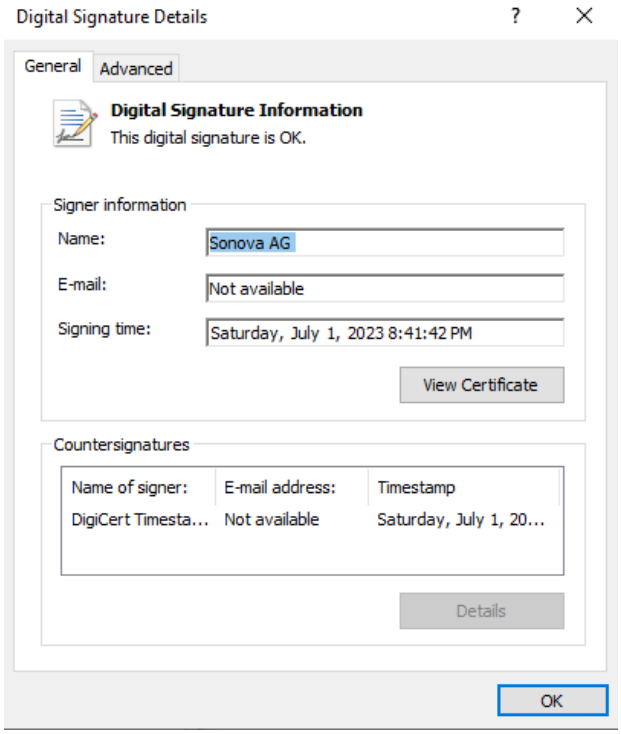
SHA256-hashen för standardinstallationens zip-fil är:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

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 installationsmedia för anpassningsprogramvaran. Om ditt installationsmedium är ett USB-minne, sätt in det i en USB-port och navigera till dess rotmapp. Om ditt installationsmedium är en zip-fil, packa upp den till en mapp och navigera till den mappen.
2. Högerklicka på SonovaVerify.exe och välj Egenskaper från snabbmenyn.
3. Välj fliken Digitala signaturer.
4. Dubbelklicka på SHA256 “Sonova AG”-signaturen.
5. Kontrollera att elementen i signaturen är giltiga. Kontrollera särskilt att meddelandet “The digital signature is OK.” (Den digitala signaturen är OK) visas långt upp och att undertecknarens namn och signeringstid matchar följande bild:



1. Stäng popup-dialogrutorna och dubbelklicka på SonovaVerify.exe.
2. Kontrollera att “NO ERRORS DETECTED” (INGA FEL UPPTÄCKTA) visas enligt följande bild:

Bilden visar att SonovaVerify har autentiserat och verifierat digitala signaturer för alla filer på installationsmediet, inklusive installationsprogrammet. Detta verifierar att installationsmediet inte har manipulerats, skadats eller på annat sätt äventyrats. SonovaVerify visar varningar eller felmeddelanden om filer eller mappar saknas, eller om oväntade filer eller mappar har lagts till i installationsmediet.

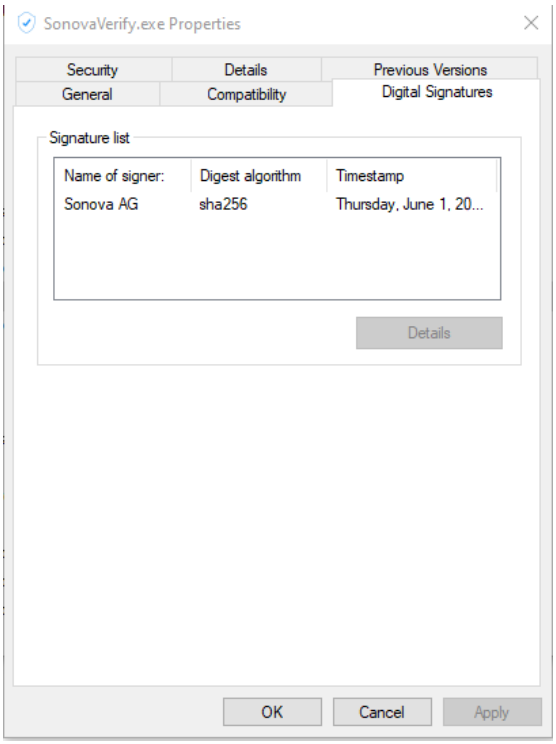
8.3 AUTOMATISK VERIFIERING AV DEN INSTALLERADE ANPASSNINGSPROGRAMVARANS INTEGRITET

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 kompromitterats.

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 anpassningsprogramvarans körbara mapp, vanligtvis i: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Högerklicka på SonovaVerify.exe och välj Egenskaper från snabbmenyn.
3. Välj fliken Digitala signaturer.
4. Dubbelklicka på SHA256 “Sonova AG”-signaturen.
5. Kontrollera att elementen i signaturen är giltiga, särskilt att meddelandet “The digital signature is OK.” (Den digitala signaturen är OK) visas långt upp och att undertecknarens namn och signeringstid matchar följande bild:



1. Stäng popup-dialogrutorna och dubbelklicka på SonovaVerify.exe.
2. Kontrollera att “NO ERRORS DETECTED” (INGA FEL UPPTÄCKTA) visas enligt följande bild:

Bilden visar att SonovaVerify har autentiserat och verifierat digitala signaturer för alla installerade programfiler. Detta verifierar att anpassningsprogramvaran inte har manipulerats, skadats eller på annat sätt äventyrats. SonovaVerify visar varningar eller felmeddelanden om filer eller mappar saknas, eller om oväntade filer eller mappar har lagts till i programfilmappen.

9. PROGRAMVARUPATCHAR OCH UPPDATERINGAR

Automatiska uppdateringar stöds inte.

10. DATAHANTERING

10.1 DATABASER

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 maskin som anpassningsprogramvaran och tillhandahåller lagring för patientdata. För att säkerhetskopiera programdata när Target CI distribueras som ett fristående program, skapa en säkerhetskopia av hela mappen som finns på %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Skydda säkerhetskopior 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 åtkomst utanför nätverket och installeras på samma dator som anpassningsprogramvaran. Konfigurera Noah-databasens kryptering för att skydda data (se HIMSA-dokumentationen).

För Noah-distributionsläget, se följande länk för instruktioner om säkerhetskopiering och återställning av Noah-patientdatabasen:

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 enhetskonfiguration och inställningar.

10.4 BORTTAGNING AV DATA

Instruktioner för borttagning av data finns i bruksanvisningen eller på följande webbplats för Noah-distribution: 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, vilket inkluderar, men inte är begränsat till, hörselanordningens användare, föräldrar eller vårdnadshavare till barn som använder hörselanordningar, vårdpersonal, IT-administratörer, hörselvårdsinrättningar och leverantörer, leverantörer av hörselanordningar och programmeringsutrustning.

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

OS-nivå

- Tillämpa åtkomstkontroller på OS-nivå, t.ex.:
  - Ta bort gästkonton
  - Aktivera Windows-användarinloggningen
  - Upprätthåll en lista över behöriga operatörer för att kontrollera åtkomst till systemet
  - Ange anpassade användare och roller
  - Tillämpa krav på starka lösenord och håll inloggningsuppgifter hemliga
- Tillämpa granskningskontroller på OS-nivå
- Håll operativsystemet uppdaterat.
- Håll den installerade versionen av anpassningsprogramvaran uppdaterad.
- Aktivera uppdaterat skydd mot skadlig kod och antivirusprogram
- Aktivera vitlistning av appar

Dataskydd

- Kryptera patientdata med hjälp av tredjepartsverktyg eller kontroller på operativsystemnivå, t.ex. genom att använda hårddiskkryptering (t.ex. gratisversionen av Microsoft BitLocker) för att skydda alla data. För Noah-distribution, överväg att använda Noah-databaskryptering.
- Externa medier som innehåller data som exporterats från anpassningsprogramvara, inklusive rapporter och loggar, bör säkras. När informationen inte längre används bör den raderas på ett säkert sätt och/eller mediet bör raderas på ett säkert sätt.
- Använd USB-lagringsmedia med inbyggd säkerhetsfunktionalitet, som krypterade USB-enheter med integrerad knappsats.
- Se till att alltid förvara data säkert:
  - När du överför data via osäkra kanaler, skicka antingen anonyma data eller kryptera dem.
  - Skydda säkerhetskopior inte bara mot dataförlust utan även mot stöld.
  - Ta bort alla data från datamedier som inte längre används eller som ska kasseras.

- Godkända procedurer och verktyg bör användas av användare för säker borttagning av data som lagras på flyttbara medier, i enlighet med gällande föreskrifter och riktlinjer för hantering av patientinformation/personligt identifierbar information (PII)/skyddad hälsoinformation (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 installeras bör vara fysiskt säkrad på ett sätt som inte gör den tillgänglig för obehöriga användare.
- Säkerställ att obehörig personal inte manipulerar systemet.
- Åtkomst till skrivare som är anslutna till arbetsstationen bör kontrolleras.
- Skärmen på arbetsstationen där anpassningsprogramvaran installeras bör placeras på ett sätt som begränsar synligheten av skärminnehållet till användaren.

Organisationsnivå

- Endast professionellt utbildad, fullt kvalificerad personal är behörig att använda systemet. Innan någon får tillstånd att använda systemet bör det kontrolleras att personen har läst och helt förstår bruksanvisningen som medföljer anpassningsprogramvaran.
- Om du upptäcker någon misstänkt aktivitet i dina konton för anpassningsprogramvaran eller någon oväntad åtgärd, 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 för anpassningsmiljön där anpassningsprogramvaran kommer att användas på olika nivåer, se

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

12. TILLVERKNINGS- OCH PROGRAMVARUUTVECKLINGSPROCESS

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 nationella sårbarhetsdatabas (NVD) bedöms och åtgärdas under utvecklingsprocessen och övervakas när anpassningsprogramvaran har släppts på marknaden.

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
ciAD Hearingloss Simulator	Hörselnedsättningssimulatorbibliotek för mediaspelare	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	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
Destructurama.Attributed	Används av Nephele-bibliotek.	Serilog Contributors	3.0
DirectShow 2005	Ger åtkomst till Microsofts DirectShow-funktion inifrån .NET-applikationer.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	National Centre for Audiology, Kanada	4.2
DSL5	DSL 5 Fitting formula library	National Centre for Audiology, Kanada	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical ompackat för Sonova	GNOtometrics	2.0.1.9
IceLink	Används för WebRTC-audio/video-konferensintegration	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect & OAuth 2.0 klientbibliotek som används av Kona.CommonServices.Authentication-komponent för OAuth 2-autentisering.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Noah Inter-Module Communication Interface Library	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Används av bibliotek från Sonova för att kommunicera med Git	LibGit2Sharp contributors	0.26.1
Mapster	Används för att mappa objekt i kod	chaowlert,eric_swann	7.2.0.0
MathNet.Numerics	Används för anpassningsalgoritmer (signalväg, målmatchning etc.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael och bidragsgivare	4.11.0
Microsoft.Bcl.AsyncInterfaces	Tillhandahåller IAsyncEnumerable < T> och IAsyncDisposable-gränssnitt och hjälptyper för .NET Standard 2.0.	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	Används av biblioteken som kommer från Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Används av biblioteken som kommer från Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Microsoft.Identity.Client	MSAL-biblioteket för .NET är en del av Microsofts identitetsplattform för utvecklare (tidigare kallat Azure AD) v2.0. Det gör att du kan hämta säkerhetstokens för att anropa skyddade API:er. Den 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
Microsoft.IdentityModel.Logging	Beroende av Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Beroende av SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
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 dina WPF-applikationer med minimal kod.	xamlexperienceteam, Microsoft	1.0.1
MS VC++ 2008 Redistributable	Microsoft Visual C++ 2008 Redistributable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Visual C++ 2010 Redistributable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistributable	Microsoft Visual C++ 2012 Redistributable	Microsoft	11.0.61030.0
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
MS-VisualC++ 7.1 runtime-bibliotek	Microsoft Visual C++ runtime-bibliotek	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1 Fitting formula library	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting formula library	Australian Hearing	2.0.11
NAudio.dll	Används för att justera volymen och spela upp ljudfiler.	Open Source	1.9
.NET Framework	.NET-miljö	Microsoft	4.8.3928.0
Newtonsoft.Json	Används för JSON-serialisering och avserialisering.	James Newton-King	12.0.3

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Nibelung	NoahLink Wireless-anpassningsbibliotek	GN ReSound	1.3.16.1
Nlog	Beroende av HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	4.4.0
NoahLink	Drivrutin för NoahLink-anpassningsenhet	HIMSA	1.55.6.166
NoahLink Wireless	Drivrutin för NoahLink Wireless-anpassning	HIMSA	2.0.0.68
Otometrics.HiPro2	HiPro-kommunikationsbibliotek	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Otometrics abstraktionslager över Noah Inter-Module Communication Interface Library	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	C# PDF-bibliotek för att skapa och redigera PDF-dokument i .Net-applikationer.	Patagames.com	4.54.2704.0
Polly	Bibliotek som låter utvecklare uttrycka resiliens och hanteringsprinciper för transienta fel, såsom återförsök, kretsbrytare, skottisolering och reservfunktion, på ett flytande och trådsäkert sätt.	App vNext	7.2.1
Polly.Extensions.Http	Ett bibliotek som innehåller noggrant utformade metoder för att konfigurera Polly-policyer för att hantera övergående fel som är typiska för anrop via HttpClient.	App vNext	3.0
Polly.Contrib.WaitAndReply	Ett bibliotek för Polly som innehåller hjälpmetoder för en mängd olika vänta-och-försök-igen-strategier.	Grant Dickinson, App vNext	1.1.1
Portable.BouncyCastle	Detta är ett beroende av HIMSA Nibelung.CPD (Noahlink Wirlesss)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Serialiseringsramverk som används för RC blob.	Open Source	2.0.0.668
Serilog	Loggningskomponenten som används för hela Chinook-applikationen.	Serilog Contributors	2.10.0
Serilog.Enrichers.Thread	Enrich Serilog-händelser med egenskaper från aktuell tråd	Serilog Contributors	3.1
Serilog.Expressions	Uttrycksbaserad händelsefiltrering för Serilog.	Serilog Contributors	2.0
Serilog.Sinks.Console	En Serilog-sink som skriver logghändelser till konsolen/terminalen.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	Serilog sink som skriver logghändelser till felsökningsfönstret.	Serilog Contributors	2.0
Serilog.Sinks.File	Skriv Serilog-händelser till textfiler i vanligt format eller JSON-format.	Serilog Contributors	4.1
Serilog.Sinks.Trace	Serilog sink för diagnostisk spårning.	Serilog Contributors	2.1

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
Serilog.Settings.AppSettings	XML-konfiguration (System.Configuration < appSettings>) stöd för Serilog.	Serilog Contributors	2.2.2
Security.Cryptography	Utökningar av säkerhets-API:erna som levereras med .NET-ramverket	Microsoft	1.7.2
SharpBITS API	SharpBITS.NET är en .NET-wrapper för BITS API och ett litet Windows UI-program för enklare åtkomst till BITS-upp- 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 den i appen Firmware Update.	Open Source	1.1.0.145
Superpower	Ett parserkombinatorbibliotek för C#	Datalust,Superpower Contributors,Sprache Contributors	2.3
SQLite.Interop	SQLite är ett programbibliotek som tillhandahåller ett relationsdatabashanteringssystem. Lite i SQLite betyder låg vikt när det gäller installation, databasadministration och nödvändiga resurser. SQLite har följande märkbara funktioner: fristående, serverlös, nollkonfigurationsbaserad, transaktionell. Det är en databas (SQLite 3.32.1) för att lagra information om patienten (i fristående läge), våra produktkatalogresurser och metadata för anpassning, tillbehör och HIs.	SQLite Development Team	1.0.113
System.Buffers	Tillhandahåller resurspooler av alla typer för prestandakritiska applikationer som allokerar och avallokerar objekt ofta.	23rogramma,dotnetframework	4.5.1
System.Collections.Immutable	Används av biblioteken som kommer från Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0
System.ComponentModel.Annotations	Tillhandahåller attribut som används för att definiera metadata för objekt som används som datakällor.	23rogramma,dotnetframework	4.7
System.Configuration.ConfigurationManager	Tillhandahåller typer som stöder användning av konfigurationsfiler.	Microsoft	5.0
System.Data.SQLite.Core	Används av biblioteken som kommer från Sonova.HardwareAbstraction. Palio.Trafo	SQLite Development Team	1.0.113.7
System.Drawing.Common	Ger åtkomst till GDI+ grafikfunktioner.	Microsoft	5.0.1

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
System.IO.Abstractions	En uppsättning abstraktioner som gör filsysteminteraktioner testbara.	Tatham Oddie & friends	12.0.10
System.Numerics.Vectors	Tillhandahåller hårdvaruaccelererade numeriska typer, lämpliga för högpresterande bearbetning och grafikapplikationer.	24rogramma,dotn etfra me work	4.5
System.Memory	Tillhandahåller typer för effektiv representation och poolning av hanterade, staplade och ursprungliga minnessegment och sekvenser av sådana segment, tillsammans med primitiver för att parsning och formatering av UTF-8-kodad text lagrad i dessa minnessegment.	24rogramma,dotn etfra me work	4.5.4
System.Reactive.Core	Reactive Extensions (Rx) för .NET	.NET Foundation	3.1.1
System.Reactive. Interfaces	Reactive Extensions (Rx) för .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Reactive Extensions (Rx) för .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Reactive Extensions (Rx) för .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Reactive Extensions (Rx) för .NET	.NET Foundation	3.1.1
System.Reflection.DispatchProxy	Tillhandahåller en klass för att dynamiskt skapa proxytyper som implementerar ett angivet gränssnitt och härleder från en angiven DispatchProxy-typ. Metodanrop på den genererade proxyinstansen skickas till den DispatchProxy-bastypen.	Microsoft	4.7.1
System.Reflection.Metadata	Det här paketet tillhandahåller en lågnivåläsare och -skrivare för .NET-metadata (ECMA-335). Den är anpassad för prestanda och är det perfekta valet för att bygga bibliotek på högre nivå som ska tillhandahålla sina egna objektmodeller, till exempel kompilatorer.	Microsoft	5.0
System.Runtime.CompilerServices.Unsafe	Tillhandahåller System.Runtime.CompilerServices.Unsafe-klassen, som tillhandahåller generisk funktionalitet på låg nivå för att manipulera pekare.	24rogramma, dotnetframework	5.0
System.Security.AccessControl	Tillhandahåller basklasser som möjliggör hantering av åtkomst- och granskningskontrollistor för skyddsvärda objekt.	Microsoft	5.0

SOUP-OBJEKT	FUNKTIONSBESKRIVNING	TILLVERKARE	VERSION
System.Security.Permissions	Tillhandahåller typer som stöder Code Access Security (CAS).	Microsoft	5.0
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
System.Text.Encoding.CodePages	Ger stöd för kodsidesbaserade kodningar, inklusive Windows-1252, Shift-JIS och GB2312.	Microsoft	5.0
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 av SOUP IdentityModel	24rogramma,dotn etfra me work	5.0
System.Text.Json	Tillhandahåller högpresterande och lågallokerande typer som serialiserar objekt till JavaScript Object Notation (JSON)-text och avserialiserar JSON-text till objekt, med inbyggt UTF-8-stöd. Tillhandahåller även typer för att läsa och skriva JSON-text kodad som UTF-8, och för att skapa en minnesskyddad dokumentobjektsmodell (DOM), som är skrivskyddad, för slumpmässig åtkomst av JSON-elementen inom en strukturerad vy av data.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	Tillhandahåller ytterligare typer som förenklar arbetet med att skriva samtidig och asynkron kod.	25rogramma,dotnetfra mework	4.5.4
System.ValueTuple	Tillhandahåller System.ValueTuple-structs, som implementerar de underliggande typerna för tupler i C# och Visual Basic. Lägger till ValueTuple-stöd eftersom de bara ingår i senare versioner av .NET-ramverk.	25rogramma,dotnetfra mework	4.5.0
Thrift	Används för definition av fjärrlänkprotokoll	Apache	0.13.0.0
Unity	Unity Container (Unity) är en fullfjädrad, utökningsbar beroendeinjektionscontainer.	Unity Container Project	5.8.13
WAP BT Dongle Driver	WAP BT-dongeldrivrutin (anpassningdongel)	iAnywhere Solutions	3.0.0.6095
WebSync	Används för integration av anpassningsdatakanaler	FM (Frozen Mountain)	4.9.32.0
Xps to Pdf render (NiXPS)	Konvertera 25rogrammatically xps-filer till PDF; används i anpassnings-apprapporter.	NiXPS	2.6.7.0

14. REFERENSER

Titel	Webbplats
Bruksanvisning (elektronisk)	https://ifu.advancedbionics.com/
Advanced Bionics Global Privacy Policy	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Backing up and restoring the data in your Noah database	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Noah System Database Capacity has been Reached.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer - List of used ports	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
LiveSwitch Server Security Documentation	https://developer.liveswitch.io/liveswitch-server/server/security.html
Best Practices for Secure Fitting of Hearing Devices EHIMA whitepaper	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA Cybersecurity-FSW-Security-Whitepaper v1-Sep2021 .pdf

CE 0123

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

info.us@advancedbionics.com

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

info.switzerland@advancedbionics.com

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.

ADVANCED BIONICS
POWERFUL CONNECTIONS

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