

Target CI v1.6

HANDLEIDING OVER CYBERBEVEILIGING

Nederlands

Bijgewerkt: juli 2026



Inhoud

1. INLEIDING	3
1.1 AFKORTINGEN EN DEFINITIES:.....	3
2. OVERIGE HULPBRONNEN	4
2.1 KLANTENSERVICE	4
2.2 AB PRO-PORTAL	4
2.3 GEAVANCEERDE INSTALLATIEHANDLEIDING	4
2.4 TARGET CI FIREWALLCONFIGURATIE.....	4
2.5 MDS2.....	4
2.6 GEBRUIKSAANWIJZING	5
2.7 HIMSA.....	5
3. NETWERK- EN CONTEXTDIAGRAMMEN	6
3.1 IMPLEMENTATIEMODEL 1: STAND-ALONE.....	6
3.2 IMPLEMENTATIEMODEL 2: NOAH DISTRIBUTED	7
3.3 IMPLEMENTATIEARTEFACTEN	8
3.4 SYSTEEMVERBINDINGEN.....	9
4. SYSTEEMVEREISTEN	11
5. CYBERBEVEILIGING IN DE PRODUCTLEVENSCYCLUS.....	12
5.1 IMPLEMENTATIE.....	12
5.2 INSTALLATIE	12
5.3 CONFIGURATIE EN WERKING	13
5.4 VERWIJDERING EN BUITENGEBRUIKSTELLING.....	14
6. BEVEILIGINGSCONTROLES	16
6.1 TOEGANGSCONTROLES.....	16
6.2 CONTROLES OP HET GEBIED VAN AUDITLOGGING EN VERANTWOORDING	17
6.3 EXTERNE TOEGANG	17
7. GEGEVENSBESCHERMING	18
7.1 PRIVACYBELEID VAN ADVANCED BIONICS	18
7.2 FEDERALE GEGEVENSVERWERKINGSNORMEN (FIPS)	18
7.3 PII/PHI VERWERKT DOOR HET PRODUCT	18
7.4 VEILIGHEID TIJDENS OVERDRACHT	19
7.5 BEVEILIGING TIJDENS INACTIVITEIT	20

8. SOFTWARE-INTEGRITEIT	24
8.1 VERIFICATIE VAN GEDOWNLOADE INSTALLATIEMEDIA	24
8.2 HANDMATIGE VERIFICATIE VAN DE AANPASSOFTWARE VÓÓR DE INSTALLATIE.....	24
8.3 AUTOMATISCHE VERIFICATIE VAN DE INTEGRITEIT VAN DE GEÏNSTALLEERDE AANPASSOFTWARE	26
8.4 HANDMATIGE VERIFICATIE VAN DE INTEGRITEIT VAN DE GEÏNSTALLEERDE AANPASSOFTWARE	26
9. SOFTWAREPATCHES EN UPDATES	28
10. GEGEVENSBEHEER.....	28
10.1 DATABASES	28
10.2 GEGEVENSMIGRATIE	29
10.3 HOORTOESTELCONFIGURATIES.....	29
10.4 GEGEVENS VERWIJDEREN	29
11. BEVEILIGDE OMGEVING – GEZAMENLIJKE VERANTWOORDELIJKHEID	29
12. PRODUCTIE, SOFTWAREONTWIKKELING EN BEVEILIGINGSBEHEER.....	32
13. SOFTWARECOMPONENTEN EN MATERIAALLIJST	34
14. REFERENTIES.....	52

1. INLEIDING

Dit document bevat informatie met betrekking tot technische beveiliging en privacy over het Target CI v1.6-softwarestelsel van Advanced Bionics, dat hierna de 'aanpassoftware' wordt genoemd. De aanpassoftware is ontworpen voor gebruik door gekwalificeerde audiciens om hoortoestellen te configureren (d.w.z. aan te passen) voor patiënten die een cochleair implantaat van Advanced Bionics gebruiken.

Dit document richt zich specifiek op de cyberbeveiligings- en privacyoverwegingen die relevant zijn voor het gebruik van de aanpassoftware. Het omvat een evaluatie van de beveiligings- en privacymaatregelen die momenteel in de software zijn geïntegreerd, evenals de maatregelen die naar verwachting zullen worden toegepast en geconfigureerd binnen de IT-omgeving waarin het product voor het beoogde doel zal worden gebruikt.

Dit document biedt geen informatie met betrekking tot technische beveiliging en privacy over:

- eerdere versies van AB-aanpassoftware
- andere AB-software dan Target CI v1.6
- AB-websites
- mobiele applicaties van AB
- AB-hoortoestellen

1.1 AFKORTINGEN EN DEFINITIES:

Acroniem	Trefwoord
FSW	Aanpassoftware
SaMD	Software als medisch hulpmiddel
Noah	Er wordt een extern patiëntenbeheersysteem van HIMSA gebruikt om demografische patiëntgegevens en aanpassingsgegevens op te slaan en te beheren
TeamViewer	Een platformafhankelijke tool voor toegang op afstand en om het bureaublad te delen
SOUP	Software met een onbekende herkomst
Audicien	Audicien
SaMD	Software als medisch hulpmiddel
AB	Advanced Bionics
Sonova	Advanced Bionics is een volledige dochteronderneming van Sonova en functioneert als een integraal onderdeel van de Sonova Groep.
IFU	Gebruiksaanwijzing
PHI	Beschermde gezondheidsinformatie
PII	Persoonlijk identificeerbare informatie
SBOM	Software-materiaallijst

2. OVERIGE HULPBRONNEN

2.1 KLANTENSERVICE

Advanced Bionics heeft een gratis nummer dat u kunt bellen voor technisch advies (877-271-6727) aan personen binnen de Verenigde Staten en Canada. Op dit nummer staat een professionele klantenservice voor u klaar van maandag t/m vrijdag van 05.00 t/m 17.00 uur Pacific Time.

Buiten de VS en Canada wordt technische ondersteuning regionaal aangeboden. Als u vragen heeft over de aanpassoftware, gerelateerde hardware of andere programmeringsproblemen, neemt u contact op met uw plaatselijke contactpersoon van AB.

2.2 AB PRO-PORTAL

U kunt de aanpassoftware en de bijbehorende documentatie downloaden via <https://www.abproportal.com> of de Sonova Web Client. Hiervoor moet u inloggen op uw account. Deze hulpbron is mogelijk niet in alle regio's beschikbaar. Neem daarom contact op met uw contactpersoon van AB voor meer informatie.

2.3 GEAVANCEERDE INSTALLATIEHANDLEIDING

De geavanceerde installatiehandleiding voor Target CI v1.6 is op aanvraag verkrijgbaar. De handleiding bevat technische informatie over het installatieprogramma van de aanpassoftware, met inbegrip van opdrachtregelopties voor achtergrond- en automatische installaties.

2.4 TARGET CI FIREWALLCONFIGURATIE

Het document voor firewallconfiguratie is op aanvraag beschikbaar. Dit document biedt IT-gerichte richtlijnen om ervoor te zorgen dat Target CI 1.6 werkt achter een zakelijke firewall, met details over de vereiste HTTP/HTTPS-toegang en de belangrijkste hostnamen. Het document behandelt WebRTC-connectiviteit via Twilio en Xirsys, beschrijft TURN- en peer-relaypoorten en benadrukt dat veel IP-adressen dynamisch zijn, waardoor waar mogelijk op hostnamen gebaseerde regels moeten worden gebruikt.

2.5 MDS2

De Manufacturer Disclosure Statement for Medical Device Security (openbaarmakingsverklaring voor fabrikanten met betrekking tot de beveiliging van medische hulpmiddelen; MDS2) is een standaardformulier voor de sector met oplossingen aangaande beveiliging en privacy-informatie over aanpassoftware van AB. Dit formulier is op aanvraag verkrijgbaar.

2.6 GEBRUIKSAANWIJZING

De gebruiksaanwijzing wordt meegeleverd met het software-installatieprogramma. In sommige regio's kan de gebruiksaanwijzing worden gedownload via www.advancedbionics.com/ifu

De volgende hoofdstukken in de gebruiksaanwijzing zijn mogelijk van belang voor IT-professionals:

- Productbeschrijving
- Minimale systeemvereisten en prestatiekenmerken
- Richtlijnen voor IT-beveiliging
- Gebruiksaanwijzing
- Afvoeren en gevaarlijke materialen
- Technische ondersteuning

2.7 HIMSA

De Hearing Instrument Manufacturer's Software Association (HIMSA) is een externe softwareleverancier die Noah System 4 produceert: een softwaresysteem dat speciaal is ontworpen voor de gehoorsector en dat audiciens een leveranciersafhankelijk systeem biedt voor het uitvoeren van cliëntgerelateerde taken.

De aanpassoftware kan optioneel worden geconfigureerd om Noah System 4 te gebruiken voor gegevensopslag in plaats van een lokale database.

Op de webpagina over HIMSA-beveiliging vindt u antwoorden op veelgestelde vragen over de IT-beveiliging van Noah System 4.

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

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

Raadpleeg het hoofdstuk Security (Beveiliging) van het HIMSA Learning Center voor aanvullende informatie over beveiliging:

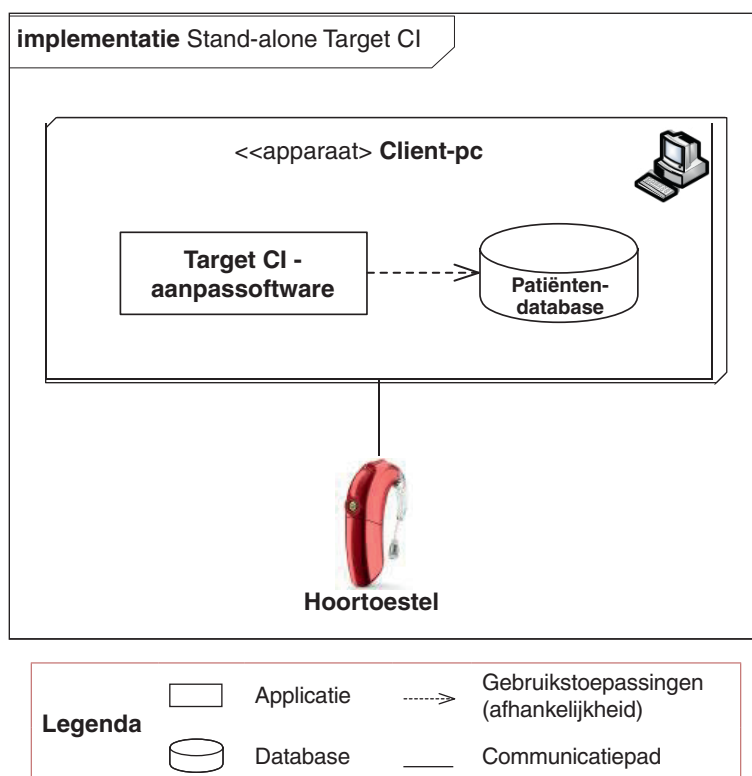
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. NETWERK- EN CONTEXTDIAGRAMMEN

Er worden twee implementatiemodellen ondersteund voor de aanpassoftware. Dit is een clienttoepassing (SaMD) die op een standaard pc met Microsoft Windows kan worden geïnstalleerd. De hardware en het besturingssysteem zijn niet inbegrepen bij de software.

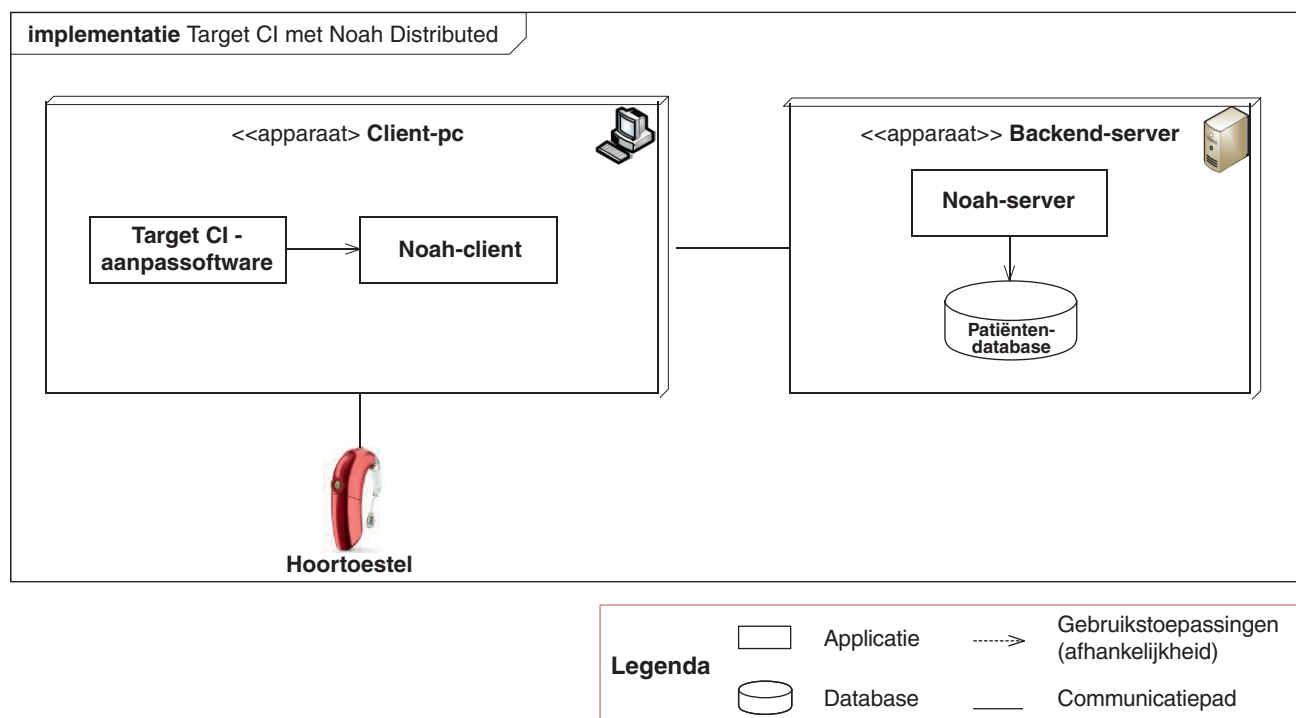
3.1 IMPLEMENTATIEMODEL 1: STAND-ALONE

Bij het stand-alone implementatiemodel wordt de aanpassoftware op een client-pc geïmplementeerd. De patiëntendatabase wordt op dezelfde pc opgeslagen en samen met de aanpassoftware geïnstalleerd.



3.2 IMPLEMENTATIEMODEL 2: NOAH DISTRIBUTED

Bij het Noah Distributed-implementatiemodel wordt de aanpassoftware op één of meerdere client-pc's met Noah geïmplementeerd. Noah, een extern patiëntenbeheersysteem, wordt op een interne server geïmplementeerd die toegankelijk is voor de client-pc's. De patiëntendatabase wordt opgeslagen op de Noah-server en is voor een of meerdere client-pc's toegankelijk via het netwerk.

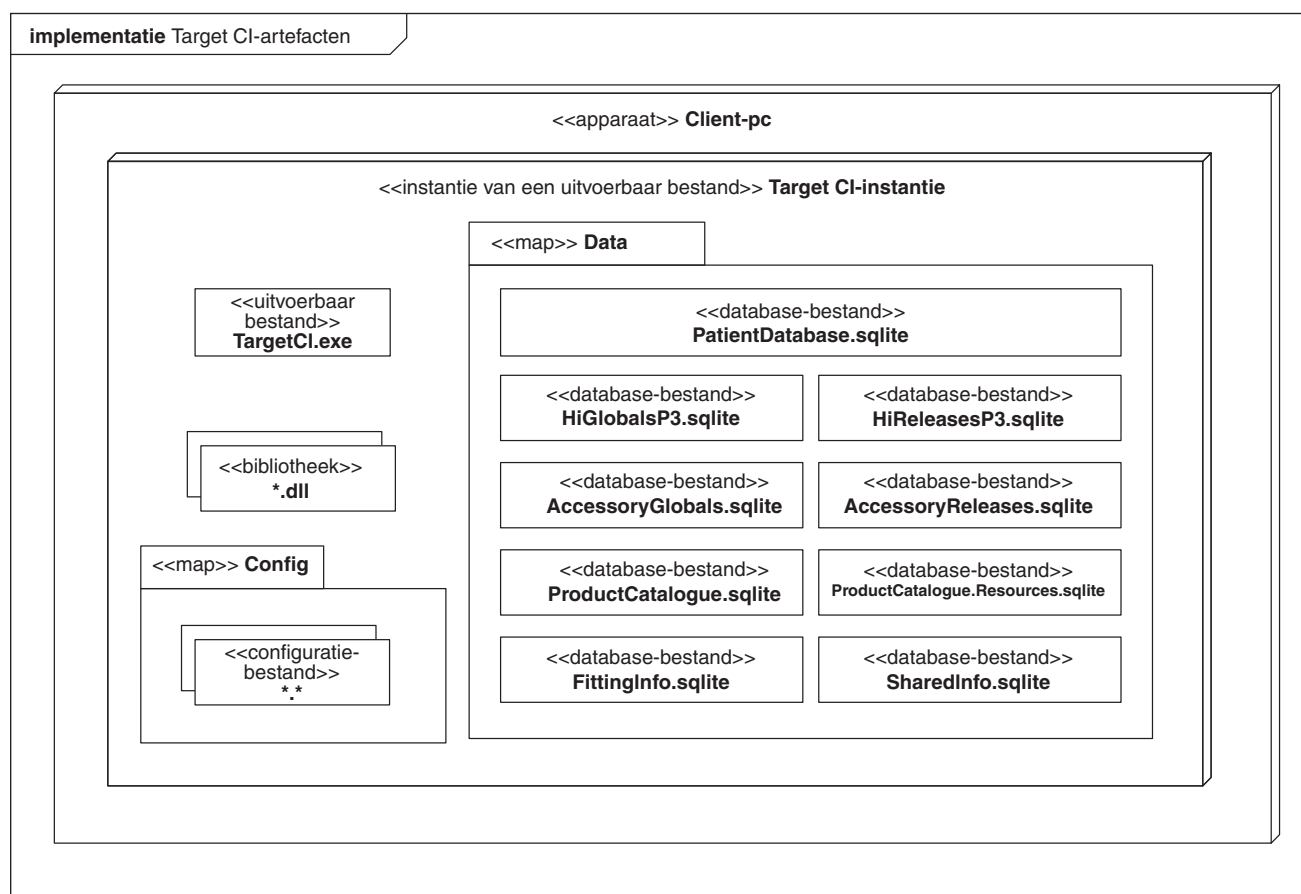


3.3 IMPLEMENTATIEARTEFACTEN

De aanpassoftware wordt geïnstalleerd met een uitvoerbaar bestand en een aantal bijbehorende bestanden, waaronder component-DLL's, configuratiebestanden en SQLite-databasebestanden. De configuratiebestanden worden in de map '%ProgramData%\Advanced Bionics\Target CI\Target CI\Config' geïnstalleerd en databasebestanden worden in de map '%ProgramData%\Advanced Bionics\Target CI\Target CI\Data' geïnstalleerd. De map Data bevat één transactioneel databasebestand en meerdere info-databasebestanden.

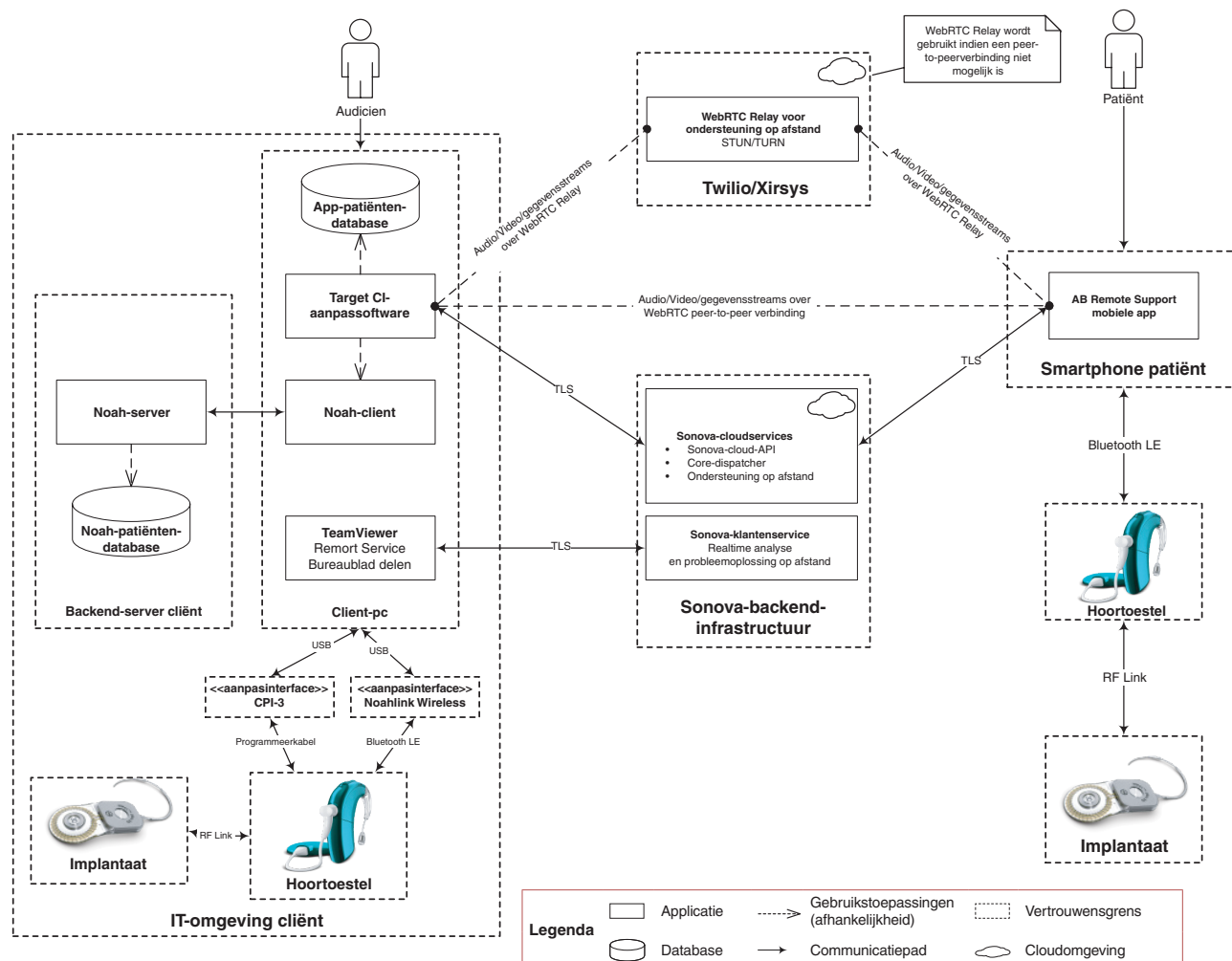
In de transactionele database, PatientDatabase.sqlite, worden de demografische gegevens en de aanpassingsgegevens van de patiënt opgeslagen. Deze database wordt alleen geïnstalleerd wanneer de aanpassoftware in de stand-alone modus wordt geïmplementeerd.

Wanneer de aanpassoftware als een Noah-module wordt geïmplementeerd, levert het Noah-systeem de vereiste persistentieservices voor patiëntgegevens aan de aanpassoftware. De overige sqlite-bestanden zijn een integraal onderdeel van de aanpassoftware en zijn vereist voor alle implementatiemodellen.



3.4 SYSTEEMVERBINDINGEN

In het diagram en de tabel hieronder worden de primaire systeemverbindingen weergegeven. Normaal gesproken wordt slechts een deel van de beschikbare verbindingen gebruikt.



Bron/ bestemming	Service	Protocol	Poort	Omschrijving
Hoortoestel	Hoortoestel-communicatie	Bekabelde verbinding/ Bluetooth® Low Energy	n.v.t.	Wordt gebruikt om te communiceren met hoortoestellen zodat ze kunnen worden bediend, geconfigureerd en zodat de status en gegevens kunnen worden uitgelezen

Bron/ bestemming	Service	Protocol	Poort	Omschrijving
Noah	API van Noah 4-module	.NET-beheer op afstand	n.v.t.	Primaire interface voor de module die wordt gebruikt voor toegang tot de Noah-software (alleen in het implementatie-model van Noah Distributed)
Sonova- cloud- services	Sonova-cloud-API, core-dispatcher, ondersteuning op afstand	SOAP, REST	443	Sonova-services die in een Microsoft Azure-datacenter worden gehost, worden gebruikt om: • de configuratiegegevens van de aanpasssoftware-client op te halen uit de Sonova backend-opslag • gegevens over logging en analyses over te dragen • realtime aanpassing op afstand tot stand te brengen
Twilio/Xirsys, AB Remote Support en AB Remote Support + mobiele apps	Ondersteuning op afstand	WebRTC	Te vinden in het configuratie-document van de Target CI-firewall	Wordt gebruikt door de functie voor ondersteuning op afstand om WebRTC-signalering en realtime aanpassingen op afstand uit te voeren
AB-klanten-service	Bureaublad delen	Bedrijfsseigen protocol van TeamViewer	5938, 443, 80 Raadpleeg de TeamViewer-poorten	Wordt gebruikt om op afstand realtime analyses uit te voeren en problemen op te lossen die van invloed zijn op de installatie van aanpasssoftware. Raadpleeg hoofdstuk 6.3 EXTERNE TOEGANG voor meer informatie.

4. SYSTEEMVEREISTEN

Besturingssysteem	Windows 10, 11, Pro/Enterprise
.NET Framework	Versie 4.8
CPU	Intel® Core™ i5 of gelijkwaardig met gelijke of betere prestaties
RAM	4 GB of meer
Beschikbare harde-schijfruimte	3 GB of meer
Minimale weergavevereisten	• Resolutie van 1280 x 1024 (maximale schaalgrootte van 125%) • 24-bits kleuren
Apparaatstuurprogramma's	• Noahlink Wireless-stuurprogramma (de nieuwste versie van HIMSA is vereist als u een externe via USB aangesloten Noahlink Wireless-programmeerinterface gebruikt). • CPI-3-stuurprogramma (vereist bij gebruik van een via USB aangesloten CPI-3-programmeerinterface).
Database	SQLite of Noah System 4 (versie 4.16 of hoger)
Internetverbinding	Voor ondersteuning op afstand en analyseregistratie is een internetverbinding vereist. Raadpleeg hoofdstuk 3.4 Interconnecties systeem. Intranet is vereist bij gebruik van Noah System 4 in een netwerk.
Netwerkpporten	Raadpleeg hoofdstuk 3.4 Interconnecties systeem. Raadpleeg hoofdstuk 2. Overige hulpbronnen — HIMSA voor de poorten die door Noah System 4 worden gebruikt.

5. CYBERBEVEILIGING IN DE PRODUCTLEVENSCYCLUS

5.1 IMPLEMENTATIE

Goedgekeurde implementatiemethoden:

1. Downloaden via de Sonova Web Client (SFTP) op <https://webclient.sonova.com> of de AB Pro Portal op <https://www.abproportal.com>
2. Installeren vanaf een officiële USB-stick van Advanced Bionics.

Controleer vóór de installatie de digitale handtekening van het installatieprogramma en scan het bestand met actuele antivirussoftware. Raadpleeg hoofdstuk 8 voor gedetailleerde instructies voor de integriteitscontrole. Pas tijdens de implementatie standaard IT-beveiligingsmaatregelen voor de gezondheidszorg toe, waaronder endpointbeveiliging en netwerkbepeningen.

Als er een USB-stick wordt gebruikt:

- Gebruik uitsluitend officiële USB-sticks van Advanced Bionics.
- Bewaar de USB-stick op een veilige plek en wijzig de inhoud ervan niet.
- Scan de USB-stick en installatieomgeving met een bijgewerkt antivirusprogramma en whitelists voor de applicatie.
- Advanced Bionics is niet verantwoordelijk voor ongeautoriseerde gegevens die zijn opgeslagen op USB-sticks met het installatiepakket.

5.2 INSTALLATIE

Voor de installatie van de aanpassoftware is een beheerdersaccount vereist. Zodra de software is geïnstalleerd, kan deze worden uitgevoerd zonder beheerdersrechten of verhoogde machtigingen.

Raadpleeg hoofdstuk 8, Software-integriteit, voor informatie over het verifiëren van de integriteit van de software vóór installatie.

Voordat de installatie wordt gestart, raden wij systeembeheerders aan om het volgende te controleren:

- of de versie van de aanpassoftware die geïnstalleerd moet worden de nieuwste beschikbare versie is.
- of het onderliggende besturingssysteem up-to-date is.
- of de integriteit en authenticiteit van de installatiegegevens van de betreffende software is geverifieerd. Raadpleeg hoofdstuk 8 voor informatie over het valideren van de integriteit van de software vóór installatie

Er zijn twee installatieprogramma's beschikbaar voor de installatie van de aanpassoftware:

- Standaard installatieprogramma
- Installatieprogramma voor IT-professionals

Het installatieprogramma voor IT-professionals bestaat uit één MSI-bestand en bevat geen vereiste componenten, maar is verder gelijkwaardig aan het Standaard installatieprogramma.

Vereiste componenten zijn onder meer het Microsoft .NET Framework v4.8 en de Microsoft Visual C++ Redistributable-pakketten.

Beide installatieprogramma's ondersteunen geavanceerde installatiefuncties, waaronder achtergrondinstallatie.

Gebruik het installatieprogramma voor IT-professionals alleen als uw organisatie vereist dat de vereiste componenten door uw organisatie worden geïnstalleerd en beheerd en niet door het bijbehorende software-installatieprogramma. In alle andere gevallen dient u het Standaard installatieprogramma te gebruiken.

Het installatieprogramma voor IT-professionals is verkrijgbaar bij een klinische contactpersoon van AB. U kunt het installatieprogramma voor IT-professionals niet gebruiken om installaties van het Standaard installatieprogramma te repareren, opnieuw te installeren of te verwijderen. Het Standaard installatieprogramma kan niet worden gebruikt om installaties van het installatieprogramma voor IT-professionals te repareren, opnieuw te installeren of te verwijderen.

Voor geavanceerde installatiescenario's volgt u de instructies in de handleiding voor geavanceerde installatie van de aanpassoftware (zie hoofdstuk 2.3). Voor standaard installatiescenario's verwijzen we naar hoofdstuk 2.5 van dit document, die een link bevat naar de gebruiksaanwijzing van de aanpassoftware.

5.3 CONFIGURATIE EN WERKING

De aanpassoftware biedt ondersteuning voor diverse privacy- en beveiligingsinstellingen en -functies. Sommige privacy- en beveiligingsfuncties van de software zijn standaard ingeschakeld, andere kunnen tijdens de installatie worden geconfigureerd en zijn afhankelijk van het gekozen implementatiemodel, en weer andere kunnen tijdens normaal gebruik via de grafische gebruikersinterface van de applicatie worden geconfigureerd.

Raadpleeg:

- Hoofdstuk 6 voor een lijst met beveiligingsmaatregelen die de bescherming van het applicatiesysteem van de aanpassoftware verbeteren
- Zie hoofdstuk 7 voor een lijst met beveiligingsmaatregelen die de bescherming van gegevens die door de betreffende softwaretoepassing worden verwerkt, verbeteren

Er wordt verwacht dat gebruikers (bijv. zorgverleners, systeembeheerders, IT-personeel) aanvullende privacy- en beveiligingsfuncties (die niet door de software op applicatieniveau worden ondersteund) op besturingssysteemniveau en/of IT-infrastructuurniveau inschakelen en configureren. Raadpleeg hoofdstuk 11 van dit document voor een gedetailleerde lijst met aanbevolen werkwijzen en beveiligingsmaatregelen voor de aanpasomgeving waarin de aanpassoftware wordt gebruikt.

Firewall

De installatiesoftware heeft geen interne firewall.

Als een externe firewall is ingeschakeld (bijvoorbeeld op besturingssysteemniveau), moet de configuratie ervan mogelijk worden bijgewerkt om het vereiste inkomende en uitgaande verkeer toe te staan (bijvoorbeeld WebRTC-audio-/video-/gegevensstromen tijdens een sessie voor ondersteuning op afstand). Raadpleeg het configuratiedocument voor de firewall van de installatiesoftware dat een lijst bevat met netwerkadressen en poorten die door de installatiesoftware worden gebruikt.

Proxy-instellingen

De aanpassoftware wordt geleverd via een lokale proxy. Via de grafische gebruikersinterface van de betreffende software kunnen de instellingen van een dergelijke proxy worden gewijzigd:

- Geen proxy
- Proxy-instellingen automatisch detecteren
- Handmatige proxyconfiguratie. Als deze optie is geselecteerd, kunnen de volgende instellingen worden geconfigureerd:
 - Adres
 - Poort
 - Proxyverificatie in-/uitschakelen (gebruikersnaam, wachtwoord, domein)

5.4 VERWIJDERING EN BUITENGEBRUIKSTELLING

Raadpleeg de gebruiksaanwijzing van de aanpassoftware voor gedetailleerde instructies over het verwijderen van de software.

Het verwijderingsprogramma verwijdert niet de gegevenscategorieën die in de volgende tabel worden vermeld. Tenzij anders vermeld in de kolom 'Opmerkingen' van de tabel, moeten dergelijke gegevens handmatig door systeembeheerders uit de systemen worden verwijderd; bijvoorbeeld door de bestanden handmatig te verwijderen of door de schijf die voor gegevensopslag wordt gebruikt te wissen.

Gegevenscategorie	Standaardlocatie	Opmerkingen
Applicatiegegevens	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI	Bevat de volgende gegevenstypen: - Analytische gegevens - Configuratiegegevens - Applicatielogboeken - Tijdelijke bestanden
Persoonsgegevens	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI\Data	Patiëntendatabase (alleen relevant voor stand-alone implementatiemodel)
Tool voor externe toegang	C:\Program Files (x86)\Common Files\ Advanced Bionics\ TeamViewer	Wordt gebruikt om realtime analyses uit te voeren en problemen op te lossen die van invloed zijn op de aanpassoftware, inclusief die tijdens installatie en verwijdering. Raadpleeg hoofdstuk 6.3 voor meer informatie.

Wanneer u de aanpassoftware verwijdert van de computer/laptop die bestemd is tegen afschrijving of verwijdering, zorg er dan voor dat alle gevoelige gegevens (bijv. medische gegevens, persoonsgegevens) worden gewist.

Voor Noah-implementaties kunt u uitgebreide instructies voor het verwijderen van gegevens raadplegen op:

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

Externe media met gegevens die zijn geëxporteerd vanuit de aanpassoftware, met inbegrip van rapporten en logboeken, moeten worden beveiligd. Wanneer ze niet meer worden gebruikt, moeten gegevens veilig worden gewist en/of moeten de media veilig worden gewist of vernietigd.

Er moeten goedgekeurde procedures en tools worden gebruikt voor het veilig verwijderen van gegevens die zijn opgeslagen op verwijderbare media, in overeenstemming met de toepasselijke regelgeving en richtlijnen voor het omgaan met patiëntgegevens/gegevens voor persoonsidentificatie/beschermde gezondheidsgegevens.

6. BEVEILIGINGSCONTROLES

De aanpassoftware is een clientapplicatie die op een standaard pc met Microsoft Windows wordt geïnstalleerd. De aanpassoftware kan als stand-alone applicatie of als Noah-module worden geïnstalleerd.

6.1 TOEGANGSCONTROLES

De aanpassoftware beperkt de toegang tot de functies niet op basis van aanmeldvereisten en rollen van afzonderlijke gebruikers. Op rollen gebaseerde toegangscontroles worden niet ondersteund.

Lokale gebruikerstoegang

Wanneer de aanpassoftware als een stand-alone applicatie wordt geïnstalleerd, is deze afhankelijk van de mechanismen voor toegangscontrole van het host-besturingssysteem. De IT-medewerkers van de klant kunnen het hostbesturingssysteem configureren om gebruikersverificatie te beheren en toegangsrechten of -machtigingen toe te wijzen. Het wordt elke gebruiker ten zeerste aangeraden om in te loggen met een uniek, individueel account.

Aanvullende compenserende maatregelen worden beschreven in hoofdstuk 11 van dit document en in het hoofdstuk Richtlijnen voor IT-beveiliging in de gebruiksaanwijzing.

Wanneer de aanpassoftware als Noah-module is geïnstalleerd, wordt de toegangscontrole beheerd via Noah System 4.

Voor meer informatie over toegangscontrolefuncties van Noah System 4 kunt u de documentatie raadplegen op www.HIMSA.com.

Toegang tot de service

Technici van de serviceafdeling op locatie hebben toegang tot de installatiesoftware, rekening houdend met de toegangsrechten die door de IT-afdeling van de klant zijn geconfigureerd voor verificatiebeheer.

Medewerkers van AB support kunnen toegang krijgen tot de aanpassoftware via de functie voor schermdeling die door de aanpassoftware wordt ondersteund. Raadpleeg hoofdstuk 6.3 voor gedetailleerde informatie over de beveiligingsmaatregelen die voor deze functie zijn ingeschakeld.

6.2 CONTROLES OP HET GEBIED VAN AUDITLOGGING EN VERANTWOORDING

De montagesoftware genereert geen extra auditlogboeken of rapporten, behalve degene die door het onderliggende besturingssysteem worden geleverd.

Stand-alone implementatiemodel

Wanneer de aanpassoftware als een stand-alone applicatie wordt geïnstalleerd, is deze afhankelijk van de auditmechanismen die door het host-besturingssysteem worden verstrekt. De aanpassoftware beschikt niet over dergelijke geïntegreerde functies. Het host-besturingssysteem kan door het IT-personeel van de klant worden geconfigureerd om bepaalde gebeurtenissen uit te voeren zoals het opstarten/uitvoeren van de aanpassoftware. Het wordt aanbevolen dat iedere gebruiker inlogt op het host-besturingssysteem met een uniek account per gebruiker om de controle te bevorderen.

Implementatiemodel Noah Distributed

Wanneer de aanpassoftware als Noah-module wordt geïnstalleerd, wordt auditlogging uitgevoerd door het Noah-systeem (Noah-activiteitenlogboek). Voor meer informatie over de beschikbare controlemechanismen in Noah System 4 raadpleegt u de documentatie op www.himsa.com

6.3 EXTERNE TOEGANG

Met de functie Bureaublad delen kunt u op afstand realtime analyses uitvoeren en problemen oplossen die van invloed zijn op de installatie van aanpassoftware. Deze functie is gebaseerd op de externe tool TeamViewer QuickSupport (standaard geïnstalleerd met de bijbehorende software) en zorgt ervoor dat medewerkers van de klantenservice van AB op afstand verbinding kunnen maken met de computer van de audicien en volledige controle over het bureaublad krijgen, waaronder toegang tot het onderliggende besturingssysteem en bestandssysteem.

Om een sessie met Bureaublad delen tot stand te brengen, is interactie met audicien vereist. De audicien moet eerst de TeamViewer QuickSupport-tool uitvoeren (bijvoorbeeld via de Target CI-aanpassoftware) en zijn/haar TeamViewer-ID doorgeven aan het AB-ondersteuningsteam via een out-of-band communicatiekanaal (bijvoorbeeld tijdens een telefoongesprek).

De naam en TeamViewer-ID van de AB-medewerker worden standaard weergegeven op het computerscherm van de audicien tijdens elke actieve sessie waarbij het bureaublad wordt gedeeld.

Al het netwerkverkeer van Bureaublad delen wordt beveiligd door cryptografische protocollen en algoritmes die volgens de huidige normen als veilig worden beschouwd (RSA openbare/publieke sleuteluitwisseling en AES 256-bits sessieversleuteling).

De tool voor externe toegang kan handmatig worden verwijderd zonder dat dit invloed heeft op andere Target FSW-functionaliteiten. Het installatieprogramma van Target FSW ondersteunt een opdrachtregel-installatieparameter waarmee u Target FSW via de opdrachtregel kunt installeren zonder dat u de tool voor externe toegang hoeft te installeren.

7. GEGEVENSBESCHERMING

7.1 PRIVACYBELEID VAN ADVANCED BIONICS

U kunt het privacybeleid, waarin wordt beschreven hoe Advanced Bionics persoonsgegevens verzamelt, overdraagt, opslaat en gebruikt, downloaden via: AdvancedBionics.com/privacy.

Advanced Bionics voert geen hosting, opslag of back-ups uit en heeft geen toegang tot gegevens die zijn opgeslagen in de aanpassoftware of Noah-databases, tenzij de gegevens uitdrukkelijk naar Advanced Bionics worden verzonden.

7.2 FEDERALE GEGEVENSVERWERKINGSNORMEN (FIPS)

Target CI v1.6 voldoet aan de FIPS 140-2-versleutelingsnormen.

7.3 PII/PHI VERWERKT DOOR HET PRODUCT

De aanpassoftware verwerkt patiëntgegevens en gezondheidsinformatie.

De patiëntgegevens worden handmatig ingevoerd door de gebruiker van de aanpassoftware, of worden door de applicatie ontvangen via een of meer van de gegevensstromen.

De volgende soorten informatie worden verwerkt in de belangrijkste gegevensstromen van de aanpassoftware:

	Sonova-cloudservices (core-dispatcher, ondersteuning op afstand)	Hoor- toestel	Mobiele apps	Patiënten- database (lokaal/ Noah)	Externe toegang
Naam				X	X(2)
Adres				X	X(2)
Geboortedatum	X(1)		X	X	X(2)
Telefoonnummer				X	X(2)
E-mailadres				X	X(2)
Medische dossiernummers				X	X(2)
Apparaatidentifi- catienummers en serienummers	X(1)	X	X	X	X(2)
IP-adres	X(1)				
Audiogrammen, RECD, REUG	X(1)	X	X	X	X(2)
Aanpasgegevens		X	X	X	X(2)
Gebruiksgegevens hoortoestel	X(1)	X	X	X	
Gebruiksgegevens aanpassoftware	X(1)				

(1) Gepseudonimiseerd voordat de informatie de Sonova-gegevensstroom bereikt.

(2) Tijdens een realtime sessie waarbij het bureaublad wordt gedeeld, krijgen AB-klantenservicemedewerkers volledige controle over het bureaublad van HCP, inclusief toegang tot het onderliggende besturingssysteem en bestandssysteem en de daarin opgeslagen gegevens. Raadpleeg hoofdstuk 6.3 voor meer informatie.

Voor meer informatie over het verzamelen en verwerken van gegevens kunt u contact opnemen met uw lokale ondersteuningsmedewerker.

7.4 VEILIGHEID TIJDENS OVERDRACHT

De communicatiebeveiliging is gewaarborgd en ingeschakeld voor alle inkomende en uitgaande netwerkcommunicatie van de aanpassoftware. Met uitzondering van de functie Ondersteuning op afstand (waarbij gebruik wordt gemaakt van het WebRTC-protocol) en Bluetooth-communicatie met hoortoestellen en accessoires, worden alle overige verbindingen beschermd door het TLS-protocol (Transport Layer Security) dat vertrouwelijkheid, integriteit en authenticiteit biedt.

TLS

De TLS-configuratie voldoet aan de huidige best-practices en beveiligingsaanbevelingen die zijn vastgelegd in BCP 195 – Aanbevelingen voor veilig gebruik van TLS en DTLS [8], met inbegrip van:

- SSL- en TLS-versies ouder dan 1.2 worden niet ondersteund
- Geen ondersteuning voor cipher-suites die gebruikmaken van cryptografische algoritmen die minder dan 128 bits aan beveiliging bieden
- Ondersteuning van aanbevolen TLS-extensies van BCP 195
- Geen ondersteuning voor onveilige extensies van BCP 195

DTLS

Versleuteling is een verplichte functie van WebRTC en wordt toegepast op alle mediastreams die via WebRTC worden verzonden. Het gebruikte versleutelingsprotocol is afhankelijk van het type kanaal. Gegevensstromen worden gecodeerd met DTLS 1.2 en mediastreams met Secure Real-time Transport Protocol (SRTP), omdat dit een minder intensieve optie is dan DTLS.

Raadpleeg de volgende link voor gedetailleerdere informatie over de beveiligingsconfiguratie van Remote Support WebRTC:

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

BLE

Draadloze Bluetooth Low Energy-communicatie met hoortoestellen en accessoires is standaard versleuteld en de integriteit ervan wordt beschermd (met uitzondering van identificatie- en detectietoepassingen). Bovendien is de Bluetooth-koppelingsmodus van het hoortoestel slechts gedurende beperkte tijd beschikbaar. Raadpleeg de documentatie van uw hoortoestel voor een gedetailleerdere beschrijving van de beveiliging van het Bluetooth-communicatiekanaal.

7.5 BEVEILIGING TIJDENS INACTIVITEIT

Applicatiegegevens

Applicatiegegevens bevinden zich op dezelfde machine, in de standaardmap:
C:\ProgramData\Advanced Bionics\Target CI\Target CI

De toegangsrechten worden overgenomen van de bovenliggende map en is beperkt tot gebruikers die tijdens de installatie van de software zijn aangemeld bij het lokale systeem (ingebouwde INTERACTIEVE gebruikersgroep¹).

Geautoriseerde gebruikers hebben lees- en schrijftoegang tot de map.

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

Om het risico op ongeautoriseerde toegang tot de applicatiegegevens via het netwerk te verkleinen, moet u ervoor zorgen dat de mappen of bestanden met de gegevens niet via het netwerk worden gedeeld. De standaardlocaties van de applicatiegegevens worden vermeld in hoofdstuk 5.4.

Patiëntendatabase – Stand-alone implementatiemodel

Wanneer de aanpassoftware als een stand-alone applicatie wordt geïnstalleerd, bevindt de patiëntendatabase zich op dezelfde computer en worden de patiëntgegevens niet versleuteld wanneer ze inactief zijn. De applicatie verzendt geen identificeerbare informatie (PII) via het netwerk.

Iedere gebruiker die kan inloggen op het apparaat met de geïnstalleerde aanpassoftware heeft volledige toegang tot alle applicatiegegevens, inclusief de patiëntendatabase. Raadpleeg het hoofdstuk 'Gegevensbescherming' voor richtlijnen met betrekking tot aanbevolen maatregelen voor gegevensbescherming.

In sommige rechtsgebieden vereisen de voorschriften dat alle patiëntgegevens worden versleuteld om mogelijke aansprakelijkheid te voorkomen in het geval van gegevensverlies of -diefstal. Schakel BitLocker of een vergelijkbare volledige schijfversleuteling (op besturingssysteem- of hardwareniveau) in om de gegevens te beschermen tegen ongeautoriseerde toegang of kopiëren terwijl de gegevens niet worden geraadpleegd.

BitLocker is een ingebouwde Windows-functie die de volledige schijf versleutelt en waarvoor een gebruiker geverifieerd moet worden om toegang te krijgen. Raadpleeg altijd de officiële richtlijnen van Microsoft en het IT-beveiligingsbeleid van uw organisatie voordat u BitLocker inschakelt.

BitLocker inschakelen

Voor het beheer van BitLocker zijn beheerdersrechten vereist.

1. Zoek naar 'Manage BitLocker' (BitLocker beheren)
Open het Start-menu, voer 'Manage BitLocker' (BitLocker beheren) in en selecteer het programma in de zoekresultaten.
2. Selecteer het systeemstation
Kies het station waarop Windows is geïnstalleerd om de versleutelingsinstellingen te configureren.
3. Kies een ontgrendelingsmethode
Selecteer een van de volgende opties:
 - Alleen TPM
 - TPM + PIN
 - TPM + USB-sleutel

Volg de best-practices van Microsoft en het IT-beveiligingsbeleid van uw organisatie bij het selecteren van de ontgrendelingsmethode.

4. Maak een back-up van de herstelsleutel

Maak een back-up van de herstelsleutel met behulp van veilige, voor bedrijven goedgekeurde methoden. Tot aanbevolen opties behoren:

- Opslaan in Microsoft Entra ID (voorheen Azure AD) of Active Directory voor apparaten die verbonden zijn in een domein
- Opslaan op een beveiligde, toegangsgecontroleerde netwerklocatie met versleuteling en auditlogging
- Gebruikmaken van een beheerde sleutelbeheeroplossing die door uw organisatie is goedgekeurd

Sla de sleutel niet op lokale stations of USB-sticks op en druk ze niet af, tenzij dit uitdrukkelijk is toegestaan in het beleid. Herstelsleutels moeten op dezelfde manier worden beschermd als andere gevoelige inloggegevens en moeten onmiddellijk opnieuw worden ingesteld als ze openbaar bekend zijn.

5. Start de versleuteling

Kies:

- Volledige schijf: aanbevolen voor de meeste bedrijfsscenario's. Hierbij worden alle sectoren versleuteld, waaronder vrije ruimte, om dataremanentie te voorkomen.

Patiëntendatabase: implementatie van Noah Distributed-module

Wanneer de aanpassoftware als Noah-module wordt geïnstalleerd, worden gegevens voor persoonsidentificatie opgeslagen in de patiëntendatabase die door Noah wordt gehost. Mogelijk bevindt de patiëntendatabase die door Noah wordt gehost zich op een andere computer. Gegevens voor persoonsidentificatie en andere patiëntgegevens worden door Noah-software beheerd en de versleuteling van de patiëntgegevens die niet actief worden geraadpleegd, wordt gewaarborgd door het Noah-systeem. De aanpassoftware kan gegevens voor persoonsidentificatie verzenden/ontvangen via een bekabelde of draadloze netwerkverbinding wanneer een Noah-database voor netwerktoegang is geconfigureerd.

Gegevens voor persoonsidentificatie die zijn opgeslagen in de Noah-netwerkdatabank zijn toegankelijk voor andere gebruikers op verschillende pc's die over toegangsmachtigingen voor dezelfde netwerkdatabank beschikken. De Noah-database kan ook worden geconfigureerd voor toegang zonder netwerkverbinding en op dezelfde pc worden geïnstalleerd als de aanpassoftware.

Noah zorgt ervoor dat aanpassoftware geen toegang krijgt tot de database met patiëntendossiers. Wanneer een gebruiker via de Noah-client een patiënt in de aanpassoftware opent, kan de aanpassoftware alleen naar het op dat moment geopende patiëntendossier lezen en schrijven. De software heeft geen toegang tot andere patiëntendossiers in de Noah-database.

Raadpleeg de volgende link voor meer informatie over de versleutelingsnormen die door Noah System worden gebruikt:

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

RMA-exportbestanden

Met de aanpassoftware kunnen er cliëntgegevens naar een bestand worden geëxporteerd. Het RMA-bestand kan naar Advanced Bionics worden verzonden om RMA-problemen of gerelateerde ondersteuningsproblemen op te lossen.

Het RMA-bestand is asymmetrisch RSA-versleuteld met een sleutellengte van 2048 bits. De aanpassoftware kan het RMA-bestand op geen enkele manier decoderen.

Geanonimiseerde exportbestanden

Met de aanpassoftware kunnen cliëntgegevens naar een bestand worden geëxporteerd waarin cliënten geanonimiseerd zijn. De gegevens voor persoonsidentificatie van de cliënt, zoals hun geboortedatum en naam, worden vervangen door generieke waarden. Het bestand is niet versleuteld en kan in dezelfde of een andere instantie van de aanpassoftware worden geïmporteerd.

Standaard exportbestanden

Met de aanpassoftware kunnen er cliëntgegevens naar een standaard exportbestand worden geëxporteerd. Het bestand maakt gebruik van een bedrijfseigen binaire indeling en het is niet versleuteld. Het bestand kan in dezelfde of een andere instantie van de aanpassoftware worden geïmporteerd. Wanneer er gebruik wordt gemaakt van deze functie moeten gebruikers van de aanpassoftware ervoor zorgen dat standaard exportbestanden worden verwerkt in overeenstemming met hun lokale IT-beleid voor het beheer van niet-versleutelde gegevens voor persoonsidentificatie.

Hoortoestel

De aanpassoftware slaat cliëntgegevens op in het hoortoestel van de cliënt. Gegevens voor persoonsidentificatie, zoals de naam en geboortedatum van de cliënt, worden niet op het hoortoestel opgeslagen. Andere gegevens dan de gegevens voor persoonsidentificatie worden opgeslagen met behulp van PBKDF2-versleuteling met een 128-bits sleutel.

De aanpassoftware kan andere cliëntgegevens dan gegevens voor persoonsidentificatie verzenden/ontvangen naar/van een hoortoestel via een bedrijfseigen bedraad apparaat (bijv. CPI-3), AB Remote Support en AB Remote Support + mobiele applicaties of via het draadloze Noahlink-apparaat. Het draadloze Noahlink-apparaat maakt verbinding met het hoortoestel via Bluetooth Low Energy (BLE) via een standaard BLE 128-bits AES-versleuteld kanaal.

8. SOFTWARE-INTEGRITEIT

8.1 VERIFICATIE VAN GEDOWNLOADE INSTALLATIEMEDIA

De installatiemedia voor de Target CI-aanpassoftware kunnen in sommige regio's worden gedownload via de Pro Portal van Advanced Bionics of de Sonova Web Client. De gedownloade installatiemedia kunnen worden geverifieerd met behulp van een vertrouwde SHA-256-hashtool.

De SHA256-hash voor het zipbestand voor de standaardinstallatie is:

A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

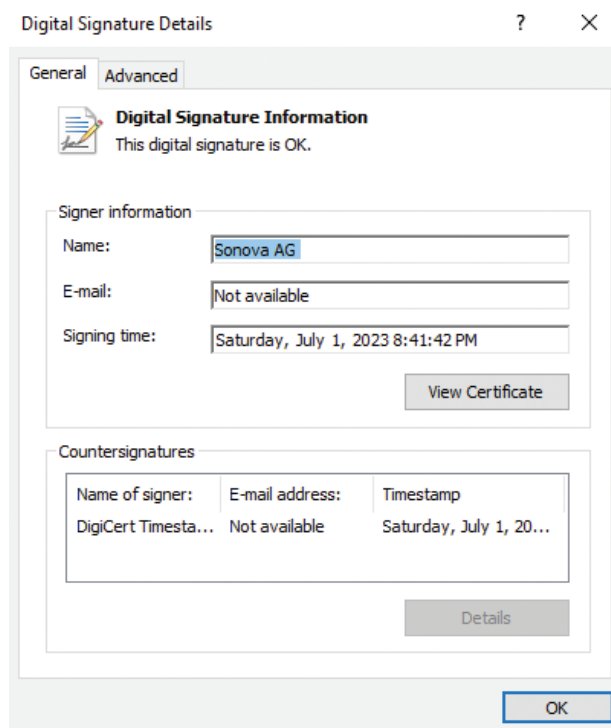
De SHA256-hash voor het zipbestand van het installatieprogramma voor IT-professionals is: DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 HANDMATIGE VERIFICATIE VAN DE AANPASSOFTWARE VÓÓR DE INSTALLATIE

Gebruikers kunnen de volgende stappen uitvoeren om de integriteit en authenticiteit van de aanpassoftware voorafgaand aan de installatie te verifiëren:

1. Open Windows Verkenner en navigeer naar de hoofdmap van de installatiemedia van de aanpassoftware. Als uw installatiemedia zich op USB-stick bevinden, plaatst u deze in een USB-poort en navigeert u naar de hoofdmap. Als uw installatiemedia zich in een zipbestand bevinden, pakt u deze uit in een map en navigeert u naar die map.
2. Klik met de rechtermuisknop op SonovaVerify.exe en selecteer Properties (Eigenschappen) in het contextmenu.
3. Selecteer het tabblad Digital Signatures (Digitale handtekeningen).
4. Dubbelklik op de SHA256-handtekening 'Sonova AG'.

5. Controleer of de elementen van de handtekening geldig zijn. Controleer met name of de melding 'The digital signature is OK' (De digitale handtekening is in orde) bovenaan wordt weergegeven en of de naam van de ondertekenaar en de ondertekeningstijd overeenkomen met de volgende afbeelding:



6. Klik op de knop 'View Certificate' (Certificaat bekijken) en vervolgens op het tabblad 'Details' en controleer of de waarde in het veld 'Thumbprint' (Vingerafdruk) overeenkomt met deze waarde: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Sluit de pop-updialoogvensters en dubbelklik op SonovaVerify.exe
8. Controleer of 'NO ERRORS DETECTED' (Geen fouten gedetecteerd) wordt weergegeven, zoals aangegeven in de volgende afbeelding:

```
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 . . .
```

De melding 'NO ERRORS DETECTED' (Geen fouten gedetecteerd) duidt op een succesvolle verificatie van de integriteit en authenticiteit van de inhoud van het installatiemedium van de betreffende software. Dit betekent dat SonovaVerify.exe de integriteit van alle bestanden en mappen heeft geverifieerd. Hiermee wordt gecontroleerd of de inhoud van de installatiemedia van de aanpassoftware niet is aangepast, is beschadigd of op een andere manier is aangetast.

SonovaVerify.exe geeft waarschuwingen of foutmeldingen weer als er bestanden of mappen ontbreken of als er onverwachte bestanden of mappen aan de installatiemedia zijn toegevoegd. Indien er waarschuwings- of foutmeldingen worden weergegeven, is de integriteits- en authenticiteitscontrole van de inhoud van de installatiemedia van de betreffende software mislukt. Het wordt aanbevolen om het volgende te doen:

- Ga niet verder met de installatie
- Als u geen enkel bestand in de installatiekopie van de betreffende software opent of uitvoert, meld dit probleem dan aan de ondersteuning van Advanced Bionics (zie hoofdstuk 2.1)

8.3 AUTOMATISCHE VERIFICATIE VAN DE INTEGRITEIT VAN DE GEÏNSTALLEERDE AANPASSOFTWARE

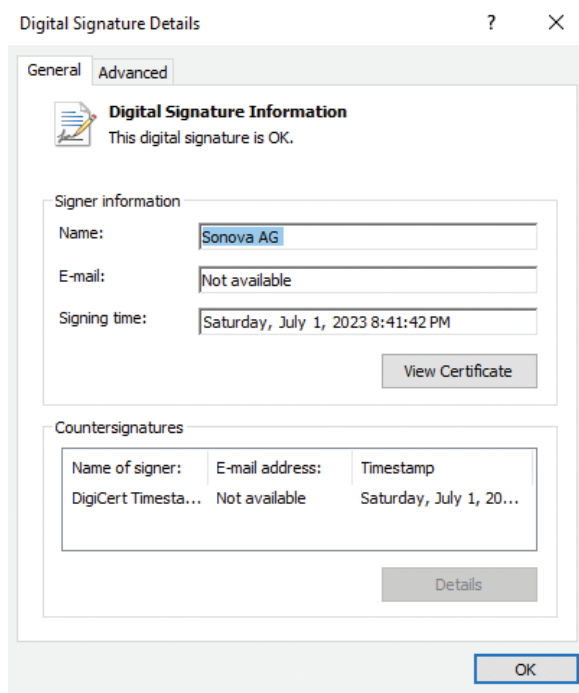
SonovaVerify is geïntegreerd met de aanpassoftware en wordt elke keer dat de applicatie wordt opgestart uitgevoerd om de integriteit van de bestanden van de aanpassoftware te controleren. Bestanden zijn digitaal ondertekend volgens de standaardpraktijken voor de sector en certificaten zijn uitgegeven door een vertrouwde certificeringsinstantie. De software waarschuwt de gebruiker via waarschuwingmeldingen als er bestanden zijn aangetast.

8.4 HANDMATIGE VERIFICATIE VAN DE INTEGRITEIT VAN DE GEÏNSTALLEERDE AANPASSOFTWARE

Gebruikers kunnen de volgende stappen uitvoeren om op elk gewenst moment de integriteit en authenticiteit van de geïnstalleerde aanpassoftware te verifiëren zonder dat ze de aanpassoftware hoeven te starten:

1. Open Windows Verkenner en navigeer naar de map met het uitvoerbare bestand van de bijbehorende software. Deze bevindt zich meestal in: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Klik met de rechtermuisknop op SonovaVerify.exe en selecteer Properties (Eigenschappen) in het contextmenu.
3. Selecteer het tabblad Digital Signatures (Digitale handtekeningen).
4. Dubbelklik op de SHA256-handtekening 'Sonova AG'.

5. Controleer of de elementen van de handtekening geldig zijn en controleer met name of de melding 'The digital signature is OK' (De digitale handtekening is in orde) bovenaan wordt weergegeven en of de naam van de ondertekenaar en de ondertekeningstijd overeenkomen met de volgende afbeelding:



6. Klik op de knop 'View Certificate' (Certificaat bekijken) en vervolgens op het tabblad 'Details' en controleer of de waarde in het veld 'Thumbprint' (Vingerafdruk) overeenkomt met deze waarde: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Sluit de pop-updialoogvensters en dubbelklik op SonovaVerify.exe
8. Controleer of 'NO ERRORS DETECTED' (Geen fouten gedetecteerd) wordt weergegeven, zoals aangegeven in de volgende afbeelding:

```
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 . . .
```

De melding 'NO ERRORS DETECTED' (Geen fouten gedetecteerd) duidt op een succesvolle verificatie van de integriteit en authenticiteit van de inhoud van het installatiemedium van de betreffende software. Dit betekent dat SonovaVerify.exe de integriteit van alle bestanden en mappen heeft geverifieerd. Hiermee wordt gecontroleerd of de inhoud van de installatiemedia van de aanpassoftware niet is aangepast, is beschadigd of op een andere manier is aangetast.

SonovaVerify.exe geeft waarschuwingen of foutmeldingen weer als er bestanden of mappen ontbreken of als er onverwachte bestanden of mappen aan de installatiemedia zijn toegevoegd. Indien er waarschuwings- of foutmeldingen worden weergegeven, is de integriteits- en authenticiteitscontrole van de inhoud van de installatiemedia van de betreffende software mislukt. Het wordt aanbevolen om het volgende te doen:

- Ga niet verder met de installatie
- Als u geen enkel bestand in de installatiekopie van de betreffende software opent of uitvoert, meld dit probleem dan aan de ondersteuning van Advanced Bionics (zie hoofdstuk 2.1)

9. SOFTWAREPATCHES EN UPDATES

Automatische updates worden niet ondersteund. Raadpleeg hoofdstuk 12 voor meer informatie.

10. GEGEVENSBEHEER

10.1 DATABASES

De aanpassoftware maakt gebruik van een transactionele database voor het opslaan van patiëntgegevens en een reeks info-databases die de door de toepassing vereiste metadata-configuraties verstrekken.

Raadpleeg hoofdstuk 3, Netwerk- en contextdiagrammen: implementatieartefacten, voor een gedetailleerde lijst van alle databases die door de aanpassoftware zijn geïmplementeerd.

Wanneer de aanpassoftware als een stand-alone applicatie wordt geïnstalleerd, is de patiëntendatabase een integraal onderdeel van de aanpassoftware.

De patiëntendatabase, die is opgeslagen in het bestand PatientDatabase.sqlite, bevindt zich op dezelfde computer als de aanpassoftware en dient als opslag voor patiëntgegevens. Om een back-up te maken van applicatiegegevens wanneer Target CI als een stand-alone applicatie wordt geïmplementeerd, dient u een back-upkopie van de volledige map op %ProgramData%\Advanced Bionics\Target CI\Target CI\Data te maken. Bescherm uw gegevensback-ups niet alleen tegen gegevensverlies, maar ook tegen diefstal. Wanneer de aanpassoftware als Noah-module wordt geïnstalleerd, worden patiëntgegevens opgeslagen in de database die door Noah System wordt verstrekt. De Noah-database kan worden geconfigureerd voor netwerktoegang. De Noah-database kan ook worden geconfigureerd voor toegang zonder netwerkverbinding en op dezelfde

pc worden geïnstalleerd als de aanpassoftware. Configureer de versleuteling van de Noah-database om gegevens te beschermen (raadpleeg de HIMSA-documentatie).

Voor de implementatiemodus van Noah Distributed raadpleegt u de volgende link voor instructies over het maken van een back-up en het herstellen van de Noah-patiëntendatabase:

<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 GEGEVENSMIGRATIE

Met de aanpassoftware kunnen gebruikers patiëntendossiers migreren vanuit de vorige aanpassoftware van AB, SoundWave 3.2. Patiëntendossiers moeten toegankelijk zijn vanaf een SoundWave 3.2-installatie op dezelfde computer als Target CI om gemigreerd te kunnen worden.

10.3 HOORTOESTELCONFIGURATIES

De aanpassoftware biedt de mogelijkheid om de configuraties en instellingen van het hoortoestel te exporteren en importeren.

10.4 GEGEVENS VERWIJDEREN

Raadpleeg hoofdstuk 5.4, Verwijdering en buitengebruikstelling, in dit document en het hoofdstuk Afvoeren en gevaarlijke materialen in de gebruiksaanwijzing voor richtlijnen voor de verwijdering van gegevens. Voor Noah-implementaties zijn gedetailleerde instructies voor het verwijderen van patiëntendossiers beschikbaar op: <https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

11. BEVEILIGDE OMGEVING – GEZAMENLIJKE VERANTWOORDELIJKHEID

De aanpassoftware is ontworpen voor een beoogd gebruik waarbij het beheer van cyberbeveiligingsrisico's wordt beschouwd als een gezamenlijke verantwoordelijkheid van stakeholders in het gehele ecosysteem van de hoorzorg. Hiertoe behoren onder andere gebruikers van hoortoestellen, ouders of wettelijke voogden van kinderen die hoortoestellen gebruiken, zorgverleners, IT-beheerders, instellingen en verstrekkers van hoorzorg, leveranciers van hoortoestellen en leveranciers van programmeerapparatuur.

Hieronder volgt een lijst met aanbevolen werkwijzen en beveiligingsmaatregelen voor de aanpasomgeving waarin de aanpassoftware wordt gebruikt:

Besturingssysteemniveau

- Pas toegangscontroles toe op besturingssysteemniveau, bijvoorbeeld:
 - Vermijd gastaccounts
 - Schakel de gebruikerslogin van Windows in
 - Houd een lijst bij van geautoriseerde gebruikers om toegang tot het systeem te controleren
 - Stel aangepaste gebruikers en rollen in
 - Stel sterke wachtwoordvereisten in en houd uw inloggegevens geheim
 - Schakel time-out voor inactieve sessies in
- Pas auditcontroles toe op besturingssysteemniveau
- Zorg ervoor dat het besturingssysteem up-to-date is
- Zorg ervoor dat de geïnstalleerde versie van de aanpassoftware up-to-date is
- Gebruik adequate en bijgewerkte malware- en antivirusbescherming
- Zorg ervoor dat de functies AutoRun en AutoPlay zijn uitgeschakeld
- Schakel whitelists voor de applicatie in

Gegevensbescherming

- Zorg ervoor dat de mappen of bestanden met applicatiegegevens niet via het netwerk worden gedeeld. De standaardlocaties van de applicatiegegevens staan vermeld in de tabel in hoofdstuk 5.4. Om te controleren welke netwerkshares door een computer beschikbaar worden gesteld, navigeert u in het Computerbeheer-programma van Microsoft naar 'Computerbeheer -> Gedeelde mappen -> Shares' of voert u de PowerShell-opdracht `Get-WmiObject -class Win32_Share` uit.
- Tijdens de installatie worden de machtigingen voor de applicatiegegevensmap ingesteld volgens hoofdstuk 6.1. Applicatiegegevensmappen nemen de toegangsrechten over van de bovenliggende map. Het beheer van de toegangsrechten voor de bovenliggende map is de verantwoordelijkheid van de softwarebeheerder.
- Versleutel patiëntgegevens met behulp van tools of controlemechanismen van derden op besturingssysteemniveau, door schijfversleuteling te gebruiken (bijvoorbeeld de gratis Microsoft BitLocker) om alle gegevens te beschermen. Als u Noah gebruikt, overweeg dan om Noah-databaseversleuteling te gebruiken.
- Externe media met gegevens die zijn geëxporteerd vanuit de aanpassoftware, met inbegrip van rapporten en logboeken, moeten worden beveiligd. Wanneer ze niet meer worden gebruikt, moeten de gegevens veilig worden gewist en/of moeten de media veilig worden verwijderd.
- Gebruik USB-opslagmedia met ingebouwde beveiligingsfunctionaliteit, zoals versleutelde USB-sticks met een geïntegreerd toetsenblok.

- Zorg altijd voor gegevensbeveiliging door de volgende werkwijzen te volgen:
 - Als u gegevens via onbeveiligde kanalen verzendt, moet u de gegevens anonimiseren of versleutelen.
 - Bescherm uw gegevensback-ups niet alleen tegen gegevensverlies, maar ook tegen diefstal.
 - Verwijder alle gegevens die niet meer worden gebruikt of verwijderd moeten worden van het opslagmedium.
- Gebruikers moeten goedgekeurde procedures en tools gebruiken voor het veilig verwijderen van gegevens die zijn opgeslagen op verwijderbare media, in overeenstemming met de toepasselijke regelgeving en richtlijnen voor het omgaan met patiëntgegevens/gegevens voor persoonsidentificatie/beschermde gezondheidsgegevens

IT-infrastructuur

Gebruik de aanpassoftware in een beveiligde netwerkomgeving, waarin bescherming wordt geboden tegen ongeautoriseerde toegang. Er zijn veel effectieve technieken voor het isoleren en beveiligen van medische gegevenssystemen, waaronder het implementeren van firewallbeveiliging, gedemilitariseerde zones, virtuele lokale netwerken (VLAN's) en netwerk-enclaves. Zorg dat er een actieve netwerkverbinding beschikbaar is, zodat u updates voor het besturingssysteem kunt blijven ontvangen.

Fysiek niveau

- Het werkstation waar de software wordt geïnstalleerd, moet fysiek worden beveiligd zodat het niet toegankelijk is voor onbevoegde personen en er niet mee kan worden geknoeid.
- De toegang tot printers die met het werkstation zijn verbonden, moet worden gecontroleerd.
- De monitor van het werkstation waarop de aanpassoftware is geïnstalleerd, moet zodanig worden geplaatst dat de inhoud op het scherm alleen zichtbaar is voor de gebruiker.

Organisatieniveau

- Alleen professioneel opgeleid, volledig gekwalificeerd personeel mag het systeem bedienen. Voordat iemand toestemming krijgt om het systeem te bedienen, moet worden gecontroleerd of die persoon de bedieningsinstructies die bij de aanpassoftware zijn geleverd, heeft gelezen en volledig begrijpt.
- Alleen personeel dat bevoegd is om de aanpassoftware te onderhouden en te gebruiken, mag een account hebben voor de machine waarop de software is geïnstalleerd. De computer- en domeinaccounts en bijbehorende toegangsrechten moeten regelmatig worden gecontroleerd en uitgeschakeld als toegang tot de machine niet langer nodig is.

- Als u verdachte activiteiten opmerkt in uw accounts voor de aanpassoftware of onverwachte handelingen opmerkt, moet u contact opnemen met Advanced Bionics. Raadpleeg hoofdstuk 2.1 voor meer informatie.

Voor meer informatie over gezamenlijke verantwoordelijkheid en voor een gedetailleerdere lijst met aanbevelingen voor best-practices en beveiligingsmaatregelen voor de aanpasomgeving waar de aanpassoftware op verschillende niveaus zal worden toegepast, raadpleegt u:

- de whitepaper EHIMA 'Best Practices for Secure Fitting of Hearing Devices' (Best-practices voor het aanpassen van hoortoestellen), [EHIMAWhitePaper](#)

12. PRODUCTIE, SOFTWAREONTWIKKELING EN BEVEILIGINGSBEHEER

Cyberbeveiliging wordt in het gehele softwareontwikkelingsproces meegenomen. De aanpassoftware is ontwikkeld in overeenstemming met de normen IEC 62304 en IEC 82304.

Als onderdeel van het productieproces wordt de aanpassoftware op virussen en malware gescand.

Kwetsbaarheden in componenten van derden die zijn opgenomen in de National Vulnerability Database (nationale database met kwetsbaarheden, NVD) van NIST, worden tijdens het ontwikkelingsproces beoordeeld en verholpen. Ook worden ze gemonitord zodra de aanpassoftware in de handel wordt gebracht.

Configuratiebeheer

AB ontwikkelt, documenteert en onderhoudt intern, onder configuratiebeheer, de basisconfiguratie van elke uitgebrachte versie van de aanpassoftware.

Alle door de aanpassoftware gebruikte softwarecomponenten van derden worden geïdentificeerd en gedocumenteerd in de software-materiaallijst (SBOM). SBOM wordt door AB gebruikt voor cybersecurity-risicobeheer om de blootstelling aan cyberdreigingen en openbaar gemaakte kwetsbaarheden te beoordelen en te monitoren met behulp van actuele tools voor het scannen op kwetsbaarheden.

Beveiligingsupdates

AB houdt voortdurend toezicht op beveiligingskwetsbaarheden die van invloed kunnen zijn op de aanpassoftware. Dit is inclusief kwetsbaarheden in de aanpassoftware en in componenten van derden die door de aanpassoftware worden gebruikt.

Gemelde kwetsbaarheden worden beoordeeld op basis van de configuratie en het gebruik van de aanpassoftware.

Indien nodig kunnen beveiligingskwetsbaarheden worden verholpen door een bredere, passende software-update die patches implementeert voor specifieke softwarecomponenten binnen de software.

Openbaar maken van kwetsbaarheden

We maken ons sterk voor het openbaar maken van kwetsbaarheden en het verbeteren van de beveiliging van onze producten en services.

Het melden van vermoedelijke kwetsbaarheden of beveiligingsproblemen met betrekking tot onze producten of de onderliggende software/infrastructuur wordt aangemoedigd.

Lees ons beleid inzake het openbaar maken van kwetsbaarheden, gepubliceerd op <https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy>, en volg de instructies om een melding te doen.

13. SOFTWARECOMPONENTEN EN MATERIAALLIJST

De aanpassoftware bevat bepaalde commerciële, algemeen beschikbare softwarecomponenten.

In de onderstaande vindt u alle SOUP-software (Software of Unknown Provenance, software van onbekende herkomst) die met de aanpassoftware wordt meegeleverd.

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
AForge.NET	AForge.NET wiskunde- en mediabibliotheek, onderdeel van en vereist door IceLink en LiveSwitch.	AForge.NET	2.2.5.0
Amplifon. Programmer	Onderdeel van het softwarepakket van Amplifon	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Onderdeel van het softwarepakket van Amplifon	Amplifon	1.0.4.0
AutoMapper	Automatiseert object-naar-object mapping	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	Bibliotheek voor benchmarking, met tools om de prestaties van code te meten en te vergelijken	BenchmarkDotNet Community	0.13.0.0
Castle.Core	Een core-bibliotheek van het Castle Project, met componenten zoals dynamische proxygeneratie en inversie van control containers voor .NET-applicaties.	Castle Project	4.4.1
Chessie	Een functionele bibliotheek voor foutbeheer voor F#	Open Source	0.6.0.0
ciAD Hearingloss Simulator	Bibliotheek met gehoorverliessimulatoren voor mediaspeler	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Maakt Excel-bestanden lezen, bewerken en schrijven gemakkelijker, zonder dat Excel geïnstalleerd hoeft te zijn	ClosedXML Community	0.95.4.0
CommandLine Parser	Biedt een overzichtelijke en beknopte API om opdrachtregelargumenten te parsen	CommandLineParser Community	2.4.3
Common.Logging	Een mobiele abstractie voor logboekregistratie voor .NET-applicaties	Common.Logging Community	3.4.1.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
CommonService Locator	Biedt een gemeenschappelijke interface voor servicelokalisatie, waardoor applicaties kunnen worden losgekoppeld van specifieke IoC-containers.	Microsoft	2.0.5.0
Credential Management	Het Credential Management-pakket is een wrapper voor de Windows Credential Management-API	iLya Lozovyy	1.0.2
CSharpAnalytics	Wordt gebruikt voor Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78.45418
Deconstructurama.Attributed	Gebruikt door Nephele-bibliotheken.	Serilog Contributors	3.1.0.0
Developer Express Suite	Een uitgebreide suite van UI-besturingselementen en -bibliotheken voor .NET-ontwikkelaars, met tools om applicaties met veel functies te bouwen.	Developer Express Inc	20.2.10.0
DirectShow 2005	Biedt toegang tot de DirectShow-functionaliteit van Microsoft vanuit .NET-toepassingen.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	National Centre for Audiology, Canada	4.2
DSL5	DSL 5-bibliotheek met aanpasformules	National Centre for Audiology, Canada	5.0.34
ExcelNumberFormat	Een functie om Excel-getalnotaties te parsen en formatteren	Open Source	1.1.0.0
FM.dll	Een integraal onderdeel van hun realtime communicatiesystemen zoals LiveSwitch en IceLink	FM (Frozen Mountain)	2.9.32
FSharp.Core	De core-bibliotheek voor de F#-programmeertaal	Microsoft	6.0.322.10402
FTDI Chip	Een driverpakket van Future Technology Devices International (FTDI) voor communicatie tussen USB-apparaten en software-applicaties.	FTDI	3.02.07
GNOtometrics.Aurical	GNOtometrics.Aurical aangepast voor Sonova	Natus Medical Incorporated	2.0.1.9
SharedUtilities.dll	Biedt algemene hulpprogramma's en gedeelde resources voor alle Natus-applicaties.	Natus Medical Incorporated	1.0.0.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Hardware.Info	Een component dat gedetailleerde informatie verzamelt en verstrekt over de hardwareconfiguratie van een systeem	Open Source	11.1.0.1
Himsa.NLWSMAPI.dll	Een bibliotheek die is gekoppeld aan Noah-software van HIMSA	HIMSA	2.0.3.0
natus.otometrics.hipro2	HiPro-communicatiebibliotheek	Natus Medical Incorporated	2.0.0.4
Iced.dll	Biedt realtime communicatie door audio-, video- en datastreaming mogelijk te maken	FM (Frozen Mountain)	1.12.0.0
IceLink	Wordt gebruikt voor integratie van audio/video-gesprekken via WebRTC	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	Biedt Unicode- en globaliseringsondersteuning voor software-applicaties	FM (Frozen Mountain)	54.1.0.0
IdentityModel	OpenID Connect en OAuth 2.0 client-bibliotheek gebruikt door de Kona.CommonServices. Authentication-component voor OAuth 2-authenticatie.	Dominick Baier, Brock Allen	6.2.0.0
IMCInterfaces	Noah-interfacebibliotheek voor intermodulaire communicatie	HIMSA II K/S	4.4.0.2266
iText 7	Pdf-bibliotheek om pdf-documenten programmatisch aan te maken, te bewerken en te inspecteren.	iText Software	7.1.16.0
JetBrains.dotMemory	Een tool voor geheugenprofielering om geheugenlekken op te sporen en geheugengebruik in .NET-applicaties te optimaliseren	JetBrains	111.0.0.0
JsonDiffPatch DotNet.dll	Biedt functies om JSON-objecten te vergelijken en te patchen	Open Source	1.0.1.0
LibGit2Sharp	Wordt gebruikt door bibliotheken van Sonova om te communiceren met Git	LibGit2Sharp-bijdragers	0.26.1.93
LiveSwitch	Wordt gebruikt voor integratie van audio/video-gesprekken via WebRTC.	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	logging framework voor .NET	Apache	4.7.0.3189
Mapster	Wordt gebruikt om objecten in code toe te wijzen	chaowlert,eric_swann	7.2.0.0
Mapster.Core	Wordt gebruikt om objecten in code toe te wijzen	chaowlert,eric_swann	1.2.0.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
MathNet.Numerics	Wordt gebruikt voor aanpassingsalgoritmen (signaalpad, doelmatcher etc.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael en bijdragers	4.11.0
Microsoft.Bcl.AsyncInterfaces	Biedt de IAsyncEnumerable<T>- en IAsyncDisposable-interfaces en helpertypen voor .NET Standard 2.0.	Microsoft	6.0.21.52210
Microsoft.CodeAnalysis.Common	Wordt gebruikt door de bibliotheken van Sonova. HardwareAbstraction.Palio.Trafo	Microsoft	3.900.21.12420
Microsoft.CodeAnalysis.CSharp	Wordt gebruikt door de bibliotheken van Sonova. HardwareAbstraction.Palio.Trafo	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Biedt compilatie en codegeneratie met behulp van C#	Microsoft	4.700.19.56404
Microsoft.Diagnostics.FastSerialization.dll	Gebruikt voor efficiënte serialisatie en deserialisatie van diagnostische gegevens	Microsoft	1.0.0.0
Microsoft.Diagnostics.NETCore.Client.dll	Een beheerde bibliotheek die interactie met de .NET Core-runtime mogelijk maakt voor diverse diagnostische taken, zoals tracering en dumps opvragen.	Microsoft	0.2.4.27602
Microsoft.Diagnostics.Runtime.dll	Biedt API's om actieve processen en crashdumps te inspecteren, zodat ontwikkelaars debug- en diagnostische tools kunnen bouwen.	Microsoft	2.0.4.26801
Microsoft.Diagnostics.Tracing.TraceEvent.dll	Een bibliotheek om Event Tracing for Windows (ETW) gebeurtenissen te parsen en te verwerken	Microsoft	2.0.70
Microsoft.DotNet.PlatformAbstractions.dll	Biedt API's voor toegang tot informatie over het .NET-platform	Microsoft	3.100.620.31604
Microsoft.Uitbreidingen.DependencyInjection.Abstractions	Definieert de abstracties voor dependency injection in .NET-applicaties	Microsoft	6.0.21.52210
Microsoft.Extensions.Logging	Biedt gestructureerde logboekregistratie in .NET-applicaties.	Microsoft	6.0.21.52210
Microsoft.Extensions.Options	Ondersteunt de configuratie van opties in .NET-applicaties	Microsoft	6.0.21.52210

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Microsoft.Extensions.Primitives	Biedt interfaces en klassen om wijzigingen en annuleringstokens bij te houden, wat helpt bij het beheren van veranderlijke gegevens en opschonen van resources.	Microsoft	6.0.21.52210
Microsoft.Identity.Client	De MSAL-bibliotheek voor .NET maakt deel uit van het Microsoft Identity Platform voor ontwikkelaars (voorheen Azure AD) v2.0. Hiermee kunt u beveiligingstokens verkrijgen om beveiligde API's aan te roepen. Hij maakt gebruik van OAuth2 en OpenID Connect als standaard voor de sector.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Veilige cross-platform tokencache voor openbare MSAL-clientapps.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Bevat typen die ondersteuning bieden voor het maken, serialiseren en valideren van JSON-webtokens. Wordt gebruikt door componenten die communiceren met backendservices die JSON-webtokens gebruiken voor authenticatie.	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Logging	Dependency of Microsoft.IdentityModel.Tokens	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Tokens	Dependency of the SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0.11012
Microsoft.ML.OnnxRuntime	Een inferentie-engine om machine learning-modellen uit te voeren in de ONNX-notatie (Open Neural Network Exchange)	Microsoft	1.12.1
Microsoft.ML.OnnxRuntime.Managed	De beheerde .NET-wrapper voor de ONNX Runtime	Microsoft	1.12.1
Microsoft.Office.Interop.Excel.dll	Deze DLL maakt deel uit van de Office Interop-assemblies en zorgt dat .NET-applicaties met Microsoft Excel communiceren	Microsoft	14.0.4733.1000

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Microsoft. VisualStudio. TextTemplating.10.0	Biedt mogelijkheden voor tekstsjablonen binnen Visual Studio, waardoor ontwikkelaars code en andere tekstgebaseerde artefacten kunnen genereren met behulp van T4-sjablonen.	Microsoft	10.0.40219.1
Microsoft.Win32. Registry.dll	Biedt toegang tot het Windows-register	Microsoft	5.0.20.51904
Microsoft.Win32. SystemEvents.dll	Ondersteunt de afhandeling van systeemgebeurtenissen in .NET-applicaties	Microsoft	8.0.23.53103
Microsoft.Win32. TaskScheduler.dll	Wordt gebruikt voor de FSW-back-up tool (automatische back-ups).	David Hall	2.5.11.0
Microsoft.Xaml. Behaviors.Wpf	XAML Behaviors is een gebruiksvriendelijke manier om met minimale code algemene en herbruikbare interactiviteit toe te voegen aan uw WPF-applicaties.	xamlexperiences-team, Microsoft	1.0.1.0
Microsoft DIA SDK	Biedt API's om met foutopsporingsinformatie in PDB-bestanden te werken	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	Wordt gebruikt om .NET-assemblies te inspecteren, te wijzigen en te maken	Microsoft	0.11.3.0
Moq.dll	Open-source .NET-bibliotheek om mock-objecten te maken tijdens unit-testen	Moq Community (Open Source)	4.16.1.0
MS-VisualC++ 7.1 runtime-bibliotheken	Microsoft Visual C++ runtime-bibliotheken	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1-bibliotheek met aanpasformules	Australian Hearing	1.1.0.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
NAL-NL2	NAL-NL2-bibliotheek met aanpasformules	Australian Hearing	2.0.11
NAudio.dll	Wordt gebruikt om het volume aan te passen en geluidsbestanden af te spelen.	Open Source	1.9.0.0
.NET Framework	.NET runtime framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Wordt gebruikt voor JSON-serialisatie en -deserialisatie.	James Newton-King	13.0.3.27908
Newtonsoft.Json.Schema.dll	Een bibliotheek voor schemavalidatie van JSON-gegevens	James Newton-King	3.0.14.25421
Nibelung	NoahLink Wireless-aanpasbibliotheken	HIMSA	1.3.16.1
Nibelung2.CPD	NoahLink Wireless-aanpasbibliotheken	HIMSA	2.0.3.0
Nlog	Dit is een afhankelijkheid van de HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	5.0.4.1331
Noahlink	Stuurprogramma Noahlink-aanpasapparaat	HIMSA	1.55.6.166
Stuurprogramma Noahlink Wireless	Stuurprogramma Noahlink Wireless-aanpasapparaat	HIMSA	1.1.0.0
Noahlink Wireless Upgrader	Noahlink Wireless firmware Upgrader	HIMSA	3.1.0.82
ModuleAPI.dll (Noah System)	Een onderdeel van Noah System van HIMSA, dat API's biedt om audiologische gegevens te integreren en te beheren	HIMSA	4.13.0.5404
NiXPS SDK	Biedt functionaliteiten voor het verwerken van XPS-documenten (XML Paper Specification)	NiXPS NV	2.6.0.0
NPOI	Een open-source bibliotheek die het lezen en schrijven van Microsoft Office-documenten in .NET-applicaties vereenvoudigt	NPOI communi	2.4.1.0
NuGet Package Manager	Een tool om .NET-bibliotheken en -pakketten te beheren	Microsoft	6.3.0.131
Nunit	Een framework voor unit-testen voor .NET-applicaties	NUnit Project	3.12.0.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
ONNX Runtime	Engine voor Open Neural Network Exchange (ONNX) modellen	Microsoft	1.12.20220803.2.7048164
Open XML SDK	Biedt tools om met Office Open XML-documenten te werken	Microsoft	2.7.2
OSExtensions.dll	Bibliotheek die uitbreidingen biedt voor functionaliteiten van het besturingssysteem	Microsoft	1.0.0.0
Otometrics.REMAccess	Abstractielaag van Otometrics boven de Noah-interfacebibliotheek voor intermodulaire communicatie	GN Otometrics	1.0.0.10
Paket.Core.dll	Een open-source dependency manager voor .NET- en Mono-projecten	Paket Community (Open Source)	7.1.5.0
Patagames.Pdf	De C# pdf-bibliotheek om pdf-documenten in .Net-applicaties te maken en te bewerken.	patagames.com	8.57.30.48
Patagames.Pdf.Wpf	De C# pdf-bibliotheek om pdf-documenten in .Net-applicaties te maken en te bewerken.	Patagames.com	4.19.18.48
Polly	Bibliotheek waarmee ontwikkelaars veerkracht en beleid voor het afhandelen van tijdelijke fouten, zoals Retry, Circuit Breaker, Bulkhead Isolation en Fallback, op een vloeiende en thread-veilige manier kunnen uitdrukken	App vNext	7.2.3.0
Portable.BouncyCastle	Dit is een afhankelijkheid van de HIMSA Nibelung. CPD (Noahlink Wireless)	The Legion of the Bouncy Castle Inc	1.8.15362.1
Portable.BouncyCastle.Crypto	Dit is een afhankelijkheid van de HIMSA Nibelung. CPD (Noahlink Wireless)	The Legion of the Bouncy Castle Inc	1.9.0.1

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
protobuf-net.dll	Serialisatieframework gebruikt voor RC blob.	Open Source	2.3.2.0
Google.Protobuf	De officiële Protocol Buffers-bibliotheek van Google voor .NET, die het serialiseren en deserialiseren van gestructureerde gegevens vergemakkelijkt.	Google Inc	3.19.3.0
Perfolizer.dll	Een open-source bibliotheek voor prestatieanalyse	Open Source	0.2.1.0
Rhino.Mocks.dll	Een dynamisch framework voor mock-objecten voor .NET	Rhino Mocks Community	3.6.0.0
Security.Cryptography.NetCore.dll	Biedt cryptografische functionaliteiten voor .NET Core-applicaties	HardDev	1.0.1.0
Serilog	De loggingcomponent die voor de gehele Chinook-applicatie wordt gebruikt.	Serilog Contributors	3.0.1.0
Serilog.Enrichers.Thread	Serilog-gebeurtenissen verrijken met eigenschappen van de huidige thread	Serilog Contributors	3.1.0.0
Serilog.Extensions.Logging	Integreert Serilog met logboekregistratie-abstracties van Microsoft	Serilog Contributors	3.1.0.0
Serilog.Expressions	Expressiegebaseerde gebeurtenisfiltering voor Serilog.	Serilog Contributors	2.0.0.0
Serilog.Sinks.Console	Een Serilog-sink die loggebeurtenissen naar de console/terminal logt.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	Een Serilog-sink die logboekgebeurtenissen naar het debug-uitvoervenster schrijft.	Serilog Contributors	2.0.0.0
Serilog.Sinks.File	Schrijft Serilog-gebeurtenissen naar tekstbestanden in algemene tekst of JSON-indeling.	Serilog Contributors	4.1.0.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Serilog.Sinks.NUnit.dll	Integreert met NUnit en stuurt loggebeurtenissen door naar de testuitvoer van NUnit, wat helpt bij testdiagnose.	Serilog Contributors	1.0.3.0
Serilog.Sinks.Trace	De diagnostische trace-sink voor Serilog.	Serilog Contributors	2.1.0.0
Serilog.Settings.AppSettings	XML-configuratie (System.Configuration <appSettings>) ondersteuning voor Serilog.	Serilog Contributors	2.2.2.0
Security.Cryptography.NetCore.dll	Uitbreidingen van de beveiligings-API's die bij het .NET Framework worden geleverd	Microsoft	1.0.1.0
SharpBITS API	SharpBITS.NET is een .NET-wrapper van de BITS API en een kleine Windows UI-applicatie voor eenvoudigere toegang tot up- en downloads van BITS.	perpetualKid	2.1.0.0
SharpZipLib	#zipLib (SharpZipLib, voorheen NzipLib) is een Zip-, Gzip-, Tar- en Bzip2-bibliotheek die volledig in C# is geschreven voor het .NET-platform. Deze bibliotheek biedt compressiefunctie (zippen, uitpakken, streamingcompressie enz.). Wij gebruiken deze in de firmware-updateapp.	Open Source	1.3.3.11
SharpDX	Gebruikt door LiveSwitch: SharpDX.Direct3D11, SharpDX.Direct2D1, SharpDX.Mathematics	Alexandre Mutel	4.0.1

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
SocketIOClient	Biedt een client voor Socket.IO, waardoor realtime bidirectionele, op gebeurtenissen gebaseerde communicatie in .NET-toepassingen mogelijk wordt	HeroWong	2.2.4.0
Superpower	Een parser-combinatorbibliotheek voor C#	Datalust, Superpower-bijdragers, Sprache-bijdragers	2.3.0.0
SQLite.Interop	SQLite 3.36.0 Native Interop Library. SQLite is de in-process database om informatie over de patiënt (in stand-alonemodus), onze productcatalogusbronnen en de metagegevens voor aanpassingen, accessoires en de hoortoestellen op te slaan. SQLite is publiek domein.	SQLite-ontwikkelingsteam	1.0.115
System.Buffers	Biedt resourcepooling van elk type voor prestatiekritieke applicaties die regelmatig objecten toewijzen en vrijgeven.	microsoft, dotnetframework	4.6.28619.01
System.Collections.Immutable	Wordt gebruikt door de bibliotheken van Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	7.0.22.51805
Systeem.Component Model. Annotations	Biedt kenmerken die worden gebruikt om metagegevens te definiëren voor objecten die als gegevensbronnen worden gebruikt.	microsoft, dotnetframework	4.6.26515.06
Systeem.Configuration. Configuration Manager	Biedt typen die het gebruik van configuratiebestanden ondersteunen.	Microsoft	5.0.20.51904

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System. CodeDom.dll	Biedt klassen voor het genereren en compileren van broncode tot uitvoerbare bestanden of assemblies	Microsoft	8.0.23.53103
System.Data. SQLite	Wordt gebruikt door de bibliotheken van Sonova. HardwareAbstraction.Palio. Trafo	SQLite-ontwikkelingsteam	1.0.115.0
Systeem. Diagnostics. DiagnosticSource	Een logboekbibliotheek waarmee ontwikkelaars diagnostische gegevens kunnen bijhouden en monitoren	Microsoft	6.0.21.52210
Systeem. Diagnostics. Performance Counter	Biedt API's voor interactie met Windows-prestatie meters	Microsoft	7.0.22.51805
System.Drawing. Common	Biedt toegang tot grafische GDI+-functionaliteit.	Microsoft	8.0.324.11603
System.Formats. Asn1.dll	Ondersteunt het coderen en decoderen van Abstract Syntax Notation One (ASN.1) gegevens	Microsoft	6.0.21.52210
System. IdentityModel. Tokens.Jwt	Bevat typen die ondersteuning bieden voor het maken, serialiseren en valideren van JSON-webtokens. Wordt gebruikt door componenten die communiceren met backendservices die JSON-webtokens gebruiken voor authenticatie.	Microsoft	6.8.0.11012
System. IO.Abstractions	Een set abstracties om interacties met bestandssystemen testbaar te maken.	Tatham Oddie en vrienden	12.0.10.46693

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System.IO.Hashing.dll	Biedt hashfunctionaliteit binnen .NET, inclusief algoritmen om checksums en cryptografische hashes te berekenen.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Maakt lezen en schrijven van pakketbestanden mogelijk	Microsoft	6.0.21.52210
System.IO.Ports.dll	Biedt klassen voor seriële poortcommunicatie, waardoor .NET-applicaties kunnen communiceren met hardware die via seriële poorten is aangesloten.	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	Een gespecialiseerde HTTP-handler voor Windows	Microsoft	6.0.422.16404
System.Numerics.Vectors	Biedt hardwareversnelde numerieke typen, geschikt voor hoogwaardige verwerking en grafische applicaties.	microsoft, dotnetframework	4.6.26515.06
System.Memory	Biedt typen voor efficiënte weergave en pooling van beheerde, stack- en native geheugensegmenten en sequenties van dergelijke segmenten, samen met primitieven voor het parseren en formatteren van UTF-8-gecodeerde tekst die in die geheugensegmenten wordt opgeslagen.	microsoft, dotnetframework	4.6.31308.01
System.Reactive.dll		Open Source	5.0.0.1

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System. Reflection. DispatchProxy	Biedt een klasse om dynamisch proxytypen te maken die een opgegeven interface implementeren en zijn afgeleid van een opgegeven DispatchProxy-type. Voor het aanroepen van methoden op de gegenereerde proxy-instanties en te verzenden naar dat DispatchProxy-basistype.	Microsoft	4.700.20.21406
System. Reflection. Metadata	Dit pakket bevat een low-level .NET (ECMA-335) metadata-lezer en -schrijver. Het is gericht op prestaties en is de ideale keuze voor het bouwen van bibliotheken op een hoger niveau die hun eigen objectmodel willen leveren, zoals compilers.	Microsoft	5.0.20.51904
System. Reflection. TypeExtensions	Biedt uitbreidingsmethoden voor de reflectie-API	Microsoft	4.700.19.56404
System.Runtime. Compiler Services.Unsafe	Biedt de System.Runtime.CompilerServices.Unsafe die generieke functionaliteit op laag niveau voor het manipuleren van pointers verstrekt.	microsoft, dotnetframework	6.0.21.52210
System.Security. AccessControl	Biedt basisklassen waarmee toegangs- en auditcontrolelijsten voor beveiligde objecten kunnen worden beheerd.	Microsoft	6.0.21.52210
System.Security. Permissions	Biedt typen die Code Access Security (CAS) ondersteunen.	Microsoft	5.0.20.51904

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System.Security.Principal.Windows	Biedt klassen voor het ophalen van de huidige Windows-gebruiker en voor interactie met Windows-gebruikers en -groepen.	Microsoft	5.0.20.51904
System.Security.Cryptography.Cng.dll	Biedt cryptografische functionaliteit met behulp van Cryptography Next Generation (CNG) API's	Microsoft	5.0.20.51904
System.Security.Cryptography.Pkcs.dll	Biedt klassen om met Public Key Cryptography Standards (PKCS) te werken, inclusief ondertekende en ingekapselde gegevens	Microsoft	6.0.1923.31806
System.Security.Cryptography.ProtectedData.dll	Biedt methoden om gegevensbeveiliging te beveiligen en op te heffen, waarbij Windows Data Protection API (DPAPI) wordt gebruikt voor veilige gegevensopslag.	Microsoft	6.0.21.52210
System.Security.Cryptography.Xml.dll	Maakt XML-versleuteling en digitale handtekeningen mogelijk, waardoor veilige verwerking van XML-gegevens in .NET-applicaties wordt ondersteund.	Microsoft	6.0.822.36306
System.ServiceModel.Http.dll	Biedt HTTP-gebaseerde communicatiefunctie voor Windows Communication Foundation (WCF)-services	Microsoft	4.700.19.56502
System.ServiceModel.Primitives.dll	Bevat fundamentele klassen voor WCF-services, waaronder basisklassen en interfaces voor servicecontracten en kanalen.	Microsoft	4.700.19.56502

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System.Text.Encoding.CodePages	Biedt ondersteuning voor op codepagina's gebaseerde coderingen, waaronder Windows-1252, Shift-JIS en GB2312.	Microsoft	5.0.20.51904
System.Text.Encodings.Web	Biedt typen voor het coderen en uitsluiten van strings voor gebruik in JavaScript, HyperText Markup Language (HTML) en Uniform Resource Locators (URL). Is een afhankelijkheid van SOUP IdentityModel	microsoft, dotnetframework	6.0.21.52210
System.Text.Json	Biedt krachtige typen met een lage toewijzingsbehoefte die objecten serialiseren naar JSON-tekst (JavaScript Object Notation) en JSON-tekst deserialiseren naar objecten, met ingebouwde UTF-8-ondersteuning. Biedt ook typen om JSON-tekst te lezen en te schrijven die is gecodeerd als UTF-8, en om een Document Object Model (DOM) in het geheugen tot stand te brengen dat alleen-lezen is, voor willekeurige toegang tot de JSON-elementen binnen een gestructureerde weergave van de gegevens.	Microsoft	6.0.222.6406
System.Threading.Tasks.Extensions	Biedt extra typen die het schrijven van gelijktijdige en asynchrone code vereenvoudigen.	microsoft, dotnetframework	4.6.28619.01

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System.Threading.Channels	Biedt een set synchronisatiedatastructuren om gegevens door te geven tussen producenten en consumenten, ter ondersteuning van hoogwaardige parallelle programmering.	Microsoft	6.0.21.52210
System.ValueTuple	Biedt de System.ValueTuple-structuren, die de onderliggende typen voor tuples implementeren in C# en Visual Basic. Voegt ondersteuning voor waarde-tuples toe, aangezien deze pas in latere versies van het .NET Framework zijn opgenomen.	microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy.dll	Een Behavior-Driven Development (BDD) framework voor .NET	TestStack Community	4.3.2.0
Thrift	Gebruikt voor de definitie van het remotelink-protocol	Apache	0.13.0.0
Unity.Container	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	5.8.13.0
Unity.Configuration	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	5.2.5.0
Unity.Abstractions	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	3.3.1.0
Unity.Interception.Configuration	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	5.1.7.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Unity. Interception	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	5.5.5.0
Unity. Registration ByConvention	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	2.1.9.0
Unity. ServiceLocation	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	2.1.2.0
WAP BT Dongle Driver	WAP BT Dongle-stuurprogramma (dongle voor aanpassingen)	iAnywhere Solutions	3.0.0.6095
WebSync	Wordt gebruikt voor integratie van het aanpasgevenskanaal	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor. dll	Een hexadecimaal bewerkingsbesturingselement voor WPF-applicaties	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	Een hulpprogrammabibliotheek voor WPF-applicaties die scherm- en monitorinformatie levert	FM (Frozen Mountain)	2.1.0.0
Xceed Extended WPF Toolkit	Een verzameling WPF-besturingselementen en -hulpprogramma's die WPF-applicaties uitbreiden met extra UI-componenten.	Xceed	3.5.0.0
xmlunit-core.dll	Een bibliotheek om XML-uitvoer te testen en te vergelijken.	XMLUnit Community	2.9.0.205
Xps to Pdf render (NiXPS)	Converteert programmatisch xps-bestanden naar pdf; wordt gebruikt bij app-rapporten voor aanpassingen.	NiXPS	2.6.7.0

14. REFERENTIES

Titel	Website
Gebruiksaanwijzing (elektronisch)	https://ifu.advancedbionics.com/
Wereldwijd privacybeleid van Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Een back-up maken en het herstellen van de gegevens in uw 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/
De databasecapaciteit van Noah System is bereikt.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer: lijst met gebruikte poorten	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Documentatie over LiveSwitch-serverbeveiliging	https://developer.liveswitch.io/liveswitch-server/server/security.html
EHIMA-whitepaper: Best Practices for Secure Fitting of Hearing Devices (Best-practices voor het aanpassen van hoortoestellen)	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
Tel.: +1.661.362.1400

info.us@advancedbionics.com

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

info.switzerland@advancedbionics.com

Neem in Nederland of Vlaanderen contact op met AB door te mailen naar
[advancedbionics.com/contact](https://www.advancedbionics.com/contact)

AB – A Sonova brand

Vraag uw plaatselijke medewerker van AB naar reglementaire goedkeuring
en beschikbaarheid in uw regio.

Het woordmerk en logo's van Bluetooth® zijn geregistreerde handelsmerken
van Bluetooth SIG, Inc. En deze merken worden door Sonova AG onder
licentie gebruikt.



029-S398-07