Target CI v1.5

HANDLEIDING OVER CYBERBEVEILIGING

Nederlands

Bijgewerkt: september 2025

A Sonova Brand

Inhoud

1. INLEIDING 4
   1.1 AFKORTINGEN EN DEFINITIES: 4
2. OVERIGE HULPBRONNEN 4
   2.1 KLANTENSERVICE 4
   2.2 AB PRO-PORTAL 4
   2.3 GEAVANCEERDE INSTALLATIEHANDLEIDING 5
   2.4 MDS2 5
   2.5 GEBRUIKSAANWIJZING 5
   2.6 HIMSA 5
3. NETWERK- EN CONTEXTDIAGRAMMEN 5
   3.1 IMPLEMENTATIEMODEL 1: STAND-ALONE 6
   3.2 IMPLEMENTATIEMODEL 2: NOAH DISTRIBUTED 6
   3.3 IMPLEMENTATIEARTEFACTEN 7
   3.4 SYSTEEMVERBINDINGEN 8
4. SYSTEEMVEREISTEN 10
5. INSTALLATIE 10
   5.1 VEREISTEN 10
   5.2 TYPEN INSTALLATIEPROGRAMMA'S 10
6. BEVEILIGINGSCONTROLES 11
   6.1 AUTHENTICATIE – STAND-ALONE IMPLEMENTATIE 11
   6.2 AUTHENTICATIE – NOAH-IMPLEMENTATIE 11
   6.3 AUTORISATIE 11
   6.4 AUDIT – STAND-ALONE IMPLEMENTATIE 11
   6.5 AUDIT – NOAH-IMPLEMENTATIE 11
   6.6 EXTERNE TOEGANG 11
7. GEGEVENSBESCHERMING 12
   7.1 PRIVACYBELEID VAN ADVANCED BIONICS 12
   7.2 FEDERALE GEGEVENSVERWERKINGSNORMEN (FIPS) 12
   7.3 VEILIGHEID TIJDENS OVERDRACHT 12
   7.4 BEVEILIGING TIJDENS INACTIVITEIT 13
8. SOFTWARE-INTEGRITEIT 15
   8.1 VERIFICATIE VAN GEDOWNLOADE INSTALLATIEMEDIA 15
   8.2 HANDMATIGE VERIFICATIE VAN DE AANPASSOFTWARE VÓÓR DE INSTALLATIE 16

8.3 AUTOMATISCHE VERIFICATIE VAN DE INTEGRITEIT VAN DE GEÏNSTALLEERDE AANPASSOFTWARE 17
8.4 HANDMATIGE VERIFICATIE VAN DE INTEGRITEIT VAN DE GEÏNSTALLEERDE AANPASSOFTWARE 17
9. SOFTWARE-PATCHES EN -UPDATES 18
10. GEGEVENSBEHEER 18
10.1 DATABASES 18
10.2 GEGEVENSMIGRATIE 19
10.3 HOORTOESTELCONFIGURATIES 19
10.4 GEGEVENS VERWIJDEREN 19
11. BEVEILIGDE OMGEVING – GEZAMENLIJKE VERANTWOORDELIJKHEID 19
12. PRODUCTIE- EN SOFTWAREONTWIKKELINGSPROCES 20
13. SOFTWARECOMPONENTEN EN MATERIAALLIJST 21
14. REFERENTIES 29

1. INLEIDING

Dit document bevat informatie met betrekking tot technische beveiliging en privacy over het Target CI v1.5-softwaresysteem 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 v1.5
- AB-websites
- mobiele applicaties van AB
- AB-hoortoestellen

1.1 AFKORTINGEN EN DEFINITIES:

Acroniem	Trefwoord
FSW	Aanpassoftware
Audicien	Audicien
SaMD	Software als medisch hulpmiddel
AB	Advanced Bionics
IFU	Gebruiksaanwijzing

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 v1.5 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 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 voor de aanpassoftware van AB. Dit formulier is op aanvraag verkrijgbaar.

2.5 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
- Installatie-instructies
- Technische ondersteuning

2.6 HIMSA

HIMSA is een externe softwareleverancier die Noah System 4 produceert: een softwaresysteem dat speciaal is ontworpen voor de gehoorsector en dat audiciens een leveranciersonafhankelijk 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/

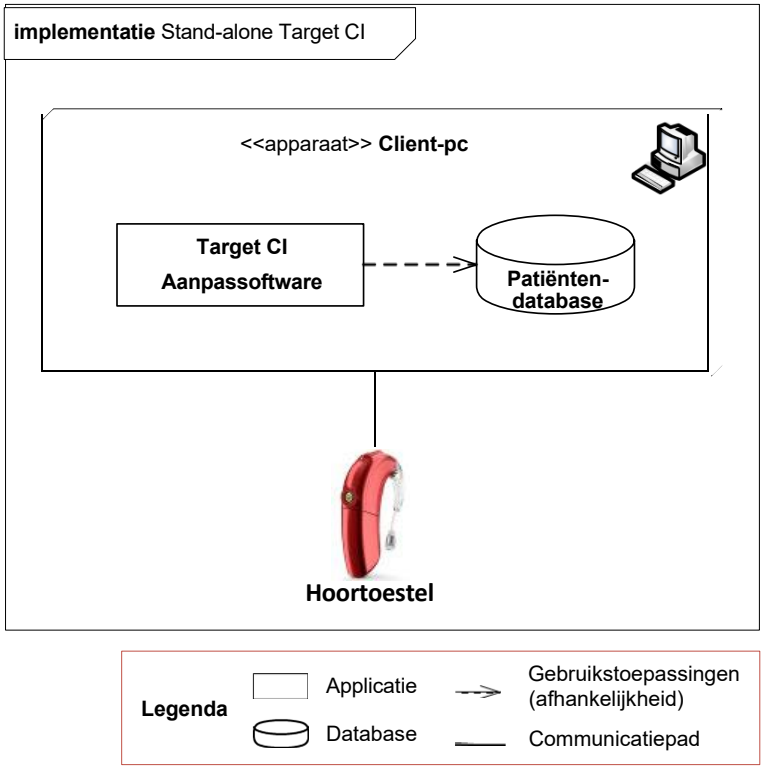
Raadpleeg het hoofdstuk Security (Beveiliging) van het HIMSA Learning Center voor aanvullende informatie over beveiliging: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

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.

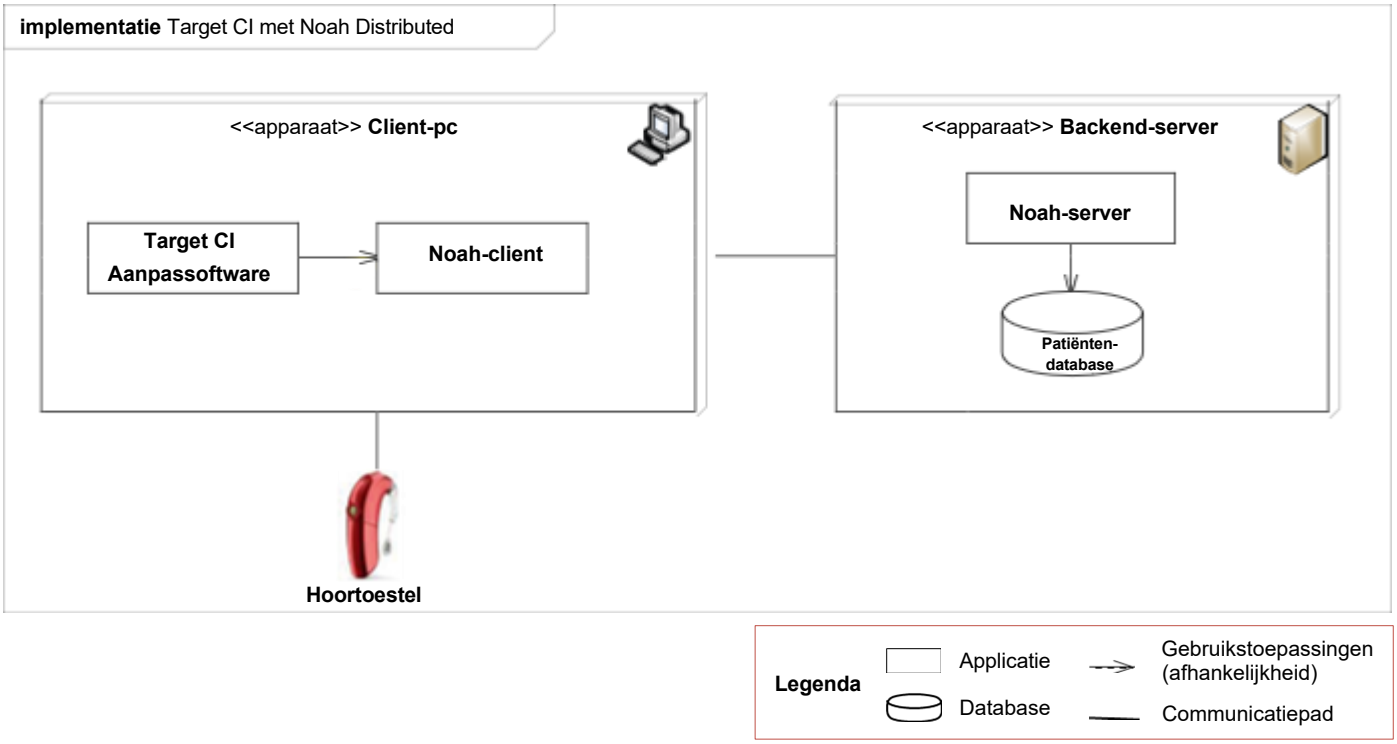
3.1 IMPLEMENTATIEMODEL 1: STAND-ALONE

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 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.

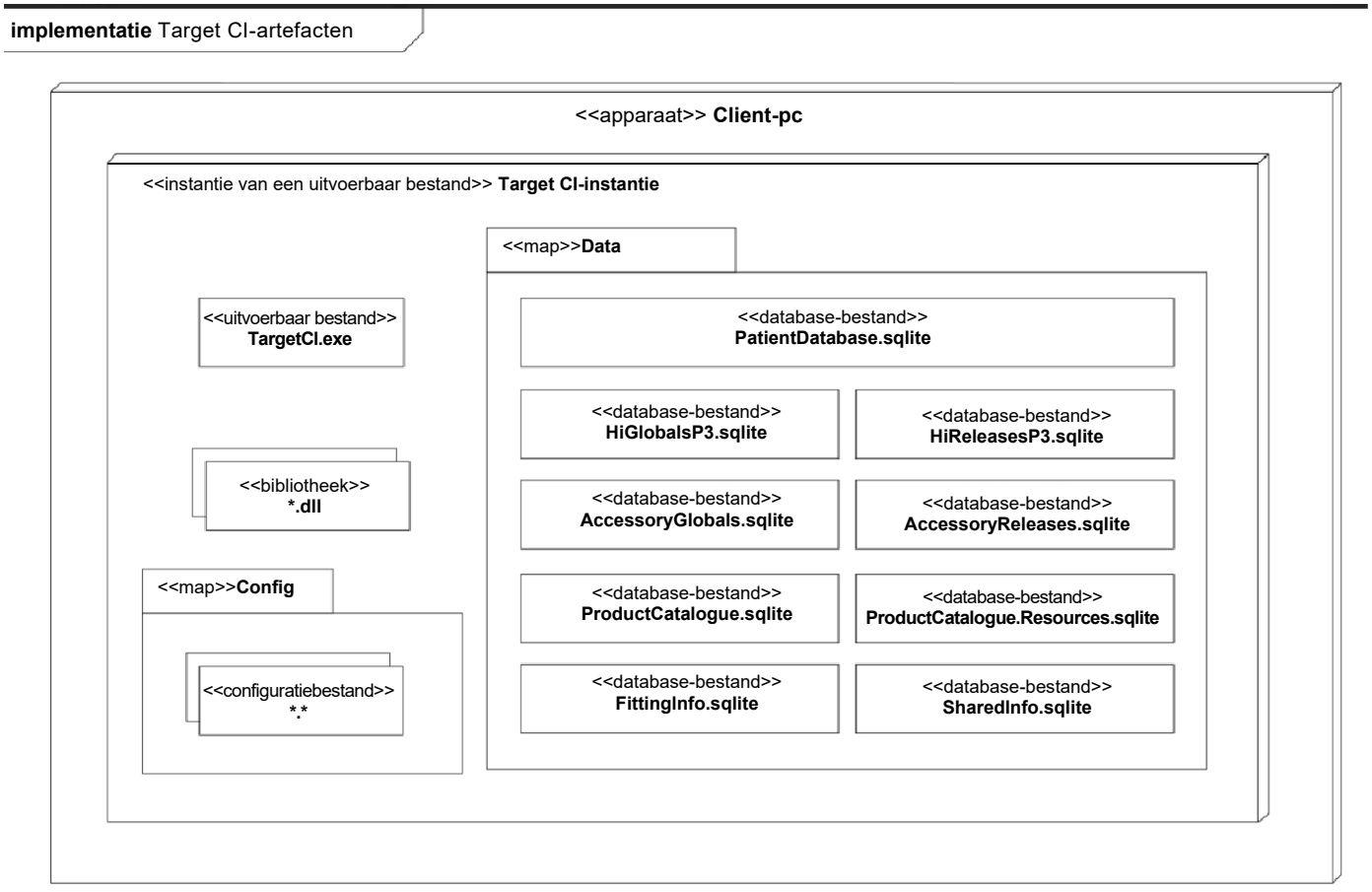


3.3 IMPLEMENTATIEARTEFACTEN

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.

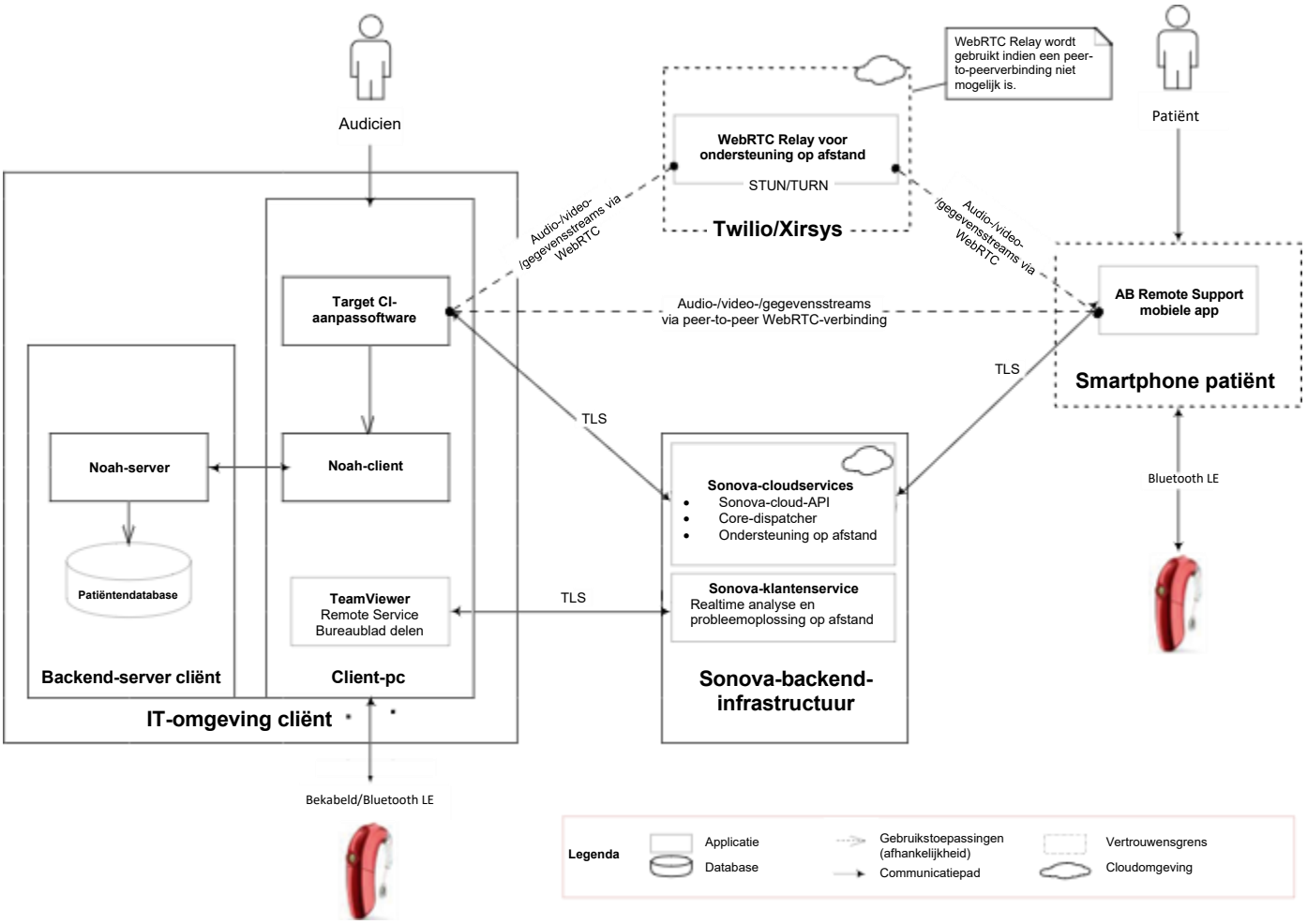
In de transactionele database, PatientDatabase.sqlite, worden de demografische gegevens en de aanpassingsgegevens van de patiënt opgeslagen. Deze database wordt alleen geïnstalleerd wanneer de aanpassoftware in de stand-alone modus wordt geïmplementeerd.

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	Beschrijving
Hoortoestellen	Hoortoestelcom-municatie	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
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 implementatiemodel van Noah Distributed)

Bron/ bestemming	Service	Protocol	Poort	Beschrijving
Sonova-cloudservices	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 aanpassoftware-client op te halen uit de Sonova backend-opslag • gegevens over logging en analyses over te dragen • realtime aanpassessies op afstand tot stand te brengen
Twilio/Xirsys, AB Remote Support mobiele app	Ondersteuning op afstand	WebRTC	De lijst met poorten is op aanvraag verkrijgbaar	De cloudcommunicatieservices van Twilio worden gehost op cloudplatforms van derden, met name Amazon Web Services (AWS) en Google Cloud Platform (GCP). Deze services worden uitsluitend gebruikt voor ondersteuning op afstand van de aanpassoftware, waardoor WebRTC-signalering en realtime aanpassessies op afstand mogelijk worden gemaakt.
AB-klantenservice	Bureaublad delen	Bedrijfseigen 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 aanpassoftware. Raadpleeg hoofdstuk 6.6 SERVICE OP AFSTAND voor meer informatie.

4. SYSTEEMVEREISTEN

Besturingssysteem	Windows 10 Pro/Enterprise, 64-bits
.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 4.14 of hoger)
Internetverbinding	Voor ondersteuning op afstand en analyseregistratie is een internetverbinding vereist. Raadpleeg hoofdstuk 4.4 Interconnecties systeem. Intranet is vereist bij gebruik van Noah System 4 in een netwerk.
Netwerkpoorten	Raadpleeg hoofdstuk 3.4 Interconnecties systeem. Raadpleeg hoofdstuk 3. Overige hulpbronnen — HIMSA voor de poorten die door Noah System 4 worden gebruikt.

5. INSTALLATIE

5.1 VEREISTEN

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 valideren 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.

5.2 TYPEN INSTALLATIEPROGRAMMA'S

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 de 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.

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 AUTHENTICATIE – STAND-ALONE IMPLEMENTATIE

Wanneer de aanpassoftware als een stand-alone applicatie wordt geïnstalleerd, is deze afhankelijk van de mechanismen voor toegangscontrole die door het host-besturingssysteem wordt verstrekt. Het host-besturingssysteem kan door het IT-personeel van de klant worden geconfigureerd om de authenticatie te beheren. De aanpassoftware beschikt niet over dergelijke integrale functies. Advanced Bionics adviseert om voor elke gebruikersaccount een unieke gebruikerslogin aan te maken waarmee gebruikers zich kunnen aanmelden op het host-besturingssysteem.

6.2 AUTHENTICATIE – NOAH-IMPLEMENTATIE

Wanneer de aanpassoftware als een Noah-module wordt geïnstalleerd, regelt Noah System 4 de toegangscontrole. Raadpleeg www.HIMSA.com voor de auditcontroles die door Noah System 4 worden gebruikt.

6.3 AUTORISATIE

De aanpassoftware beperkt de toegang tot de functies niet op basis van de rollen van afzonderlijke gebruikers. De software ondersteunt één hoofdfunctie voor het aanmeten van hoortoestellen bij de patiënt en één rol voor de audicien. Op rollen gebaseerde toegangscontroles zijn niet van toepassing.

6.4 AUDIT – STAND-ALONE IMPLEMENTATIE

Wanneer de aanpassoftware als een stand-alone applicatie wordt geïnstalleerd, is deze afhankelijk van de auditmechanismen die door het host-besturingssysteem wordt verstrekt. De aanpassoftware beschikt niet over dergelijke geïntegreerde functies. Het host-besturingssysteem kan door het IT-personeel van de klant worden geconfigureerd om het opstarten/uitvoeren van de aanpassoftware en gebruikerslogins te loggen. Advanced Bionics adviseert om voor elke gebruikersaccount een unieke gebruikerslogin aan te maken waarmee gebruikers zich kunnen aanmelden op het host-besturingssysteem om de controle te bevorderen.

6.5 AUDIT – NOAH-IMPLEMENTATIE

Wanneer de aanpassoftware als Noah-module wordt geïnstalleerd, worden er door het Noah-systeem auditlogs aangemaakt. Raadpleeg http://www.himsa.com/ for auditcontroles die door Noah System 4 worden gebruikt.

6.6 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 te voldoen aan cryptografische protocollen en algoritmestandaarden (RSA) of deze te overtreffen (openbare/publieke sleuteluitwisseling en AES 256-bits sessieversleuteling).

TeamViewer QuickSupport 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 het TeamViewer QuickSupport-hulpprogramma 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 v1.5 voldoet aan de FIPS 140-2-versleutelingsnormen.

7.3 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, BCP195, 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. Gegevensstreams worden gecodeerd met DTLS 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.

7.4 BEVEILIGING TIJDENS INACTIVITEIT

Patiëntendatabase – Stand-alone implementatiemodel

Als de aanpassoftware als een stand-alone applicatie wordt geïnstalleerd, wordt de patiëntendatabase lokaal opgeslagen op: C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

Deze gegevens worden standaard niet-versleuteld opgeslagen. Beschermde gezondheidsgegevens en gegevens voor persoonsidentificatie worden opgeslagen in een database die een integraal onderdeel van de aanpassoftware is, en worden niet via het netwerk verzonden.

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 geauthenticeerd 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

Maak een keuze:

- 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. Het is mogelijk dat de patiëntendatabase die door Noah wordt gehost zich op een andere computer bevindt. 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-netwerkdatabase zijn zichtbaar voor andere apparaatgebruikers op verschillende pc's die over toegangsmachtigingen voor dezelfde netwerkdatabase 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.

Zie www.HIMSA.com voor de versleutelingsnormen die door Noah System 4 worden gebruikt.

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 512 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 apparaat (bijv. CPI-3) dat met behulp van een bekabelde verbinding is aangesloten, via de mobiele AB-applicatie voor ondersteuning op afstand 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.

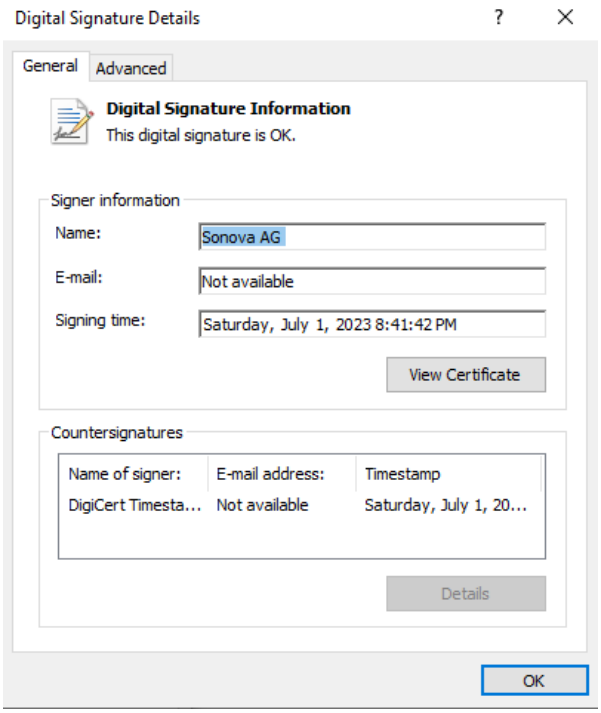
De SHA256-hash voor het zipbestand voor de standaardinstallatie is:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

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 ze 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:



1. Sluit de pop-updialoogvensters en dubbelklik op SonovaVerify.exe.
2. Controleer of 'NO ERRORS DETECTED' (Geen fouten gedetecteerd) wordt weergegeven, zoals aangegeven in de volgende afbeelding:

In de afbeelding kunt u zien dat SonovaVerify de digitale handtekeningen van alle bestanden op de installatiemedia, waaronder het installatieprogramma, heeft geverifieerd. Hiermee wordt gecontroleerd of de installatiemedia niet zijn aangepast, beschadigd zijn of op een andere manier zijn aangetast. SonovaVerify geeft waarschuwingen of foutmeldingen weer als er bestanden of mappen ontbreken of als er onverwachte bestanden of mappen aan de installatiemedia zijn toegevoegd.

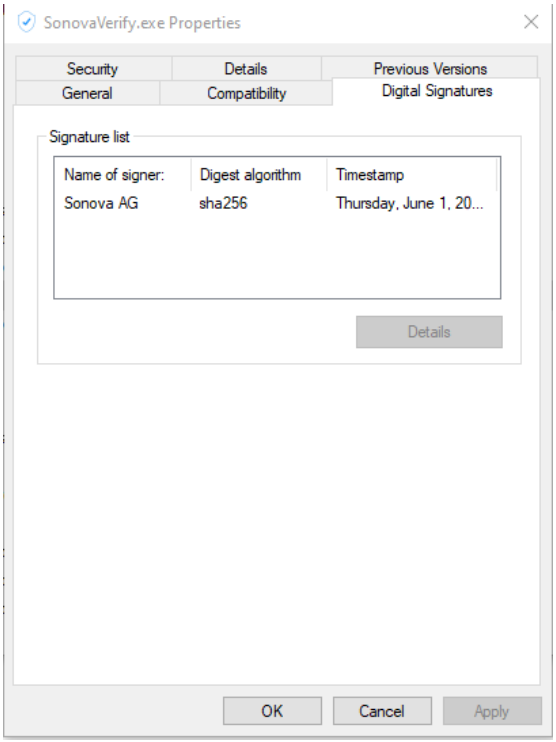
8.3 AUTOMATISCHE VERIFICATIE VAN DE INTEGRITEIT VAN DE GEÏNSTALLEERDE AANPASSOFTWARE

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 waarschuwingsmeldingen 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:



1. Sluit de pop-updialoogvensters en dubbelklik op SonovaVerify.exe.
2. Controleer of 'NO ERRORS DETECTED' (Geen fouten gedetecteerd) wordt weergegeven, zoals aangegeven in de volgende afbeelding:

In de afbeelding kunt u zien dat SonovaVerify de digitale handtekeningen van alle geïnstalleerde bestanden heeft geverifieerd. Hiermee wordt gecontroleerd of de aanpassoftware niet is aangepast, beschadigd is of op een andere manier is aangetast. SonovaVerify geeft waarschuwingen of foutmeldingen weer als er bestanden of mappen ontbreken of als er onverwachte bestanden of mappen aan de bestandsmap zijn toegevoegd.

9. SOFTWARE-PATCHES EN -UPDATES

Automatische updates worden niet ondersteund.

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 configuratie en instellingen van het hoortoestel te exporteren en importeren.

10.4 GEGEVENS VERWIJDEREN

In de gebruiksaanwijzing of op de volgende site voor Noah-implementaties vindt u instructies voor het verwijderen van gegevens: 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
- Pas auditcontroles toe op besturingssysteemniveau
- Houd het besturingssysteem up-to-date
- Houd de geïnstalleerde versie van de aanpassoftware up-to-date
- Schakel up-to-date malware- en antivirusbescherming in
- Schakel whitelists voor de applicatie in

Gegevensbescherming

- Versleutel patiëntgegevens met behulp van hulpmiddelen of controlemechanismen van derden op besturingssysteemniveau, bijvoorbeeld door schijfversleuteling te gebruiken (bijvoorbeeld de gratis Microsoft BitLocker) om alle gegevens te beschermen. Als u gebruikmaakt van Noah, 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 ervoor dat de gegevens altijd worden beveiligd:
    - Wanneer u gegevens via onveilige kanalen overdraagt, verstuur dan anonieme gegevens of versleutel ze.
    - 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 hulpmiddelen 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 gebruikers die geen toegang tot het werkstation mogen hebben.
- Zorg ervoor dat onbevoegde personen het systeem niet kunnen aantasten.
- 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 scherminhoud alleen door de gebruiker kan worden bekeken.

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.
- Als u verdachte activiteiten opmerkt in uw accounts voor de aanpassoftware of onverwachte handelingen opmerkt, dient u contact op te nemen 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- EN SOFTWAREONTWIKKELINGSPROCES

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.

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
ciAD Hearingloss Simulator	Bibliotheek met gehoorverliessimulatoren voor mediaspeler	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	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
Destructurama.Attributed	Gebruikt door Nephele-bibliotheken.	Serilog-bijdragers	3.0
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 Fitting formula library	National Centre for Audiology, Canada	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical aangepast voor Sonova	GNOtometrics	2.0.1.9
IceLink	Wordt gebruikt voor integratie van audio/video-gesprekken via WebRTC	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	OpenID Connect en OAuth 2.0-clientbibliotheek gebruikt door de Kona.CommonServices.Authentication-component voor OAuth 2-authenticatie.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	Noah-interfacebibliotheek voor intermodulaire communicatie	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	Wordt gebruikt door bibliotheken van Sonova om te communiceren met Git	LibGit2Sharp-bijdragers	0.26.1
Mapster	Wordt gebruikt voor het toewijzen van objecten in code	chaowlert,eric_swann	7.2.0.0
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	5.0.0
Microsoft.CodeAnalysis.Common	Wordt gebruikt door de bibliotheken van Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	Wordt gebruikt door de bibliotheken van Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
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
Microsoft.IdentityModel.Logging	Afhankelijkheid van Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	Afhankelijkheid van de SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	Wordt gebruikt voor de FSW-back-uptool (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.	xamlexperiencesteam, Microsoft	1.0.1
MS VC++ 2008 Redistributable	Microsoft Visual C++ 2008 Redistributable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Visual C++ 2010 Redistributable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistributable	Microsoft Visual C++ 2012 Redistributable	Microsoft	11.0.61030.0
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
MS-VisualC++ 7.1 runtime-bibliotheken	Microsoft Visual C++ runtime-bibliotheken	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	Wordt gebruikt om het volume aan te passen en geluidsbestanden af te spelen.	Open-source	1.9
.NET Framework	.NET runtime framework	Microsoft	4.8.3928.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Newtonsoft.Json	Wordt gebruikt voor JSON-serialisatie en -deserialisatie.	James Newton-King	12.0.3
Nibelung	NoahLink Wireless-aanpasbibliotheken	GN ReSound	1.3.16.1
Nlog	Dit is een afhankelijkheid van de HIMSA Nibelung.CPD (Noahlink Wireless)	Kim Christensen	4.4.0
NoahLink	Stuurprogramma NoahLink-aanpasapparaat	HIMSA	1.55.6.166
NoahLink Wireless	Stuurprogramma NoahLink Wireless-aanpasapparaat	HIMSA	2.0.0.68
Otometrics.HiPro2	HiPro-communicatiebibliotheken	GNOtometrics	2.0.0.4
Otometrics.REMaccess	Abstractielaag van Otometrics boven de Noah-interfacebibliotheek voor intermodulaire communicatie	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	De C# pdf-bibliotheek voor het maken en bewerken van pdf-documenten in .Net-applicaties.	Patagames.com	4.54.2704.0
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	7.2.1
Polly.Extensions.Http	Een bibliotheek met eigenzinnige, handige methoden voor het configureren van Polly-beleid voor het verwerken van tijdelijke fouten die gebruikelijk zijn voor het aanroepen via een http-client.	App vNext	3.0
Polly.Contrib.WaitAndRetry	Een bibliotheek voor Polly met hulpmethoden voor verschillende strategieën voor Wait en Retry.	Grant Dickinson, App vNext	1.1.1
Portable.BouncyCastle	Dit is een afhankelijkheid van de HIMSA Nibelung.CPD (Noahlink Wireless)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	Serialisatieframework gebruikt voor RC blob.	Open-source	2.0.0.668
Serilog	De loggingcomponent die voor de gehele Chinook-applicatie wordt gebruikt.	Serilog-bijdragers	2.10.0
Serilog.Enrichers.Thread	Serilog-gebeurtenissen verrijken met eigenschappen van de huidige thread	Serilog-bijdragers	3.1
Serilog.Expressions	Expressiegebaseerde gebeurtenisfiltering voor Serilog.	Serilog-bijdragers	2.0
Serilog.Sinks.Console	Een Serilog-sink die loggebeurtenissen naar de console/terminal logt.	Serilog-bijdragers	4.0.0.0
Serilog.Sinks.Debug	Een Serilog-sink die logboekgebeurtenissen naar het debug-uitvoervenster schrijft.	Serilog-bijdragers	2.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Serilog.Sinks.File	Schrijft Serilog-gebeurtenissen naar tekstbestanden in algemene tekst of JSON-indeling.	Serilog-bijdragers	4.1
Serilog.Sinks.Trace	De diagnostische trace-sink voor Serilog.	Serilog-bijdragers	2.1
Serilog.Settings.AppSettings	XML-configuratie (System.Configuration <appSettings>)-ondersteuning voor Serilog.	Serilog-bijdragers	2.2.2
Security.Cryptography	Uitbreidingen van de beveiligings-API's die bij het .NET Framework worden geleverd	Microsoft	1.7.2
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 compressiefunctionaliteit (zippen, uitpakken, streamingcompressie enz.). Wij gebruiken deze in de firmware-updateapp.	Open-source	1.1.0.145
Superpower	Een parser-combinatorbibliotheek voor C#	Datalust, Superpower-bijdragers, Sprache-bijdragers	2.3
SQLite.Interop	SQLite is een softwarebibliotheek die een relationeel databasebeheersysteem biedt. Het woord 'lite' in SQLite betekent lichtgewicht wat betreft installatie, databasebeheer en benodigde bronnen. SQLite heeft de volgende opvallende kenmerken: zelfstandig, serverloos, geen configuraties, transactioneel. Het is een database (SQLite 3.32.1) om informatie over de patiënt (in stand-alonemodus), onze productcatalogusbronnen en de metagegevens voor aanpassingen, accessoires en de hoortoestellen op te slaan.	SQLite-ontwikkelingsteam	1.0.113
System.Buffers	Biedt resourcepooling van elk type voor prestatiekritieke applicaties die regelmatig objecten toewijzen en vrijgeven.	23rogramma,dotnetframework	4.5.1
System.Collections.Immutable	Wordt gebruikt door de bibliotheken van Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0
System.ComponentModel.Annotations	Biedt kenmerken die worden gebruikt om metagegevens te definiëren voor objecten die als gegevensbronnen worden gebruikt.	23rogramma,dotnetframework	4.7
System.Configuration.ConfigurationManager	Biedt typen die het gebruik van configuratiebestanden ondersteunen.	Microsoft	5.0
System.Data.SQLite.Core	Wordt gebruikt door de bibliotheken van Sonova.HardwareAbstraction. Palio.Trafo	SQLite-ontwikkelingsteam	1.0.113.7

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System.Drawing.Common	Biedt toegang tot grafische GDI+-functionaliteit.	Microsoft	5.0.1
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
System.IO.Abstractions	Een set abstracties om interacties met bestandssystemen testbaar te maken.	Tatham Oddie en vrienden	12.0.10
System.Numerics.Vectors	Biedt hardwareversnelde numerieke typen, geschikt voor hoogwaardige verwerking en grafische applicaties.	24rogramma,dotn etfra me work	4.5
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.	24rogramma,dotn etfra me work	4.5.4
System.Reactive.Core	Reactive Extensions (Rx) voor .NET	.NET Foundation	3.1.1
System.Reactive. Interfaces	Reactive Extensions (Rx) voor .NET	.NET Foundation	3.1.1
System.Reactive.Linq	Reactive Extensions (Rx) voor .NET	.NET Foundation	3.1.1
System.Reactive.PlatformServices	Reactive Extensions (Rx) voor .NET	.NET Foundation	3.1.1
System.Reactive.Windows.Threading	Reactive Extensions (Rx) voor .NET	.NET Foundation	3.1.1
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	4.7.1
System.Reflection.Metadata	Dit pakket bevat een low-level .NET (ECMA-335) metadata-lezer en -schrijver. Hij 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
System.Runtime.CompilerServices.Unsafe	Biedt de klasse System.Runtime.CompilerServices.Unsafe die generieke functionaliteit op laag niveau voor het manipuleren van pointers verstrekt.	24rogramma, dotnetframework	5.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
System.Security.AccessControl	Biedt basisklassen waarmee toegangs- en auditcontrolelijsten voor beveiligde objecten kunnen worden beheerd.	Microsoft	5.0
System.Security.Permissions	Biedt typen die Code Access Security (CAS) ondersteunen.	Microsoft	5.0
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
System.Text.Encoding.CodePages	Biedt ondersteuning voor op codepagina's gebaseerde coderingen, waaronder Windows-1252, Shift-JIS en GB2312.	Microsoft	5.0
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	24rogramma,dotn etfra me work	5.0
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	5.0.1
System.Threading.Tasks.Extensions	Biedt extra typen die het schrijven van gelijktijdige en asynchrone code vereenvoudigen.	25rogramma,dotnetfra mework	4.5.4
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.	25rogramma,dotnetfra mework	4.5.0
Thrift	Gebruikt voor de definitie van het remotelink-protocol	Apache	0.13.0.0
Unity	De Unity Container (Unity) is een volledig functionele, uitbreidbare container voor afhankelijkheidsinjectie.	Unity Container Project	5.8.13
WAP BT Dongle Driver	WAP BT Dongle-stuurprogramma (dongle voor aanpassingen)	iAnywhere Solutions	3.0.0.6095
WebSync	Wordt gebruikt voor integratie van het aanpasgegevenskanaal	FM (Frozen Mountain)	4.9.32.0

SOUP-ITEM	FUNCTIONALITEITSBESCHRIJVING	FABRIKANT	VERSIE
Xps to Pdf render (NiXPS)	Converteert 25rogrammatically 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

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

Neem in Nederland of Vlaanderen contact op met AB via
advancedbionics.com/contact

AB – A Sonova brand

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

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S396-07 Rev A 2025-09-15