ADVANCED BIONICS
POWERFUL CONNECTIONS

Target CI v1.6

VEILEDNING I CYBERSIKKERHET

Norsk

Oppdatert: juli 2026



A Sonova brand

NO

Innhold

1. INNLEDNING 3
   1.1 FORKORTELSER OG DEFINISJONER: 3

2. ANDRE RESSURSER 4
   2.1 KUNDESUPPORT 4
   2.2 AB PRO PORTAL 4
   2.3 AVANSERT INSTALLASJONSVEILEDNING 4
   2.4 TARGET CI-BRANNMURKONFIGURASJON 4
   2.5 MDS2 4
   2.6 BRUKSANVISNING (IFU) 5
   2.7 HIMSA 5

3. NETTVERKS- OG KONTEKSTDIAGRAMMER 6
   3.1 UTPLASSERINGSMODDELL 1: FRITTSTÅENDE 6
   3.2 UTPLASSERINGSMODDELL 2: NOAH DISTRIBUTED 7
   3.3 UTPLASSERINGSARTEFAKTER 8
   3.4 SYSTEMSAMMENKOBLINGER 9

4. SYSTEMKRAV 11

5. CYBERSIKKERHET I PRODUKTLIVSSYKLUSEN 12
   5.1 DISTRIBUSJON 12
   5.2 Installasjon 12
   5.3 KONFIGURASJON OG BRUK 13
   5.4 FJERNING OG AVVIKLING 14

6. SIKKERHETSKONTROLLER 16
   6.1 TILGANGSKONTROLL 16
   6.2 REVISJONSLOGGING OG ANSVARLIGHETSKONTROLLER 17
   6.3 EKSTERN TILGANG 17

7. INFORMASJONSBESKYTTELSE 18
   7.1 PERSONVERNERKLÆRING FOR ADVANCED BIONICS 18
   7.2 AMERIKANSKE FØDERALE STANDARDER FOR INFORMASJONSBEHANDLING (FIPS) 18
   7.3 PERSONLIG IDENTIFISERENDE INFORMASJON/ HELSEOPPLYSNINGER SOM BEHANDLES AV PRODUKTET 18
   7.4 SIKKERHET UNDER OVERFØRING 19
   7.5 SIKKERHET FOR LAGREDE DATA 20

NO

8. PROGRAMVAREINTEGRITET 23
8.1 VERIFISERING AV NEDLASTET INSTALLASJONSMEDIUM 23
8.2 MANUELL VERIFISERING AV TILPASNINGSPROGRAMVAREN FØR INSTALLASJON 24
8.3 AUTOMATISK VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE 25
8.4 MANUELL VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE 26

9. PROGRAMVAREOPPDATERINGER OG -OPPDATERINGSFILER 28

10. DATABEHANDLING 28
10.1 DATABASER 28
10.2 DATAMIGRASJON 28
10.3 KONFIGURASJONER AV HØREAPPARATER 28
10.4 DATADESTRUKSJON 28

11. SIKKERHETSMILJØ – DELT ANSVAR 29

12. PRODUKSJON, PROGRAMVAREUTVIKLING OG SIKKERHETSSTYRING 31

13. PROGRAMVAREKOMPONENTER OG STYKKLISTE 32

14. REFERANSER 49

1. INNLEDNING

Dette dokumentet gir teknisk informasjon om sikkerhet og personvern for Target CI v1.6 programvaresystem fra Advanced Bionics, heretter kalt «tilpasningsprogramvaren.» Tilpasningsprogramvaren er utviklet for bruk av kvalifiserte audiografer for å konfigurere (dvs. tilpasse) høreapparater for pasienter som har fått cochleaimplantater fra Advanced Bionics.

Dette dokumentet fokuserer spesielt på hensynene til cybersikkerhet og personvern som er relevante for bruken av tilpasningsprogramvaren. Den inkluderer en evaluering av sikkerhets- og personvernkontrollene som for øyeblikket er integrert i programvaren, samt de som forventes å bli brukt og konfigurert i IT-miljøet der produktet skal brukes til det tiltenkte formålet.

Dette dokumentet inneholder ikke teknisk sikkerhets- og personverninformasjon om:

- Tidligere versjoner av AB-tilpasningsprogramvare
- Annen AB-programvare enn Target CI v1.6
- AB-nettsteder
- AB mobilapplikasjoner
- AB høreapparater

1.1 FORKORTELSER OG DEFINISJONER:

Forkortelse	Begrep
FSW	Tilpasningsprogramvare
SaMD	Programvare som medisinsk utstyr
Noah	Et tredjeparts pasientadministrasjonssystem fra HIMSA som brukes til å lagre og administrere demografiske opplysninger om pasienter og tilpasningsdata.
TeamViewer	Et verktøy for ekstern tilgang og skrivebordsdeling på tvers av plattformer.
SOUP	Programvare av ukjent opprinnelse
HCP	Audiograf
SaMD	Programvare som medisinsk utstyr
AB	Advanced Bionics
Sonova	Advanced Bionics er et heleid datterselskap av Sonova og fungerer som en integrert enhet i Sonova-konsernet.
IFU (Bruksanvisning)	Bruksanvisning
PHI	Personlig helseinformasjon
PII	Personlig identifiserende informasjon
SBOM	Programvarekomponentliste

NO

2. ANDRE RESSURSER

2.1 KUNDESUPPORT

For de som befinner seg innenfor USA og Canada, tilbyr Advanced Bionics et gratis telefonnummer for teknisk støtte (877-271-6727) der dedikert profesjonell support er tilgjengelig fra mandag til fredag fra kl. 05.00 til 17.00 (PST).

Hvis du befinner deg utenfor USA og Canada, leveres teknisk support lokalt. Hvis du har spørsmål om tilpasningsprogramvaren, tilhørende maskinvare eller andre programmeringsspørsmål, kontakter du din lokale AB-representant.

2.2 AB PRO PORTAL

Tilpasningsprogramvaren og tilhørende dokumentasjon kan lastes ned fra https://www.abproportal.com eller Sonova Web Client. En kontoinnlogging er nødvendig. Denne ressursen er muligens ikke tilgjengelig i alle markeder. Kontakt din AB-representant for mer informasjon.

2.3 AVANSERT INSTALLASJONSVEILEDNING

Den avanserte installasjonsveiledningen for Target CI v1.6 er tilgjengelig på forespørsel. Veiledningen gir teknisk informasjon om installasjonsprogrammet for tilpasningsprogramvaren, inkludert kommandolinjealternativer for stille og automatiserte installasjoner.

2.4 TARGET CI-BRANNMURKONFIGURASJON

Dokumentet for brannmurkonfigurasjon er tilgjengelig på forespørsel. Dette dokumentet gir IT-rettet veiledning for å sikre at Target CI 1.6 fungerer bak en bedriftsbrannmur, og beskriver kravene til HTTP-/HTTPS-tilgang samt de viktigste vertsnavnene. Den omhandler WebRTC-tilkobling via Twilio og Xirsys, og beskriver porter for TURN og peer-relay, samt påpeker at mange IP-adresser er dynamiske, slik at regler basert på vertsnavn bør brukes der det er mulig.

2.5 MDS2

Produsentens erklæring om sikkerhet for medisinsk utstyr (MDS2) er et bransjestandardskjema som inneholder informasjon om sikkerhet og personvern om ABs tilpasningsprogramvare. Dette skjemaet er tilgjengelig på forespørsel.

2.6 BRUKSANVISNING (IFU)

Bruksanvisningen leveres med programvareinstallasjonsmediet. For enkelte markeder er den elektroniske bruksanvisningen tilgjengelig for nedlasting på www.advancedbionics.com/ifu

Følgende avsnitt i bruksanvisningen kan være relevante for IT-fagfolk:

- Produktbeskrivelse
- Minimumskrav for system og ytelsesegenskaper
- Retningslinjer for IT-sikkerhet
- Bruksanvisning
- Kassering og farlige stoffer
- Teknisk kundestøtte

2.7 HIMSA

The Hearing Instrument Manufacturer's Software Association (HIMSA) er en tredjeparts programvareleverandør som utvikler Noah System 4, et programvaresystem utviklet for høreapparatbransjen som gir fagpersoner innen hørselsomsorg et leverandøruavhengig system for å utføre oppgaver knyttet til klienter.

Tilpasningsprogramvaren kan eventuelt konfigureres til å bruke Noah System 4 til datalagring i stedet for en lokal database.

HIMSAs sikkerhetsnettside gir svar på vanlige IT-sikkerhetsspørsmål om Noah System 4.

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

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

Se sikkerhetsdelen av HIMSA-læringssenteret for ytterligere sikkerhetsinformasjon: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

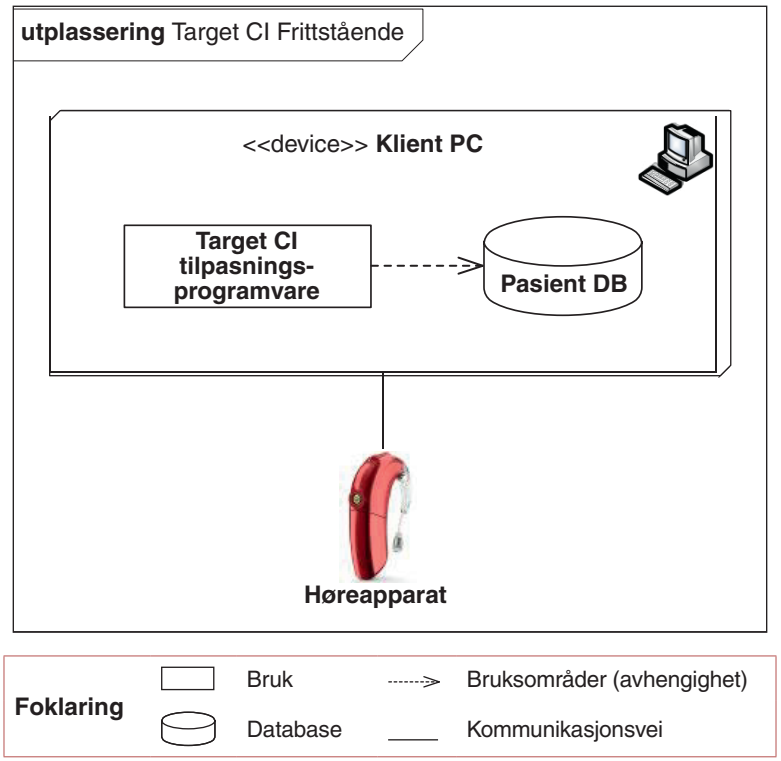
NO

3. NETTVERKS- OG KONTEKSTDIAGRAMMER

To distribusjonsmodeller støttes for tilpasningsprogramvaren, som er et klientprogram (SaMD) installert på en kommersielt tilgjengelig, standard Microsoft Windows-PC. Programvaren inkluderer ikke maskinvare eller operativsystem.

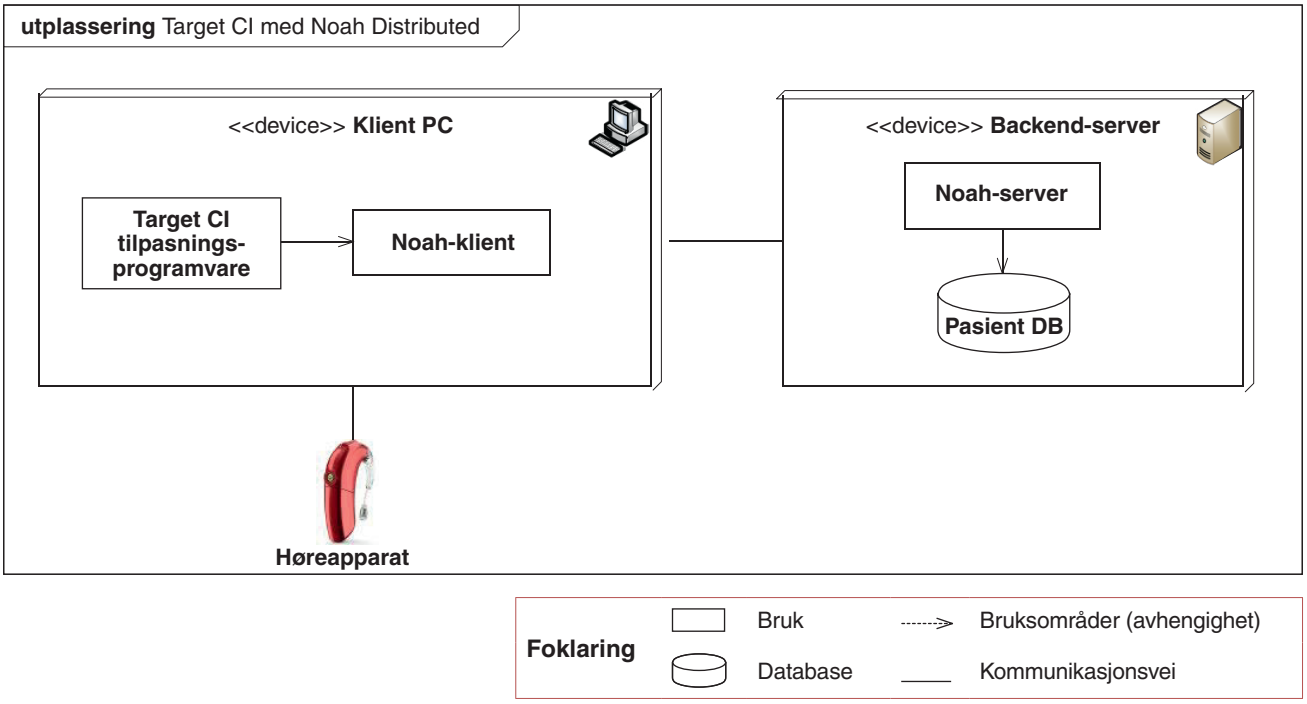
3.1 UTPLASSERINGSMODDELL 1: FRITTSTÅENDE

I den frittstående utplasseringsmodellen installeres tilpasningsprogramvaren på en klient-PC. Pasientdatabasen lagres på samme PC og installeres sammen med tilpasningsprogramvaren.



3.2 UTPLASSERINGSMODDELL 2: NOAH DISTRIBUTED

I Noah Distributeds utplasseringsmodell insalleres tilpasningsprogramvaren til én eller flere klient-PC-er med Noah installert. Noah, et tredjeparts pasientbehandlingssystem, er utplassert på en intern server som er tilgjengelig for klient-PC-ene. Pasientdatabasen lagres på Noah-serveren og er tilgjengelig over nettverket fra én eller flere klient-PC-er.



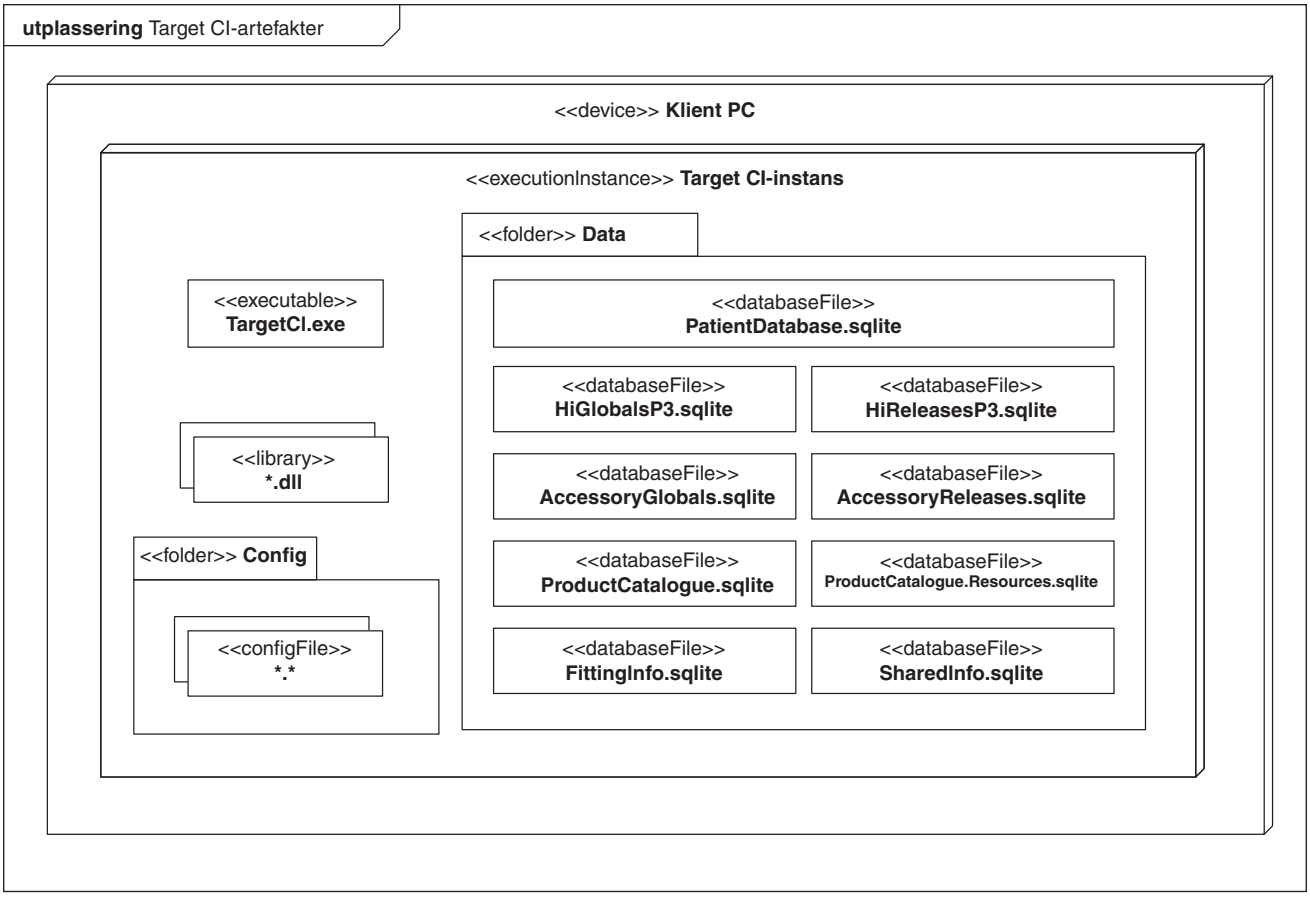
NO

3.3 UTPLASSERINGSARTEFAKTER

Tilpasningsprogramvaren installeres med en kjørbar fil og et sett tilhørende filer, inkludert komponent-DLL-er, konfigurasjonsfiler og SQLite-databasefiler. Konfigurasjonsfilene er installert i mappen «%ProgramData%\ Advanced Bionic\Target CI\Target CI\ Config» og databasefiler er installert i mappen "%ProgramData%\Advanced Bionics\ Target CI\Target CI\Data.» Mappen Data inneholder én transaksjonsdatabasefil og flere informasjonsdatabasefiler.

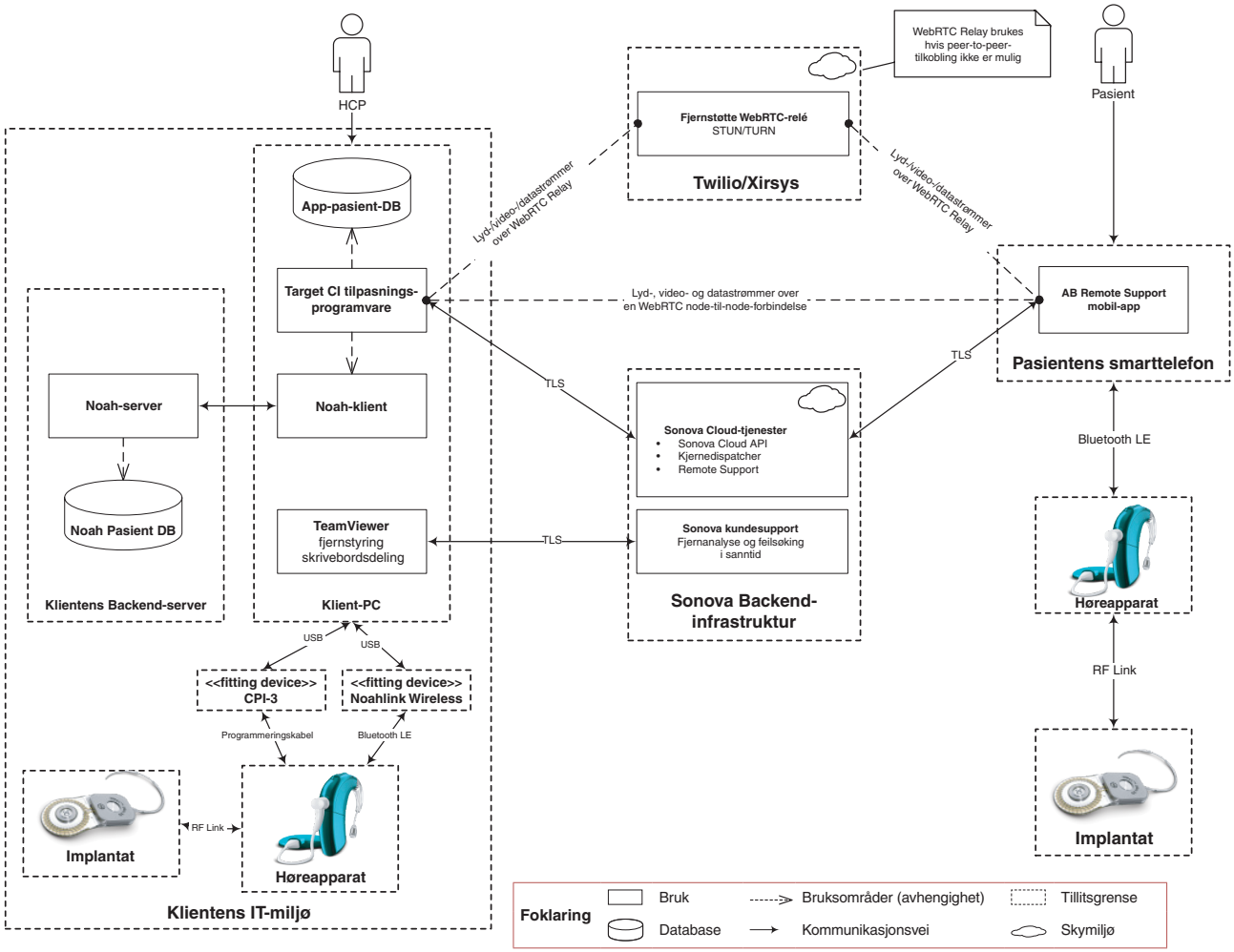
Transaksjonsdatabasen, PatientDatabase.sqlite, lagrer pasientens demografiske data og tilpasningsdata, og installeres kun når tilpasningsprogramvaren utplasseres i frittstående modus.

Når tilpasningsprogramvaren utplasseres som en Noah-modul, leverer Noah-systemet de nødvendige tjenestene for lagring av pasientdata til tilpasningsprogramvaren.
De resterende sqlite-filene er en integrert del av tilpasningsprogramvaren og kreves for alle utplasseringsmodeller.



3.4 SYSTEMSAMMENKOBLINGER

Diagrammet og tabellen nedenfor illustrerer de primære systemsammenkoblingene. Vanligvis blir bare en del av de tilgjengelige sammenkoblingene utnyttet.



Kilde / destinasjon	Tjeneste	Protokoll	Port	Beskrivelse
Høreapparat	Kommunika-sjon med høreapparater	Kablet tilkobling / Bluetooth® Lav energi	Ikke tilgjengelig	Brukes til kommunikasjon med høreapparater for kontroll, konfigurasjon og lesing av status og data.
Noah	Noah 4 ModuleAPI	.NET Remoting	Ikke tilgjengelig	Primærgrensesnittet for modulen som brukes til å få tilgang til Noah-programvaren (kun i Noah distribuert utplasseringsmodell)

NO

Kilde / destinasjon	Tjeneste	Protokoll	Port	Beskrivelse
Sonova Cloud-tjenester	Sonova Cloud API, kjernedis-patcher, fjernstøtte	SOAP, REST	443	Sonova-tjenester som ligger i et Microsoft Azure-datasenter brukes til å: • hente konfigurasjons-data for tilpasnings-programvareklienten fra Sonovas backend-lagring • overføre logg- og analysedata • opprette fjerntilpas-ning i sanntid
Twilio/Xirsys, AB Remote Support og AB Remote Support + mobilapper	Remote Support	WebRTC	Finnes i dokumentet for brann-murkonfigu-rasjon for Target CI	Brukes av funksjonen for ekstern støtte til å utføre WebRTC-signalering og gjennomføre eksterne tilpasningsøkter i sanntid.
AB kunde-support	Skrivebords-deling	TeamViewer proprietær protokoll	5938, 443, 80 Se TeamViewerPorts	Brukes til å utføre ekstern sanntidsanalyse og feilsøking av problemer som påvirker installasjoner av tilpasningsprogramvare. Se avsnitt 6.3 EKSTERN TILGANG for mer informasjon.

4. SYSTEMKRAV

Operativsystem	Windows 10,11, Pro/Enterprise
.NET Framework	Versjon 4.8
CPU	Intel® Core™ i5 eller tilsvarende med lik eller bedre ytelse
RAM	4 GB eller mer
Harddiskplass	3 GB eller mer
Minimumskrav for skjerm	• 1280 x 1024 oppløsning (maksimal skalering 125 %) • 24-bits farge
Enhetsdrivere	• Noahlink Wireless-driver (nyeste versjon tilgjengelig fra HIMSA kreves hvis du bruker et tredjeparts USB-tilkoblet Noahlink Wireless-programmeringsgrensesnitt). • CPI-3-driver (påkrevd hvis du bruker et USB-tilkoblet CPI-3-programmeringsgrensesnitt).
Database	SQLite eller Noah System 4 (versjon 4.16 eller høyere)
Internett-tilkobling	Internett-tilkobling kreves for fjernstøtte og analyselogging, se avsnitt 3.4 Systemtilkoblinger; intranett kreves ved bruk av nettverkstilkoblet Noah System 4.
Nettverksporter	Se avsnitt 3.4 Systemsammenkoblinger; se avsnitt 2. Andre ressurser – HIMSA for porter brukt av Noah System 4.

NO

5. CYBERSIKKERHET I PRODUKTLIVSSYKLUSEN

5.1 DISTRIBUSJON

Godkjente distribusjonsmetoder:

1. Last ned fra Sonova Web Client (SFTP) på https://webclient.sonova.com, eller fra AB Pro Portal på https://www.abproportal.com
2. Installer fra en offisiell Advanced Bionics USB-minnepinne.

Før installasjon skal installasjonsprogrammets digitale signatur verifiseres, og filen skal skannes med oppdatert antivirusprogramvare. Se avsnitt 8 for detaljerte instruksjoner om integritetsverifisering. Ved distribusjon skal det benyttes standard sikkerhetskontroller for IT-systemer i helsesektoren, herunder endepunktbeskyttelse og nettverksbegrensninger.

Når du bruker en USB-minnepinne:

- Bruk kun offisielle USB-minnepinner fra Advanced Bionics.
- Oppbevar USB-enheten fysisk sikret, og ikke endre innholdet.
- Skann USB-enheten og installasjonsmiljøet med oppdatert antivirusprogramvare, og bruk applikasjonshvitelisting.
- Advanced Bionics er ikke ansvarlig for uautoriserte data som er lagret på USB-minnepinner som inneholder installasjonspakken.

5.2 Installasjon

En administratorkonto er nødvendig for å installere tilpasningsprogramvaren. Når programvaren er installert, kan den kjøres uten administratorrettigheter eller utvidede tillatelser.

Se avsnitt 8, Programvareintegritet, for informasjon om verifisering av programvarens integritet før installasjon.

Før installasjon anbefales det at systemadministratorer sørger for at:

- versjonen av tilpasningsprogramvaren som skal installeres er den nyeste tilgjengelige.
- det underliggende operativsystemet er oppdatert.
- Integriteten og autentisiteten til dataene i installasjonsprogrammet for tilpasningsprogramvaren verifiseres. Se avsnitt 8 for informasjon om validering av programvarens integritet før installasjon

To installasjonsprogrammer er tilgjengelige for å installere tilpasningsprogramvaren:

- Installasjonsprogrammet Standard
- Installasjonsprogrammet IT Professional

Installasjonsprogrammet IT Professional er én MSI-fil og ekskluderer nødvendige komponenter, men er ellers tilsvarende installasjonsprogrammet Standard.

Forutsetningskomponenter inkluderer Microsoft .NET Framework v4.8 og Microsoft Visual C++ Omdistribuerbare pakker.

Begge installasjonsprogrammene støtter avanserte installasjonsscenarier, inkludert stille installasjon.

Installasjonsprogrammet IT Professional bør bare brukes hvis organisasjonen din krever at nødvendige komponenter installeres og administreres av organisasjonen din, og ikke av installasjonsprogrammet til tilpasningsprogramvaren. Installasjonsprogrammet Standard bør brukes i alle andre tilfeller.

Installasjonsprogrammet IT Professional kan fås fra ABs kliniske representant. Installasjonsprogrammet IT Professional kan ikke brukes til å reparere, installere på nytt eller avinstallere installasjoner fra standardinstallasjonsprogrammet. Installasjonsprogrammet Standard kan ikke brukes til å reparere, installere på nytt eller avinstallere installasjoner av IT-profesjonelle installasjonsprogrammer.

For avanserte installasjonsscenarier, følg instruksjonene i veiledningen for avansert installasjon av tilpasningsprogramvaren (se avsnitt 2.3). For standard installasjonsscenarioer, se avsnitt 2.5 i dette dokumentet, som inneholder en lenke til bruksanvisningen for tilpasningsprogramvaren (IFU).

5.3 KONFIGURASJON OG BRUK

Tilpasningsprogramvaren støtter et sett med personvern- og sikkerhetskontroller og -funksjoner. Noen av tilpasningsprogramvarens personvern- og sikkerhetsfunksjoner er aktivert som standard, noen kan konfigureres ved installasjon og avhenger av den valgte distribusjonsmodellen, mens andre kan konfigureres under vanlig bruk via programmets grafiske brukergrensesnitt.

Se:

- Avsnitt 6 for en liste over sikkerhetskontroller som forbedrer beskyttelsen av tilpasningsprogramvaresystemet.
- Avsnitt 7 for en liste over sikkerhetskontroller som forbedrer beskyttelsen av data behandlet av tilpasningsprogramvaren

Ytterligere personvern- og sikkerhetskontroller (som ikke støttes av tilpasnings-programvaren på applikasjonsnivå) forventes å bli aktivert og konfigurert av brukere (f.eks. helsepersonell, systemadministratorer og IT-personell) på operativsystemnivå og/eller på IT-infrastrukturnivå. Se avsnitt 11 i dette dokumentet for en detaljert liste over beste praksis-anbefalinger og sikkerhetskontroller for tilpasningsmiljøet der tilpasningsprogramvaren skal brukes.

Brannmur

Tilpasningsprogramvaren er ikke utstyrt med en intern brannmur.

Dersom en ekstern brannmur er aktivert (f.eks. på operativsystemnivå), kan det være nødvendig å oppdatere konfigurasjonen for å tillate den nødvendige inn- og utgående trafikken (f.eks. WebRTC-lyd-, video- og datastrømmer under en økt med ekstern støtte). Se dokumentet for brannmurkonfigurasjon for tilpasningsprogramvaren, som inneholder en liste over nettverksadresser og porter som brukes av tilpasningsprogramvaren.

NO

Proxy-innstillinger

Tilpasningsprogramvaren er utstyrt med en lokal proxy. Gjennom tilpasningsprogramvarens grafiske brukergrensesnitt er det mulig å endre innstillingene til en slik proxy:

- Ingen proxy
- Oppdag proxy-innstillinger automatisk
- Manuell proxy-konfigurasjon. Hvis dette alternativet er valgt, kan følgende innstillinger konfigureres:
  - Adresse
  - Port
  - Aktivere/deaktivere proxygodkjenning (brukernavn, passord, domene)

5.4 FJERNING OG AVVIKLING

Se bruksanvisningen for tilpasningsprogramvaren for detaljert veiledning om avinstallering av programvaren.

Avinstalleringsprogrammet fjerner ikke datakategoriene som er oppført i tabellen nedenfor. Med mindre annet er angitt i kolonnen «Merknader» i tabellen, må slike data fjernes manuelt fra systemene av systemadministratorer, for eksempel ved å fjerne filene manuelt eller ved å slette innholdet på systemdisken som brukes til datalagring.

Datakategori	Standardplassering	Merknader
Applikasjonsdata	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI	Inkluderer følgende type data: • Analysedata • Konfigurasjonsdata • Applikasjonslogger • Midlertidige filer
Personopplysninger	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI\Data	Pasientdatabase (kun relevant for frittstående utplasseringsmodell)
Verktøy for ekstern tilgang	C:\Program Files (x86)\Common Files\ Advanced Bionics\ TeamViewer	Brukes til å utføre sanntidsanalyse og feilsøking av problemer som påvirker tilpasningsprogramvaren, inkludert problemer som oppstår under installasjon og avinstallasjon. Se avsnitt 6.3 for mer informasjon.

Når du avinstallerer tilpasningsprogramvaren fra datamaskinen/den bærbare datamaskinen som skal tas ut av drift eller avhendes, må du sørge for at alle sensitive data (f.eks. personlig helseinformasjon, personlig identifiserende informasjon) er slettet.

For Noah-distribusjoner finnes detaljerte instruksjoner for sletting av data på:

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

Eksterne medier som inneholder data eksportert fra tilpasningsprogramvare, inkludert rapporter og logger, bør sikres. Når dataene ikke lenger brukes, skal de slettes på en sikker måte, og/eller lagringsmediet skal slettes på en sikker måte eller destrueres.

Godkjente prosedyrer og verktøy skal benyttes for sikker sletting av data lagret på flyttbart lagringsmedium i henhold til gjeldende regelverk og retningslinjer for håndtering av pasientinformasjon / personlig identifiserbar informasjon (PII) / beskyttet helseinformasjon (PHI).

NO

6. SIKKERHETSKONTROLLER

Tilpasningsprogramvaren er et klientprogram som er installert på en kommersiell Microsoft Windows-PC. Tilpasningsprogramvaren kan installeres som et frittstående program eller som en Noah-modul.

6.1 TILGANGSKONTROLL

Tilpasningsprogramvaren begrenser ikke tilgangen til funksjonene basert på innloggingskrav og rollene til individuelle brukere. Rollebasert tilgangskontroll er ikke støttet.

Lokal brukertilgang

Når tilpasningsprogramvaren installeres som et frittstående program, er den avhengig av tilgangskontrollmekanismene fra vertsoperativsystemet. Kundens IT-personell kan konfigurere vertsoperativsystemet for å administrere brukergodkjenning og tildele tilgangsrettigheter eller privilegier. Det anbefales på det sterkeste at hver bruker logger på med en unik, individuell konto.

Ytterligere kompenserende kontroller er beskrevet i avsnitt 11 i dette dokumentet og i avsnittet Retningslinjer for IT-sikkerhet i bruksanvisningen.

Når tilpasningsprogramvaren installeres som en Noah-modul, administreres tilgangskontrollen via Noah System 4.

For detaljer om tilgangskontrollfunksjonene som er implementert av Noah System 4, se dokumentasjonen som er tilgjengelig på www.HIMSA.com.

Tjenestetilgang

Serviceingeniører på stedet kan få tilgang til tilpasningsprogramvaren i henhold til tilgangskontrollene som er konfigurert av kundens IT-personell for å administrere godkjenning.

AB-supportteknikere kan få tilgang til tilpasningsprogramvaren ved å bruke skrivebordsdelingsfunksjonen som støttes av tilpasningsprogramvaren. Se avsnitt 6.3 for detaljert informasjon om sikkerhetskontrollene som er aktivert for denne funksjonen.

6.2 REVISJONSLOGGING OG ANSVARLIGHETSKONTROLLER

Tilpasningsprogramvaren genererer ingen ytterligere revisjonslogger eller rapporter utover de som leveres av det underliggende operativsystemet.

Frittstående distribusjonsmodell

Når tilpasningsprogramvaren installeres som et frittstående program, er den avhengig av revisjonsmekanismene som tilbys av vertsoperativsystemet. Tilpasningsprogramvaren har ingen slik integralfunksjon. Vertsoperativsystemet kan konfigureres av kundens IT-personell til å logge bestemte hendelser, for eksempel oppstart og kjøring av tilpasningsprogramvaren. Det anbefales at hver bruker logger seg på verts-OS-et med en unik konto per bruker for å forenkle revisjon.

Noah Distributed-distribusjonsmodell

Når tilpasningsprogramvaren er installert som en Noah-modul, håndteres revisjonslogging av Noah System (Noah Activity Log). For mer informasjon om revisjonskontrollene som er tilgjengelige i Noah System 4, se dokumentasjonen som finnes på www.himsa.com.

6.3 EKSTERN TILGANG

Funksjonen for deling av skrivebord muliggjør fjernanalyse og feilsøking i sanntid av problemer som påvirker installasjoner av tilpasningsprogramvaren. Denne funksjonen er basert på tredjepartsverktøyet TeamViewer QuickSupport (distribuert som standard sammen med tilpasningsprogramvare) og lar ABs kundesupportmedarbeidere eksternt koble seg til audiografens datamaskin og få full kontroll over den på skrivebordet, inkludert tilgang til det underliggende operativsystemet og filsystemet.

For å opprette en skrivebordsdelingsøkt kreves det interaksjon fra audiografen. Audiografen skal først kjøre TeamViewer QuickSupport-verktøyet (f.eks. gjennom tilpasningsprogramvaren Target CI) og kommunisere TeamViewer ID-legitimasjonen sin til AB-supportteamet via en ekstern kommunikasjonskanal (f.eks. telefonsamtale).

Navnet og TeamViewer-ID-en til AB-supportmedlemmet vises som standard på audiografens dataskjerm under hver aktive skrivebordsdelingsøkt.

All nettverkstrafikk for skrivebordsdeling sikres ved hjelp av kryptografiske protokoller og algoritmer som anses som sikre etter dagens standarder (utveksling av offentlige/private RSA-nøkler og AES 256-bits øktkryptering).

Verktøyet for ekstern tilgang kan fjernes manuelt uten at det påvirker andre funksjoner i Target FSW. Target FSW-installasjonsprogrammet støtter en kommandolinjeparameter for å tillate en Target FSW-kommandolinjeinstallasjon uten å inkludere verktøyet for fjerntilgang.

NO

7. INFORMASJONSBESKYTTELSE

7.1 PERSONVERNERKLÆRING FOR ADVANCED BIONICS

Personvernerklæringen som beskriver hvordan Advanced Bionics samler inn, overfører, lagrer og bruker personopplysninger, kan lastes ned fra: AdvancedBionics.com/privacy.

Advanced Bionics verken er vert for, lagrer, sikkerhetskopierer eller har tilgang til data som er lagret i tilpasningsprogramvaren eller Noah-databasene, med mindre dataene uttrykkelig sendes til Advanced Bionics.

7.2 AMERIKANSKE FØDERALE STANDARDER FOR INFORMASJONSBEHANDLING (FIPS)

Target CI v1.6 er kompatibel med FIPS 140-2-krypteringsstandardene.

7.3 PERSONLIG IDENTIFISERENDE INFORMASJON/ HELSEOPPLYSNINGER SOM BEHANDLES AV PRODUKTET

Tilpasningsprogramvaren behandler pasientens personlige og helsemessige informasjon.

Pasientinformasjonen legges enten inn manuelt av brukeren av tilpasningsprogramvaren, eller den mottas av applikasjonen gjennom én eller flere av dataflytene.

Følgende typer informasjon behandles i de viktigste dataflytene i tilpasningsprogramvaren:

	Sonovas skytjenester (kjerne-dispatcher, ekstern støtte)	Høreapparat	Mobilapper	Pasient-DB (lokal/ Noah)	Ekstern tilgang
Navn				X	X(2)
Adresse				X	X(2)
Fødselsdato	X(1)		X	X	X(2)
Telefonnummer				X	X(2)
E-postadresse				X	X(2)
Medisinske journalnumre				X	X(2)
Enhetsidentifikatorer og serienumre	X(1)	X	X	X	X(2)
IP-adresse	X(1)				
Audiogram, RECD, REUG	X(1)	X	X	X	X(2)
Tilpasningsdata		X	X	X	X(2)
Bruksdata for høreapparater	X(1)	X	X	X	
Bruksdata for tilpasnings-programvaren	X(1)				

(1) Pseudonymisert før dataene lagres i Sonovas datalake.

(2) Under en sanntidsøkt med skrivebordsdeling får ABs kundestøtteingeniører full kontroll over helsepersonellets skrivebord, inkludert tilgang til det underliggende operativsystemet og filsystemet samt data som er lagret der. Se avsnitt 6.3 for mer informasjon.

For mer detaljert informasjon om innsamling og behandling av data, kontakt din lokale supportrepresentant.

7.4 SIKKERHET UNDER OVERFØRING

Kommunikasjonssikkerhet er sikret og aktivert i all innkommende og utgående nettverkskommunikasjon for tilpasningsprogramvaren. Med unntak av fjernstøttefunksjonen (som bruker WebRTC-protokollen) og Bluetooth-kommunikasjon med høreapparater og tilbehør, alle andre tilkoblinger er beskyttet av Transport Layer Security (TLS)-protokollen som gir konfidensialitet, integritet og autentisitet.

NO

TLS

TLS-konfigurasjonen er i samsvar med gjeldende beste praksis og sikkerhetsanbefalinger dokumentert i BCP 195 – Anbefalinger for sikker bruk av TLS og DTLS [8], inkludert:

- støtter ikke SSL- og TLS-versjoner før 1.2
- støtter ikke krypteringspakker som bruker kryptografiske algoritmer som tilbyr mindre enn 128 bits sikkerhet
- støtter anbefalte TLS-utvidelser av BCP 195
- støtter ikke usikre utvidelser av BCP 195

DTLS

Kryptering er en obligatorisk funksjon i WebRTC og håndheves på alle mediestrømmer som sendes over WebRTC. Krypteringsprotokollen som brukes avhenger av kanaltypen; datastrømmer krypteres med DTLS 1.2 og mediestrømmer krypteres med Secure Real-time Transport Protocol (SRTP) som brukes fordi det er et lettere alternativ enn DTLS.

Se følgende lenke for mer detaljert informasjon om sikkerhetskonfigurasjon av Remote Support WebRTC:

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

BLE

Trådløs Bluetooth Low Energy-kommunikasjon med høreapparater og tilbehør er kryptert og integritetsbeskyttet som standard (med unntak av bruk i identifikasjons- og deteksjonstilfeller). I tillegg til dette er varigheten av høreapparatets Bluetooth-paringsmodus tidsbegrenset. Se tilgjengelig dokumentasjon for høreapparater for mer detaljert beskrivelse av sikkerheten til Bluetooth-kommunikasjonskanalen.

7.5 SIKKERHET FOR LAGREDE DATA

Applikasjonsdata

Applikasjonsdataene finnes på samme maskin, i standardmappen:
C:\ProgramData\Advanced Bionics\Target CI\Target CI

Tilgangsrettigheten arves fra den overordnede mappen og er begrenset til brukere som er logget på det lokale systemet (den innebygde INTERACTIVE-brukergruppen1[1]) under installasjonen av programvaren.

Autoriserte brukere har lese- og skrivetilgang til mappen.

For å redusere risikoen for uautorisert tilgang til programdataene via nettverket, må du sørge for at ingen av mappene eller filene som inneholder dataene deles på nettverket. Standardplasseringene for applikasjonsdataene er oppført i 5.4.

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

Pasientdatabase – Frittstående utplasseringsmodell

Når tilpasningsprogramvaren er installert som en frittstående applikasjon, ligger pasientdatabasen på samme maskin, og pasientopplysningene er ikke kryptert i hvile. Applikasjonen overfører ikke personlig identifiserende informasjon via nettverket.

Alle brukere som kan logge på maskinen der tilpasningsprogramvaren er installert, vil ha full tilgang til alle applikasjonsdata, inkludert pasientdatabasen. Se avsnittet Personvern for veiledning om anbefalte databeskyttelsestiltak.

I enkelte jurisdiksjoner kan forskrifter kreve kryptering av alle pasientdata for å unngå potensielle ansvarsforhold i tilfelle datatap eller tyveri. Aktiver BitLocker eller tilsvarende fulldiskkryptering (på OS-nivå eller maskinvarebasert) for å beskytte dataene mot uautorisert tilgang eller kopiering mens dataene er lagret.

BitLocker er en innebygd Windows-funksjon som krypterer hele harddisken og krever autentisering for å få tilgang. Se alltid Microsofts offisielle veiledning og organisasjonens IT-sikkerhetspolicy før du aktiverer BitLocker.

Slik aktiverer du BitLocker

Det kreves administratorrettigheter for å administrere BitLocker.

1. Søk etter «Administrer BitLocker»
   Åpne Start-menyen, skriv inn «Administrer BitLocker», og velg den fra søkeresultatene.
2. Velg systemstasjonen
   Velg stasjonen der Windows er installert for å konfigurere krypteringsinnstillinger.
3. Velg en opplåsingsmetode
   Velg ett av følgende alternativer:
   - Kun TPM
   - TPM + PIN-kode
   - TPM + USB-nøkkel

   Følg Microsofts beste praksis og organisasjonens IT-sikkerhetspolicy når du velger opplåsingsmetode.
4. Sikkerhetskopier gjenopprettingsnøkkelen
   Sikkerhetskopier gjenopprettingsnøkkelen ved hjelp av sikre, bedriftsgodkjente metoder. Anbefalte alternativer inkluderer:
   – Lagring i Microsoft Entra ID (tidligere Azure AD) eller Active Directory for domenetilknyttede enheter
   – Lagring på en sikker, tilgangskontrollert nettverksplassering med kryptering og revisjonslogging
   – Bruk av en administrert nøkkeldeponeringsløsning godkjent av organisasjonen din

   Unngå å lagre nøkkelen på lokale stasjoner, USB-er eller skrive den ut med mindre det er uttrykkelig tillatt i retningslinjene. Gjenopprettingsnøkler må beskyttes med samme strenghet som annen sensitiv påloggingsinformasjon og roteres umiddelbart hvis de blir eksponert.

5. Start kryptering

   Velg:

   – Hele harddisken – anbefales for de fleste bedriftsscenarioer. Krypterer alle sektorer, også ubrukt plass, slik at slettede data ikke kan gjenopprettes.

Pasientdatabase – Noah Distributed Deployment-modul

Når tilpasningsprogramvaren installeres som en Noah-modul, lagres personlig identifiserende informasjon i pasientdatabasen som Noah drifter. Pasientdatabasen som Noah drifter, kan ligge på en annen maskin. Personlig identifiserende informasjon og andre pasientopplysninger administreres av Noah-programvaren, og krypteringen av pasientopplysningene i hvile ivaretas av Noah System. Tilpasningsprogramvaren kan sende eller motta personlig identifiserende informasjon over en kablet eller trådløs nettverkstilkobling når en Noah-database er konfigurert for nettverkstilgang.

Personlig identifiserende informasjon som er lagret i en nettverkstilkoblet Noah-database, vil være tilgjengelige for andre brukere på andre PC-er som har tilgang til den samme nettverkstilkoblede databasen. Noah-databasen kan også konfigureres for ikke-nettverkstilgang og installeres på samme PC som tilpasningsprogramvaren.

Noah hindrer tilpasningsprogramvaren i å få tilgang til pasientjournaldatabasen. Når en bruker åpner en pasient i tilpasningsprogramvaren via Noah-klienten, kan tilpasningsprogramvaren bare lese fra og skrive til den gjeldende åpnede pasientjournalen, og den kan ikke få tilgang til andre pasientjournaler i Noah-databasen.

Se følgende lenke for mer informasjon om krypteringsstandardene som brukes av Noah System:

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

RMA-eksportfiler

Tilpasningsprogramvaren tillater eksport av klientinformasjon til en fil. RMA-filen kan sendes til Advanced Bionics for å løse RMA- eller relaterte støtteproblemer.

RMA-filen er asymmetrisk RSA-kryptert med en nøkkellengde på 2048 bit. Tilpasningsprogramvaren har ingen funksjon for å dekryptere en RMA-fil.

Anonymiserte eksportfiler

Tilpasningsprogramvaren tillater eksport av klientinformasjon til en klientanonymisert fil. Klientens personlig identifiserbare informasjon, som fødselsdato og navn, erstattes med generiske verdier. Filen er ikke kryptert og kan importeres til enten samme eller en annen installasjon av tilpasningsprogramvaren.

Standard eksportfiler

Tilpasningsprogramvaren tillater eksport av klientinformasjon til en standard eksportfil. Filen bruker et proprietært binært format og er ikke kryptert. Filen kan importeres til samme eller en annen installasjon av tilpasningsprogramvaren. Når denne funksjonen brukes, må brukere av tilpasningsprogramvaren sørge for at standard eksportfiler håndteres i henhold til deres lokale IT-policyer for håndtering av ukryptert personlig identifiserende informasjon.

Høreapparat

Tilpasningsprogramvaren lagrer klientinformasjon på klientens høreapparat. Personlig identifiserbar informasjon som klientens navn og fødselsdato lagres ikke på høreapparatet. Annen informasjon som ikke er personlig identifiserende informasjon, lagres ved hjelp av PBKDF2-kryptering med en 128-biters nøkkel.

Tilpasningsprogramvaren kan sende/motta klientinformasjon som ikke er personlig identifiserende informasjon, til/fra et høreapparat via en proprietær kablet enhet (dvs. CPI-3), AB Remote Support og AB Remote Support + mobilapplikasjoner eller Noahlink Wireless-enheten. Noahlink Wireless-enheten kobles til høreapparatet ved hjelp av Bluetooth Low Energy (BLE) via en standard BLE-kanal med 128-bit AES-kryptering.

8. PROGRAMVAREINTEGRITET

8.1 VERIFISERING AV NEDLASTET INSTALLASJONSMEDIUM

Installasjonsmediet for Target CI-tilpasningsprogramvaren kan i enkelte regioner lastes ned fra Advanced Bionics' Pro Portal eller Sonova Web Client. Det nedlastede installasjonsmediet kan autentiseres ved hjelp av et hvilket som helst pålitelig SHA-256 hashing-verktøy.

SHA256-hashen for standard zip-fil for installasjon er:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

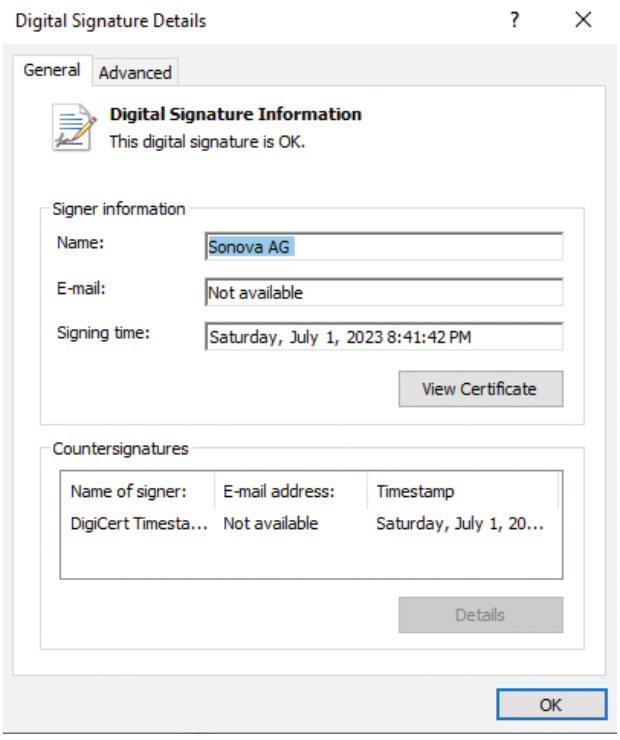
SHA256-hashen for zip-filen for IT Professional-installasjoner er:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

NO

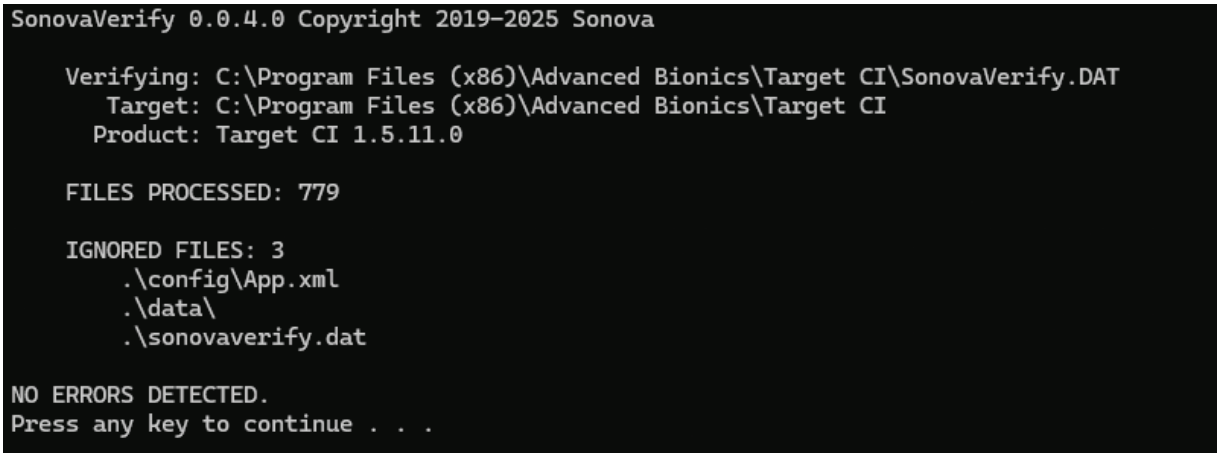
8.2 MANUELL VERIFISERING AV TILPASNINGSPROGRAMVAREN FØR INSTALLASJON

Brukere kan utføre følgende trinn for å bekrefte tilpasningsprogramvarens integritet og autentisitet før installasjon:

1. Åpne Windows Explorer og gå til rotmappen på installasjonsmediet for tilpasningsprogramvaren. Hvis installasjonsmediet er en minnepenn, setter du den inn i en USB-port og går til rotmappen. Hvis installasjonsmediet er en zip-fil, pakk den ut til en mappe og gå til den mappen.
2. Høyreklikk på SonovaVerify.exe, og velg Egenskaper fra hurtigmenyen.
3. Velg fanen Digitale signaturer.
4. Dobbeltklikk på SHA256 «Sonova AG»-signaturen.
5. Bekreft at elementene i signaturen er gyldige. Kontroller spesielt at meldingen «Den digitale signaturen er OK» vises nær toppen, og at underskriverens navn og signeringstidspunkt samsvarer med det følgende bildet:



6. Klikk på knappen «Vis sertifikat» og fanen «Detaljer», og kontroller at verdien i feltet «Fingeravtrykk» samsvarer med denne: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Lukk popup-dialogboksene og dobbeltklikk på SonovaVerify.exe
8. Bekreft at «INGEN FEIL OPPDAGET» vises som vist på bildet nedenfor:



Utdataene «INGEN FEIL OPPDAGET» tilsvarer en vellykket utført integritets- og autentisitetsverifisering av innholdet i installasjonsmediet for tilpasningsprogramvaren. Dette betyr at SonovaVerify.exe har autentisert og bekreftet integriteten til alle filer og mapper. Dette bekrefter at innholdet på installasjonsmediet for tilpasningsprogramvaren ikke har blitt tuklet med, ødelagt eller på annen måte kompromittert.

SonovaVerify.exe vil vise advarsler eller feilmeldinger hvis filer eller mapper mangler, eller uventede filer eller mapper er lagt til installasjonsmediet. Dersom det vises advarsler eller feilmeldinger, betyr det at verifiseringen av integriteten og autentisiteten til innholdet på installasjonsmediet for tilpasningsprogramvaren har mislyktes. Det anbefales derfor å:

- ikke fortsette med installasjonen
- Ikke åpne eller kjøre noen filer som finnes i installasjonsavbildningen for tilpasningsprogramvaren. Rapporter problemet til Advanced Bionics' kundestøtte (se avsnitt 2.1).

8.3 AUTOMATISK VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE

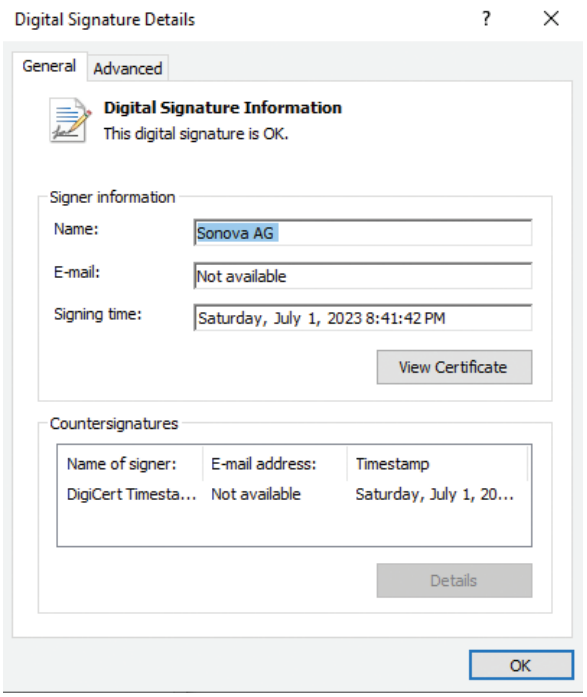
SonovaVerify er integrert med tilpasningsprogramvaren og kjører hver gang programmet startes for å bekrefte integriteten til tilpasningsprogramvarens programfiler. Programfilene signeres digitalt ved hjelp av bransjestandardpraksis og sertifikater utstedt av en pålitelig sertifiseringsinstans. Programvaren varsler brukeren via advarselsmeldinger hvis programfiler er kompromittert.

NO

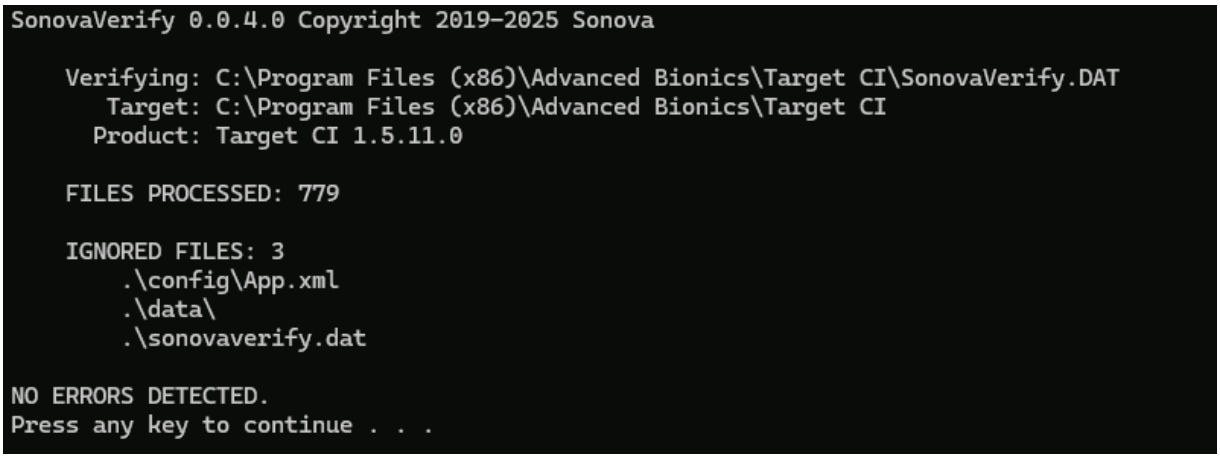
8.4 MANUELL VERIFISERING AV INTEGRITETEN TIL INSTALLERT TILPASNINGSPROGRAMVARE

Brukerne kan når som helst utføre følgende trinn for å bekrefte den installerte tilpasningsprogramvarens integritet og autentisitet uten å måtte starte tilpasningsprogramvaren:

1. Åpne Filutforskeren og gå til den kjørbare mappen for tilpasningsprogramvaren, vanligvis plassert i:C:\Program Filer (x86)\Advanced Bionics\Target CI\
2. Høyreklikk på SonovaVerify.exe, og velg Egenskaper fra hurtigmenyen.
3. Velg fanen Digitale signaturer.
4. Dobbeltklikk på SHA256 «Sonova AG»-signaturen.
5. Bekreft at elementene i signaturen er gyldige, spesielt at meldingen «Den digitale signaturen er OK» vises nær toppen, og at underskriverens navn og signeringstidspunkt samsvarer med følgende bilde:



6. Klikk på knappen «Vis sertifikat» og fanen «Detaljer», og kontroller at verdien i feltet «Fingeravtrykk» samsvarer med denne: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Lukk popup-dialogboksene og dobbeltklikk på SonovaVerify.exe
8. Bekreft at «INGEN FEIL OPPDAGET» vises som vist på bildet nedenfor:



Utdataene «INGEN FEIL OPPDAGET» tilsvarer en vellykket utført integritets- og autentisitetsverifisering av innholdet i installasjonsmediet for tilpasningsprogramvaren. Dette betyr at SonovaVerify.exe har autentisert og bekreftet integriteten til alle filer og mapper. Dette bekrefter at innholdet på installasjonsmediet for tilpasningsprogramvaren ikke har blitt tuklet med, ødelagt eller på annen måte kompromittert.

SonovaVerify.exe vil vise advarsler eller feilmeldinger hvis filer eller mapper mangler, eller uventede filer eller mapper er lagt til installasjonsmediet. Dersom det vises advarsler eller feilmeldinger, betyr det at verifiseringen av integriteten og autentisiteten til innholdet på installasjonsmediet for tilpasningsprogramvaren har mislyktes. Det anbefales derfor å:

- ikke fortsette med installasjonen
- Ikke åpne eller kjøre noen filer som finnes i installasjonsavbildningen for tilpasningsprogramvaren. Rapporter problemet til Advanced Bionics' kundestøtte (se avsnitt 2.1)

NO

9. PROGRAMVAREOPPDATERINGER OG -OPPDATERINGSFILER

Automatiske oppdateringer støttes ikke. Se avsnitt 12 for mer informasjon.

10. DATABEHANDLING

10.1 DATABASER

Tilpasningsprogramvaren bruker en transaksjonsdatabase for lagring av pasientdata, samt et sett med informasjonsdatabaser som leverer metadata-konfigurasjoner som kreves av applikasjonen.

Se avsnitt 3. Nettverks- og kontekstdiagrammer – Utplasseringsartefakter for en detaljert liste over alle databaser som er utplassert av tilpasningsprogramvaren.

Når tilpasningsprogramvaren installeres som et frittstående program, er pasientdatabasen intern i tilpasningsprogramvaren. Pasientdatabasen, lagret i filen PatientDatabase.sqlite, ligger på samme maskin som tilpasningsprogramvaren og fungerer som lagringsplass for pasientdata. For å sikkerhetskopiere programdata når Target CI distribueres som et frittstående program må du opprette en sikkerhetskopi av hele mappen som ligger på %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Beskytt sikkerhetskopier av data ikke bare mot datatap, men også mot tyveri. Når tilpasningsprogramvaren installeres som en Noah-modul, lagres pasientdata i databasen som leveres av Noah-systemet. Noah-databasen kan være konfigurert for nettverkstilgang. Noah-databasen kan også konfigureres for ikke-nettverkstilgang og installeres på samme PC som tilpasningsprogramvaren. Konfigurer Noah-databasekryptering for å beskytte data (se HIMSA-dokumentasjonen).

For Noahs distribuerte distribusjonsmodus, se følgende lenke for instruksjoner om sikkerhetskopiering og gjenoppretting av Noah-pasientdatabasen:

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 DATAMIGRASJON

Tilpasningsprogramvaren lar brukere migrere pasientjournaler fra ABs tidligere tilpasningsprogramvare, SoundWave 3.2. Pasientjournalene må være tilgjengelige fra en SoundWave 3.2-installasjon på samme datamaskin som Target CI for å kunne migreres.

10.3 KONFIGURASJONER AV HØREAPPARATER

Tilpasningsprogramvaren muliggjør eksport og import av enhetskonfigurasjoner og -innstillinger.

10.4 DATADESTRUKSJON

Se avsnitt 5.4, «Fjerning og avvikling», i dette dokumentet og avsnittet «Kassering og farlige materialer» i bruksanvisningen for veiledning om datasletting. For Noah-distribusjoner finnes detaljerte instruksjoner for datasletting av pasientjournaler på: https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

11. SIKKERHETSMILJØ – DELT ANSVAR

Tilpasningsprogramvaren er utviklet for en tiltenkt bruk der risikostyring for cybersikkerhet anses som et delt ansvar mellom interessenter i hele økosystemet for hørselspleie, som inkluderer, men ikke er begrenset til brukere av høreapparater, foreldre eller foresatte til barn som bruker høreapparater, audiografer, IT-administratorer, hørselsinstitusjoner og -leverandører, leverandører av høreapparater og programmeringsutstyr.

Her følger en liste over beste vanlige praksisanbefalinger og sikkerhetskontroller for tilpasningsmiljøet der tilpasningsprogramvaren skal brukes:

OS-nivå

- Bruk tilgangskontroller på OS-nivå, f.eks.:
  - Fjern gjestekontoer
  - Aktiver Windows-brukerpålogging
  - Før en liste over autoriserte operatører for å kontrollere tilgang til systemet
  - Angi tilpassede brukere og roller
  - Bruk krav til sterkt passord, og hold påloggingsinformasjon hemmelig
  - Aktiver tidsavbrudd for inaktiv økt
- Bruk revisjonskontroller på OS-nivå
- Sørg for at operativsystemet er oppdatert
- Sørg for at den installerte versjonen av tilpasningsprogramvaren oppdatert
- Bruk hensiktsmessig og oppdatert beskyttelse mot skadelig programvare og antivirus
- Sørg for å deaktivere AutoRun og AutoPlay-funksjonene
- Aktiver hvitelisting av apper

Personvern

- Sørg for at ingen av mappene eller filene som inneholder programdata deles på nettverket. Standardplasseringene for applikasjonsdataene er oppført i tabellen i avsnitt 5.4. For å kontrollere hvilke nettverksressurser som er delt fra en datamaskin, går du til «Datamaskinbehandling → Delte mapper → Delinger» i Microsofts verktøy Datamaskinbehandling, eller kjører PowerShell-kommandoen Get-WmiObject -class Win32_Share.
- Under installasjonen angis tillatelsene for programdatamappen i henhold til avsnitt 6.1. Programdatamapper arver tilgangstillatelser fra den overordnede mappen. Det er programvareoperatørens ansvar å administrere tilgangsrettighetene til den overordnede mappen.
- Krypter pasientdata ved hjelp av tredjepartsverktøy eller -kontroller på OS-nivå ved å bruke diskkryptering (f.eks. gratisversjonen av Microsoft BitLocker) for å beskytte alle data. For Noah-utplasseringer, bør du vurdere å bruke Noah databasekryptering.
- Eksterne medier som inneholder data eksportert fra tilpasningsprogramvare, inkludert rapporter og logger, bør sikres. Når dataene ikke lenger brukes, bør de slettes på en sikker måte og/eller mediet bør slettes på en sikker måte.

- Bruk USB-lagringsmedier med innebygd sikkerhetsfunksjonalitet, som krypterte USB-stasjoner med integrert tastatur.
- Sørg alltid for datasikkerheten ved å følge disse fremgangsmåtene:
  - Ved overføring av data via usikrede kanaler skal dataene enten anonymiseres eller krypteres.
  - Beskytt sikkerhetskopier av data ikke bare mot datatap, men også mot tyveri.
  - Fjern alle data fra datamediet som ikke lenger er i bruk eller som skal kastes.
- Godkjente prosedyrer og verktøy skal benyttes av brukere for sikker sletting av data lagret på flyttbart lagringsmedium i henhold til gjeldende regelverk og retningslinjer for håndtering av pasientinformasjon / personlig identifiserbar informasjon (PII) / beskyttet helseinformasjon (PHI)

IT-infrastruktur

Bruk tilpasningsprogramvaren i et sikkert nettverksmiljø beskyttet mot uautorisert inntrenging. Det finnes mange effektive teknikker for å isolere og beskytte medisinske informasjonssystemer, blant annet implementering av brannmur, demilitariserte soner (DMZ), virtuelle lokalnettverk (VLAN) og nettverksenklaver. Opprettholde en aktiv nettverkstilkobling for å motta oppdateringer til operativsystemet.

Fysisk nivå

- Arbeidsstasjonen der tilpasningsprogramvaren er installert, skal sikres fysisk på en slik måte at den ikke er tilgjengelig for eller kan manipuleres av uautorisert personell.
- Tilgang til skrivere som er koblet til arbeidsstasjonen skal kontrolleres.
- Skjermen på arbeidsstasjonen der tilpasningsprogramvaren er installert, skal plasseres på en slik måte at innholdet på skjermen bare er synlig for brukeren.

Organisasjonsnivå

- Kun yrkesopplært, fullt kvalifisert personell har tillatelse til å bruke systemet. Før en person får tillatelse til å bruke systemet, må det bekreftes at personen har lest og fullt ut forstår bruksanvisningen som følger med tilpasningsprogramvaren.
- Det skal bare opprettes brukerkontoer for personell som er autorisert til å vedlikeholde og bruke tilpasningsprogramvaren, på maskinen der programvaren er installert. Datamaskin- og domenekontoer samt de tilknyttede tilgangsrettighetene bør gjennomgås regelmessig og deaktiveres dersom tilgangen til maskinen ikke lenger er nødvendig.
- Hvis du oppdager mistenkelig aktivitet på kontoene dine for tilpasningsprogramvaren eller uventede operasjoner, kontakt Advanced Bionics. Se avsnitt 2.1 for mer informasjon.

For mer informasjon om delt ansvar og en mer detaljert liste over anbefalinger for beste praksis og sikkerhetskontroller som skal anvendes på ulike nivåer i tilpasningsmiljøet der tilpasningsprogramvaren skal brukes, se:

- EHIMA-hviteboken «Beste praksis for sikker tilpasning av høreapparater», EHIMAWhitePaper

12. PRODUKSJON, PROGRAMVAREUTVIKLING OG SIKKERHETSSTYRING

Cybersikkerhet vurderes gjennom hele programvareutviklingsprosessen. Tilpasningsprogramvaren er utviklet i samsvar med standardene IEC 62304 og IEC 82304.

Tilpasningsprogramvaren skannes for virus og skadelig programvare som en del av produksjonsprosessen.

Sårbarheter i tredjepartskomponenter som er oppført i NISTs nasjonale sårbarhetsdatabase (NVD), vurderes og reduseres under utviklingsprosessen, og overvåkes når tilpasningsprogramvaren er lansert på markedet.

Konfigurasjonsstyring

AB utvikler, dokumenterer og vedlikeholder internt grunnkonfigurasjonen for hver utgitte versjon av tilpasningsprogramvaren under konfigurasjonsstyring.

Alle tredjepartsprogramvarekomponenter som brukes av tilpasningsprogramvaren, er identifisert og dokumentert i programvarekomponentlisten (SBOM). AB bruker SBOM i styringen av cybersikkerhetsrisiko for å vurdere og overvåke eksponeringen for cybersikkerhetstrusler og offentliggjorte sårbarheter ved hjelp av oppdaterte verktøy for sårbarhetsskanning.

Sikkerhetsoppdateringer

AB overvåker kontinuerlig sikkerhetssårbarheter som påvirker tilpasningsprogramvaren. Dette inkluderer sårbarheter i tilpasningsprogramvaren og i tredjepartskomponenter som brukes av tilpasningsprogramvaren.

Offentliggjorte sårbarheter vurderes basert på konfigurasjonen og bruken av tilpasningsprogramvaren.

Ved behov kan sikkerhetssårbarheter utbedres gjennom en bredere utgivelse av tilpasningsprogramvaren som inneholder sikkerhetsoppdateringer for spesifikke programvarekomponenter i programvarepakken.

Sårbarhetsvarsling

Vi er forpliktet til å varsle om sårbarheter og til å forbedre sikkerheten til våre produkter og tjenester.

Det oppfordres til å rapportere mistenkte sårbarheter eller sikkerhetsproblemer knyttet til våre produkter eller den underliggende programvaren/infrastrukturen.

Les retningslinjene våre for varsling om sårbarheter, som er publisert på https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy og følg instruksjonene for å sende inn en rapport.

NO

13. PROGRAMVAREKOMPONENTER OG STYKKLISTE

Tilpasningsprogramvaren inneholder visse kommersielle, standard programvarekomponenter.

Tabellen nedenfor viser all SOUP (programvare av ukjent opprinnelse) som distribueres med tilpasningsprogramvaren.

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
AForge.NET	AForge.NET matematikk- og mediebibliotek, en del av og nødvendig for IceLink og LiveSwitch.	AForge.NET	2.2.5.0
Amplifon. Programmer	Komponent av Amplifons programvarepakke	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Komponent av Amplifons programvarepakke	Amplifon	1.0.4.0
AutoMapper	Automatiserer objekt-til-objekt-kartlegging	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	bibliotek for ytelsesmåling som tilbyr verktøy for å måle og sammenligne ytelsen til kode.	BenchmarkDotNet Nettverk for CI-brukere	0.13.0.0
Castle.Core	Et kjernebibliotek i Castle Project som tilbyr komponenter som dynamisk generering av proxyer og beholdere for kontrollinversjon for .NET-applikasjoner.	Castle Project	4.4.1
Chessie	Et funksjonelt feilhåndteringsbibliotek for F#	Åpen kildekode	0.6.0.0
ciAD hørselstapsimulator	Bibliotek for simulatorer for hørselstap for mediespiller	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Forenkler lesing, redigering og skriving av Excel-filer uten at Excel må være installert.	ClosedXML Nettverk for CI-brukere	0.95.4.0
CommandLine Parser	Tilbyr et rent og konsist API for tolking av kommandolinjeargumenter.	CommandLineParser Nettverk for CI-brukere	2.4.3
Common.Logging	En bærbar loggingabstraksjon for .NET-applikasjoner	Common.Logging Nettverk for CI-brukere	3.4.1.0
CommonService Locator	Tilbyr et felles grensesnitt for tjenestelokalisering, slik at applikasjoner kan frikobles fra spesifikke IoC-beholdere.	Microsoft	2.0.5.0
Credential Management	Pakken for legitimasjonshåndtering er et omslag (wrapper) for Windows Credential Management API.	iLya Lozovyy	1.0.2

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
CSharpAnalytics	Brukes til Google Analytics.	Angrepsmønster	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78.45418
Destructurama. Attributed	Brukes av Nephele-biblioteker.	Serilog Contributors	3.1.0.0
Developer Express Suite	En omfattende pakke med UI-kontroller og biblioteker for .NET-utviklere, som tilbyr verktøy for å bygge funksjonsrike applikasjoner.	Developer Express Inc	20.2.10.0
DirectShow 2005	Gir tilgang til Microsofts DirectShow-funksjonalitet fra .NET-applikasjoner.	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
ExcelTallFormat	Tilbyr funksjonalitet for å analysere og formatere tallformater i Excel	Åpen kildekode	1.1.0.0
FM.dll	Integrert i deres rammeverk for sanntidskommunikasjon som LiveSwitch og IceLink	FM (Frozen Mountain)	2.9.32
FSharp.Core	Kjernebiblioteket for programmeringsspråket F#	Microsoft	6.0.322.10402
FTDI Chip	En driverpakke fra Future Technology Devices International (FTDI) som forenkler kommunikasjonen mellom USB-enheter og programvare.	FTDI	3.02.07
GNOtometrics. Aurical	GNOtometrics.Aurical ompakket for Sonova	Natus Medical Incorporated	2.0.1.9
SharedUtilities.dll	tilbyr felles verktøyfunksjoner og delte ressurser på tvers av Natus-applikasjoner.	Natus Medical Incorporated	1.0.0.0
Hardware.Info	En komponent som samler inn og gir detaljert informasjon om maskinvarekonfigurasjonen til et system	Åpen kildekode	11.1.0.1
Himsa.NLWSMAPI. dll	Et bibliotek tilknyttet HIMSAs Noah-programvare	HIMSA	2.0.3.0
natus.otometrics. hipro2	HiPro-kommunikasjonsbiblioteker	Natus Medical Incorporated	2.0.0.4

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Iced.dll	forenkler sanntidskommunikasjon ved å muliggjøre streaming av lyd, video og data	FM (Frozen Mountain)	1.12.0.0
IceLink	Brukes til WebRTC audio/video konferanseintegrasjon	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	tilbyr Unicode- og globaliseringsstøtte for programvareapplikasjoner	FM (Frozen Mountain)	54.1.0.0
IdentityModel	Klientbibliotek for OpenID Connect og OAuth 2.0 som brukes av komponenten Kona.CommonServices. Authentication til OAuth 2-autentisering.	Dominick Baier,Brock Allen	6.2.0.0
IMCInterfaces	Noah grensesnittbibliotek for kommunikasjon mellom moduler	HIMSA II K/S	4.4.0.2266
iText 7	PDF-bibliotek for å opprette, endre og undersøke PDF-dokumenter programmatisk.	iText-programvare	7.1.16.0
JetBrains. dotMemory	Et minneprofileringsverktøy for å oppdage minnelekkasjer og optimalisere minnebruken i .NET-applikasjoner	JetBrains	111.0.0.0
JsonDiffPatch DotNet.dll	Tilbyr funksjoner for å sammenligne og oppdatere JSON-objekter	Åpen kildekode	1.0.1.0
LibGit2Sharp	Brukes av biblioteker som kommer fra Sonova for å kommunisere med Git	LibGit2Sharp-bidragsytere	0.26.1.93
LiveSwitch	Brukes til WebRTC audio/video konferanseintegrasjon.	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	loggføringsrammeverk for .NET	Apache	4.7.0.3189
Mapster	Brukes til kartlegging av objekter i kode	chaowlert,eric_swann	7.2.0.0
Mapster.Core	Brukes til kartlegging av objekter i kode	chaowlert,eric_swann	1.2.0.0
MathNet.Numerics	Brukes for tilpasning av algoritmer (signalbane, målmatching, osv.)	Christoph Ruegg, Marcus Cuda, Jürgen Van Gael og bidragsytere	4.11.0
Microsoft.Bcl. AsyncInterfaces	Tilbyr IAsyncEnumerable<T>- og IAsyncDisposable-grensesnittene samt hjelpeklasser for .NET Standard 2.0.	Microsoft	6.0.21.52210

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Microsoft.CodeAnalysis.Common	Brukes av bibliotekene som kommer fra Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	3.900.21.12420
Microsoft.CodeAnalysis.CSharp	Brukes av bibliotekene som kommer fra Sonova.HardwareAbstraction.Palio.Trafo	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Tilbyr kompilering og kodegenerering ved hjelp av C#	Microsoft	4.700.19.56404
Microsoft.Diagnostics.FastSerialization.dl	Brukes for effektiv serialisering og deserialisering av diagnostiske data	Microsoft	1.0.0.0
Microsoft.Diagnostics.NETCore.Client.dll	Et administrert bibliotek som gjør det mulig å samhandle med .NET Core-kjøremiljøet for ulike diagnostikkoppgaver, for eksempel sporing og innhenting av dumpfiler.	Microsoft	0.2.4.27602
Microsoft.Diagnostics.Runtime.dll	tilbyr API-er for inspeksjon av prosesser som kjører, og krasjdumper, slik at utviklere kan lage feilsøkings- og diagnoseverktøy.	Microsoft	2.0.4.26801
Microsoft.Diagnostics.Tracing.TraceEvent.dll	Et bibliotek for analyse og behandling av Event Tracing for Windows (ETW)-hendelser.	Microsoft	2.0.70
Microsoft.DotNet.PlatformAbstractions.dll	Tilbyr API-er for tilgang til informasjon om .NET-plattformen	Microsoft	3.100.620.31604
Microsoft.Utvidelser.Avhengighets-injisering.Abstraksjoner	Definerer abstraksjonene for avhengighetsinjisering i .NET-applikasjoner	Microsoft	6.0.21.52210
Microsoft.Extensions.Logging	Forenkler strukturert logging i .NET-applikasjoner.	Microsoft	6.0.21.52210
Microsoft.Extensions.Options	Støtter konfigurasjon av alternativer i .NET-applikasjoner	Microsoft	6.0.21.52210
Microsoft.Extensions.Primitives	Tilbyr grensesnitt og klasser for endringssporing og kanselleringssymboler, som bidrar til å administrere data som kan endres, og til å frigjøre ressurser.	Microsoft	6.0.21.52210

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Microsoft.Identity.Client	MSAL-biblioteket for .NET er en del av Microsofts identitetsplattform for utviklere (tidligere kalt Azure AD) v2.0. Det gjør det mulig å skaffe sikkerhetstokener for å kalle beskyttede API-er. Biblioteket benytter industristandardene OAuth2 og OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Sikker tverrplattform-tokenbuffer for MSAL offentlige klientapplikasjoner.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Inkluderer typer som gir støtte for å opprette, serialisere og validere JSON-webtokens. Brukes av komponenter som kommuniserer med backend-tjenester som bruker JSON Web Tokens for autentisering.	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Logging	Dependecy 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	En inferensmotor for kjøring av maskinlæringsmodeller i ONNX-format (Open Neural Network Exchange).	Microsoft	1.12.1
Microsoft.ML.OnnxRuntime.Managed	Den administrerte .NET-innpakningen for ONNX Runtime	Microsoft	1.12.1
Microsoft.Office.Interop.Excel.dll	Denne DLL-filen er en del av Office Interop-samlingene og gjør det mulig for .NET-applikasjoner å samhandle med Microsoft Excel.	Microsoft	14.0.4733.1000
Microsoft.VisualStudio.TextTemplating.10.0	Tilbyr funksjonalitet for tekstmaler i Visual Studio, slik at utviklere kan generere kode og andre tekstbaserte artefakter ved hjelp av T4-maler.	Microsoft	10.0.40219.1
Microsoft.Win32.Registry.dll	Gir tilgang til Windows-registeret	Microsoft	5.0.20.51904
Microsoft.Win32.SystemEvents.dll	Støtter håndtering av systemhendelser i .NET-applikasjoner	Microsoft	8.0.23.53103

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Microsoft.Win32.TaskScheduler.dll	Brukes for FSW-sikkerhetskopieringsverktøyet (automatiske sikkerhetskopier).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors er en enkel metode for å legge til vanlig og gjenbrukbar interaktivitet i WPF-applikasjonene dine med minimal kode.	xamlexperiencesteam, Microsoft	1.0.1.0
Microsoft DIA SDK	Tilbyr API-er for arbeid med feilsøkingsinformasjon i PDB-filer	Microsoft	2.0.0.0
MS VC++ 2008 Redistributable	Microsoft Visual C++ 2008 Redistributable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Visual C++ 2010 Redistributable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistributable	Microsoft Visual C++ 2012 Redistributable	Microsoft	11.0.51106.1
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
Mono.Cecil	Brukes til å inspisere, modifisere og opprette .NET-samlinger	Microsoft	0.11.3.0
Moq.dll	Åpen kildekode .NET-bibliotek for å lage simulerte objekter under enhetstesting	Moq Nettverk for CI-brukere (Åpen kildekode)	4.16.1.0
MS-VisualC++ 7.1 kjøretidsbiblioteker	Microsoft Visual C++ kjøretidsbiblioteker	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	Brukes til å justere volum og spille av lydfiler.	Åpen kildekode	1.9.0.0
.NET Framework	.NET runtime framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Brukes til JSON-serialisering og deserialisering.	James Newton-King	13.0.3.27908
Newtonsoft.Json.Schema.dll	Et skjemavalideringsbibliotek for JSON-data	James Newton-King	3.0.14.25421
Nibelung	NoahLink Wireless tilpasningsbiblioteker	HIMSA	1.3.16.1
Nibelung2.CPD	NoahLink Wireless tilpasningsbiblioteker	HIMSA	2.0.3.0

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Nlogg	Dette er en avhengighet av HIMSA Nibelung.CPD (Noahlink Wirlesss)	Kim Christensen	5.0.4.1331
Noahlink	Noahlink-driver for tilpasningsenhet	HIMSA	1.55.6.166
Noahlink Wireless Driver	Noahlink trådløs driver for tilpasningsenhet	HIMSA	1.1.0.0
Noahlink Wire-less-oppgraderings-verktøy	Noahlink trådløs fastvareoppgraderingsverktøy	HIMSA	3.1.0.82
ModuleAPI.dll (Noah-system)	En komponent i HIMSA Noah System som tilbyr API-er for integrering og administrasjon av audiologiske data.	HIMSA	4.13.0.5404
NiXPS SDK	Tilbyr funksjoner for håndtering av XPS-dokumenter (XML Paper Specification)	NiXPS NV	2.6.0.0
NPOI	Et bibliotek med åpen kildekode som forenkler lesing og skriving av Microsoft Office-dokumenter i .NET-applikasjoner.	NPOI-kommunikasjon	2.4.1.0
NuGet Package Manager	Et verktøy for å administrere .NET-biblioteker og -pakker	Microsoft	6.3.0.131
Nunit	Et enhetstestingsramme-verk for .NET-applikasjoner	NUnit Project	3.12.0.0
ONNX Runtime	Motor for ONNX-modeller (Open Neural Network Exchange)	Microsoft	1.12.20220803.2.7048164
Open XML SDK	Inneholder verktøy for arbeid med Office Open XML-dokumenter	Microsoft	2.7.2
OSExtensions.dll	bibliotek som tilbyr utvidelser for operativsystemfunksjoner	Microsoft	1.0.0.0
Otometrics. REMaccess	Otometrics' abstraksjonslag over Noah Inter-Module Communication Interface Library	GN Otometrics	1.0.0.10

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Paket.Core.dll	En avhengighetsbehandler med åpen kildekode for .NET- og Mono-prosjekter.	Paket Nettverk for CI-brukere (Åpen kildekode)	7.1.5.0
Patagames.Pdf	PDF-biblioteket for C# for å opprette og redigere PDF-dokumenter i .NET-applikasjoner.	patagames.com	8.57.30.48
Patagames.Pdf.Wpf	PDF-biblioteket for C# for å opprette og redigere PDF-dokumenter i .NET-applikasjoner.	Patagames.com	4.19.18.48
Polly	Bibliotek som lar utviklere uttrykke motstandskraft og håndtering av midlertidige feil med strategier som Retry, Circuit Breaker, Bulkhead Isolation og Fallback på en flytende og trådsikker måte.	App vNext	7.2.3.0
Portable.BouncyCastle	Dette er en avhengighet av HIMSA Nibelung.CPD (Noahlink Wirlesss)	The Legion of the Bouncy Castle Inc	1.8.15362.1
Portable.BouncyCastle.Crypto	Dette er en avhengighet av HIMSA Nibelung.CPD (Noahlink Wirlesss)	The Legion of the Bouncy Castle Inc	1.9.0.1
protobuf-net.dll	Serialiseringsrammeverk brukt for RC-blob.	Åpen kildekode	2.3.2.0
Google.Protobuf	Googles offisielle Protocol Buffers-bibliotek for .NET, som forenkler serialisering og deserialisering av strukturerte data.	Google Inc	3.19.3.0
Perfolizer.dll	Et åpen kildekode-bibliotek for ytelsesanalyse	Åpen kildekode	0.2.1.0
Rhino.Mocks.dll	Et rammeverk for dynamiske mock-objekter for .NET.	Rhino Mocks Nettverk for CI-brukere	3.6.0.0
Security.Cryptography.NetCore.dll	tilbyr kryptografiske funksjoner for .NET Core-applikasjoner	HardDev	1.0.1.0

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Serilog	Loggkomponenten som brukes for hele Chinook-applikasjonen.	Serilog Contributors	3.0.1.0
Serilog.Enrichers.Thread	Berik Serilog-hendelser med egenskaper fra gjeldende tråd.	Serilog Contributors	3.1.0.0
Serilog.Extensions.Logging	Integrerer Serilog med Microsofts loggingabstraksjoner	Serilog Contributors	3.1.0.0
Serilog.Expressions	Uttrykksbasert hendelses-filtrering for Serilog.	Serilog Contributors	2.0.0.0
Serilog.Sinks.Console	En Serilog-sink som skriver logghendelser til konsollen/terminalen.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	En Serilog-sink som skriver logghendelser til debug-utdata-vinduet.	Serilog Contributors	2.0.0.0
Serilog.Sinks.File	Skriv Serilog-hendelser til tekstfiler i vanlig format eller JSON-format.	Serilog Contributors	4.1.0.0
Serilog.Sinks.NUnit.dll	Integreres med NUnit og dirigerer logghendelser til NUnits testutdata, noe som bidrar til testdiagnostikk.	Serilog Contributors	1.0.3.0
Serilog.Sinks.Trace	Den diagnostiske trace-sink-en for Serilog.	Serilog Contributors	2.1.0.0
Serilog.Settings.AppSettings	Støtte for XML-konfigurasjon (System.Configuration <appSettings>) for Serilog.	Serilog Contributors	2.2.2.0
Security.Cryptography.NetCore.dll	Utvidelser til sikkerhets-API-ene som følger med .NET-rammeverket	Microsoft	1.0.1.0
SharpBITS API	SharpBITS.NET er en .NET-innpakning for BITS-API-et og en liten Windows GUI-applikasjon for enklere tilgang til BITS-opplastinger og nedlastinger.	perpetualKid	2.1.0.0

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
SharpZipLib	#ziplib (SharpZipLib, tidligere NzipLib) er et Zip-, Gzip-, Tar- og Bzip2-bibliotek skrevet utelukkende i C# for .NET-plattformen. Dette biblioteket tilbyr komprimeringsf-unksjonalitet (zip, unzip, stream-komprimering osv.). Vi bruker den i Firmware Update-appen.	Åpen kildekode	1.3.3.11
SharpDX	Brukt av LiveSwitch: SharpDX.Direct3D11, SharpDX.Direct2D1, SharpDX.Mathematics	Alexandre Mutel	4.0.1
SocketIOClient	Tilbyr en klient for Socket.IO som muliggjør sanntids, toveis hendelsesbasert kommunikasjon i .NET-applikasjoner.	HeroWong	2.2.4.0
Superpower	Et bibliotek for parser-kombinatorer for C#	Datalust,Superpower Contributors,Sprache Contributors	2.3.0.0
SQLite.Interop	SQLite 3.36.0 Native Interop Library. SQLite er den innebygde databasen som brukes til å lagre informasjon om pasienter (i frittstående modus), produktkatalogen vår og tilhørende ressurser samt metadata for tilpasning, tilbehør og høreapparater. SQLite er offentlig eiendom.	SQLite Development Team	1.0.115
System.Buffers	Tilbyr ressurspooling av alle typer for ytelseskritiske applikasjoner som ofte allokerer og avallokerer objekter.	microsoft, dotnetframework	4.6.28619.01

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
System. Collections. Immutable	Brukes av bibliotekene som kommer fra Sonova. HardwareAbstraction. Palio.Trafo	Microsoft	7.0.22.51805
System. Komponent Modell. Annoteringer	Inneholder attributter som brukes til å definere metadata for objekter som brukes som datakilder.	microsoft, dotnetframework	4.6.26515.06
System. Konfigurasjon. Konfigurasjons-behandler	Tilbyr typer som støtter bruk av konfigurasjonsfiler.	Microsoft	5.0.20.51904
System. CodeDom.dll	Tilbyr klasser for generering og kompilering av kildekode til kjørbare filer eller samlinger	Microsoft	8.0.23.53103
System.Data. SQLite	Brukes av bibliotekene som kommer fra Sonova. HardwareAbstraction. Palio.Trafo	SQLite Development Team	1.0.115.0
System. Diagnostikk. DiagnosticSource	Et loggbibliotek som lar utviklere spore og overvåke diagnostiske data	Microsoft	6.0.21.52210
System Diagnostikk Ytelsesteller	Tilbyr API-er for å samhandle med Windows-ytelsestellere	Microsoft	7.0.22.51805
System.Drawing. Common	Gir tilgang til GDI+-grafikkfunksjonalitet.	Microsoft	8.0.324.11603
System.Formats. Asn1.dll	Støtter koding og dekoding av Abstract Syntax Notation One (ASN.1)-data	Microsoft	6.0.21.52210

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
System.IdentityModel.Tokens.Jwt	Inkluderer typer som gir støtte for å opprette, serialisere og validere JSON-webtokens. Brukes av komponenter som kommuniserer med backend-tjenester som bruker JSON Web Tokens for autentisering.	Microsoft	6.8.0.11012
System.IO.Abstractions	Et sett med abstraksjoner som bidrar til å gjøre filsysteminteraksjoner testbare.	Tatham Oddie & friends	12.0.10.46693
System.IO.Hashing.dll	Tilbyr funksjonalitet for hashing i .NET, inkludert algoritmer for beregning av kontrollsummer og kryptografiske hasher.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Muliggjør lesing og skriving av pakkefiler	Microsoft	6.0.21.52210
System.IO.Ports.dll	Tilbyr klasser for kommunikasjon via serielle porter, slik at .NET-applikasjoner kan kommunisere med maskinvare som er koblet til via serielle porter.	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	En spesialisert HTTP-behandler for Windows.	Microsoft	6.0.422.16404
System.Numerics.Vectors	Tilbyr maskinvareakselererte numeriske typer, egnet for høyytelsesbehandling og grafikkapplikasjoner.	microsoft, dotnetframework	4.6.26515.06

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
System.Memory	Tilbyr typer for effektiv representasjon og pooling av administrerte, stakk- og native minnesegmenter og sekvenser av slike segmenter, sammen med primitive funksjoner for å analysere og formatere UTF-8-kodet tekst lagret i disse minnesegmentene.	microsoft, dotnetframework	4.6.31308.01
System.Reactive.dll		Åpen kildekode	5.0.0.1
System.Reflection.DispatchProxy	Tilbyr en klasse for dynamisk å opprette proxy-typer som implementerer et spesifisert grensesnitt og arver fra en spesifisert DispatchProxy-type. Metodekallinger på den genererte proxy-instansen sendes til den DispatchProxy-basistypen.	Microsoft	4.700.20.21406
System.Reflection.Metadata	Disse pakkene gir en lavnivå .NET (ECMA-335) metadata-leser og -skriver. Det er laget for ytelse og er det ideelle valget for å bygge høyere nivå-biblioteker som har til hensikt å tilby sin egen objektmodell, slik som kompilatorer.	Microsoft	5.0.20.51904
System.Reflection.TypeExtensions	Tilbyr utvidelsesmetoder for refleksjons-API-et	Microsoft	4.700.19.56404

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
System.Runtime.Compiler Services.Unsafe	Tilbyr System.Runtime.CompilerServices.Unsafe-klassen, som gir generisk, lavnivå funksjonalitet for å manipulere pekere.	microsoft, dotnetframework	6.0.21.52210
System.Security.AccessControl	Tilbyr basisklasser som muliggjør administrasjon av tilgangs- og revisjonskontrolllister på sikre objekter.	Microsoft	6.0.21.52210
System.Security.Permissions	Tilbyr typer som støtter Code Access Security (CAS).	Microsoft	5.0.20.51904
System.Security.Principal.Windows	Tilbyr klasser for å hente den nåværende Windows-brukeren og for å samhandle med Windows-brukere og -grupper.	Microsoft	5.0.20.51904
System.Security.Cryptography.Cng.dll	Tilbyr kryptografisk funksjonalitet ved hjelp av Cryptography Next Generation (CNG) API-er	Microsoft	5.0.20.51904
System.Security.Cryptography.Pkcs.dll	Tilbyr klasser for håndtering av Public Key Cryptography Standards (PKCS), inkludert signerte og innkapslede data.	Microsoft	6.0.1923.31806
System.Security.Cryptography.ProtectedData.dll	Tilbyr metoder for å beskytte og oppheve beskyttelsen av data ved hjelp av Windows Data Protection API (DPAPI) for sikker lagring av data.	Microsoft	6.0.21.52210
System.Security.Cryptography.Xml.dll	Muliggjør XML-kryptering og digitale signaturer, og støtter sikker håndtering av XML-data i .NET-applikasjoner.	Microsoft	6.0.822.36306

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
System.ServiceModel.Http.dll	Tilbyr funksjonalitet for HTTP-basert kommunikasjon for Windows Communication Foundation (WCF)-tjenester.	Microsoft	4.700.19.56502
System.ServiceModel.Primitives.dll	Inneholder grunnleggende klasser for WCF-tjenester, inkludert basisklasser og grensesnitt for tjenestekontrakter og kanaler.	Microsoft	4.700.19.56502
System.Text.Encoding.CodePages	Tilbyr støtte for kodesidebaserte kodinger, inkludert Windows-1252, Shift-JIS og GB2312.	Microsoft	5.0.20.51904
System.Text.Encodings.Web	Tilbyr typer for koding og escaping av strenger til bruk i JavaScript, HyperText Markup Language (HTML) og uniform resource locators (URL). Er en avhengighet av SOUP IdentityModel	microsoft, dotnetframework	6.0.21.52210
System.Text.Json	Tilbyr høyytelses- og lavallokerings-typer som serialiserer objekter til JavaScript Object Notation (JSON) tekst og deserialiserer JSON-tekst til objekter, med innebygd støtte for UTF-8. Tilbyr også typer for å lese og skrive JSON-tekst kodet som UTF-8, og for å lage en minnebasert dokumentobjektmodell (DOM), som er skrivebeskyttet, for tilfeldig tilgang til JSON-elementene innenfor en strukturert visning av dataene.	Microsoft	6.0.222.6406

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
System.Threading.Tasks.Extensions	Tilbyr tilleggstyper som forenkler arbeidet med å skrive samtidig og asynkron kode.	microsoft, dotnetframework	4.6.28619.01
System.Threading.Channels	Tilbyr et sett med datastrukturer for synkronisering som brukes til å overføre data mellom produsenter og forbrukere, og som støtter parallellprogrammering med høy ytelse.	Microsoft	6.0.21.52210
System.ValueTuple	Tilbyr System.ValueTuple-strukturene, som implementerer de underliggende typene for tupler i C# og Visual Basic. Legger til støtte for value tuples siden de kun er inkludert i nyere versjoner av .NET Framework.	microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy.dll	Et atferdsdrevet utviklingsrammeverk (BDD) for .NET	TestStack Nettverk for CI-brukere	4.3.2.0
Thrift	Brukt for definisjon av remotelink-protokollen	Apache	0.13.0.0
Unity.Container	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjons-beholder.	Unity Container Project	5.8.13.0
Unity.Configuration	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjons-beholder.	Unity Container Project	5.2.5.0
Unity.Abstractions	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjons-beholder.	Unity Container Project	3.3.1.0

NO

SOUP-ELEMENT	FUNKSJONALITETS-BESKRIVELSE	PRODUSENT	VERSJON
Unity. Interception. Configuration	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjons-beholder.	Unity Container Project	5.1.7.0
Unity. Interception	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjons-beholder.	Unity Container Project	5.5.5.0
Unity. Registration ByConvention	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjons-beholder.	Unity Container Project	2.1.9.0
Unity. ServiceLocation	Unity Container (Unity) er en fullverdig, utvidbar avhengighetsinjeksjons-beholder.	Unity Container Project	2.1.2.0
WAP BT Dongle-driver	WAP BT Dongle-driver (tilpassingsdongle)	iAnywhere Solutions	3.0.0.6095
WebSync	Brukes for integrering av tilpasningsdatakanal	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor. dll	En heksadesimal editor-kontroll for WPF-applikasjoner	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	Et hjelpebibliotek for WPF-applikasjoner som gir informasjon om skjermer og monitorer.	FM (Frozen Mountain)	2.1.0.0
Xceed Extended WPF Toolkit	En samling WPF-kontroller og hjelpefunksjoner som utvider WPF-applikasjoner med flere brukergrense-snittkomponenter.	Xceed	3.5.0.0
xmlunit-core.dll	Et bibliotek for testing og sammenligning av XML-utdata.	XMLUnit Nettverk for CI-brukere	2.9.0.205
Xps til PDF-gjengivelse (NiXPS)	Konverterer xps-filer til PDF programmatisk og brukes i rapporter fra tilpasningsprogrammet.	NiXPS	2.6.7.0

14. REFERANSER

Tittel	Nettsted
Bruksanvisning (elektronisk)	https://ifu.advancedbionics.com/
Advanced Bionics global personvernerklæring	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Sikkerhetskopiering og gjenoppretting av data i Noah-databasen din	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Noah-systemets databasekapasitet er nådd.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer – Liste over brukte porter	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Sikkerhetsdokumentasjon for LiveSwitch-server	https://developer.liveswitch.io/liveswitch-server/server/security.html
Beste praksis for sikker tilpasning av høreapparater EHIMA-hvitbok	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
Tel.: +1.661.362.1400

info.us@advancedbionics.com

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

info.switzerland@advancedbionics.com

Hvis du ønsker informasjon om flere AB-kontorer, kan du gå til *advancedbionics.com/contact*

AB – A Sonova brand

Kontakt den lokale AB-representanten vedrørende offentlig godkjennelse og tilgjengelighet i ditt land.

Bluetooth®-merket og -logoene er registrerte varemerker som eies av Bluetooth SIG, Inc., og all bruk av disse varemerkene av Sonova AG er lisensiert.

029-S398-10

ADVANCED BIONICS
POWERFUL CONNECTIONS

029-S398-10 Rev A 2026-07-13
©2026 Advanced Bionics LLC og partnere.
Med enerett.