

Target CI v1.6

GUIDE DE CYBERSÉCURITÉ

Français

Mise à jour : juillet 2026



Sommaire

1. INTRODUCTION	3
1.1 ABRÉVIATIONS ET DÉFINITIONS :	3
2. AUTRES RESSOURCES	4
2.1 SERVICE CLIENT	4
2.2 AB PRO PORTAL	4
2.3 GUIDE D'INSTALLATION AVANCÉ	4
2.4 CONFIGURATION DU PARE-FEU TARGET CI	4
2.5 MDS2	4
2.6 INSTRUCTIONS D'UTILISATION	5
2.7 HIMSA	5
3. DIAGRAMMES DE RÉSEAU ET DE CONTEXTE	6
3.1 MODÈLE DE DÉPLOIEMENT 1 : AUTONOME	6
3.2 MODÈLE DE DÉPLOIEMENT 2 : DISTRIBUTION NOAH	7
3.3 ARTÉFACTS DE DÉPLOIEMENT	8
3.4 INTERCONNEXIONS DU SYSTÈME	9
4. CONFIGURATION REQUISE	11
5. LA CYBERSÉCURITÉ DANS LE CYCLE DE VIE DES PRODUITS	12
5.1 DÉPLOIEMENT	12
5.2 INSTALLATION	12
5.3 CONFIGURATION ET FONCTIONNEMENT	13
5.4 DÉMONTAGE ET MISE HORS SERVICE	14
6. CONTRÔLES DE SÉCURITÉ	16
6.1 CONTRÔLES D'ACCÈS	16
6.2 JOURNAUX D'AUDIT ET CONTRÔLES DE RESPONSABILISATION	16
6.3 ACCÈS À DISTANCE	17
7. PROTECTION DES INFORMATIONS	18
7.1 POLITIQUE DE CONFIDENTIALITÉ D'ADVANCED BIONICS	18
7.2 NORMES FÉDÉRALES DE TRAITEMENT DE L'INFORMATION (FIPS)	18
7.3 DONNÉES À CARACTÈRE PERSONNEL/DE SANTÉ PROTÉGÉES TRAITÉES PAR LE PRODUIT	18
7.4 SÉCURITÉ DES DONNÉES EN TRANSIT	20
7.5 SÉCURITÉ AU REPOS	21

8. INTÉGRITÉ DU LOGICIEL	24
8.1 VÉRIFICATION DU SUPPORT D'INSTALLATION TÉLÉCHARGÉ	24
8.2 VÉRIFICATION MANUELLE DU LOGICIEL D'APPAREILLAGE AVANT L'INSTALLATION	24
8.3 VÉRIFICATION AUTOMATIQUE DE L'INTÉGRITÉ DU LOGICIEL D'APPAREILLAGE INSTALLÉ.....	26
8.4 VÉRIFICATION MANUELLE DE L'INTÉGRITÉ DU LOGICIEL D'APPAREILLAGE INSTALLÉ.....	26
9. CORRECTIFS ET MISES À JOUR LOGICIELLES	28
10. GESTION DES DONNÉES	28
10.1 BASES DE DONNÉES	28
10.2 MIGRATION DES DONNÉES	29
10.3 CONFIGURATIONS DES APPAREILS AUDITIFS	29
10.4 ÉLIMINATION DES DONNÉES.....	29
11. ENVIRONNEMENT DE SÉCURITÉ – RESPONSABILITÉ PARTAGÉE...	30
12. FABRICATION, DÉVELOPPEMENT DE LOGICIELS ET GESTION DE LA SÉCURITÉ	33
13. COMPOSANTS LOGICIELS ET NOMENCLATURE	34
14. RÉFÉRENCES	56

1. INTRODUCTION

Ce document fournit des informations techniques de sécurité et de confidentialité sur le système logiciel Target CI v1.6 d'Advanced Bionics, ci-après « logiciel d'appareillage ». Le logiciel d'appareillage est conçu pour être utilisé par des audioprothésistes qualifiés pour configurer (c'est-à-dire appareiller) des appareils auditifs pour les patients ayant reçu des implants cochléaires d'Advanced Bionics.

Ce document se concentre spécifiquement sur les considérations de cybersécurité et de confidentialité qui sont pertinentes pour l'utilisation du logiciel d'appareillage. Il comprend une évaluation des contrôles de sécurité et de confidentialité actuellement intégrés au logiciel, ainsi que ceux qui devraient être appliqués et configurés dans l'environnement informatique où le produit sera utilisé aux fins prévues.

Ce document ne fournit pas d'informations techniques de sécurité et de confidentialité sur :

- les versions précédentes du logiciel d'appareillage AB
- tout logiciel AB autre que Target CI v1.6
- les sites Web AB
- les applications mobiles AB
- les appareils auditifs AB

1.1 ABRÉVIATIONS ET DÉFINITIONS :

Acronyme	Terme
FSW	Logiciel d'appareillage
SaMD	Le logiciel en tant que dispositif médical
Noah	Un système tiers de gestion des patients développé par HIMSA, utilisé pour stocker et gérer les données démographiques des patients ainsi que les données relatives aux appareillages
TeamViewer	Un outil multiplateforme d'accès à distance et de partage de bureau
SOUP	Logiciel d'origine inconnue (Software of Unknown Provenance)
HCP	Audioprothésiste
SaMD	Logiciel en tant que dispositif médical
AB	Advanced Bionics
Sonova	Advanced Bionics est une filiale à 100 % de Sonova et fait partie intégrante du groupe Sonova.
IFU	Instructions d'utilisation
PHI	Données de santé protégées
PII	Données à caractère personnel
SBOM	Nomenclature logicielle

2. AUTRES RESSOURCES

2.1 SERVICE CLIENT

Pour les personnes situées aux États-Unis et au Canada, Advanced Bionics offre un numéro de téléphone d'assistance technique sans frais (877-271-6727) assurant une assistance professionnelle dédiée du lundi au vendredi de 5 h à 17 h, heure du Pacifique.

Pour les personnes situées en dehors des États-Unis et du Canada, une assistance technique est disponible au niveau régional. Pour toute question relative au logiciel d'appareillage ou en cas de problème de matériel ou de programmation, veuillez contacter votre représentant AB local.

2.2 AB PRO PORTAL

Le logiciel d'appareillage et la documentation associée peuvent être téléchargés sur <https://www.abproportal.com> ou sur Sonova Web Client. Une connexion à un compte est requise. Cette ressource peut ne pas être disponible sur tous les marchés ; contactez votre représentant AB pour plus d'informations.

2.3 GUIDE D'INSTALLATION AVANCÉ

Le guide d'installation avancé de Target CI v1.6 est disponible sur demande. Le guide fournit des informations techniques sur le programme d'installation du logiciel d'appareillage, y compris les options de ligne de commande pour les installations silencieuses et automatisées.

2.4 CONFIGURATION DU PARE-FEU TARGET CI

Le document relatif à la configuration du pare-feu est disponible sur simple demande. Ce document fournit des recommandations techniques visant à garantir le bon fonctionnement de Target CI 1.6 derrière un pare-feu d'entreprise. Il détaille les accès HTTP/HTTPS requis ainsi que les noms d'hôtes essentiels. Ce document traite de la connectivité WebRTC via Twilio et Xirsys, en décrivant les ports TURN et de relais entre pairs, et en soulignant que de nombreuses adresses IP sont dynamiques ; il est donc recommandé d'utiliser, dans la mesure du possible, des règles basées sur les noms d'hôte.

2.5 MDS2

La déclaration du fabricant sur la sécurité des dispositifs médicaux (MDS2) est un formulaire standard de l'industrie contenant des informations sur la sécurité et la confidentialité concernant le logiciel d'appareillage d'AB. Ce formulaire est disponible sur demande.

2.6 INSTRUCTIONS D'UTILISATION

Les instructions d'utilisation sont fournies avec le support d'installation du logiciel. Pour certains marchés, les instructions d'utilisation électroniques sont disponibles pour le téléchargement à l'adresse www.advancedbionics.com/ifu

Les sections suivantes des instructions d'utilisation peuvent être pertinentes pour les professionnels de l'informatique :

- Description du produit
- Configuration minimale requise et caractéristiques de performance
- Consignes pour la sécurité informatique
- Instructions d'utilisation
- Mise au rebut et matériaux dangereux
- Assistance technique

2.7 HIMSA

L'association HIMSA (Hearing Instrument Manufacturer's Software Association) est un fournisseur de logiciels tiers qui produit Noah System 4, un système logiciel conçu pour le secteur des soins auditifs qui fournit aux audioprothésistes un système indépendant des fournisseurs pour effectuer des tâches liées aux clients.

Le logiciel d'appareillage peut éventuellement être configuré pour utiliser Noah System 4 pour le stockage des données plutôt qu'une base de données locale.

La page Web de sécurité de HIMSA fournit des réponses aux questions courantes sur la sécurité informatique concernant Noah System 4.

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

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

Consultez la section Sécurité du Centre d'apprentissage de HIMSA pour obtenir des informations de sécurité supplémentaires :

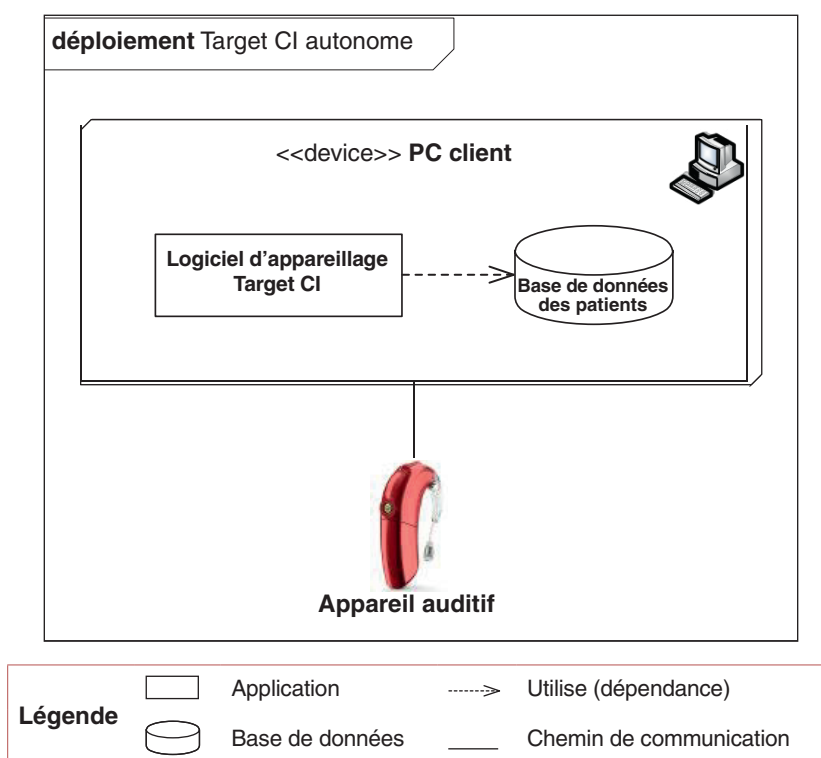
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. DIAGRAMMES DE RÉSEAU ET DE CONTEXTE

Il existe deux modèles de déploiement pris en charge pour le logiciel d'appareillage, qui est une application client (SaMD) installée sur un ordinateur Microsoft Windows de bureau disponible dans le commerce. Le logiciel n'inclut aucun matériel ni système d'exploitation.

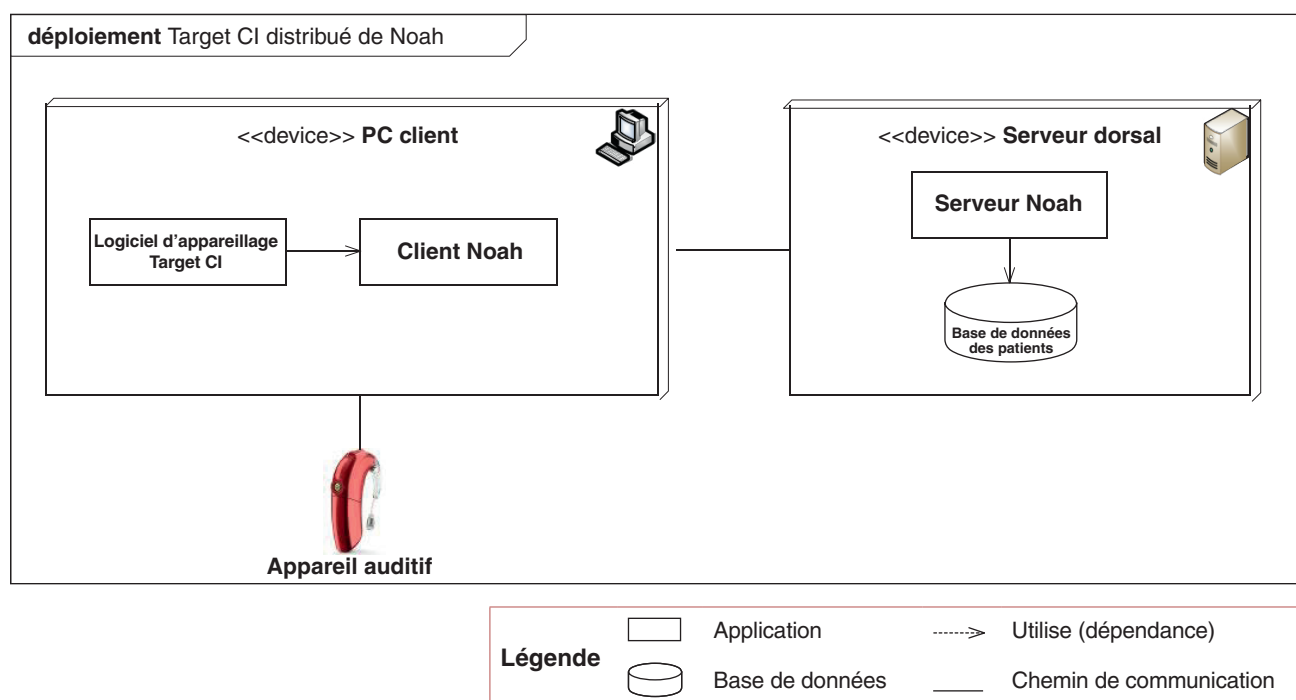
3.1 MODÈLE DE DÉPLOIEMENT 1 : AUTONOME

Dans le modèle de déploiement autonome, le logiciel d'appareillage est déployé sur un ordinateur de bureau client. La base de données des patients est stockée sur le même ordinateur de bureau et installée avec le logiciel d'appareillage.



3.2 MODÈLE DE DÉPLOIEMENT 2 : DISTRIBUTION NOAH

Dans le modèle de déploiement distribué de Noah, le logiciel d'appareillage est déployé sur un ou plusieurs PC clients sur lesquels Noah est installé. Noah, un système de gestion tiers des patients, est déployé sur un serveur interne accessible aux PC clients. La base de données des patients est stockée sur le serveur Noah et accessible via le réseau par un ou plusieurs PC clients.

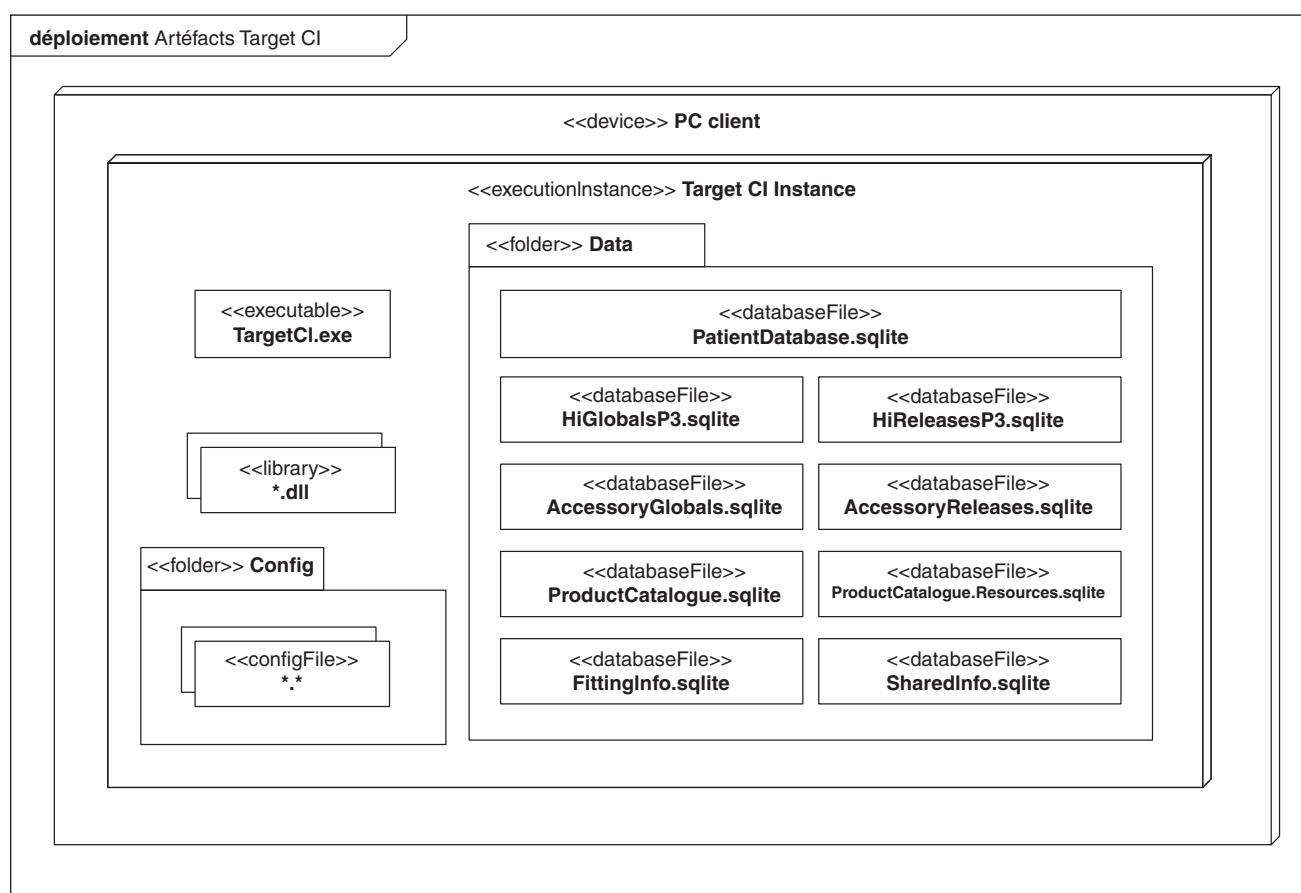


3.3 ARTÉFACTS DE DÉPLOIEMENT

Le logiciel d'appareillage s'installe avec un fichier exécutable et un ensemble de fichiers associés comprenant des DLL de composants, des fichiers de configuration et des fichiers de base de données SQLite. Les fichiers de configuration sont installés dans le dossier « %ProgramData%\Advanced Bionics\Target CI\Target CI\Config » et les fichiers de base de données sont installés dans le dossier « %ProgramData%\Advanced Bionics\Target CI\Target CI\Data ». Le dossier Data contient un seul fichier de base de données transactionnelle et plusieurs fichiers de base de données d'informations.

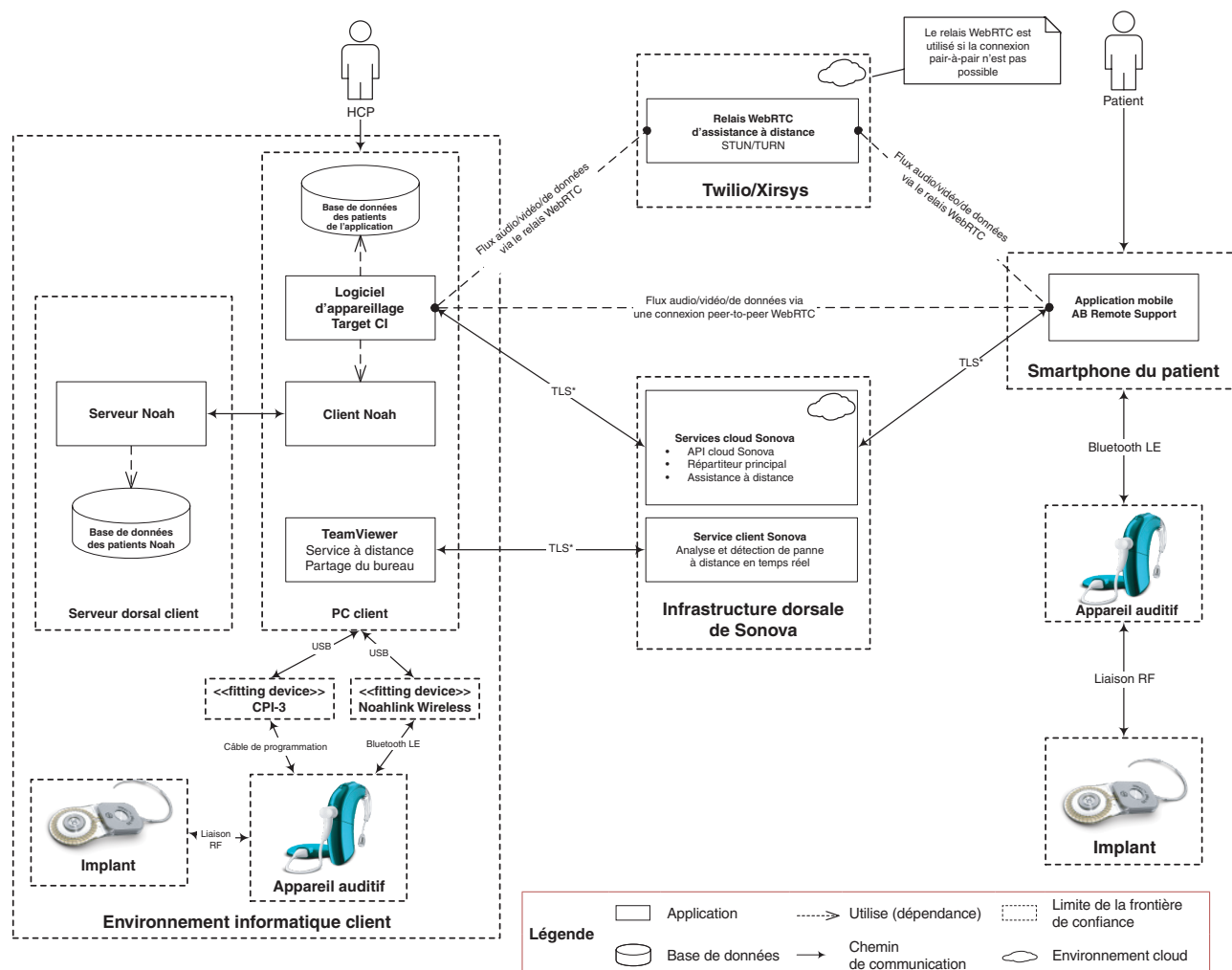
La base de données transactionnelle, PatientDatabase.sqlite, stocke les données démographiques et d'appareillage du patient et n'est installée que lorsque le logiciel d'appareillage est déployé en mode autonome.

Lorsque le logiciel d'appareillage est déployé en tant que module Noah, le système Noah fournit les services de persistance des données des patients requis au logiciel d'appareillage. Les fichiers sqlite restants font partie intégrante du logiciel d'appareillage et sont requis pour tous les modèles de déploiement.



3.4 INTERCONNEXIONS DU SYSTÈME

Le diagramme et le tableau ci-dessous illustrent les principales interconnexions du système. En règle générale, seule une partie des interconnexions disponibles est utilisée.



Source/ Destination	Service	Protocole	Port	Description
Appareil auditif	Communication des appareils auditifs	Connexion filaire / Bluetooth® Low Energy	N/A	Utilisée pour communiquer avec les appareils auditifs à des fins de contrôle, de configuration et de lecture des données et de l'état

Source/ Destination	Service	Protocole	Port	Description
Noah	Module API Noah 4	.NET Remoting	N/A	Interface principale du module utilisée pour accéder au logiciel Noah (dans le modèle de déploiement distribué de Noah uniquement)
Services cloud Sonova	API cloud Sonova, répartiteur principal, assistance à distance	SOAP, REST	443	Les services Sonova hébergés dans un centre de données Microsoft Azure sont utilisés pour : • récupérer les données de configuration du client du logiciel d'appareillage à partir du stockage dorsal de Sonova • transférer des données de journalisation et d'analyse • mettre en place l'appareillage à distance en temps réel
Twilio/Xirsys, applications mobiles AB Remote Support et AB Remote Support +	Assistance à distance	WebRTC	Ces informations figurent dans le document de confi- guration du pare-feu Target CI.	Utilisé par la fonctionnalité d'assistance à distance pour gérer la signalisation WebRTC et mener des sessions d'appareillage à distance en temps réel
Service client AB	Partage du bureau	Protocole propriétaire TeamViewer	5938, 443, 80 Reportez-vous à TeamViewerPorts	Utilisé pour effectuer une analyse et une détection de panne à distance en temps réel des problèmes affectant les installations de logiciels d'appareillage. Reportez- vous à la section 6.3 ACCÈS À DISTANCE pour plus d'informations.

4. CONFIGURATION REQUISE

Système d'exploitation	Windows 10,11, Professionnel/Entreprise
.NET Framework	Version 4.8
Processeur	Intel® Core™ i5 ou équivalent avec des performances égales ou supérieures
RAM	4 Go ou plus
Espace sur le disque dur	3 Go ou plus
Configuration minimale requise pour l'affichage	• Résolution 1280 x 1024 (mise à l'échelle maximale 125 %) • Couleur 24 bits
Pilotes de périphériques	• Pilote Noahlink Wireless (la dernière version disponible auprès de HIMSA est requise si vous utilisez une interface tierce de programmation Noahlink Wireless connectée par USB). • Pilote CPI-3 (requis si vous utilisez une interface de programmation CPI-3 connectée par USB).
Base de données	SQLite ou Noah System 4 (version 4.16 ou supérieure)
Connexion Internet	Connexion Internet requise pour l'assistance à distance et la journalisation de l'analyse, reportez-vous à la section 3.4 Interconnexions du système ; intranet requis lors de l'utilisation de Noah System 4 en réseau.
Ports réseau	Voir la section 3.4 Interconnexions du système ; voir la section 2. Autres ressources — HIMSA pour les ports utilisés par Noah System 4.

5. LA CYBERSÉCURITÉ DANS LE CYCLE DE VIE DES PRODUITS

5.1 DÉPLOIEMENT

Méthodes de déploiement approuvées :

1. Télécharger le logiciel depuis le client Web Sonova (SFTP) à l'adresse <https://webclient.sonova.com> ou depuis le portail AB Pro à l'adresse <https://www.abproportal.com>
2. Installer à partir d'une clé USB officielle Advanced Bionics.

Avant l'installation, vérifiez la signature numérique du programme d'installation et analysez le fichier à l'aide d'un logiciel antivirus à jour. Reportez-vous à la section 8 pour obtenir des instructions détaillées sur la vérification de l'intégrité. Appliquez les mesures de sécurité informatiques standard dans le secteur de la santé lors du déploiement, notamment la protection des terminaux et les restrictions réseau.

Lors de l'utilisation d'une clé USB :

- Utilisez exclusivement les clés USB officielles fournies par Advanced Bionics.
- Veillez à la sécurité physique de la clé USB et n'en modifiez pas le contenu.
- Analysez la clé USB et l'environnement d'installation à l'aide d'un antivirus à jour et d'une liste blanche d'applications.
- Advanced Bionics décline toute responsabilité concernant les données non autorisées stockées sur les clés USB contenant le pack d'installation.

5.2 INSTALLATION

Un compte administrateur est requis pour installer le logiciel d'appareillage. Une fois le logiciel installé, il peut être exécuté sans autorisations administratives ou de haut niveau.

Consultez la section 8. Intégrité du logiciel, pour obtenir des informations sur la vérification de l'intégrité du logiciel avant l'installation.

Avant l'installation, il est recommandé aux administrateurs du système de s'assurer que :

- la version du logiciel d'appareillage à installer est la dernière disponible ;
- le système d'exploitation sous-jacent est à jour ;
- l'intégrité et l'authenticité des données du programme d'installation du logiciel sont vérifiées. Consultez la section 8 pour obtenir des informations sur la validation de l'intégrité du logiciel avant l'installation.

Deux programmes d'installation sont disponibles pour installer le logiciel d'appareillage :

- Programme d'installation standard
- Programme d'installation informatique professionnelle

Le programme d'installation informatique professionnelle est un fichier MSI unique et exclut les composants prérequis, mais est par ailleurs équivalent au programme d'installation standard.

Les composants prérequis incluent Microsoft .NET Framework v4.8 et les packages Microsoft Visual Studio C++ Redistributable.

Les deux programmes d'installation prennent en charge les scénarios d'installation avancés, y compris l'installation silencieuse.

Le programme d'installation informatique professionnelle ne doit être utilisé que si votre organisation exige que les composants prérequis soient installés et gérés par votre organisation et non par le programme d'installation du logiciel d'appareillage. Dans tous les autres cas, le programme d'installation standard doit être utilisé.

Le programme d'installation informatique professionnelle peut être obtenu auprès d'un représentant clinique AB. Le programme d'installation informatique professionnelle ne peut pas être utilisé pour réparer, réinstaller ou désinstaller des installations effectuées par le programme d'installation standard. Le programme d'installation standard ne peut pas être utilisé pour réparer, réinstaller ou désinstaller des installations effectuées par le programme d'installation informatique professionnelle.

Pour les scénarios d'installation avancés, suivez les instructions figurant dans le Guide d'installation avancée du logiciel d'appareillage (voir section 2.3). Pour les cas d'installation standard, veuillez vous reporter à la section 2.5 du présent document, qui contient un lien vers les instructions d'utilisation du logiciel d'appareillage (IFU).

5.3 CONFIGURATION ET FONCTIONNEMENT

Le logiciel d'appareillage prend en charge un ensemble de contrôles et de fonctionnalités liés à la confidentialité et à la sécurité. Certaines fonctionnalités du logiciel d'appareillage relatives à la confidentialité et à la sécurité sont activées par défaut, d'autres sont configurables lors de l'installation et dépendent du modèle de déploiement sélectionné, tandis que d'autres encore sont configurables en cours d'utilisation via l'interface graphique de l'application.

Se référer à :

- Section 6 : liste des mesures de sécurité permettant de renforcer la protection du système d'application du logiciel d'appareillage
- Section 7 : liste des mesures de sécurité permettant de renforcer la protection des données traitées par l'application du logiciel d'appareillage

Les contrôles supplémentaires en matière de confidentialité et de sécurité (qui ne sont pas pris en charge par le logiciel d'appareillage au niveau de l'application) doivent être activés et configurés par les utilisateurs (par exemple, les professionnels de santé, les administrateurs système, le personnel informatique) au niveau du système d'exploitation et/ou au niveau de l'infrastructure informatique. Veuillez vous reporter à la Section 11 de ce document pour obtenir une liste détaillée de recommandations de bonnes pratiques courantes et de contrôles de sécurité pour l'environnement d'appareillage dans lequel le logiciel d'appareillage sera utilisé.

Pare-feu

Le logiciel d'appareillage n'est pas équipé d'un pare-feu interne.

Si un pare-feu externe est activé (par exemple au niveau du système d'exploitation), il peut être nécessaire de mettre à jour sa configuration afin d'autoriser le trafic entrant et sortant requis (par exemple, les flux audio, vidéo et de données WebRTC lors d'une session d'assistance à distance). Consultez le document Configuration du pare-feu du logiciel de calibrage, qui contient la liste des adresses réseau et des ports utilisés par le logiciel d'appareillage.

Paramètres du proxy

Le logiciel d'appareillage est fourni avec un proxy local. Il est possible de modifier les paramètres de ce proxy via l'interface graphique du logiciel d'appareillage :

- Pas de proxy
- Détection automatique des paramètres de proxy
- Configuration manuelle du proxy. Si cette option est sélectionnée, les paramètres suivants sont configurables :
 - Adresse
 - Port
 - Activer/désactiver l'authentification par proxy (nom d'utilisateur, mot de passe, domaine)

5.4 DÉMONTAGE ET MISE HORS SERVICE

Veuillez vous référer au document IFU (Instructions d'utilisation) du logiciel d'appareillage pour obtenir des instructions détaillées sur la désinstallation du logiciel.

Le programme de désinstallation ne supprime pas les catégories de données répertoriées dans le tableau ci-dessous. Sauf indication contraire dans la colonne « Remarques » du tableau, ces données doivent être supprimées manuellement des systèmes par les administrateurs système ; par exemple, en supprimant manuellement les fichiers ou en effaçant le disque système utilisé pour le stockage des données.

Catégorie de données	Emplacement par défaut	Remarques
Données de l'application	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI	Comprend les types de données suivants : • Données analytiques • Données de configuration • Journaux d'application • Fichiers temporaires

Catégorie de données	Emplacement par défaut	Remarques
Données personnelles	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI\Data	Base de données des patients (pertinente uniquement pour le modèle de déploiement autonome)
Outil d'accès à distance	C:\Program Files (x86)\Common Files\ Advanced Bionics\ TeamViewer	Utilisé pour effectuer une analyse et une détection de panne en temps réel des problèmes affectant les logiciels d'appareillage, y compris ceux survenant lors de leur installation ou de leur désinstallation. Reportez-vous à la section 6.3 pour plus d'informations.

Lorsque vous désinstallez le logiciel d'appareillage de l'ordinateur de bureau ou portable destiné à être mis hors service ou éliminé, veillez à ce que toutes les données sensibles (par exemple, les données de santé protégées (PHI) et les données à caractère personnel (PII)) soient effacées.

Pour les déploiements Noah, veuillez consulter les instructions détaillées concernant la suppression des données pour les déploiements Noah, disponibles à l'adresse suivante :

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

Les supports externes contenant des données exportées à partir du logiciel d'appareillage, y compris les rapports et les journaux, doivent être sécurisés. Lorsqu'elles ne sont plus utilisées, les données doivent être effacées de manière sécurisée et/ou les supports doivent être effacés ou détruits de manière sécurisée.

Des procédures et des outils approuvés doivent être utilisés pour la suppression sécurisée des données stockées sur des supports amovibles, conformément aux réglementations et directives applicables en matière de traitement des informations des patients / données à caractère personnel (PII) / données de santé protégées (PHI).

6. CONTRÔLES DE SÉCURITÉ

Le logiciel d'appareillage est une application client installée sur un ordinateur de bureau Microsoft Windows disponible dans le commerce. Le logiciel d'appareillage peut être installé en tant qu'application autonome ou en tant que module Noah.

6.1 CONTRÔLES D'ACCÈS

Le logiciel d'appareillage ne restreint pas l'accès à ses fonctionnalités en fonction des conditions de connexion et des rôles des utilisateurs individuels. Les contrôles d'accès basés sur les rôles ne sont pas pris en charge.

Accès utilisateur local

Lorsque le logiciel d'appareillage est installé en tant qu'application autonome, il dépend des mécanismes de contrôle d'accès du système d'exploitation hôte. Le personnel informatique du client peut configurer le système d'exploitation hôte pour gérer l'authentification des utilisateurs et attribuer des droits d'accès ou des privilèges. Il est vivement recommandé à chaque utilisateur de se connecter à l'aide d'un compte individuel et unique.

Des contrôles compensatoires supplémentaires sont décrits dans la section 11 de ce document et dans la section « Directives pour la sécurité informatique » du manuel d'utilisation.

Lorsque le logiciel d'appareillage est installé en tant que module Noah, le contrôle d'accès est géré via Noah System 4.

Pour plus de détails sur les fonctionnalités de contrôle d'accès mises en œuvre par Noah System 4, reportez-vous à la documentation disponible sur www.HIMSA.com.

Accès au service

Les techniciens de maintenance sur site peuvent accéder au logiciel d'appareillage dans le respect des contrôles d'accès configurés par le service informatique du client pour gérer l'authentification.

Les techniciens d'assistance d'AB peuvent accéder au logiciel d'appareillage grâce à la fonctionnalité de partage de bureau prise en charge par ce dernier. Reportez-vous à la section 6.3 pour obtenir des informations détaillées sur les contrôles de sécurité activés pour cette fonctionnalité.

6.2 JOURNAUX D'AUDIT ET CONTRÔLES DE RESPONSABILISATION

Le logiciel d'appareillage ne génère aucun journal d'audit ni rapport supplémentaire en dehors de ceux fournis par le système d'exploitation sous-jacent.

Modèle de déploiement autonome

Lorsque le logiciel d'appareillage est installé en tant qu'application autonome, il s'appuie sur les mécanismes d'audit fournis par le système d'exploitation hôte. Le logiciel d'appareillage ne dispose pas d'une telle fonctionnalité intégrée. Le système d'exploitation hôte peut être configuré par le personnel informatique du client pour enregistrer certains événements comme les lancements/exécutions du logiciel d'appareillage. Il est recommandé que chaque utilisateur se connecte au système d'exploitation hôte avec un compte utilisateur unique pour faciliter l'audit.

Modèle de déploiement distribué de Noah

Lorsque le logiciel d'appareillage est installé en tant que module Noah, des journaux d'audit sont générés et la gestion de ces journaux est assurée par le système Noah (journal d'activité Noah). Pour plus de détails sur les fonctionnalités de contrôle d'audit disponibles dans Noah System 4, reportez-vous à la documentation fournie sur www.himsa.com

6.3 ACCÈS À DISTANCE

La fonctionnalité de partage de bureau permet une analyse et une détection de panne à distance en temps réel des problèmes affectant les installations de logiciels d'appareillage. Cette fonctionnalité est basée sur l'outil tiers TeamViewer QuickSupport (déployé par défaut avec le logiciel d'appareillage) et permet aux professionnels du service client AB de se connecter à distance à l'ordinateur de l'audioprothésiste et d'obtenir un contrôle total sur le bureau, y compris l'accès au système d'exploitation et de fichiers sous-jacent.

Pour établir une session de partage du bureau, l'interaction de l'audioprothésiste est requise. L'audioprothésiste doit d'abord exécuter l'outil TeamViewer QuickSupport (par exemple, via le logiciel d'appareillage Target CI) et communiquer ses informations d'identification TeamViewer à l'équipe d'Assistance AB via un canal de communication hors bande (par exemple, un appel téléphonique).

Le nom du membre de l'équipe d'Assistance AB et son identifiant TeamViewer sont affichés par défaut sur l'écran de l'ordinateur de l'audioprothésiste pendant chaque session de partage du bureau active.

Tout le trafic réseau de partage du bureau est sécurisé à l'aide des normes des protocoles et algorithmes cryptographiques considérés comme sûrs selon les normes actuelles (échange de clés publiques/privées RSA et chiffrement de session AES 256 bits).

L'outil d'accès à distance peut être supprimé manuellement sans affecter les autres fonctionnalités du FSW Target. Le programme d'installation du FSW Target prend en charge un paramètre d'installation de ligne de commande pour permettre une installation de ligne de commande du FSW Target sans inclure l'outil d'accès à distance.

7. PROTECTION DES INFORMATIONS

7.1 POLITIQUE DE CONFIDENTIALITÉ D'ADVANCED BIONICS

La politique de confidentialité décrivant comment Advanced Bionics collecte, transfère, stocke et utilise les données personnelles peut être téléchargée sur : AdvancedBionics.com/privacy.

Advanced Bionics n'héberge, ne stocke, ne sauvegarde et n'a accès à aucune donnée stockée dans le logiciel d'appareillage ou dans les bases de données Noah, à moins que les données ne soient expressément envoyées à Advanced Bionics.

7.2 NORMES FÉDÉRALES DE TRAITEMENT DE L'INFORMATION (FIPS)

Target CI v1.6 est conforme aux normes de chiffrement FIPS 140-2.

7.3 DONNÉES À CARACTÈRE PERSONNEL/DE SANTÉ PROTÉGÉES TRAITÉES PAR LE PRODUIT

Le logiciel d'appareillage traite les données personnelles et médicales des patients.

Les informations relatives au patient sont soit saisies manuellement par l'utilisateur du logiciel d'appareillage, soit transmises à l'application via un ou plusieurs de ses flux de données.

Les types d'informations suivants sont traités dans les principaux flux de données du logiciel d'appareillage :

	Services cloud Sonova (répartiteur principal, assistance à distance)	Appareil auditif	Appli- cations mobiles	Base de données patient (locale/ Noah)	Accès à distance
Nom				X	X(2)
Adresse				X	X(2)
Date de naissance	X(1)		X	X	X(2)
Numéro de téléphone				X	X(2)
Adresse e-mail				X	X(2)
Numéros de dossier médical				X	X(2)
Identifiants des appareils et numéros de série	X(1)	X	X	X	X(2)
Adresse IP	X(1)				
Audiogrammes, RECD, REUG	X(1)	X	X	X	X(2)
Données d'appareillage		X	X	X	X(2)
Données relatives à l'utilisation des appareils auditifs	X(1)	X	X	X	
Données d'utilisation du logiciel d'appareillage	X(1)				

(1) Données pseudonymisées avant leur enregistrement dans le lac de données de Sonova.

(2) Lors d'une session de partage d'écran en temps réel, les techniciens du service client d'AB prennent le contrôle total du poste de travail de HCP, y compris l'accès au système d'exploitation sous-jacent, au système de fichiers et aux données qui y sont stockées. Reportez-vous à la section 6.3 pour plus d'informations.

Pour obtenir des informations plus détaillées sur la collecte et le traitement des données, veuillez contacter votre interlocuteur local.

7.4 SÉCURITÉ DES DONNÉES EN TRANSIT

La sécurité des communications est assurée et activée dans toutes les communications réseau entrantes et sortantes du logiciel d'appareillage. À l'exception de la fonctionnalité d'assistance à distance (qui utilise le protocole WebRTC) et de la communication Bluetooth avec les appareils auditifs et les accessoires, toutes les autres connexions sont protégées par le protocole Transport Layer Security (TLS) qui assure la confidentialité, l'intégrité et l'authenticité.

TLS

La configuration TLS est conforme aux bonnes pratiques et aux recommandations de sécurité actuelles documentées dans le document BCP 195 – Recommandations pour une utilisation sécurisée de TLS et DTLS [8], notamment :

- Pas de prise en charge des versions de SSL et TLS antérieures à 1.2
- Pas de prise en charge des suites de chiffrement qui utilisent des algorithmes cryptographiques offrant moins de 128 bits de sécurité
- Prise en charge des extensions TLS recommandées par le BCP 195
- Pas de prise en charge des extensions non sécurisées selon le BCP 195

DTLS

Le chiffrement est une fonctionnalité obligatoire de WebRTC et est appliqué à tous les flux multimédias envoyés via WebRTC. Le protocole de chiffrement utilisé dépend du type de canal ; les flux de données sont chiffrés à l'aide de DTLS 1.2 et les flux multimédias sont chiffrés à l'aide du protocole SRTP (Secure Real-time Transport Protocol) utilisé, car il s'agit d'une option plus légère que DTLS.

Consultez le lien suivant pour obtenir des informations plus détaillées sur la configuration de sécurité de l'assistance à distance WebRTC :

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

BLE

La communication sans fil Bluetooth Low Energy avec les appareils auditifs et les accessoires est chiffrée et protégée en intégrité par défaut (sauf pour les cas d'utilisation d'identification et de détection). De plus, la durée du mode d'appairage Bluetooth de l'appareil auditif est limitée dans le temps. Reportez-vous à la documentation disponible sur l'appareil auditif pour une description plus détaillée de la sécurité du canal de communication Bluetooth.

7.5 SÉCURITÉ AU REPOS

Données de l'application

Les données de l'application se trouvent sur la même machine, dans le répertoire par défaut : C:\ProgramData\Advanced Bionics\Target CI\Target CI

Le droit d'accès hérite de celui de son dossier parent et est limité aux utilisateurs connectés au système local (utilisateur intégré INTERACTIF group¹) lors de l'installation du logiciel.

Les utilisateurs autorisés disposent d'un accès en lecture et en écriture au répertoire.

Afin de réduire le risque d'accès non autorisé aux données de l'application via le réseau, veuillez vous assurer qu'aucun des dossiers ou fichiers contenant ces données n'est partagé sur le réseau. Les emplacements par défaut des données de l'application sont répertoriés au point 5.4.

Base de données des patients – Modèle de déploiement autonome

Lorsque le logiciel d'appareillage est installé en tant qu'application autonome, la base de données des patients se trouve sur la même machine et les dossiers des patients ne sont pas chiffrés au repos. L'application ne transmet aucune donnée à caractère personnel sur le réseau.

Tout utilisateur capable de se connecter à la machine sur laquelle le logiciel d'appareillage est installé aura un accès complet à toutes les données de l'application, y compris la base de données des patients. Veuillez consulter la section Protection des données pour obtenir des conseils sur les mesures de protection des données recommandées.

Dans certaines juridictions, la réglementation peut exiger le chiffrement de toutes les données des patients afin d'éviter toute responsabilité potentielle en cas de perte ou de vol de données. Activez BitLocker ou un chiffrement complet du disque équivalent (au niveau du système d'exploitation ou basé sur le matériel) pour protéger les données contre tout accès ou copie non autorisés pendant que les données sont au repos.

BitLocker est une fonctionnalité Windows intégrée qui chiffre l'intégralité du disque et nécessite une authentification pour y accéder. Consultez toujours les directives officielles de Microsoft et la politique de sécurité informatique de votre organisation avant d'activer BitLocker.

Comment activer BitLocker

Des droits d'administration sont requis pour gérer BitLocker.

1. Rechercher « Gérer BitLocker »

Ouvrez le menu Démarrer, saisissez « Gérer BitLocker » et sélectionnez-le dans les résultats de la recherche.

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

2. Sélectionner le disque système

Choisissez le disque sur lequel Windows est installé pour configurer les paramètres de chiffrement.

3. Choisir une méthode de déverrouillage

Sélectionnez l'une des options suivantes :

- TPM uniquement
- TPM + PIN
- TPM + clé USB

Suivez les bonnes pratiques de Microsoft et la politique de sécurité informatique de votre organisation lors de la sélection de la méthode de déverrouillage.

4. Sauvegarder la clé de récupération

Sauvegardez la clé de récupération à l'aide de méthodes sécurisées et approuvées par l'entreprise. Les options recommandées incluent :

- le stockage dans Microsoft Entra ID (anciennement Azure AD) ou Active Directory pour les appareils appartenant au domaine ;
- l'enregistrement dans un emplacement réseau sécurisé et à accès contrôlé avec chiffrement et journalisation d'audit ;
- l'utilisation d'une solution d'entiercement de clés gérée approuvée par votre organisation.

Évitez d'enregistrer la clé sur des disques locaux, des clés USB ou de l'imprimer, sauf si cela est explicitement autorisé par la politique. Les clés de récupération doivent être protégées avec la même rigueur que les autres informations d'identification sensibles et immédiatement renouvelées si elles sont exposées.

5. Démarrer le chiffrement

Choisissez :

- Disque entier : recommandé pour la plupart des scénarios d'entreprise. Chiffre tous les secteurs, y compris l'espace inutilisé, pour empêcher la rémanence des données.

Base de données des patients – Module de déploiement distribué de Noah

Lorsque le logiciel d'appareillage est installé en tant que module Noah, les données à caractère personnel sont stockées dans la base de données des patients hébergée par Noah. La base de données des patients hébergée par Noah peut se trouver sur une autre machine. Les données à caractère personnel et autres données des patients sont conservées par le logiciel Noah et le chiffrement des données au repos des patients est assuré par le système Noah. Le logiciel d'appareillage peut transmettre/recevoir les données à caractère personnel via une connexion réseau filaire ou sans fil lorsqu'une base de données Noah est configurée pour l'accès au réseau.

Les données à caractère personnel stockées dans la base de données Noah en réseau seront accessibles par d'autres utilisateurs sur différents PC disposant d'autorisations sur la même base de données en réseau. La base de données Noah peut également être configurée pour un accès hors réseau et installée sur le même PC que le logiciel d'appareillage.

Noah empêche le logiciel d'appareillage d'accéder à la base de données des dossiers des patients. Lorsqu'un utilisateur ouvre un dossier patient dans le logiciel d'appareillage via Noah Client, le logiciel d'appareillage ne peut que lire et écrire dans le dossier patient actuellement ouvert et n'est pas en mesure d'accéder aux autres dossiers patients dans la base de données Noah.

Pour plus d'informations sur les normes de chiffrement utilisées par Noah System, veuillez consulter le lien suivant :

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

Fichiers d'exportation de RMA

Le logiciel d'appareillage permet d'exporter les informations client vers un fichier. Le fichier RMA peut être envoyé à Advanced Bionics pour résoudre les problèmes de RMA ou d'assistance associés.

Le fichier RMA est chiffré de manière asymétrique avec RSA à l'aide d'une longueur de clé de 2048 bits. Le logiciel d'appareillage ne dispose d'aucune fonctionnalité permettant de déchiffrer un fichier RMA.

Fichiers d'exportation anonymisés

Le logiciel d'appareillage permet d'exporter les informations client vers un fichier anonymisé. Les données à caractère personnel du client, telles que la date de naissance et le nom, sont remplacées par des valeurs génériques. Le fichier n'est pas chiffré et peut être importé dans la même instance ou dans une instance différente du logiciel d'appareillage.

Fichiers d'exportation standard

Le logiciel d'appareillage permet d'exporter les informations client vers un fichier d'exportation standard. Le fichier utilise un format binaire propriétaire et n'est pas chiffré. Le fichier peut être importé dans la même instance ou dans une instance différente du logiciel d'appareillage. Lors de l'utilisation de cette fonctionnalité, les utilisateurs de logiciels d'appareillage doivent s'assurer que les fichiers d'exportation standard sont traités conformément à leurs politiques informatiques locales pour la gestion des données à caractère personnel non chiffrées.

Appareil auditif

Le logiciel d'appareillage stocke les informations client sur l'appareil auditif du client. Les données à caractère personnel, telles que le nom et la date de naissance du client, ne sont pas stockées sur l'appareil auditif. Les autres informations non PII sont stockées à l'aide du chiffrement PBKDF2 avec une clé de 128 bits.

Le logiciel d'appareillage peut transmettre/recevoir des informations client non-PII depuis/vers un appareil auditif via un appareil filaire propriétaire (c.-à-d. CPI-3), les applications mobiles AB Remote Support et AB Remote Support + ou un appareil Noahlink Wireless.

L'appareil Noahlink Wireless se connecte à l'appareil auditif à l'aide de Bluetooth Low Energy (BLE) via un canal chiffré AES de 128 bits BLE standard.

8. INTÉGRITÉ DU LOGICIEL

8.1 VÉRIFICATION DU SUPPORT D'INSTALLATION TÉLÉCHARGÉ

Le support d'installation du logiciel d'appareillage Target CI peut être téléchargé dans certaines régions depuis Pro Portal d'Advanced Bionics ou Sonova Web Client. Le support d'installation téléchargé peut être authentifié à l'aide de n'importe quel outil de hachage SHA-256 de confiance.

Le hachage SHA256 du fichier zip d'installation standard est :

A42B8F41A5A4111D1C6F67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

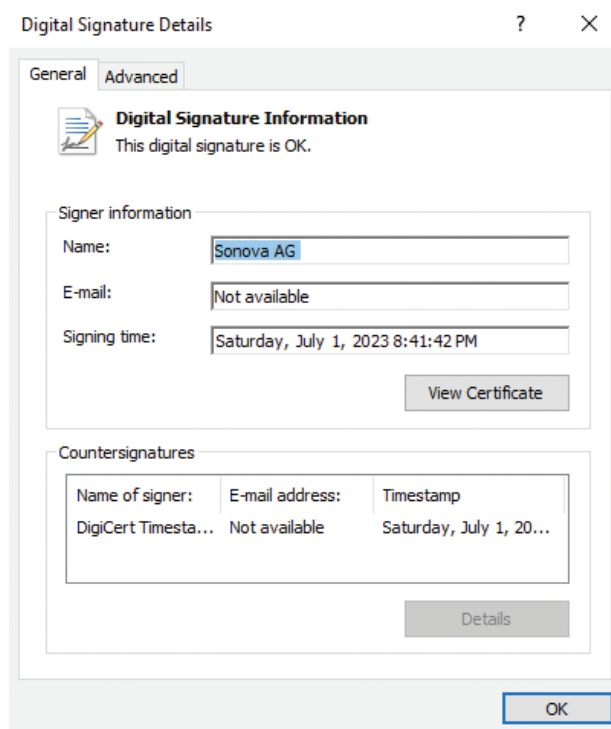
Le hachage SHA256 du fichier zip d'installation pour professionnels de l'informatique est :
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 VÉRIFICATION MANUELLE DU LOGICIEL D'APPAREILLAGE AVANT L'INSTALLATION

Les utilisateurs peuvent effectuer les étapes suivantes pour vérifier l'intégrité et l'authenticité du logiciel d'appareillage avant l'installation :

1. Ouvrez l'Explorateur Windows et accédez au dossier racine du support d'installation du logiciel d'appareillage. Si votre support d'installation est une clé USB, insérez-la dans un port USB et accédez à sa racine. Si votre support d'installation est un fichier zip, décompressez-le dans un dossier et accédez à ce dossier.
2. Faites un clic droit sur SonovaVerify.exe et sélectionnez Propriétés dans le menu contextuel.
3. Sélectionnez l'onglet Signatures numériques.
4. Double-cliquez sur la signature SHA256 « Sonova AG ».

5. Vérifiez que les éléments de la signature sont valides. Vérifiez en particulier que le message « La signature numérique est valide. » apparaît en haut et que le nom du signataire et l'heure de signature correspondent à l'image suivante :



6. Cliquez sur le bouton « Afficher le certificat », puis sur l'onglet « Détails » et vérifiez que la valeur du champ « Empreinte digitale » correspond à celle-ci : db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Fermez les boîtes de dialogue contextuelles et double-cliquez sur SonovaVerify.exe
8. Vérifiez que « NO ERRORS DETECTED » (AUCUNE ERREUR DÉTECTÉE) s'affiche comme indiqué dans l'image suivante :

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

Le message « NO ERRORS DETECTED » (AUCUNE ERREUR DÉTECTÉE) indique que la vérification de l'intégrité et de l'authenticité du contenu du support d'installation du logiciel d'appareillage a été effectuée avec succès. Cela signifie que SonovaVerify.exe a authentifié et vérifié l'intégrité de tous les fichiers et dossiers. Cela permet de vérifier que les contenus du support d'installation du logiciel d'appareillage n'ont pas été altérés, corrompus ou compromis d'une autre manière.

SonovaVerify.exe affichera des avertissements ou des messages d'erreur si des fichiers ou des dossiers sont manquants ou si des fichiers ou des dossiers inattendus ont été ajoutés au support d'installation. Si des messages d'avertissement ou d'erreur s'affichent, cela signifie que la vérification de l'intégrité et de l'authenticité du contenu du support d'installation du logiciel d'appareillage a échoué. Il est donc recommandé de :

- ne pas procéder à l'installation
- n'ouvrir ni n'exécuter aucun fichier contenu dans l'image d'installation du logiciel d'appareillage ; signaler le problème au service d'assistance d'Advanced Bionics (voir la section 2.1).

8.3 VÉRIFICATION AUTOMATIQUE DE L'INTÉGRITÉ DU LOGICIEL D'APPAREILLAGE INSTALLÉ

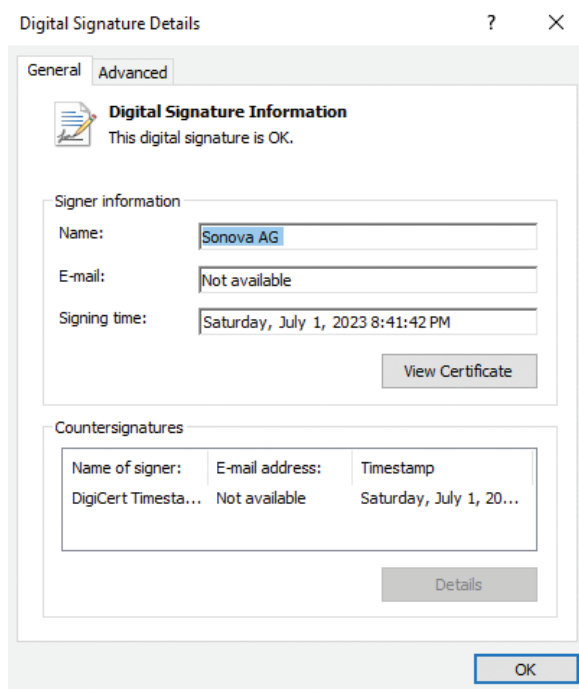
SonovaVerify est intégré au logiciel d'appareillage et s'exécute à chaque lancement de l'application pour vérifier l'intégrité des fichiers de programme du logiciel d'appareillage. Les fichiers de programme sont signés numériquement à l'aide de pratiques normalisées du secteur et de certificats émis par une autorité de certification de confiance. Le logiciel avertit l'utilisateur via des messages d'avertissement si des fichiers de programme sont compromis.

8.4 VÉRIFICATION MANUELLE DE L'INTÉGRITÉ DU LOGICIEL D'APPAREILLAGE INSTALLÉ

Les utilisateurs peuvent effectuer les étapes suivantes pour vérifier l'intégrité et l'authenticité du logiciel d'appareillage installé à tout moment sans avoir besoin de lancer le logiciel d'appareillage :

1. Ouvrez l'Explorateur Windows et accédez au dossier exécutable du logiciel d'appareillage, généralement situé dans :C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Faites un clic droit sur SonovaVerify.exe et sélectionnez Propriétés dans le menu contextuel.
3. Sélectionnez l'onglet Signatures numériques.
4. Double-cliquez sur la signature SHA256 « Sonova AG ».

5. Vérifiez que les éléments de la signature sont valides, en particulier que le message « La signature numérique est valide. » apparaît en haut et que le nom du signataire et l'heure de signature correspondent à l'image suivante :



6. Cliquez sur le bouton « Afficher le certificat », puis sur l'onglet « Détails » et vérifiez que la valeur du champ « Empreinte digitale » correspond à celle-ci : db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Fermez les boîtes de dialogue contextuelles et double-cliquez sur SonovaVerify.exe
8. Vérifiez que « NO ERRORS DETECTED » (AUCUNE ERREUR DÉTECTÉE) s'affiche comme indiqué dans l'image suivante :

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

Le message « NO ERRORS DETECTED » (AUCUNE ERREUR DÉTECTÉE) indique que la vérification de l'intégrité et de l'authenticité du contenu du support d'installation du logiciel d'appareillage a été effectuée avec succès. Cela signifie que SonovaVerify.exe a authentifié et vérifié l'intégrité de tous les fichiers et dossiers. Cela permet de vérifier que les contenus du support d'installation du logiciel d'appareillage n'ont pas été altérés, corrompus ou compromis d'une autre manière.

SonovaVerify.exe affichera des avertissements ou des messages d'erreur si des fichiers ou des dossiers sont manquants ou si des fichiers ou des dossiers inattendus ont été ajoutés au support d'installation. Si des messages d'avertissement ou d'erreur s'affichent, cela signifie que la vérification de l'intégrité et de l'authenticité du contenu du support d'installation du logiciel d'appareillage a échoué. Il est donc recommandé de :

- ne pas procéder à l'installation
- n'ouvrir ni n'exécuter aucun fichier contenu dans l'image d'installation du logiciel d'appareillage ; signaler le problème au service d'assistance d'Advanced Bionics (voir la section 2.1).

9. CORRECTIFS ET MISES À JOUR LOGICIELLES

Les mises à jour automatiques ne sont pas prises en charge. Reportez-vous à la Section 12 pour plus d'informations.

10. GESTION DES DONNÉES

10.1 BASES DE DONNÉES

Le logiciel d'appareillage utilise une base de données transactionnelle pour stocker les données des patients et un ensemble de bases de données d'informations qui fournissent les configurations de métadonnées requises par l'application.

Consultez la section 3. Diagrammes de réseau et de contexte – Artéfacts de déploiement pour obtenir une liste détaillée de toutes les bases de données déployées par le logiciel d'appareillage.

Lorsque le logiciel d'appareillage est installé en tant qu'application autonome, la base de données des patients est interne au logiciel d'appareillage. La base de données des patients, stockée dans le fichier PatientDatabase.sqlite, se trouve sur la même machine que le logiciel d'appareillage et fournit le stockage des données des patients. Pour sauvegarder les données d'application lorsque Target CI est déployé en tant qu'application autonome, créez une copie de sauvegarde de l'intégralité du dossier situé à l'emplacement %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Protégez les sauvegardes de données non seulement contre la perte de données, mais également contre le vol. Lorsque le logiciel d'appareillage est installé en tant que module Noah, les données des patients sont stockées dans la base de données fournie par le système

Noah. La base de données Noah peut être configurée pour l'accès au réseau. La base de données Noah peut également être configurée pour un accès hors réseau et installée sur le même PC que le logiciel d'appareillage. Configurez le chiffrement de la base de données Noah pour protéger les données (reportez-vous à la documentation HIMSA).

Pour le mode de déploiement distribué de Noah, reportez-vous au lien suivant pour obtenir des instructions sur la sauvegarde et la restauration de la base de données des patients Noah :

<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 MIGRATION DES DONNÉES

Le logiciel d'appareillage permet aux utilisateurs de migrer les dossiers des patients depuis le logiciel d'appareillage précédent d'AB, SoundWave 3.2. Les dossiers des patients doivent être accessibles depuis une installation SoundWave 3.2 sur le même ordinateur que Target CI afin d'être migrés.

10.3 CONFIGURATIONS DES APPAREILS AUDITIFS

Le logiciel d'appareillage permet d'exporter et d'importer les configurations et les paramètres de l'appareil.

10.4 ÉLIMINATION DES DONNÉES

Pour obtenir des conseils sur l'élimination des données, veuillez vous reporter à la section 5.4, Démontage et mise hors service, du présent document, ainsi qu'à la section Élimination et matières dangereuses du mode d'emploi. Pour les déploiements de Noah, des instructions détaillées concernant la suppression des dossiers des patients sont disponibles à l'adresse suivante :

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

11. ENVIRONNEMENT DE SÉCURITÉ – RESPONSABILITÉ PARTAGÉE

Le logiciel d'appareillage a été conçu pour une utilisation prévue dans laquelle la gestion des risques de cybersécurité est considérée comme une responsabilité partagée entre les parties prenantes de l'ensemble de l'écosystème des soins auditifs, qui incluent, sans s'y limiter, les utilisateurs d'appareils auditifs, les parents ou tuteurs légaux d'enfants qui sont des utilisateurs d'appareils auditifs, les audioprothésistes, les administrateurs informatiques, les établissements et prestataires de soins auditifs, les fournisseurs d'appareils auditifs et d'équipements de programmation.

Voici une liste de recommandations de bonnes pratiques courantes et de contrôles de sécurité pour l'environnement d'appareillage dans lequel le logiciel d'appareillage sera utilisé :

Niveau du système d'exploitation

- Appliquez des contrôles d'accès au niveau du système d'exploitation, par exemple :
 - Supprimez les comptes invités
 - Activez la connexion utilisateur Windows
 - Maintenez une liste d'opérateurs autorisés pour contrôler l'accès au système
 - Définissez des utilisateurs et des rôles personnalisés
 - Appliquez des exigences de mots de passe forts et gardez les informations d'identification secrètes
 - Activer le délai d'expiration des sessions inactives
- Appliquez les contrôles d'audit au niveau du système d'exploitation
- Assurez-vous que le système d'exploitation est à jour
- Assurez-vous que la version du logiciel d'appareillage installée est à jour
- Utilisez une protection antivirus et contre les logiciels malveillants adaptée et à jour
- Veillez à désactiver les fonctions AutoRun et AutoPlay
- Activez la liste blanche des applications

Protection des données

- Veuillez vous assurer qu'aucun des dossiers ou fichiers contenant des données d'application n'est partagé sur le réseau. Les emplacements par défaut des données de l'application sont répertoriés dans le tableau de la section 5.4. Pour vérifier les partages réseau mis à disposition par un ordinateur, accédez à « Gestion de l'ordinateur -> Dossiers partagés -> Partages » dans l'outil Gestion de l'ordinateur de Microsoft ou exécutez la commande PowerShell `Get-WmiObject -class Win32_Share`.

- Lors de l'installation, les droits d'accès au dossier de données de l'application sont configurés conformément à la section 6.1. Les dossiers de données d'application héritent des droits d'accès du dossier parent. La gestion des droits d'accès au dossier parent relève de la responsabilité de l'exploitant du logiciel.
- Chiffrez les données des patients à l'aide d'outils ou de contrôles tiers au niveau du système d'exploitation, en utilisant le chiffrement de disque (par exemple, la fonctionnalité gratuite Microsoft BitLocker) pour protéger toutes les données. Pour les déploiements de Noah, envisagez d'utiliser le chiffrement de la base de données Noah.
- Les supports externes contenant des données exportées à partir du logiciel d'appareillage, y compris les rapports et les journaux, doivent être sécurisés. Lorsqu'elles ne sont plus utilisées, les données doivent être effacées de manière sécurisée et/ou les supports doivent être supprimés de manière sécurisée.
- Utilisez des supports de stockage USB dotés de fonctionnalités de sécurité intégrées, comme des clés USB chiffrées avec clavier intégré.
- Veillez à garantir en permanence la sécurité des données en respectant les bonnes pratiques suivantes :
 - Lors de la transmission de données sur des canaux non sécurisés, veillez à les anonymiser ou à les chiffrer.
 - Protégez les sauvegardes de données non seulement contre la perte de données, mais également contre le vol.
 - Supprimez toutes les données du support de données qui ne sont plus utilisées ou qui doivent être éliminées.
- Les utilisateurs doivent appliquer des procédures et des outils approuvés pour la suppression sécurisée des données stockées sur des supports amovibles, conformément aux réglementations et directives applicables en matière de traitement des informations des patients / données à caractère personnel (PII) / données de santé protégées (PHI).

Infrastructure informatique

Utilisez le logiciel d'appareillage dans un environnement réseau sécurisé protégé contre toute intrusion non autorisée. Il existe de nombreuses techniques efficaces pour isoler et protéger les systèmes d'informations médicales, notamment la mise en œuvre d'une protection par pare-feu, de zones démilitarisées (DMZ), de réseaux locaux virtuels (VLAN) et d'enclaves réseau. Maintenez une connexion réseau active pour recevoir les mises à jour du système d'exploitation.

Niveau physique

- Le poste de travail sur lequel le logiciel d'appareillage est installé doit être physiquement sécurisé de manière à ce qu'il ne soit pas accessible à des personnes non autorisées et à ce que celles-ci ne puissent pas y porter atteinte.
- L'accès aux imprimantes connectées au poste de travail doit être contrôlé.
- L'écran du poste de travail où le logiciel d'appareillage est installé doit être placé de manière à ce que seul l'utilisateur puisse voir ce qui s'affiche à l'écran.

Niveau organisationnel

- Seul le personnel professionnellement formé et entièrement qualifié est autorisé à utiliser le système. Avant d'autoriser quiconque à utiliser le système, il convient de vérifier que la personne a lu et compris parfaitement les instructions d'utilisation fournies avec le logiciel d'appareillage.
- Seul le personnel autorisé à assurer la maintenance et à utiliser le logiciel d'appareillage doit disposer de comptes d'accès à la machine sur laquelle ce logiciel est installé. Les comptes informatiques et de domaine, ainsi que les droits d'accès associés, doivent être vérifiés régulièrement et désactivés si l'accès à la machine n'est plus nécessaire.
- Si vous remarquez une activité suspecte sur vos comptes du logiciel d'appareillage ou une opération inattendue, contactez Advanced Bionics. Reportez-vous à la section 2.1 pour plus d'informations.

Pour plus d'informations sur la responsabilité partagée et pour obtenir une liste plus détaillée des recommandations de bonnes pratiques et des contrôles de sécurité pour l'environnement d'appareillage où le logiciel d'appareillage sera utilisé pour être appliqué à différents niveaux, reportez-vous au :

- au livre blanc de l'EHIMA « Best Practices for Secure Fitting of Hearing Devices », [EHIMAWhitePaper](#)

12. FABRICATION, DÉVELOPPEMENT DE LOGICIELS ET GESTION DE LA SÉCURITÉ

La cybersécurité est prise en compte tout au long du processus de développement logiciel. Le logiciel d'appareillage est développé en conformité avec les normes CEI 62304 et CEI 82304.

Le logiciel d'appareillage est analysé pour détecter la présence de virus et de logiciels malveillants dans le cadre du processus de fabrication.

Les vulnérabilités des composants tiers répertoriés dans la base de données nationale des vulnérabilités (National Vulnerability Database, NVD) du National Institute of Standards and Technology (NIST) sont évaluées et réduites pendant le processus de développement et surveillées une fois que le logiciel d'appareillage a été mis sur le marché.

Gestion de la configuration

AB développe en interne, documente et assure la gestion, dans le cadre d'un contrôle de configuration, de la configuration de référence de chaque version de logiciel d'appareillage de raccords mise en production.

Tous les composants logiciels tiers utilisés par l'application logicielle d'appareillage sont identifiés et répertoriés dans la nomenclature logicielle (SBOM). AB utilise la liste SBOM dans le cadre de la gestion des risques liés à la cybersécurité afin d'évaluer et de surveiller l'exposition aux menaces de cybersécurité et aux vulnérabilités rendues publiques, à l'aide d'outils de détection des vulnérabilités à jour.

Mises à jour de sécurité

AB surveille en permanence les failles de sécurité affectant les logiciels d'appareillage. Cela inclut les vulnérabilités du logiciel d'appareillage et des composants tiers utilisés par l'application du logiciel d'appareillage.

Les vulnérabilités annoncées sont évaluées en fonction de la configuration et de l'utilisation du logiciel d'appareillage.

Si nécessaire, les failles de sécurité peuvent être corrigées par une mise à jour plus générale du logiciel d'appareillage qui intègre des correctifs destinés à des composants spécifiques de la suite logicielle.

Signalement des vulnérabilités

Nous nous engageons à prendre en compte les signalements de vulnérabilités et à améliorer la sécurité de nos produits et services.

Nous vous encourageons à nous signaler toute vulnérabilité présumée ou tout problème de sécurité lié à nos produits ou aux logiciels/infrastructures sous-jacents.

Veuillez lire notre politique de divulgation des vulnérabilités publiée à l'adresse <https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy> et suivre les instructions pour soumettre un rapport.

13. COMPOSANTS LOGICIELS ET NOMENCLATURE

Le logiciel d'appareillage intègre certains composants logiciels commerciaux prêts à l'emploi.

Le tableau suivant énumère tous les SOUP (logiciels de provenance inconnue) distribués avec le logiciel d'appareillage.

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
AForge.NET	Bibliothèque mathématique et multimédia AForge.NET, intégrée à IceLink et LiveSwitch et requise par ces derniers.	AForge.NET	2.2.5.0
Amplifon. Programmer	Composant de la suite logicielle d'Amplifon	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Composant de la suite logicielle d'Amplifon	Amplifon	1.0.4.0
AutoMapper	Automatise le mappage d'objet à objet	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	bibliothèque dédiée aux tests de performance, fournissant des outils permettant de mesurer et de comparer les performances du code	Communauté BenchmarkDotNet	0.13.0.0
Castle.Core	Bibliothèque centrale du projet Castle, proposant des composants tels que la génération dynamique de proxys et des conteneurs d'inversion de contrôle pour les applications .NET.	Projet Castle	4.4.1
Chessie	Une bibliothèque de gestion des erreurs fonctionnelle pour F#	Open Source	0.6.0.0
ciAD Hearingloss Simulator	Bibliothèque de simulateurs de perte auditive pour lecteur multimédia	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Simplifie la lecture, la modification et l'écriture de fichiers Excel sans nécessiter l'installation d'Excel	Communauté ClosedXML	0.95.4.0
CommandLine Parser	Fournit une API claire et concise pour l'analyse des arguments de ligne de commande	Communauté CommandLineParser	2.4.3
Common.Logging	Une abstraction de journalisation portable pour les applications .NET	Communauté Common.Logging	3.4.1.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
CommonService Locator	Fournit une interface commune pour la localisation des services, permettant ainsi aux applications de s'affranchir de conteneurs IoC spécifiques.	Microsoft	2.0.5.0
Credential Management	Le package Credential Management est un wrapper pour l'API de gestion des informations d'identification Windows.	iLya Lozovyy	1.0.2
CSharpAnalytics	Utilisé pour Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78.45418
Deconstructurama.Attributed	Utilisé par les bibliothèques Nephele	Contributeurs de Serilog	3.1.0.0
Suite Developer Express	Une suite complète de contrôles d'interface utilisateur et de bibliothèques destinée aux développeurs .NET, proposant des outils permettant de créer des applications riches en fonctionnalités.	Developer Express Inc	20.2.10.0
DirectShow 2005	Permet d'accéder à la fonctionnalité DirectShow de Microsoft à partir des applications .NET.	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
ExcelNumberFormat	Offre des fonctionnalités permettant d'analyser et de mettre en forme les formats numériques d'Excel	Open Source	1.1.0.0
FM.dll	Ils font partie intégrante de leurs infrastructures de communication en temps réel, telles que LiveSwitch et IceLink	FM (Frozen Mountain)	2.9.32
FSharp.Core	La bibliothèque principale du langage de programmation F#	Microsoft	6.0.322.10402

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Puce FTDI	Un ensemble de pilotes proposé par Future Technology Devices International (FTDI) qui facilite la communication entre les périphériques USB et les applications logicielles.	FTDI	3.02.07
GNOtometrics.Aurical	GNOtometrics.Aurical reconditionné pour Sonova	Natus Medical Incorporated	2.0.1.9
SharedUtilities.dll	fournit des fonctions utilitaires communes et des ressources partagées pour l'ensemble des applications Natus.	Natus Medical Incorporated	1.0.0.0
Hardware.Info	Composant qui recueille et fournit des informations détaillées sur la configuration matérielle d'un système	Open Source	11.1.0.1
Himsa.NLWSMAPI.dll	Une bibliothèque associée au logiciel Noah de HIMSA	HIMSA	2.0.3.0
natus.otometrics.hipro2	Bibliothèques de communication HiPro	Natus Medical Incorporated	2.0.0.4
Iced.dll	facilite les communications en temps réel en permettant la diffusion en continu de contenu audio, vidéo et de données	FM (Frozen Mountain)	1.12.0.0
IceLink	Utilisé pour l'intégration des conférences audio/vidéo WebRTC	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	offre une prise en charge d'Unicode et de la mondialisation pour les applications logicielles	FM (Frozen Mountain)	54.1.0.0
IdentityModel	Bibliothèque cliente OpenID Connect et OAuth 2.0 utilisée par le composant Kona.CommonServices. Authentication pour l'authentification OAuth 2.	Dominick Baier, Brock Allen	6.2.0.0
IMCInterfaces	Bibliothèque d'interfaces de communication intermodules Noah	HIMSA II K/S	4.4.0.2266
iText 7	Bibliothèque PDF permettant de créer, de modifier et de consulter des documents PDF par programmation.	Logiciel iText	7.1.16.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
JetBrains. dotMemory	Un outil d'analyse de la mémoire permettant de détecter les fuites de mémoire et d'optimiser l'utilisation de la mémoire dans les applications .NET	JetBrains	111.0.0.0
JsonDiffPatch DotNet.dll	Offre des fonctionnalités permettant de comparer et de corriger des objets JSON	Open Source	1.0.1.0
LibGit2Sharp	Utilisé par les bibliothèques provenant de Sonova pour communiquer avec les contributeurs	Contributeurs de LibGit2Sharp	0.26.1.93
LiveSwitch	Utilisé pour l'intégration des conférences audio/vidéo WebRTC.	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	framework de journalisation pour .NET	Apache	4.7.0.3189
Mapster	Utilisé pour mapper des objets dans le code	chaowlert,eric_swann	7.2.0.0
Mapster.Core	Utilisé pour mapper des objets dans le code	chaowlert,eric_swann	1.2.0.0
MathNet.Numerics	Utilisé pour les algorithmes de l'appareillage (chemin du signal, outil de correspondance de cible, etc.)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael et contributeurs	4.11.0
Microsoft.Bcl. AsyncInterfaces	Fournit les interfaces <code>IAsyncEnumerable<T></code> et <code>IAsyncDisposable</code> et les types d'assistance pour .NET Standard 2.0.	Microsoft	6.0.21.52210
Microsoft. CodeAnalysis. Common	Utilisé par les bibliothèques provenant de Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft. CodeAnalysis. CSharp	Utilisé par les bibliothèques provenant de Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Permet la compilation et la génération de code en C#	Microsoft	4.700.19.56404
Microsoft. Diagnostics. FastSerialization.dl	Utilisé pour la sérialisation et la désérialisation efficaces des données de diagnostic	Microsoft	1.0.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Microsoft. Diagnostics. NETCore.Client.dll	Une bibliothèque gérée qui permet d'interagir avec le runtime .NET Core pour diverses tâches de diagnostic, telles que le traçage et la demande de vidages mémoire.	Microsoft	0.2.4.27602
Microsoft. Diagnostics. Runtime.dll	fournit des API permettant d'analyser les processus en cours d'exécution et les fichiers de vidage mémoire, ce qui permet aux développeurs de créer des outils de débogage et de diagnostic.	Microsoft	2.0.4.26801
Microsoft. Diagnostics.Tracing. TraceEvent.dll	Une bibliothèque permettant d'analyser et de traiter les événements ETW (Event Tracing for Windows)	Microsoft	2.0.70
Microsoft. DotNet.Platform Abstractions.dll	Fournit des API permettant d'accéder à des informations sur la plateforme .NET	Microsoft	3.100.620.31604
Microsoft. Extensions. Dépendance Injection. Abstractions	Définit les abstractions pour l'injection de dépendances dans les applications .NET	Microsoft	6.0.21.52210
Microsoft. Extensions.Logging	Permet la mise en place d'une journalisation structurée dans les applications .NET.	Microsoft	6.0.21.52210
Microsoft. Extensions.Options	Permet de configurer les options dans les applications .NET	Microsoft	6.0.21.52210
Microsoft. Extensions. Primitives	Fournit des interfaces et des classes pour le suivi des modifications et les jetons d'annulation, facilitant ainsi la gestion des données modifiables et le nettoyage des ressources.	Microsoft	6.0.21.52210
Microsoft.Identity. Client	La bibliothèque MSAL pour .NET fait partie de la plateforme d'identité Microsoft pour développeurs (anciennement Azure AD) v2.0. Elle permet d'acquérir des jetons de sécurité pour appeler des API protégées. Elle utilise les normes industrielles OAuth2 et OpenID Connect.	Microsoft	4.38.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Microsoft.Identity.Client.Extensions.Msal	Cache de jetons multiplateforme sécurisé pour les applications client publiques MSAL	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Inclut des types qui fournissent une prise en charge pour la création, la sérialisation et la validation des Web JSON Tokens. Utilisé par les composants qui communiquent avec les services dorsaux qui utilisent des Web JSON Tokens pour l'authentification.	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Logging	Dépendance de Microsoft.IdentityModel.Tokens	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Tokens	Dépendance de la bibliothèque SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0.11012
Microsoft.ML.OnnxRuntime	Un moteur d'inférence permettant d'exécuter des modèles d'apprentissage automatique au format ONNX (Open Neural Network Exchange)	Microsoft	1.12.1
Microsoft.ML.OnnxRuntime.Managed	Le wrapper .NET géré pour ONNX Runtime	Microsoft	1.12.1
Microsoft.Office.Interop.Excel.dll	Faisant partie des assemblages Office Interop, cette DLL permet aux applications .NET d'interagir avec Microsoft Excel	Microsoft	14.0.4733.1000
Microsoft.VisualStudio.TextTemplating.10.0	Offre des fonctionnalités de création de modèles de texte au sein de Visual Studio, permettant aux développeurs de générer du code et d'autres éléments textuels à l'aide de modèles T4.	Microsoft	10.0.40219.1
Microsoft.Win32.Registry.dll	Permet d'accéder au registre Windows	Microsoft	5.0.20.51904
Microsoft.Win32.SystemEvents.dll	Prend en charge la gestion des événements système dans les applications .NET	Microsoft	8.0.23.53103
Microsoft.Win32.TaskScheduler.dll	Utilisé pour l'outil de sauvegarde du FSW (sauvegardes automatisées)	David Hall	2.5.11.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Microsoft.Xaml.Behaviors.Wpf	Les comportements XAML sont un moyen simple à utiliser d'ajouter une interactivité commune et réutilisable à vos applications WPF avec un minimum de code.	xamlexperienceteam, Microsoft	1.0.1.0
Kit de développement logiciel Microsoft DIA	Fournit des API permettant de manipuler les informations de débogage contenues dans les fichiers PDB	Microsoft	2.0.0.0
MS VC++ 2008 Redistribuable	Microsoft Visual C++ 2008 Redistribuable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistribuable	Microsoft Visual C++ 2010 Redistribuable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistribuable	Microsoft Visual C++ 2012 Redistribuable	Microsoft	11.0.51106.1
Microsoft Visual C++ 2017 Redistribuable (x86)	Microsoft Visual C++ 2017 Redistribuable	Microsoft	14.16.27024.1
Mono.Cecil	Permet d'inspecter, de modifier et de créer des assemblages .NET	Microsoft	0.11.3.0
Moq.dll	Bibliothèque .NET open source permettant de créer des objets fictifs lors des tests unitaires	Communauté Moq (Open Source)	4.16.1.0
MS-VisualC++ 7.1 runtime libraries	Bibliothèques d'exécution Microsoft Visual C++	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	Utilisé pour régler les volumes et lire des fichiers sonores	Open Source	1.9.0.0
.NET Framework	Cadriciel d'exécution .NET Framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Utilisé pour la sérialisation et la désérialisation JSON.	James Newton-King	13.0.3.27908
Newtonsoft.Json.Schema.dll	Une bibliothèque de validation de schémas pour les données JSON	James Newton-King	3.0.14.25421
Nibelung	Bibliothèques d'appareillage NoahLink Wireless	HIMSA	1.3.16.1
Nibelung2.CPD	Bibliothèques d'appareillage NoahLink Wireless	HIMSA	2.0.3.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Nlog	Il s'agit d'une dépendance de Nibelung.CPD (Noahlink Wireless) de HIMSA.	Kim Christensen	5.0.4.1331
Noahlink	Pilote de périphérique d'appareillage Noahlink	HIMSA	1.55.6.166
Pilote Noahlink Wireless	Pilote de périphérique d'appareillage Noahlink Wireless	HIMSA	1.1.0.0
Outil de mise à jour Noahlink Wireless	Outil de mise à jour du micrologiciel Noahlink Wireless	HIMSA	3.1.0.82
ModuleAPI.dll (Système Noah)	Un composant du système Noah de HIMSA, fournissant des API pour l'intégration et la gestion des données audiologiques	HIMSA	4.13.0.5404
Kit de développement logiciel NiXPS	Offre des fonctionnalités permettant de gérer les documents XPS (XML Paper Specification)	NiXPS NV	2.6.0.0
NPOI	Une bibliothèque open source qui facilite la lecture et l'écriture de documents Microsoft Office dans les applications .NET	NPOI communi	2.4.1.0
Gestionnaire de packages NuGet	Un outil de gestion des bibliothèques et des packages .NET	Microsoft	6.3.0.131
Nunit	Un framework de tests unitaires pour les applications .NET	Projet NUnit	3.12.0.0
Exécution ONNX	Moteur pour les modèles ONNX (Open Neural Network Exchange)	Microsoft	1.12.20220803.2.7048164
Kit de développement logiciel Open XML	Fournit des outils permettant de travailler avec des documents Office Open XML	Microsoft	2.7.2

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
OSExtensions.dll	bibliothèque proposant des extensions pour les fonctionnalités du système d'exploitation	Microsoft	1.0.0.0
Otometrics. REMaccess	Couche d'abstraction d'Otometrics au-dessus de la bibliothèque d'interface de communication intermodules Noah	GN Otometrics	1.0.0.10
Paket.Core.dll	Un gestionnaire de dépendances open source pour les projets .NET et Mono	Communauté Paket (Open Source)	7.1.5.0
Patagames.Pdf	La bibliothèque PDF C# permettant de créer et de modifier des documents PDF dans les applications .Net.	patagames.com	8.57.30.48
Patagames.Pdf. Wpf	La bibliothèque PDF C# permettant de créer et de modifier des documents PDF dans les applications .Net.	Patagames.com	4.19.18.48
Polly	Bibliothèque qui permet aux développeurs d'exprimer des politiques de résilience et de gestion des fautes transitoires, telles que Retry, Circuit Breaker, Bulkhead Isolation et Fallback, de manière fluide et thread-safe	App vNext	7.2.3.0
Portable. BouncyCastle	Il s'agit d'une dépendance de Nibelung. CPD (Noahlink Wireless) de HIMSA.	The Legion of the Bouncy Castle Inc	1.8.15362.1

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Portable. BouncyCastle. Crypto	Il s'agit d'une dépendance de Nibelung. CPD (Noahlink Wireless) de HIMSA.	The Legion of the Bouncy Castle Inc	1.9.0.1
protobuf-net.dll	Cadre de sérialisation utilisé pour le blob RC	Open Source	2.3.2.0
Google.Protobuf	Bibliothèque officielle Protocol Buffers de Google pour .NET, facilitant la sérialisation et la désérialisation de données structurées.	Google Inc	3.19.3.0
Perfolizer.dll	Une bibliothèque open source dédiée à l'analyse des performances	Open Source	0.2.1.0
Rhino.Mocks.dll	Un framework dynamique d'objets fictifs pour .NET	Communauté Rhino Mocks	3.6.0.0
Security. Cryptography. NetCore.dll	fournit des fonctionnalités cryptographiques pour les applications .NET Core	HardDev	1.0.1.0
Serilog	Composant de journalisation utilisé pour l'ensemble de l'application Chinook	Contributeurs de Serilog	3.0.1.0
Serilog. Enrichers.Thread	Enrichit les événements Serilog avec les propriétés du thread courant.	Contributeurs de Serilog	3.1.0.0
Serilog. Extensions. Logging	Intègre Serilog aux abstractions de journalisation de Microsoft	Contributeurs de Serilog	3.1.0.0
Serilog. Expressions	Filtrage d'événements basés sur des expressions pour Serilog	Contributeurs de Serilog	2.0.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Serilog.Sinks.Console	Récepteur Serilog qui écrit les événements du journal dans la console/ le terminal	Contributeurs de Serilog	4.0.0.0
Serilog.Sinks.Debug	Récepteur Serilog qui écrit les événements du journal dans la fenêtre de sortie de débogage	Contributeurs de Serilog	2.0.0.0
Serilog.Sinks.File	Écrit les événements Serilog dans des fichiers texte au format brut ou JSON.	Contributeurs de Serilog	4.1.0.0
Serilog.Sinks.NUnit.dll	S'intègre à NUnit, en redirigeant les événements de journalisation vers la sortie de test de NUnit, ce qui facilite le diagnostic des tests.	Contributeurs de Serilog	1.0.3.0
Serilog.Sinks.Trace	Récepteur de trace de diagnostic pour Serilog	Contributeurs de Serilog	2.1.0.0
Serilog.Settings.AppSettings	Prise en charge de la configuration XML (System.Configuration <appSettings>) pour Serilog.	Contributeurs de Serilog	2.2.2.0
Security.Cryptography.NetCore.dll	Extensions des API de sécurité fournies avec .NET Framework	Microsoft	1.0.1.0
SharpBITS API	SharpBITS.NET est un wrapper .NET de l'API BITS et une petite application d'interface utilisateur Windows pour un accès plus facile aux téléchargements et téléversements avec BITS.	perpetualKid	2.1.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
SharpZipLib	#zipLib (SharpZipLib, anciennement NzipLib) est une bibliothèque Zip, Gzip, Tar et Bzip2 entièrement écrite en C# pour la plateforme .NET. Cette bibliothèque fournit des fonctionnalités de compression (compression, décompression, compression de flux, etc.). Nous l'utilisons dans l'application de mise à jour du micrologiciel.	Open Source	1.3.3.11
SharpDX	Utilisé par LiveSwitch : SharpDX.Direct3D11, SharpDX.Direct2D1, SharpDX.Mathematics	Alexandre Mutel	4.0.1
Client SocketIO	Fournit un client pour Socket.IO, permettant une communication bidirectionnelle en temps réel basée sur les événements dans les applications .NET	HeroWong	2.2.4.0
Superpower	Bibliothèque de combinateurs d'analyseurs pour C#	Datalust, contributeurs de Superpower, contributeurs de Sprache	2.3.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
SQLite.Interop	Bibliothèque d'interopérabilité native SQLite 3.36.0. SQLite est la base de données intégrée utilisée pour stocker des informations sur le patient (en mode autonome), nos ressources de catalogue de produits et les métadonnées pour l'appareillage, les accessoires et les appareils auditifs. SQLite est dans le domaine public.	Équipe de développement SQLite	1.0.115
System Buffers	Fournit un regroupement de ressources de tout type pour les applications critiques en matière de performances qui affectent et désaffectent fréquemment des objets.	microsoft, dotnetframework	4.6.28619.01
System.Collections.Immutable	Utilisé par les bibliothèques provenant de Sonova. HardwareAbstraction. Palio.Trafo	Microsoft	7.0.22.51805
Système. Composant Modèle. Annotations	Fournit des attributs utilisés pour définir les métadonnées des objets utilisés comme sources de données.	microsoft, dotnetframework	4.6.26515.06
Système. Configuration. Configuration Manager	Fournit des types qui prennent en charge l'utilisation de fichiers de configuration.	Microsoft	5.0.20.51904

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.CodeDom.dll	Fournit des classes permettant de générer et de compiler du code source en fichiers exécutables ou en assemblages	Microsoft	8.0.23.53103
System.Data.SQLite	Utilisé par les bibliothèques provenant de Sonova. HardwareAbstraction. Palio.Trafo	Équipe de développement SQLite	1.0.115.0
Système.Diagnostics.DiagnosticSource	Une bibliothèque de journalisation qui permet aux développeurs de suivre et de surveiller les données de diagnostic	Microsoft	6.0.21.52210
Système.Diagnostics.Performance Counter	Fournit des API permettant d'interagir avec les compteurs de performances Windows	Microsoft	7.0.22.51805
System.Drawing.Common	Donne accès aux fonctionnalités graphiques de GDI+.	Microsoft	8.0.324.11603
System.Formats.Asn1.dll	Prend en charge l'encodage et le décodage des données au format ASN.1 (Abstract Syntax Notation One)	Microsoft	6.0.21.52210

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.IdentityModel.Tokens.Jwt	Inclut des types qui fournissent une prise en charge pour la création, la sérialisation et la validation des Web JSON Tokens. Utilisé par les composants qui communiquent avec les services dorsaux qui utilisent des Web JSON Tokens pour l'authentification.	Microsoft	6.8.0.11012
System.IO.Abstractions	Ensemble d'abstractions pour aider à rendre les interactions du système de fichiers testables	Tatham Oddie & friends	12.0.10.46693
System.IO.Hashing.dll	Fournit des fonctionnalités de hachage dans .NET, notamment des algorithmes permettant de calculer des sommes de contrôle et des hachages cryptographiques.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Permet la lecture et l'écriture de fichiers de packages	Microsoft	6.0.21.52210
System.IO.Ports.dll	Fournit des classes pour la communication via les ports série, permettant ainsi aux applications .NET d'interagir avec du matériel connecté via ces ports.	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	Un gestionnaire HTTP spécialisé pour Windows	Microsoft	6.0.422.16404

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.Numerics.Vectors	Fournit des types numériques accélérés par le matériel, adaptés aux applications de traitement et graphiques hautes performances.	microsoft, dotnetframework	4.6.26515.06
System.Memory	Fournit des types pour une représentation et un regroupement efficaces des segments de mémoire gérée, de pile et native et des séquences de ces segments, ainsi que des primitives pour analyser et formater le texte codé en UTF-8 stocké dans ces segments de mémoire.	microsoft, dotnetframework	4.6.31308.01
System.Reactive.dll		Open Source	5.0.0.1
System.Reflection.DispatchProxy	Fournit une classe pour créer dynamiquement des types de proxy qui implémentent une interface spécifiée et dérivent d'un type DispatchProxy spécifié. Les invocations de méthode sur l'instance de proxy générée sont envoyées à ce type de base DispatchProxy.	Microsoft	4.700.20.21406

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.Reflection.Metadata	Ces ensembles fournissent un lecteur et un rédacteur de métadonnées .NET (ECMA-335) de bas niveau. Il est conçu pour les performances et constitue le choix idéal pour créer des bibliothèques de niveau supérieur qui visent à fournir leur propre modèle d'objet, comme des compilateurs.	Microsoft	5.0.20.51904
System.Reflection.TypeExtensions	Fournit des méthodes d'extension pour l'API de réflexion	Microsoft	4.700.19.56404
System.Runtime.CompilerServices.Unsafe	Fournit l'interface System.Runtime.CompilerServices.Unsafe, qui fournit des fonctionnalités génériques de bas niveau pour la manipulation de pointeurs.	microsoft, dotnetframework	6.0.21.52210
System.Security.AccessControl	Fournit des classes de base qui permettent de gérer les listes de contrôle d'accès et d'audit sur les objets sécurisables.	Microsoft	6.0.21.52210
System.Security.Permissions	Fournit des types prenant en charge la sécurité d'accès au code (CAS).	Microsoft	5.0.20.51904
System.Security.Principal.Windows	Fournit des classes permettant de récupérer l'utilisateur Windows actuel et d'interagir avec les utilisateurs et les groupes Windows.	Microsoft	5.0.20.51904

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.Security.Cryptography.Cng.dll	Fournit des fonctionnalités cryptographiques à l'aide des API Cryptography Next Generation (CNG)	Microsoft	5.0.20.51904
System.Security.Cryptography.Pkcs.dll	Propose des cours sur l'utilisation des normes de cryptographie à clé publique (PKCS), notamment les données signées et encapsulées	Microsoft	6.0.1923.31806
System.Security.Cryptography.ProtectedData.dll	Fournit des méthodes permettant de protéger et de déprotéger des données, en utilisant l'API de protection des données de Windows (DPAPI) pour un stockage sécurisé des données.	Microsoft	6.0.21.52210
System.Security.Cryptography.Xml.dll	Active le chiffrement XML et les signatures numériques, permettant ainsi un traitement sécurisé des données XML dans les applications .NET.	Microsoft	6.0.822.36306
System.ServiceModel.Http.dll	Fournit des fonctionnalités de communication HTTP pour les services Windows Communication Foundation (WCF)	Microsoft	4.700.19.56502
System.ServiceModel.Primitives.dll	Contient les classes fondamentales pour les services WCF, notamment les classes de base et les interfaces pour les contrats de service et les canaux.	Microsoft	4.700.19.56502

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.Text.Encoding.CodePages	Fournit une prise en charge des codages basés sur les pages de codes, notamment Windows-1252, Shift-JIS et GB2312.	Microsoft	5.0.20.51904
System.Text.Encodings.Web	Fournit des types pour l'encodage et l'échappement des chaînes à utiliser en JavaScript, en langage hypertexte (HTML) et dans les URL. Est une dépendance du SOUP IdentityModel	microsoft, dotnetframework	6.0.21.52210
System.Text.Json	Fournit des types hautes performances et à faible allocation qui sérialisent les objets en texte JSON (JavaScript Object Notation) et désérialisent le texte JSON en objets, avec prise en charge UTF-8 intégrée. Fournit également des types pour lire et écrire du texte JSON encodé en UTF-8 et pour créer un DOM (Document Object Model) en mémoire, en lecture seule, pour un accès aléatoire aux éléments JSON dans une vue structurée des données.	Microsoft	6.0.222.6406
System.Threading.Tasks.Extensions	Fournit des types supplémentaires qui simplifient le travail d'écriture de code concurrent et asynchrone.	microsoft, dotnetframework	4.6.28619.01

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
System.Threading.Channels	Fournit un ensemble de structures de données de synchronisation permettant le transfert de données entre producteurs et consommateurs, et facilitant la programmation parallèle haute performance.	Microsoft	6.0.21.52210
System.ValueTuple	Fournit les structures System.ValueTuple, qui implémentent les types sous-jacents des tuples dans C# et Visual Basic. Ajoute la prise en charge des tuples de valeur, car ils ne sont inclus que dans les versions ultérieures de .NET Framework.	microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy.dll	Un cadre de développement piloté par le comportement (BDD) pour .NET	Communauté TestStack	4.3.2.0
Thrift	Utilisé pour la définition du protocole de liaison à distance	Apache	0.13.0.0
Unity.Container	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	5.8.13.0
Unity.Configuration	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	5.2.5.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Unity. Abstractions	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	3.3.1.0
Unity. Interception. Configuration	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	5.1.7.0
Unity. Interception	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	5.5.5.0
Unity. Registration ByConvention	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	2.1.9.0
Unity. ServiceLocation	Le conteneur Unity (Unity) est un conteneur d'injection de dépendances complet et extensible.	Unity Container Project	2.1.2.0
WAP BT Dongle Driver	Pilote de dongle WAP BT (dongue d'appareillage)	iAnywhere Solutions	3.0.0.6095
WebSync	Utilisé pour l'intégration du canal de données d'appareillage	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor.dll	Un contrôle d'éditeur hexadécimal pour les applications WPF	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	Une bibliothèque d'utilitaires pour les applications WPF qui fournit des informations sur l'écran et le moniteur	FM (Frozen Mountain)	2.1.0.0

ÉLÉMENT SOUP	DESCRIPTION DES FONCTIONNALITÉS	FABRICANT	VERSION
Kit d'outils WPF étendu Xceed	Une collection de contrôles et d'utilitaires WPF qui enrichissent les applications WPF grâce à des composants d'interface utilisateur supplémentaires.	Xceed	3.5.0.0
xmlunit-core.dll	Une bibliothèque permettant de tester et de comparer des sorties XML.	Communauté XMLUnit	2.9.0.205
Xps to Pdf render (NiXPS)	Convertit des fichiers XPS de manière programmatique en PDF ; utilisé dans les rapports d'application d'appareillage.	NiXPS	2.6.7.0

14. RÉFÉRENCES

Titre	Site Web
Instructions d'utilisation (électroniques)	https://ifu.advancedbionics.com/
Politique de confidentialité mondiale d'Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Backing up and restoring the data in your Noah database	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Noah System Database Capacity has been Reached.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
Ports et URL utilisés par TeamViewer	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
Documentation sur la sécurité du serveur LiveSwitch	https://developer.liveswitch.io/liveswitch-server/server/security.html
Best Practices for Secure Fitting of Hearing Devices EHIMA whitepaper	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA_Cybersecurity-FSW-Security-Whitepaper_v1-Sep2021.pdf

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

info.us@advancedbionics.com

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

info.switzerland@advancedbionics.com

Pour plus d'informations sur les autres filiales AB, consultez le site
advancedbionics.com/contact

AB – Une marque Sonova

Veuillez contacter votre représentant AB pour vérifier l'autorisation
réglementaire et la disponibilité dans votre région.

Le nom de marque et les logos Bluetooth® sont des marques déposées
appartenant à Bluetooth SIG, Inc. et toute utilisation de ces marques
par Sonova AG est faite sous licence.



029-S398-04