Best Practices for Secure Fitting of Hearing Devices

EHIMA Whitepaper

Revision: 1.0

Date: 3.9.2021

Abstract:

The EHIMA Cybersecurity Working Group has created this whitepaper to facilitate security through collaboration with key stakeholders in the hearing care ecosystem with special focus on hearing device fitting. The aim of this whitepaper is to educate and inform the target audience by providing best practice recommendations and security controls to enable secure fitting of hearing devices and to strengthen security and resilience of the entire hearing care ecosystem.

EHIMA, European Hearing Instrument Manufacturers Association AISBL
www.ehima.com

Revision History

Revision Number	Date	Comments
1.0	03.9.2021	Initial release
1.0	13.09.2021	Approved by EHIMA Technical Committee

Contributors

Name	Company
Alexander Maksyagin	Sonova Holding AG
Allan Munk Vendelbo	GN Hearing A/S
Joe Honnold	Starkey
Klaus Härtl	WS Audiology A/S
Nadica Hrgarek Lechner	MED-EL Elektromedizinische Geräte GmbH
Thomas Krohn	Demant A/S

1 Introduction

Traditionally, hearing device fittings were conducted using the fitting systems in a non-Internet connected environment. Using remote connectivity, wireless communication, connections to cloud services, and other networking capabilities, attention has turned to the cybersecurity of medical devices which also include hearing devices. In context of the hearing care ecosystem, cybersecurity addresses safety risks associated with hearing device fitting as well as protection of any sensitive information used within the ecosystem.

The EHIMA Cybersecurity Working Group fully acknowledges the security implications of the hearing devices across the entire hearing care ecosystem and has created this whitepaper to facilitate security through collaboration with key stakeholders. Key stakeholders in the hearing care ecosystem include, but are not limited to, hearing device users, Hearing Care Professionals (HCPs), Information Technology (IT) personnel providing technical assistance to HCPs, Hearing Care Delivery Organizations (HCDOs), as well as vendors of hearing devices and programming equipment.

1.1 Purpose

The purpose of this whitepaper is to provide best practice recommendations and security controls to enable secure fitting of hearing devices and to strengthen security, data integrity and resilience of the hearing care ecosystem.

1.2 Scope

This whitepaper focuses on hearing devices (e.g., hearing aids, hearing implants, bone conduction systems) and associated fitting systems that are needed to conduct a hearing device fitting.

2 References

ANSI/NEMA HN 1-2019, American National Standard – Manufacturer Disclosure Statement for Medical Device Security

ANSI/UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

IEC TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the communication of medical device security needs, risks and controls

IMDRF, Principles and Practices for Medical Device Cybersecurity, 2020

ISO 21388:2020, Acoustics – Hearing aid fitting management (HAFM)

ISO 27002:2013, Information technology – Security techniques – Code of practice for information security controls

ISO 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

NIST SP 800-121 Rev. 2, Guide to Bluetooth Security, 2017

NIST SP 800-53 Rev. 4[1], Security and Privacy Controls for Federal Information Systems and Organizations

NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management

U.S. FDA, Postmarket Management of Cybersecurity in Medical Devices, 2016

[1] This publication was superseded by SP 800-53 Rev. 5 on September 23, 2020. Revision 4 will be officially withdrawn on September 23, 2021.

3 Definitions

3.1 Acronyms

Acronym	Definition
2FA	Two-Factor Authentication
AD	Active Directory
CISA	Cybersecurity and Infrastructure Security Agency
DMZ	Demilitarized Zone
FA	Fitting Authorization
FDA	Food and Drug Administration
HCDO	Hearing Care Delivery Organization
HCP	Hearing Care Professional
HD	Hearing Device
IMDRF	International Medical Device Regulators Forum
ISO	International Organization for Standardization
MDS2	Manufacturer Disclosure Statement for Medical Device Security
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
PC	Personal Computer
PHI	Protected Health Information
PII	Personally Identifiable Information
SLA	Service Level Agreement
VLAN	Virtual Local Area Network

Table 1 Acronyms

3.2 Roles

Role	Definition
HCP	A person who is appropriately trained and has proven competency in professionally assessing hearing, fitting, and delivering hearing devices and rehabilitation services to individuals with hearing loss [Source adapted: ISO 21388]. This person is authorized to fit hearing devices, particularly to modify safety-related configuration settings.
Hearing device user	An individual who wears a hearing device.
IT administrator	A system administrator or other employee from the IT department supporting an HCP by installing and/or configuring the fitting software. In smaller organizations, this role can be performed by HCP.
Vendor	A manufacturer, reseller, or supplier of a hearing device, that shares responsibility with other stakeholders for the cybersecurity of that product towards the purchaser and/or hearing device user. [Source adapted: ANSI/UL 2900-1]

Table 2 Involved roles

3.3 Other Definitions

Term	Definition
Authentication	The process of verifying the identity of an entity. [Source: ANSI/UL 2900-1]
Bluetooth	A technology which permits a hearing device to communicate wirelessly with other compatible devices.

Term	Definition
Endpoint security	Refers to protecting endpoints such as PCs, laptops, and mobile devices which can be connected to a network.
Cryptography	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [Source: ISO 7498-2] The purpose of cryptography is to provide confidentiality, integrity, non-repudiation, and authentication of stored and transmitted information.
Fitting authorization	The process of giving an entity permission to access or manipulate fitting settings. [Source adapted: ANSI/UL 2900-1]
Fitting environment	Physical and technical environment that is needed for hearing device fitting. A facility for hearing device fitting shall be sufficiently private so that no other person within the facility can overhear conversations taking place. [Source adapted: ISO 21388]
Fitting system	Set of devices typically comprising a personal computer or a mobile device, fitting software, and a programming interface used to adjust hearing devices. [Source adapted: ISO 21388]
Hearing care ecosystem	An interconnected system of people, components (e.g., hearing devices, wireless accessories, fitting systems, cloud services, apps for hearing device users, patient management systems, etc.), and interfaces between the components that are necessary for providing hearing care.
Hearing device	Any implantable and non-implantable device that is designed to improve, treat, or restore hearing of an individual with hearing loss. For example: hearing aids, hearing implants, bone conduction systems, etc.
Hearing device fitting	A systematic procedure for individualizing and optimizing configuration settings of a hearing device to fit hearing preferences of an individual with hearing loss. The procedure is typically performed by an HCP. [Source adapted: ISO 21388]
Hearing device programming interface	A hardware interface designed to program hearing devices. For example: HI-PRO 2, NOAHlink[2], Noahlink Wireless, or any other programming interface provided by the hearing device vendor.
Local fitting	Fitting which is performed in a facility where an HCP and a hearing device user are both physically present.
Remote fitting	When participating in a remote fitting both the hearing device user and HCP are connecting to each other via a secure Internet connection. During the remote fitting, the HCP and hearing device user are typically not at the same physical location. The hearing device user's mobile device is directly connected to the HDs (for example, via Bluetooth), which play the role of the programming interface.
Security dongle	A roaming, hardened physical device that contains a unique, verifiable digital identity and can be used as an authenticator.
Service and repair	Personnel who perform servicing and/or maintenance of hearing devices.
Wireless fitting	Fitting that is performed via a wireless interface that uses electromagnetic waves over the air, rather than some form of wire, to carry communication signals to and from a hearing device.

Table 3 Other terms

[2] NOAHlink is no longer available for purchase as of February 2021.

4 Shared Responsibility

Cybersecurity risk management is a shared responsibility among stakeholders[3] across the entire hearing care ecosystem (Figure 1). Key stakeholders include, but are not limited to, hearing device users, parents or legal guardians of children who are hearing device users, HCPs, IT administrators, hearing care facilities and providers, vendors of hearing devices and programming equipment. Security of a hearing device fitting can be ensured only if the fitting system and the fitting environment in which the fitting software is installed and used are protected by appropriate technical, physical[4], and administrative[5] safeguards. Therefore, cybersecurity is always a shared responsibility between an HCDO and vendors which manufacture and supply hearing devices, fitting software, and other components of the fitting system.

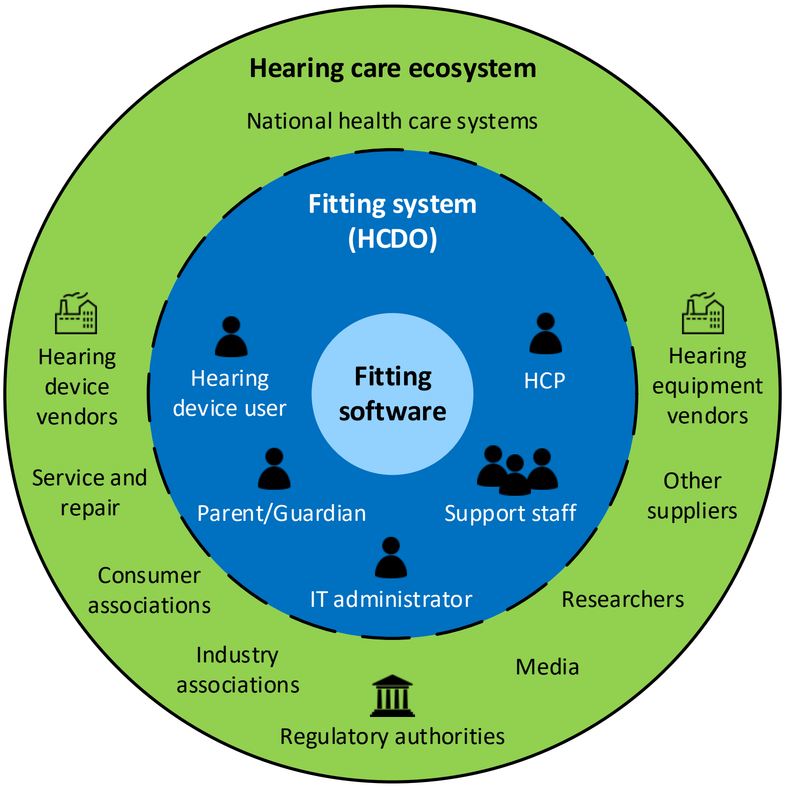

Figure 1 Stakeholder map

While a hearing device vendor is responsible for adopting cybersecurity industry standards and best practices and incorporating technical safeguards into fitting system components that it manufactures, the HCDO operating a fitting system is ultimately responsible for providing effective overall cybersecurity risk management within their environment. This responsibility includes, but is

[3] Source: U.S. FDA, Postmarket Management of Cybersecurity in Medical Devices

[4] Examples may include facility access controls to ensure only authorized personnel have access, security seals for computer ports and servers, PC security measures to guard against theft and restrict access to authorized users, PC use policies to ensure proper access to and use of PCs.

[5] Examples may include staff training, access control administration tasks performed by an IT administrator to manage user accounts, access, and accountability, information access management to limit access to electronic health records containing PHI, contingency plans to respond to emergencies or restore lost data.

not limited to, conducting a cybersecurity risk assessment for the fitting system in its operational context but also putting into place additional technical, physical, and administrative safeguards to mitigate any remaining, unacceptable risks. The HCDO shall consider additional security controls recommended by the vendor and follow closely the vendor's instructions on secure deployment, installation, operation, maintenance, and decommissioning of the fitting system or its individual components.

A high-level overview of responsibilities within the hearing care ecosystem for security of a local fitting is shown in the table below.

Responsibility area		**HD vendor**	**HCDO**	
			HCP	**IT administrator**
Fitting environment	Physical security		x	
	Security of network infrastructure			x
Fitting system	Endpoint security			x
	Identity and access management			x
	Fitting software	x		
	Hearing device programming interface (e.g., Noahlink Wireless)	x		
	Hearing devices	x		

Table 4 Shared responsibility model for local fitting

A remote fitting typically utilizes cloud services to provide a communication channel between HCP and a hearing device user as well as a remote connection between fitting software and hearing devices. Although cloud services are typically hosted by a 3rd-party cloud service provider, the hearing device vendor is ultimately responsible for their product security. This responsibility includes careful selection of a cloud service provider which can ensure the required security level and entering into an SLA between the hearing device vendor and the cloud service provider.

The hearing device vendor and the HCDO must co-operate to ensure that only authorized users have access to the cloud services. The hearing device vendor implements technical safeguards to restrict the access and provides a service for managing user identities and their access rights (or integrates with an existing one). The HCDO puts effective identity and access management policies and process in place. The HDCO is responsible for their implementation.

Hearing device users also play an important role in ensuring security of the remote fitting. They are responsible for secure use of their hearing devices and mobile devices connected to the hearing devices.

A high-level overview of responsibilities within the hearing care ecosystem for security of a remote fitting is shown in the table below.

Responsibility area			HD vendor	HCDO		HD user
				HCP	IT administrator	
Fitting environment	HCDO facilities	Physical security		x		
		Security of network infrastructure	x		x	
Fitting system	Cloud service provider facilities	Cloud services	x			
		Identity and access management	x		x	
	HCDO facilities	Endpoint security			x	
		Hearing device programming interface (e.g., Noahlink Wireless)	x			
		Fitting software	x			
	HD users' site	Mobile device				x
		Hearing devices				x

Table 5 Shared responsibility model for remote fitting

The following two chapters provide best practice recommendations by the EHIMA Cybersecurity Working Group to hearing device vendors and HCDOs on how they can fulfill some of their responsibilities in ensuring hearing device fitting safety and security. Chapter 5 contains recommendations to HCDOs on securing their fitting environment. Chapter 6 describes mechanisms for fitting authorization and HCP authentication which are recommended for implementation in a fitting system to hearing device vendors.

Note that the recommendations provided in this whitepaper do not constitute a complete set of safeguards necessary for ensuring safety and security of hearing device fitting in the specific context. In each individual case, hearing device vendors and HCDOs shall conduct cybersecurity risk assessments to identify the risks and determine appropriate measures to control them.

5 Best Practice Recommendations and Security Controls for the Fitting Environment

To ensure secure fitting of hearing devices in an environment where hearing care is provided, HCDOs should consider, at minimum, adopting and implementing best practice recommendations and security controls listed in this whitepaper.

5.1 User-related Recommendations

Table 6 provides an overview of user-related security recommendations for the operating environment in which hearing device fitting is performed. The recommendations are divided into several categories.

Category	Best Practice Recommendations
Security guides	• Follow the operating instructions and any available product security documentation provided by the vendor. Pay special attention to the environment in which the fitting software is intended to be used and the security recommendations provided by the vendor. • Request from the vendor a MDS2 form[6] (refer to ANSI/NEMA HN 1-2019) for the fitting software and the associated equipment and services. This standardized form consists of 216 questions that cover 23 different categories of medical device security capabilities. The questions in MDS2 form have been mapped with corresponding sections of IEC TR 80001-2-2, NIST SP 800-53 Rev. 4, and ISO 27002. MDS2 form is intended to supply HCDOs with important information to assist them in assessing cybersecurity risks associated with medical devices.
Password security	• Use unique user ID and a sufficiently strong and unique password that cannot be easily guessed. The SANS Institute's Password Construction Guidelines[7] provide the best practices for the creation of strong passwords. See CISA's Security Tip ST04-002[8] for more information on password security. • Ensure that any default password is changed as soon as possible (i.e., prior to fitting software installation, during the installation, or upon next log in).
Network security	• When a data connection via Wi-Fi or a mobile network is required, avoid connecting to networks in public places (e.g., coffee shops, airports) that can be accessed by many people.
Malware protection	• Use caution with e-mail attachments and untrusted links. ○ Look very carefully at the sender of the e-mail message. ○ Be cautious when receiving attachments from senders with whom you do not regularly correspond. It is important to detect malicious attachments, which may contain malware or exploit scripts that may compromise your computer/laptop on which the fitting software is running. ○ Hover the cursor over each untrusted link to check the corresponding URL and determine whether it is credible. Mismatched URLs (i.e.,

[6] The form can be downloaded from https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security

[7] Source: https://www.sans.org/information-security-policy/?category=general

[8] Source: https://us-cert.cisa.gov/ncas/tips/ST04-002

Category	Best Practice Recommendations
	those where the name of the link in the e-mail does not match the corresponding URL) are highly suspect and may lead to malicious websites. • Do not install or download unknown or unsolicited applications on the computer/laptop on which the fitting software is running.
Access control	• Enable automatic log off on your computer/laptop on which the fitting software is running after a specific period of inactivity. • Shut down, lock screen, log off manually, or put your computer/laptop to sleep before leaving the fitting software unattended. • PCs should be configured to require a password to start up or wake-up from sleep.
Health data de-identification	• If data is exported from the fitting software, ensure that all sensitive data is protected from unauthorized access. Follow vendor's instructions to remove sensitive data, if available.
Repair and decommissioning	• Some product repairs may involve replacing your computer/laptop's hard drive, and some may not. If your hard drive contains sensitive or confidential data, you should back up your important data. Before sending in your computer/laptop for service, third-party shredding tools can be used to ensure deleted files cannot be recovered in Windows. • When you uninstall the fitting software from the computer/laptop that is slated for decommissioning or disposal, ensure that all sensitive data (e.g., PHI, PII) are wiped.
Bluetooth security	• Consider turning off a device's Bluetooth when not needed or in use. Especially while in certain public areas (e.g., shopping malls, coffee shops, public transportation). In general, Bluetooth capabilities should be disabled on all Bluetooth devices, except when the user explicitly enables Bluetooth to establish a connection. • Pairing Bluetooth devices should take place in a secure non-public area that is indoors away from windows in locations with physical access controls. Users should not respond to any messages requesting a PIN, unless the user has initiated a pairing and is certain the PIN request is being sent by one of the user's devices. • Users should not accept transmissions of messages, files, and images from unknown or suspicious devices. [Source adapted: NIST SP 800-121 Revision 2]
Authorizing remote fitting sessions	• Hearing device users should never authorize a remote fitting session unless it is expected and agreed to occur at a designated time. • If during a remote fitting session, a request is received by the hearing device user or the HCP that is not expected, the fitting authorization should be denied. If the incident involves a hearing device user, the HCP should be notified about the issue to take the appropriate action and to ensure the continued safety of the hearing device user data. • The HCPs should ensure they are connected to the intended hearing device user.
Other recommendations	• If you notice any suspicious activity on your fitting software accounts or any unexpected operation of the hearing device, contact the vendor.

Table 6 User-related security recommendations

5.2 Recommended Security Controls

Table 7 provides an overview of recommended technical, physical, and administrative security controls. The controls are divided into several categories. The recommended security controls listed below are not exhaustive. There can be additional security controls required by the HCDO to ensure a sufficient level of security when using the fitting software/system.

Category	Security Control
Physical and environmental security	• Consider protecting the fitting system from physical access by unauthorized people.
Access control	• Control access to the fitting software/system by assigning roles using the principles of least privilege and separation of duties (e.g., ensuring that users have only the minimum access rights that they need to perform their jobs). • Secure access to the fitting software/system by using a unique login for each user. • More than a few unsuccessful password submissions during an attempt to logon to a computer/laptop on which the fitting software is running may represent an attacker's attempts to guess the correct user password by trial and error. If possible, configure the operating system to disable the user account for a certain amount of time after a specified number of unsuccessful logon attempts. • Limit public access to passwords used for privileged access to the fitting software/system. • Control remote access (e.g., via a remote desktop) to the fitting software by deploying MFA. HCDO is responsible for deploying a multi-factor authentication solution. • In case the fitting software supports a remote service feature (e.g., the fitting software can be serviced remotely by establishing remote desktop control sessions), follow the instructions provided by the vendor for enabling remote service sessions and protect the fitting system from unauthorized remote access. • Remove or disable all unused user accounts which are no longer required (e.g., when an individual changes the role or leaves the organization). • If the computer/laptop on which the fitting software is running is connected to a public network, use appropriate mechanisms (e.g., VPN, operating system’s firewall) to protect it from unauthorized access.
User authentication and authorization	• Ensure that an HCP is authenticated and authorized prior to access to the fitting software. For example, ensure that each HCP has unique username and password and assigned appropriate permissions.
IT network security	• Configure the IT network environment to which the fitting system connects to in order to protect it from unauthorized intrusion. There are many techniques for isolating and protecting medical information systems, including implementing firewall protection, DMZs providing a buffer between an organization’s internal network and the Internet, VLANs, and network enclaves which do not interact with other information systems or networks.
Remote communication	• If a communication session over a remote desktop interface is lost or terminated, renewed authentication prior to allowing access over the remote desktop interface must be required.
System and	• Ideally, a dedicated computer/laptop confined to performing the fitting

Category	Security Control
application hardening	workflows should be used. • Ensure that the computer/laptop on which the fitting software is running uses the latest version of the operating system including all up-to-date security patches. • Always keep the antivirus/anti-malware software up-to-date.
Product upgrades and security patches	• Always keep the fitting software up-to-date and use the latest version provided by your vendor.
Malware detection and protection	• If possible, enable and use an "External email" tagging feature to show the received e-mail is from users outside of your organization. This feature can help to protect against spam and phishing threats. • Enable strong spam filters to prevent phishing emails from reaching users. • Ensure that the computer/laptop on which the fitting software is running is protected by the antivirus/anti-malware software. • Never attach untrusted storage media such as USB sticks to the computer/laptop on which the fitting software is running.
Health data storage confidentiality and integrity	• When you store sensitive data on a hard drive of the computer/laptop on which the fitting software is running, use the full disk encryption feature (e.g., BitLocker for Windows, FileVault for Mac OS) to protect the files from being seen or copied. • Always remember to make a backup of your important data before using any erase or encryption options, as any rewriting of data includes a risk of data loss. • When you store sensitive data in the cloud, ensure the cloud service provider implements data protection measures such as encryption of data at rest and in transit as well as data segregation.
Data backup and disaster recovery	• Make regular backup copies of important files or data (e.g., fitting software installation/configuration files, patient database). • Follow the 3-2-1 backup rule: ○ Create three (3) copies of any important file: 1 primary copy and 2 backups. ○ Store the files on at least two (2) different storage media types (e.g., local drive, network share, tape drive, etc.). ○ Store one (1) of these copies off-site (e.g., outside the business facility) or in the cloud.
Logging and auditing	• Rely on the logging and auditing of security-related events (e.g., addition of new user accounts, password changes, user logins, login failures, remote access, etc.) provided by the underlying operating system in which the fitting software is executed to record evidence which can be used for forensic analysis at a later date to reconstruct actions and events in case of a security incident and/or data breach. • If logging and auditing of security-related events is provided in the fitting software, it can also be useful for forensic analysis and troubleshooting purposes.

Table 7 Technical, physical, and administrative security controls

6 Best Practice Recommendations for Fitting Authorization and HCP Authentication

As modern technology and the Internet has matured in recent years the process of fitting a hearing device has seen improvements that allow HCDOs and hearing device users to choose from two different types of fitting sessions. In the past the most common fitting method has been a hearing device user's visit to the HCP's physical office (i.e., local fitting). In a fitting session that occurs at the HCP's office, the hearing device user and the HCP meet and interact to connect the hearing device(s) to programming software using a physical connection to the programming interface of the hearing device or a short-range wireless connection via a wireless programming interface.

A remote fitting allows the hearing device user and the HCP to meet virtually via a secure Internet connection. Remote fittings require additional considerations so that the hearing device user can be assured the same level of safety and security as when the hearing device user sees the HCP in a physical office. In a remote fitting session, the hearing device user authorizes the HCP to access the user's hearing device remotely.

To ensure that the hearing device user gets most benefits from a hearing device and to ensure safety, fitting should be performed by trained HCPs. Both the hearing device and the fitting system need to be designed in a way to prevent unauthenticated and unauthorized users from modifying the fitting settings.

6.1 Fitting Authorization Requirements

IMDRF's guidance on medical device cybersecurity outlines the design principles that medical device manufacturers should consider in designing their products. The guidance is intended to facilitate international regulatory convergence on medical device cybersecurity and can be considered as international best practice.

The EHIMA Cybersecurity Working Group considers that hearing device vendors should adhere to the design principles outlined by IMDRF. With respect to the fitting authentication and authorization, the following design principle is applicable to hearing devices and therefore should be implemented by hearing device vendors:

> **User Authentication:** *The manufacturer should consider user access controls that validate who can use the device or allows granting of privileges to different user roles or allow users access in an emergency. Additionally, the same credentials should not be shared across devices and customers. Examples of authentication or access authorization include passwords, hardware keys, or biometrics, or a signal of intent that cannot be produced by another device.*

The EHIMA Cybersecurity Working Group recognizes that the user access controls and mechanisms to grant privileges to different user roles as recommended above may be vendor-specific in many cases. However, in a special case of the fitting authorization, the EHIMA Cybersecurity Working Group encourages hearing device vendors to follow the common guidance for authorization methods which may be used to ensure an adequate level of fitting security and safety. Recommended fitting authorization methods are described in the next section.

6.2 Fitting Authorization Methods

Hearing device vendors need to ensure – with a reasonable level of trust – that only professional HCPs can access and modify the fitting settings in hearing devices. Loss or degradation of integrity of the fitting settings in a hearing device may result in harm by using such a device.

Today's hearing devices will in many cases allow fitting to be done using the Bluetooth interface which is also used by the hearing device user for enhancing the hearing experience by using a mobile phone application also designed and provided by the hearing device vendor.

Using a Bluetooth wireless programming interface poses a challenge for the hearing device vendor, as it needs to ensure the hearing device fitting is only possible for the HCP. This can be implemented as suggested in cybersecurity literature by authentication and authorization controls and defining user roles with different rights assigned to them.

The hearing device should go through the following steps to allow fitting:

- normal mode (hearing device does not allow fitting)
- authentication (e.g., verify an identity)
- authorization (assign fitting rights only to the right identity)
- allow fitting to be performed
- close session and return to the "normal mode"

For any chosen authentication method, the following should be considered by the hearing device vendor:

- Cybersecurity challenges of doing authentication over a wireless interface must be considered. This includes items like e.g. replay attack, data integrity and confidentiality.
- The right to do fitting should be earned – never assumed, meaning the hearing device by default shall reject fitting until it is convinced it can let down it's guards and allow fitting for only a specific session.

Convincing the hearing device that it should allow fitting can be implemented in many ways depending on what technology is available to the hearing device vendor. Hearing devices that are not restricted regarding physical size for instance, might have possibilities to e.g. allow fitting based on something as simple and low-level as an "allow fitting on/off" switch on the device. The end-user would with this solution of course be expected only to flip the switch when allowing the HCP access to the hearing device. A dedicated gesture to allow fitting could also be performed – for these kinds of solutions it is required that the end user must not be mistaken about what their action means or results in.

This whitepaper does not describe all the specific solutions that may exist but does recognize the fitting authorization problem can be solved in different ways.

For instance, in device where a physical switch is not an option, fitting authorization could be based on cryptography. Cryptography is widely used today in many online solutions on the internet as well as in computing/medical devices to protect data confidentiality and integrity, and for entity authentication, providing the basis for implementation of digital identities.

Several off-the-shelf solutions, using cryptography exist today. However, due to resource constraints (such as processing power and memory capacity) that hearing devices typically have today, such off-the-shelf, cryptography-based solutions cannot be directly applied to the hearing devices and therefore need to be adapted. The adaptations should be made in a way that ensures the same general, cryptographic principles as used in computers and mobile devices are preserved.

For the specific purpose of granting access to a hearing device fitting, cryptography can be used to manage digital identities and ensure authenticity and integrity of fitting configurations. With managed digital identities a security architecture can be created that handles both HCPs and e.g., a dedicated security dongle whose possession grants the right to fit hearing devices. From a security perspective digital identity for individual persons such as HCPs or dedicated devices is handled in the same way. The creation and distribution of digital identities needs to be tightly controlled if the hearing device is expected to trust the digital identity. As stated earlier the goal is to restrict fitting to only professional HCPs.

With a digital identity solution, hearing devices would be able to identify exactly who or what device it grants fitting access to – based on the trusted identify of a verifiable digital certificate. A digital identity solution would typically handle both authentication and authorization based on access to cryptographic keys which is assumed by the hearing device to be kept secret/secure. This system must also be based on recognized and approved cryptographic algorithms. A system that uses cryptography would be significantly more challenging to implement compared to the example of a simple "on/off switch".

A potentially more secure but at the same time more complex scheme of fitting authorization is based on a *Trusted Authority*[9], an entity which is trusted by a hearing device. The trust is based on the hearing device being able to authenticate the Trusted Authority (e.g., based on a valid certificate installed in HD), and the Trusted Authority being able to authenticate the HCP (e.g., based on HCP credentials such as username and password). First the Trusted Authority authenticates HCP and then cryptographically attests HCP’s identity to the hearing device. If the attestation is successful, the hearing device starts to trust HCP, which means it grants the HCP the right to perform the fitting. Figure 2 illustrates on a conceptual level this scheme.

[9] A Trusted Authority service may be located in the organization’s network or on the Internet (e.g., hosted by a cloud provider).

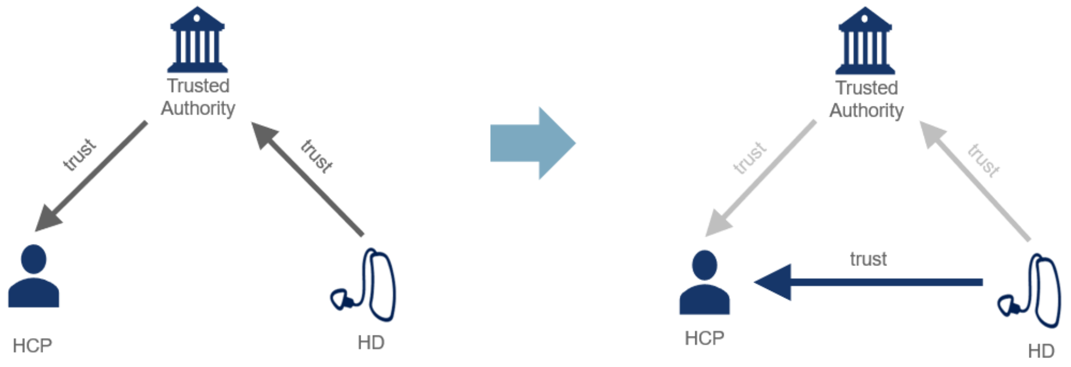

Figure 2 Establishing a trust relationship between hearing device and HCP via a Trusted Authority

With developments in technology the list of ways to authorize fitting is expected to be extended in the future – possibly with methods that cannot be considered useable or valid today.

6.3 HCP Authentication

Based on the latest cybersecurity practices, HCP authentication before accessing the fitting software is essential part of ensuring a safe and secure user experience. User identification, account management, authentication and password management can be challenging if not designed with data security and data privacy in mind. The most important rule is to safely store sensitive user information, including the user's password. User data should be treated as confidential and handled appropriately.

The EHIMA Cybersecurity Working Group recommends the following best practices for performing HCP authentication to computer systems that run fitting software or access Internet connected remote fitting applications such as the software that runs on a mobile phone.

- On the fitting software PC or in the remote fitting systems, passwords should be salted and hashed using a suitable one-way key derivation function (refer to NIST SP 800-63B) and never stored in plaintext.
    - Passwords should use a cryptographically strong hash that cannot be reversed.
    - Store passwords in the system credential storage (e.g., use Credential Manager[10] on Windows operating system).
- Enable the PC fitting software and remote fitting systems to use third-party identity providers if possible.
    - Identity providers[11] allow the fitting software and remote fitting system to rely on a trusted service to authenticate an HCP or hearing device user's identity.

[10] Source: https://support.microsoft.com/en-us/windows/accessing-credential-manager-1b5c916a-6a16-889f-8581-fc16e8165ac0

[11] Examples of identity providers: Microsoft Azure Active Directory, Auth0, Amazon Web Services, Okta.

- Validate the users’ identity to ensure they are who they say they are.
    - When creating user accounts validate the contact as soon as possible. Send a validation code or link to the contact’s email address or phone number. In any cases users with mis-entered contact information may inadvertently hand over the full control of their account to an unknown third party.
- Require a 2-step log in verification (also known as two-factor authentication or 2FA).
    - A 2-step log in verification ensures that the user’s data is not suspectable to password cracking or password reuse.
- Establish practical application session length.
    - A session once established allows users to use an application without having to re-authenticate. Consider making the session length appropriate for successful fitting but not too long so that user never has to re-validate their identity to the application.

7 Conclusion

The developments in technology introduce new opportunities that offer great benefits and freedom for both HCPs and hearing device users. For the hearing care ecosystem, remote fitting and wireless technologies are good examples. In today's world, however, any connected system also poses cybersecurity risks that need to be considered and mitigated.

Understanding how to use the hearing care ecosystem securely must be considered during the whole lifecycle of the hearing device. Each role covered in this whitepaper will have their part to fulfill, to ensure the enabled technological opportunities can be achieved with minimal impact on safety and data privacy.

8 Acknowledgments

The EHIMA Cybersecurity Working Group would like to thank all reviewers for their valuable comments and suggestions that significantly improved this whitepaper.