Bluetooth® Security

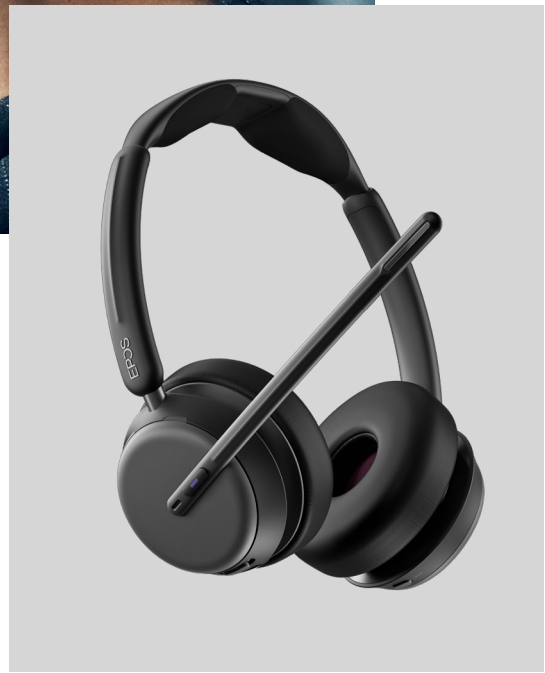
EPOS

Introducing Bluetooth® Security

Bluetooth® is a global wireless standard designed for secure short-range transmission of audio and data between compatible devices. Governed by the Bluetooth® Special Interest Group (SIG), Bluetooth® is one of the most widely adopted wireless technologies worldwide, used across audio, mobile, computing, automotive, and industrial applications.

As the technology has evolved, Bluetooth® security has advanced significantly. Modern standards include secure pairing, device authentication, and strong encryption to protect user data and prevent unauthorized access. Technologies such as Bluetooth® Low Energy (LE) and LE Audio further enhance security while improving energy efficiency.

When implemented correctly, Bluetooth® provides a high level of built-in protection, and the overall risk of unauthorized access is low. EPOS goes beyond standard requirements by combining Bluetooth® technologies with dedicated product design and security measures to deliver reliable, professional-grade audio solutions.



How Bluetooth® works

Bluetooth® enables secure wireless communication between devices over short distances. Before devices can communicate, they must first be paired.

Pairing is a user-initiated, secure digital “handshake” that allows two devices to recognize and trust each other. During this process, devices are temporarily made discoverable so they can establish a connection and authenticate securely.

Once paired, the devices generate and store a shared security key. This key is never exposed to the user and is used to protect future communication. After pairing is complete, the devices can reconnect automatically without repeating the process ensuring fast, seamless, and secure use.

While pairing enables devices to connect, Bluetooth® security relies on a broader architecture that governs how trust, keys, and encryption are managed.

In brief

Bluetooth® is a globally adopted wireless standard with built-in security features such as secure pairing, authentication, and encryption, making unauthorized access unlikely when correctly implemented.

Bluetooth® Security architecture

Bluetooth® security is built directly into the specification and applies throughout the connection lifecycle. It is based on three core elements:

1. Pairing and Bonding

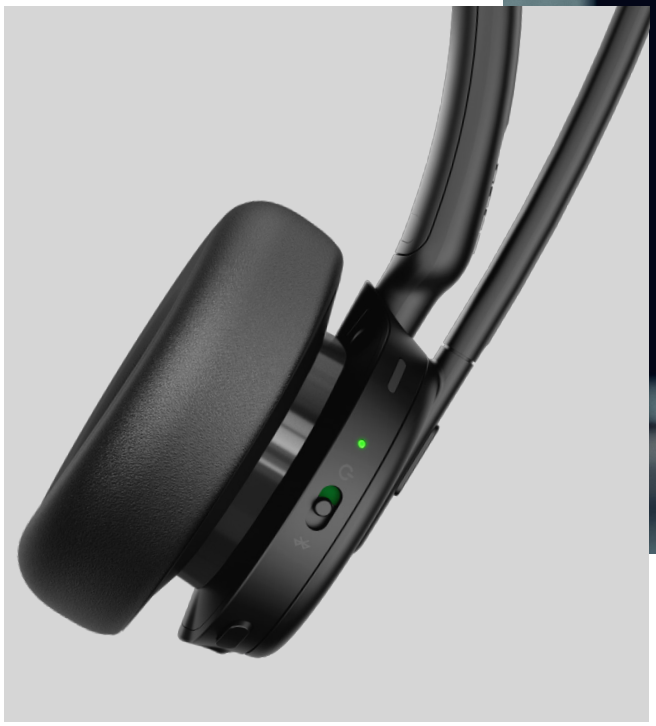
Pairing authenticates devices and establishes trust. When bonding is enabled, devices store shared security information, allowing them to reconnect securely in the future.

2. Key Generation and Exchange

During pairing, devices generate encryption keys using standardized cryptographic procedures defined by the Bluetooth SIG. These keys are stored securely and are never transmitted in plain form.

3. Encrypted Link-Layer Communication

All Bluetooth® communication takes place over an encrypted link-layer connection.



Encryption protects audio and data from eavesdropping, ensures only authenticated devices can communicate, and maintains data integrity.

Encryption is handled automatically by the Bluetooth® protocol and does not require user interaction during normal operation.*

Managing Trusted Devices

Bluetooth® security includes lifecycle controls that support enterprise device management. Users or administrators can remove bonded devices, reset connections, or control discoverability settings, ensuring that lost, replaced, or unused devices cannot reconnect.

This architecture establishes the foundation for secure communication. The following section focuses on how this encryption protects audio and data during everyday use.

In brief

Bluetooth® security is based on a standardized architecture that authenticates devices through pairing and bonding, generates and securely stores cryptographic keys, encrypts all wireless communication, and provides lifecycle controls to manage, reset, or remove trusted devices throughout their use.

* IMPACT 500 supports Secure Connections, allowing customers to use the higher-grade AES-128 encryption with supported dongles, phones and computers.

Encryption during use

Once devices are paired, Bluetooth® communication is automatically encrypted. Audio and data are encrypted at transmission and decrypted only by the intended receiving device.

Together, authenticated device access and encrypted communication form the foundation of Bluetooth®'s built-in security model.

High Level of Built-In Security
Bluetooth® security is designed to mitigate common risks through short operating range, authenticated connections, and encrypted transmission. The pairing phase is the most exposed moment, as devices must briefly be discoverable, but the risk remains low in real-world environments.

Examining common enterprise threat scenarios helps illustrate how these risks are addressed in practice.

Commonly Discussed Threats
To explain the advantages of the secure EPOS headsets, it is useful to list the different types of threats that are being discussed.

Man-in-the-Middle Attacks (MITM)
An attempt by an unauthorized device to intercept or manipulate communication between two Bluetooth® devices – typically during the initial pairing process. This requires very close proximity, precise timing and active intervention, and is protected by authenticated pairing, limited Radio Frequency range, and EPOS pairing safeguards.

Malware / Virus Transmission
The spread of malicious software via Bluetooth® connection. EPOS Bluetooth® headsets and USB dongles support audio-only Bluetooth® profiles. They do not transmit files or executable data, eliminating the environment required for malware transmission.

Eavesdropping
An attempt to listen to Bluetooth® communication without authorization. Audio streams are encrypted and transmitted digitally. Interception would require presence during pairing, highly specialized equipment, and a successful MITM attack.

Supplementary EPOS Security Measures
To strengthen Bluetooth®'s built-in security even further, EPOS applies additional safeguards:

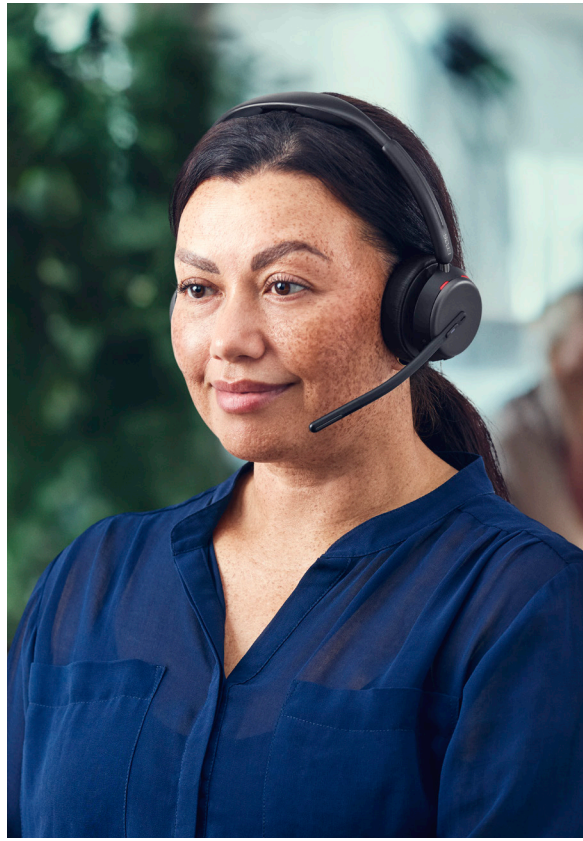
Intelligent Power Management
During pairing, the transmit power of EPOS Bluetooth® devices is reduced. This results in a much shorter range when performing the pairing process. "Man in the Middle" attacks become extremely difficult to undertake as the attacking device would have to be very close to the pairing devices.

Host Device Access Security
EPOS headsets and the corresponding USB-dongles only support audio related Bluetooth® profiles. Data content stored on the host device can never be transmitted to the headset or other devices. This means that viruses cannot be transferred, either.

Short Pairing Window
Devices are discoverable only for a brief, user-initiated period before Bluetooth® access is automatically disabled again.

EPOS Authenticated Firmware Security
All EPOS Bluetooth® headsets rely on a secure firmware authentication model digitally signed exclusively by EPOS, protecting EPOS headsets and dongles against unauthorized and malicious third-party modification.

EPOS uses Secure Simple Pairing (SSP) and LE Secure Connections, which rely on Elliptic Curve Diffie-Hellman (ECDH) cryptography to establish shared keys securely – even in the presence of passive attackers.



In brief
In everyday use, Bluetooth® protects audio and data through automatic encryption, authenticated connections, and short operating range, mitigating common threats such as eavesdropping, man-in-the-middle attacks, and malware transfer – further reinforced by EPOS product-level security measures.

ISO Certification

EPOS is certified under ISO/IEC 27001, the international standard for Information Security Management Systems. This certification demonstrates a structured approach to risk management, operational resilience, and global compliance—ensuring that the organization supporting EPOS products meets enterprise-level security expectations.

By meeting these stringent requirements, EPOS has demonstrated expertise in:

Risk Management: Proactively identifying and mitigating potential data vulnerabilities.

Operational Resilience: Establishing rigorous protocols to ensure business continuity.

Global Compliance: Aligning our internal processes with the highest legal and regulatory requirements worldwide.

By securing our internal data frameworks, we ensure that the ecosystem supporting your devices is as robust as audio engineering inside them. For us, security is not an afterthought; it is an essential component of the premium. Achieving ISO/IEC 27001 requires an exhaustive audit of our internal processes, from how we handle intellectual property to how we manage third-party vendor risks. For our enterprise clients, this means reduced risk and increased reliability.

In brief

ISO/IEC 27001 certification confirms that EPOS operates a formally audited information security management system aligned with enterprise requirements.

EPOS legal disclaimer

At EPOS we strive to ensure the best security measures in our Bluetooth® products. However, we cannot be held responsible for compensation for damages or expenses due to any security breaches taking place on the part of the customer using our Bluetooth® products.

Although EPOS has implemented precautionary measures to ensure a high security level, it is the customer's responsibility to check and configure appropriate settings of his Bluetooth® device to maintain security. Security measures implemented in the EPOS device may not be supported by the customer's device, which may reduce the security level of a Bluetooth® connection.

The customer acknowledges that Bluetooth® encryption protects the wireless link itself; end-to-end encryption at the application or telephony layer depends on the services used.

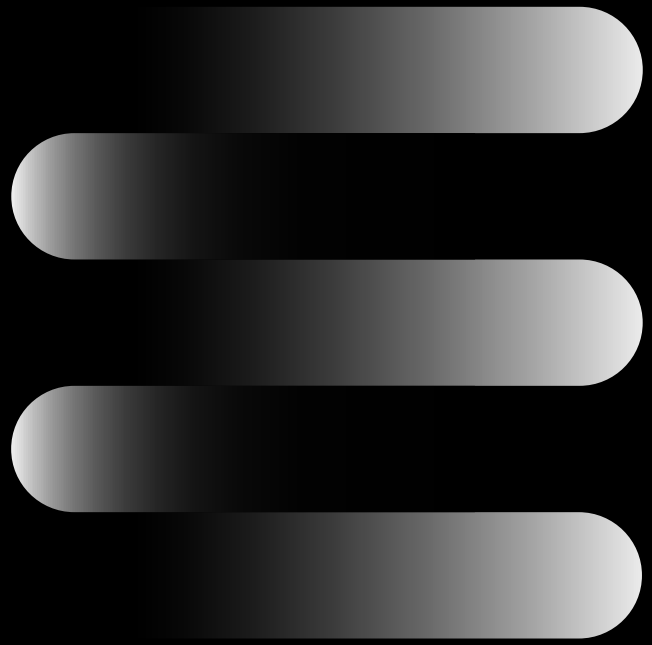
Communication links and contents transferred by an encrypted Bluetooth® connection (i.e. telephone calls) are not encrypted by the EPOS Bluetooth® device. The customer further acknowledges that no technology provides complete security. For higher security requirements than provided by the Bluetooth® standard, additional measures must be implemented by the customer.

Nevertheless, EPOS will be liable for damages from injury to life, body or health due to negligent breach of duty by EPOS or damages arising from a breach caused by gross negligence or willful intent by EPOS.

EPOS is also liable for negligent breaches of essential contractual obligations. Essential contractual obligations mean obligations whose performance is a fundamental prerequisite for the proper execution of the contract and on which a contracting party may rely upon. In this case, compensation is limited to foreseeable, typical damage.

The above provisions also apply to damages caused by a legal representative or a person used to perform an obligation of EPOS.

EPOS' liability according to the Danish/ European Product Liability Act unaffected.



EPOS Group A/S
Industriparken 27
2750 Ballerup, Denmark
eposaudio.com