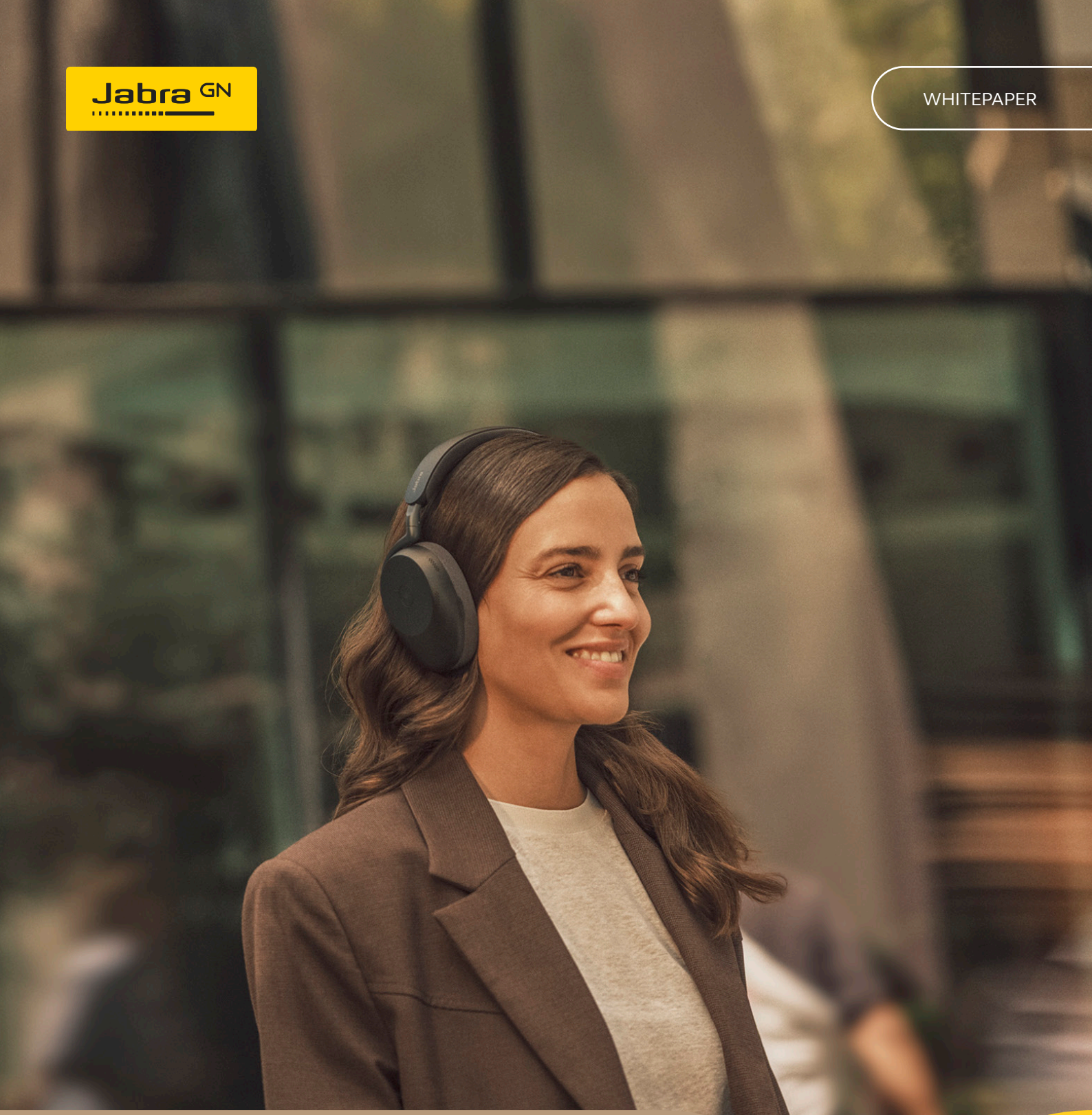
WHITEPAPER



Jabra Evolve3 Bluetooth Low Energy (LE) Audio

Stronger security and better performance than Bluetooth Classic

From Bluetooth Classic to LE Audio: What Enterprises Need to Know

Bluetooth has become the standard for professional wireless headsets. Millions of Jabra devices are used every day across offices, homes, and shared workspaces around the world.

As wireless technology evolves, many organizations are asking an important question: does newer Bluetooth technology actually improve security, reliability, and audio performance in a meaningful way?

The Jabra Evolve3 headsets use **Bluetooth LE Audio**, built on the Bluetooth Low Energy (LE) stack and the LC3 codec, rather than relying solely on traditional **Bluetooth Classic (BR/EDR)** audio profiles. This evolution is not just a radio update. It's a smarter, more efficient foundation for professional wireless audio that delivers tangible benefits in three critical areas for enterprises:

Stronger, more modern security model – LE Audio relies on LE Secure Connections and always-on link encryption for unicast streams, reducing exposure to legacy Bluetooth Classic modes and simplifying secure configuration.

Improved performance and robustness – LE Audio with LC3 offers more stable latency, better perceived audio quality at lower bitrates, and more graceful handling of packet loss and RF congestion than typical Classic SBC-based audio.

Better power efficiency – LE Audio's low-duty-cycle radio and efficient codec design reduce power consumption per minute of audio, supporting all-day professional use.

This paper explains how Bluetooth LE Audio used in Jabra Evolve3 differs from Bluetooth Classic in terms of performance and why, from a security point of view, LE Audio represents a more future-proof foundation for enterprise-grade wireless communication.

Bluetooth in professional headsets

Bluetooth as a critical link in enterprise communication

Wireless headsets are no longer optional workplace accessories. They are now a core part of how people communicate and collaborate.

Employees regularly move between calls, meetings, shared spaces, home offices, and public environments throughout the day. That means wireless audio devices need to perform reliably wherever work happens.

For enterprises, headset connections need to:

- Keep conversations confidential.
- Deliver high, consistent call quality.
- Remain robust in RF-busy environments.
- Support long battery life over a full working day.

Jabra has previously documented Bluetooth security for professional headsets, concluding that well-implemented Bluetooth links can offer a high level of protection for voice calls, comparable to other segments of the communication path.

Bluetooth LE Audio now raises that bar further by combining a modern security architecture with improved radio behavior and audio processing.

Classic vs LE – two Bluetooth families

Bluetooth audio in professional headsets currently exists across two different wireless approaches.

Bluetooth Classic (BR/EDR)

The original Bluetooth radio, optimized for continuous, higher-throughput streams. Classic headsets typically use profiles like HFP/HSP for telephony and A2DP/AVRCP for media.

Bluetooth Low Energy (LE) and LE Audio

A newer radio optimized for low-power connections. LE Audio adds standardized audio over LE using the LC3 codec and new audio profiles/services.

Jabra Evolve3 headsets are designed to take advantage of LE Audio where supported, while still maintaining compatibility with Bluetooth Classic devices when needed. For enterprise buyers, the important question is: what does LE Audio change in terms of security and performance?

Security architecture: LE Audio vs Bluetooth Classic

Why security matters in wireless audio

Professional headsets regularly carry confidential conversations, customer information, financial discussions, and internal business communication. As a result, wireless audio security matters.

Pairing and authentication

Bluetooth Classic

Bluetooth Classic implements two generations of pairing:

01 **Legacy Pairing** – an older mechanism with known weaknesses and limited protection against man-in-the-middle attacks. For security reasons, Jabra enterprise headsets do not support this pairing methodology.

02 **Secure Simple Pairing (SSP)** – introduced in later versions of Bluetooth to improve security, but supporting several association models (Just Works, Passkey Entry, Numeric Comparison) with different security strengths.

As Bluetooth Classic must remain interoperable with a wide range of devices, implementations often need to handle multiple modes and fallbacks. This increases complexity and the risk of using weaker configurations if not carefully controlled. Jabra enterprise Bluetooth products allow pairing with the legacy E0 cipher only if the host does not support secure connections, but if the host supports secure connections while pairing, legacy connections from that host are not permitted, preventing a downgrade attack.

Jabra's previous Bluetooth security white paper shows how, with correct configuration and implementation, headset links using Bluetooth Classic can nonetheless offer a high level of security.

Bluetooth LE and LE Audio

Bluetooth LE introduced **LE Secure Connections**, which uses Elliptic Curve Diffie-Hellman (ECDH) for key agreement and more modern cryptographic primitives than those used in Legacy Pairing. LE Secure Connections is designed to:

- Offer strong protection against passive eavesdropping.
- Provide better resilience against active attacks when authenticated association methods are used.
- Reduce reliance on legacy or weaker mechanisms.

LE Audio builds directly on this LE security framework. For unicast audio (such as a personal headset connection), LE Audio:

- Uses LE pairing with LE Secure Connections by design.
- Requires link-level encryption for audio transport.

In practice, this means that when a Jabra Evolve3 headset uses LE Audio, the cryptographic foundation of the audio link is modern and consistent across the product family.

For IT teams, that means fewer legacy exceptions to manage and a more consistent security model across deployments.

Encryption and integrity of the audio stream

Both Bluetooth Classic and LE Audio can encrypt audio after pairing. The difference is how consistently modern encryption and security methods are applied.

Bluetooth Classic

- Generally, the stack must accommodate historical options and modes, increasing the complexity of ensuring that weak variants are never used.
- Encryption depends on the negotiated link mode and can be influenced by legacy requirements of older devices. However, all Jabra Bluetooth products require the use of 128-bit encryption keys.
- All Jabra Bluetooth devices support BR/EDR secure connections. This protocol is always used when the Jabra product is used with the Jabra Link 390 USB adapter, and whenever the connected host supports it.

LE Audio

- For unicast streams, encryption is not optional; it is part of the design of the audio transport.
- LE Secure Connections defines the cryptographic algorithms and key sizes in a modern, harmonized way. Just like with Bluetooth Classic, Jabra products are required to use 128-bit encryption keys.

Jabra's security approach, as documented for DECT headsets, has been to go beyond minimum industry standards, using strong algorithms and secure pairing mechanisms verified by independent experts. Evolve3 extends this thinking into the Bluetooth domain by leveraging LE Audio's newer security architecture rather than relying solely on legacy Classic behavior.

Attack surface and legacy complexity

From a security engineering perspective, some of the key advantages of LE Audio are:

Reduced legacy baggage – LE Audio does not need to support decades of audio profiles and behaviors. The specification incorporates lessons learned from earlier generations.

Narrower attack surface – LE Audio uses a focused set of profiles and services, with mandatory encryption for unicast streams, reducing variability and misconfiguration risk.

Future-proofing – LE is the active focus of ongoing Bluetooth SIG development. Security improvements and clarifications are more likely to be applied here first.

For IT security teams, this reduces the number of exceptional cases, optional modes, and historical constraints they need to understand when evaluating the headset link in their threat models. In practice, that makes Bluetooth security easier to assess, standardize, and scale across an organization.

Table of Key Differences in Security Framework Between Bluetooth Classic and LE Audio

	Bluetooth Classic	LE Audio (via LE Security)
KEY EXCHANGE	Often uses E22/SAFER+ (Older)	ECDH (Elliptic Curve Diffie-Hellman)
ENCRYPTION	AES-CCM (128-bit)	AES-CCM (128-bit)
PRIVACY	Static MAC addresses (trackable)	Resolvable Private Addresses (Randomized)

Performance: how LE Audio differs from Bluetooth Classic

Security alone is not enough. Professional wireless headsets also need to deliver reliable performance in real working environments. LE Audio was designed with performance improvements in mind.

Latency and call responsiveness

Latency affects how well audio syncs with video and how natural conversations feel. Bluetooth Classic-based audio can sometimes introduce noticeable delays, particularly once operating system buffering and host processing are added.

LE Audio with the LC3 codec is designed to support:

+ **Smaller frame sizes** – reducing codec contribution to latency.
+ **More flexible packetization** – allowing better tuning of the end-to-end pipeline.

The result is more responsive, natural communication across calls, meetings, and media.

Audio quality and robustness: LC3 vs SBC

Bluetooth Classic's mandatory codec for A2DP is SBC, originally designed for consumer media streaming. While widely deployed, SBC was not optimized for the latest requirements in speech quality at low bitrates and under challenging RF conditions.

LE Audio introduces **LC3 (Low Complexity Communications Codec)**, designed from the outset to improve on SBC:

- At similar bitrates, LC3 provides higher subjective audio quality than SBC.
- LC3 offers better quality retention when bitrates are reduced, which is useful for optimizing power and RF robustness.
- LC3 degrades more gracefully under packet loss, preserving intelligibility and reducing artifacts when conditions are poor.

For users of Jabra Evolve3 headsets, this translates into:

Clearer, more natural stereo channel super-wideband speech as opposed to mono wideband only with Bluetooth Classic.

Fewer audible glitches in RF-dense offices.

Better overall listening comfort during long calls.

In busy offices or hybrid environments, that means conversations stay clearer and more consistent, even when wireless conditions are less than ideal.

Power efficiency and all-day use

Professional users expect their headset to last an entire working day without needing a recharge. Bluetooth LE was originally designed for low-power applications, and LE Audio builds on this strength:

- The LE radio operates with a **lower duty cycle** than Classic for a given audio experience.
- LC3 can deliver high perceived quality at lower bitrates, reducing radio transmission time and processing load.
- Connection events and isochronous channels in LE Audio allow more efficient scheduling of transmissions.

This means that Evolve3 headsets can deliver:

Longer talk time for a given battery size  or  Smaller batteries for similar runtime, enabling lighter, more comfortable designs.

For employees, that means fewer charging interruptions and more comfortable headsets during long workdays.

Coexistence and RF robustness in the office

Modern offices are crowded 2.4 GHz environments: multiple Wi-Fi networks, Bluetooth devices, cordless peripherals, and IoT systems all share the same band. LE Audio's link-layer behavior is designed to coexist more effectively with a different PHY and channel structure compared with Classic.

In combination with Jabra's RF design and interference management, this enables Evolve3 to maintain:

Stable connections as users move around the office.

Fewer audio dropouts in congested RF conditions.

Additional density countermeasures when using the headset with the Jabra Link 390 by configuring to use mono super wideband or mono wideband for voice communications.

More predictable behavior in large deployments, such as shared floors and call centres.

In real-world terms, users experience fewer interruptions and more reliable audio throughout the day.

Evolve3: combining LE Audio with Jabra's security approach

Jabra's approach to wireless security, well documented in the Engage DECT security white paper, is to go beyond compliance and design solutions that are practical, testable, and independently verifiable. Evolve3 carries this approach into the Bluetooth space.

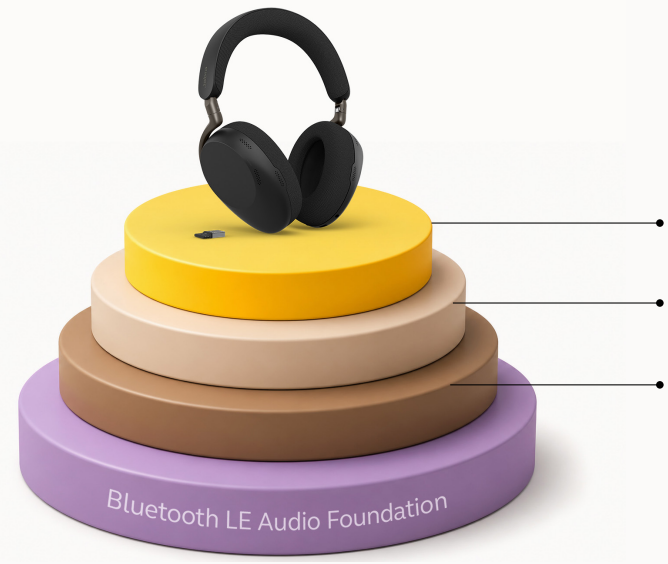
Secure default configurations

Evolve3 headsets are designed so that secure operation is the default, not an option:

- LE Audio unicast connections use LE Secure Connections and enforce link-level 128-bit encryption.
- Internal firmware is designed to avoid weaker modes where platform and interoperability requirements allow.
- When the headset is used with the included and pre-paired Jabra Link 390, additional pairing steps by the end user are not needed, reducing the risk of unintentional pairing with untrusted devices.

Performance tuned for professional communication

On top of the LE Audio foundation, Evolve3 adds Jabra's audio and RF expertise:



- LC3 settings and DSP chains optimized for speech clarity in UC scenarios.
- Microphone arrays and noise-suppression tuned for open offices and hybrid workspaces.
- RF design and antenna placement engineered for mobility within typical office floorplans.

The result is that users not only benefit from the inherent advantages of LE Audio, but also from Jabra's tuning for enterprise communication.

That means audio performance designed specifically for the realities of modern work, not just consumer listening.

Practical implications for IT and security teams

From an enterprise perspective, adopting Evolve3 with Bluetooth LE Audio offers:

Stronger security posture

- Audio streams protected by modern LE Secure Connections and mandatory encryption for unicast audio.
- Reduced reliance on legacy Classic modes and profiles with more variable security characteristics.

Better user experience

- Clearer speech and more robust performance in challenging RF environments.
- All-day battery life supporting hybrid working patterns.

Simplified security assessment

- A more modern, homogeneous security architecture compared to mixed legacy Classic deployments.
- Clearer alignment with current best practices from the Bluetooth SIG and the wider security community.

IT and security teams can therefore treat the headset link as a well-defined, modern segment in their overall communication security model, alongside secure UC platforms, VPNs, and endpoint protections.

Conclusion

Bluetooth Classic has enabled the rise of wireless headsets in professional environments, and when properly implemented, it can provide a high level of security for voice calls. However, as expectations around security, performance, and battery life continue to rise, the limitations and legacy complexity of Classic become more apparent.

Bluetooth LE Audio, used in the Jabra Evolve3 headsets, represents the next step:

- A **more secure** foundation built on LE Secure Connections and mandatory encrypted unicast audio streams.
- **Higher and more consistent performance**, with improved audio quality and RF robustness through the LC3 codec and LE isochronous channels.
- **Better power efficiency**, supporting all-day professional use in modern workplaces.

For organizations balancing security, productivity, and employee experience, LE Audio provides a more modern foundation for professional wireless communication.

For organizations that depend on confidential, real-time communication, moving to LE Audio–based headsets such as Jabra Evolve3 is a practical way to strengthen wireless security while delivering a better experience for users.