Bluetooth® Security

Introduction Bluetooth® Security

For EPOS, comfort, quality and security are high priority areas. This paper addresses the security of Bluetooth® technology and the supplementary security that EPOS' Contact Center and Office (CC&O) headsets provide.

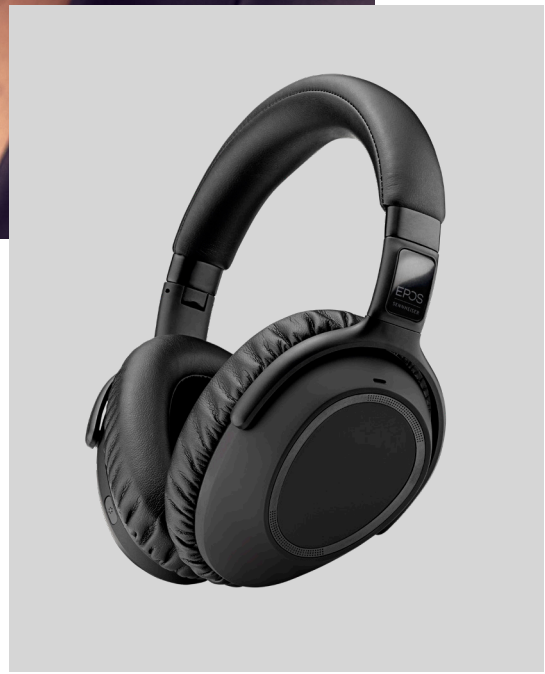
Introduction

Bluetooth® is a wireless technology standard for exchanging voice and data over short distances between Bluetooth® enabled devices. Ericsson introduced Bluetooth® to the market in 1994 to overcome the challenges of connecting devices with different types of technology and communication protocols.

Since its introduction, the Bluetooth® Special Interest Group has collected more than 20,000 member companies and the Bluetooth® standard has become a widespread and popular method of connecting devices. More than 2 billion units are able to use Bluetooth® technology, which has consequentially raised concerns about security issues.

Before getting into details about Bluetooth® security, it should be mentioned that overall, the risk of unauthorized access to communication via Bluetooth® is limited. In general, Bluetooth® offers a very high level of security, which EPOS has chosen to enhance further through the intelligent use of innovative solutions.

How Bluetooth® works



The Bluetooth® standard offers a wireless connection between devices in proximity to each other. To do so, the two devices have to first be paired. The pairing is like a “technological handshake” that introduces the two devices to each other and enables them to communicate.

The pairing requires that the two devices can find each other – they must be made “discoverable”. For most Bluetooth® devices, this requires an active process of putting the devices in pairing mode. While in this setting, the devices become discoverable for a short while and can begin to exchange a security key for authentication.

After exchanging this security key, which is not transmitted through the air and cannot be stolen, the devices are successfully paired. The secret key is the “bridge” between the devices that is formed after the initial pairing. In the future, these devices can continue to use this key, which eliminates the need for repeating the pairing each time the devices are used.

Encryption during usage

After successful exchange of secret keys, the two Bluetooth devices can communicate. All EPOS products benefit from the best encryption level by using a 128-bit key generated by the pairing process. Thanks to this encryption, the data sent between devices can only be read by the intended recipient. The receiving unit decrypts the data back to its original format based on the same algorithm.

High level of security

As mentioned earlier, Bluetooth® technology offers a high level of security for the user. It is extremely difficult to eavesdrop or to interfere with Bluetooth® communication for many reasons, including the short range and the authentication that must take place in order to use the devices.

In theory, the most vulnerable point for Bluetooth® devices is when they are pairing as they have to be visible/discoverable to do that. Even though the security threat is highly hypothetical, EPOS has addressed the issue with several intelligent measures.

Different types of threats

In order 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 attack – An attacker tries to intercept information over to his device without the knowledge of the attacked. It is extremely difficult to do that in real life, as the attacker would have to be very close to the devices.

Virus – Wireless transmission of a harmful virus. The EPOS Bluetooth® headset and the Bluetooth® dongle only transmit speech, not data like other Bluetooth® devices. Therefore, there is no environment for a virus to run.

Eavesdropping – An attacker listening in on a conversation. The attacker would have to be present at the pairing and furthermore have extremely advanced equipment. The voices are encrypted and converted to a digital stream.

Modern devices use the Bluetooth® 4.0 standard and higher, especially for the use of voice transmission, which provides a high level of protection.

Supplementary EPOS security

For EPOS, security for the user plays an important role in product development. We have taken extra steps in order to strengthen the high level of security that Bluetooth® technology provides. Here are some examples:

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 – EPOS headsets are only discoverable for a very short period during pairing. After that short period, they automatically turn off the Bluetooth® access until access is reactivated by the authorized user.

EPOS legal disclaimer

At EPOS we strive for ensuring the best security measures in our Bluetooth® products. However, we cannot be held responsible with regard to compensation for damages or expenses due to any security breaches taking place on the part of the customer by 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 encryption of the Bluetooth® connection only applies to the wireless connection between paired devices. 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 means 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 damages.

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.

406839258

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