WHITEPAPER

Wiliot IoT Pixel and Cloud Privacy



© 2023 WILIOT

TABLE OF CONTENTS

Wiliot IoT Pixel and Cloud Privacy

01	Overview	03
02	What the IoT Pixels Broadcast	03
03	No Logging	04
04	Data stored on Wiliot Pixels	04
05	End-to-end Encryption	05
06	Security Standards Compliance	06
07	Summary	08

01

Overview

The Wiliot solution has been designed with privacy in mind. The use of end-to-end encryption between Wiliot's Ambient IoT Pixel tags and the cloud, having no personal information on the tags, and zero logging on the tags, makes them a great building block for GDPR compliant solutions.

In this whitepaper we detail the information that is stored on Wiliot tags, what can be seen by customers and third parties, how data is secured and some of the principles applied to building private and secure solutions using Wiliot technology.

02

What the IoT Pixels Broadcast

Wiliot ambient IoT Pixels, or tags, only broadcast secure tag identifiers and environmental sensing information. These are encrypted using AES-128-bit encryption with CBC-MAC. This ensures that only the tag owner has access to the data.

CBC-MAC (Cipher Block Chaining Message Authentication Code) is a message authentication code algorithm that is used to verify the integrity and authenticity of digital messages. It is a type of MAC algorithm that is based on the CBC mode of encryption.

CBC-MAC works by dividing a message into blocks, and then encrypting each block using a block cipher algorithm (such as AES). The encrypted blocks are then combined in a way that depends on the previous block, using a process called chaining. The result is a fixed-length code (the MAC) that can be used to verify the integrity and authenticity of the message.

The CBC-MAC algorithm is designed to be secure against a variety of attacks, including replay attacks, where an attacker intercepts and resends a legitimate message in an attempt to deceive the receiver. It is also resistant to modification attacks, where an attacker attempts to modify the message without being detected.

The encryption keys are periodically changed or rotated so in many cases the number of tags present in each location cannot be determined even if a radio sniffer is being used to monitor traffic. Each tag will appear as a random number of encrypted tags. Rotation is achieved using a KDF (key derivation function) which uses the salt (random number) and the keys stored in the tags NVM. Two consecutive packets will appear completely random to the reader.

Rotation occurs after the power available to harvest drops from a continuous level, such as when parcels are moved from place to place, the line of sight between power source and tag is obscured or a reader that provides power is transient.

Wiliot uses Random Static Address within the Bluetooth advertising packets used to transfer data from tags. which The MAC Address in the Bluetooth header, otherwise known as the Advertiser Address or ADVA is randomized every power cycle. This is important as the Bluetooth protocol is designed to broadcast it in the clear. This randomization takes place so that the data can't be used as an identifier for unauthorized tracking of a tag by someone that is not authorized to do so.

03

No Logging

Wiliot IoT Pixels do not log data locally on the tag. The tag is a read-only device. Tags cannot listen to or monitor radio or audio, they only transmit their ID and certain environmental sensing information, such as temperature measurements, encrypted until received by the Wiliot cloud.

Any logging of data, such as the place that the tag was seen, is performed in the cloud under control of an application which must disclose the nature of the information that is being logged in the application provider's privacy policy.

The Wiliot tag doesn't have a sense of its own location. There is no GPS like functionality on the tag. Any location information is detected by the device reading the broadcast from the tag, such as a phone. It is then the responsibility of the phone application to pass the location coordinates and the time the tag was seen to the Wiliot cloud.

04

Data stored on Wiliot Pixels

The data that is encoded in the tags is burnt into the chip at the time the silicon chip wafer is manufactured and tested. It includes:

- Bluetooth Manufacturer ID – this identifies Wiliot as the manufacturer
- Group ID that is used to optimize the speed of decryption
- Calibration values used to normalize temperature measurement
- A unique Pixel ID – A GS1 Serial Global Trade Item Number (SGTIN), the IoT Pixel identifier that is encrypted before it is transmitted.
- Two encryption keys

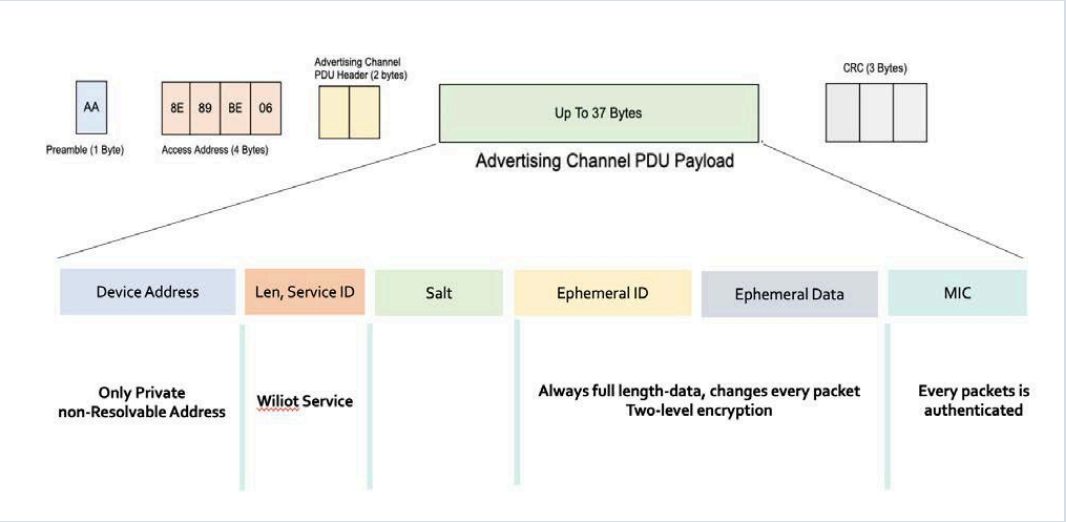

Figure 1 – Wiliot Ephemeral ID Format

Tags don't store any information that relates to the owner or user of the tag. The tag doesn't know who owns it. This information is securely stored in the Wiliot Cloud and is assigned when the tag is associated with an account on the Wiliot Cloud.

Wiliot tags broadcast a secure manufacturer specific payload called W-EID or Wiliot Ephemeral ID. This format was developed as an alternative to unencrypted formats such as Apple iBeacon.

05

End-to-end Encryption

Unlike QR codes or RAIN RFID tags, Wiliot proves end-to-end encryption, starting on the IoT Pixel Chip and ending at the Wiliot Cloud. This ensures that the owner of every tag is designated in the Wiliot cloud so that accountability for privacy rule compliance such as GDPR is clearly attributed to a specific IoT Pixel owner.

End-to-end encryption means that edge devices that are relaying the broadcasts from tags do not have visibility into the encrypted contents that they relay to the Wiliot Cloud.

Only the owner of the tag may receive the ID, sensing and location information from the tags, once they have authenticated themselves with the Wiliot Cloud using two factor authentication. Third parties will not be able to interpret or appropriate the encrypted broadcast from Wiliot IoT Pixels.

Data in Transit Encryption

Wiliot implements HTTPS and MQTT data in transit encryption using TLSv1.2 between edge devices such as gateways and the Wiliot Cloud environment. This provides secure transfer of data across the gateway such as a Wi-Fi access point with the Bluetooth radio, the API Proxy, load balancers, Wiliot's internal service and a customer's cloud.

TLSv1.2, or Transport Layer Security version 1.2, is a protocol used for establishing secure communication channels over the internet. It is a widely used encryption protocol that provides secure data transfer between web servers and web clients.

Data at Rest Encryption:

All Wiliot databases are hosted in our public cloud environment are encrypted using RDS or Relational Database Service Encryption. This is a feature that allows users to encrypt their data at rest in RDS databases. With RDS encryption is enabled, data stored in an RDS instance is encrypted using industry-standard AES-256 encryption.

RDS encryption provides an additional layer of security to protect sensitive data from unauthorized access or theft, even if an attacker gains access to the underlying storage media. It also helps organizations meet regulatory compliance requirements related to data privacy and security.

AES (Advanced Encryption Standard) is a widely used symmetric key encryption algorithm that is used to encrypt and decrypt data. It is a block cipher algorithm that uses fixed-length blocks of data to encrypt and decrypt data.

06

Security Standards Compliance

Wiliot's software as a service provides APIs and cloud interfaces such as MQTT to the applications that are owned by the owner of a Wiliot IoT Pixel. Wiliot provides the building blocks to create a GDPR compliant application.

The Wiliot cloud service which delivers that is designated a Processor for the purposes of GDPR (as opposed to a Controller).

The Wiliot cloud platform does not store data for long term use or processing. Data such as the name or address of a customer, or their purchase history is stored outside the Wiliot platform in the systems owned or developed by the owner of the Wiliot Pixels. This simplifies our customers' GDPR obligations to enable access, rectify, erase, and restrict the processing of personal data, as Wiliot does not store such data on a long-term basis.

One of the primary responsibilities of a Data Processor under GDPR is to implement appropriate technical and organizational measures to ensure the security of personal data, including measures to prevent unauthorized access, use, disclosure, modification, or destruction. The processor must also have procedures in place to detect, report, and investigate data breaches. Wiliot takes these obligations seriously. Our full-time Chief Information Security Officer provides reports directly to our executive committee, including a member of our board of directors. CFO & CEO every month and has implemented the following standards to underpin the security of what we do.

01 **ISO/IEC 27001:2013.** This is an international standard for information security management systems (ISMS). Wiliot has obtained this certification, which demonstrates that the company has implemented appropriate security controls and measures to protect its information assets.

02 **NIST 800-53.** Wiliot has also implemented security controls and measures based on the guidelines set forth in the National Institute of Standards and Technology (NIST) Special Publication 800-53, which provides a framework for securing federal information systems.

03 **GDPR.** Wiliot has also implemented measures to comply with the principles of the General Data Protection Regulation (GDPR), a set of regulations designed to protect the privacy and security of personal data of EU citizens.

04 **AICPA SOC 1 and 2.** Wiliot has started the process of implementing SOC 1 and 2 and expects to have been audited and compliant by the end of 2023. SOC stands for "Service Organization Control." It is a set of standards created by the American Institute of Certified Public Accountants (AICPA) to evaluate the internal controls of service organizations. SOC reports provide independent third-party assurance that a service organization has appropriate controls and measures in place to safeguard customer data and ensure the security, availability, processing integrity, confidentiality, and privacy of its systems and data.

Wiliot also complies with the ISO/IEC 27018:2014 standard which demonstrates commitment to protecting the privacy of personal data in the cloud. In line with this, Wiliot has implemented appropriate measures to safeguard personal data, including the secure processing, transmission, and storage of data.

07

Summary

Wiliot IoT Pixels provide a level of security not available from alternative low-cost scalable auto-ID technologies. By leveraging the power of the Wiliot designed multi-core processor built into these postage-stamp sized computers, Wiliot has balanced the need for security and privacy with a technology that can scale in an affordable manner and address a number of society's major challenges.

