# Amazon Sidewalk Privacy and Security Whitepaper

## Contents

## Introduction

Amazon Sidewalk is a shared network designed to help customer devices work better, both at home and beyond the front door. Operated by Amazon—with no charge to customers—Sidewalk helps simplify new device setup, extends the working range of low-bandwidth devices, and helps devices stay online, even if they are outside the range of the user's home wifi.

Customers with a Sidewalk gateway are able to contribute a small portion of their internet bandwidth, which is pooled together to create a network that benefits all Sidewalk-enabled devices in a community.  This can include experiences ranging from finding pets or valuables that may be lost and improving reliability for devices like leak sensors or smart lighting, to diagnostics for appliances and power tools. For example, smart lighting at the edge of a user's property, or a garage door lock in a poor coverage zone, can receive connectivity support from a participating neighbor's gateway and continue to operate if the device falls offline for a period of time. Similarly, a pet-finder device can leverage Amazon Sidewalk to locate a dog that has left the yard and is out of reach of the user's personal network. Amazon caps the amount of bandwidth shared to reduce the chances of any degradation in a customer's home network performance[1]. Participation in the neighborhood network is optional for all customers.

A simple control is provided to enable and disable participation in the neighborhood network. When customers first turn on a new Sidewalk gateway device, they will be asked whether they want to join the network. For customers with existing devices that are Sidewalk capable, an over-the-air (OTA) update will connect them to the network—no action is needed.  These customers will first receive an email about the pending update and instructions for how to disable, if that is their choice.

As a crowdsourced, community benefit, Amazon Sidewalk is only as powerful as the trust our customers place in us to safeguard customer data. To that end, this document outlines the steps we have taken to secure the network and maintain customer privacy. These efforts are core to our mission and will continue to evolve and improve over time.

---

[1] The maximum bandwidth of a Sidewalk Bridge to the Sidewalk server is 80Kbps, which is about 1/40th of the bandwidth used to stream a typical high definition video. Today, total monthly data used by Sidewalk enabled-devices, per customer, is capped at 500MB, which is equivalent to streaming about 10 minutes of high definition video.

# Amazon Sidewalk Privacy and Security Whitepaper

## Overview

This paper provides information about two areas of interest to Amazon customers: how Amazon secures customer data, and how Amazon limits the collection and storage of customer information. These key components will be referenced throughout this paper: Sidewalk Gateways, Sidewalk Endpoints, Sidewalk Network Server, Application Servers, and Packets.

**Sidewalk Gateways** (also knowns as Sidewalk Bridges or GWs) forward packets to/from the Sidewalk Endpoints and the Sidewalk Network Server. Gateways are Amazon devices, like the Ring Floodlight Cam, that use 900 MHz (LoRa and/or frequency-shift keying (FSK), and/or Bluetooth Low Energy (BLE) to provide connection to the Sidewalk network.

**Sidewalk Endpoints** (also known as Sidewalk-Enabled devices, edge devices, endpoints, or Applications) can roam on the Sidewalk network by connecting to Sidewalk Gateways. Endpoints are low-bandwidth/low-power smart products such as leak sensors, door locks, lights, or devices you can attach to valuables or a pet to know where it is. Sidewalk endpoints can be built and maintained by Amazon or third party (3P) developers. Sidewalk Gateways can also act as an endpoint and receive Sidewalk benefits like maintaining functionality when the device falls offline.
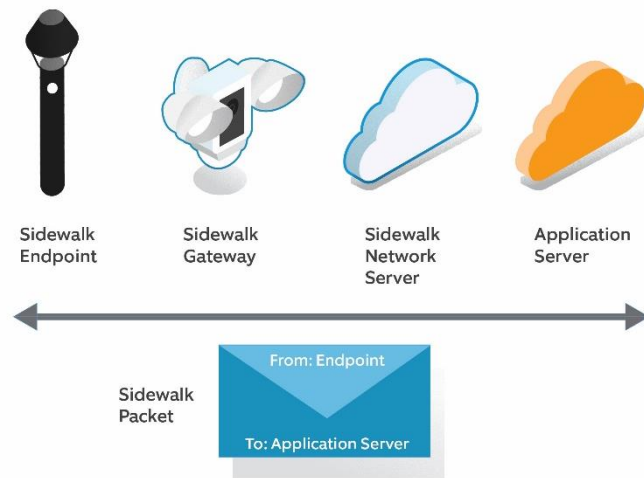
The **Sidewalk Network Server** (or SNS) is the backbone of the Sidewalk network. It is responsible for verifying that the incoming packets are coming from authorized Sidewalk devices, routing packets to the desired destination (an application server, endpoint or GW device), and keeping the network time-synchronized. The SNS is operated by Amazon.

**Application Servers** host the Sidewalk endpoints and implement the business logic for the user experience and the desired product functionality. Application servers are managed by the Sidewalk endpoint manufacturer, which can be Amazon or a 3P.

**Packets** (also known as Messages) are sent to (from) the Sidewalk Endpoints from (to) the Application Server (through the GW and SNS). Similar to a letter in the mail, the letter inside the envelope (or packet) contains information needed to perform a service (i.e. the command, "Turn on Light"). Like the post office, the SNS reads the routing information on the outside of the envelope to direct the packet to the correct endpoint and application server.

## Amazon Sidewalk Privacy

Amazon has carefully designed privacy protections into how Sidewalk collects, stores, and uses metadata. Sidewalk protects customer privacy by limiting the amount and type of metadata that Amazon needs to receive from Sidewalk endpoints to manage the network. For example, Sidewalk needs to know an endpoint's Sidewalk-ID to authenticate the endpoint before allowing the gateway to route the endpoint's packets on the network. Sidewalk also tracks a gateway's usage to ensure bandwidth caps are not exceeded and latency is minimized on a customer's private network. Information customers would deem sensitive, like the contents of a packet sent over the Sidewalk network, is not seen by Sidewalk; only the intended destinations (the endpoint and application server)

possess the keys required to access this information. Sidewalk's design also ensures that owners of Sidewalk gateways do not have access to the contents of the packet from endpoints (they do not own) that use their bandwidth. Similarly, endpoint owners do not have access to gateway information. The Sidewalk Network Server continuously "rolls", or changes transmission IDs (TX-ID) and Sidewalk Gateway IDs every 15 minutes to prevent tracking devices and associating a device to a specific user.

### *Data Minimization*

Sidewalk minimizes the use of metadata wherever possible. Sidewalk uses the metadata needed to route packets from (to) the endpoint to (from) the Sidewalk gateway, and then to (from) the Application Server. For example, when a packet is sent from the endpoint to the Application Server, the Sidewalk Network Server needs to know:

- **Endpoint Sidewalk-ID** to authenticate the Sidewalk-compatible device
- **Endpoint Payload Size** to ensure the packet meets bandwidth limitations
- **Transmission Time** to apply the correct rolling transmission ID
- **Gateway ID** to select the appropriate gateway (GW) needed to relay the packet
- **Application Server** to route the packet from the endpoint to its respective cloud

The Sidewalk Network Server (SNS) does not know the contents of the packets or commands being sent over Sidewalk. In addition to the SNS, there are four other entities with access to certain types of data.

- **Endpoint Owner:** The owner of the endpoint can only view information that pertains to the normal operation of their device (i.e. whether their smart light is on or off). They are unable to see routing information, or what GW (if they do not own it) the smart light is receiving support from, as well as any information about that GW and GW owner. The GW information is encrypted behind the Sidewalk Network Layer and Flex Layer.
- **Gateway Owner:** The GW owner is unable to see what endpoints (they do not own) are receiving support from their GW. They have no idea what types of endpoints are connected, times in which they are connected, or information about the owner of the endpoint. The endpoint information is encrypted behind the Sidewalk Application Layer.
- **Application Server:** The Application Server is unable to see any information pertaining to the GW owner, just the endpoint information. The GW-ID and information is encrypted behind the Sidewalk Network Layer and Flex Layer.
- **Amazon Web Services (AWS):** For Application Servers hosted on AWS, AWS only sees the data the Application Server grants through Key Management Service (KMS). This data is generally used in AWS for storage, processing, and other services the Application Server utilizes.

## Encryption

Packets traversing the Sidewalk network have three layers of encryption to ensure data is visible only to the intended party. This approach to encryption means that Amazon will not be able to interpret the contents of commands or messages sent through Sidewalk by third party services or endpoints (applications). See additional encryption information below in the *Amazon Sidewalk Security* section.

1. The **Sidewalk Application Layer** enables secure and private communication between the endpoint and the Application Server.
2. The **Sidewalk Network Layer** protects the endpoint's Sidewalk packet over the air. Plain-text data in this layer is accessible only to the endpoint and the Sidewalk Network Server (SNS).
3. The **Flex Layer**, which is added by the Sidewalk Gateway (GW), provides the SNS with a trusted reference of message-received time and adds an additional layer of packet confidentiality. Plain-text data in this layer is accessible only to the GW and the SNS.
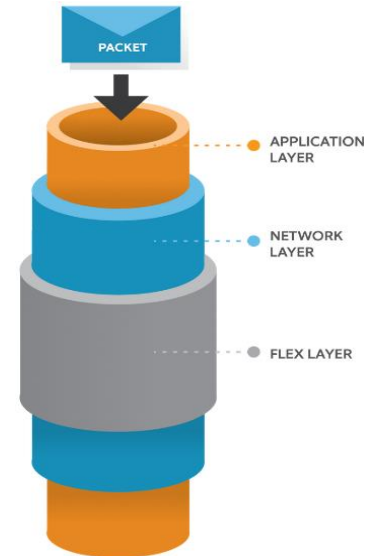
## Trusted Device Identities

Unique identifying credentials make sure trusted devices can enter the Sidewalk network while preventing unauthorized devices from joining. The Sidewalk Network Server (SNS), Application Server, and each Sidewalk device (both gateways and endpoints) are provisioned with a unique set of Sidewalk credentials that are used during the Sidewalk device registration process to mutually authenticate each devices' identity and to derive unique session keys between them. Encryption keys are derived periodically from their respective session keys using algorithmic encryption functions.

## Amazon Sidewalk Security

Preserving customer privacy and security is foundational to the design of Amazon products and services, and Amazon Sidewalk provides multiple layers of privacy and security to secure data travelling on the network and to keep customers safe and in control. The Sidewalk security model is designed to authenticate the identity of all network participants, and to provide authenticity and confidentiality for all packets traversing the network. This helps to ensure that only the authorized, intended receivers have access to the corresponding packet information, and to ensure that user's identity remains private while using the network.

To illustrate the flow of data and encryption at each stage, we will begin with a tour through the system. This is demonstrated by an outdoor smart light (Sidewalk-ID A8905) with a motion detection event.

## Device Registration and Deriving the Transmission-ID (TX-ID)

When an endpoint starts the registation process on the Sidewalk Network, it must authenticate its identity and establish a unique session key with the Sidewalk Network Server (SNS) and Application Server. Upon identity authentication, the SNS creates a random and unique index-ID (random value generated by the SNS when entering it into the lookup database), and a database (DB) record containing the following five elements: (1) index-ID, (2) unique session key, (3) transmission-ID (TX-ID) generation key, and (4) TX-ID (75757). Next, the SNS adds this record to its lookup DB of authenticated devices, and forwards the association index-ID/Sidewalk-ID match to the Application Server. From this point forward, the SNS cannot identify a user or Sidewalk-ID from an index entry or TX-ID (only the

Application Server can). The SNS and device must refresh the session key periodically, creating a new index-ID and DB record. Failure to do so will prevent the device from roaming on the network and require it to complete the registration process again.

The SNS makes it difficult for anyone, including Amazon, to piece together activity history over time, by changing the TX-ID every 15 minutes to a different unique identifier (*see Figure 1*). For example, the TX-ID is 75757 at *t(0)* or 7:00, and 43759 at t(1) or 7:15. For latency considerations, four unique codes are created at *t(0)*, representing every 15 minutes for the next hour.

Sidewalk limits the ability to work backwards through a trail of old IDs linked to the original device by continuously flushing the previous IDs after it has changed over two time periods. For example, at 7:31pm when the TX-ID is now 87305, the *t(0)* TX-ID, 75757 is deleted. The SNS cannot resolve the source of the packet to a user/Sidewalk-ID. It stores the packet for one minute, and the packet routing information of the packet for one day. Once the packet reaches the Application Server, the TX-ID is matched to the real customer identifier and can only be seen by the Application Server, not the AWS host[2].

**Figure 1: Breaking the Chain**
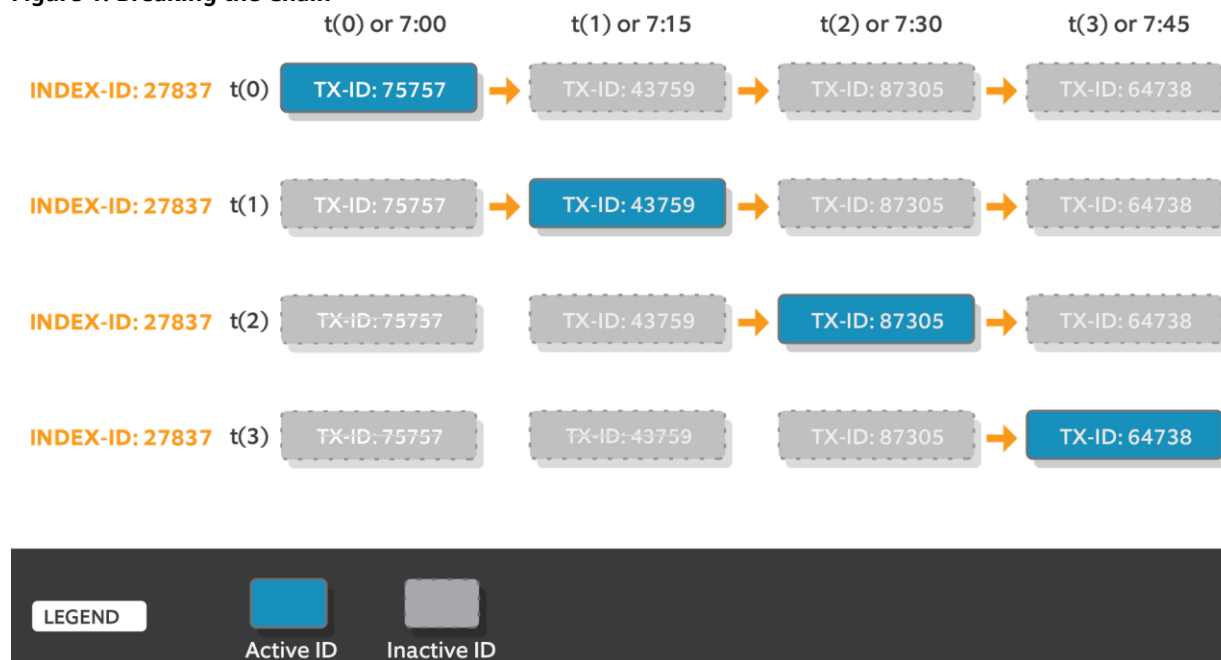
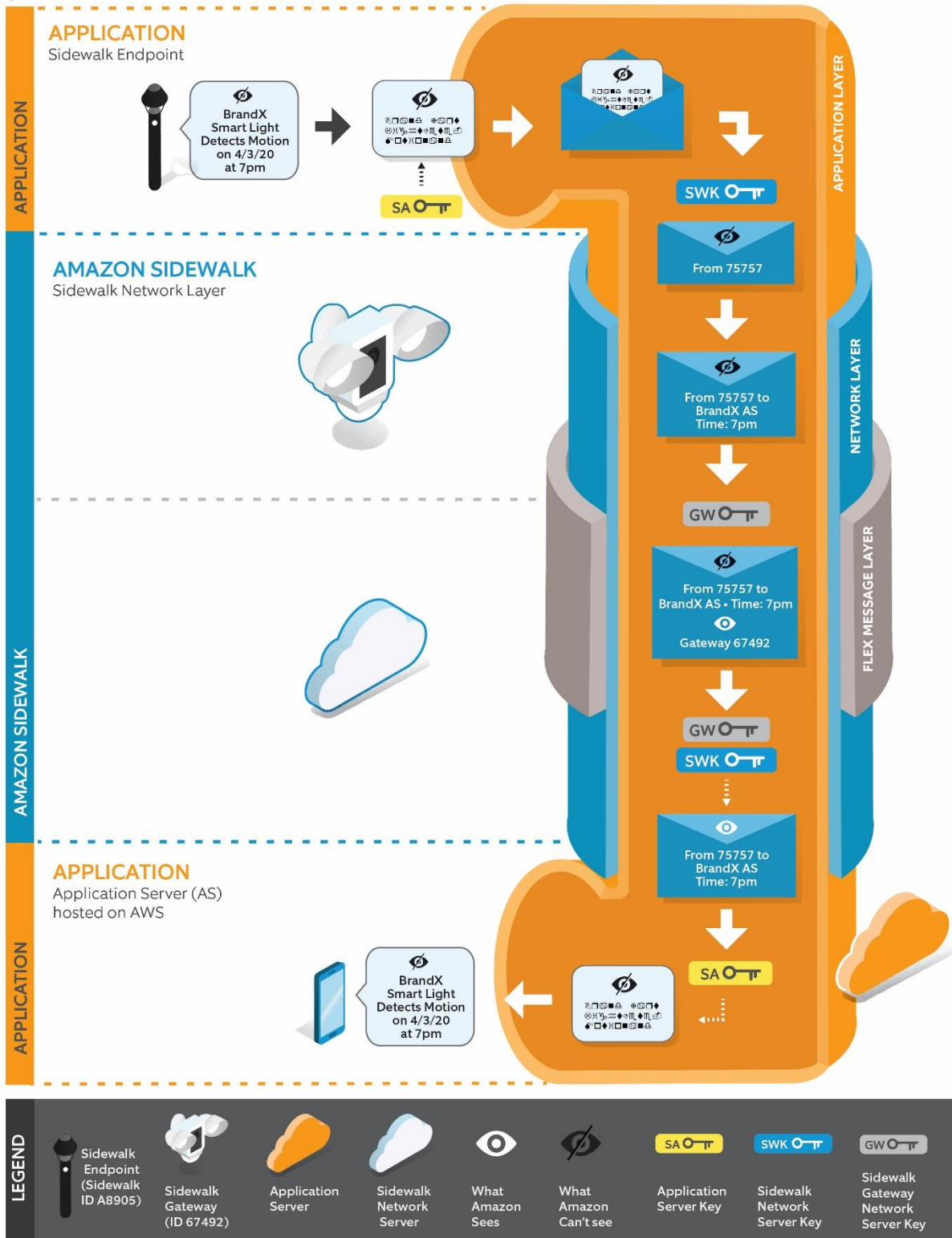

---

## Packet from the Endpoint to the Application Server (Cloud)

Next, we'll walk through the smart light (A8905) sending a packet (motion detected) through Sidewalk to the Application Server.

**Figure 2: Endpoint Packet→Application Server**

The endpoint encrypts the first and second layer before transmitting the packet to Amazon Sidewalk. The first encryption layer encrypts the packet "BrandX smart light detects motion at 7:00 pm on 4/3/2020" using the Application Server Key; only the endpoint and Application Server have access to the endpoint-specific Application Server Key. This yields the Encrypted Application Payload. The second encryption layer encrypts the Encrypted Application Payload and other Sidewalk frame fields using the Amazon Sidewalk Network Server Key; only the endpoint and the Sidewalk Network Server have access to the Sidewalk Network Server Key. This yields the Encrypted Sidewalk Packet.

At this point, the endpoint transmits the Sidewalk packet over the air. The Sidewalk Network Server (SNS) can gather routing information for regular operations (i.e. to forward the packet to the Application Server, network health status, and network bandwidth caps).

The third layer of encryption is performed by the Sidewalk gateway after it receives the Encrypted Sidewalk Packet and before it is transmitted to the SNS. Once the incoming packet is inspected, the Sidewalk gateway creates a Flex message with the Encrypted Sidewalk Packet and encrypts using the Gateway Network Server Key, yielding the Encrypted Flex Message. Only the Sidewalk gateway and the SNS have access to the Gateway Network Server Key.

Once the SNS receives the Encrypted Flex Message, the decryption process begins. The decryption and inspection of the Encrypted Flex Message and the Encrypted Sidewalk Packet is performed by the SNS in the same manner as the encryption process, but in reverse order. The SNS forwards the Encrypted Application Payload to the Application Server, which then decrypts it with its endpoint-specific Application Server Key. The plain-text message can only be seen by the Application Server.

In this example, the Application Server is hosted as a standalone AWS managed service. Access to data that is generated, stored, and flowing within AWS is governed by the Applications' (endpoints') AWS key. The Application Server stores all of its persistent data (device identifiers, authentication material, certificates, and encryption keys) encrypted in databases, and the master encryption key is stored in AWS Key Management Service (KMS). For Sidewalk (provisioning, key derivation, packet encryption/decryption) and AWS (rules-engine) libraries/services to access data, the Application server owner must grant access to Sidewalk/AWS by using KMS grant. If the Application server owner revokes access, Sidewalk and AWS no longer have access to Application resources (endpoint data) and the Application Server and endpoints can no longer operate on the Sidewalk Network. Please refer to AWS Shared Responsibility for more information on shared security for applications hosted on AWS.[3]

### *Packet from the Application Server (Cloud) to the Endpoint*
The encryption example above depicts any type of packet traveling from the endpoint to the Application Server.  The Sidewalk Network Server stores only the routing information from the last packet received, which is how the correct Sidewalk gateway-to-endpoint relationship is maintained for the packet flow we will discuss in Figure 3. In this example, a customer queries the Application Server to turn on their BrandX smart light.

---

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

**Figure 3: Application Server Packet→ Endpoint**
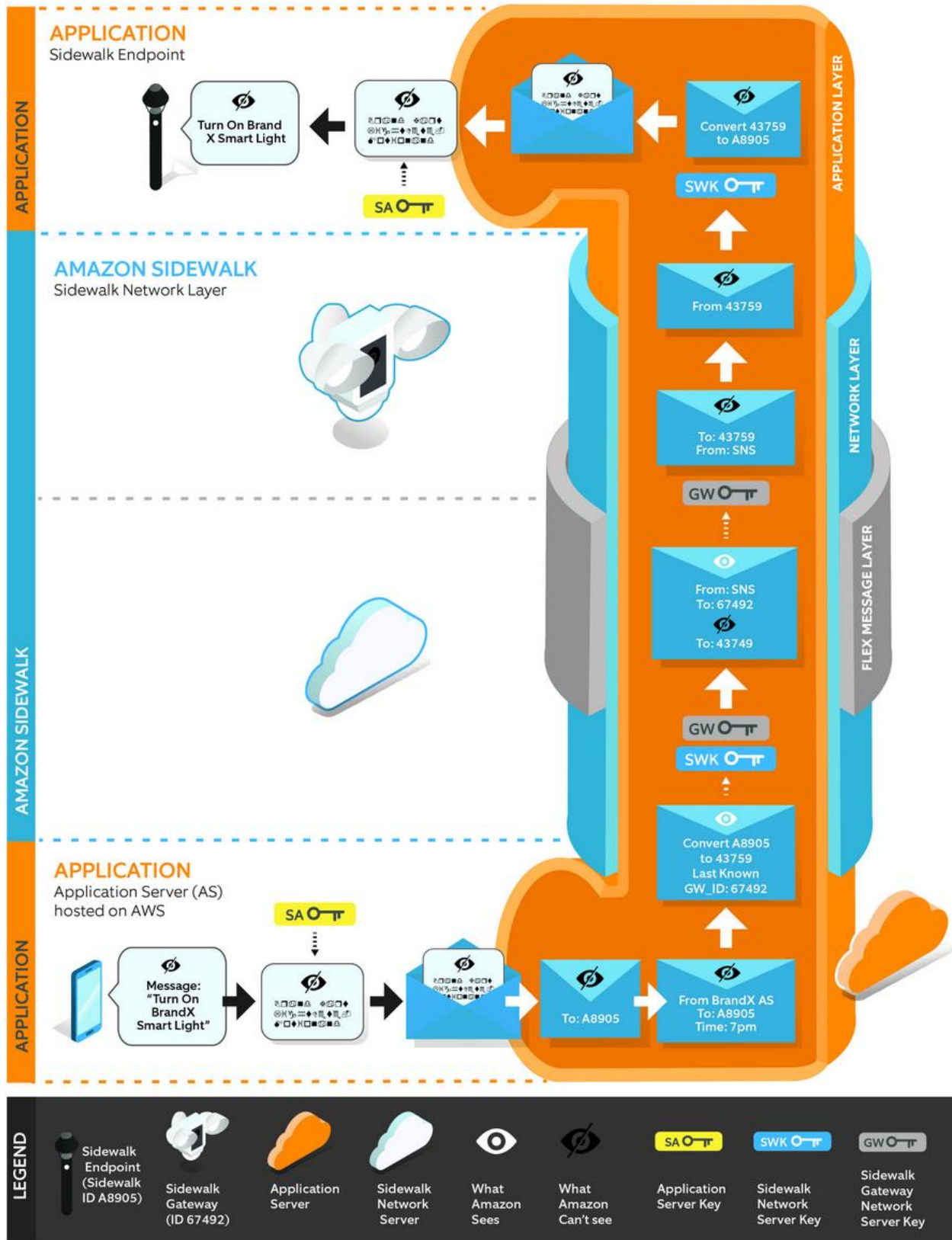
When the customer uses their mobile app to turn on their light, the command is identified by the Sidewalk Device ID (or Sidewalk-ID), which is A8905. The Sidewalk-ID is established during the device manufacturing process, and can be the device serial number for certain devices. The encryption process is similar to the incoming packet described previously, but in reverse order with several nuances. In this example, the Application Server sends a packet destined for a Sidewalk endpoint with the endpoint's Sidewalk-ID as the destination (A8905). The Application Server does not know the transmission-ID (TX-ID) for a given endpoint, so the Sidewalk Network Server must first identify the TX-ID (43759) that is currently associated with the endpoint. This is done by performing a look-up against a table that retains only the previous two TX-IDs. The Sidewalk Network Server then identifies the Gateway-ID (67492) that sent the most recent uplink packet associated with the device, and then sends the packet to that Gateway through the Sidewalk Network Server for delivery to the endpoint. This approach to encryption allows us to deliver information through the Sidewalk network while protecting the privacy of all the parties involved.

## Conclusion

With connectivity support from the community, Amazon Sidewalk improves coverage, provides offline functionality, and enables troubleshooting to improve the smart home experience. By sharing a small portion of their home network bandwidth, neighbors give a little—but get a lot in return. As a crowdsourced capability, security and privacy are foundational principles designed into all aspects of Sidewalk. Amazon Sidewalk is just one of many programs demonstrating Amazon's continued commitment to improving the overall experience of smart devices for our customers.

## Appendix
### *Security & Privacy FAQs*

1. **How does Amazon Sidewalk protect customer information?**
   Preserving customer privacy and security is foundational to how we've built Amazon Sidewalk. Sidewalk is designed with multiple layers of privacy and security to secure data travelling on the network and to keep customers safe and in control. A summary of steps we took to better protect customer information are listed below:
   - We designed Amazon Sidewalk with three layers of encryption to secure data travelling on Sidewalk.
   - We require third-party applications to certify devices (endpoints) to ensure the same encryption standards and to prevent unauthorized access to the contents of packets.
   - The routing information that Amazon does receive for operating the network components of Sidewalk is automatically cleared every 24 hours.
   - We've designed Sidewalk to prevent customers with Sidewalk Gateways from viewing the data from other customers' Sidewalk endpoints—and vice versa.
   - We use one-way hashing keys, cryptographic algorithms and rotating device IDs to dissociate data tied to customers.
   - We set maximum upload limits and bandwidth caps to avoid latency impact for Sidewalk Gateway customers.
   - We provide a feature setting for customers who own a Sidewalk Gateway to be able to choose to disable Amazon Sidewalk at any time.

2. **Will I know what other Sidewalk devices are connected to my devices?**
   Preserving customer privacy and security is foundational to how we've built Amazon Sidewalk. Information transferred over Sidewalk Gateway devices is encrypted and Gateway customers are not able to see that Sidewalk endpoint are connected to their gateway. Customers who own Sidewalk endpoints will know their device is connected to Sidewalk but will not be able to identify which Gateway they are connected to.

3. **How do you ensure data traveling over the network is not tied to customers?**
   One of the tenets when designing Amazon Sidewalk was to limit the amount of information that Amazon would need to receive from 3P endpoints to manage the network. Amazon Sidewalk uses one-way hashing keys, cryptographic algorithms and rotating device IDs to minimize data tied to customers. In addition, routing information that Amazon does receive for operating the network components of Sidewalk is automatically cleared every 24 hours.

4. **How does Amazon maximize privacy while routing messages on Sidewalk?**
   Preserving customer privacy and security is foundational to how we've built Amazon Sidewalk. We've designed Amazon Sidewalk to limit the amount of information that Amazon would need to receive from 3P endpoints to manage the network. While Amazon is not able to see the contents of third-party packets travelling on Sidewalk without permission, Amazon Sidewalk needs to know a third-party Sidewalk-enabled device's serial number to route the message to its respective application server, and the size of the message to ensure bandwidth caps are met and network health is maintained. In the case of first-party Amazon and Ring devices, Amazon has access to additional data needed to maintain application server keys to ensure proper operation of customer devices.

5. **What protections are in place to prevent unauthorized devices from entering the network?**
   All Sidewalk devices are authenticated when joining the Sidewalk network and a symmetric transmission-ID (TX-ID) transmission is required for authorized devices. The network has different levels to deal with unauthorized, or rogue devices:
   - **Sidewalk Gateway (GW) packet inspection**: a received packet by the GW has to pass CRC and Sidewalk format checks.
   - **Random TX-ID Device:** After the GW forwards the packet to the Sidewalk Network Server (SNS), the SNS looks for a TX-ID and Application Server destination ID match in the authorized devices lookup database (DB). If no match is found, the packet is dropped and the SNS generates a "monitor" metric entry for the GW.
     - If a match is found (and is not blocklisted), the SNS attempts to decrypt/authenticate the packet. If the process fails, since the TX-ID is valid, the SNS must attempt to prevent denial of service (DOS) of a device, thus it sends a device-specific CMAC authentication key to the GW and requests the GW to authenticate packets from the device TX-ID prior to uploading. The SNS also sends a packet to the TX-ID device, requesting to use CMAC for packet authentication. This packet will instruct a valid device to change its Network layer algorithm from AES-GCM to AES-CTR + AES-CMAC. The GW will continue dropping packets unless the authentication passes. This mode is valid until the next TX-ID period.
   - **Multiple "Monitor" Entries:** If a GW has multiple "monitor" entries for a TX-ID validity period, the SNS will look at the routing data from that GW and surrounding GWs, and send a safelist of all valid devices. Any packets from new TX-IDs that are not in that safelist are dropped. This is valid until the next TX-ID period.
   - **Re-authentication:** If a Sidewalk endpoint has not re-authenticated, the SNS marks the TX-ID(s) as "re-auth-needed" in the authorized devices lookup DB. If a GW forwards a packet from a re-auth-needed device, the SNS will respond with a "re-authenticate" packet. If no re-auth response is received, any further packets from that TX-ID will be dropped.
   - **Lost Sidewalk Endpoints:** If an endpoint is reported as lost or stolen by the Application Server, the SNS will blocklist the device by marking its entry in the authorized devices lookup DB as "blocklisted". If a packet from a blocklisted TX-ID is received, the SNS drops that packet and responds with a "de-auth" packet to the device, and adds the TX-ID of the device to the GW blacklist to drop the packets.

6. **How is a Sidewalk device registered on the Network?**
   During device registration, a Sidewalk endpoint uses the Sidewalk Handshake protocol to authenticate and establish two unique session encryption keys: (1) Sidewalk Network Server (SNS) session symmetric key, and (2) Sidewalk Application Server session symmetric key. The Sidewalk Handshake protocol is a mutually-authenticated Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) key agreement protocol. It relies on the Sidewalk certificate chain to mutually authenticate each Sidewalk-enabled device (gateway or endpoint), and the SNS.

   The Sidewalk Network Server has two public certificate chains, one for each supported Elliptic Curve (EC): NIST-P256 and ED25519. Each certificate chain is composed of a Root Certificate Authority (CA), and depending on the type of partner engagement, two or three intermediate CAs. A Sidewalk CA also issues the Sidewalk Network Server certificate, while the Application Server can be a self-signed certificate or a certificate signed by Sidewalk CA.

   In addition to the Sidewalk certificate chain, each device is provisioned with a unique, random Sidewalk-ID (A8905), a set of EC public-private key pairs (NIST-P256 and ED25519), and their corresponding signed certificates. Their respective Intermediate Manufacturing CA signs these certificates. Every Sidewalk-enabled device must have all these Sidewalk certificates provisioned to

be able to authenticate its device certificate, and other Sidewalk participant's during device registration.

7. **How does Amazon manage Sidewalk?**
Amazon Sidewalk is a "pipeline" that moves data back and forth between an endpoint and its respective application server. In addition to security and privacy, a third key area of focus during these transmissions is network optimization. Sidewalk supports multiple protocols for endpoints to communicate with a gateway, including 900 MHz (LoRa and FSK) and BLE. To optimize the network, Sidewalk allows an endpoint to "find" the best solution given the radios it supports. For example, let's take an endpoint that has LoRa and BLE onboard. While it communicates primarily on LoRa for longer range, when in range of a BLE gateway, the endpoint can switch to BLE (which required less power) to preserve battery life.

An important role Amazon plays when managing the network, is to ensure no single gateway becomes overburdened with Amazon Sidewalk traffic. The maximum bandwidth of a Sidewalk Bridge to the Sidewalk server is 80Kbps, which is about 1/40th of the bandwidth used to stream a typical high definition video. Today, total monthly data used by Sidewalk enabled-devices, per customer, is capped at 500MB, which is equivalent to streaming about 10 minutes of high definition video.

8. **Is it possible for customers on Sidewalk to use signals to pinpoint the location of other devices and users?**
Just like your wifi router, it's possible to look at signals to try to triangulate the location of a device on the Sidewalk network. However, we've designed Amazon Sidewalk with encryption and other security protocols to protect against the disclosure of our customers' private information and any sensitive data that may be transmitted using Sidewalk.

9. **What data can law enforcement access via subpoena?**
Amazon knows customers care deeply about privacy and data security. We optimize our work to get the issues right for customers. Amazon does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order. We routinely object to overly broad requests by law enforcement. Our data minimization policies and encryption policies reduce the scope and usefulness of data that we would be able to produce if legally required.

10. **How do you hold application (endpoint) developers accountable to ensure customers stay protected in the Sidewalk ecosystem?**
At launch we won't have any third-party applications running on Sidewalk. We'll have terms of service for third-party Sidewalk device developers. If the developers violate those terms, we'll respond appropriately, including terminating their access, if necessary. Third-party devices that won't honor our terms won't be allowed on Sidewalk.

11. **What data will application developers get from Amazon Sidewalk?**
Amazon Sidewalk won't support third-party devices immediately at launch, but we will make careful choices about the information they receive from Sidewalk. We'll have more details in the future.