Amazon Sidewalk Privacy and Security Whitepaper

Contents

Amazon Sidewalk Privacy and Security Whitepaper

Last updated March 2023

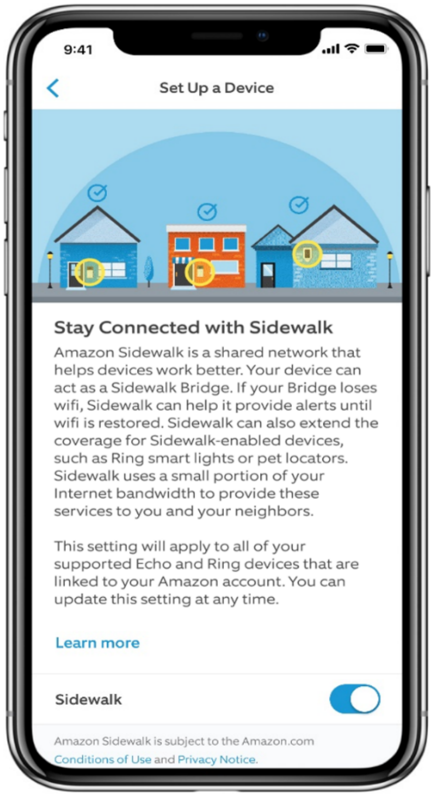
This paper, which serves as an overview of Amazon Sidewalk security features, was originally published in 2020. We will update this paper from time to time to reflect the continuous improvements we make to delight customers, such as strengthening protections, optimizing performance, and increasing resilience.

Introduction

Amazon Sidewalk (Sidewalk) is a shared network developed by Amazon to allow third-party developers to create and bring to market all types of consumer, enterprise, and public sector smart and connected devices and services. This paper serves as an overview of Sidewalk privacy and security features, including data minimization, encryption, and more.

Customers with an Amazon device that works as a Sidewalk Gateway, also known as a Sidewalk Bridge, can contribute a small portion of their internet bandwidth to be pooled together to create a network that benefits all Sidewalk-enabled devices in a community. This can include experiences like finding pets or valuables that may be lost, improving reliability for devices like leak sensors or smart lighting, or running 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 use 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 determine participation in the neighborhood network. When customers complete setup on a Sidewalk Gateway device (or when an existing device becomes Sidewalk capable) for the first time, they will be asked whether they want to join the network[2].



Stay Connected with Sidewalk

Amazon Sidewalk is a shared network that helps devices work better. Your device can act as a Sidewalk Bridge. If your Bridge loses wifi, Sidewalk can help it provide alerts until wifi is restored. Sidewalk can also extend the coverage for Sidewalk-enabled devices, such as Ring smart lights or pet locators. Sidewalk uses a small portion of your Internet bandwidth to provide these services to you and your neighbors.

This setting will apply to all of your supported Echo and Ring devices that are linked to your Amazon account. You can update this setting at any time.

Sidewalk: on

Amazon Sidewalk is subject to the Amazon.com Conditions of Use and Privacy Notice.

Figure 1

As a crowdsourced, community benefit, Sidewalk is only as powerful as the trust our customers place in us to safeguard customer data. To that end, this paper outlines the steps we have taken to secure the

[1] The maximum bandwidth of a Sidewalk Gateway to the Sidewalk Network 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 is capped at 500MB for one customer, which is equivalent to streaming about 10 minutes of high-definition video.

[2] For customers who had already set up Sidewalk Gateway devices at the time Sidewalk was initially launched, an Over-The-Air (OTA) update connected the devices to the network. These customers received email notifications prior to the pending update and instructions for how to turn it off, if that was their choice. Sidewalk will also be turned on for customers who do not complete setup, unless they have previously turned off the setting.

network and maintain customer privacy. These efforts are core to our mission and will continue to evolve and improve over time.

Overview

This paper provides information about two areas of interest to Sidewalk users: 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.

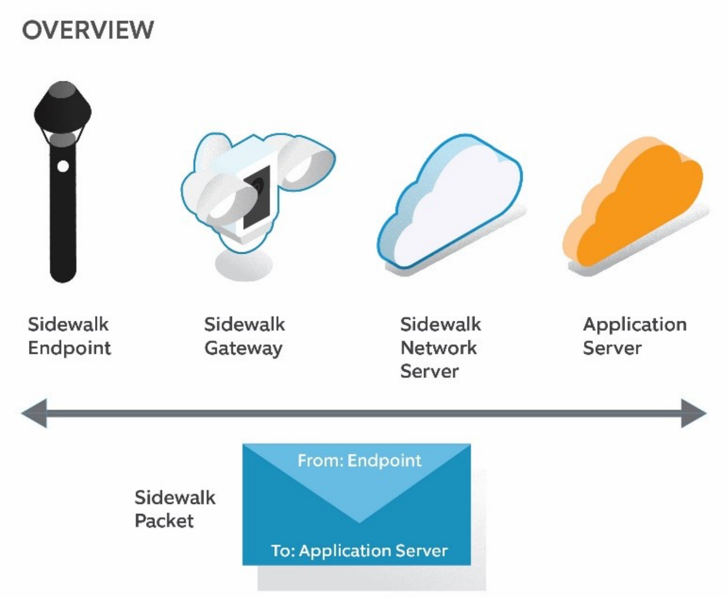


Figure 2

Sidewalk Gateways (also known as Sidewalk Bridges or GWs) forward packets to/from the Sidewalk Endpoints and the Sidewalk Network Server. GWs 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 a connection to Sidewalk.

Sidewalk Endpoints (also known as Sidewalk-enabled devices, edge devices, Endpoints, or Applications) can roam on the Sidewalk network by connecting to GWs. Endpoints are low-bandwidth/low-power smart products such as leak sensors, door locks, lights, or devices users can attach to valuables or a pet to know where it is. Sidewalk Endpoints can be built and maintained by Amazon or third-party developers. GWs can also act as an Endpoint and receive Sidewalk benefits like maintaining functionality when the device falls offline.

The **Sidewalk Network Server** is the backbone of Sidewalk. 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), and keeping the network time-synchronized. The Sidewalk Network Server 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 third party.

Packets (also known as messages) are sent to (from) the Sidewalk Endpoints from (to) the Application Server (through the GW and Sidewalk Network Server). Similar to a letter in the mail, the letter inside the envelope (or packet) contains information needed to perform a service (for example, the command, “Turn on light.”) Like the post office, the Sidewalk Network Server reads the routing information on the outside of the envelope to direct the packet to the correct Endpoint and Application Server.

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 GW to route the Endpoint's packets on the network. Sidewalk also tracks a GW's usage to ensure bandwidth caps are not exceeded and network congestion 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 GWs 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 GW information. The Sidewalk Network Server changes transmission IDs (TX-IDs) every 15 minutes to help prevent the tracking of 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 GW, 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 (GW-ID)** to select the appropriate GW needed to relay the packet
- **Application Server** to route the packet from the Endpoint to its respective cloud destination

The Sidewalk Network Server does not know the contents of the application layer packets or commands being sent over Sidewalk. In addition to the Sidewalk Network Server, 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 (such as 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 the GW and GW owner. The GW information is encrypted behind the Sidewalk Network Layer and Flex Layer, which are defined in the next section of this paper.
- **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, which is defined in the next section of this paper.
- **Application Server:** The Application Server is unable to see any information pertaining to the GW owner; it just sees the Endpoint information. The GW-ID and GW information are 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 AWS Key Management Service (AWS KMS). This data is generally used in AWS for storage, processing, and other services the Application Server uses.

Encryption

Packets traversing Sidewalk have multiple layers of encryption to ensure data is visible only to the intended party. This approach to encryption means that the Sidewalk Network Server will not be able to interpret the contents of commands or messages sent through Sidewalk by third-party services or Endpoints (applications). For additional details on encryption methods, see the *Sidewalk Security* section. These layers include:

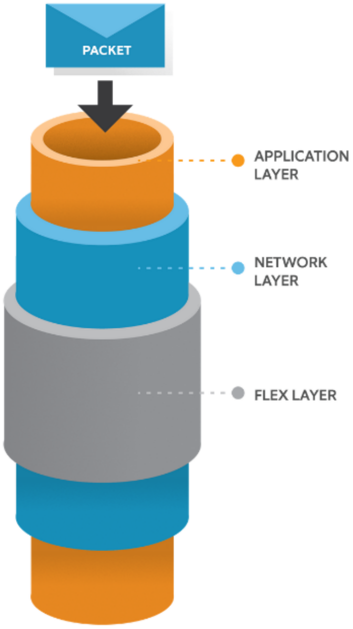


Figure 3

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.
3. The ***Flex Layer***, which is added by the GW, provides the Sidewalk Network Server 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 Sidewalk Network Server. When transmitting GW information over 900 MHZ, Flex Layer and Transport Layer Security (TLS) encryption are used. When transmitting over BLE, TLS encryption is used.

Trusted Device Identities

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

Sidewalk Security

Preserving customer privacy and security is foundational to the design of Amazon products and services, and Sidewalk provides multiple layers of privacy and security to help secure data travelling on the network. The Sidewalk security model is designed to authenticate the identity of all network participants, and to provide authenticity and confidentiality for data traversing the network. This helps to ensure that only the authorized, intended receivers have access to the device application data, and to ensure a 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 registration process on Sidewalk, it must authenticate its identity and establish a unique session key with the Sidewalk Network Server and Application Server. Upon identity authentication, the Sidewalk Network Server assigns a unique Sidewalk Device ID (Sidewalk-ID) and a database (DB) record containing the following elements: (1) Sidewalk-ID, (2) unique session key, (3) TX generation key, and (4) TX-ID (75757). Next, the Sidewalk Network Server adds this record to its lookup DB of authenticated devices, and forwards the association Sidewalk-ID match to the Application Server.

The Sidewalk Network Server makes it difficult for an external attacker to piece together activity history over time. One of the ways it does this is by changing the TX-ID every 15 minutes to a different unique identifier (*see Figure 4*). For example, the TX-ID is 75757 at *t(0)* or 7:00, and 43759 at t(1) or 7:15. For latency considerations, multiple codes are generated at *t(0)*, each representing a 15 minute interval.

Sidewalk limits the ability to work backwards through a trail of old IDs linked to the original device by periodically flushing the previous IDs. The Sidewalk Network Server stores the packet metadata for one minute, and the packet routing information for 24 hours[3]. The TX-ID is matched to the Sidewalk-ID in the Sidewalk Network Server, and the Application Server receives packets using the Sidewalk-ID as a device identifier[4]. Sidewalk regularly rotates the unique Sidewalk Network Server session key to provide forward secrecy of derived key material, which includes the key used for TX-ID generation.

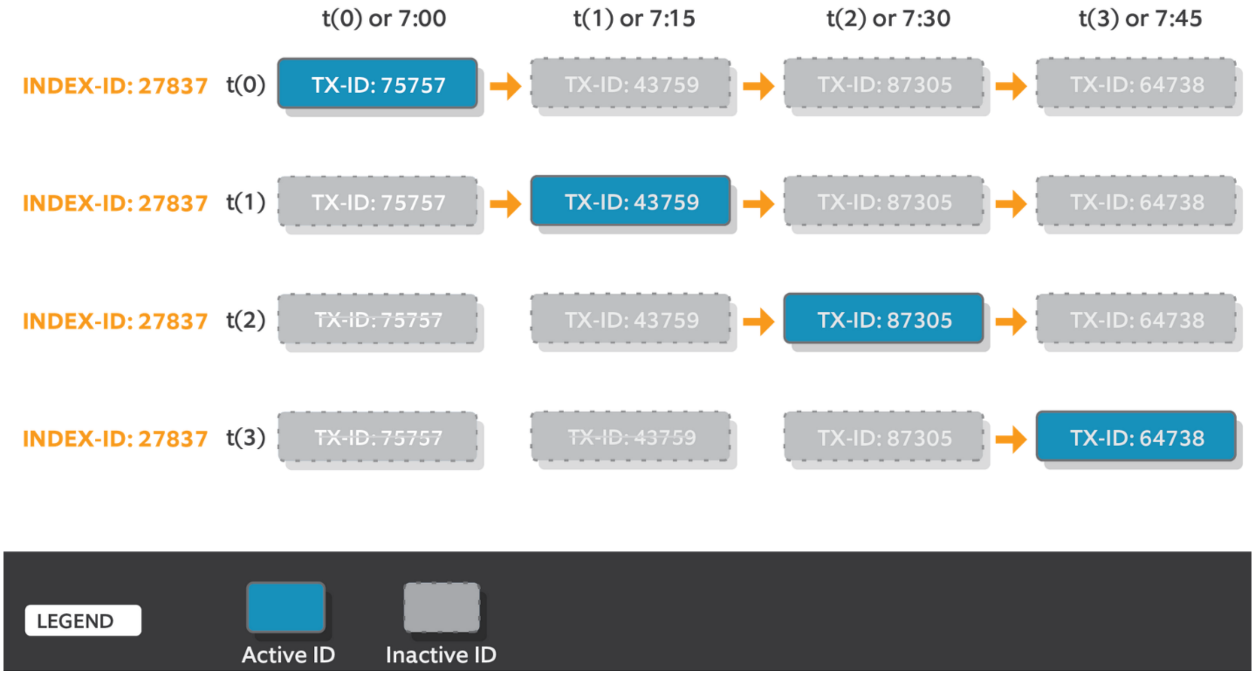


Figure 4: TX-ID Generation

[3] Third-party Sidewalk device manufacturers may maintain their own logs that are subject to their respective retention periods and privacy notices.

[4] In some instances, other device identifiers may be used. Sidewalk-ID is used throughout this paper for simplicity.

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 over 900 MHz.

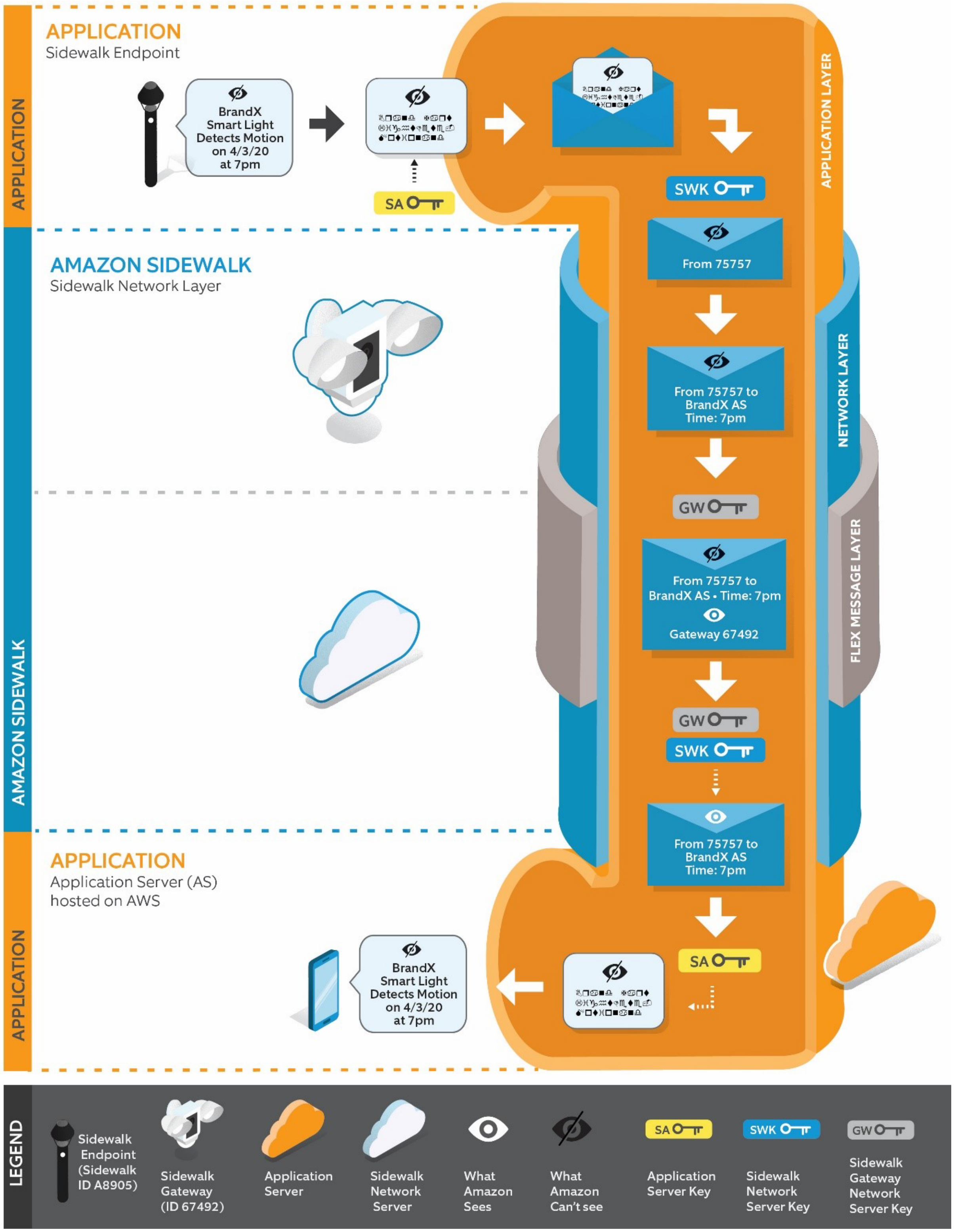

APPLICATION
APPLICATION
Sidewalk Endpoint
BrandX Smart Light Detects Motion on 4/3/20 at 7pm
SA
APPLICATION LAYER
SWK
From 75757
AMAZON SIDEWALK
AMAZON SIDEWALK
Sidewalk Network Layer
From 75757 to BrandX AS Time: 7pm
NETWORK LAYER
GW
From 75757 to BrandX AS • Time: 7pm
Gateway 67492
FLEX MESSAGE LAYER
GW
SWK
From 75757 to BrandX AS Time: 7pm
APPLICATION
APPLICATION
Application Server (AS) hosted on AWS
SA
BrandX Smart Light Detects Motion on 4/3/20 at 7pm
LEGEND
Sidewalk Endpoint (Sidewalk ID A8905)
Sidewalk Gateway (ID 67492)
Application Server
Sidewalk Network Server
What Amazon Sees
What Amazon Can't see
SA
Application Server Key
SWK
Sidewalk Network Server Key
GW
Sidewalk Gateway Network Server Key

Figure 5: Endpoint Packet to Application Server

The Endpoint encrypts the first and second layer before transmitting the packet to 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 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 Encrypted Sidewalk Packet over the air. The Sidewalk Network Server can gather routing information for regular operations (such as to forward the packet to the Application Server, network health status, and network bandwidth caps).

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

Once the Sidewalk Network Server 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 Sidewalk Network Server in the same manner as the encryption process, but in reverse order. The Sidewalk Network Server 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 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 a grant in KMS. 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 Sidewalk. Please refer to AWS Shared Responsibility Model for more information on shared security for applications hosted on AWS.

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 the routing information from the packet(s) received, which is how the correct GW-to-Endpoint relationship is maintained for the packet flow we will discuss in Figure 6. In this example, a customer queries the Application Server to turn on their BrandX smart light over 900 MHz.

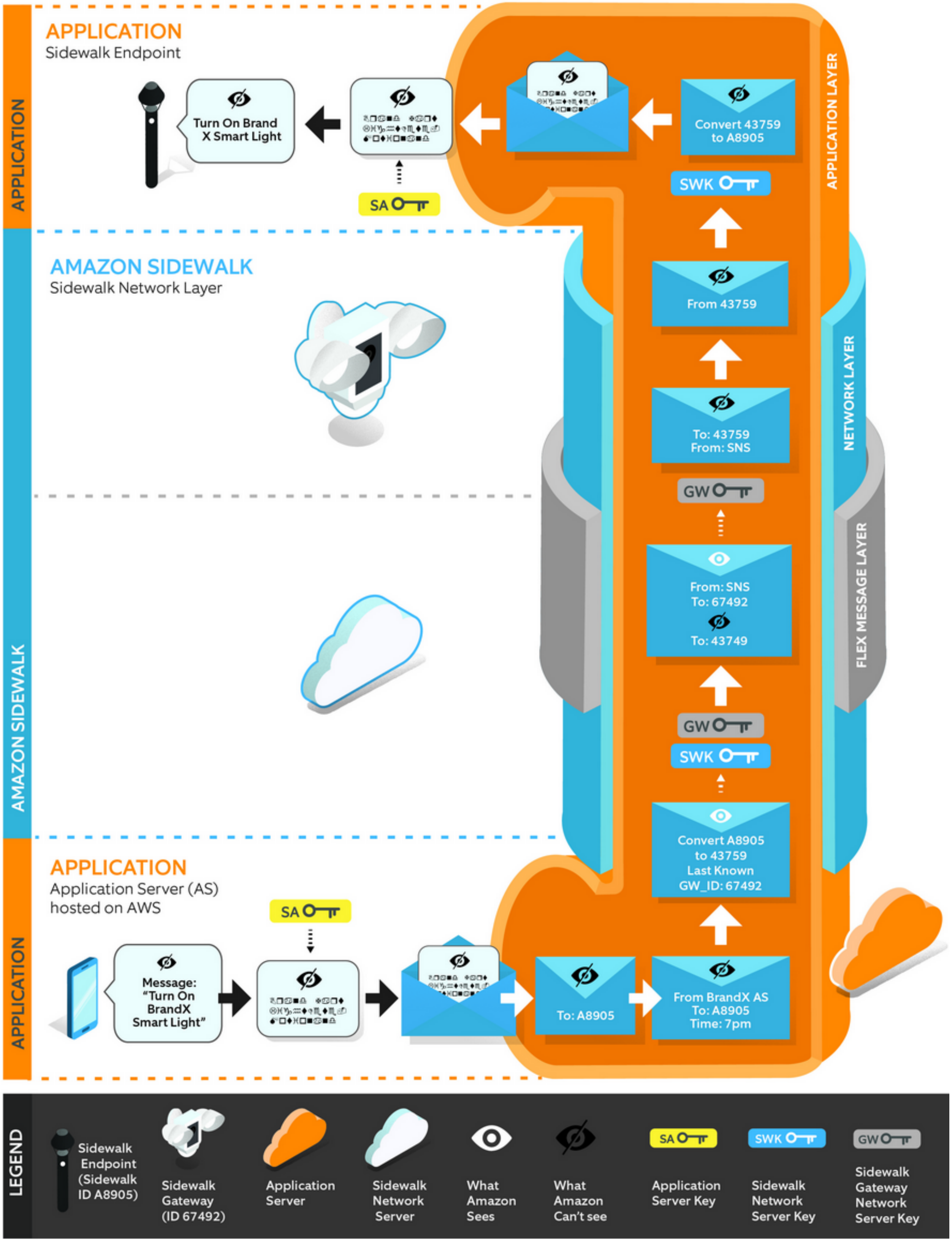


Figure 6: Application Server Packet to Endpoint

When the customer uses their mobile app to turn on their light, the command is identified by the Sidewalk-ID A8905. The Sidewalk-ID is established during the device manufacturing process, and can be the 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 an Endpoint with the Endpoint's Sidewalk-ID as the destination (A8905). The Application Server does not know the 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 check against a look-up table that erases stale data, such as TX-IDs[5]. The Sidewalk Network Server then identifies the GW-ID (67492) that sent the most recent uplink packet associated with the device, and then sends the packet to that GW through the Sidewalk Network Server for delivery to the Endpoint. This approach to encryption allows us to deliver information through Sidewalk while protecting the privacy of all the parties involved.

Tile and Sidewalk

Tile uses its own communication protocol to communicate with Sidewalk GWs. The data is routed to/from Tile Cloud through Sidewalk's cloud services infrastructure. The specifics of the communication protocol, such as the authentication scheme and precise encryption practices, may differ in certain respects from Sidewalk's protocol.

Conclusion

With connectivity support from the community, Sidewalk improves coverage, provides offline functionality, and improves 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. Sidewalk is just one of many programs demonstrating Amazon's continued commitment to improving the overall experience of smart devices for our customers.

[5] Depending on the size and activity level of a table, the actual delete operation of an expired item can vary. Because time to live (TTL) is meant to be a background process, the nature of the capacity used to expire and delete items through TTL is variable. For more information on DynamoDB TTL, visit the AWS Developer Guide: https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/howitworks-ttl.html.

Appendix

Security & Privacy FAQs

1. How does Sidewalk protect customer information?

Preserving customer privacy and security is foundational to how we've built Sidewalk. Sidewalk is designed with multiple layers of privacy and security to help secure data traveling on the network. A summary of steps we took to better protect customer information are listed below:

- We designed Sidewalk with multiple layers of encryption to secure data traveling on Sidewalk.
- For device platforms that seek to use the Sidewalk protocol, we certify that they conform to the Sidewalk protocol and specification.
- The routing information that Amazon receives for operating the network components of Sidewalk is automatically cleared every 24 hours[6].
- We've designed Sidewalk to prevent customers with GWs from viewing the data from other customers' Sidewalk Endpoints—and the reverse.
- We use one-way hashing keys, cryptographic algorithms, and rotating device IDs to minimize data tied to customers.
- We set maximum upload limits and bandwidth caps to avoid network congestion impacts for GW customers.
- We provide a feature setting for customers who own a GW to be able to choose to turn off 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 Sidewalk. Information transferred over GWs is encrypted and GW customers are not able to see that particular Endpoints are connected to their GW. Customers who own Endpoints will know their device is connected to Sidewalk, but will not be able to identify which GW 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 Sidewalk was to limit the amount of information that Amazon would need to receive from third-party Endpoints to manage the network. 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.

[6] Third-party Sidewalk device manufacturers may maintain their own logs that are subject to their respective retention periods and privacy notices.

4. How does Amazon maximize privacy while routing messages on Sidewalk?

Preserving customer privacy and security is foundational to how we've built Sidewalk. We've designed Sidewalk to limit the amount of information that Amazon would need to receive from third-party Endpoints to manage the network. While the Sidewalk Network Server is not able to see the contents of third-party packets travelling on Sidewalk, 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 Sidewalk and a symmetric TX-ID transmission is required for authorized devices. The network has different methods to manage unauthorized or rogue devices:

- **Sidewalk GW packet inspection**: a received packet by the GW must pass Cyclic Redundancy Checks (CRC) and Sidewalk format checks.
- **Rotating TX-ID:** After the GW forwards the packet to the Sidewalk Network Server, the Sidewalk Network Server 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 Sidewalk Network Server generates a “monitor” metric entry for the GW.
    - If a match is found (and is not blocklisted), the Sidewalk Network Server attempts to decrypt/authenticate the packet. If the process fails, since the TX-ID is valid, the Sidewalk Network Server must attempt to prevent denial-of-service (DoS) of a device, so it sends a device-specific Cipher-based Message Authentication Code (CMAC) authentication key to the GW and requests the GW to authenticate packets from the device TX-ID prior to uploading. The Sidewalk Network Server 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 Sidewalk Network Server 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 Sidewalk Network Server 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 Sidewalk Network Server 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 Sidewalk Network Server 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 Sidewalk Network Server drops that packet and responds with a "de-auth" packet to the device, and adds the TX-ID of the device to the GW blocklist to drop the packets.

6. How is a Sidewalk device registered on the Network?

During device registration, an Endpoint uses the Sidewalk Handshake Protocol to authenticate and establish two unique session encryption keys: (1) Sidewalk Network Server session symmetric key, and (2) Sidewalk Application Server session symmetric key. The Sidewalk Handshake Protocol is a mutually-authenticated Ephemeral Elliptic Curve Diffie-Hellman Key Agreement Protocol. It relies on the Sidewalk certificate chain to mutually authenticate each Sidewalk-enabled device (GW or Endpoint), and the Sidewalk Network Server.

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, a set of EC public-private key pairs (NIST-P256 and ED25519), and their corresponding signed certificates. Their respective intermediate 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 participants during device registration.

7. How does Amazon manage Sidewalk?

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 GW, 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 requires less power) to preserve battery life.

An important role Amazon plays when managing the network is to ensure no single GW becomes overburdened with Sidewalk traffic. The current maximum bandwidth of a GW to the Sidewalk Network 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 is capped at 500MB for one customer, 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 Wi-Fi router, it's possible to look at signals to try to triangulate the location of a device on Sidewalk. However, we've designed Sidewalk with encryption and other security protocols to help protect against the disclosure of our customers' private information and any sensitive data that may be transmitted using Sidewalk.

9. What is Amazon's approach to law enforcement requests?

Amazon knows customers care deeply about privacy and data security, and 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. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course. Amazon reserves the right to respond immediately to urgent law enforcement requests for information in cases involving a threat to public safety or risk of harm to any person. For more information see Amazon's Law Enforcement Information Requests page.

10. How do you hold application developers accountable to ensure customers stay protected on Sidewalk?

To protect customer data, if a third party fails to act in good faith, Sidewalk's Public Key Infrastructure and access management controls provide the ability to revoke specific devices or an entire product line until the security issues are addressed.

11. What data will application developers get from Sidewalk?

Third parties are only able to receive application data generated by their devices. Sidewalk network content is stripped from messages before being delivered to third-party applications. Because third parties are responsible for managing all application keys negotiated between third-party devices and their applications, Sidewalk Network Server does not have access to messages shared between third-party devices and their applications.

12. How do I turn Amazon Sidewalk on or off?

Customers can turn Sidewalk on or off at any time from Account Settings in the Ring or Alexa app. This setting will apply to all applicable Echo and Ring devices linked to the customer's account. When customers complete setup on a Sidewalk Gateway device (or when an existing device becomes Sidewalk capable) for the first time, they will be asked whether they want to join the network. For customers who had already set up Sidewalk Gateway devices at the time Sidewalk was initially launched, an Over-The-Air (OTA) update connected the devices to the network. These customers received email notifications prior to the pending update and instructions for how to turn it off, if that was their choice. Sidewalk will also be turned on for customers who do not complete setup, unless they have previously turned off the setting.

13. If I turn off Amazon Sidewalk, will my Sidewalk Bridges still work?

Yes. All of your Sidewalk Bridges will continue to have their original functionality even if you decide to turn off Amazon Sidewalk. However, turning it off means missing out on Sidewalk's connectivity and location related benefits. You also will no longer contribute your internet bandwidth to support community extended coverage benefits such as locating pets and valuables with Sidewalk-enabled devices.