End-to-End Encryption

January 2021

Notices

Table of Contents

Purpose: This whitepaper provides an intermediate-level technical overview of Ring's new video End-to-End Encryption (E2EE) feature.

I. Introduction

At Ring, security, privacy, and user control are foundational. With the launch of End-to-End Encryption (E2EE) for Ring, we release this whitepaper to provide a technical overview of the feature. E2EE will be available starting on January 11, 2021 as a new setting in the Ring mobile application (within Control Center) on compatible Android and iOS devices.

E2EE is the latest in the evolution of Ring's security and privacy features. In January 2020, we launched Control Center, a dashboard where users can view and manage important security and privacy settings. Then, in February 2020, we were the first in the smart home security industry to require Two-Step Verification for all user sign-ins. In November 2020, we launched Compromised Password Checks[1] when a user signs into their Ring account. With this feature, login credentials are checked against a list of known compromised passwords published by third-party (non-Ring) sources, and customers are notified to change their passwords.

With security and privacy at the forefront, E2EE empowers users with added protection over their videos through enhanced opt-in video encryption that is backed by features designed to prevent unauthorized access. E2EE gives users control and additional choices for encrypting and decrypting their videos and is designed so that no unauthorized third party can access user video content. This additional security- and privacy-centric feature works with Ring's core functionality, providing users with even more peace of mind. While our current security and privacy features meet the needs of the majority of our customers, Ring regularly collects feedback to design and add layers of security and privacy – like E2EE – to our products and services. E2EE demonstrates our commitment to providing new security- and privacy-centric features that delight our customers.

Security and privacy assurance with existing encryption capabilities

Users have, and continue to benefit from, Ring's default security and privacy practices and capabilities. These include systems and services that have been through rigorous penetration testing, mandatory Two-Step Verification for user sign-in, and automatically encrypted user videos both in storage (encryption at rest) and in transmission (encryption in transit).

Strict security controls, including the principle of least privilege and role-based access restrictions, are also in place to help prevent unintended access to customer videos by employees or services. With these protections in place, users can feel assured that existing defense-in-depth capabilities help prevent unauthorized access to user videos even without E2EE enabled.

II. Encryption and Defense-in-Depth Security with Ring

From its inception, Ring has focused on building services and features to a high security and privacy bar to continuously improve our defense-in-depth[2] capabilities. This includes existing safeguards like video encryption in transit and at rest, and implementing cryptographic protocols that authenticate data

[1] https://support.ring.com/hc/en-us/articles/360050453111-How-Ring-protects-your-accounts-from-a-third-party-non-Ring-data-breach
[2] Defense-in-depth is an approach that layers a series of security mechanisms so no one failure compromises a system.

transfer between servers, systems, applications, and users, such as Transport Layer Security (TLS) and Secure Real-Time Protocol (SRTP). Ring also uses enhanced account security measures, such as mandatory Two-Step Verification for user sign-ins, and user-controlled video storage time limits. Encryption is a critical component of a defense-in-depth strategy. Our existing encryption capabilities reflect home security industry best practices and satisfy many use cases. While Ring's existing default security practices and encryption capabilities for videos will continue, E2EE adds an enhanced security and privacy option for users who enable this feature.

Ring's E2EE is founded on the premise that no party other than the receiving device (i.e., user's mobile device) can decrypt the encrypted video content from the sending device (i.e., Ring camera). This E2EE foundation is supported by three principles: 1) Users fully control E2EE, 2) Encryption and decryption are performed securely on the user's enrolled Ring and mobile devices, and 3) E2EE is designed so that no unauthorized third party can access user video content.

E2EE's enhanced security and privacy feature requires some functionality trade-off as certain capabilities require processing and analysis of decrypted video content. For instance, applying computer vision to video content cannot be performed if the content is encrypted – any Ring cloud service that needs to decrypt videos for processing will not work.[3] Therefore, features such as Motion Verification and People-Only Mode will be disabled.[4] Some of our users prefer the functionality trade-off for enhanced security and privacy. Others prioritize performance of our full feature set. To meet this range of needs, E2EE is an additional privacy-centric option we want to put in the hands of our users to further empower them to customize security settings based on personal needs and preferences.

The effectiveness of E2EE relies on the security of two important user controls: security of the mobile device and confidentiality of the E2EE passphrase (i.e., not sharing passwords). We built E2EE so that users can enable this encryption feature at any time and control who can view their videos while still being able to use core functionality, such as video streaming.[5] Ring and the user continue to maintain a strong partnership to secure user videos. Ring protects our cloud services, which include our infrastructure and software services (i.e., compute, storage, database, networking); applies security by design into our services, apps, and devices; and offers new security features like E2EE. Users secure their mobile devices by implementing best practices such as device locking.[6] The additional layers of security the user manages can vary, however, depending on the features they select. Users can rely on Ring's default security controls and features or shift more control to their own devices by enabling E2EE.

E2EE is designed to balance security, performance, and device compatibility. Ring users with compatible devices noted in Table 1 and supported mobile operating systems (OSes) noted in Table 2 will be able to turn on E2EE.

[3] Also, turning on E2EE will not encrypt any videos created before E2EE enrollment – the service only encrypts videos created after enrollment.
[4] Refer to https://support.ring.com/hc/en-us/articles/360046520692 for a list of Ring cameras and mobile devices that support E2EE and https://support.ring.com/hc/en-us/articles/360046520812 for more information on deactivated features when enrolled in E2EE and how to re-enable them.
[5] Live View, which decrypts video only on the user's enrolled mobile device, will continue to operate when E2EE is enabled.
[6] See International Standards Organization (ISO) 27001:2013 A.6.2.1 Mobile Device Policy which recommends setting a passcode to unlock a device. Also refer to your mobile device manufacturer's security best practices and guidance. Also see https://support.ring.com/hc/en-us/articles/360037591452-Keeping-Your-Ring-Account-Secure.

Table 1: Compatible Ring devices with E2EE

Ring Device	Compatible	Not Compatible	Available
Video Doorbell Pro	X		2016-Present
Video Doorbell Elite	X		2017-Present
Floodlight Cam	X		2017-Present
Spotlight Cam Wired	X		2019-Present
Spotlight Cam Mount	X		2017-Present
Stick Up Cam Plug-In	X		2019-Present
Stick Up Cam Elite	X		2018-Present
Indoor Cam	X		2019-Present
Doorbot		X	2012-2014
Video Doorbell (1st Gen)		X	2014-2020
Video Doorbell (2nd Gen)		X	2020-Present
Stick Up Cam Battery		X	2018-2020
Stick Up Cam Solar		X	2018-Present
Spotlight Cam Battery		X	2017-Present
Spotlight Cam Solar		X	2017-Present
Peephole Cam		X	2019-Present
Video Doorbell 2		X	2017-2020
Video Doorbell 3		X	2020-Present
Video Doorbell 3 Plus		X	2020-Present

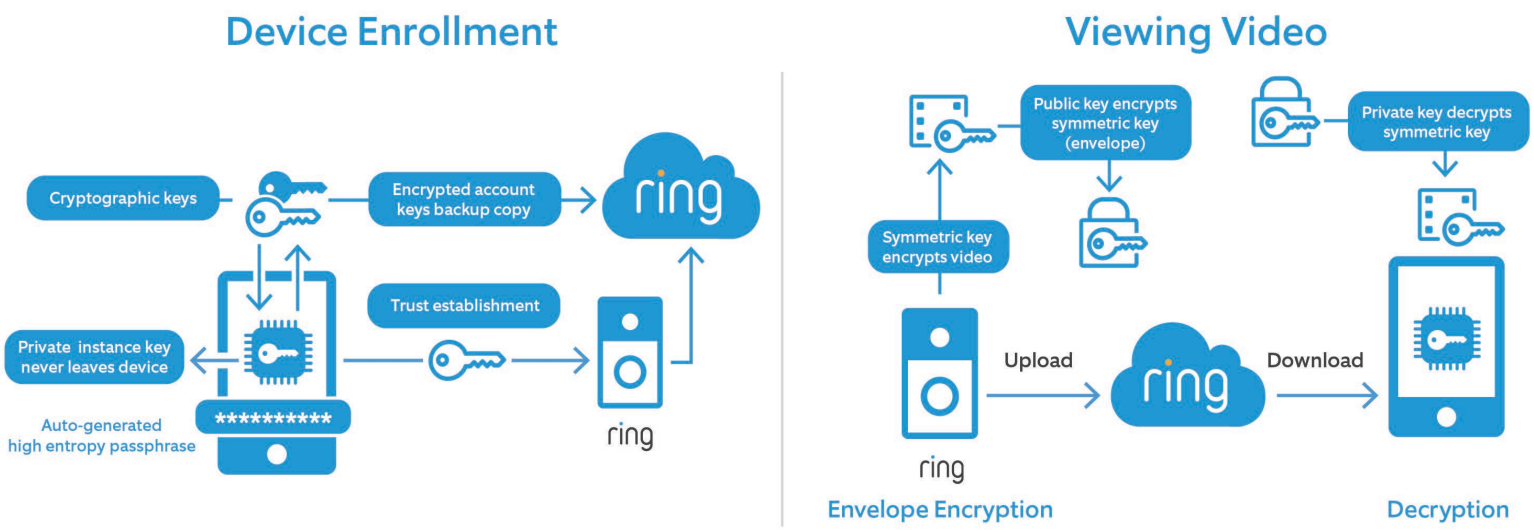
Table 2: Mobile OSes that support Ring E2EE

Mobile OS	Supports E2EE	Does not support E2EE
Apple iOS [12.0] and above	X	
Android OS [8.0] and above	X	
Apple iOS [11.4.1] and below		X
Android OS [7.1.2] and below		X

III. How the Technology Works: End-to-End Encryption (E2EE)

This section describes how Ring E2EE uses multiple cryptographic techniques to maintain security and performance for our users. Ring's E2EE technology implements a series of security best practices, including auto-generated high-entropy passphrases, envelope encryption, and secure key exchange, among others. The section will outline the technical fundamentals of Ring E2EE and how they are used across three main aspects of the design. The first is enrolling the user's mobile device– this process generates a high entropy passphrase and cryptographic key pairs locally on the mobile device. The next focus area is enrolling a Ring device– this is done through a setup mode that creates a direct local Wi-Fi connection between the Ring device and the user's mobile phone where cryptographic keys and identity certificates are exchanged to establish trust. The final aspect is the encryption and decryption of video between enrolled devices.

Diagram 1- End-to-End Encryption Overview



Before diving into device enrollment and video viewing, the following are key terms for E2EE encryption components.

Cryptographic key types

- Symmetric key encryption – Cryptography that uses the same key for encryption and decryption. This technique typically provides performance and efficiency for cryptographic functions.

- Asymmetric key encryption – Cryptography that relies on using a key pair - a public key and a private key. The public key is used to encrypt and the private key to decrypt. In some schemes, the key pairs can be used for digital signing and validation. These asymmetric keys are cryptographically linked to allow this operation. The benefit of asymmetric encryption is that it allows for the safe distribution of keys for encryption and signature validation since the public key is meant to be shared while the private key is known only to the owner.

Cryptographic Techniques

- Auto-generated passphrases – To create a sufficiently random and strong passphrase for users, the Ring app generates a unique 10-word passphrase locally on the device. The technique to create this passphrase is similar to the idea of a dice-generated passphrase. The concept uses rolls of dice as a strong random number generator for selecting passphrase words from a large dictionary. For Ring E2EE, a 10-word minimum passphrase is randomly selected from a dictionary of 7,776 words[7]. This process creates a unique and strong passphrase composed of a minimum of 128-bits of entropy[8]. Additionally, the passphrase is not retained after local creation and other controls such as limiting the number of passphrase attempts are implemented to further increase protections against unauthorized users.

[7] 7776 words^number of words in a phrase equal ~800,000,000,000,000,000,000,000,000,000,000,000,000,000 possible phrases or 13 nonillion possible phrases.
[8] Each word has a minimum of ~12.8 bits of entropy for a total of a minimum of ~128 bits of entropy.

- Key exchange – Ring E2EE uses public key infrastructure concepts[9] to securely manage and exchange cryptographic keys and associated digitally signed identity certificates. Ring cloud is not included in this trust establishment and hence cannot decrypt the video data.

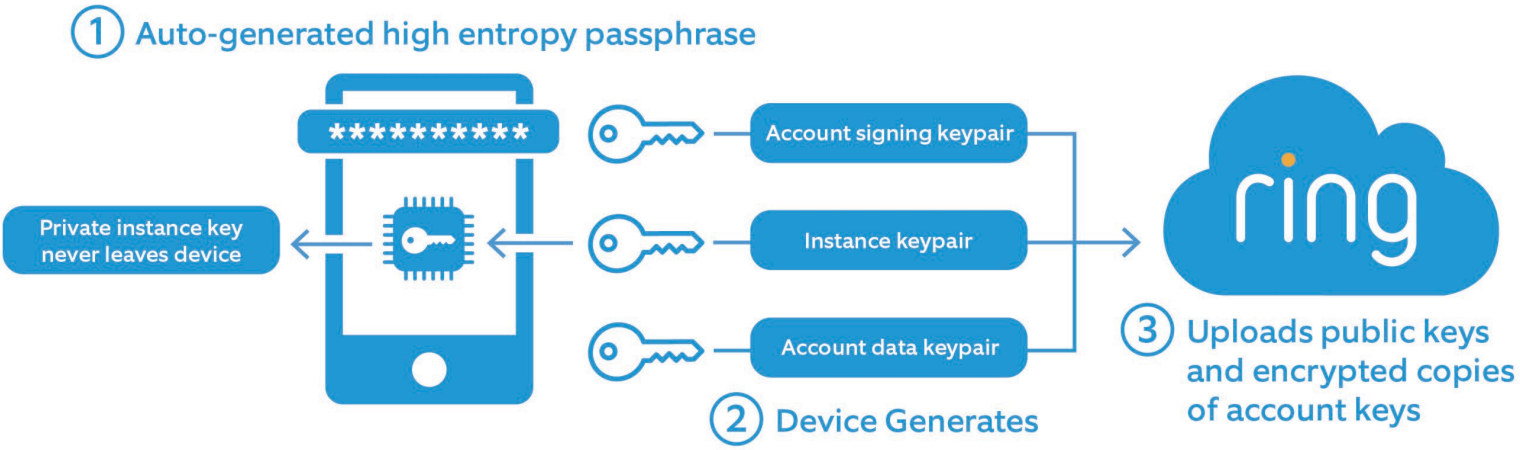
- Envelope encryption – The process of encrypting data with a data key then encrypting the data key with another key, in essence a key wrapping a key. Typically, the data is first encrypted with a symmetric data key to achieve faster data encryption. That symmetric data key is then encrypted with an asymmetric public key. The encrypted symmetric data key can be later decrypted with the corresponding private key, which then enables decryption of the encrypted data.

High-Level Design: Enrolling in E2EE

Enrolling a mobile device

A Ring user enrolls in E2EE through the Ring app on their mobile device on the supported iOS or Android device. The following three steps outline the process of enrolling a mobile device:

Diagram 2- Enrolling a mobile device



1. When the user begins the process of enrolling E2EE using their Ring app, the app presents a 10-word auto-generated passphrase that will be used to secure cryptographic keys. The passphrase is generated locally by the Ring app and is neither sent outside of the mobile device nor retained on the device. The user may need the passphrase in the future, for example, to enroll additional mobile devices. It is recommended the user securely store a copy of the passphrase, such as in a personal password manager.

2. After the user passphrase is created, three asymmetric key pairs are generated by the Ring app on the mobile device.

[9] See https://docs.aws.amazon.com/crypto/latest/userguide/awspki-whatis-toplevel.html

a. The first asymmetric key pair generated in the mobile device is RSA 2048-bit asymmetric account signing key pair. This account signing key pair performs cryptographic signing operations. It functions as a self-signed root of trust in the customer's E2EE setup to validate the authenticity of the other keys. The self-signed root of trust is used to issue certificates to Ring devices and mobile apps. The self-signed root of trust certificate is used by Ring devices to verify public portions of asymmetric keys that it downloads from the Ring cloud. See section on "Enrolling a Ring Device and Using E2EE – Viewing a Video Clip" for more details.

b. An additional ECC 256-bit key pair (prime256v1) asymmetric key pair[10], called the instance key pair, is generated locally on the mobile device. The public key portion of the instance key pair is signed by the account signing key to maintain the chain of trust. The private portion of the instance key pair is stored in a secure key store[11] on the user's mobile device and is designed to always remain there. For example, on iOS this means the hardware-backed Secure Enclave. This instance key pair is later used for envelope encryption, which is part of the process for encryption and decryption of videos. See section on "Using E2EE – Viewing a Video Clip section". A new instance key pair is created for each enrolled mobile device.

c. A final RSA 2048-bit asymmetric key pair, the account data key pair, is generated locally on the mobile device. This key pair acts as a backup encryption/decryption key pair for envelope encryption that can be used if the private portion of the instance key pair is not available. For example, when a user enrolls a new mobile device into E2EE and then views video that was envelope encrypted by a key from a prior enrolled mobile device. By design, the private portion of the account data key pair can only be decrypted on the user's E2EE enrolled mobile device.

3. The public portion of both the instance key pair and account data key pair are signed by the account signing key and copied to the Ring cloud. Enrolled Ring devices will use these public keys to perform envelope encryption. The private portions of the account signing key pair and account data key pair (from Step 2) are locally encrypted and then stored on the Ring cloud for later use[12]. For example, the key pairs are retrieved when a user is enrolling a new mobile device. The following describes the process for encrypting and backing up the private portions of the account key pairs:

   a. A passphrase derived key is generated from the 10-word passphrase selected in Step 1 and a random "salt" using the scrypt algorithm[13]. That scrypt output is then used as a password for a Password-based Key Derivation Function (PBKDF2) to derive a key[14].

   b. The private portion of the account signing key pair is then locally encrypted with the passphrase derived key then stored on the Ring cloud[15].

   c. The passphrase derived key is locally encrypted by the public portion of the instance key pair

[10] At release, E2EE will use the ecc-prime256v1 algorithm for iOS devices and RSA 2048-bit algorithm for Android devices.
[11] Ring uses the security offerings provided by the mobile device and or operating system producer, for example, StrongBox in Android and Secure Enclave in iOS. Availability of these security capabilities is dependent on the device vendor.
[12] The encrypted keys are stored in Public-Key Cryptography Standards (PKCS) #12 format. This is a common technique to store cryptographic objects such as private keys and certificates.
[13] In cryptography, salt is a randomly generated data string. For more information on scrypt, see Internet Engineering Task Force (IETF) RFC 7914 (https://tools.ietf.org/html/rfc7914).
[14] PBKDF2 is used in addition to scrypt to support compatibility with available PKCS#12 file generation libraries.
[15] E2EE uses the derived key as a password input function for PKCS12 generation for encrypting the private portion of the account signing key pair.

and then stored on the Ring cloud. This allows the enrolled mobile device to access the private portion of the account signing key pair in order to setup Ring devices without prompting for the passphrase.

d. The private portion of the account data key pair is locally encrypted with a new derived key and then stored on the Ring Cloud. This new derived key is created by using a locally generated 32-byte random[16] value as a password for scrypt and then for PBKDF2.

e. This new password derived key is then locally encrypted with the public portion of the account signing key pair and then stored on the Ring cloud. This allows the derived key to be accessed by using the private portion of the account signing key pair such as during enrollment of an additional mobile device.

f. This derived key is also encrypted locally by the public portion of the Instance key pair and stored In the Ring cloud. This allows the enrolled mobile device to access the account data key pair as needed to decrypt the envelope encryption for viewing videos (see Using E2EE – Viewing a Video Clip).

The example of enrolling an additional mobile device can provide further context for using account keys. If the user needs to enroll a new mobile device on an existing E2EE account and wishes to access past videos on it, the user provides the passphrase (from Step 1) in their new Ring app. This enables the Ring app to recreate the passphrase derived key. The Ring app can then download the encrypted private portion of the account signing key pair from the Ring cloud and decrypt it with the passphrase derived key. The decrypted private portion of the account signing key is then used to decrypt the key that was derived from the 32-byte random value which in turn is used to decrypt the private portion of the account data key pair. As mentioned earlier, the account data key pair is used by the Ring app to make videos previously encrypted with E2EE available on the newly enrolled mobile device.

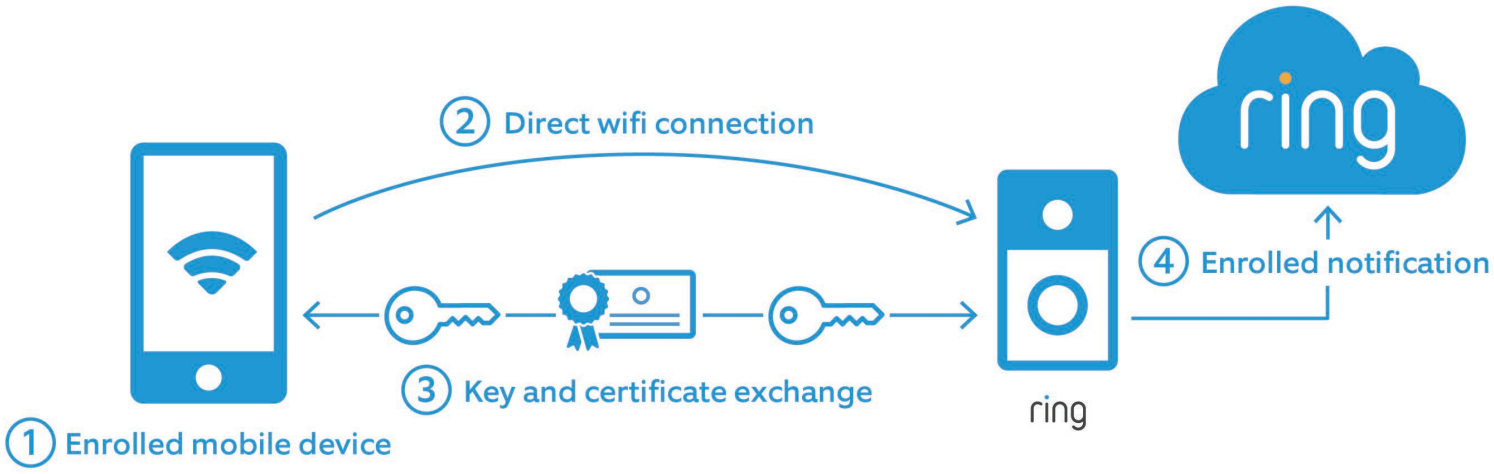
The user's mobile device is now enrolled in Ring E2EE. Deciding which mobile devices to enroll in E2EE is important because only enrolled mobile devices can interact with the Ring devices that are also enrolled in E2EE. This also means viewing videos from Ring.com or desktop apps is not currently possible as they are not compatible with Ring E2EE.

Enrolling a Ring device

The next step is enrolling a compatible Ring device[17]. After the user enrolls their mobile device, they can enable E2EE on a compatible Ring device in the Ring app. On the Ring device, "setup" mode must be initiated for E2EE setup.

[16] The 32-bytes are generated using cryptographically secure random number generation algorithms.
[17] Refer to Table 1.

Diagram 3- Enrolling a Ring device



1. When enrolling a compatible Ring device, an enrolled mobile device is required to initiate the setup workflow. Step-by-step instructions will be displayed in the Ring app.

2. A direct wifi channel is set up between the Ring device and the user's enrolled mobile device. This direct local connection is established when the Ring device creates a temporary local wifi access point that the mobile device joins. This prepares the devices for local key exchange.

3. After the direct connection is established, the Ring device creates its own asymmetric key pair for the purpose of a PKI-based certificate request process to the user's enrolled mobile device and for signing[18] the symmetric keys used for video encryption. The Ring app on the mobile device receives the certificate request and uses the account signing key to sign and return a certificate for the Ring device. The Ring app on the mobile device also transfers a root certificate with the public portion of the account signing key pair and key identifier information. This root certificate and key information is used by the Ring device to verify the public keys it can use for envelope encryption.

4. To complete enrollment, the Ring device sends a copy of its certificate to the Ring cloud, which registers the device as enrolled in E2EE. These steps are repeated to enroll additional compatible Ring devices into E2EE.

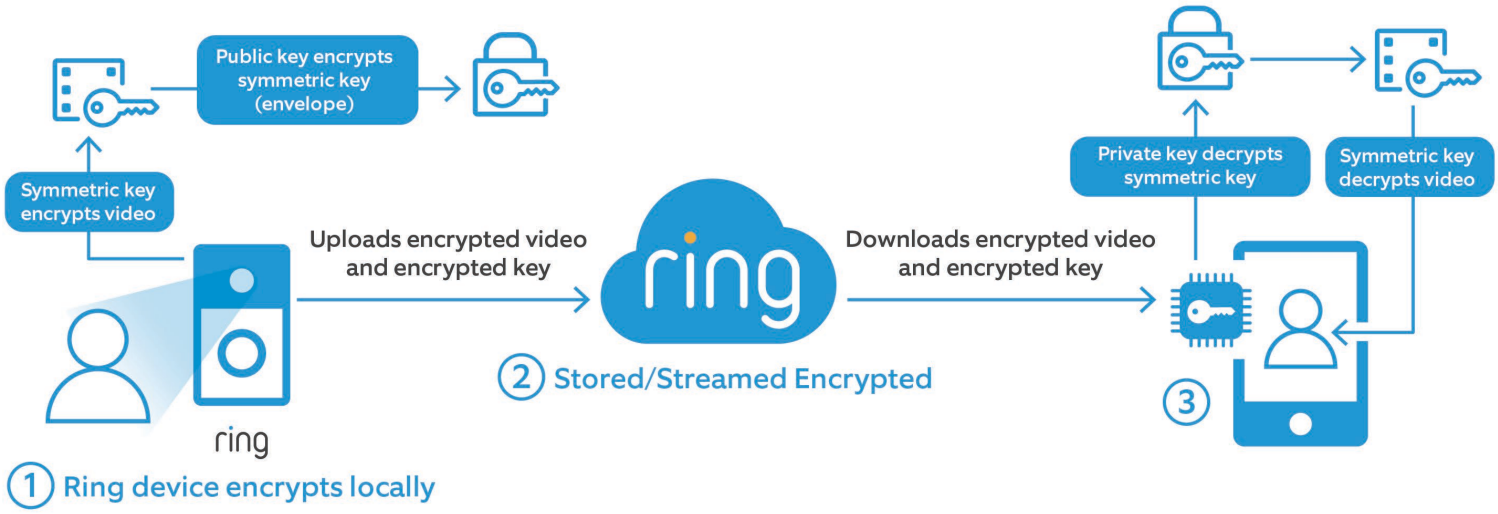
For flexibility, users can turn off Ring E2EE or disenroll their mobile and Ring devices at any time. When turning off E2EE, any videos encrypted with E2EE cannot be decrypted since the keys to access those videos are removed permanently. When an individual Ring device is unenrolled from E2EE, the videos previously encrypted by that device can still be decrypted by an enrolled mobile device.

Using E2EE – Viewing a Video Clip

Now that devices are enrolled in Ring E2EE, it's time to step through an overview of using the service to encrypt and decrypt video for viewing on an enrolled mobile device.

[18] The signing algorithm uses SHA256 with RSA-PSS.

Diagram 4- Encrypting and decrypting videos



1. The Ring device locally creates an AES 128-bit[19] symmetric encryption key to encrypt[20] the video produced by the device. A new symmetric key is created for every video and each key is purged from the Ring device immediately following the encryption process. Next, the Ring device will use envelope encryption[21] to protect the symmetric key. This process involves using the public portions of the mobile devices' instance key pairs (see Step 2 under enrolling a mobile device) and encrypting the symmetric key with it. This process is also performed using the public key from the account data key pair. Encrypting with the public key portion of the account data key pair is for cases when the instance private key is not available, such as when the mobile device is lost and the user is enrolling a new mobile device and viewing the previously encrypted video[22]. These public portions of the key pairs are downloaded from the Ring cloud and validated using the root certificate and key identifier information that was sent from the mobile device to the Ring device during enrollment[23]. The encrypted symmetric key and relevant public key association are stored in a manifest file. The encrypted video is then tagged with the manifest identifier. The manifest allows the Ring app to identify the appropriate keys needed for decryption.

2. After envelope encryption is performed, the encrypted video and manifest file are sent to Ring cloud. Depending on the feature used, this means the video is either stored for later viewing or streamed. In either case, E2EE is designed so only an enrolled mobile device can decrypt the video.

3. The Ring app on the user's enrolled mobile device retrieves the encrypted video and manifest file from the Ring cloud then uses the manifest to determine the appropriate keys to use for decryption. In this case, the Ring app decrypts the symmetric key retrieved from the manifest with the private

[19] Ring uses a 128-bit symmetric key to allow E2EE compatibility across the broadest range of devices while maintaining industry-accepted security standards and cryptographic strength.
[20] Symmetric encryption uses AES-128 with GCM.
[21] For RSA based keys, RSAES-OAEP encryption scheme is used with SHA-256 and MGF1. For ECC based keys, Elliptic Curve Integrated Encryption Scheme (ECIES) is used.
[22] The user's passphrase is required to decrypt the encrypted video.
[23] See Step 3 under Enrolling a Ring Device.

instance key, that is only stored locally on the enrolled mobile device. The Ring app can then use the symmetric key to decrypt the video for viewing.

IV. Security- and Privacy-Centric Practices

Ring's implementation of E2EE provides users with additional control and options over who can view their videos. Users can opt-in to have enhanced security and privacy designed to prevent unauthorized access to an enrolled user's end-to-end encrypted videos.

Privacy and security are foundational at Ring. Our policies and practices to protect personal data are based on recognized and emerging industry best practices, and we continuously strive to raise the privacy bar. For instance, we are not in the business of selling customer information to third parties, and users can opt-out of sharing their information[24] with third-party service providers for the purpose of receiving personalized ads. Users can also opt out of third-party web and app analytics services used by Ring to understand how users navigate and use our sites. In addition to directly deleting their video recordings, users can also request access to or deletion of their personal data. Ring's policies and practices also align with applicable privacy regulations.[25]

Ring E2EE restricts video sharing with public safety agencies

When a user enables Ring E2EE, end-to-end encrypted videos are excluded from any video sharing requests from public safety agencies. The user still has the option to share a video by downloading an unencrypted copy to their mobile device and providing it directly to a public safety agency; however, the user cannot generate a share link via the Ring app for a video recorded by an enrolled Ring device.

We are committed to building privacy and security into our products, services, and apps; giving users control over who can access their videos, devices, and personal information; and being transparent with users about our privacy and security practices.[26] We demonstrate this commitment from privacy-centric product offerings like Always Home Cam - which rests in a base where the camera is physically blocked and operates at a louder volume to makes its presence known[27] – to how we architect and operate community safety apps like Neighbors.

Ring designed Neighbors to help communities connect with each other and the public safety agencies that serve them. Through the Neighbors for Public Safety Service (NPSS) portal, public safety agencies may ask the public for assistance when investigating an incident; however, responding to those requests is up to the user - users retain absolute control to determine whether they might have potentially relevant videos, whether to share any videos, or whether to opt out of future requests.[28]

The NPSS portal does *not* enable public safety agencies to access a user's Ring device, view user video recordings or Live Views, or see a user's name, contact information, location or whether they received a video request notification, unless the user chooses to share specific videos in response to the video request. Users can also disable the Neighbors feed from their Ring app altogether. For additional information on our privacy-preserving practices and how we are moving the needle on transparency, accountability, and assurance, refer to Ring's Privacy page https://ring.com/privacy.

[24] https://blog.ring.com/2020/02/18/extra-layers-of-security-and-control/
[25] Refer to Ring's Privacy Notice page https://shop.ring.com/pages/privacy-notice
[26] https://ring.com/privacy
[27] https://blog.ring.com/2020/09/24/introducing-ring-always-home-cam-an-innovative-new-approach-to-always-being-home/
[28] https://support.ring.com/hc/en-us/articles/360023205151-A-Helpful-Guide-to-Video-Requests

V. Conclusion

E2EE gives our users enhanced security and privacy options that they control – only the user's enrolled mobile devices can access the key to decrypt and see videos from compatible enrolled Ring devices. That means E2EE is built to prevent unauthorized access to an enrolled user's end-to-end encrypted videos. We designed E2EE so that users can enable this encryption feature at any time and control who can view their videos while still being able to use core functionality, such as video streaming. Even if a user disables E2EE, the videos that were encrypted while it was enabled will stay encrypted. We expanded our security and privacy capabilities with E2EE, but it is still Day 1[29] of our continuous improvement efforts. We will continue to listen to our customers when designing offerings that keep security and privacy at the forefront.

VI. Further Reading

Refer to the following resources to learn more about E2EE:

- Executive Summary and FAQ ring.com/e2ee-summary

[29] https://www.aboutamazon.com/news/company-news/2016-letter-to-shareholders

Appendix A- Upcoming Releases

Ring seeks to continuously improve our security and privacy capabilities to meet, if not exceed, customer expectations and E2EE is no different. Planned Ring E2EE improvements from the technical preview will include:

- Provisioning an additional encryption key to maintain the principle of single-purpose-use for cryptographic keys
- Enhancements to passphrase generation to reduce the possibility of offensive phrases while maintaining the minimum required entropy
- Enabling Snapshots
- Enabling Shared Users

Customers can share feedback on the feature via the End-to-End Encryption page in Control Center within the Ring app.