ring

End-to-End Encryption

Executive Summary

January 2021

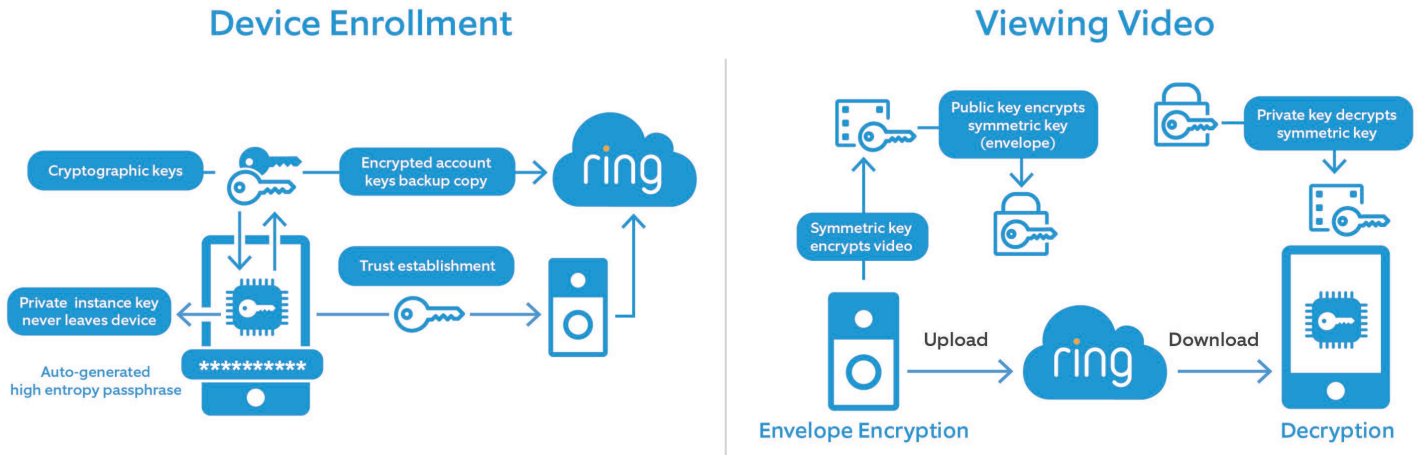
At Ring, security, privacy, and user control are foundational. With the launch of End-to-End Encryption (E2EE) for Ring, we release this whitepaper to provide a technical overview of the feature. E2EE will be available starting on January 13, 2021 as a new setting in the Ring mobile application (within Control Center) on compatible Android and iOS devices.

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. Ring's E2EE feature 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. 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).

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. This additional security- and privacy-centric feature works with Ring's core functionality, such as video streaming, providing users with even more peace of mind. E2EE's enhanced security and privacy feature requires some functionality trade-off as certain features require processing and analysis of decrypted video content. 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.

How the technology works

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.



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

1. When the user begins the process of enrolling, the app presents a 10-word auto-generated passphrase that will be used to secure cryptographic keys.
2. After the user passphrase is created, three RSA 2048-bit asymmetric keypairs are generated by the Ring app on the mobile device: the account signing keypair, the instance keypair, and the account data keypair.
3. The public portion of both the instance keypair and account data keypair are signed by the account signing keypair 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 keypair and account data keypair are locally encrypted and then stored on the Ring cloud for later use.

The user's mobile device is now enrolled in Ring E2EE. The next step is enrolling a compatible Ring device. See Section III in the whitepaper for additional details. For flexibility, users can turn off Ring E2EE or un-enroll 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.

Now that devices are enrolled in E2EE, it's time to use the service to encrypt and decrypt video for viewing on an enrolled mobile device.

1. The Ring device locally creates an AES-GCM 128-bit symmetric encryption key to encrypt 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 to protect the symmetric key.
2. After envelope encryption is performed, the encrypted video is sent to Ring cloud.
3. The Ring app on the user's enrolled mobile device decrypts the video with the appropriate keys and then retrieves the encrypted video from the Ring cloud.

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. 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. 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. For additional information on our privacy-preserving practices and how we are moving the needle on transparency, accountability, and assurance, refer to our E2EE FAQs [add link] and Ring's Privacy page https://ring.com/privacy.

To read the full whitepaper, download it at ring.com/end-to-end-encryption

Notices