WICKR

CUSTOMER SECURITY PROMISES

MARCH 2019

BUILDING THE MOST TRUSTED PLATFORM IN THE WORLD

At Wickr, our mission is to transform how companies and organizations protect valuable, high-target communications. In doing so, we strive to build the most trusted communication platform in the world by investing in comprehensive and transparent security testing. We are motivated by the belief that private and trusted communications are critical for organizations of all sizes. We understand that in order to earn this level of trust, our platform must be verifiably **secure, ephemeral & available**.

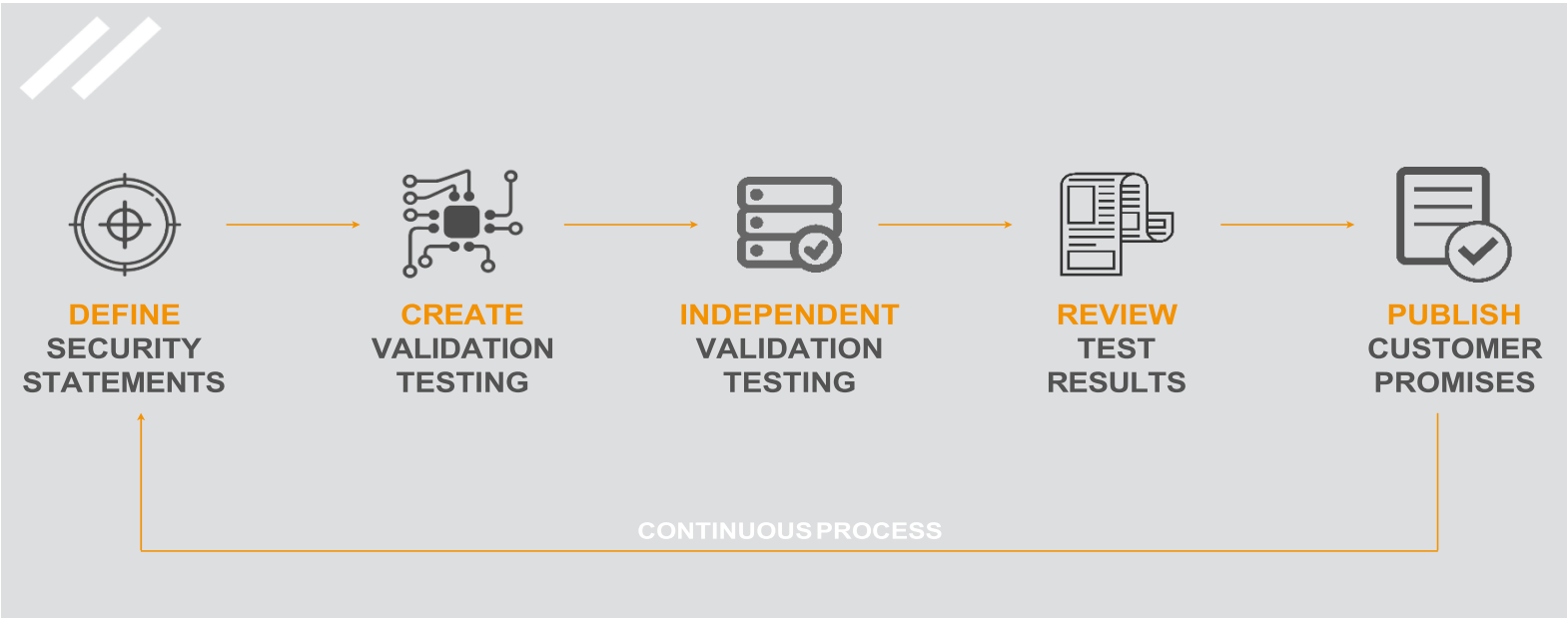
Fulfilling this mission requires significant engineering effort and transparency about how our technology works and why. From the start, Wickr has committed to delivering **unique and advanced** secure and ephemeral communication solutions, while adhering to a **unique and advanced** Security Program built upon the following core processes:

- Opening Wickr's cryptographic protocols for independent public review
- Running an open Bug bounty program focused on ensuring confidentiality and integrity of user data
- A public Vulnerability Disclosure Policy
- Publication of Legal Process Guidelines to share how Wickr responds to government request for user information
- Regular publication of Transparency Reports
- Independent testing by world class security consultants
- Unit testing for applicable security issues identified through testing and bounties

Customer Security Promises

To further advance our security program, we have built a set of **Customer Security Promises** to guide our internal engineering and testing processes, enable Wickr users to gain a clear understanding of the level of security Wickr aims to provide, and provide public transparency into the methodology and results of independent security testing related to these promises.

By committing to a continuous process of refining and delivering on our Customer Security Promises, we aim to set a new standard in how companies build trust with their users. We are making a public commitment to our customers that Wickr products will perform to these promises *and* a commitment to the Wickr team internally that we will provide the resources and support required to live up to these high standards for protecting user privacy and security.



Wickr's Customer Security Promises

The Wickr protocol provides end-to-end encryption and integrity protection
The Wickr protocol enforces forward secrecy
The Wickr protocol enforces authentication of messages
Compromise of Wickr infrastructure does not compromise message content
The applications reliably manage ephemerality policy.
Group messaging protocol provides the same security assurances as Core protocol
Video and audio calling provides the same security assurances as Core protocol
Message content and supporting encryption keys are managed properly on official supported Wickr clients
Wickr manages sensitive customer data in cloud-hosted networks in accordance with the Wickr Privacy Policy

While not indicative of everything we do to provide security and privacy in our products, these Customer Security Promises are the fundamental promises that we believe any security or privacy oriented communication and collaboration tool should make to their users. They will evolve as we add new functionality and products to the Wickr product portfolio and as more test plans are developed with our partners. Wickr will publish updated documents regularly in line with our ongoing testing efforts, the full scope of which are described below and extend far beyond promise verification.

The creation of Wickr's Customer Security Promises and the above description of the overall testing framework and verification processes is a collaborative effort between Wickr and NCC Group, a global expert in cyber security. Our collective goal is to ensure that Wickr customers understand the process and results of the independent validation testing, and ultimately have the information they need to confidently determine that Wickr's Customer Security Promises are achieved. We always welcome feedback from Wickr customers and hope this document provides a clear view into how Wickr builds privacy and security in its products.

The remainder of this document has been provided by NCC Group.

Testing Engagement and Methodology Overview

NCC Group has performed regular security assessments of Wickr Pro starting in January 2017. While precautions have been taken in the preparation of this document, NCC Group the publisher of this section, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NCC Group's services does not guarantee the security of a system, or that computer intrusions will not occur. NCC Group does not endorse the views of its clients nor the products and/or services they offer.

NCC Group's security assessments have two goals:

1. Verify that features that support Wickr's Customer Security Promises conform to the relevant Security Test Criteria.

2. Identify opportunities to improve security, including identifying vulnerabilities to be fixed, feature requests that provide defense-in-depth, design and architectural review of new features, and testing strategies that improve quality.

During the course of 2017, 2018 and 2019, NCC Group and Wickr evaluated features related to Wickr's Customer Security Promises across the entire Wickr technology stack, including Wickr Pro mobile and desktop applications, the Wickr Pro administrative portal, and supporting server infrastructure. As this effort is intended to evaluate the design and behavior of features, NCC Group relied primarily on manual, as opposed to automated, analysis in all reviews of Wickr Pro.

Wickr provided NCC Group with all relevant source code, ongoing access to engineers and developers, a private test environment, beta client builds, and internal documentation. NCC Group reviewed the design and implementation of Wickr's cryptographic protocol and core technology to understand its security model and detect any design weaknesses. NCC Group analyzed the security-relevant code of the Wickr technology stack using manual code review and performed targeted security testing in a private network.

NCC Group worked with Wickr to identify both short-term and long-term solutions for any vulnerabilities identified during these efforts. A key part of this process involved verifying that no known high-risk vulnerabilities are present in the application at the end of each test round. NCC Group expects any low-risk findings to be addressed responsibly according to expected risk and mitigation strategies. Any issues found during testing that impact Wickr's Customer Security Promises are explicitly documented in the sections that follow. The full reports at the end of each round of security testing were provided to Wickr and are not shared publicly.

Verification of Customer Promises

The promises below were verified using **Wickr Pro Beta v5.2.3** and contemporary supporting infrastructure.

Core Protocol Security

The following security promises relate to the Wickr Messaging Protocol, which provides end-to-end secure communications for users.

1. The Wickr messaging protocol provides end-to-end encryption and integrity protection of communications – Verified

Security Test Criteria

- Verify that end-to-end encryption and integrity protection are provided in all cases.
- Verify that recommended cryptographic algorithms and parameters are used.
- Verify appropriate use of standard cryptographic implementations.
- Verify the proper use of secure random numbers for cryptographic operations.
- Verify that cryptographic keys are stored securely and in only required locations.

Analysis

Full details of the Wickr Messaging Protocol can be found in the Wickr Messaging Protocol Technical Paper. [1] The paper specifies that message content is encrypted using the Advanced Encryption Standard in Galois Counter Mode (AES-GCM) with a 256-bit key. This mode provides cryptographic confidentiality and integrity protections for message content. NCC Group verified that Wickr implemented this as described and used recommended cryptography algorithms, parameters, and secure random numbers.

Each Wickr message is encrypted using a cryptographically-random, per-message symmetric encryption key, and this key must be shared securely with all recipients of the message. This is accomplished using the elliptic curve Diffie-Hellman key agreement protocol (ECDH) over curve P521. The sender and each recipient use ephemeral, authenticated ECDH to agree upon a shared secret, which is then used to encrypt the message encryption key. NCC Group verified that neither the ephemeral key negotiated by ECDH nor the message encryption key are known, disclosed, or able to be calculated by Wickr or any party other than valid sender and recipients of the message.

Each message is digitally signed by the sending device's long-term private key. This signature authenticates the full serialized message by using a key that can be associated with the sending user. Encrypted data is also transmitted inside a TLS channel to provide an extra layer of protection from passive and active attackers. As of this writing, Wickr uses OpenSSL's implementations of the above-referenced cryptographic primitives and protocols.

[1] https://www.wickr.com/s/White-Paper_Wickr-Messaging-Protocol.pdf

Wickr has an end-to-end encrypted and authenticated channel through its messaging service; however, clients still rely on Wickr infrastructure to accomplish important practical tasks such as storing and transmitting the client-encrypted account recovery bundle. In order to facilitate a smooth multi-device user experience, Wickr stores a recovery bundle, which includes the user's long-term private key, server side. This recovery bundle is encrypted client side before being uploaded by a key derived from the user's password. It remains necessary for users to choose high quality passwords to ensure this Customer Promise remains applicable.

2. The Wickr messaging protocol enforces forward secrecy – Verified

Security Test Criteria

- Verify that Wickr's security mechanisms to provide forward secrecy are appropriate for the purpose.
- Verify that Wickr generates ephemeral keys as expected to provide forward secrecy

Analysis

Forward Secrecy is remarkably difficult to define[2] despite its common use. This analysis conforms to the definition from *the Handbook of Applied Cryptography*[3] – "A protocol is said to have perfect forward secrecy if compromise of long-term keys does not compromise past session keys" (496).

The Wickr Messaging Protocol provides forward secrecy by generating a random encryption key per-message and using ephemeral ECDH key pairs to exchange this message key. The user's long-term key pair and each of their device's long-term key pairs are used only to authenticate the ephemeral public keys used for ECDH. The compromise of the user's or any of their devices' private keys would compromise trust in future ephemeral keys signed by the compromised key, but would not compromise previously-generated ephemeral keys, negotiated session keys, or traffic protected by those keys. These keys are not stored in any Wickr messaging infrastructure.

Wickr has fulfilled the core requirements of this Customer Promise as outlined in the security test criteria; however, NCC Group has outlined the following corner cases that serve as room for improvement in the future:

Ensure that the protocol enforces forward secrecy for offline devices in all cases.

In normal operation, all ephemeral keys will be used only for a single message. Under abnormal conditions—server error or the server-side pool of ephemeral public keys being exhausted via natural occurrence or malicious action while a device is offline and unable to replenish its key pool—a device's ECDH ephemeral key may be re-used. This is a known risk that was acknowledged by Wickr prior to NCC Group's assessment and represents a design trade-off between security and usability goals to facilitate communication with offline clients. However unlikely, we note the possibility that such conditions could lead to sufficient ephemeral key reuse to impact forward secrecy in the case of offline devices.

---

[2] https://tools.ietf.org/html/rfc4949#page-218

[3] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography (1st ed.).* Boca Raton: CRC Press, Inc., 1996. Print.

3. The Wickr messaging protocol enforces authentication of messages – Verified

Security Test Criteria

- Verify that message signature is computed and verified as designed.
- Verify that the device's signing key is used to compute message signature.
- Verify that the device's signing key is properly authenticated by the user's root signing key.

Analysis

The Wickr Messaging Protocol specifies that the message sender sign the serialized packet using the sending device's private key. This is accomplished using Elliptic Curve Digital Signature Algorithm (ECDSA) as implemented in OpenSSL (Curve P521). Message recipients use context communicated from the server, the transmitted message, and client-managed state to establish that the message signature is valid. Additionally, Wickr verifies that the device is associated with a known user, and that the device's signing key is properly signed by the user's identity key. Furthermore, derivation of the key that protects the message encryption key integrates context from the sending and receiving users' public keys; an attempt to replay a message from a device outside of the expected context will result in failure to decrypt the message. NCC Group verified that users are informed in the event of an authentication failure.

Wickr has fulfilled the core requirements of this Customer Promise as outlined in the security test criteria; however, NCC Group has outlined corner cases that serve as room for improvement in the future, such as:

Ensure that the protocol has comprehensive replay message protection.

Replay of a message between two users may be possible, but is limited to the duration of time in which the ephemeral keys are valid and in the context of a specific source and destination user. The window of practical attack is limited in context and duration in the order of minutes, and Wickr is continuing to explore ways to minimize this window. Due to the difficulty of exploitation by an external adversary, NCC Group considers this threat to be minimal during normal protocol operation for the majority of Wickr users.

4. Compromise of Wickr infrastructure does not compromise message content – Verified

Security Test Criteria

- Verify that compromise of any Wickr messaging infrastructure does not provide message content to attackers.
- Verify that no clear-text keys, private keys or passwords are stored in the database.
- Verify that authentication failures interrupt communications and/or adequately warn users.
- Determine whether unexpected or highly sensitive message metadata is available.

Analysis

At the time of this writing, NCC Group has completed security assessments that focused on Wickr server infrastructure, which showed that Wickr follows recommended security best practices in their messaging infrastructure, and no vulnerabilities that impact this Customer Promise were reported. Based on the completed security assessments to date of the Wickr messaging protocol, associated applications, and its security architecture and infrastructure, NCC Group is confident that users' message content is not available to Wickr or any other party in the event of Wickr infrastructure compromise. NCC Group verified current security controls exist to prevent and/or detect compromise of Wickr's source code check-in and build process.

Additionally, NCC Group reviewed client security and cryptographic protocols over the course of the security assessments in 2017 and 2018. No functional requirements or features exist that violate this Customer Promise or components intended to bypass the client-oriented design of Wickr Secure Messaging.

5. **The applications reliably manage ephemerality policy – Verified**

Security Test Criteria

- Verify that Wickr client applications user interface inform their users of the ephemerality policy.
- Ensure Wickr client applications follow the ephemerality policy attached to each message. Testing was completed on Android, iOS, Linux, Windows and macOS.
- Verify that messages are deleted as indicated by the ephemerality policy.

Analysis

NCC Group verified that ephemerality policy applies on all platforms and users are informed of the ephemerality policy. The applications display the current applicable ephemerality policy in the background of the message entry field, making it very clear what policy applies to the next sent message. Further, the user is notified that past message history will not appear on a newly enrolled device to preserve privacy.

Wickr has fulfilled the core requirements of this Customer Promise as outlined in the security test criteria; however, NCC Group has outlined a corner case that could serve as room for improvement in the future, such as:

Ephemerality policy does not apply to screen capture notifications.
Screen capture notifications are assigned and attached to a separate, fixed ephemerality policy that may be different than the sender's current settings. Further, the ephemerality policy assigned and attached to a screen capture may be longer than the policies for the individual messages it contains. As the ephemerality policy attached to a mobile screen capture message may not reflect the current policy setting effective on the client, the notification message policy will be enforced differently (where enforcement refers to deletion).

6. Group messaging protocol provides the same security assurances as Core protocol – Verified

Security Test Criteria

- Verify that group messaging protocols use proper cryptographic mechanisms related to end-to-end encryption, integrity protection and forward secrecy.

Analysis

NCC Group verified that group messaging is supported by an extension of the core Wickr pairwise messaging protocol. Each device in the group must securely establish a pairwise key with every other device included in the group and this is completed using the existing Wickr messaging protocol. NCC Group verified that Wickr's servers are not able to add members to groups and that the Wickr servers distribute messages utilizing a one-to-many delivery mechanism in which an encrypted payload is delivered to all the devices in the Wickr group.

Therefore the security guarantees of Wickr's group messaging system are equivalent to the guarantees of the existing Wickr protocol and includes forward secrecy, confidentiality and authentication.

7. Video and audio calling provides the same security assurances as Core protocol – Verified

Security Test Criteria

- Verify that video and audio protocols use proper cryptographic mechanisms related to end-to-end encryption, integrity protection and forward secrecy.

Analysis

NCC Group reviewed Wickr's video and audio encryption which is provided with a separate symmetric encryption key for audio and video calls via the in-band messaging protocols. NCC Group verified that the security guarantees of the distribution of the key are equivalent to those for the standard messages delivered via Wickr's core protocol.

Wickr has fulfilled the core requirements of this Customer Promise as outlined in the security test criteria; however, NCC Group has outlined the following corner cases that serve as room for improvement in the future:

Implement voice and video rekeying.
The data within a single text exchange is small and represents a conservative length of data to be protected with a single key. When the key exchange is used to bootstrap a secured audio or video stream, the data protected by the exchanged key will be much larger. NCC Group reviewed code in the early stage of integration when a single key is used to protect all communications but rekeying happens whenever group members change. Forward secrecy is provided by ensuring that every audio and video call has a new key provisioned and the group membership rekey process helps to further reduce the session size from a forward secrecy perspective.

User Privacy

The following security promise relates to the confidentiality and integrity of user data.

8. Wickr manages sensitive customer data in cloud-hosted networks in accordance with the Wickr Privacy Policy – Verified

Security Test Criteria

- Verify that only limited log data and necessary Personally Identifiable Information of users is available to Wickr for cloud-hosted networks.
- Review a sample of logging statements and active log files on Wickr servers to identify any deviations from Wickr's privacy policy.
- Verify that statements made in Wickr's privacy policy are enforced as intended in the version of Wickr Pro tested.
    - https://www.wickr.com/privacy/#pp_wickrpro
    - https://www.wickr.com/privacy/#privacypolicy
- Verify that any exceptions to this promise—such as not applying to self-hosted networks—are publicly documented.

Analysis

During the security reviews thus far, NCC Group focused on aspects of the Wickr privacy policy that directly impacts Personally Identifiable Information for cloud-hosted networks as described above in the security test criteria. As of the most recent security assessment completed by NCC Group, Wickr application logs do not record source IP addresses and only keep account-related activity for a limited time (less than one week) as outlined in the privacy policy "*We retain certain account data (i.e., types of messages sent and account settings changes) which contain no PII for up to 6 days.*" Furthermore, Wickr does not store any sensitive information that is not outlined in the Wickr privacy policy. Self-hosted networks follow the privacy policy of the customer's administrator and were not in scope for this Customer Promise.

NCC Group notes that it is impossible to review every single log statement and considers this Customer Promise verified by reviewing a random sample of the logging statements and ensuring that it is in accordance with the Wickr privacy policy. NCC Group has considered that Wickr has fulfilled the core requirements of this Customer Promise as outlined in the security test criteria; however, NCC Group recommends additional areas reviewed in future assessments, as described below:

<u>Continue to perform reviews of Wickr's privacy policy.</u>

In future assessments, NCC Group plans to focus on additional aspects of the Wickr privacy policy that would be documented in the security test criteria. These assessments would include any applicable privacy testing on self-hosted networks.

Client Security

The following security promise relates to management of cryptographic keys and sensitive content by Wickr Pro.

9. Message content and supporting encryption keys are managed properly on official supported Wickr clients – Verified

Security Test Criteria

- Verify that message content and encryption keys are secured according to client platform best practices.
- Verify that caches of message content and supporting encryption keys are deleted in a timely manner.
- Verify that plaintext keys are not exposed on Wickr Pro clients when “cold boot” forensic analysis is performed and key scrubbing is correctly implemented.

Analysis

NCC Group has reviewed client-specific code for managing cryptographic keys and sensitive content. Wickr Pro secures message content and encryption keys according to recommended best practices. NCC group also verified that message content and plaintext keys are deleted as expected from devices and that Wickr promptly deletes cached, plaintext graphics files on supported operating systems.

Wickr has fulfilled the core requirements of this Customer Promise as outlined in the security test criteria; however, NCC Group has outlined areas for future testing in subsequent rounds, such as the following:

Perform comprehensive memory analysis of Wickr clients.

NCC Group will complete additional memory analysis of Wickr clients in subsequent rounds of testing to augment the “cold boot” forensic analysis which was completed in earlier rounds of security testing. The goal of this additional testing would be to validate that no encryption key material or related metadata is available at any time to attackers.