# WICKR

## CUSTOMER SECURITY PROMISES

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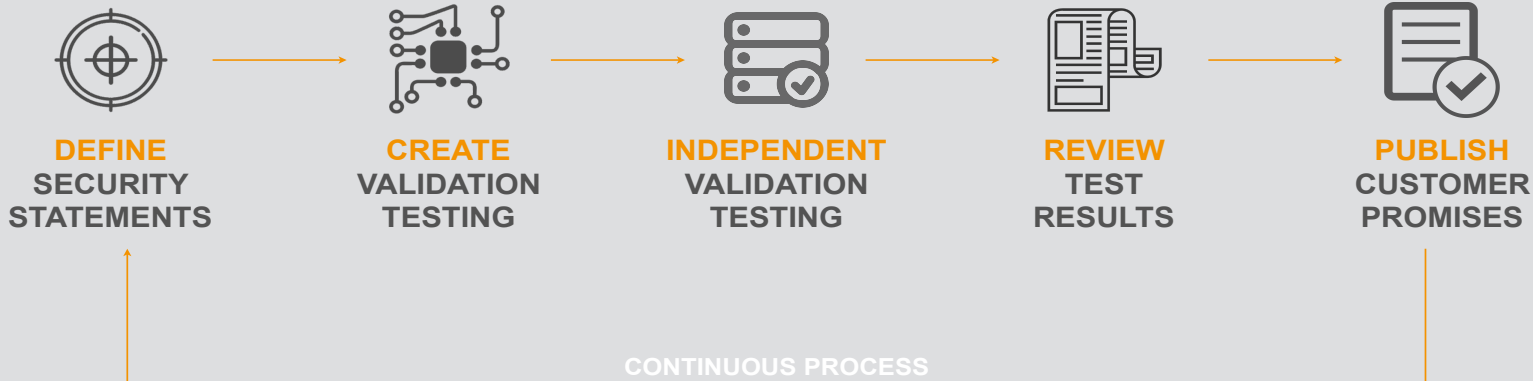
Fulfilling this mission requires significant engineering effort and transparency about how our technology works and why. From the start, Wickr has committed to delivering **unique and advanced** secure and ephemeral communication solutions, while adhering to a **unique and advanced** Security Program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

**DEFINE** SECURITY STATEMENTS → **CREATE** VALIDATION TESTING → **INDEPENDENT** VALIDATION TESTING → **REVIEW** TEST RESULTS → **PUBLISH** CUSTOMER PROMISES

CONTINUOUS PROCESS

## 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 |
| Protocol reliably informs messaging partners of 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 Bishop Fox, a global security consulting firm. 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 Bishop Fox.*

8240 S. Kyrene Road      P 480 621 8967
Suite A-113      F 480 383 6401
Tempe, AZ 85284      BishopFox.com

**BISHOPFOX**

# WICKR — CUSTOMER SECURITY PROMISES

In 2018, Bishop Fox was engaged to review Wickr's architecture and system implementation and to summarize Wickr's security guarantees. This document provides an overview of the core security promises made by the Wickr messaging and communications system. The summary addresses several specific security questions and presents the assessment team's findings with respect to each one.

Beginning in Q4 2019 and continuing into 2020, Wickr again engaged Bishop Fox for a long-term assessment. The priority for the Q3 2020 assessment was the following Wickr Pro clients:

- Windows — Wickr Pro 5.64.7

- iOS — Wickr Pro 5.65.5

- Android — Wickr Pro 5.64.1

As of October 23, 2020, Bishop Fox had not observed any functional changes or identified any issues that would compromise or otherwise alter the outcome of the promises verified in this document. As the engagement progresses, this document will continue to be updated to reflect the current status of the Wickr Customer Security Promises.

## 2018 Approach
The assessment team analyzed the Wickr protocol design and implementation at two levels. First, the team performed a manual cryptographic architecture review of the Wickr protocol to ensure that it achieved its end-to-end encryption goals. Second, the team conducted a cryptographic review of C language implementation to ensure that the implementation correctly reflected the cryptographic design specifications.

## 2019-2020 Approach
The assessment team continues to review Wickr's protocol design and implementation. The team monitors feature and implementation changes between engagements and performs a targeted in-depth manual review of Wickr's protocols and implementation. These engagements aim to further reinforce the promises previously verified by the assessment team and ensure that, as the product evolves, the promises made to Wickr's customers are not compromised.

## Summary of Findings

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

## The Wickr protocol provides end-to-end encryption and integrity protection — Verified

For this security test, the assessment team had the following goals:

- Verify that Wickr's encryption protocol uses industry standard components for encryption and integrity protection.
- Ensure that secret keys are retained solely on the client.

The team's review was based on the following sources:

- The Wickr Messaging Protocol technical paper
- The Wickr Messaging Protocol cryptographic implementation, which is a public implementation of the Wickr protocol written in the C programming language
- Conversations with Wickr engineers

**FINDINGS**

The team found that the Wickr cryptographic protocol provides end-to-end encryption using a combination of public-key and symmetric-key cryptography. Wickr maintains all secret decryption keys and authentication keys on each device and does not transmit these secrets to Wickr servers. Wickr's servers transmit only public identity keys and ephemeral encryption keys.

To register a user on the Wickr network, the user generates an identity keypair for authentication. To register a new device on the Wickr network, the device also generates an identity keypair. The public key is transmitted to Wickr's key server, while the secret key is retained locally. In addition to these keys, the device generates a collection of ephemeral elliptic curve Diffie-Hellman (ECDH) public keys and signs each key with the appropriate device identity key.

To establish a connection with one or more remote devices belonging to a user, the Wickr client software obtains the user public identity key and the public identity key for each registered device from Wickr's infrastructure. The client also verifies that the device key is correctly signed using the user public identity key. The device also obtains signed ephemeral keys from the Wickr servers and verifies the signatures.[1]

Using the ephemeral key and its own identity key to authenticate the key exchange, the initiator establishes a separate shared symmetric key using a 521-bit ECDH public key

---

[1] Like all such protocols, the security of the protocol assumes that the client device obtains the correct public key from the server. The Wickr device uses an identity verification string to allow users to compare keys.

agreement protocol with each device associated with the user account. This key is used to encrypt a randomly generated 256-bit AES payload key. The resulting payload key is used to encrypt the message payload packet using the 256-bit AES-GCM authenticated encryption mode.

Using these mechanisms, the Wickr protocol additionally offers extensions for endpoint devices to securely agree on cryptographic keys for use in encrypted voice and video calls. It also provides a mechanism for devices to perform secure group chat, where each device transmits encrypted content to the other members of the group.

In summary, the team's review found that the Wickr protocol securely achieves end-to-end encryption using standard cryptographic primitives.

# The Wickr protocol enforces forward secrecy — Verified

**SECURITY TEST CRITERIA**

For this security test, the assessment team had the following goals:

- 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.

**FINDINGS**

The Wickr protocol uses ephemeral elliptic curve Diffie-Hellman (ECDH) to provide forward secrecy for messages transmitted from one node to another. Forward secrecy is a property that ensures the loss or compromise of a device does not result in the compromise of past encrypted data. This mechanism is motivated by a model in which target devices can be compromised at arbitrary points (and secrets extracted), and the attacker may attempt to determine the content of previous messages.

By using ECDH, the Wickr protocol provides the following two security guarantees:

1. Messages transmitted from one client to another use an unpredictable shared key.
2. Once messages have been received and decrypted by a recipient client, the recipient's ephemeral key can be destroyed (zeroized) in memory, ensuring that any compromise of the device will not allow subsequent decryption.

The assessment team's review verified that Wickr correctly generates and destroys ephemeral key material, which ensures forward secrecy for past messages that have been transmitted. Each device uses separate ephemeral key material, and only identity keys are retained long term.

The Wickr cryptographic mechanism generates and delivers Diffie-Hellman keys to Wickr infrastructure, where they can be delivered to devices for transmission. This results in the storage of a pool of keys in the Wickr key server infrastructure. In principle, this pool of keys can be exhausted by a resourceful attacker, which would reduce forward secrecy for asynchronous communications. However, such attacks would require significant resources and are fundamentally challenging to defend against in messaging systems such as Wickr.

As a final element, Wickr includes protections to prevent replay attacks. These include sequence numbers included in packets to detect and reject replayed messages. Additionally, the regular destruction of ephemeral keys ensures that replay attacks cannot be performed after key zeroization.

# The Wickr protocol enforces authentication of messages – Verified

For this security test, the assessment team had the following goals:

- Verify that Wickr's security mechanisms to provide authentication operate correctly.
- Verify that Wickr correctly derives keys and authenticates messages.

**FINDINGS**

The assessment team found that the Wickr protocol employs several mechanisms to protect messages transmitted between clients. First, it uses a 521-bit ECDH key agreement protocol to derive a shared secret between the clients by combining ephemeral keys between initiator and recipient. Second, it uses digital signatures to ensure that the ephemeral keys received from the recipient are authentic; this signature is computed using ECDSA with 521-bit keypairs. Third, it employs a secure Key Derivation Function (KDF) on this shared secret to derive symmetric keys used to encrypt data payloads; this key derivation binds identities into the KDF to prevent an unknown keyshare attack. Fourth, it uses digital signatures over the message contents to authenticate this data. Finally, it uses the authenticated AES-GCM mode to encrypt data transmitted between clients.

These cryptographic mechanisms combine to ensure the following:

- That communications cannot be altered by an attacker without resulting in a detectable error condition at either client;
- That communications cannot be forged by an attacker without resulting in a detectable error condition.

This ensures that all data received by a client can be authenticated as deriving from the appropriate root (user) account, and from a device registered to that user account. Additional payloads, such as keys and group management messages, are authenticated using this mechanism.

As noted above, the assumption of authenticity relies on the ability for users to verify that user identity public keys received from Wickr's servers are legitimate. The team verified this ability using the techniques described above.

# Compromise of Wickr infrastructure does not compromise message content — Verified

For this security test, the assessment team had the following goals:

- Verify that Wickr's encryption mechanisms do not reveal keys to servers.
- Verify that Wickr's encryption covers all payload content.
- Verify that Wickr group messages do not allow the unauthorized addition of group members.
- Verify that new devices cannot be added to a user's account without authorization of the user.

## FINDINGS

The Wickr messaging protocol ensures that all messages transmitted between clients are end-to-end encrypted, and the secret portions of the keys used for encryption are not shared with Wickr infrastructure. The only secret key material sent to the server consists of identity secret keys that are encrypted under a key derived from the user's password. Subject to caveats described further below, this design fundamentally ensures that message content cannot be decrypted by Wickr's infrastructure or any attacker who compromises Wickr's infrastructure.

There are two essential caveats to this guarantee. These are described below.

First, an attacker who compromises Wickr's key management infrastructure can cause a compromised key server to distribute invalid (root) identity public key and ephemeral key material for targeted users. While this attack does not reveal the secret key material for the users themselves, it can cause other parties to encrypt sensitive content under a public key chosen by the attacker. As a result, payloads and payload keys may be revealed to unauthorized users.

This attack can be leveraged against many end-to-end encryption protocols, and it can be mitigated using key verification countermeasures. Wickr includes a key verification mechanism that allows the user to share a hash of their identity public key with others via an out-of-band communication channel. Senders can verify that the shared key hash matches the identity public key that they have received from Wickr's servers. While this requires additional effort on the sender's behalf, it provides one mechanism to detect and prevent attacks that abuse a compromised key server.

A second potential attack involves the storage of an encrypted identity secret key on Wickr's servers. This mechanism first derives a secret key by hashing the user's password through a memory-intensive key derivation function. The resulting key is then used to AES encrypt the user's identity secret key, forming an encrypted blob that is transmitted to the Wickr servers for storage. As a result, an attacker who compromises Wickr infrastructure may be able to obtain this encrypted blob. Such an attacker could perform an offline dictionary attack to determine the user's password and obtain the Identity secret key. While this would not allow the attacker to immediately decrypt ciphertexts (or decrypt past ciphertexts), the user could register a new device to Wickr's services using the identity key. Future messages sent to this user's account would then be vulnerable to decryption by the attacker.

The primary countermeasure to this attack is Wickr's use of a memory-hard variant of scrypt to hash the user's password. While this does not absolutely prevent dictionary attacks, the strength of this hashing significantly increases the cost of an offline dictionary attack to recover the user's identity secret key. However, it does present a new risk that a user who selects a weak password, or whose password is compromised in some manner, could be vulnerable to such attacks.

Finally, in the several months preceding this assessment, multiple encryption systems that support group messaging (including WhatsApp and Signal) have proven vulnerable to group membership manipulation by a compromised server. Wickr is not vulnerable to these attacks. This is due to the fact that in Wickr's implementation of group messaging, the group servers have no ability to add or remove members of the group. In Wickr, only the authorized manager of a group can modify the membership of a group, by transmitting specialized authenticated management messages to the group. This approach mitigates the possible addition of "phantom" devices or users to a group, even if the Wickr infrastructure is compromised.

# Protocol reliably informs messaging partners of ephemerality policy — Verified

**SECURITY TEST CRITERIA**

For this security test, the assessment team had the following goals:

- Verify that Wickr client applications inform their users of the ephemeral messaging policy.
- Ensure Wickr client implementations follow the ephemerality policy.

**FINDINGS**

The Wickr client implementations on all platforms inform users of the application that messages will follow the Wickr ephemerality policy. The applications force a user to read a prompt acknowledging the ephemerality policy. There is no way to send messages from the application before this prompt is acknowledged. A reasonable user of the application will be well informed of the ephemerality policy before being able to use the application to send and receive messages. The Wickr client applications follow the ephemerality policy by not making messages available on devices on which the message was not initially received.

# Group messaging protocol provides the same security assurances as Core protocol — Verified

## SECURITY TEST CRITERIA

For this security test, the assessment team had the following goal:
- Verify that Wickr's group messaging protocol provides strong cryptographic guarantees.

## FINDINGS

Wickr supports group messaging using an extension of the core Wickr protocol. Group messaging allows a larger number of users (greater than two) to simultaneously engage in secure messaging conversation. Group messaging traditionally differs from standard pairwise messaging in the following ways:

1. Groups must be established and managed by a group manager. (Group managers may add and remove users.)
2. Messages transmitted by each party in the group must be encrypted such that all group members can receive, decrypt, and authenticate them.
3. Encrypted messaging material must be delivered to all members of the group by Wickr's infrastructure.

The mechanisms for supporting group messaging are based on Wickr's pairwise messaging protocol. In this system, group managers transmit management messages to individual members of a Wickr system using the existing pairwise protocol. These messages allow the addition of users. These messages are authenticated using the techniques provided by the standard Wickr protocol. Wickr's servers cannot add members to groups, and thus even a compromised server cannot add new members to a group.

To transmit messages to the group, each device in the group must establish a pairwise key with every other device included in the group. This is accomplished using the existing Wickr messaging protocol described above. A single payload encryption key is repeatedly copied and encrypted multiple times using the pairwise encryption mechanisms, once for each device-device relationship. The message contents are encrypted using the payload encryption key. The resulting package includes ciphertexts that are destined for each device in the group and that can be decrypted by any of the appropriate devices.

To deliver messages from one device to other devices, the Wickr servers implement a one-to-many delivery mechanism in which an encrypted payload is delivered to all relevant devices. This delivery requires that Wickr's servers know the membership of the group, but it serves purely as an efficiency measure to avoid unnecessary copying.

As a result of this design, the security guarantees of Wickr's group messaging system are substantially identical to the guarantees offered by the existing Wickr protocol. These include forward secrecy, confidentiality, and authentication.

## Video and audio calling provides the same security assurances as Core protocol — Verified

**SECURITY TEST CRITERIA**

For this security test, the assessment team had the following goal:

- Verify that Wickr's audio and video protocols use correct cryptographic mechanisms.

**FINDINGS**

Wickr accomplishes video and audio encryption by transmitting a separate symmetric encryption key for audio and video calls via the in-band pairwise/group messaging protocols described above. This key is derived using a secure key generation protocol. The security guarantees surrounding the delivery of this key are identical to those for standard messaging delivered via Wickr's core protocol.

## Message content and supporting encryption keys are managed properly on official supported Wickr clients — Verified

### SECURITY TEST CRITERIA

For this security test, the assessment team had the following goals:

- Verify the correctness of the techniques used by Wickr clients to derive and manage encryption keys.
- Ensure that keys are stored and destroyed as described in the Wickr technical whitepaper.

### FINDINGS

The assessment team reviewed the techniques used to derive and manage encryption keys on Wickr clients. This review was conducted in three phases: First, the team reviewed the Wickr technical whitepaper and verified the cryptographic techniques were correct and appropriate for task. Next, the team examined the Wickr client source code and the Wickr cryptographic libraries.

The assessment team determined that Wickr encryption/decryption keys take several forms. These include:

- **Ephemeral keypairs used to derive shared secrets in the elliptic curve Diffie-Hellman protocol.** The assessment team reviewed the Wickr C cryptographic implementation to verify that ephemeral keys are derived on the client, stored locally in NVRAM or hard drive storage, and destroyed when they are no longer required.
- **Derived session keys used to encrypt message contents.** The assessment team verified that encryption keys for message contents are derived on the client (in RAM) and are zeroized when they are no longer required.
- **Key backups.** The assessment team verified that stored identity secret keys are encrypted using a symmetric key derived from the user's passphrase using a memory-hard function (`scrypt`) in RAM and that this encryption key never leaves the client.

The assessment team also verified that Wickr uses techniques to minimize the retention of data on Solid State Drives by generating large temporary files that consume space on the hard drive. While this technique is not guaranteed to ensure the destruction of ephemeral keys stored on these drives, it increases the likelihood that keys will be permanently destroyed beyond the ability of forensic recovery software to obtain them.

Finally, the assessment team verified that no secret decryption keys are transmitted to the server, or otherwise stored on Wickr infrastructure.

# Wickr manages sensitive customer data in cloud-hosted networks in accordance with the Wickr Privacy Policy — Verified

**SECURITY TEST CRITERIA**

For this security test, the assessment team had the following goals:

- Verify the techniques used to record cloud-hosted Wickr data and logs.
- Ensure that all data storage and logging is consistent with the current Wickr privacy policies.

**FINDINGS**

Wickr maintains its server infrastructure in the Amazon Web Services cloud. The system consists of a number of virtual servers that manage stored account and ciphertext data and ELK repositories for storing logging data. All Wickr servers interface with clients via the Amazon Elastic Load Balancer (ELB) system.

The assessment team reviewed Wickr's privacy policy for Wickr ME and Wickr Pro[2] and consulted with Wickr engineers to verify data retention policies. With the assistance of Wickr engineers, the team examined Wickr's log databases to verify that the logged information matched Wickr's stated policies. The team further reviewed portions of Wickr's server-side logging code to ensure that this code logged data consistent with Wickr's privacy policies.

The team determined that Wickr stores data in a manner consistent with the stated policies for Wickr ME and Wickr Pro. Specifically:

- In the case of Wickr ME, the team verified that Wickr stores encrypted messaging data for up to six days prior to delivery. In the case of Wickr Pro, the team verified that Wickr stores encrypted messaging data for up to 30 days prior to delivery. This represents an upper bound on storage time.
- The team verified by inspection of the server logs that Wickr logs only the IP address of the Wickr load balancer, and does not record IP addresses of clients accessing the system. Wickr engineers assert that they do not record or retain logs from the Amazon ELB.
- The team verified by inspection of the server logs and server-side logging code that Wickr logs account events, including registration, login, and message transmission events, for a duration of seven days. These logs incorporate the time of a message transmission and the sender username (for Wickr Pro) or a hash of the sender's

---

[2] Both privacy policies can be found at: https://wickr.com/privacy/

username (for Wickr ME). The team verified that Wickr does not record the identity of intended message recipients in the log.

- The team verified through discussion with Wickr engineers and through code inspection that Wickr contact discovery does not transmit plaintext phone numbers to Wickr's servers. Phone numbers from a client's contact list are hashed using a time-consuming hash function that involves several thousand iterations of SHA256, and only the resulting hashes are transmitted to the server for matching. These hashed phone numbers are used only for contact matching and are not stored on Wickr's servers.
- The assessment team confirmed that Wickr implements throttling to restrict the number of searches for a given identifier.
- To provide for multi-device support, Wickr stores an encrypted copy of device identity secret keys on the Wickr infrastructure. This data is encrypted using a secret key derived from the user's password via the memory-hard `scrypt` key derivation function.

The assessment team notes that these findings do not address log data that may be retained by Wickr's cloud hosting provider, Amazon Web Services. Determining how this data is recorded was outside the scope of the assessment.