NoTrace Messenger Privacy & Security

	TRUST ESTABLISHMENT						CONVERSATION SECURITY												TRANSPORT PRIVACY				
	Network MitM Prevention	Operator MitM Prevention	Operator MitM Detection	Operator Accountability	Key Revocation Possible	Privacy Preserving	Confidentiality	Authentication	Participant Consistency	Destination Validation	Forward Secrecy	Backward Secrecy	Anonymity Preserving	Speaker Consistency	Causality Preserving	Global Transcript	Message Unlinkability	Message Repudiation	Participation Repudiation	Sender Anonymity	Recipient Anonymity	Participation Anonymity	Unlinkability	Global Adversary Resistant
Chat Message																								
NoTrace Direct	N/A	N/A	N/A	N/A	-	+	+	+	+	-	+-	+-	+	-	-	-	+	+	+	+	+	+	+	-
NoTrace 2 [1]	+	+	+	+	-	+	+	+	-	-	+-	+-	-	-	-	-	+	+	+	+	-	-	+	-
NoTrace 3 [1]	+	+	+	+	-	+	+	+	+	+	+	+	+	+-	+	-	+	+	+	+	-	-	+	-
Signal*	+-	+-	+-	+-	+	+	+	+	+	+	+	+	-	+-	+	-	+	+	+	+	-	-	+	-

[1] Includes all the features of NoTrace Direct but presented herein without them for clarity. By default, serverless communication is used with the server-based method is a fallback option.

+- = Partial; N/A = Not Applicable.

* Signal® is a registered trademark of Signal Messenger LLC. Signal messenger is used herein for comparison.

VERSIONS

NoTrace Direct : serverless — all communications are direct between the communicating parties.

NoTrace 2: NoTrace anonymous chat/signaling server infrastructure.

NoTrace 3: NoTrace anonymous chat/signaling server infrastructure with Signal messaging protocol support.

Network MitM Prevention	N/A	
Operator MitM Prevention	N/A	
Operator MitM Detection	N/A	
Operator Accountability	N/A	
Key Revocation Possible	-	Not possible because Tor address is the same as the public key and it is used as an identifier.
Privacy Preserving	+	No information is leaked to other participants because no operator is present.
Confidentiality	+	Communications are end-to-end (e2e) encrypted (X25519-XSalsa20-Poly1305). Therefore, only the intended recipient(s) can read the messages.
Authentication	+	“Public-key authenticated encryption” provides the authentication.
Participant Consistency	+	Only p2p connections are possible, which are consistent.
Destination Validation	-	Not implemented.
Forward Secrecy	+-	Partially implemented via short lifetime encryption keys (changed periodically).
Backward Secrecy	+-	Partially implemented via short lifetime encryption keys (changed periodically).
Anonymity Preserving	+	P2p communication method.
Speaker Consistency	-	Not implemented.
Causality Preserving	-	Not implemented.
Global Transcript	-	Not implemented.
Message Unlinkability	+	Implemented via “Public-key authenticated encryption”.
Message Repudiation	+	Implemented via “Public-key authenticated encryption”.
Participation Repudiation	+	Implemented via “Public-key authenticated encryption”.
Sender Anonymity	+	Implemented via a “sealed sender” method and Tor.
Recipient Anonymity	+	Implemented via Tor.
Participation Anonymity	+	Implemented via Tor.
Unlinkability	+	Implemented via a “sealed sender” method
Global Adversary Resistant	-	Not implemented.

Network MitM Prevention	+	Key Fingerprint Verification is used to prevent MitM attacks.
Operator MitM Prevention	+	Key Fingerprint Verification is used to prevent MitM attacks.
Operator MitM Detection	+	Key Fingerprint Verification is used to prevent MitM attacks.
Operator Accountability	+	Key Fingerprint Verification verify that operators behaved correctly during trust establishment.
Key Revocation Possible	-	Not possible because Tor address is the same as the public key and it is used as an identifier.
Privacy Preserving	+	Key Fingerprint Verification preserves privacy.
Confidentiality	+	Communications are end-to-end (e2e) encrypted (X25519-XSalsa20-Poly1305). Therefore, only the intended recipient(s) can read messages.
Authentication	+	“Public-key authenticated encryption” provides the authentication.
Participant Consistency	-	Not implemented.
Destination Validation	-	Not implemented.
Forward Secrecy	+-	Partially implemented via short lifetime encryption keys (changed periodically).
Backward Secrecy	+-	Partially implemented via short lifetime encryption keys (changed periodically).
Anonymity Preserving	+	Implemented via a “sealed sender” method and Tor. “Sealed sender” method preserves anonymity of the sender.
Speaker Consistency	-	Not implemented.
Causality Preserving	-	Not implemented.
Global Transcript	-	Not implemented.
Message Unlinkability	+	Implemented via “Public-key authenticated encryption”.
Message Repudiation	+	Implemented via “Public-key authenticated encryption”.
Participation Repudiation	+	Implemented via “Public-key authenticated encryption”.
Sender Anonymity	+	Implemented via a “sealed sender” method and Tor.
Recipient Anonymity	-	Not implemented.
Participation Anonymity	-	Not implemented.
Unlinkability	+	Implemented via a “sealed sender” method.
Global Adversary Resistant	-	Not implemented.

Network MitM Prevention	+	Key Fingerprint Verification is used to prevent MitM attacks.
Operator MitM Prevention	+	Key Fingerprint Verification is used to prevent MitM attacks.
Operator MitM Detection	+	Key Fingerprint Verification is used to prevent MitM attacks.
Operator Accountability	+	Key Fingerprint Verification verify that operators behaved correctly during trust establishment.
Key Revocation Possible	-	Not possible because Tor address is the same as the public key and it is used as an identifier.
Privacy Preserving	+	Key Fingerprint Verification preserves privacy.
Confidentiality	+	Communications are end-to-end (e2e) encrypted (X3DH-AES-256-SHA-256). Therefore, only the intended recipient(s) can read messages.
Authentication	+	HKDF based on SHA-256 provides the authentication.
Participant Consistency	+	Implemented with authenticated key exchange.
Destination Validation	+	Implemented with authenticated key exchange.
Forward Secrecy	+	Implemented via Double-Ratchet (Axolotl) algorithm.
Backward Secrecy	+	Implemented via Double-Ratchet (Axolotl) algorithm.
Anonymity Preserving	+	Implemented via a “sealed sender” method and Tor. “Sealed sender” method preserves anonymity of the sender.
Speaker Consistency	+-	Partially obtained with use of key derivation functions (KDFs) - messages cannot be dropped by an adversary without dropping future messages.
Causality Preserving	+	Achieved by attaching preceding message identifiers to messages.
Global Transcript	-	Not implemented.
Message Unlinkability	+	Implied since messages are authenticated with shared MAC.
Message Repudiation	+	Implied since messages are authenticated with shared MAC.
Participation Repudiation	+	Implemented via triple DH (3-DH) handshake.
Sender Anonymity	+	Implemented via a “sealed sender” method and Tor.
Recipient Anonymity	-	Not implemented.
Participation Anonymity	-	Not implemented.
Unlinkability	+	Implemented via a “sealed sender” method.
Global Adversary Resistant	-	Not implemented.

Trust Establishment

Security and Privacy

- **Network MitM Prevention:** Prevents Man-in-the-Middle (MitM) attacks by local and global network adversaries.
- **Operator MitM Prevention:** Prevents MitM attacks executed by infrastructure operators.
- **Operator MitM Detection:** Allows the detection of MitM attacks performed by operators after they have occurred.
- **Operator Accountability:** It is possible to verify that operators behaved correctly during trust establishment.
- **Key Revocation Possible:** Users can revoke and renew keys (e.g., to recover from key loss or compromise).
- **Privacy Preserving:** The approach leaks no conversation metadata to other participants or even service operators.

Conversation Security

Security and Privacy

- **Confidentiality:** Only the intended recipients are able to read a message. Specifically, the message must not be readable by a server operator that is not a conversation participant.
- **Integrity:** No honest party will accept a message that has been modified in transit.
- **Authentication:** Each participant in the conversation receives proof of possession of a known long-term secret from all other participants that they believe to be participating in the conversation. In addition, each participant is able to verify that a message was sent from the claimed source.
- **Participant Consistency:** At any point when a message is accepted by an honest party, all honest parties are guaranteed to have the same view of the participant list.
- **Destination Validation:** When a message is accepted by an honest party, they can verify that they were included in the set of intended recipients for the message.
- **Forward Secrecy:** Compromising all key material does not enable decryption of previously encrypted data.
- **Backward Secrecy:** Compromising all key material does not enable decryption of succeeding encrypted data.
- **Anonymity Preserving:** Any anonymity features provided by the underlying transport privacy architecture are not undermined (e.g., if the transport privacy system provides anonymity, the conversation security level does not deanonymize users by linking key identifiers).
- **Speaker Consistency:** All participants agree on the sequence of messages sent by each participant. A protocol might perform consistency checks on blocks of messages during the protocol, or after every message is sent.
- **Causality Preserving:** Implementations can avoid displaying a

message before messages that causally precede it.

- **Global Transcript:** All participants see all messages in the same order.
- **Message Unlinkability:** If one authored one message in the conversation, this does not provide evidence that he/she authored other messages.
- **Message Repudiation:** Given a conversation transcript and all cryptographic keys, there is no evidence that a given message was authored by any particular user.
- **Participation Repudiation:** Given a conversation transcript and all cryptographic key material for all but one accused (honest) participant, there is no evidence that the honest participant was in a conversation with any of the other participants.

Transport Privacy

The transport privacy layer defines how messages are exchanged, with the goal of hiding message metadata.

Privacy Features

- **Sender Anonymity:** When a chat message is received, no non-global entities except for the sender can determine which entity produced the message.
- **Recipient Anonymity:** No non-global entities except the receiver of a chat message know which entity received it.
- **Participation Anonymity:** No non-global entities except the conversation participants can discover which set of network nodes are engaged in a conversation.
- **Unlinkability:** No non-global entities except the conversation participants can discover that two protocol messages belong to the same conversation.
- **Global Adversary Resistant:** Global adversaries cannot break the anonymity.