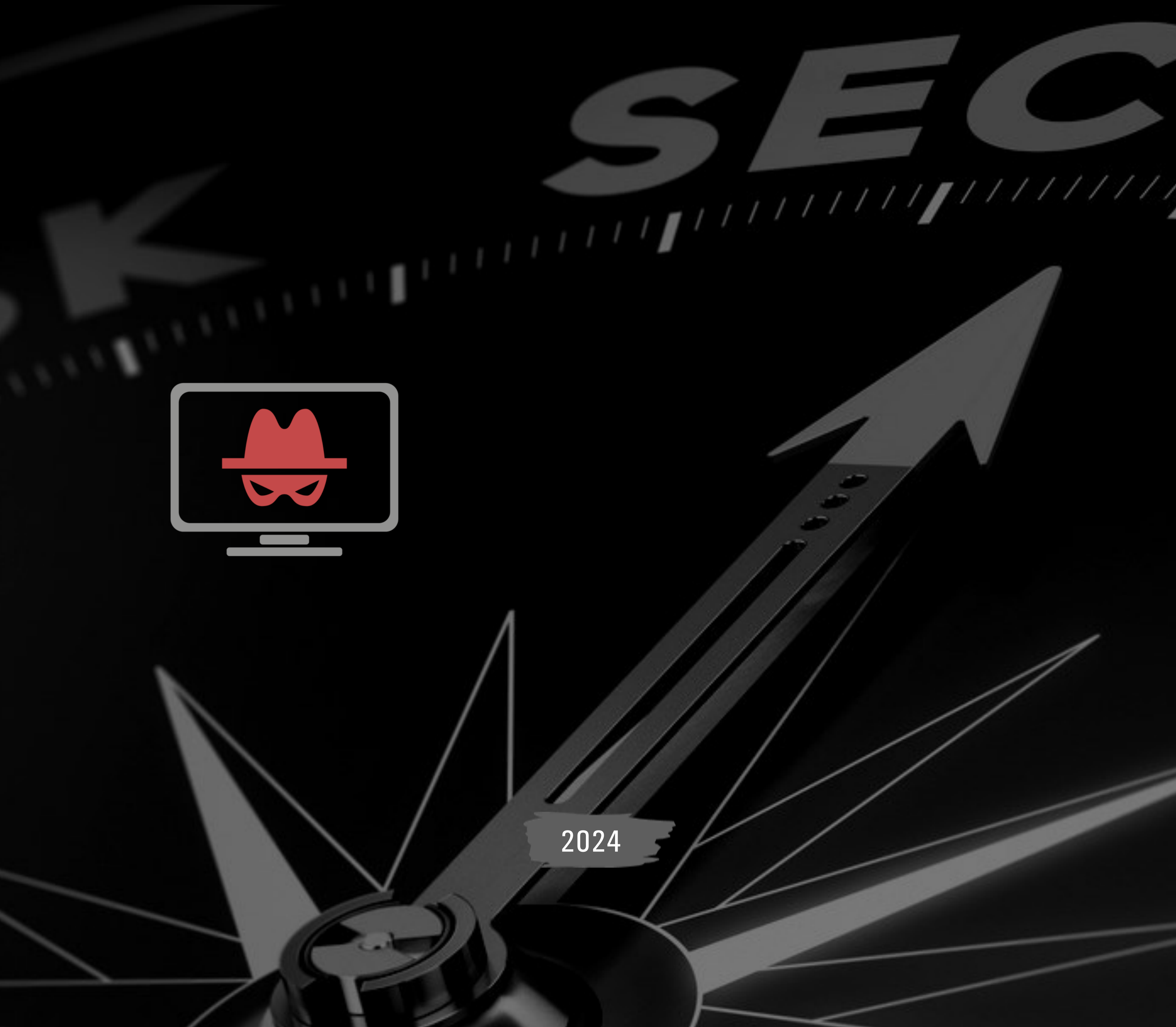
NoTrace

Solution Roadmap | **Security & Privacy**

MULTIMEDIA/COMMUNICATION PLATFORM

EMPOWERING YOUR RIGHTS OVER YOUR OWN INFORMATION



2024

Table of Contents

NoTrace 3

NoTrace Current Services 4

Direct Voice 4

Direct Messaging 4

NoTrace Future Services 5

Chat 5

Pay 5

Blog 5

VOD 6

Ads 6

Marketplace 7

Phone 8

Voicemail 8

Privacy & Security 9

NoTrace Direct 10

NoTrace 2 11

NoTrace 3 12

Definitions 13

NoTrace is for

- Empowering and sustaining democratic societies, being an enabling element of media freedom
- Economic viability and long-term sustainability of quality journalism
- All legitimate users for whom privacy matters
- Journalists, publishers, and their sources
- Activists in repressive countries and the concerned organizations

We stand for

- Freedom of speech and expression for all people
- Independent, pluralistic, and quality media

Key benefit

- Peace of mind — be safe and protected while freely communicating publicly and privately, sharing and monetizing digital content

NoTrace

PRIVACY-CENTRIC COMMUNICATION/MULTIMEDIA PLATFORM, PROVIDING CONFIDENTIALITY AND PRIVACY FOR VOICE, CHAT, SOCIAL COMMUNICATIONS, AND E-COMMERCE TRANSACTIONS

NoTrace develops a unique privacy-centric, secure multi-channel communication, social media, and peer-to-peer marketplace platform. It allows users to securely communicate, broadcast, and monetize digital content, as well as advertise and sell products — all in complete privacy.

> *NoTrace is like Telegram® and Craigslist® but with full privacy*

NoTrace is similar and it is just as easy to use as other communication and social media solutions. However, it leverages unique NoTrace technologies to provide unmatched privacy, confidentiality, and resistance to blocking attempts. It is also the only commercial service today capable of providing true anonymity when calling a regular telephone network.

Contrary to popular belief, security and privacy are not synonymous. Privacy relates to protecting information about you, while security refers to protecting your information. Today, protecting your privacy is more challenging than just providing security. However, NoTrace gives you both, and it does it on a level that others cannot.

Using NoTrace and following information security best practices, you can turn your ordinary smartphone into a device that enables you to freely communicate publicly and privately, share and monetize your digital content, buy, sell, and make electronic payments — all in complete privacy.

NoTrace Current Services

Direct Voice

NoTrace offers anonymous, end-to-end encrypted direct over-the-Internet voice calls. Direct means that the parties communicate without an operator. Thus, no operator's side metadata is generated, relying on The Onion Router (Tor) for anonymization. However, since NoTrace does not use carriers' push messages (to protect user privacy), both parties must be online, and the receiving app must be awake. This is a small usability tradeoff, should the receiving party remain truly anonymous. Currently, this is the only over-the-Internet voice service that fully preserves callers' privacy.

- Voice calls
- End-to-end encryption
- No IP address
- No operator and no metadata

Direct Messaging

NoTrace offers serverless messaging and media sharing, which means that the information is sent directly from one party to another without an operator. This is the most private Internet communication option available today. All information is end-to-end encrypted, and no operator means that no operator-side metadata is generated. However, to preserve maximum user privacy, NoTrace does not use carriers' push messages — a small usability tradeoff, meaning that if the app is asleep, there could be a delay in receiving new messages.

- Text and voice messages
- Pictures, videos and files
- End-to-end encryption
- No IP address
- No operator and no metadata

Privacy

NoTrace is intended for legal purposes only, such as for journalists and their sources, activists in repressive countries, and all other legitimate users for whom privacy matters. It shall not be used for illegal purposes. We stand for and support the freedom of speech for all people, as well as free and independent media. No other solution today offers the same level of privacy across communication channels as NoTrace.

NoTrace

Website: https://notrace.app

Email: support@notrace.app

NoTrace: hmmyhxg34umia7fpbzuxdel526uxy3bqetzyh662y6lrpymt22jtipqd

Crypto (ETH): notrace.eth

Contribute through Open Collective (US/EU tax deductible): https://opencollective.com/notrace-feature-bounty

NoTrace Future Services

Chat

NoTrace plans to offer a unique secure chat/media sharing service that guarantees message delivery while still preserving full user privacy — the level of privacy that no other Internet chat offers today. All messages are end-to-end encrypted, and thanks to NoTrace's unique technology, no sensitive metadata is generated. Therefore, trusting NoTrace is not required. No one, including NoTrace, has knowledge about the communicating parties or even the fact of communication itself. In addition, where possible, NoTrace uses its Direct Messaging service for even greater privacy.

- Text and voice messages
- Pictures, videos and files
- Group chat
- End-to-end encryption
- No IP address
- No sensitive metadata

Pay

NoTrace Pay is an Ethereum-based crypto token payment service, but with full user privacy. NoTrace leverages its unique technology — a combination of a non-private blockchain, such as Ethereum, where transactions are public (amount, wallet address, date/time, etc.) and a NoTrace messaging platform that allows the transfer of control over crypto-assets from one party to another in full privacy. All transactions between the parties are encrypted, and no sensitive metadata is generated. With NoTrace Pay, payments can be made using public blockchain -based crypto tokens without revealing the transaction itself and recording it on the ledger.

- Peer-to-peer private payments with Ethereum-based crypto tokens
- Nontraceable payment "vouchers"
- Integration with NoTrace Blogs and NoTrace Marketplace
- End-to-end encryption
- No blockchain transaction record
- No payer and payee IP addresses
- No sensitive metadata

Blogs

NoTrace Blogs is a microblog service for broadcasting multimedia content to large audiences while providing complete privacy to both viewers and publishers. Similar to other public and private discussion boards, publishers can interact with subscribers, directly monetize their content through

NoTrace Pay, and participate in the platform's monetization services, such as NoTrace Ads (ad revenue sharing), while remaining anonymous.

In addition, NoTrace will allow users to reserve unique public names, and for those who prefer to disclose their identity, NoTrace will provide an identity verification service. Even if a blogger's identity is publicly known, it won't impact its ability to directly monetize its blog, and its Internet whereabouts will remain unknown to everyone, including NoTrace.

To reach a wider audience, NoTrace public blogs can be embedded in websites and viewed without the NoTrace app. However, in this case, only the publisher's privacy will be preserved.

- Public blogs (anyone can subscribe)
- Private blogs (subscribers must be approved)
- Rich text/HTML and embedded media (including NoTrace VOD)
- Moderated reply threads
- Emoji reactions
- Admin rights delegation
- Exclusive name reservation
- Flagging to report inappropriate postings
- Public blog widgets and API for easy website integration
- Paid search engine promotion of blogs
- Direct and indirect (through NoTrace Ads) content monetization
- No publisher and viewer IP addresses
- No sensitive metadata

VOD

The NoTrace Video on Demand (VOD) service will allow users to embed pre-recorded video and audio content in chat messages and public or private blogs. The content is then streamed to viewers on demand while maintaining the privacy of both publishers and viewers. If the VOD content is shared in a private blog or chat, it is automatically encrypted and can be viewed only by the intended recipients.

- Embeddable VOD for blogs and messages
- Encrypted and access controlled for private blogs and messages
- No publisher and viewer IP addresses
- No sensitive metadata

Ads

NoTrace Ads is a NoTrace-operated online advertisement service that works in concert with NoTrace Blogs and NoTrace Marketplace to analyze

the platform’s public content and deliver contextual advertisements.

Publishers of popular blogs can get up to 65% of the revenue NoTrace receives from advertisers for displaying ads in their blogs. NoTrace utilizes an ad management platform and fully manages the service, giving its publishers another monetization option while preserving their full privacy.

- Contextual targeting (AI-enhanced public content/topic analysis)
- Single advertising format (lightweight text/ multimedia ads)
- Up to 65% revenue sharing with publishers
- CPM payment model (paid monthly through NoTrace Pay)
- Publisher’s control over the ads inventory
- Flagging to report inappropriate ads
- Full privacy of publishers and viewers (operated by NoTrace)

Marketplace

NoTrace Marketplace is an online classified advertisement/customer-to-customer marketplace that connects people who want to sell or rent any kind of product or service with people who need that product or service — all in complete privacy.

The marketplace will be primarily focused on local buyers and sellers in specific regions. It is an advertising service that allows users to list a diverse array of items and services, including online retail, job vacancies, gigs, items wanted, and even personals. The platform then connects both parties by allowing them to privately communicate using the platform’s communication services and reach an agreement on the terms of the exchange.

NoTrace does not facilitate the sales process, acting merely as a conduit for negotiation, and will only intervene if a complaint is laid by the parties. To further preserve users’ privacy, NoTrace Pay can be used as a medium of exchange, or the parties can use an alternative payment method.

NoTrace promotes free and open trade; however, it will “lightly” moderate the service to comply with local laws and regulations, such as concerning the "censored" content or to prevent illegal trade.

While NoTrace will not charge users for the listings, certain marketplace services will be monetized. Among them are NoTrace Ads and NoTrace search engine promotion. The fees will vary depending on the product or service category and the region.

- Free listings
- Paid search engine promotion of listings

- Flagging to report inappropriate listings
- Public marketplace widgets and API for easy website integration
- Optional monetization of listings through NoTrace Ads
- Full privacy of sellers and buyers through all the transaction phases
- No buyer and seller IP addresses
- No sensitive metadata

Phone

NoTrace Phone is an anonymous calling service to and from a regular telephone network (PSTN). Using state-of-the-art infrastructure, NoTrace bridges NoTrace Direct Voice with a regular telephone network. With NoTrace Phone, users can own multiple PSTN phone numbers (domestic and international) and make and receive calls completely anonymously.

This service is intended for journalists and their sources, emergency service providers, and other legitimate users where callers' privacy must be preserved. To prevent service misuse, NoTrace requires the account owners to disclose their identities through the NoTrace identity verification service.

Though identity verification is required, NoTrace app users can make and receive calls to and from a regular telephone network while remaining completely anonymous. However, the account owner will be responsible for the service.

- NoTrace voice calls to and from PSTN
- Encrypted up to PSTN
- Call block/screen
- Integrated with NoTrace Pay
- Dedicated domestic and international phone numbers
- No caller's IP address
- Minimum metadata

Voicemail

In addition to NoTrace Phone, NoTrace also offers an anonymous voicemail service. Anyone can leave a message for a NoTrace Phone user by calling its PSTN phone number. The user can then retrieve its voice messages using the NoTrace app while remaining completely anonymous.

- Encrypted up to PSTN
- Encrypted voice message storage
- No voicemail owner's IP address
- Minimum metadata

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.

NoTrace Direct

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.

NoTrace 2

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.

NoTrace 3

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.

Definitions

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.