UBINODES

FEATURES FOR COMMUNICATION APPS

Features for Communication apps.

To benchmark communication applications systematically, ensuring comprehensive feature coverage across our articles, we formulated a review checklist.

1.1 Code & developers.

- Code: The code should be open source or audited by a trusted third party.
- License: The app should be either Free Open Source Software (FOSS) or operate on a freemium model.
- Maintenance: The app should be actively maintained with regular updates.
- Support: The provider should offer emergency assistance and respond to user support requests.
- In-App Communication with Support Team: Users should be able to communicate directly with the support team within the app.
- Whitepaper: A detailed whitepaper explaining the concept should be available.
- Ownership: It should be clear who is responsible for the app's development and maintenance.

1.2 Package.

- Code: The code should be open source or audited by a trusted third party.
- License: The app should be either Free Open Source Software (FOSS) or operate on a freemium model.
- Maintenance: The app should be actively maintained with regular updates.
- Support: The provider should offer emergency assistance and respond to user support requests.
- In-App Communication with Support Team: Users should be able to communicate directly with the support team within the app.
- Whitepaper: A detailed whitepaper explaining the concept should be available.
- Ownership: It should be clear who is responsible for the app's development and maintenance.

1.3 Usability.

- **Intuitive Adoption**: User-friendly for everyone, simplifying installation and feature usage.
- **Uniform Features**: Consistent features across various operating systems like Android, iOS, Windows, and Linux.
- **User Administration**: Admin capabilities for communication apps and websites/blogs, allowing invitation, removal, moderation, and editor access.
- **Desktop Application**: Supports desktop apps for enhanced productivity and ease of use.
- **Synchronicity**: Enables offline messaging, allowing communication without both parties being connected simultaneously, addressing the limitation of peer-to-peer apps like Jami or Briar.
- **Content Search**: In-app content search engine that works offline.
- **Contact Search**: Search field for locating contacts within the app's contact list.
- **QR Code for Contact**: Streamlined contact addition through QR code scanning.
- **QR Code for Additional Device**: Effortless addition of new devices via barcode scanning, eliminating the need to re-enter credentials.
- **File Support**: Specifies supported file types, including text, images, video, and sound.
- **Delivery and Read Receipts**: Notifies the sender about message delivery and read status.
- **Typing Indicator**: Indicates when your contact is typing.
- **App Notifications**: Displays the number of new messages and allows customizable notification settings for vibration, sound, and deletion.
- **Message Notifications**: Manage notification preferences for different message types (direct chat, group, forum).
- **Trimming**: Option to trim older messages based on date or size.
- **Export**: Encrypts data for secure export to an external device or cloud for device migration.
- **Device Synchronization**: Ensures messages and contacts are synchronized across devices for seamless chat transitions.
- **Night Mode**: Enables a dark mode for reduced eye strain.
- **Status Indicator**: Allows users to indicate availability or choose to hide it.
- **Quote**: Facilitates quoting and replying to specific messages within a chat.
- **Format**: Supports text formatting options like bold, italic, and strikethrough.
- **Go to Last Message Button**: Quick navigation to the latest message in a chat.
- **Chat Continuity**: Resumes conversations from where they were left off upon returning.
- **Contact List**: A dedicated list for managing contacts.
- **Multi-Account**: Supports multiple accounts on a single device.
- **Message Segregation**: Separates one-on-one, group, and forum messages into distinct spaces.

- **Screen Rotation**: Automatically rotates the app when the device is rotated, enhancing user experience.

1.4 Productivity.

- Provides Forums:
- Provides private blog:
- Provides RSS feed:
- File sharing: Ability to share any type of files with contacts
- Own domain name: For emails.
- Can share GPS position:
- Supports bots:
- Voice meetings:
- Video meetings:
- Group invite by link: Ability to invite by giving a link.
- Contact member of a group: Ability to see group members and contact them oneonone.
- IRC like commands: Can obtain lists by using "/" commands.

1.5 Security & Privacy.

- No Identifying Information: No personal details (email, phone number, credit card) are collected during purchase and setup.
- No Permission Requests for Device Access: Installation does not involve accessing device data, contacts, or media files.
- Resistance to State-Sponsored Criminals: Guards against legal misconduct by corrupt state entities, mitigating interception of IMAP, POP3, TLS, SSL, and email provider SSL certificate spoofing. Ensures protection against unauthorized access to SMS and emails.
- Not in a Five Eyes Country: App development and server usage are not associated with Australia, Canada, New Zealand, the United Kingdom, or the United States.
- End-to-End Encryption: Ensures cryptographic security for every message and file.
- Encrypted by Default: Applies encryption automatically to both direct and group chats, not as an optional feature.
- Zero-Knowledge: Encryption key remains on the user's device, not shared with the server. Data is not stored on a central server after delivery, and no logs are retained.
- Ephemerality: Messages are automatically deleted from all recipients' devices after a set time period.
- Data Shredding: Deleted files are rendered unrecoverable by forensic software.
- Chat History: New group members or added devices may or may not have access to older messages based on the threat model. Access is restricted as a security measure.
- Tamper-Proof: Warns of Man-in-the-Middle attacks or any attempt to tamper with communication, data, or updates.

- Security Word: Allows verification of communication integrity through a security word at the beginning of each voice call.
- Contact Verification: Enables verification of addressees through device fingerprinting, with a list in the app's settings.
- Auto Log Off: The app logs off after a set delay, distinct from screen lock.
- Password Protected: Requires a password or code when launching the app.
- No Recovery Option: Eliminates recovery via email or SMS to protect against state-sponsored criminals. Recovery options include a code, seed phrase, or none.
- Data at Rest is Encrypted: Decryption occurs at app launch, and messages remain inaccessible to third parties, even under legal compulsion.
- Anonymous: Sends data through anonymizing networks and encrypts metadata.
- Plausible Deniability: Prevents the creation of identical IDs (same fingerprint) on different devices.
- Prohibits Screenshot: Can prevent recipients from taking screenshots.
- Screenshot Warning: Sends a notification to the sender if the addressee takes a screenshot.
- Lock Screen: Allows setting a delay to lock the screen after inactivity.
- Disable Keyboard Learning: Disables the device's keyboard learning.
- Disable Link Preview: Option to disable link preview in messages.
- ID Revocation: Ability to revoke an ID from a website if devices are compromised.
- Panic Button: Ability to trigger an action to delete data or the account.
- Mobile Data In-App Deactivation: Ability to deactivate the use of mobile data in app settings.
- Off-Grid Connection: Possibility to connect directly using Bluetooth or Wi-Fi without the internet.
- Decentralization or Distribution: Members can communicate even without a central server or host.
- Delete Own Messages: Ability to delete a message from all devices and recipients' devices.
- Delete Groups: Ability to delete a group so it disappears from all members' devices.
- Transparency Report or Warrant Canary: Publicly shares any request received by a governmental agency.
- Access and Activity Logs: Provides information on when and by whom the app has been accessed.
- IP Restrictions: Restricts access to pre-approved IP addresses.
- TOR Signup: Ability to create an account using TOR.
- Self-Destruct Account: Account is deleted after a set period without logging in.

1.6 Price and value.

- Cost-Efficiency: Offers affordable plans suitable for large user bases, such as a 15-member team, with options for a monthly fee or a one-time license fee.
- Anonymous Payment: Accepts payments via anonymous cryptocurrencies like Monero.
- Group Size Limitations: Group size limits vary across platforms (e.g., Wickr allows 50 members, Threema accommodates 100, Wire supports 250, while Telegram permits thousands).
- File Sharing: Specifies the maximum file size for sharing, including videos, which varies per platform.

