Encipher

Decentralized & Distributed Secure Messaging System

Powered by **KAINOTOMIA,** a sister concern of **Prelysis Communications**
Info@kainotomia.tech
kobi@prelysis.com
+1-800-456-478-23

Why Encipher?

The government and armed forces have unique challenges to manage sensitive data

Armed forces and government organizations have unique challenges to communicate while also protecting critical information doing so.

Encipher is a secure military-grade end-to-end decentralized messaging platform that leveraged a well thought-out military messaging solution that comes with the best possible benefits for your organization.

What is Encipher?

- Encipher is a military-grade secure instant communication platform that is custom-built for defense organizations, government entities, and large corporate enterprises.
- Organize virtual meetings that include audio/video calls, screen sharing.
- High-efficiency collaboration features, made for low-internet bandwidths.
- Shields your files and interactions

Why You Shouldn’t Use WhatsApp Or Other Commercial Messaging Services For Official Communication?

- Does not allow you to host the communications data on your servers and your data is dissected through metadata for commercial benefits leaving your security under risk while your communication contains the most critical and sensitive information of your country or organization.
- Limited administrative controls for groups.
- Lack of ownership of Sovereign Data and the data cannot be erased or claimed or suspended, if and when needed – once uploaded belongs to the corporation who is providing you the service.
- Not secured, as the application(s) is also allows personal communications, on the same platform making the data leak a real threat.
- Government Policy Violation as the data is stored usually outside your country.
- Can be exploited through personal communications to compromise the device and all data in it.

Encipher Features

Security-Level Benefits

- Multi-layered security for all communications
- Data encryption while at transit and rest
- Multi-layered admin privileges
- Mitigates the risk of data theft
- High-quality audio/video calling/conferencing
- Private chat burnout window for confidential conversations
- Use proven security protocols and practices

Feature-Level Benefits

- Real-time defense collaboration tools allowing multi-domain operations once integrated into the force intranet.
- Group conversations with strict administration rights.
- Works best for high latency satellite communications
- Designed for private networks
- Bio-metric and Passcode authentication access

Use Cases

- Made for all hierarchies

Report your higher authorities of all cadres just right within a single interface. Role based communication means that you have a firm grip on interorganizational communication – be it military or corporate.

- Meetings

Shift your conference room meetings to Encipher quick chat groups. Get to know field level operational details to make quick command decisions using this defense collaboration tool seamlessly.

- Stay in touch with people around you

Integrate our chat APIs to communicate with the people of your zone to increase awareness of the services you extend to them. This can also be integrated into battle management systems for multi-domain operations.

- Learning and Development

Train your teams online through Encipher chat groups. This military-grade chat application offers you end-to-end encrypted chats and calls allowing you to train your team on sensitive issues without anyone else prying on the details.

- Dedicated War Rooms

Respond and react promptly in all sudden and major incidents and outbreaks. Create a shared workspace and exchange ideas and information to understand and redefine the priorities in evolving scenarios.

- Informed investigations

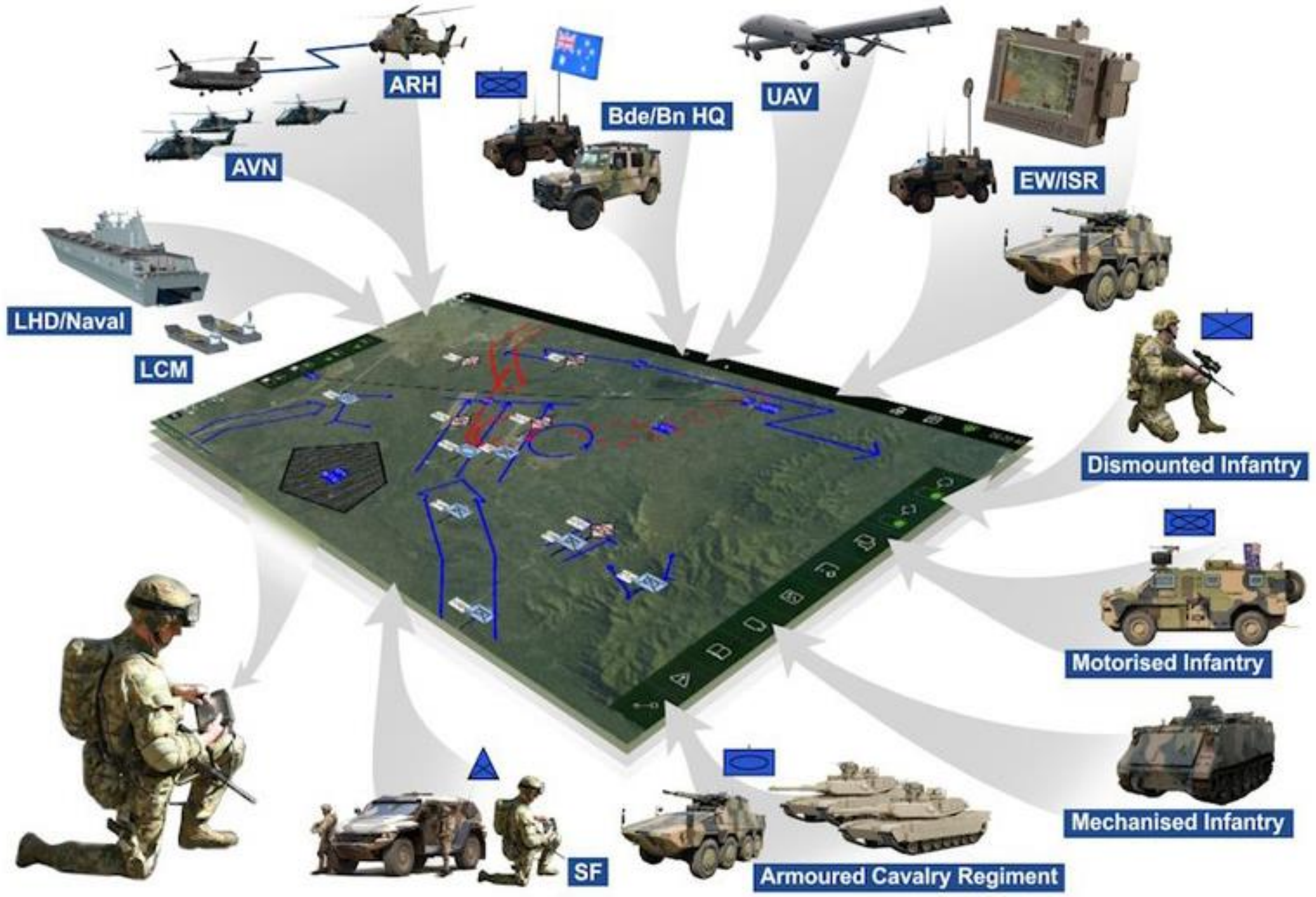
Stay in touch with your subordinates to receive prompt information updates on all the nationwide operations and investigations that you handle.

Designed for Tactical & Strategic Defence Communications

- Helps communicate between your ground-based, airborne, and sea-based tactical and strategic assets with high-trust messaging and voice-video calling abilities.
- A collaborative and user-friendly unified digital workspace that shall bring your Command & Control systems and hierarchies to a single interface.
- Takes care of your armed force's command and control instructions using an encrypted messaging window.
- Has role-based access control for enhanced communication security.

Works in your Air-Gapped networks

- Works on your isolated networks to protect your communication, securely.
- Made for compliance-minded organizations
- Single communication interface which works across all terrains where the bandwidths are low and have high latency, such as satellite transmissions.
- Enables rapid recovery in the case of data theft or loss.
- Shaping it up to a fully-grown defense-grade product with a secured offline-based on-premise communication system.
- Can create a seamless communication network over long distances using digital HF radios to create an intranet infrastructure providing a protected communication network between friendly forces spread-out geographically.
- If used as a communication backbone it can enable multi-domain operations



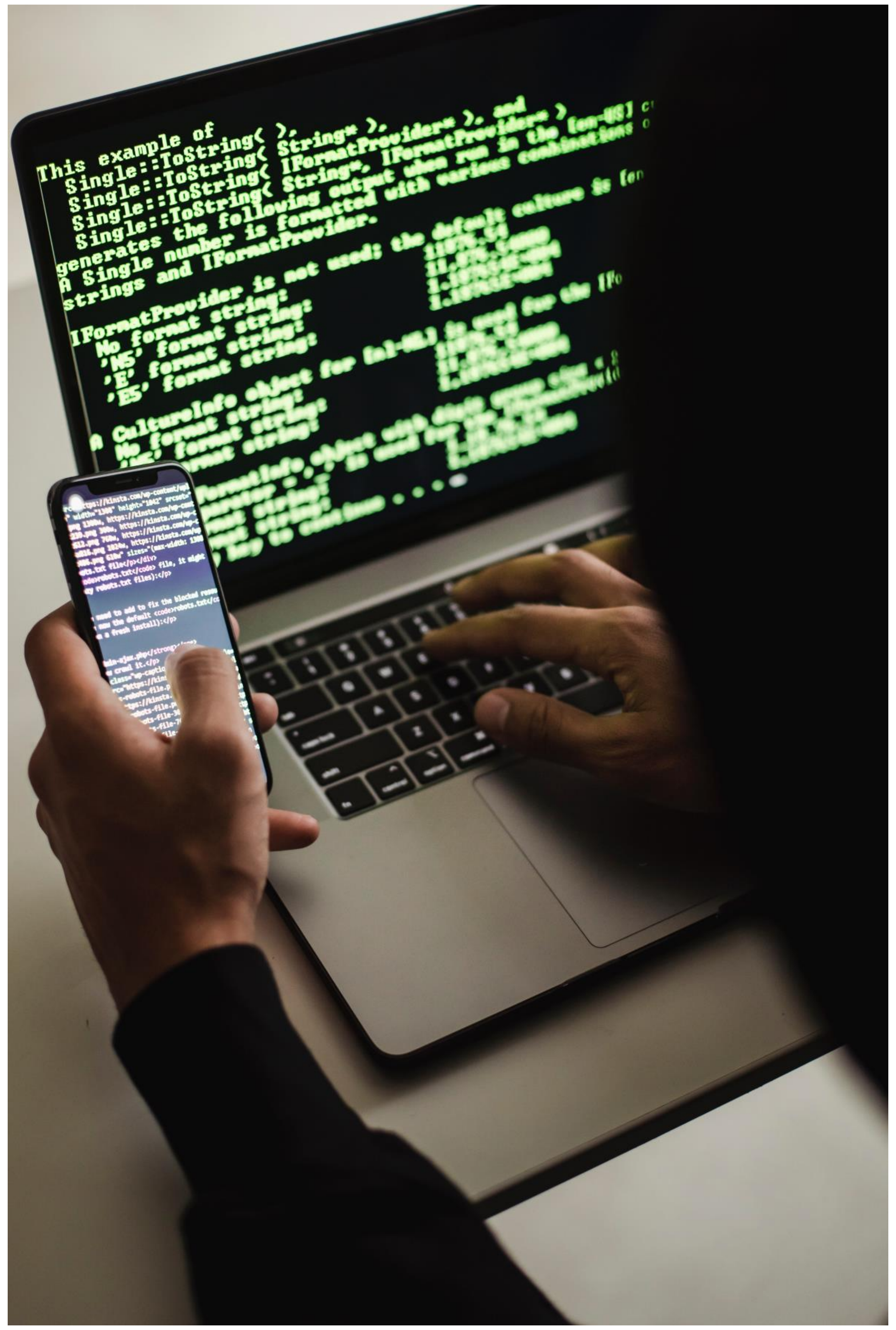
End-to-End Encrypted

- Allows you to exchange your defense communications' situational awareness across completely encrypted channels.
- We employ Curve25519, AES-256, and HMAC-SHA256 as primitives and use the world's best and proven security protocols and procedures, which combine the Double Ratchet algorithm, Pre-keys, and a triple Elliptic-curve Diffie–Hellman (3-DH) handshake.
- End-to-end encryption protects all communication channels, including texting, audio-video conversations, conferencing, and screen sharing.
- Third-party intruders or hackers will be unable to view the message's contents.

C3 Systems [Command-Control-Communication]

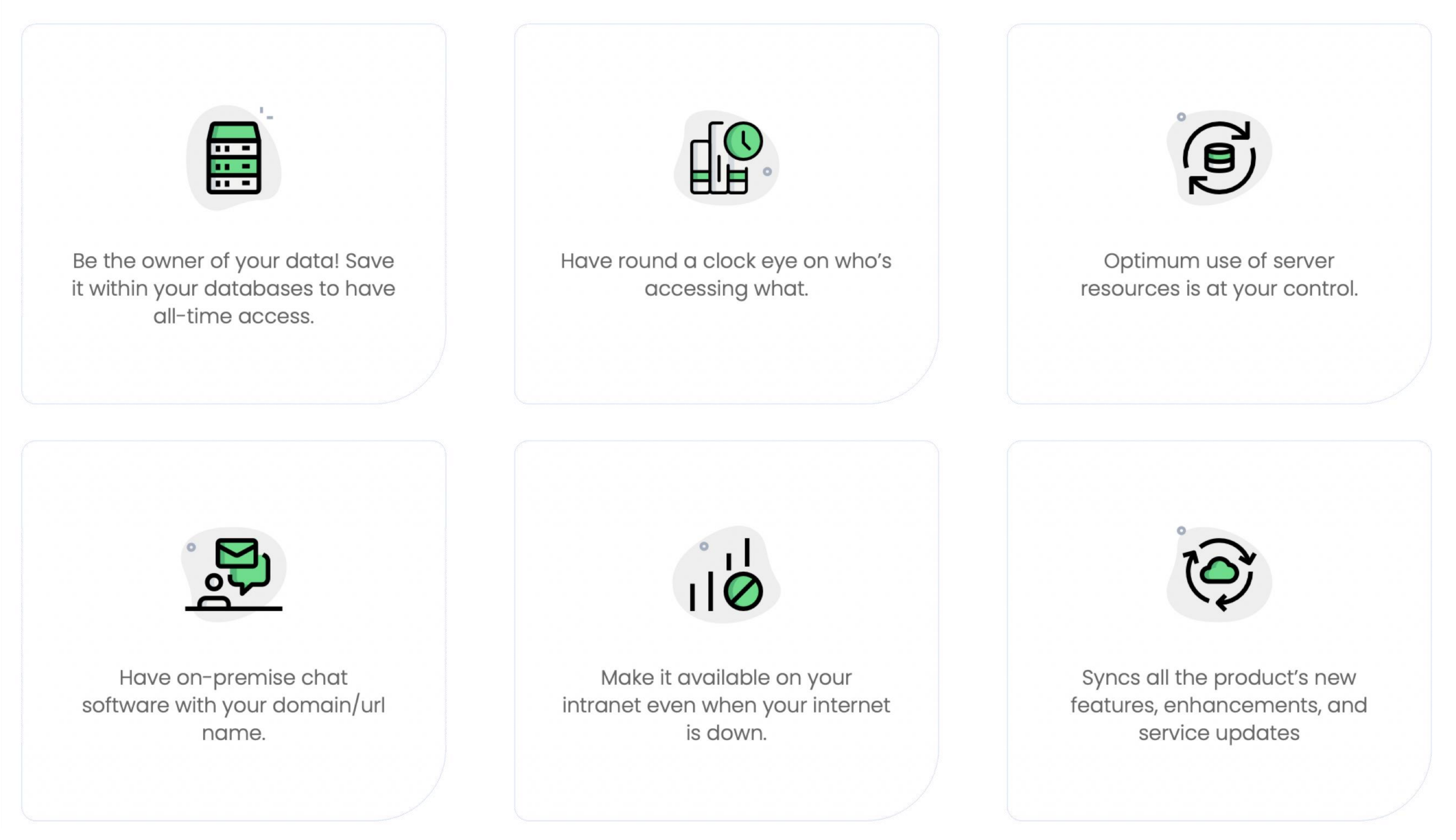
- Can be integrated with battle management systems
- This secure and unified digital workspace lets you bring your Ministry of Defense (MoD) & hierarchies of all departments and troops to communicate over mission-critical controls.
- Encipher takes care of important components of messaging & collaboration within your military systems which can help accomplish the organization’s objectives and goals.
- Carry out the communication of your complex C3 functions seamlessly across all the end-points and keep track of friendly, neutral, enemy ships, aircraft & weapon systems, and soldiers.

Units & Master-Unit Module



- The Units functionality helps you segregate your office staff, for quick and fast communication and reachability.
- Configure Units based on locations, department, real projects, or cross-functional teams. United by interface and separated by geographies.
- Create Master-Units, which can include multiple Units, which are related.
- Restrict or Allow access for personnel between different Units, by writing Rules.
- Know who are stationed at which locations.
- Our ‘User Authorizations’ feature will help restrict personnel access to the top management, restricted and need-on basis.
- This module is scalable to add large volumes of users, and best suited for Armed Forces.

On-Premise Deployment



Be the owner of your data! Save it within your databases to have all-time access.

Have round a clock eye on who's accessing what.

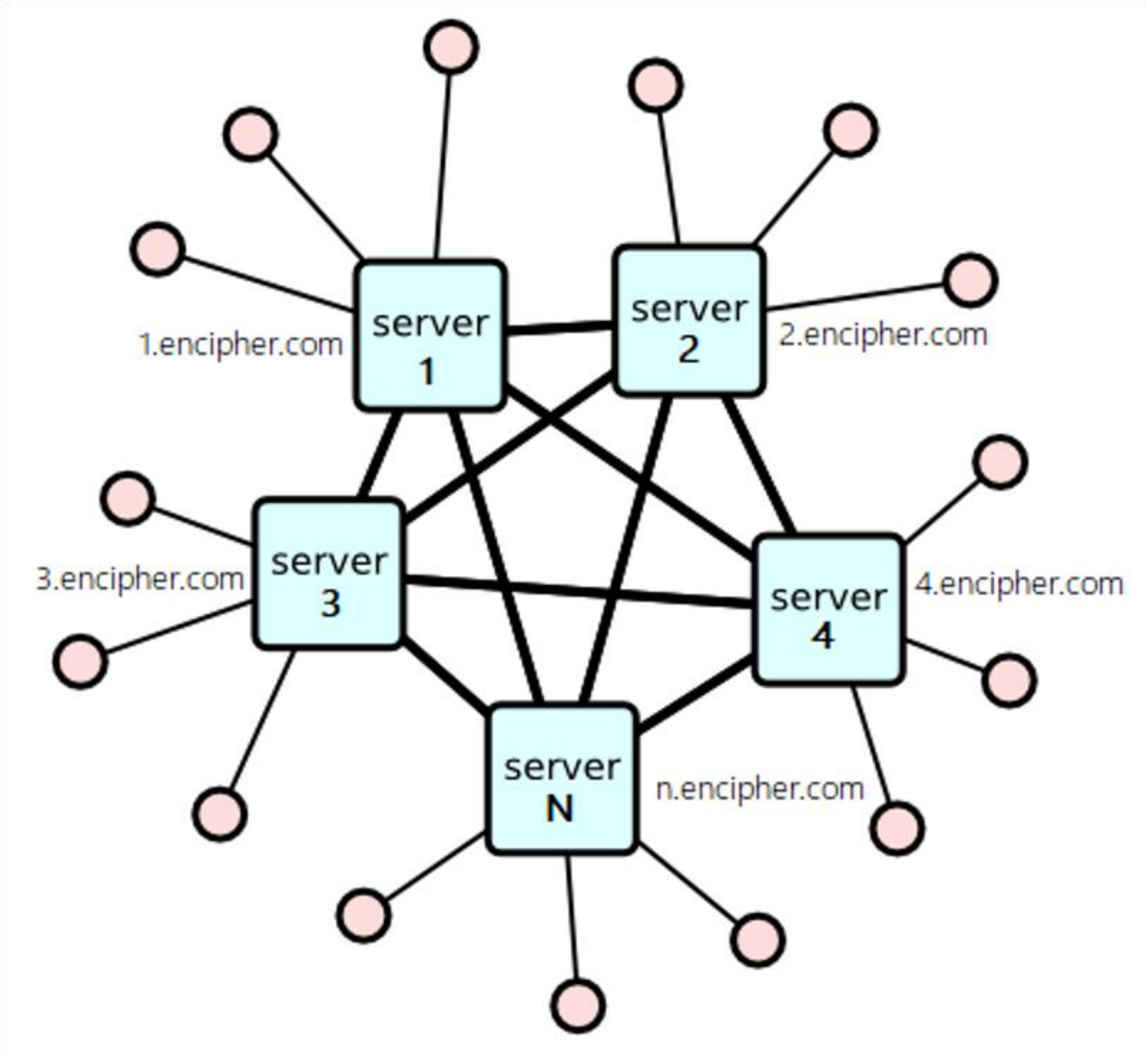
Optimum use of server resources is at your control.

Have on-premise chat software with your domain/url name.

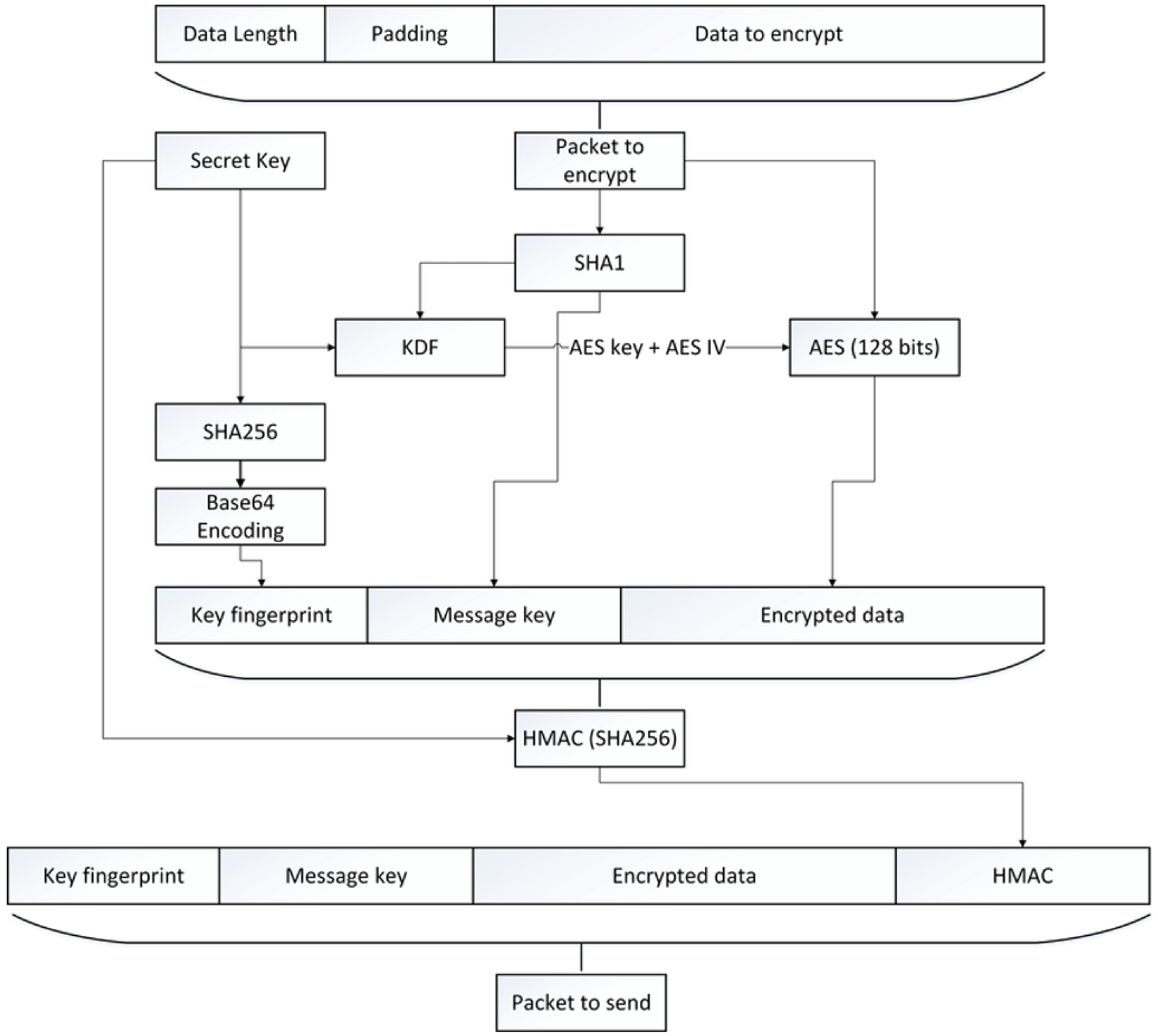
Make it available on your intranet even when your internet is down.

Syncs all the product's new features, enhancements, and service updates

System Architecture of ENCIPHER



Decentralized Server



KDF key generation process

FAQ

Q: How will the user get the secured encryption key for the first time?

A: When the user logs out from the session, a confirmation pop out will appear asking for the user’s consent to encrypt the message. If the user agrees to encrypt his messages, an encryption key will be downloaded to his device.

Q: Can a user log in from multiple devices?

A: Yes

Q: How do you ensure security with multi device login process?

A: For each new login in new additional device, the user will be required to provide the encryption key which he downloaded earlier. User can authorize new device login by currently active logged in device.

Q: How are the audio and video calls secured the system?

A: Audio & Video Calls are initiated by WEBRTC mechanism. Additionally, it has the similar secured encryption process as the text messages of the encipher platform. It also uses the TURN server to secure all the encryption keys to secure the communication.

Q: Is there any way to delete all data of a user and restrict a user from any further login?

A: Yes. This can be done by ENCIPHER admin.

Q: Can the encipher admin ready my messages?

A: No ENCIPHER admin won’t be able to read user’s message since it will require them to have the public key to decrypt the message.

Q: Can the admin of ENCIPHER adopt an option to read user’s encrypted message?

A: Yes. (But not recommended)