
*Ability to choose your own app name

**System for secure communication and transmission of confidential information,** designed specifically for businesses, corporate clients, and professional teams.

**“If you’re not paying for the product — then you are the product.”**

CEO of TechnoDreams — Serhii Cherskoi

# WeWe3 Enterprise: Corporate Secure Communication System

**WeWe3 Enterprise** is a comprehensive communication ecosystem designed for businesses, teams, organizations, and their families. It was created to ensure secure information exchange, access management, and confidentiality control.

👥 Who is it for:

**WeWe3 Enterprise** is designed for businesses, corporate teams, government institutions, law firms, medical organizations, political parties, and anyone working with confidential or critically important information.

## 🔐 Key Advantages:

**End-to-end encryption (NATO-level):** No vulnerable “modern protocols” or exposure to other types of attacks. Guarantees that only the sender and recipient can read the message.

**Isolated environment:** Operates independently of email, SMS, contacts, GPS, and App Store/ Google Play.

**Instant data deletion:** Can be triggered by a code, the account owner's command, or trusted delegates.

**Leak protection:** Access cannot be compromised, even if the password is stolen.

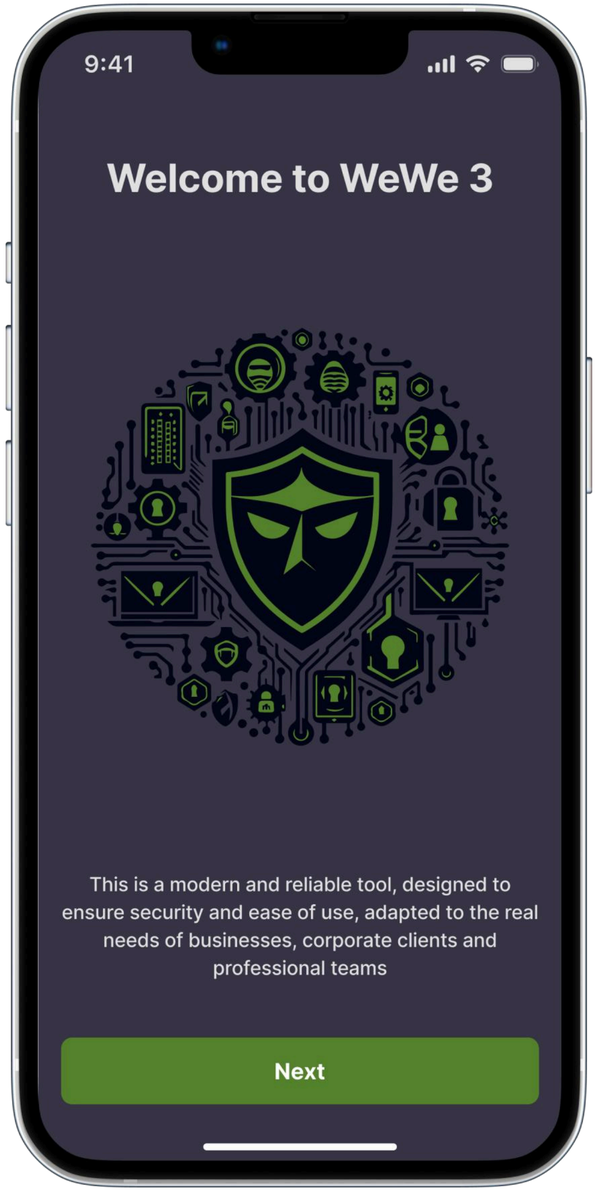
**No third-party access:** No external party, including server administrators, can access any data.

**Encrypted storage:** All data on both the device and server is always stored in encrypted form, preventing interception even on smartphones or PCs.

**Flexible architecture:** Centralized management of clients, servers, and access rights.

**All-in-one solution:** Enables unrestricted data transfer, replacing both email and FTP.

**Client-owned infrastructure: Server infrastructure is fully owned by the client, ensuring complete control over the system and eliminating any access by potential threats.**




The system enables the exchange of open and service information

The system allows clients to exchange instant text messages between two clients or within groups (chats), as well as voice and video information between two clients online

The system guarantees communication exclusively between two subscribers, eliminating all existing methods of parallel online or offline interception (chats, video, audio, files)

The system supports the rapid transfer of data of any size, with or without compression

The system offers a guaranteed selection of operational modes, with or without geolocation, and prevents connection via other systems to determine the exact location of a subscriber or group

# Data Destruction – Unique Features of WeWe3 Without Global Analogues

The system enables the immediate destruction of transmitted information using a password or code from the user’s device

The system allows for the immediate destruction of transmitted information via a command from the control center or a superuser device. This capability is available for both groups of subscribers and individual users

The system ensures the guaranteed deletion of part or all communication data with other chat users from a personal device

The system provides the capability to erase all traces of its activity after the application is removed

The system supports the configuration of automatic message deletion in chats after they have been read

# WeWe3 employs modes and methods designed to prevent information leakage, even if a user's login and password are compromised

The system includes anti-phishing capabilities for transferring user registration data. This ensures secure system access and prevents unauthorized retrieval of transmitted or stored information, eliminating common issues related to information leakage through fraudulent methods of password acquisition

The system features an isolated contact book, separate from the operating system, which prevents unauthorized access to data such as call signs, job titles, ranks, personal phone numbers, family phone numbers, and other information about colleagues. This ensures that external programs or hacking methods, including those from other installed apps, cannot retrieve this data

The system does not support code execution (e.g., bots or scripts), preventing the creation of viral code that could be used to attack the system or compromise personal data

The system protects against the creation of additional devices that could access past information or impersonate the user’s identity during communication. This prevents potentially catastrophic consequences caused by unauthorized access

## WeWe3 employs modes and methods that ensure the protection of information on devices

The system prevents code execution (e.g., bots or scripts) to eliminate the risk of creating viral code aimed at attacking the system or compromising personal data

It is protected against the creation of additional devices that could access past information or impersonate the user's identity during communication, which could lead to catastrophic consequences

The system does not allow registration via email, SMS, identity providers, or other methods used by other messengers, which could enable unauthorized parallel access to data either online or offline

It employs a unique user registration system via code or server administrator approval, preventing unauthorized individuals from joining the system for communication or system analysis

The system does not support remote collection of information using device capabilities (e.g., microphone, camera, or geolocation features that are available in proprietary or third-party software from other communication systems)

The system is capable of rapid improvements and updates to enhance security both in individual components and as a whole

**Personal devices and information transmitted through the WeWe system use a highly secure channel and applications**

All group chats created in the system guarantee the absence of public usage (no viewing or access by non-group members)

The system supports group notifications targeting specific individuals or all users within the user base

**The system is continuously improved and updated to enable rapid changes for enhancing security across individual components and the system as a whole**

The system notifies users of new messages without revealing the content until the application is opened. This ensures that even nearby individuals or those using specialized photo or video capture devices cannot read the content of the new notification

The system can hide photo and video data in chats during scrolling, making it significantly harder to visually interpret the content of the chat and the transmitted information

# THE SYSTEM SUPPORTS THE USE OF PERSONAL COMPUTERS AS CLIENTS ON WINDOWS AND MACOS PLATFORMS

The system enables the use of **PROPRIETARY** cellular devices with operating systems such as iOS and Android

The system can operate on **CORPORATE** devices where only the WeWe3 Enterprise communication system is accessible

WeWe3 Enterprise can operate via installation **WITHOUT USING** загальних магазинів general app stores (Apple Store, Google Play, and others)

| | |
|---|---|
| **The server component of WeWe3 Enterprise has no analogues worldwide, developed by a proficient team, and is fully adaptable to accommodate rapid changes based on specific needs** | The WeWe3 Enterprise server ensures information security entirely under the control of its owner<br><br>WeWe3 Enterprise provides the capability to control the distribution of installed system copies<br><br>The system supports centralized and hierarchical management, including features such as enabling/disabling clients or servers within the system and remotely deleting information on client devices |
| **For secure data exchange, WeWe3 Enterprise utilizes the most reliable transmission methods, proven over time** | The system implements End-to-End Encryption, ensuring that only the sender and the recipient can read the messages<br><br>Encryption employs cryptographic algorithms that comply with the most secure NATO military standards. The reliability of WeWe3 encryption methods is affirmed by their use in armies worldwide, as opposed to newer, untested encryption techniques |

Leading armies and special units globally use WeWe technologies in specialized and military operations, underscoring their reliability and simplicity of use

The server component ensures protection against the dissemination of information from hardware or cloud server components to unauthorized third parties

Physical access, compromise, or hacking of the server does not result in successful retrieval of data stored or transmitted via the system's servers

The system implements dedicated roles for system administrators, who can add/remove users from the system, configure server interactions within the system, and more

**The server system is designed so that no third party, including server administrators, can interfere with, access, modify, or intercept the data being transmitted or stored during communication. This guarantees absolute confidentiality and data protection for users**

All data transmitted through or stored on the server is for transport purposes only and remains encrypted, with no possibility of decryption

Servers do not store keys, passwords, or any data that could decrypt the information exchanged between users

Once information is received by the recipient, it is deleted from the server

The system enables the complete deletion of all information from the server and user devices by authorized personnel

The system includes an API to facilitate integration with existing or future systems

**DATA SECURITY ON THE CLIENT SIDE IS THE RESULT OF 20 YEARS OF PRACTICAL EXPERIENCE IN COUNTERING ALL METHODS OF MALICIOUS ATTEMPTS TO STEAL, MODIFY, OR INTERCEPT DATA. IT IS BASED ON MULTI-LAYERED PROTECTION AND CONTINUOUS MONITORING OF POTENTIAL THREATS**

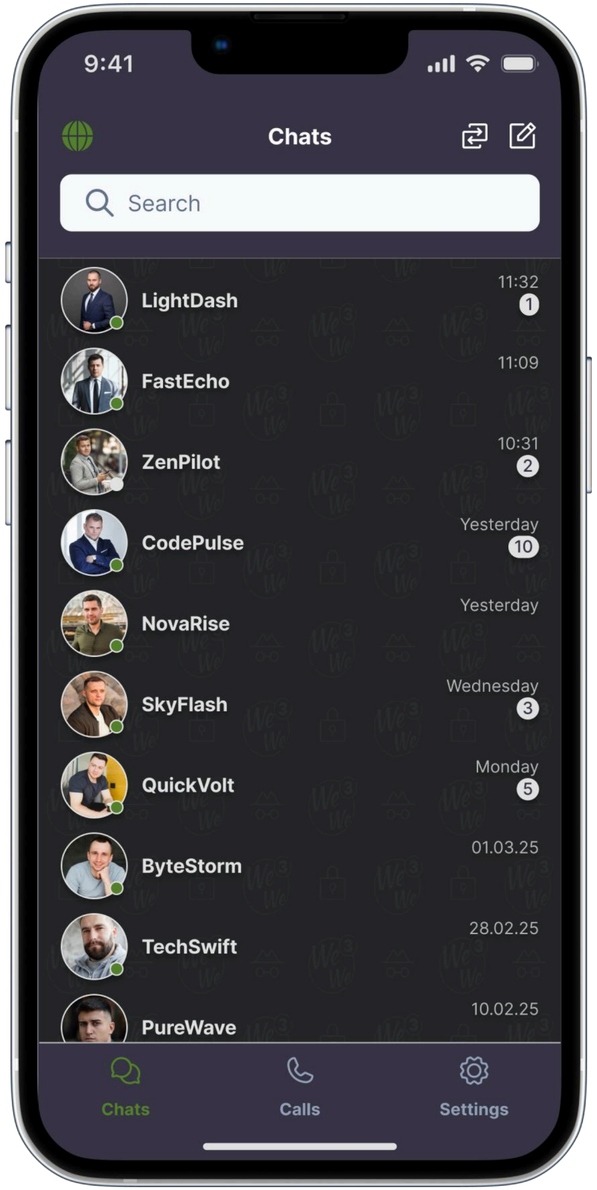
Information on the client side within the application is stored in encrypted form.

The system uses an encrypted container on the device, where all transmitted and received data is stored. This prevents its dissemination through the general system of the device or in case the device falls into the hands of an adversary

The system does not allow the storage of any data or backups on remote servers. This method is currently one of the most common and straightforward ways to gain unauthorized access to information, and it is nearly impossible to track

The system enables remote deletion of information within the application from the user’s device

The system includes protection against unauthorized actions with data during its storage and exchange




**A simplified user system has been designed to meet the needs of users without experience using modern messengers. It is thoughtfully created for intuitive use, providing easy access to key functions and convenience in everyday communication**

The system features a simple and user-friendly interface

It allows input of a subscriber's numeric number, similar to a standard phone interface, making it accessible to a large number of employees without requiring knowledge of modern IT technologies

**The system is optimized to minimize the number of requests and notifications, enabling users to send and receive information quickly without unnecessary distractions**

**This approach is based on 20 years of experience with extensive use of previous versions, which has enabled functional improvements to make the system as convenient and efficient as possible for users**

The WeWe3 Enterprise version is a reliable tool that meets the requirements of security and convenience while adapting to the real needs of businesses. The system is the result of practical resistance to aggressors worldwide

We are proud to work with such needs.
Development team:

technodreams.biz

weltwelle.com