

# EEZY KEYZ® Conferencing Solution

IPRA Technologies, Finland



## Contents

1.	What we offer .....	3
2.	Why EEZY KEYZ® .....	4
3.	Design principle.....	5
3.1	Chat and VoIP audio and video calls .....	6
4.	Architecture .....	8
4.1.	Parts of the system .....	8
4.2	Admin functions .....	8
4.3.	Communication protocols .....	8
5.	EEZY KEYZ® Encryption .....	9
5.1	Registration to the service and the messaging process .....	11
Registration by email	.....	11
Registration by handle (without validation)	.....	11
User login	.....	11
Connections to other users	.....	12
Signaling server	.....	12
Messaging	.....	12
VoIP	.....	12
5.2	Encryption customizing options.....	13
6.	EEZY KEYZ® Background system .....	14
7.	EEZY KEYZ® Chat app .....	15
7.1	EEZY KEYZ® Chat app features .....	16
7.2	EEZY KEYZ® Chat app system requirements .....	16
7.3	EEZY KEYZ® compared with other solutions.....	16
8.	Implementation .....	17
9.	Contact .....	18

# 1. What we offer

Cybersecurity, operating safely online is one of the challenges that modern digitally-operating businesses, organizations and individuals face in today's inter-connected world. The Covid-19 pandemic has made everyone even more reliant on e-services provided by governments and health care officials. In a crisis situation, getting communications channels up and running quickly is often the first priority, and security considerations may be (needlessly, in our view) over-looked. As TRAFICOM's *Cyber Weather May 2020*<sup>1</sup> states "several high-performance computing environments have been targeted by data breaches" world-wide.

There are many service providers on the market and it may be difficult to choose the best option from the varied offering. EEZY KEYZ® Conferencing Solution is a complete option for you, when security cannot be compromised. EEZY KEYZ® combines chat, VoIP audio and video calls and up to unlimited file transfer all in one solution that guarantees secure communication on different platforms and devices, even over unsecure networks. Furthermore, we offer the option for technology transfer. An organization can have self-hosted key and chat servers, and have the email and chat app customized.

Our number one focus point is combining security with usability, it is what we know, and we do not want anyone to go without. EEZY KEYZ® makes sure your messages cannot be intercepted or hacked while in transit or when stored. Also, spear phishing attacks will be eliminated.

EEZY KEYZ® Conferencing Solution represents the future of secure communications and is currently available for iOS mobile devices and on Chrome, Edge and Firefox browsers. In the near future, EEZY KEYZ® will be available also for Android and as a desktop solution.

This article provides you with a full description of our EEZY KEYZ® solution and at the end you will find our contact details for more information on how EEZY KEYZ® can be customized for your organization.

---

<sup>1</sup> National Cyber Security Centre of Finland (<https://www.kyberturvallisuuskeskus.fi/en/news/may-bathed-spring-sunshine-cyber-weather-saw-rainy-skies>)

## 2. Why EEZY KEYZ®

This is what we promise:

1. Our end-to-end encrypted, peer-to-peer (P2P) architecture achieves an unparalleled level of privacy and security, as no communication goes through servers or other pre-determined network locations without encryption.
2. There is no risk of a data breach and your communications will be compliant with data security laws and regulations.
3. EEZY KEYZ® has been developed as a military-grade encryption solution but at the same time it is as user-friendly as a normal communications solution. It is easy to adopt, operate and use on the existing hardware of your organization.
4. EEZY KEYZ® relies on widely peer-reviewed and time-tested open source software standards and best-practice cryptographic algorithms and methods – and gives you unprecedented privacy exceeding any cloud-based service.
5. You stay in full control of your data, including chat messages, attachments and the encryption keys. This also helps you avoid possible political risks relating to encryption products; in some countries, vendors can be forced to turn over encryption keys to the authorities. With EEZY KEYZ® this is not possible as only the customer has access to the keys.

All of this benefits your organization and the whole framework you operate in. You can adopt new, safe communications practices with little effort.

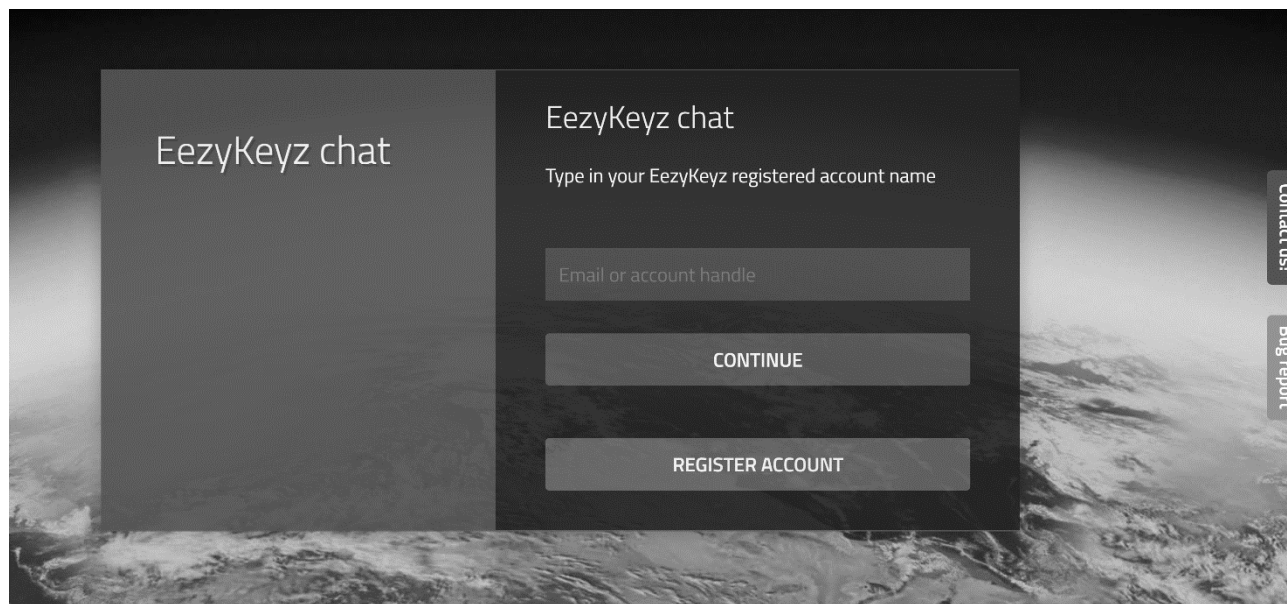


Figure 1 EEZY KEYZ® on a desktop

### 3. Design principle

EEZY KEYZ® Conferencing Solution has been designed security-first and so that it can be customized according to your organization's requirements. Chat messages, attachments and calls are truly end-to-end encrypted with a unique method developed by IPRA Technologies that combines symmetrical and asymmetrical encryption keys.

The solution provides high audio/video quality, resilience over networks with inconsistent quality, and what is more, ultimate privacy.

According to the EEZY KEYZ® concept, users do not need to know encryption methods; the chat app is designed for a seamless user experience.

### 3.1 Chat and VoIP audio and video calls

The image below shows you step-by-step how the EEZY KEYZ® messaging process flows on the chat app.

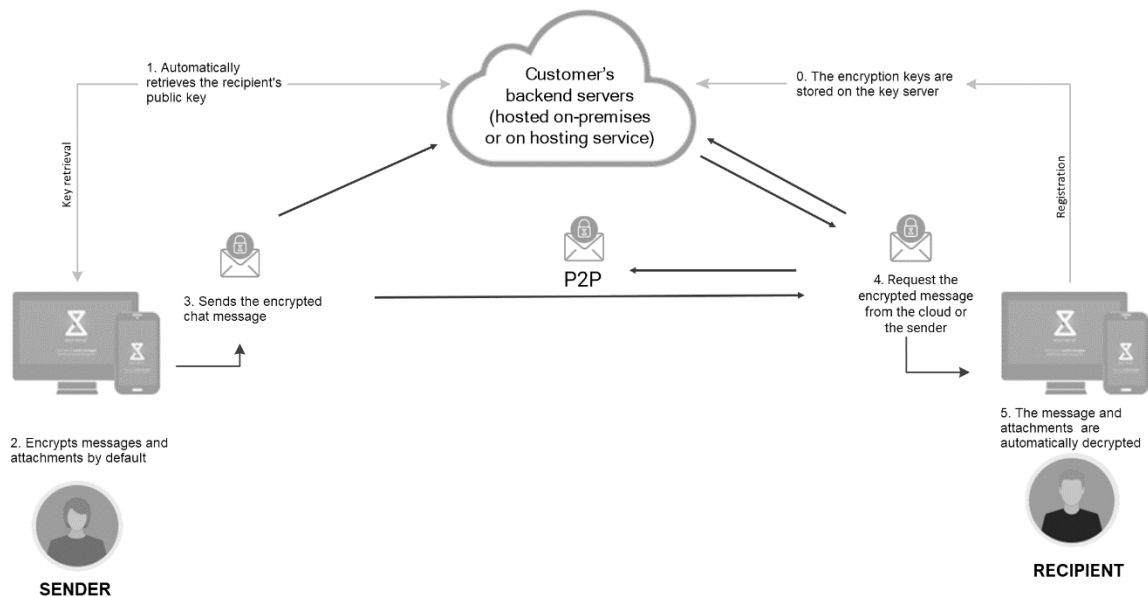
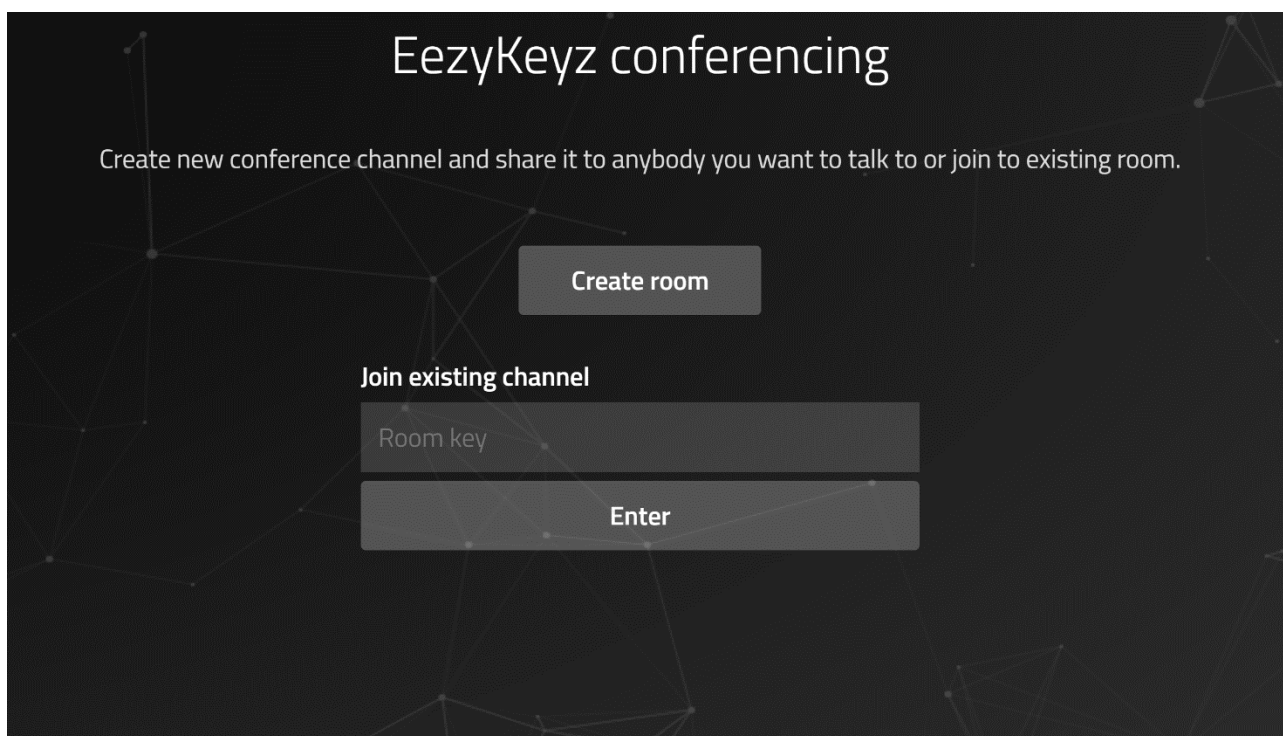


Figure 2 EEZY KEYZ® Conferencing Solution

0. When users register to the system, their private key is stored encrypted on the key server. The public key is stored to the server as it is.
1. When the sender inserts a message on the chat, the EEZY KEYZ® chat app automatically retrieves the recipient's public key from the key server.
2. The sender composes the chat message. The chat app automatically encrypts all messages and attachments and digitally signs the messages by default.
3. There are no extra steps when sending the message. The encrypted chat message passes through the company chat servers or P2P.
4. The recipient requests the encrypted message from the cloud or the sender.
5. The message is decrypted when it is received, and stored unencrypted to a database that is encrypted. Logout offers the option to remove all locally stored data.

On the app, it is easy to create conferencing rooms, with a room key if needed.



*Figure 3 Safe conferencing*

## 4. Architecture

EEZY KEYZ® Conferencing Solution has been designed security-first, allowing a flexible implementation of the system. Conferencing Solution, as well as the Email Encryption Solution, can be used as stand-alone options, they can be integrated as one communications solution, or integrated as the communications solution of a larger system.

### 4.1. Parts of the system

EEZY KEYZ® Conferencing Solution has three main parts: the backend, API and the chat apps.

The backend functions as the encryption key exchange and storage system. The web API of the backend and the chat app handle the encryption, key exchange process and digital signing of messages automatically. Metadata (e.g. names of the attachments) is also encrypted.

The backend system, chat apps and used algorithms can be built and customized to fit the needs of your organization. The result is a state-of-the-art encryption system that specifically serves your organization and delivers confidential messages in all formats (images, videos, documents, etc.) with proof-of-origin and proof-of-integrity.

### 4.2 Admin functions

A member of your personnel can act as the Admin of the system and handle user registration, enable and disable user accounts and manage the key life cycle.

### 4.3. Communication protocols

EEZY KEYZ® Conferencing Solution uses open source Web Real Time Communication (WebRTC) peer-to-peer architecture, which makes EEZY KEYZ® the most secure private one on the market. The communication between the server and chat apps is secured through Transport Layer Security (TLS).

The initial communication between the chat apps is done using WebSocket wss protocol that secures the connection through TLS. The required details for further communication are exchanged through this WebSocket. Then, DTLS-SRTP (Datagram Transport Layer Security, DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP) is formed to secure the connection where the messages are delivered encrypted.



## 5. EEZY KEYZ<sup>®</sup> Encryption

In the EEZY KEYZ<sup>®</sup> encryption method messages and files are symmetrically end-to-end encrypted, using:

- AES-GCM (Galois/Counter Mode), which also provides data authenticity/integrity and confidentiality, and
- a randomly generated IV.

For 1-on-1 channels, private messages are encrypted with a shared secret generated between the sender's private key and the recipient's public key.

For group channels, messages are encrypted with what we call universal keys (public/private keys that are shared between multiple parties).

The default algorithms and curve are:

- AES-GCM 256-bit to encrypt messages and files
- ECDH for shared secret generation between users on private and group channels
- SHA-256 for hashing the shared secret, prefixed with a random IV and suffixed with data related to the use of said shared secret
- Default EC curve: secp256r1 offering 128 bits of security

The image below shows you how the encrypted messages are sent:

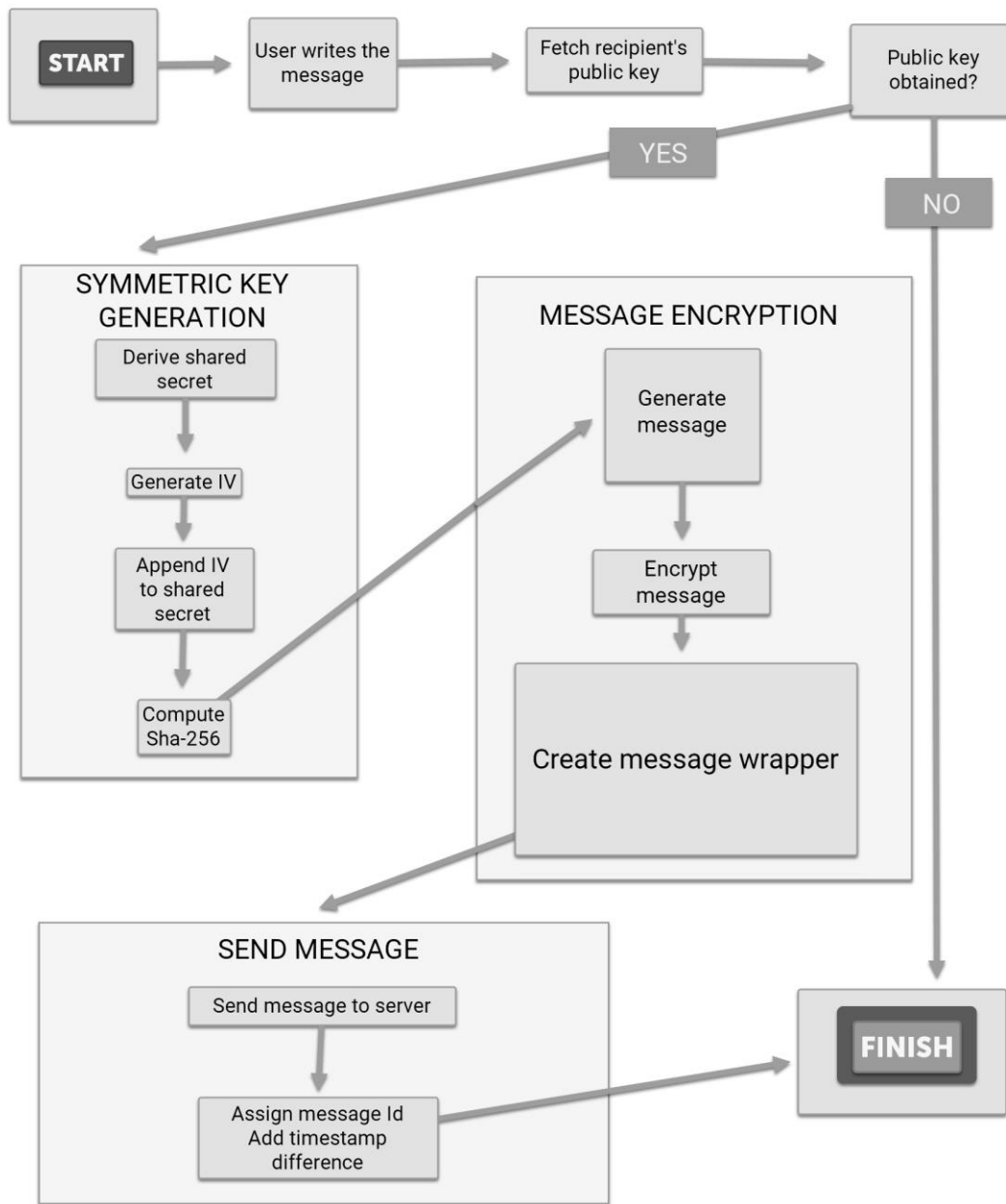


Figure 4 Encryption

## 5.1 Registration to the service and the messaging process

### Registration by email

You must first register into the EEZY KEYZ® Email Encryption Solution, and after that, the registration into the EEZY KEYZ® Conferencing Solution is possible.

1. Enter your email address.
2. Enter your proof-of-knowledge.
3. When access is granted, the system creates a new public/private key pair to be used only in chat.
4. Request a new password (cannot be the same as the email decryption password) and use the password to encrypt the private key, and generate the proof-of-knowledge.
5. Store the public key, encrypted private key and the proof-of-knowledge to the EEZY KEYZ key server.
6. Log into the chat server.

### Registration by handle (without validation)

You can create an unvalidated handle (an unvalidated user name that does not contain the character @) to log into the EEZY KEYZ® Conferencing Solution.

1. Enter your handle name.
2. Check from the server that the handle name is not already in use.
3. When access is granted, the system creates a new public/private key pair to be used only in chat.
4. Request a new password and use the password to encrypt the private key, and generate the proof-of-knowledge.
5. Store the public key, encrypted private key and the proof-of-knowledge to the EEZY KEYZ key server.
6. Log into the chat server

### User login

1. Enter your handle or email address that has been registered to the conferencing solution.
2. Enter your password to generate the proof-of-knowledge that is used to validate the access.
3. Log into the chat server.
4. Decrypt the private key received from the server.
5. Store the public and private keys locally.

## Connections to other users

You can search recipients in the system by their registered handle or the email address, or even parts of handles or email addresses.

- You can send a message to a recipient even without prior connection
- You can block other users from sending private messages

There are three types of connections:

- **Contact** – you have searched a recipient and made connection by sending them a message
- **Channel group** – you know a recipient only through a group where you have a mutual contact
- **Community group** – a company-assigned group, for example

## Signaling server

A signaling server handles messaging between connected chat apps and pushes messages from the server.

A user online status can be queried from the signaling server, and when connected, user status changes are pushed to the chat app for user connections

## Messaging

- Messages can be fetched from the server in encrypted format
- If users have an open P2P DataChannel, messages can be requested directly from other chat apps (and not from the server)

## VoIP

- **Voice and video calls:** available with WebRTC P2P technology
- **DataChannel connection:**
  1. A user generates an SDP (Session Description Protocol) offer to request a DataChannel connection and delivers it to the requested user via the signaling server.
  2. Recipient handles the offer, generates an answer and sends it back via the signaling server.
  3. DataChannel connection is formed between the two parties.
- **Audio/Video connection:** Audio/Video channel messaging is handled via WebRTC DataChannel, including messages about an incoming call, call disconnect, etc., which requires DataChannel connection between the users
  1. A user generates an SDP offer to request an Audio/Video connection and delivers the request to the recipient via WebRTC DataChannel.
  2. Recipient handles the offer, generates an answer and sends it back via WebRTC DataChannel.
  3. Audio/Video connection is formed between the parties.

## 5.2 Encryption customizing options

EEZY KEYZ® encryption can be customized to suit your organization's needs:

- Customized ECC curve up to NATO Secret Level
- Front door mechanism to open all encrypted emails or chat messages sent using the organization's own encryption system
- Other customer-specific customizations

## 6. EEZY KEYZ® Background system

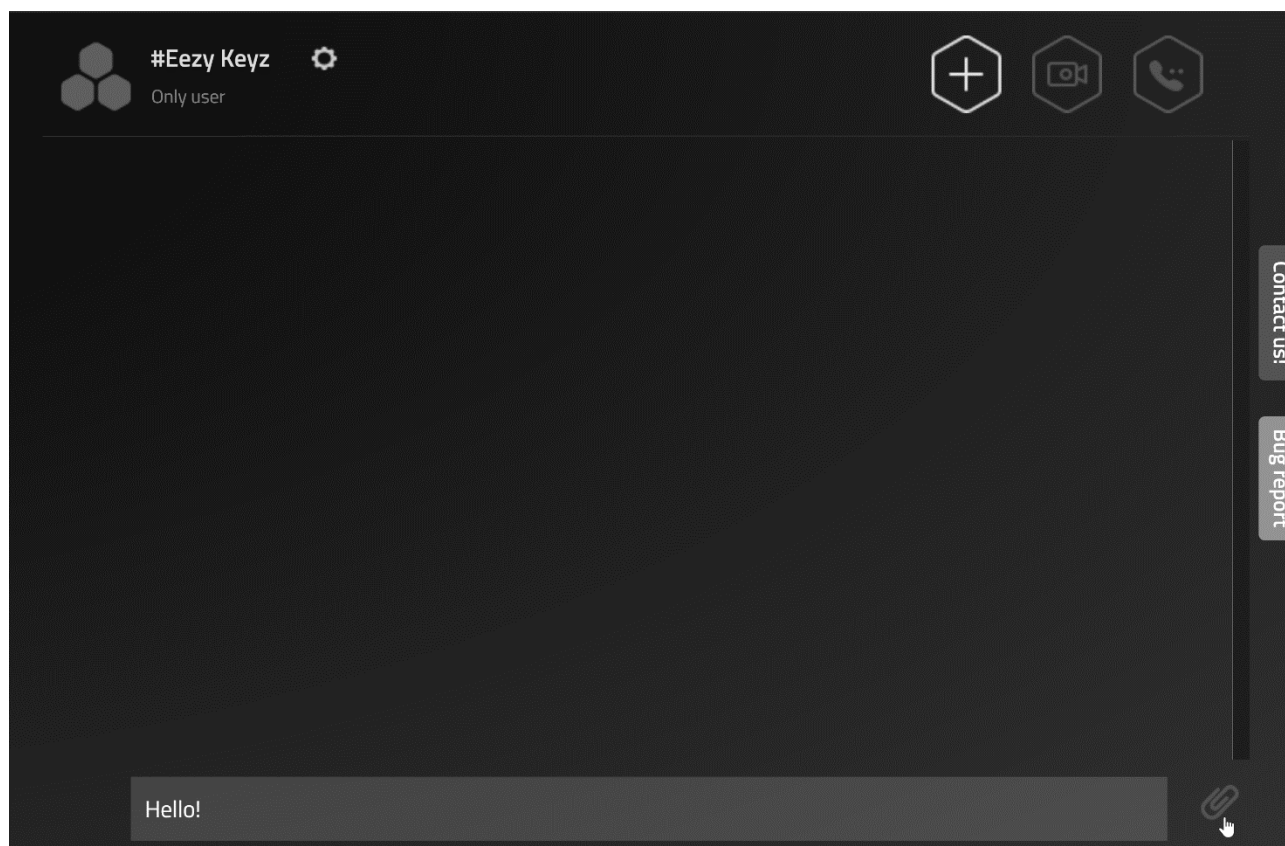
The current EEZY KEYZ® SaaS chat installation is as follows:

- EEZY KEYZ® key server with basic key server installation
- EEZY KEYZ® chat server:
  - ✓ Apache WWW server (PHP) serving resources
  - ✓ Signaling server (WebSocket nodeJS)
  - ✓ PostgreSQL storing registered accounts, encrypted messages, etc.
  - ✓ Redis for session management, data cache and pub/sub between WWW server and WebSocket server
  - ✓ ICE (Interactive Connectivity Establishment) servers
- File transfer
  - ✓ AWS (Amazon Web Services) S3 object storage

## 7. EEZY KEYZ® Chat app

EEZY KEYZ® Chat app is currently available for iOS mobile devices and on Chrome, Edge and Firefox browsers. In the near future, EEZY KEYZ® will be available also for Android and as a desktop solution.

The chat app has all the usual features of a normal chat solution. However, EEZY KEYZ® chat app uses strong encryption to protect messages, attachments and VoIP calls. And yet, the user user-experience is completely seamless.



*Figure 5 Creating a group, starting a chat and adding attachments is secure and easy*

When the sender/caller is composing chat messages or calling, the chat app automatically checks the recipient's credentials from the backend. At the recipient's end, if they are using EEZY KEYZ®, messages and attachments are stored unencrypted in a database that is encrypted. All information stored by EEZY KEYZ® locally on the device can be deleted when logging out of the system.

The private keys used on Android are stored on the device in a database that is encrypted with Android KeyStore.

The encrypted private keys used on iOS are stored on the iOS Keychain.

EEZY KEYZ® makes sure your messages cannot be intercepted or hacked while in transit or when stored. Also, spear phishing attacks will be eliminated.

## 7.1 EEZY KEYZ® Chat app features

- Easy-to-use EEZY KEYZ® user interface
- In English, localizations possible later
- Private chat and audio/video call
- Unlimited group chat
- Private max 8-participant group audio/video call in HD quality
- Screen sharing
- Unlimited file transfer
- Full forward secrecy
- Chat and calls can be joined by a link

## 7.2 EEZY KEYZ® Chat app system requirements

- Android 6.0 (API level 23), and newer operating systems
- Apple iPhone and iPad running the iOS 10.0, and newer operating systems
- Supported on Chrome, Edge and Firefox browsers

## 7.3 EEZY KEYZ® compared with other solutions

Please see a full description of features and how EEZY KEYZ® compares with other solutions on the market in a separate comparison table that we have compiled for your benefit, delivered with this white paper.



## 8. Implementation

EEZY KEYZ<sup>®</sup> supports the full process from the initial needs' assessment to after sales services, as agreed with the customer. Each implementation process is unique and carefully planned together with your organization.

Please contact us for more information.

## 9. Contact



IPRA Technologies Ltd Oy  
Assi Group Vapaudenaukio  
Valtakatu 51, 53100  
Lappeenranta, Finland  
[sales@eezykeyz.eu](mailto:sales@eezykeyz.eu)

Lauri Valjakka  
CEO, Co-Founder  
Phone: +358 50 467 0090  
Email: [lauri.valjakka@eezykeyz.fi](mailto:lauri.valjakka@eezykeyz.fi)

Misa Munde  
Software Development  
Phone: +358 50 3465 336  
Email: [misa.munde@eezykeyz.fi](mailto:misa.munde@eezykeyz.fi)