IPRA
TECHNOLOGIES LTD

EEZY KEYZ® Email Encryption Solution

IPRA Technologies, Finland

Contents

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*[1] 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® Email Encryption Solution is a complete option for you, when security cannot be compromised. 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. The customizable EEZY KEYZ® solution makes end-to-end encrypted and authenticated email communications easy.

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 emails cannot be intercepted or hacked while in transit or when stored. Also, spear phishing attacks will be eliminated.

EEZY KEYZ® Email Encryption Solution represents the future of secure communications and is available for Android and iOS mobile devices. In the near future there will also be an Outlook add-on for Windows and a desktop version for Mac.

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.

[1] 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 true end-to-end encryption 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 email 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 exceling any cloud-based service.
5. You stay in full control of your data, including email 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® for your phone

3. Design principle

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

The EEZY KEYZ® email app automatically encrypts and digitally signs emails. Sensitive metadata, such as the title of the email and names of attachments are also encrypted.

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

3.1 Email

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

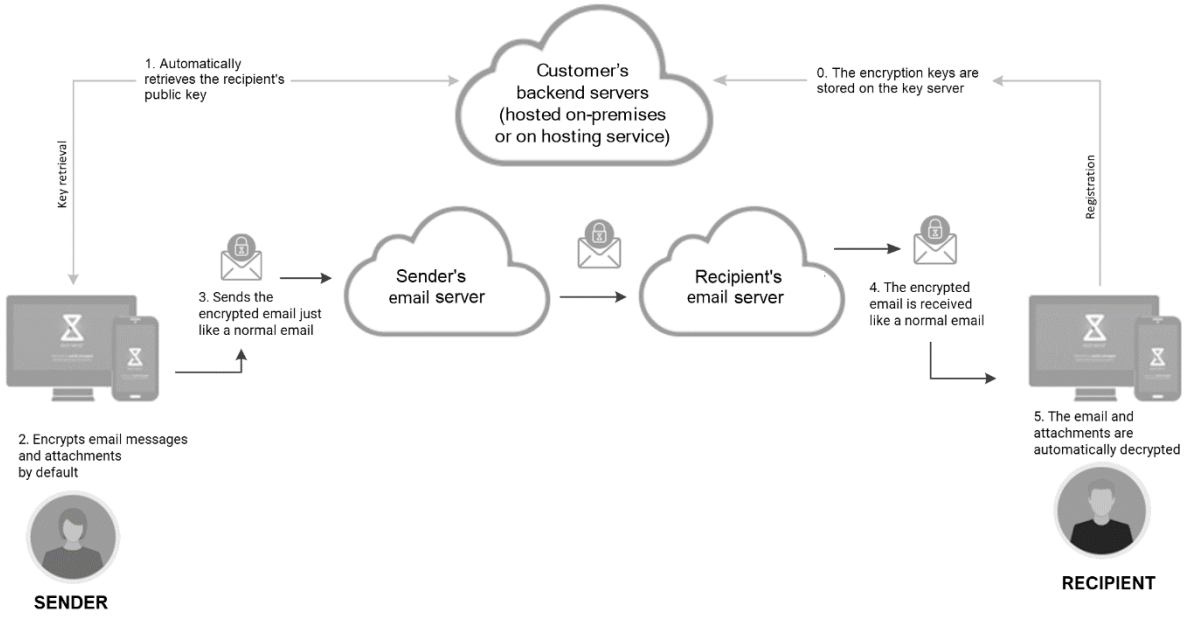

Figure 2 EEZY KEYZ® Email Encryption Solution

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 the recipient(s), the EEZY KEYZ® email app automatically retrieves the recipient's public key from the key server.
2. The sender composes the email message. The email app automatically encrypts the message and attachments and digitally signs the message by default.
3. There are no extra steps when sending the email. The encrypted email passes through the company email servers like any other message.
4. The recipient receives the encrypted email to their inbox like any other email.
5. The email is decrypted on the device when it is received, and stored unencrypted to a database that is encrypted. The email stays encrypted on the email server.

4. Architecture

EEZY KEYZ® Email Encryption Solution has been designed security-first, allowing a flexible implementation of the system. Email Encryption Solution, as well as the Conferencing 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. EEZY KEYZ® is compatible with all the leading email services. There is no need to change email addresses or the email service provider.

4.1. Parts of the system

EEZY KEYZ® Email Encryption has three main parts: the backend, API and the email apps.

The backend functions as the encryption key exchange and storage system. The web API of the backend and the email app handle the encryption, key exchange process and digital signing of messages automatically.

The email app creates the asymmetric encryption keys that are stored in the database of the backend system. The email app encrypts the email messages with symmetric-key encryption, while the asymmetric-key encryption is used to encrypt the used symmetric-key encryption key. Metadata (e.g. the title of the email and names of the attachments) is also encrypted. Emails are delivered to the recipient via the organization's email servers.

The backend system, email 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.

5. EEZY KEYZ® Encryption

EEZY KEYZ® encryption method is based on

- public-key cryptography using Elliptic-Curve Cryptography (ECC), and
- symmetric-key encryption using Advanced Encryption Standard (AES) algorithm.

Email messages are handled as follows:

- end-to-end encrypted using Elliptic-curve Diffie-Hellman (ECDH), and
- AES-GCM (Galois/Counter Mode), which also provides data authenticity/integrity and confidentiality, and
- Elliptic Curve Digital Signature Algorithm (ECDSA) is used to verify the sender by digitally signing the hash of the sender's public key.

The default algorithms and curve are:

- AES-GCM 256-bit to encrypt messages and attachments
- ECDH for shared secret generation between users
- ECDSA signature to validate sender authenticity
- Default EC curve: secp256r1 offering 128 bits of security
- Signature algorithm: ECDSA-SHA2-512
- Hash algorithm: SHA2-512

The email message encryption process is illustrated below.

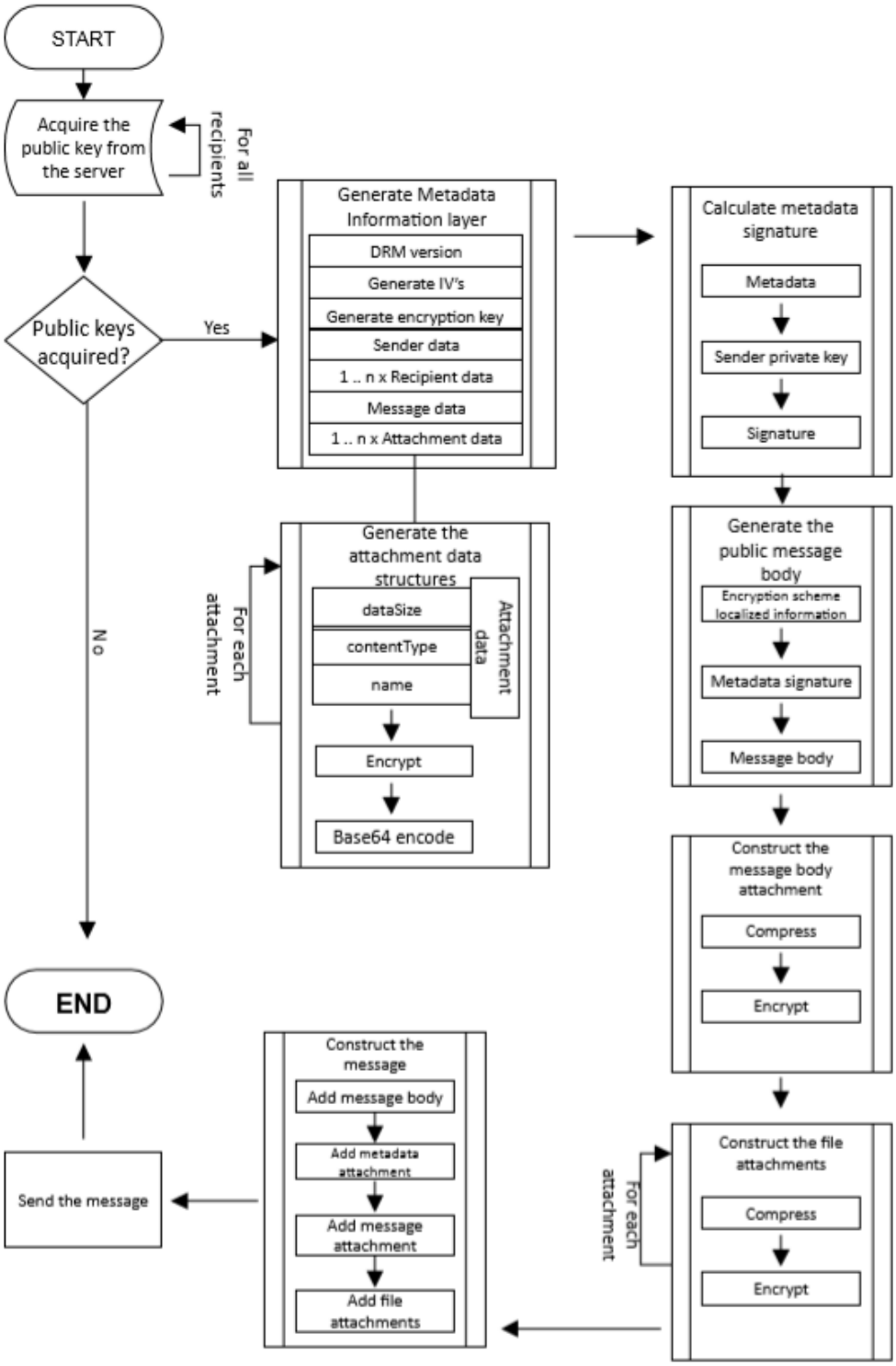

Figure 3 EEZY KEYZ® email encryption process

5.1. 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® Backend

6.1 Backend functions

The EEZY KEYZ® encryption method combines symmetrical and asymmetrical encryption keys.

The extensive EEZY KEYZ® backend system handles the encryption keys and has the following functions:

- Key exchange
- Storage for users' private keys encrypted by the EEZY KEYZ® email app
- Web API to retrieve the keys from the backend database
- Contact lookup for the email app to retrieve recipients' public keys

This structure allows users to move their private key between devices easily. The EEZY KEYZ® email apps communicate automatically with the backend system through the web API.

The private asymmetric encryption keys are stored encrypted with symmetric key encryption. They are only available to the appropriate users who know the password used to decrypt the private asymmetric encryption key. The public asymmetric encryption keys are available to all users of the system.

6.2 Connections to the backend

For the self-hosted option, the connections to the backend servers should be restricted only to a few IP addresses by default for the Admins to connect to the system. Only the API should be available to the EEZY KEYZ® email apps. All connections between email apps and the backend web API are made using HTTPS/TLS (Hypertext Transfer Protocol Secure/Transport Layer Security) connections.

6.3 Backend services

The backend is divided into micro services that run in Docker containers. For the self-hosted option, the initial containers and later on updates are delivered through the Docker registry, from where the containers can be pulled. Containers can also be delivered as TAR files. The maintenance of the backend system is minimal; only renewing the certificate and installing updates.

The backend system consists of the following services:

EEZY KEYZ® API

- Verifying user accounts
- Storing users' public keys
- Storing users' encrypted private keys > from which the unique password is derived
- Delivering users' private encryption keys > the private key is delivered only if the user provides the password

Admin API (for your organization's Admin)

- Enabling and disabling user accounts
- Deactivating encryption keys
- Deleting or removing encryption keys > encrypted messages cannot be opened again
- Managing the length and active period of keys

EEZY KEYZ® Email

- Delivering account verification emails to users

Logstash and Filebeat

- Remote logging of the system information
  - ✓ Changes in the encryption key states and timestamps of each private key fetch
  - ✓ Server and Docker module errors

Maria Database

- Storing user accounts and the associated encryption keys

Nginx

- Providing the communication interface between the chat apps and the web API

Example EEZY KEYZ® backend

The backend runs distributed to multiple servers with a load balancer managing traffic to servers.

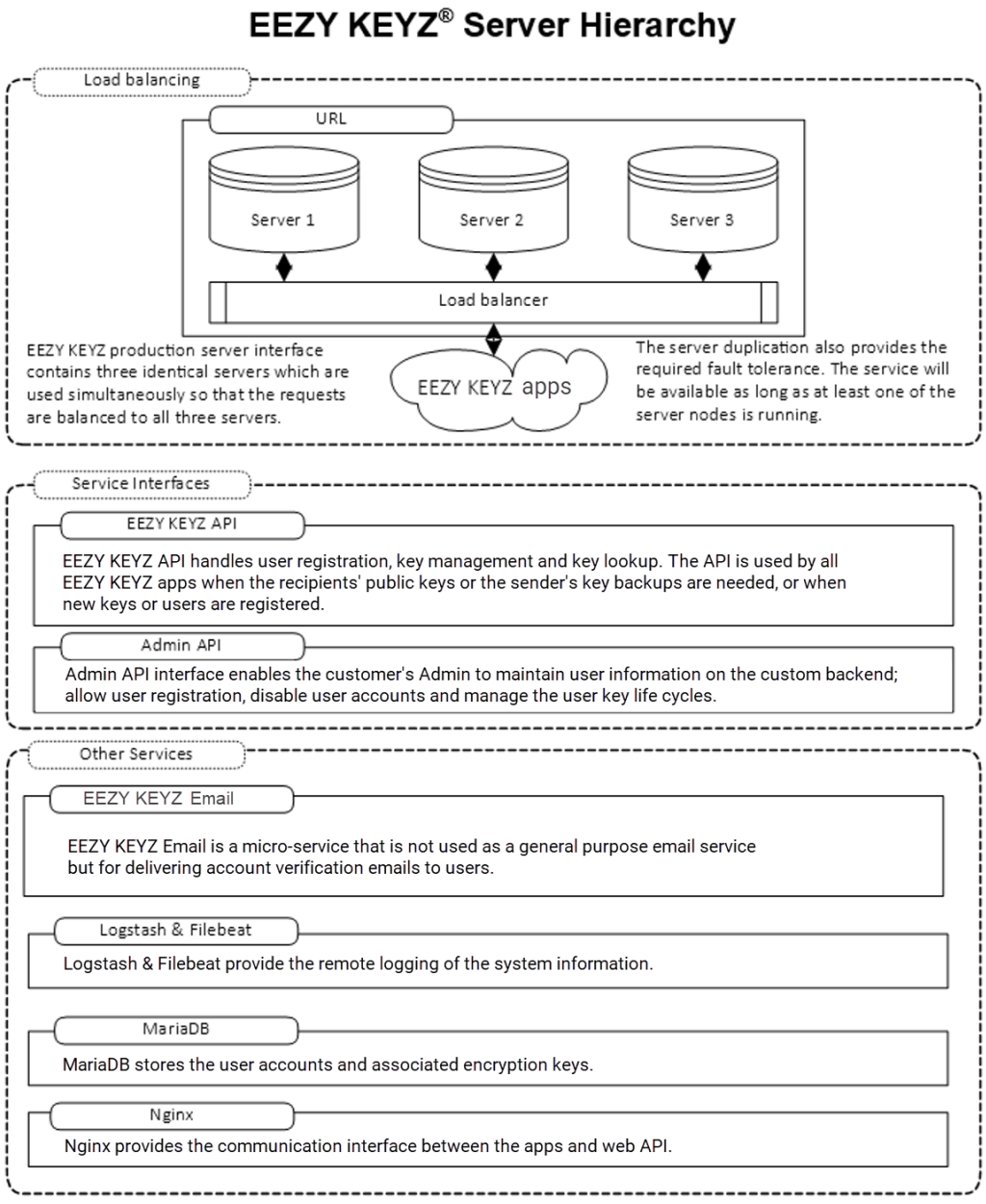

Figure 4 EEZY KEYZ® backend

6.4 Backend customizing options

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

- User authentication when registering to the system. For example,
  - ✓ OAuth2
  - ✓ Token-based system.
- Certifications used in the system are from Let's Encrypt by default.
- Logging of the system information can be adjusted according to your requirements.
- Admin login portal can be modified according to your requirements. For example,
  - ✓ Certificate-based login system
  - ✓ Username + password + authenticator code system
  - ✓ Your existing authentication system.
- Rate-limited API calls
- Locking the user account after too many incorrect password inputs
- Alternative backend system delivery format to Docker containers
- Other possible customer-specific customizations in the Admin features

7. EEZY KEYZ® Email app

EEZY KEYZ® Email app is available for Android and iOS mobile devices. In the near future there will also be an Outlook add-on for Windows and a desktop version for Mac.

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

When the sender is composing the email, the 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 on the device. On email server the emails are stored encrypted.

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 emails cannot be intercepted or hacked while in transit or when stored. Also, spear phishing attacks will be eliminated.

7.1 EEZY KEYZ® Email app features

- Seamless user experience on easy-to-use EEZY KEYZ® user interface
- In English, localizations possible later
- Encryption features integrated in the app
- Automatic end-to-end encryption and digital signing of emails and attachments
- Full forward secrecy

7.2 EEZY KEYZ® Email 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
- Supports IMAP and Exchange (EWS) email protocols

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® 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

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

Misa Munde
Software Development
Phone: +358 50 3465 336
Email: misa.munde@eezykeyz.fi