Customer-Tailored EEZY KEYZ® Email Encryption System

IPRA Technologies Ltd Finland 2019

Contents

Date: July 1st 2019

IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

1. Introduction

The customer-tailored EEZY KEYZ® email encryption system makes end-to-end encrypted and authenticated email communications easy. The system consists of the backend system and EEZY KEYZ® email clients. The backend system functions as the encryption key exchange and storage system. The EEZY KEYZ® email clients automatically encrypt and digitally sign email messages and attachments sent to other users. The sensitive metadata of the email is also encrypted, such as the names of the attachments, the subject of the email, etc. The backend system and EEZY KEYZ® email clients are developed and customized for each customer. The result is a state-of-the-art customer dedicated end-to-end email encryption system which provides confidential messages with proof-of-origin and proof-of-integrity.

The customer remains in control of the whole system and all email data. Updates are provided for both the backend system and the EEZY KEYZ® email clients by IPRA Technologies. EEZY KEYZ® is compatible with all leading email services. There is no need to change email addresses or email service provider. The cross-platform solution is currently available for Android and iOS devices as an email client application. It will also be available for all devices, supporting browser extensions, as Chrome & Firefox browser extensions later in 2019. There is also an option for it to be developed as an MS Outlook Add-in for the Windows PCs.

Deploying, administering and using EEZY KEYZ® is easy and seamless. The encryption and key exchange processes and digital signing of the messages are automatically handled by the software and the web API of the backend system. The user experience doesn't differ from the normal unencrypted email the employees are used to. The messages are also saved encrypted both locally on the devices and on the email server.

EEZY KEYZ® eliminates the risks of email data breach and makes your email compliant with data security laws and regulations. It makes your organization more efficient by enabling fast, flexible and secure communications by email. By securing and authenticating email communications it also makes it possible to adopt new practices.

THE BENEFITS OF YOUR OWN DEDICATED ENCRYPTION SYSTEM

There have been different email encryption products available since the 1990s. However, the reliable solutions have been too complex to take in use and too difficult to use for end-users. In the latest years different cloud-based encryption providers have introduced user-friendly and convenient solutions. However, these cloud-based solutions do not offer high enough security level and control for the demanding customers. As a result, many organizations have prohibited the use of email and have decided to rely on alternative systems when communicating confidential information. Secure alternative systems are often less efficient and user-friendly than email so confidential information tends to end up in the email in spite of prohibitions.

EEZY KEYZ® has been developed as a military-grade encryption solution while simultaneously being as user-friendly as normal email. It is easy-to-adopt, operate and use on customer's existing hardware. The customer tailored and dedicated encryption system brings a lot of benefits. Firstly, there is no need to depend or trust cloud providers or service providers. The customer stays in complete control of its data, including email messages, attachments and encryption keys. This helps avoiding political risks relating to encryption products; in many countries' vendors can be forced to turn over encryption keys to the authorities. With EEZY KEYZ® this is not possible because only the customer has access to the keys.

It is possible to tailor the system features to perfectly match customer's needs; including the backend system features, email application features, used algorithms, etc. The result is an encryption system which allows easy, quick and secure way to deliver confidential information in any format (image, video, documents, etc.) whenever and wherever.

IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

HOW IT WORKS

The Figure 1 illustrates how the EEZY KEYZ® system works.

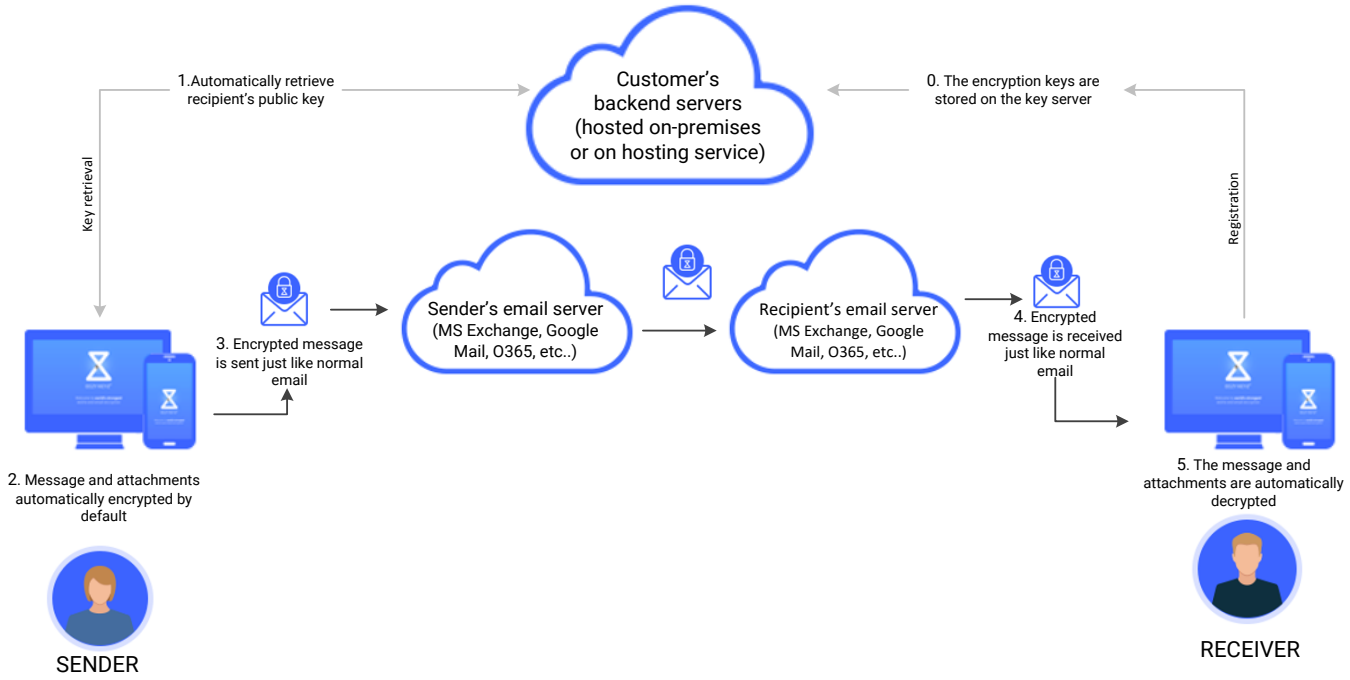


Figure 1. How EEZY KEYZ® works

0. Users' encrypted asymmetric encryption keys are automatically stored on the key server when users register to the system.
1. When user inserts the message recipients, the EEZY KEYZ® email client software automatically retrieves the public keys of the recipients from the key server.
2. User composes the email message normally. The software automatically encrypts all messages and attachments and digitally signs the messages by default.
3. User sends the email normally without any extra steps. The encrypted email messages pass through company email servers like any other messages.
4. Receivers receive the encrypted email in their inbox like any other email.
5. The message is automatically decrypted on user's device temporarily when viewed. The message and attachments are stored encrypted both on the user's device and on the email server.

CONCLUSION

- Eliminate the risks of email
  - Ensure that your email data in transit cannot be intercepted and hacked
  - Ensure that your email data stored cannot be hacked
  - Eliminate spear phishing attacks
- Streamline processes
  - Turn email into secure communication and information exchange channel

IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

  - Take advantage of secure encrypted and authenticated communication wherever even over unsecure public networks
- Stay in control of your data
  - You and only you have complete control of the data
  - No trust on third parties required
  - Possibility to tailor the system features
- Easy to operate and use
  - The encryption system can easily be integrated with existing email architecture
  - Easy to operate for the system admin
  - Seamless end user experience

2. Technical Overview

The EEZY KEYZ® system consists of the email clients with built in automated encryption capabilities and of the backend system. The admin of the system can allow user registration to the system and disable users from the system and the admin handles the key lifecycle management.

EMAIL CLIENTS WITH BUILT IN AUTOMATED ENCRYPTION CAPABILITIES

To use the encryption system the user needs an EEZY KEYZ® email client. The email clients handle the creation of the asymmetric encryption keys which are also stored on the backend system's database. The email clients automatically handle the encryption of the email messages and attachments, which are then delivered to the recipients normally via customer's email servers. The email messages and attachments are encrypted with symmetric-key encryption, while the asymmetric-key encryption is used to encrypt the used symmetric-key encryption key.

For Android and iOS there are standalone EEZY KEYZ® email clients. For the desktop there will be EEZY KEYZ® Firefox and Chrome browser extensions later in 2019. There is also an option for it to be developed as an MS Outlook Add-in for the Windows PCs. All of these clients are compatible with each other in regards of encrypting and decrypting emails.

BACKEND SYSTEM

The backend is divided into micro services which run in Docker containers. The web API of the backend system is used when storing and delivering the required asymmetric encryption keys. The private asymmetric encryption keys are stored encrypted with symmetric-key encryption. They are only available to the correct users who know the passphrase which is used to decrypt the private asymmetric encryption key. The public asymmetric encryption keys are available to all users of the system.

The backend system consists of the following services:

web API
- user account verification
- storing the users' encrypted private and public asymmetric encryption keys
- delivering the users' asymmetric encryption keys

admin services
- User & encryption key management

email service
- delivering account verification emails to users

3. EEZY KEYZ® Encryption

The default encryption of the EEZY KEYZ® system utilizes public-key cryptography using Elliptic Curve Cryptography (ECC) and symmetric-key encryption using Advanced Encryption Standard (AES) algorithm. The emails are end-to-end encrypted using Elliptic-curve Diffie-Hellman (ECDH) and AES-GCM which provides data authenticity/integrity and confidentiality. Elliptic Curve Digital Signature Algorithm (ECDSA) is used to verify the sender by digitally signing the hash of the sender's public key.

The used default algorithms and curve are listed below:

- The used symmetric encryption algorithm is AES-GCM 256bit which provides proof of data integrity and confidentiality
- The used public-key cryptography uses EC keys. The used cryptography schemes are ECDH for shared secret generation between users and ECDSA signature to validate sender authenticity. The default EC curve is secp256r1 offering 128 bits of security.
- The used signature algorithm is ECDSA-SHA2-512
- The used hash algorithm is SHA2-512
- Messages and attachments are also stored locally encrypted
- The sensitive message-related metadata is also encrypted, such as the names of the attachments, the subject of the email, etc. and only the information retrieved from the encrypted container is regarded as trusted

When sending encrypted email, the main process involves acquiring the recipients' public EC keys from the backend by using the web API and using these keys and AES 256-bit encryption to encrypt the whole email message including attachments.

Process of sending encrypted email with EEZY KEYZ® email client is following:

1. User creates a new email
2. User inputs the recipients
3. The client checks from the backend using the web API if the recipients are EEZY KEYZ® users and automatically fetches their public keys
    a. In case all of the recipients are users, email is sent encrypted
    b. In case all of the recipients are not users, a warning notification message is shown and if accepted the email is sent normally without encryption
    c. In case some of the recipients are users and some are not, warning is issued and, if accepted, email is sent normally without encryption to all of the recipients
4. ECDSA-SHA2-512 is used to verify the sender by digitally signing the sender's public key's hash
5. Unencrypted email body is created which states that this email is encrypted email
6. The email composed by the user and the possible attachments of the email are compressed and then encrypted into separate EEZY KEYZ® attachments using AES-GCM 256-bit encryption using different IV for the email message and each of the attachments of the email
7. AES key is encrypted using symmetric key which is derived with ECDH using receiver's public and sender's private EC keys
8. Of these encrypted EEZY KEYZ® attachments the encrypted email is built including:
    a. 1 attachment containing the metadata, which contains the information about the email and instructions for the EEZY KEYZ® email clients to decrypt the email
    b. 1 attachment containing the user's composed email
    c. any attachments included in the email
    d. Email message is created with at least two attachments. The metadata attachment and the actual encrypted message.

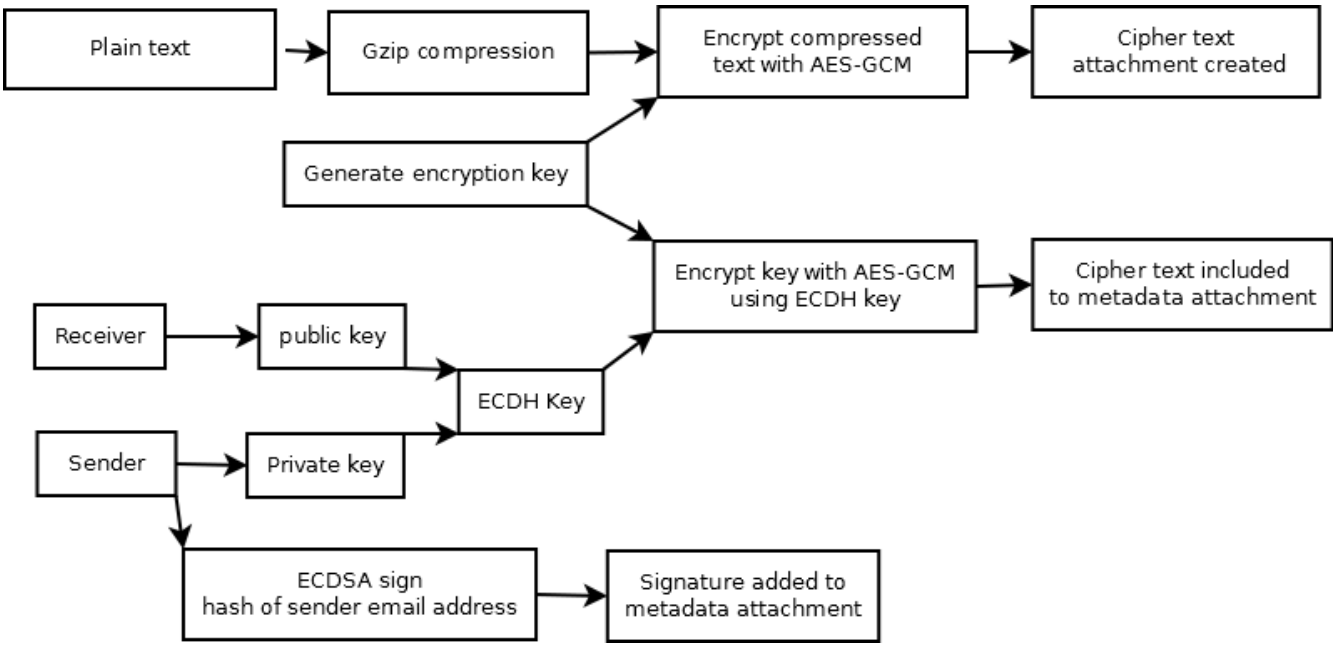


Figure 2. EEZY KEYZ® encryption process

ENCRYPTION TAILORING OPTIONS

The tailoring options for the EEZY KEYZ® system's encryption include e.g:

- Different ECC curve than the standard. We can provide ECC curves up to NATO Secret Level.
- Front door mechanism to encrypted emails. This provides the customer organization an option to open any of the encrypted emails sent using their system for the encryption.
- Other customer specific customizations.

4. Backend System

The EEZY KEYZ® backend system functions as the key exchange and key storage system. It works as the contact lookup for the software to retrieve recipients' public keys. It also serves as a secure private key storage: users' private keys which are encrypted by the EEZY KEYZ® email clients are stored on and retrieved from the backend system's database by using the web API. This allows users to move the private key between devices easily. The EEZY KEYZ® email clients communicate automatically with the backend system through the web API.

The connections to the backend servers should be restricted to a few IP addresses by default from where the system admins can connect to the system. Only the API should be available to the EEZY KEYZ® email clients. All of the connections between clients and the backend web API are done using HTTPS/TLS connections.

The backend system consists of the following services:

web API

- account verification
- storing the users' private and public ECC keys
    - The private key is encrypted with AES 256 GCM, of which key is derived from the user's passphrase
    - With the private EC key, a Proof of Knowledge value is stored on the backend database. This Proof of Knowledge is used to determine that the user knows the passphrase and can get the encrypted private key to the EEZY KEYZ® email client. The passphrase is never sent to the backend.

- delivering the users' ECC keys
    - Over TLS connection
    - User's encrypted private key is delivered only if the user can provide proof that the user knows the passphrase associated with the stored key. Knowledge of proof calculation is used to achieve this.

admin services

- Allowing the user registration to the system and disabling the user accounts
    - The admin can submit a list of the allowed email addresses to the system which have the right to create an account on the system to utilize the EEZY KEYZ® encryption
- Deactivation of the encryption keys
- Destruction/Removal of the encryption keys
    - In extreme cases the admin can delete the encryption keys. After this the encrypted emails cannot be opened again and because of this it should not be done lightly.
- Adjustable encryption key lifecycle
    - Admin decides the length of the active period of the newly generated keys

email service

- delivering account verification emails to users

logstash and filebeat

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

database

- storing of the user accounts and the associated encryption keys

Nginx

- used to provide communication interface between the email clients and the web API

The backend system runs in Docker containers. Initial containers and updates are delivered to the customer:

- through Docker registry from which the customer can pull them from
- or as TAR files delivered as desired by the customer
- The backend system requires minimal maintenance (certificate renewal & installing updates)

An example of EEZY KEYZ® service backend:

Backend runs distributed to multiple servers with load balancer managing traffic to servers

- Services/Modules used: API, Admin, Nginx, Email, Logstash, Filebeat, MariaDB
- The modules require certificates signed by trusted CA
    - Certificates used by the backend services should be managed by the customer (initial support is offered)

Example of the EEZY KEYZ® service's backend is presented in figure 3 on the next page.

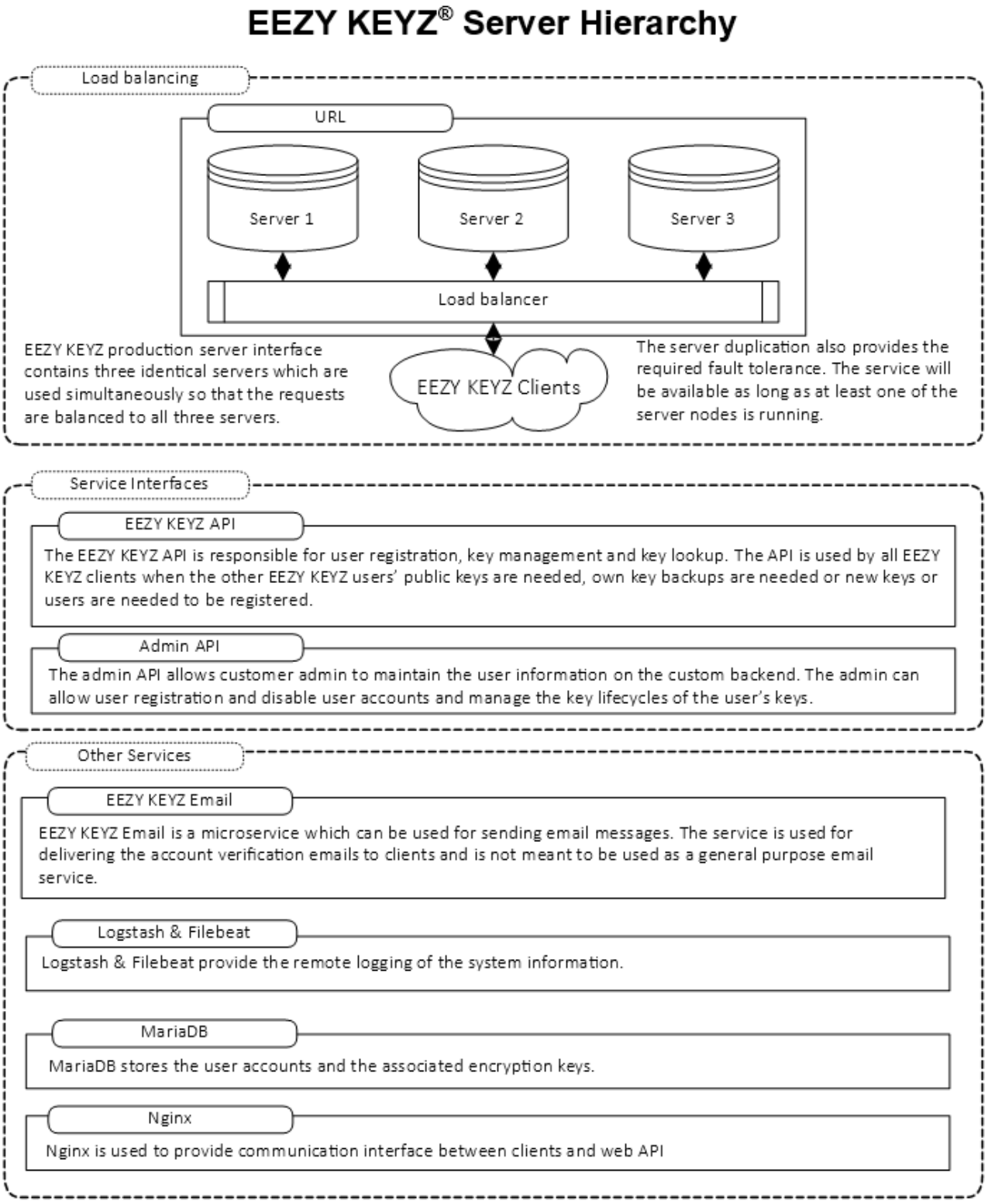


Figure 3. Default EEZY KEYZ® server setup

BACKEND TAILORING OPTIONS

The tailoring options for the EEZY KEYZ® backend system include e.g:

- User authentication when registering to the system. Options include for example OAuth2 or token-based system
- Certifications used in the system are from the Let's Encrypt by default. As an option certificates can also be made using the CA of the customer organization.
    - If the CA of the customer organization is used to create certificates, the browser plugins won't work unless the organization has its own build of the browser which includes their certificates. Because of this the public certificates from Let's Encrypt are recommended.
- Logging of the system information can be adjusted according to the customer requirements.
- The login to Admin portal can be modified according to the customer's requirements. Options include: Certificate based login system, Username + password + Authenticator code system, or using customer's existing authentication system
- The API calls can be rate limited
- Locking the user's account after too many wrong passphrase inputs
- Some another backend system delivery format than Docker containers
- Other possible customer specific customizations in the admin features

5. EEZY KEYZ® Email Clients

EEZY KEYZ® Android and iOS applications are custom mobile email client applications with all the usual features one would expect from an email application. The applications use strong encryption to protect the email messages and attachments. When composing email messages, the application automatically checks the recipient's email address from the backend and retrieves the public key of the recipient, if available. All messages to other users are automatically end-to-end encrypted using ECDH and AES-GCM which provides data authenticity/integrity and confidentiality and ECDSA is used to verify the sender by digitally signing the hash of the sender's public key. The user-experience is completely seamless. The messages and attachments are also saved encrypted on both the device and on the email server. The developed customer specific application will be delivered, as desired by the customer, within the limitations of the platforms.

The private EC keys used by the Android EEZY KEYZ® email clients are securely stored on the Android device in encrypted database. Database is encrypted using randomly generated key that is secured with Android KeyStore.

On iOS the encrypted EC private key is stored on the iOS Keychain.

When the user logs out of the account on Android and iOS EEZY KEYZ® email client, all of the information stored by EEZY KEYZ® on the device is deleted.

EEZY KEYZ® application default features:

- Available for Android 6.0 (API level 23) or newer operating systems
- Available for Apple iPhone and iPads running the iOS 9.0 operating system or later
- Supports IMAP and Exchange (EWS) email protocols
- The maximum size of attachments supported by the application is currently 10 MB
- Messages and attachments stored locally encrypted
- English language
- Default EEZY KEYZ® User Interface
- Warning messages displayed when sending unencrypted messages

The User's Guide for the applications is provided as attachment "EEZY KEYZ® Email Client User's Guide".

EEZY KEYZ® EMAIL CLIENT TAILORING OPTIONS

The tailoring options for the EEZY KEYZ® system's email clients include e.g:

- Customer-tailored application can support different kinds of security levels as desired by the customer.
  - The information in the notifications shown by the EEZY KEYZ® email client can be adjusted.
  - The PIN code and the passphrase can be asked in the situations the customer desires.
  - Warning messages when sending emails to non-users can be adjusted. For example, when sending email which can't be encrypted the user is always alerted. Or no notification is shown.
  - Allow the user only to send encrypted emails.
- Different kinds of UI customizations. For example, custom color templates, custom logo, custom graphics
- Localizations
- Adjusting the maximum size of attachments to the organization's needs. This is affected by the devices the organization is using as well as the email provider the organization is using.
- Other customer specific customizations

6. Chrome & Firefox Browser Extensions

EEZY KEYZ® Chrome & Firefox browser extensions are currently under development and will be released later in 2019.

CHROME & FIREFOX BROWSER EXTENSIONS

EEZY KEYZ® Chrome and Firefox browser extensions will be compatible with webmail e.g. Gmail/Gsuite, O365 or customer specific webmail. Emails encrypted using the webmail extension can be read on other clients as well and vice versa. The EEZY KEYZ® Chrome and Firefox extensions will seamlessly be integrated in the webmail interface. The extension automatically encrypts emails sent to other users. The received encrypted emails can be read through the webmail the same way as normal emails.

CHROME & FIREFOX BROWSER EXTENSIONS TAILORING OPTIONS

The tailoring options for the EEZY KEYZ® browser extensions include e.g:

- Tailoring the integration for organization's own webmail system, i.e. not Gsuite or O365 based webmail.
- Customer-tailored browser extensions can support different kinds of security levels as desired by the customer.
  - The intervals of inserting the passphrase while reading encrypted messages can be adjusted.
  - Warning messages when sending emails to non-users. For example, when sending email which can't be encrypted the user is always alerted. Or no notification is shown.
  - Allow the user only to send encrypted emails.
- Different kinds of UI customizations. For example, custom color templates, custom logo, custom graphics
- Localizations
- Adjusting the maximum size of attachments to the organization's needs. This is affected by the email provider the organization is using.
- Other customer specific customizations

IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

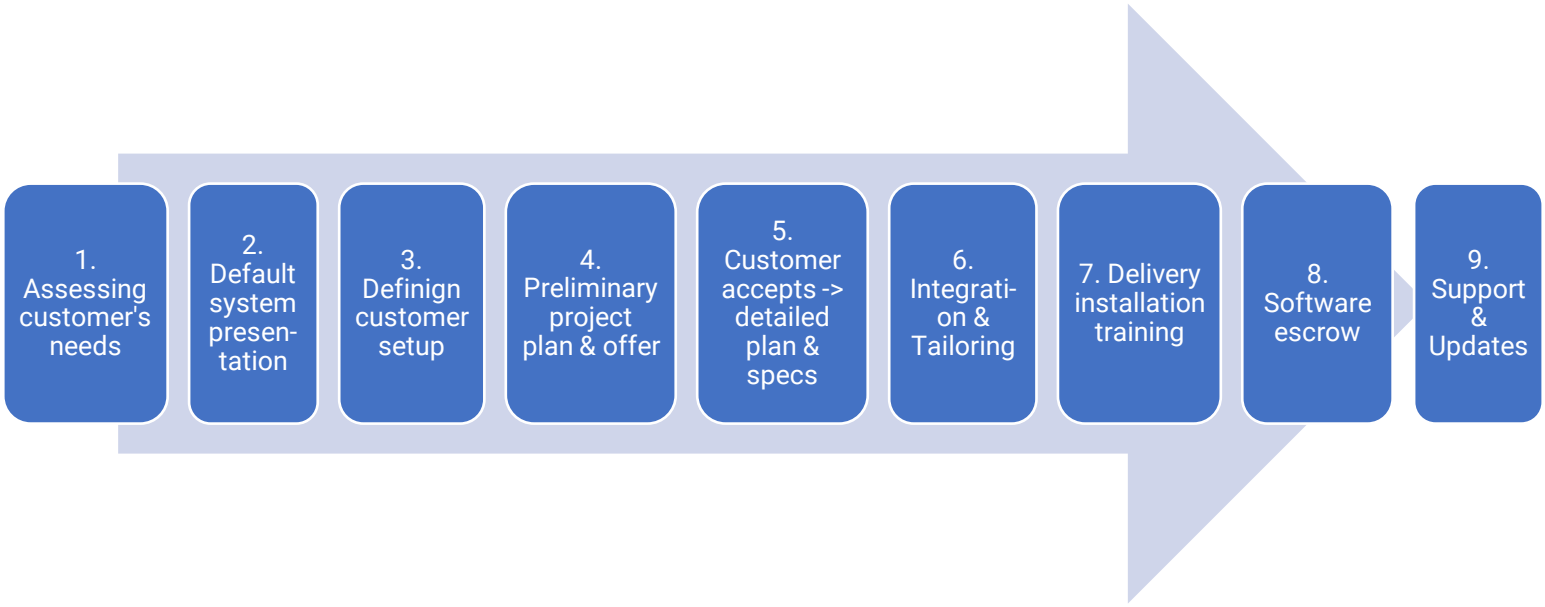
7. The Deployment Process

This chapter presents the complete deployment process of the customer-tailored EEZY KEYZ® email encryption system from the initial customer need assessment until the after sales services. Each tailoring process is always unique and different and therefore the process includes multiple steps. The careful planning of the project, determining the tailored system requirements and features in addition to continuous dialog between the customer and IPRA is crucial for the success of the project.

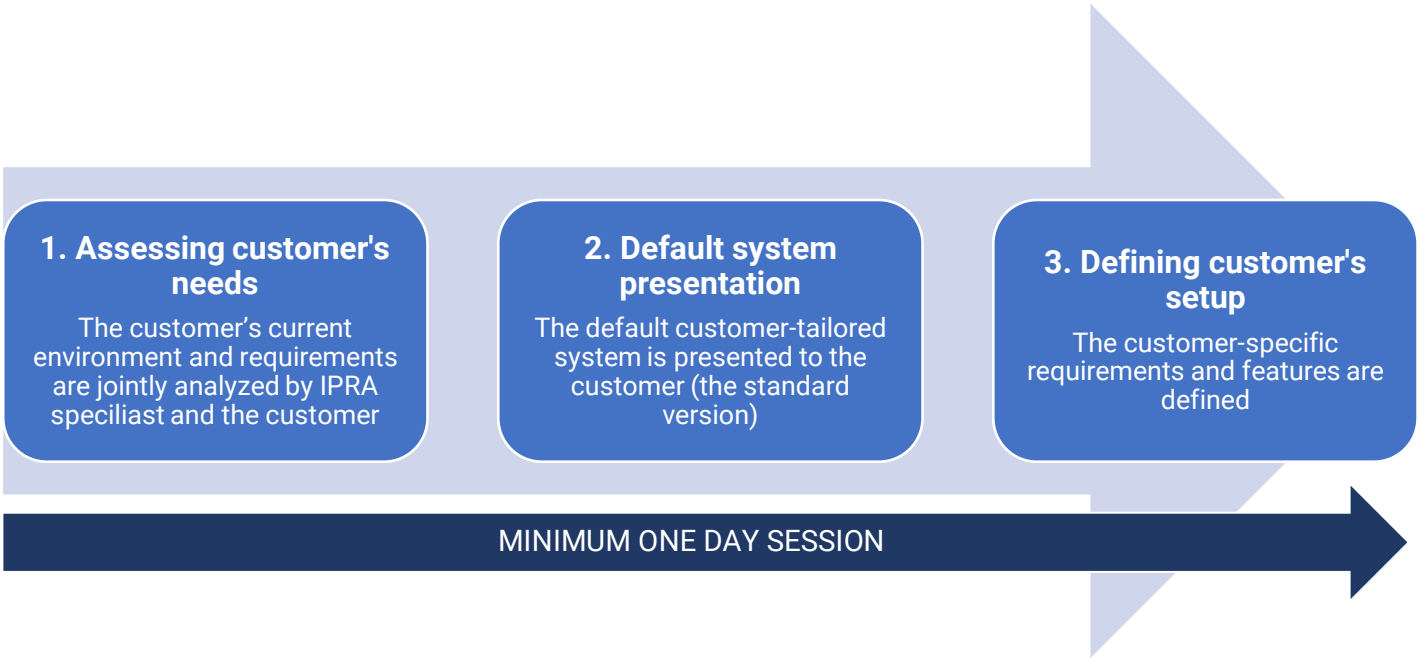
There are no special pre-requirements for the customer-tailored EEZY KEYZ® email encryption system project. However, the customer should be capable of hosting their own servers or alternatively be prepared in acquiring the server hosting service from a 3rd party. The customer-tailored backend system runs on self-managed server environment which adds the requirement for the customer organization to have its own IT capabilities. These should include operating in server environment hosting the backend system and having knowledge of managing Docker containers. IPRA offers comprehensive training in the required backend management.

The customer's Admin and other IT staff are trained during the initial delivery to use and maintain the backend system and also to use the encryption clients so that they can provide support for the customer's end users. The initial deployment of the system is conducted under the guidance of IPRA experts. This can also be used as a preliminary training on the management of the backend system for the customer's Admin and other IT staff. After the initial setup and training IPRA continues to offer support and updates to the system as a part of the license agreement.

The complete deployment process from the very beginning of the project until after sales services of the customer-tailored EEZY KEYZ® is illustrated below:



PRESALES



The presales part of the process starts after the customer has expressed interest to purchase the system. A minimum one-day session is organized between IPRA's and customer's technical personnel. The customer needs are assessed and mapped, default EEZY KEYZ® system presented and the customer-specific requirements and features defined.

1. Assessing customer's needs
    a. Analyzing the customer's current environment
        i. Email architecture
        ii. Devices used in the customer organization (Android, iOS, PCs, Browsers, Operating systems...)
        iii. Server architecture (existing self-hosted servers or hosted servers)
        iv. IT capabilities (in-house organization or outsourced)
        v. Other customer specific factors?
    b. Analyzing customer's requirements
        i. Preliminary screening of the customer specific needs and requirements
        ii. Other customer expectations?
2. Default system presentation
    a. Detailed presentation of the customer-tailored EEZY KEYZ® system
    b. Presenting possible customizations and tailoring
3. Defining customer's tailored system setup
    a. After analyzing the customer's environment & requirements and presenting the default system the customer tailored system can be jointly defined
    b. The result is a preliminary high-level specifications of the customer tailored system. At this point this can include multiple different possible scenarios/setups.

IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

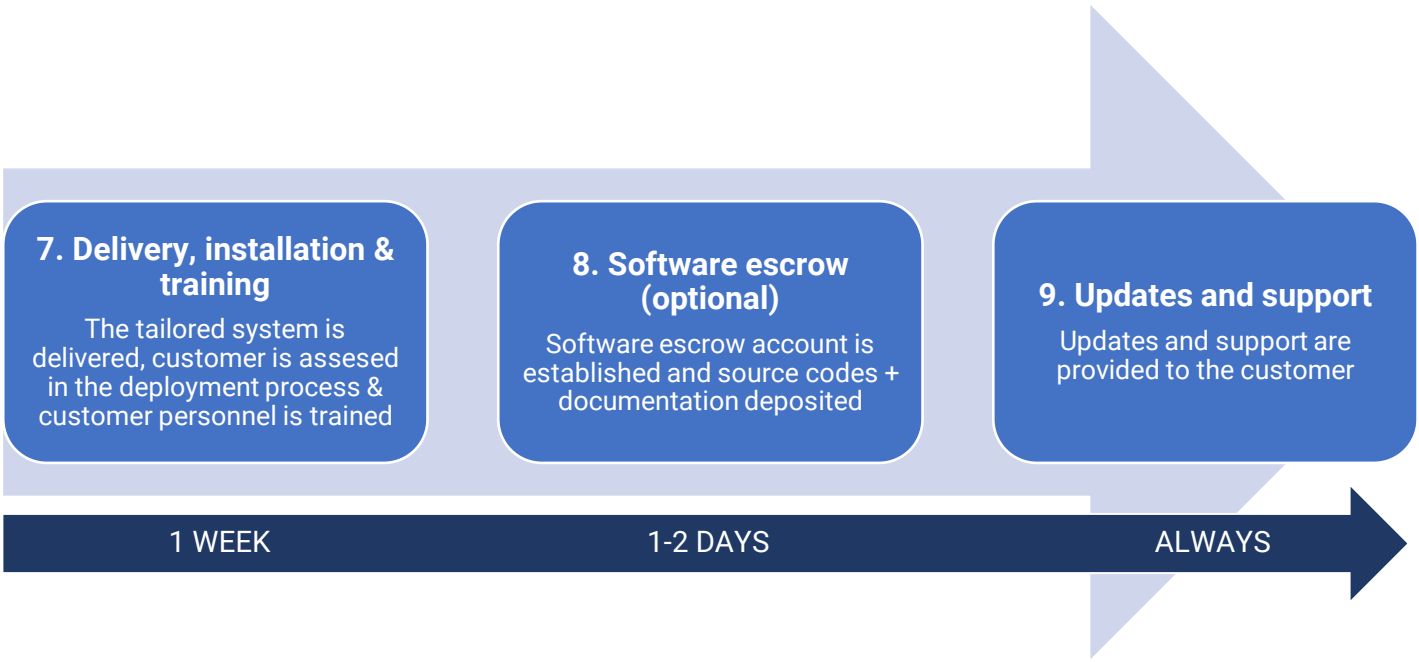
TAILORING PROJECT

The actual tailoring process starts with creating an initial project plan and offer. Once customer accepts the offer, a detailed project plan and specifications are created. The default system is tailored to be integrated with customer's environment and customer-specific features developed according to the plan and specifications.

4. Preliminary project plan, offer & contract
    a. Based on the information gathered during the previous session a preliminary project plan and offer are generated and delivered to the customer
    b. Project plan includes the estimated timetable for the project, main development features, high level specifications, project personnel (both sides), etc.
    c. Preliminary project plan can have more than one project scenarios based on the customer's requirements
    d. Offer is created based on the preliminary project plan. The offer can also include more than one scenario (The price of setup 1 is X€, The price of setup 2 is Y€)
    e. Customer and IPRA have a dialogue until final consensus is reached and contract is signed
5. Detailed project plan & specifications
    f. Once customer has accepted the offer and the project plan, a detailed final project plan is created, and system specifications are generated
    g. Final project plan jointly created by IPRA and customer
    h. Detailed system specifications of the tailored backend and encryption clients include comprehensive system documentation
6. Integration & developing the tailored system
    a. The tailored backend system and encryption clients are developed as set forth in the project plan and system specifications
    b. Schedule depends on the number of customizations and the complexity of the tailored features

IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

DEPLOYMENT & AFTER SALES



The final part of the process includes system deployment and training. At this point a software escrow can be established if the customer wishes. Regular updates and support are offered and included in the license agreement.

7. Delivery, installation & training
    a. The tailored-system is delivered to the customer and customer is assessed in the installation and deployment process of the backend system and encryption clients
    b. Acceptance testing is conducted by the customer after the system has been set up
    c. Customer's personnel are trained to operate the system by IPRA experts
8. Software escrow
    a. Software escrow account is established if the customer wants so
    b. All of the tailored system source codes and system documentations are deposited in the escrow account
9. After sales: Updates and support
    a. After the system has been successfully deployed and customer trained to operate it IPRA continues to provide support for the customer
    b. Updates are provided to the customer regularly
    c. Completely new features desired by the customer are developed and billed separately as agreed upon separately (not included in the updates)

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

Asian market representation:
Jari Vepsäläinen
jari@fintrade.com.hk
Room 2506, 25/F, China Insurance Group Building,
141 Des Voeux Road Central, Hong Kong
Tel: (852) 2850 7125, Fax (852) 2543 0747