Customer-Tailored EEZY KEYZ® Email Encryption System

IPRA Technologies Ltd Finland 2018

Contents

Date: January 12th 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 encryption clients. The backend system functions as the encryption key exchange and storage system. The encryption clients automatically encrypt and digitally sign email messages and attachments sent to other users. The message-related metadata is also encrypted and only the information retrieved from the encrypted container is regarded as trusted. The backend system and encryption 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 encryption 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 Windows PCs as an MS Outlook Add-in and to all devices as Chrome & Firefox browser extensions in 2019.

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 backend system. The user experience doesn't differ from normal unencrypted email 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, encryption 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.

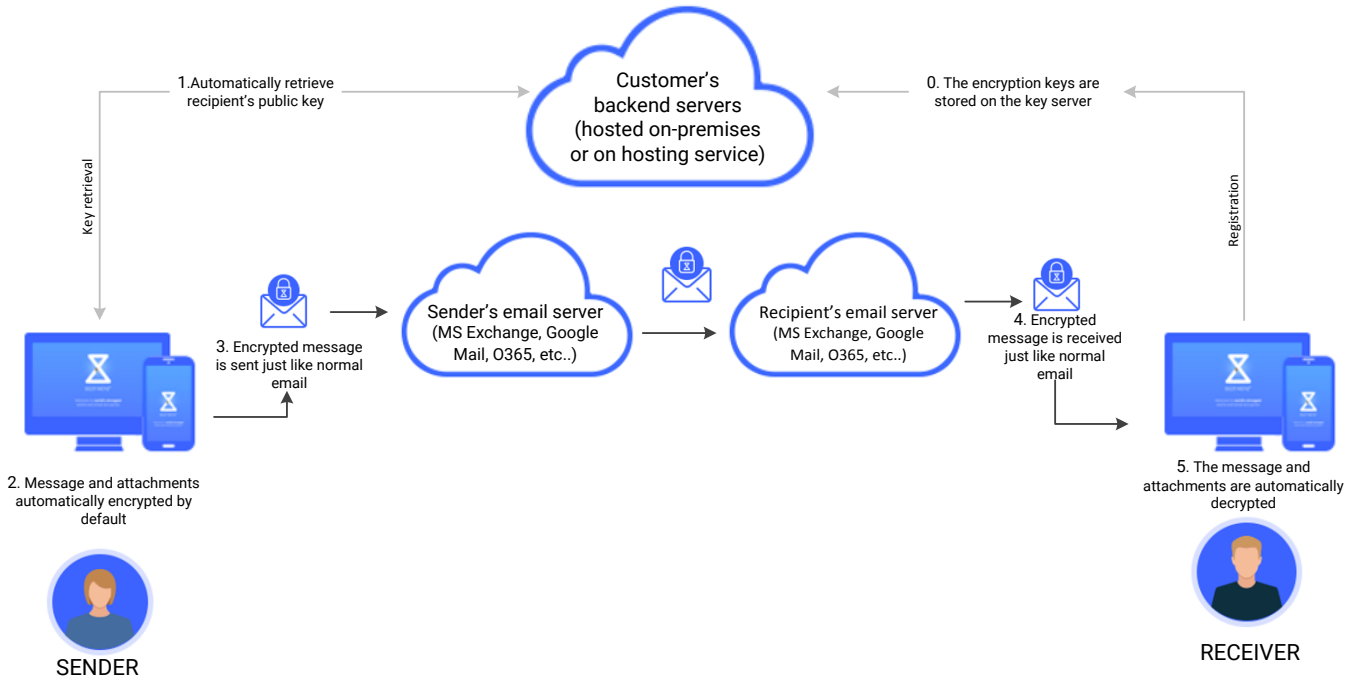


Figure 1. How EEZY KEYZ® works

0. Users' encryption keys are automatically stored on the key server when users register to the system.
1. When user inserts the message recipients, the encryption 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 email server.

CONCLUSION

- Eliminate the risks of email
  - Ensure that your email data in transit cannot be intercepted
  - Ensure that your email data stored cannot be hacked
  - Eliminate spear phishing attacks
- Streamline processes

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

  - Turn email into secure and efficient communication and information exchange channel
  - 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 encryption clients and the backend system. The clients handle the creation of the ECC keys and encryption and decryption of the email messages and attachments automatically, while the backend system handles the storing and delivering of the required ECC keys. The private ECC keys are stored encrypted with AES 256-bit encryption. They are only available to the correct users who know the passphrase which is used to decrypt the private key. The public ECC keys are available to all users. The email messages and related data are encrypted with AES 256, while the ECC is used to encrypt the used AES keys.

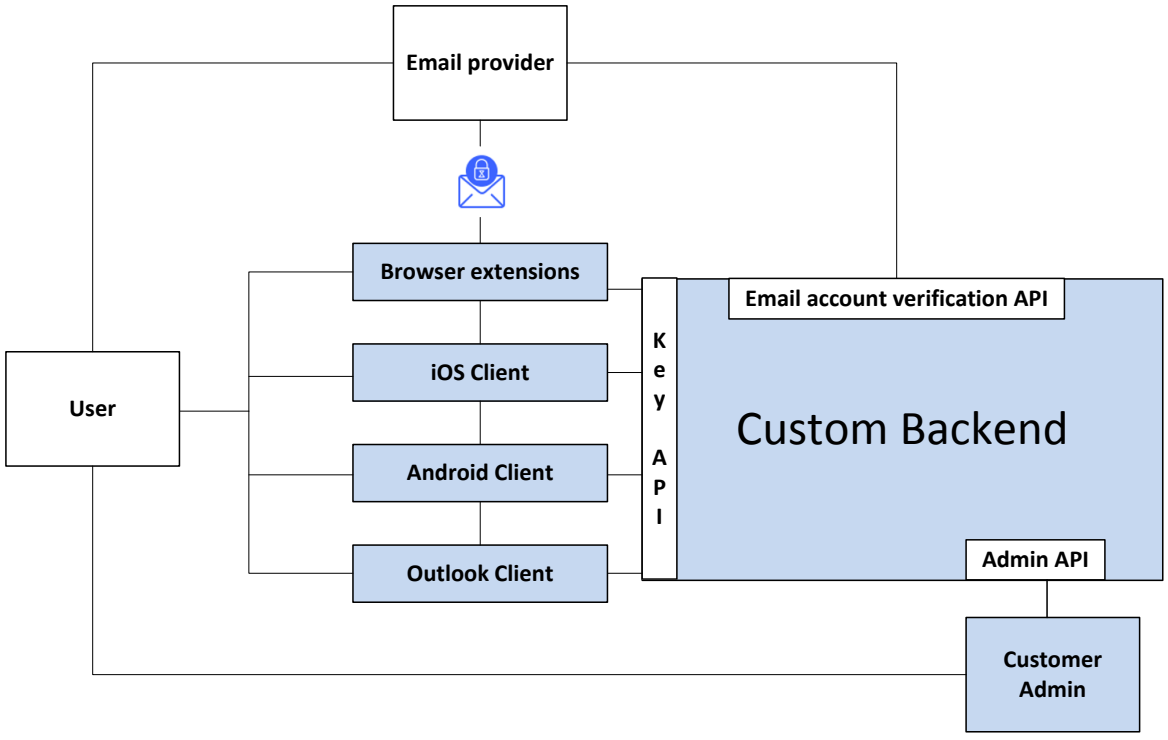


Figure 2. EEZY KEYZ® system overview

Figure 2 presents the overview of the EEZY KEYZ® system. Custom Backend handles the encryption key and user management via Key API and Admin API. It also handles the user's email account verification during registration. Customer Admin can add and delete users from the system and handle key lifecycle management. Users use the encryption clients to send and receive encrypted email. The encryption clients handle the end-to-end encryption and digital signing of the messages which are then delivered normally via customer's email servers.

ENCRYPTION CLIENTS

To use the encryption system the user needs an EEZY KEYZ® encryption client. For Android and iOS there are standalone EEZY KEYZ® email clients. For the desktop there will be an EEZY KEYZ® Outlook Plugin and Firefox and Chrome browser extensions later in 2019. All of these clients are compatible with each other in regards of encrypting and decrypting emails.

The private ECC keys used by the clients are securely stored on the clients:

- On iOS the encrypted ECC private key is stored on the iOS Keychain or encrypted database.
- On Android the keys are stored in encrypted database. The database is encrypted using with 256-bit AES. The password for the database is generated randomly when the database is created. The password for the database is stored in a local Android KeyStore.
- When user logs out of the account on mobile clients, all of the information stored by EEZY KEYZ® on the device is deleted.

BACKEND SYSTEM

The backend is divided in microservices which run in Docker containers. The connections to the backend servers should be restricted to a few IP addresses by default. Only the API should be available to the clients.

All of the connections between clients and the backend are done using HTTPS/TLS connections. EEZY KEYZ® uses a custom certificate authority. This allows the clients to authenticate the backend during communication by checking that the certificate provided by the backend matches the one they are expecting. The clients also need to provide authentication when using the backend API. The backend system consists of the following services:

key service

- user registration
- storing the users' private and public ECC keys
    - The private key is encrypted with AES 256 GCM, which is derived from the user's passphrase
    - With the private ECC key, a Proof of Knowledge value is stored on the backend. This is used to determine that the user knows the passphrase and is allowed to get the encrypted private key to the client. The passphrase is never sent to backend.
- delivering the users' ECC keys
    - Over TLS connection & to authenticated clients
    - 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.
    - The backend does not allow multiple passphrase guesses in row. This is implemented to prevent the brute forcing of the passphrase.

admin services

- User & encryption key management

email service

- delivering registering emails to users

3. EEZY KEYZ® Encryption

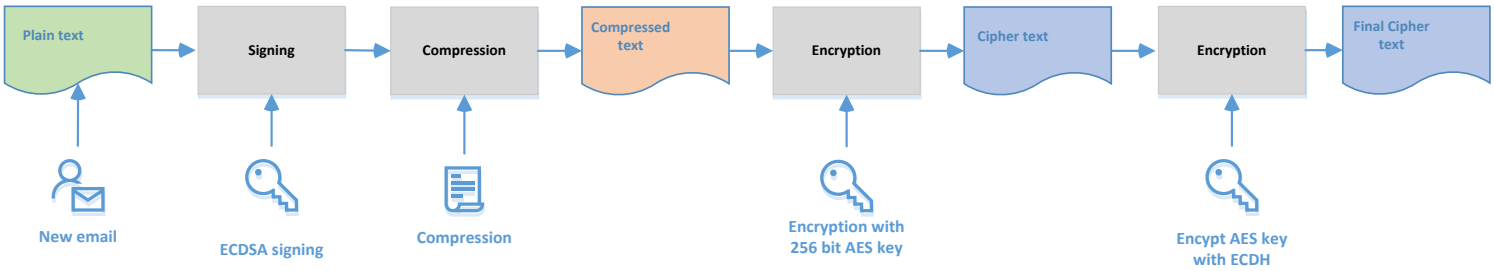
The default encryption of the EEZY KEYZ® system utilizes Elliptic Curve Cryptography and Advanced Encryption Standard. The used default algorithms and curve are listed below:

- The used symmetric encryption algorithm is AES-GCM 256
- 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 encryption. The default EC curve is curve25519 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 message-related metadata is also encrypted 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 ECC keys from the backend and using these keys and AES 256-bit encryption to encrypt the whole email message (header, attachments and content) for all of the recipients. The recipients' public keys are stored on the device, in case they are needed in the future. A sent copy is created with the same encryption but the sender's public ECC key is used. This copy is shown in the sender's sent messages folder.

User sends email with EEZY KEYZ® client:

1. User creates a new email
2. User inputs the recipients
3. Client checks from the backend 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. Email is compressed
6. Email is encrypted with AES-GCM 256-bit encryption.
7. AES key is encrypted using symmetric key which is derived with ECDH using receiver's public and sender's private ECC keys
8. Email message is created with at least two attachments. The email body is unencrypted notification message that this is an encrypted message. The actual encrypted message and its attachments are attached as encrypted containers.
9. Copy of the sent email is created and encrypted the same way as recipients' emails but using the sender's public ECC key. This email is shown in the sent folder.



ENCRYPTION TAILORING OPTIONS

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

- Different ECC curve than the standard curve25519. 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 Certificate Authority of the system and contact lookup for the software to retrieve recipients' public keys. It also serves as a secure private key backup: users' private keys which are encrypted by the encryption clients are stored on and retrieved from the backend system. This allows users to move the private key between devices easily. The encryption clients communicate automatically with the backend system. The default backend system is as follows:

The Customer Admin handles the user and key management through the Admin portal running on the backend system:

- Addition/Creation & deletion of users
  - User authentication and validation through verification emails
- Activation of the encryption keys
- Deactivation of the encryption keys
- Destruction/Removal of the encryption keys
- Adjustable encryption key lifecycle (Admin decides the length of the active period of the newly generated keys)

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)

The default backend/server configuration:

Backend runs on three servers with load balancer managing traffic to servers

- Services/Modules used: API, Admin, Nginx, Health-Check, Email
- The modules require certificates signed by trusted CA
  - Certificates used by the backend services should be managed by the customer (initial support is offered)
- Database cluster and Load Balancer should come from the server service provider
- A hosted HAproxy load balancer manages the traffic to 3 hosted virtual servers. The servers connect to database which runs in hosted Galera cluster.

Default logging:

- Changes in the encryption key states & timestamps of each Private key fetch

EEZY KEYZ Server Hierarchy

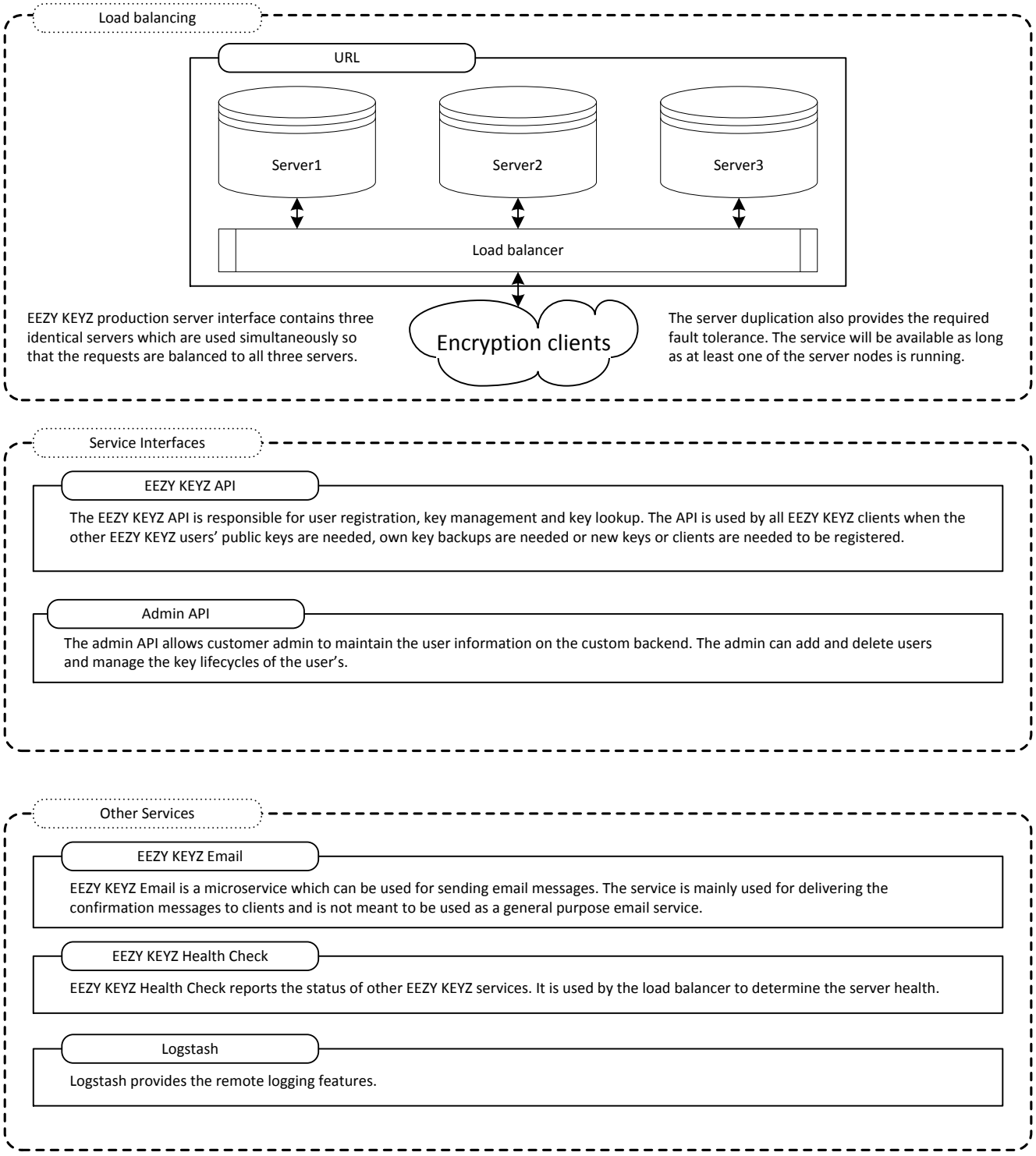


Figure 5. Default EEZY KEYZ® server setup

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. Options include for example certificates made using the CA of the customer organization, public certificates like Let's Encrypt, or IPRA created custom CA which is delivered during the initial system delivery with guidance how to manage it and renew certificates.
- Logging of the system can be adjusted according to the customer requirements.
- The login to Admin portal can be modified according to the customer requirements. Options include: Certificate based login system, Username + password + Authenticator code system, or using customer's existing authentication system
- Server configuration can be modified according to the customers' requirements.
- Some another backend system delivery format than Docker containers
- Other possible customer specific customizations in the admin features

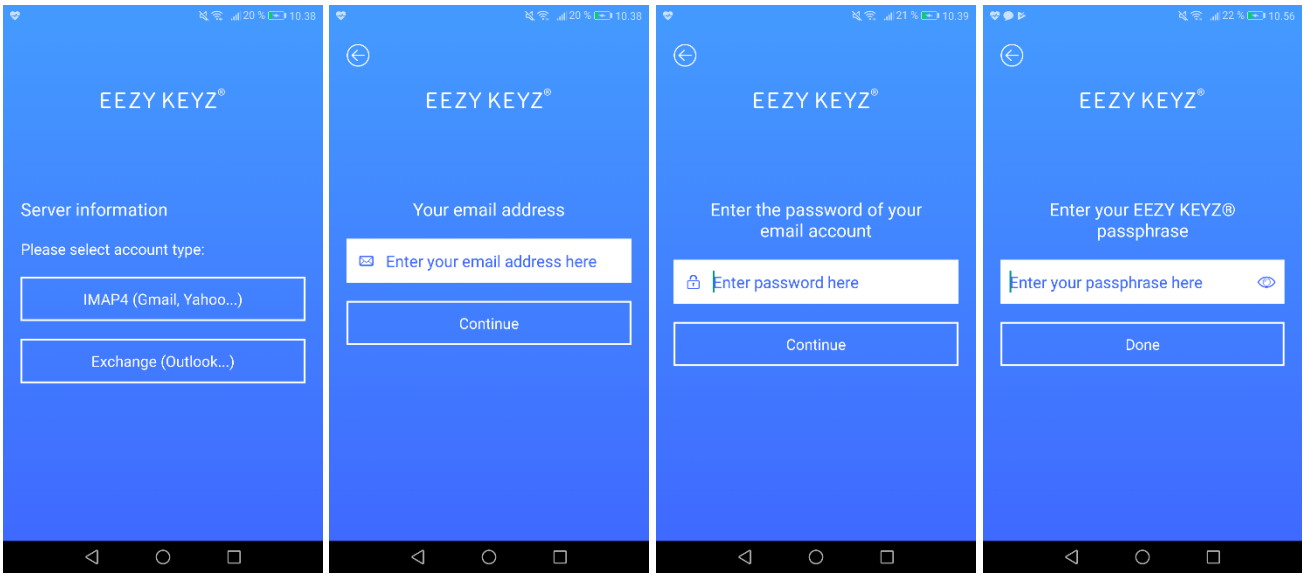
5. Android Client

EEZY KEYZ® Android application is a custom mobile email client application with all the usual features one would expect from an email application. The application uses 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 and digitally signed by default. The user-experience is completely seamless. The messages and attachments are also saved encrypted on both the devices and on the email server. The developed customer specific application will be delivered as an APK file, as desired by the customer.

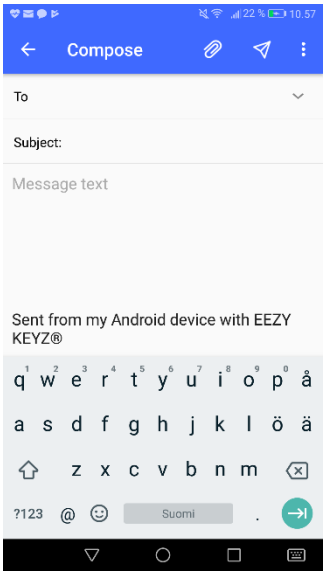
EEZY KEYZ® Android application default features:

- Available for Android 6.0 (API level 23) or newer operating systems
- 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 in an encrypted database
- English language
- Default EEZY KEYZ® User Interface
- Passphrase asked during initial login
- Warning messages displayed when sending unencrypted messages

The screenshots below show the default EEZY KEYZ® Android client login process interfaces for a registered user.



The screenshot below shows the default EEZY KEYZ® Android client message composing interface.



ANDROID CLIENT TAILORING OPTIONS

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

- Customer-tailored Android application can support different kinds of security levels as desired by the customer.
    - The intervals of inserting the passphrase while using the app or the PIN code can be adjusted. For example, the passphrase/PIN code could be asked every time an encrypted email is opened or only on the initial start of the application.

  - Notifications can be adjusted. For example, when receiving encrypted email, the user is notified that he has received encrypted email. The other option is to show the sender, the third option to show also the subject of the message and the fourth option to show also the beginning of the message.
  - 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 send encrypted emails.
- Different kinds of UI customizations. For example, custom color templates, custom logo, custom graphics
- Localizations, for example language
- Adjusting the maximum size of attachments to the organization's needs. This is affected by the Android devices the organization is using as well as the email provider the organization is using.
- Other customer specific customizations

6. iOS Client

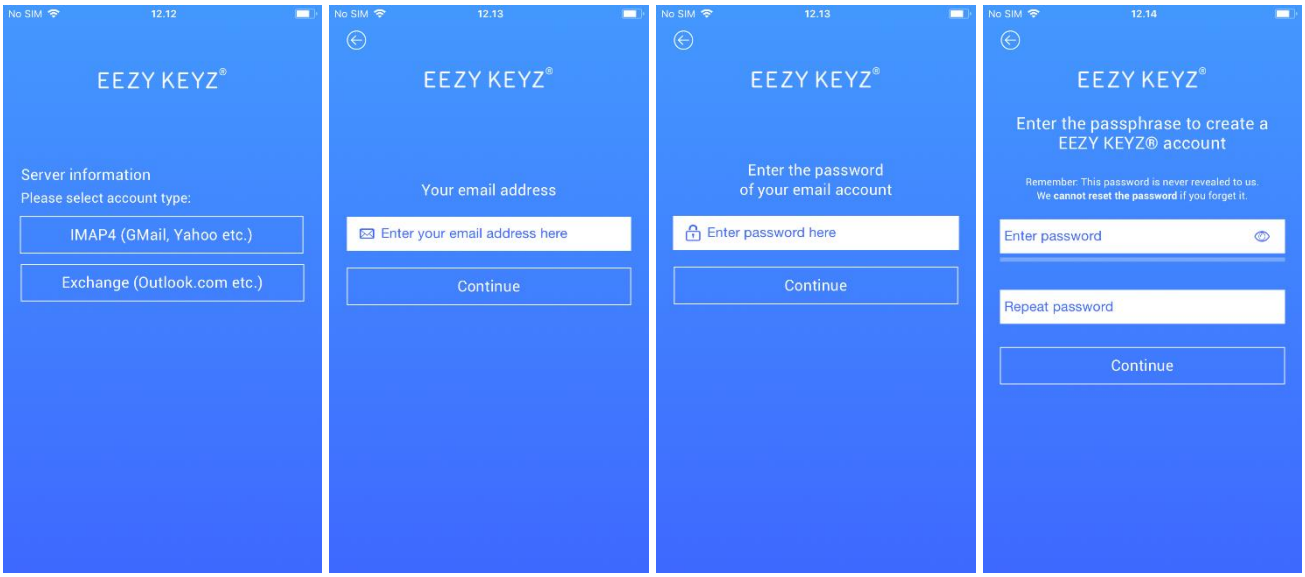
EEZY KEYZ® iOS application is a custom mobile email client application with all the usual features one would expect from an email application. The application uses strong encryption to protect the email messages and attachments. When composing email messages, the application automatically checks the 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 and digitally signed by default. The user-experience is completely seamless. The messages and attachments are also saved encrypted on both the devices and on the email server. The developed customer specific application will be delivered as desired by the customer.

EEZY KEYZ® iOS application default features:

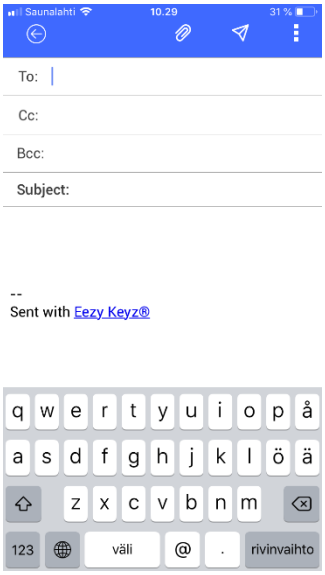
- Available for Apple iPhone and iPads running the iOS 9.0 operating system or later
- Supports IMAP and Exchange (EWS) email protocols
- The maximum size of attachments supported by the application is currently 10 MB
- Messages and attachments stored locally in an encrypted database
- English language
- Default EEZY KEYZ® User Interface
- Passphrase asked during initial login
- Warning messages displayed when sending unencrypted messages

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

The screenshots below show the default EEZY KEYZ® iOS client login process interfaces for a new unregistered user.



The screenshot below shows the default EEZY KEYZ® iOS client message composing interface.



iOS CLIENT TAILORING OPTIONS

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

- Customer-tailored iOS application can support different kinds of security levels as desired by the customer.
    - The intervals of inserting the passphrase while using the app or the PIN code can be adjusted. For example, the passphrase/PIN code could be asked every time an encrypted email is opened or only on the initial start of the application.

  - Notifications can be adjusted. For example, when receiving encrypted email the user is notified that he has received encrypted email. The other option is to show the sender, the third option to show also the subject of the message and the fourth option to show also the beginning of the message.
  - 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 send encrypted emails.
- Different kinds of UI customizations. For example, custom color templates, custom logo, custom graphics
- Localizations, for example language
- Adjusting the maximum size of attachments to the organization's needs. This is affected by the Android devices the organization is using as well as the email provider the organization is using.
- Other customer specific customizations

7. Outlook Add-In & Chrome/Firefox Browser Extensions

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

OUTLOOK ADD-IN

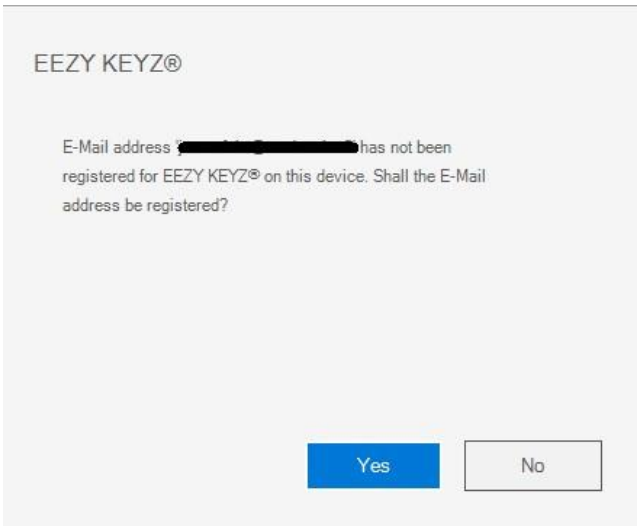
With the EEZY KEYZ® Add-In, Outlook can be used just as before. The only difference is that users can send messages and attachments that are protected using very strong end-to-end encryption to other EEZY KEYZ® users. It works with all email services. EEZY KEYZ® Add-In automatically handles the encryption process and key exchange between users. All messages to other users are automatically end-to-end encrypted and digitally signed by default. Emails and attachments saved in local folders and in the email provider's servers are also encrypted, to ensure that the email data remains protected at all times. The customer-tailored EEZY KEYZ® Outlook Add-In will be delivered as desired by the customer for example in .exe or .msi files.

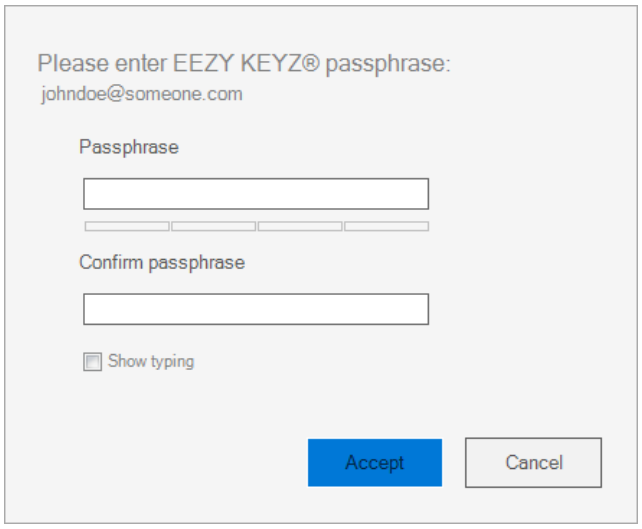
EEZY KEYZ® Outlook Add-In default features:

- Available for Windows 7 and Windows 10.
- Compatible with Microsoft Outlook 2010, 2013, 2016, 2019 and O365
- POP3, IMAP and Exchange email protocols supported
- All the same functionalities as Vanilla Outlook and the same user experience. Emails between EEZY KEYZ® users are automatically encrypted by default.
- The Outlook plugin supports attachments of up to 10 MB.
- Possible to choose to automatically decrypt incoming messages if required by the organization's policy. It is also possible to decrypt all messages if the customer decides to stop using the solution, or wants to periodically archive the messages in unencrypted format.

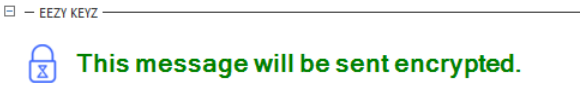
IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

The screenshots below show the default EEZY KEYZ® Outlook Add-In registering process interfaces for a new unregistered user.





User can choose if the email should be encrypted or not. By default, the email messages to other users are always sent encrypted.



OUTLOOK ADD-IN TAILORING OPTIONS

The tailoring options for the EEZY KEYZ® Outlook Add-In include e.g:

- Customer-tailored Outlook Add-In 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. For example, the passphrase/PIN code could be asked every time an encrypted email is opened or only on the initial start of the application.
    - 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 send encrypted emails.

- Different kinds of UI customizations. For example, custom color templates, custom logo, custom graphics
- Localizations, for example language
- Adjusting the maximum size of attachments to the organization's needs. This is affected by the Android devices the organization is using as well as the email provider the organization is using.
- Customizing how the Decrypt options are shown to the users. For example, some users have the option to decrypt emails while other users do not have these rights.
- Other customer specific customizations

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. For example, the passphrase/PIN code could be asked every time an encrypted email is opened or only on the initial start of the application, or when webmail is opened.
    - 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 send encrypted emails.
- Different kinds of UI customizations. For example, custom color templates, custom logo, custom graphics
- Localizations, for example language
- Adjusting the maximum size of attachments to the organization's needs. This is affected by the Android devices the organization is using as well as the email provider the organization is using.
- Other customer specific customizations

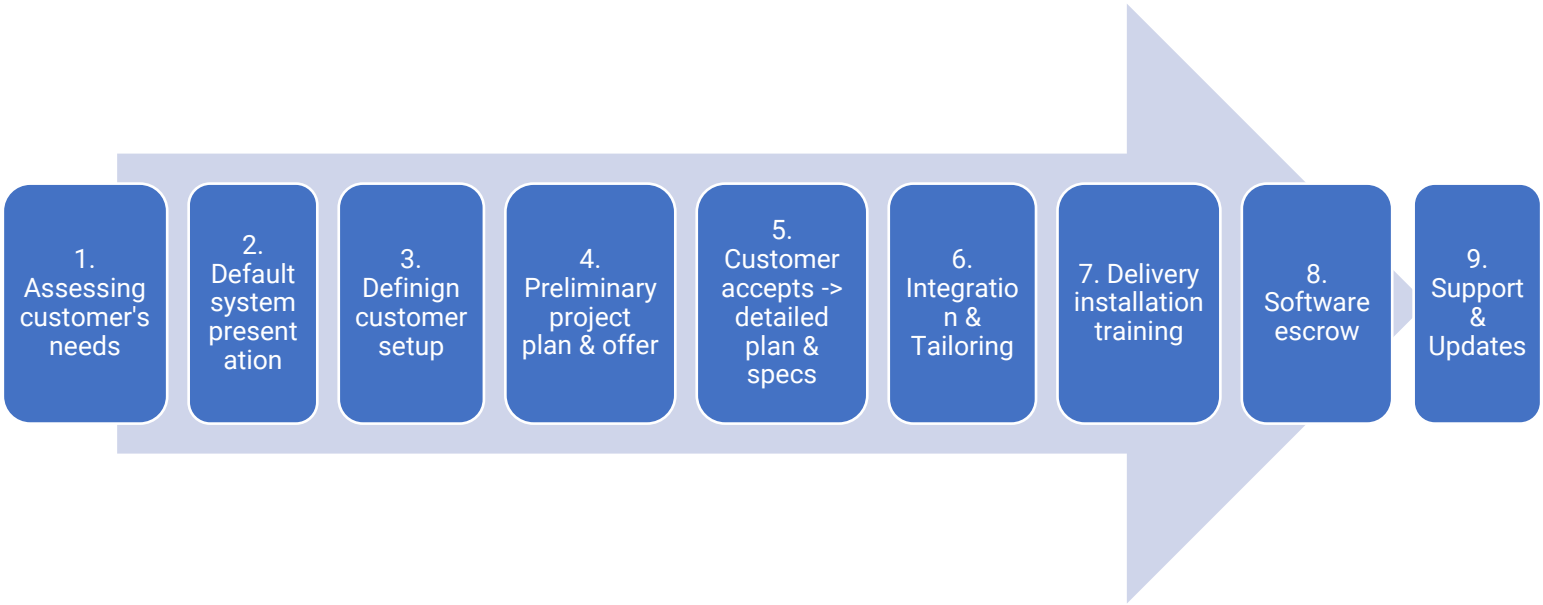
8. The Deployment Process

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.

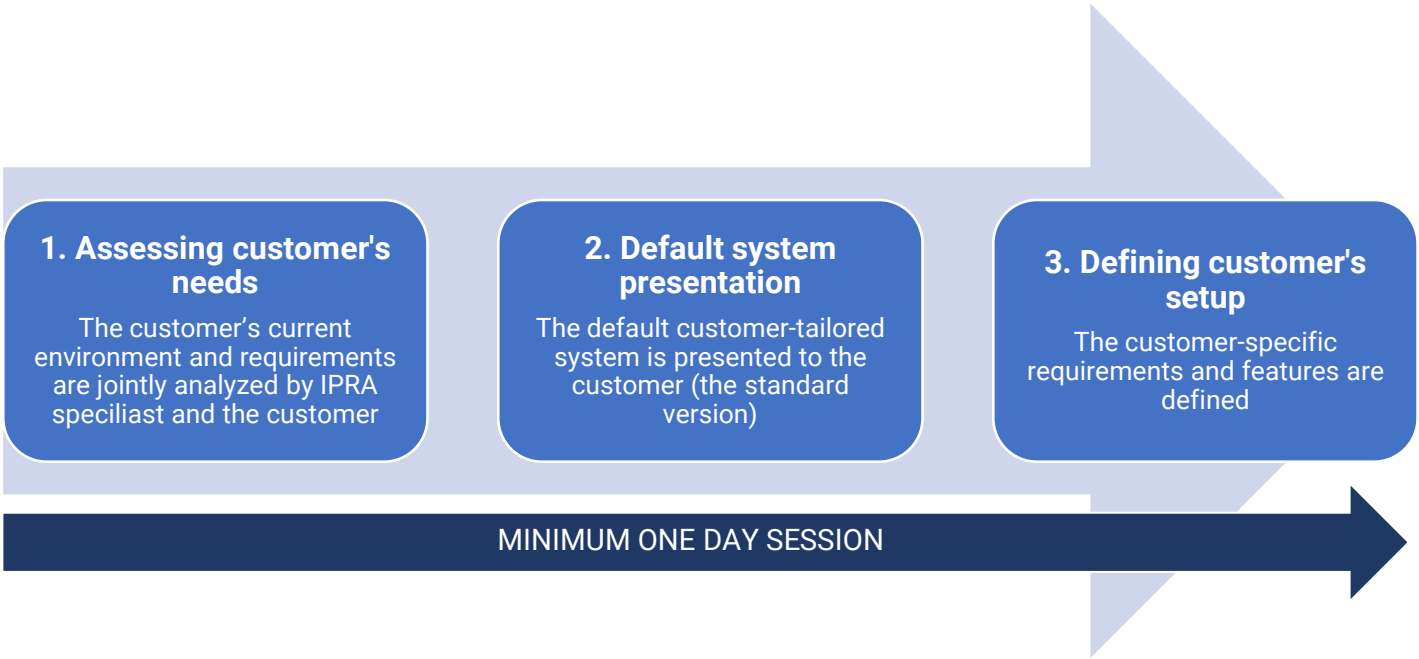
There are no special pre-requirements for the customer-tailored EEZY KEYZ® email encryption system project. However, the customer should be capable of hosting their own servers or alternatively be prepared in acquiring the server hosting service from a 3rd party. The customer-tailored backend system 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 tailorings
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.

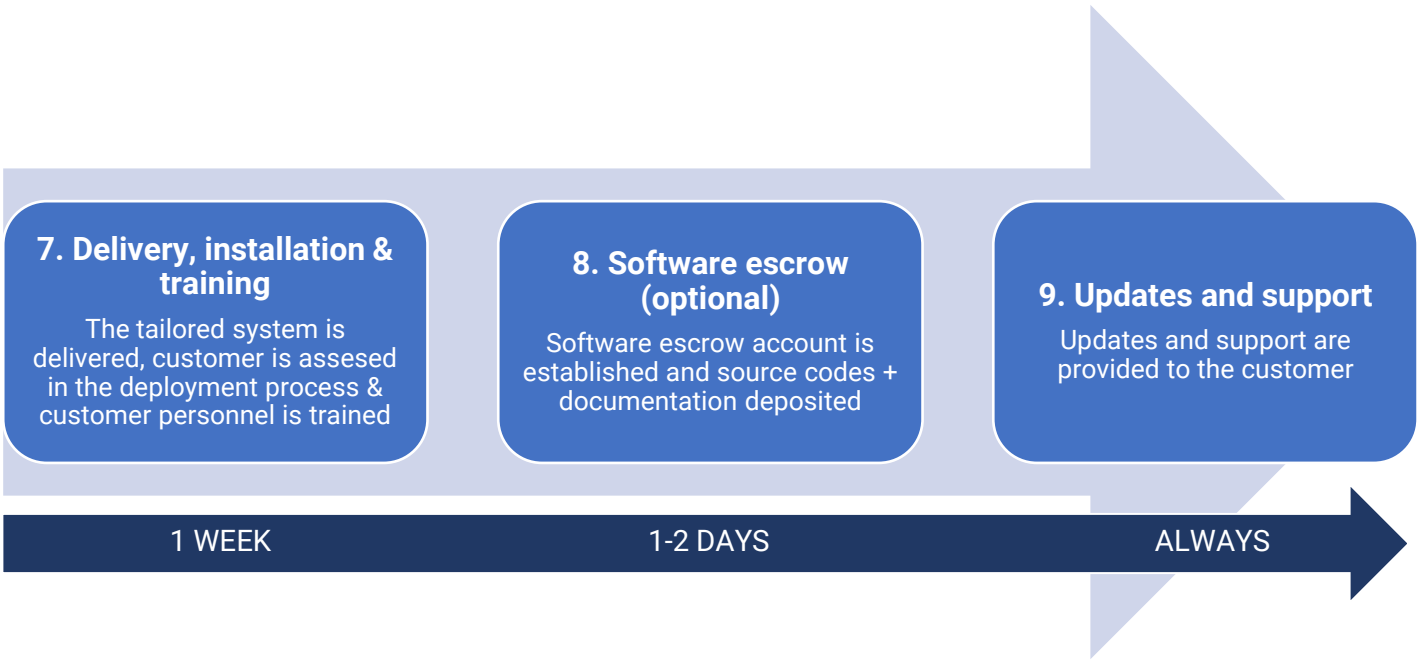
IPRA Technologies Ltd, Valtakatu 51, 53100 Lappeenranta, Finland.

TAILORING PROJECT

The actual tailoring process starts with creating a 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 scenarios (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

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)

Attachment 1. Pricing

The pricing of the customer-tailored EEZY KEYZ® email encryption system can be found in the separate attachment document 1. “Customer-Tailored EEZY KEYZ® Pricing”

Contact

IPRA Technologies Ltd Oy
Assi Group Vapaudenaukio
Valtakatu 51, 53100
Lappeenranta, Finland
sales@eezykeyz.fi

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