Soliton®

Protection Mechanisms of MailZen

All data within the MailZen Container is encrypted and separated from other data on the device. A whole range of measures are used to protect the information within MailZen. This includes the encryption of local data on the device, jailbreak protection and securing the communication with back-end systems.

Seperation of private and business data via container technology

The MailZen Container creates a segregated, secure area on the device. All corporate data within this container is encrypted and strictly separated from other apps on the device. No other application (e.g., Facebook, WhatsApp), system, or unauthorized person can access the data within the container; the data is further protected with a password. The container technology provides companies a secure and easy-to-use solution enabling employees to work remotely.

Local encryption

All data within the MailZen Container are encrypted (hybrid encryption with RSA up to 4096 Bit and AES-256) and protected with a PIN, password, or fingerprint.

Encryption in transit

Encryption of data in transit ensures that sensitive information is transmitted securely over any network. MailZen establishes a secure communication with the following backend systems:

- With MS ActiveSync or IBM Traveler servers via the ActiveSync protocol (TLS encryption)
- With the MailZen Management Portal via a web service interface (TLS encryption)
- Communication with the corporate network can be established via the MailZen Gateway

The gateway´s security relies on a key-based authentication and does not require a VPN Infrastructure or VPN profiles for mobile devices. The MailZen Gateway checks the user ‘s identity and provides access to verified users only.

End-to-End encryption with S/MIME and IBM Domino

In order to protect sensitive information MailZen can encrypt emails by applying the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. The email remains secure from access by third parties during its entire trajectory: from the moment it is sent, until it has been decrypted by the receiver and throughout all data links and servers. This ensures that only an authorized person can read the email and its attachments.

The S/MIME standard is applied for both encryption and decryption, as well as for signing and validating the signature in emails. This helps to secure against email phishing and identity theft. MailZen is also available for IBM Domino users. This eliminates the need for middleware or additional companion apps for S/MIME and IBM Notes encryption and decryption.

Certificate-Based authentication

In addition to TLS encryption, access to sensitive systems can be made more secure through activating certificate-based authentication. Access to the ActiveSync server or intranet applications can be configured so they require certificate-based authentication. This is a standard configuration setting for MailZen TLS-Gateway. MailZen checks the server certificate, the server checks the user certificate. The Client (MailZen App) and server perform a TLS handshake, in which the communication partners authenticate each other and agree on the cryptographic algorithms to be used. After the TLS channel is established, data can be transmitted in an encrypted format.

Central management via MailZen management portal

All security-related settings of MailZen can be centrally managed via its own Management Portal:

- User management
- Defining rules and settings for encryption
- Password policies
- Defining timeout periods, leading to an automatic log-out
- Remote reset of all company data within MailZen container in case of device loss
- Group management and configuration of different security policies for various user groups
- Granting access or blocking data interfaces between MailZen and the device
- Further security policies for working within the container (e.g. enabling or disabling functionalities like copy/paste, auto-complete, open-in or screenshots).

These policies help to ensure that the security requirements are met on all employees' mobile devices. All security-related functionalities can be correspondingly changed, depending on the desired configuration latitude and security level. If required, MailZen can be managed via an MDM solution.

Prevent manipulation

In order to secure data on mobile devices from manipulation, MailZen offers the possibility to quickly identify attacks and prevent access to MailZen.

- **Integrity check:** The MailZen integrity check provides full control over all MailZen versions, which users can use. Every version of the app has a fingerprint that is unique and enables the exact identification of the software. This ensures that only the versions of MailZen authorised by the company can be set up and used.
- **Jailbreak detection:** Jailbreaking modifies the device's operating system and can turn off the security mechanisms of the device. This way a user or an app can get root privileges and have full access to the operating system of the device. Manipulated devices can be detected in the MailZen Management Portal. The usage of the MailZen app and the container are then blocked.

Interested in reading more? Download the security white paper on MailZen here >

Soliton®
Want to learn more about our solutions? Contact us at: emea@solitonsystems.com | www.solitonsystems.com