Mail Manager

Mail Manager
Encryption and Security

Introduction

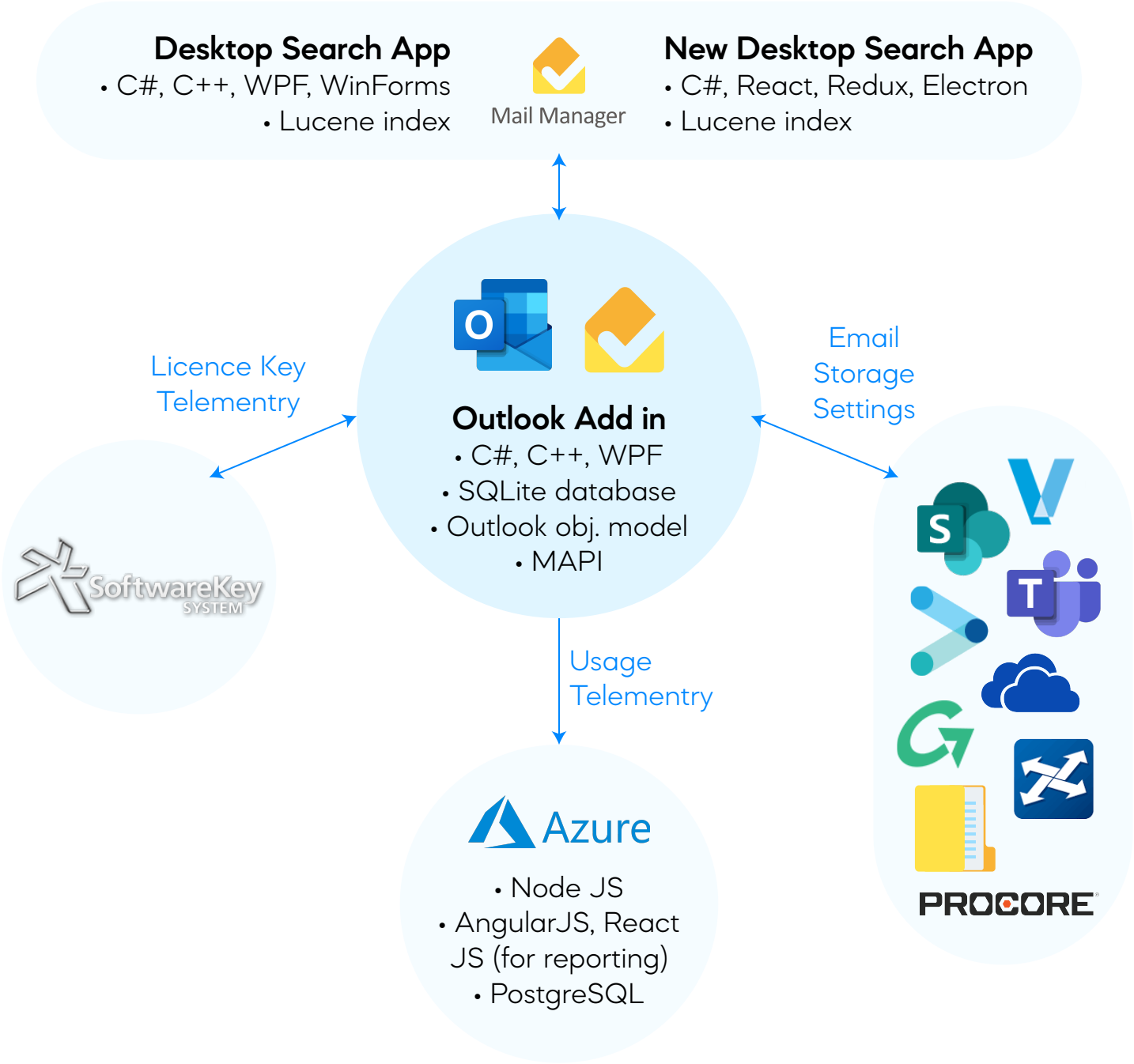
This document sets out the architecture of Mail Manager, highlighting encryption and personal data storage.

The product's architecture can be split between the desktop product and the mobile apps and web add-in, so you will see there are two sections in this document.

In a separate section, you will see detail on Mail Manager's storage of personal data.

Desktop Product

Architecture



Storage at Rest

Data and settings are stored on the local PC in the registry, in configuration files and in local databases that control the state of the filing process – i.e. for managing the queue for filing emails and holding the list of filing locations. It is assumed that local disk encryption in place according to customers' policies will protect this data.

User setting data is also stored in a personal OneDrive folder. This data is encrypted when synchronised with Microsoft's servers and is in the geographic region associated with the customer's 365 organisation.

Emails are stored in a local folder cache before being filed and are retained in that cache for off-line working. Local disk encryption will protect these files.

The encryption state of emails in their ultimate storage location is within the control of our customers. In the case of the Microsoft suite of storage (SharePoint, OneDrive, and Teams), this data is encrypted and is in the geographic region associated with the customer's 365 organisation.

Licence count data and customer names are stored on SoftwareKey's system in an encrypted state. This data is stored in North America.

No state data or emails are stored on the Mail Manager Azure cloud, and hence the question of storage encryption is not applicable.

Usage data or "telemetry" sent by the user's client machines is stored in an encrypted Azure PostgreSQL database. This data is stored in Azure Europe North (Ireland). We are planning a project to migrate this to Azure UK South (London, England) at the time of writing.

Data in Transit

Emails copied from the PC to the ultimate windows folder storage are encrypted based on the customer systems in use.

Emails transferred to cloud storage systems, e.g., SharePoint, OneDrive, Teams, and our other third-party cloud storage partners, are encrypted in transit using HTTPS. The location of these end points depends upon the system concerned. The Microsoft suite of storage is in the geographic region associated with the customer's 365 organisation.

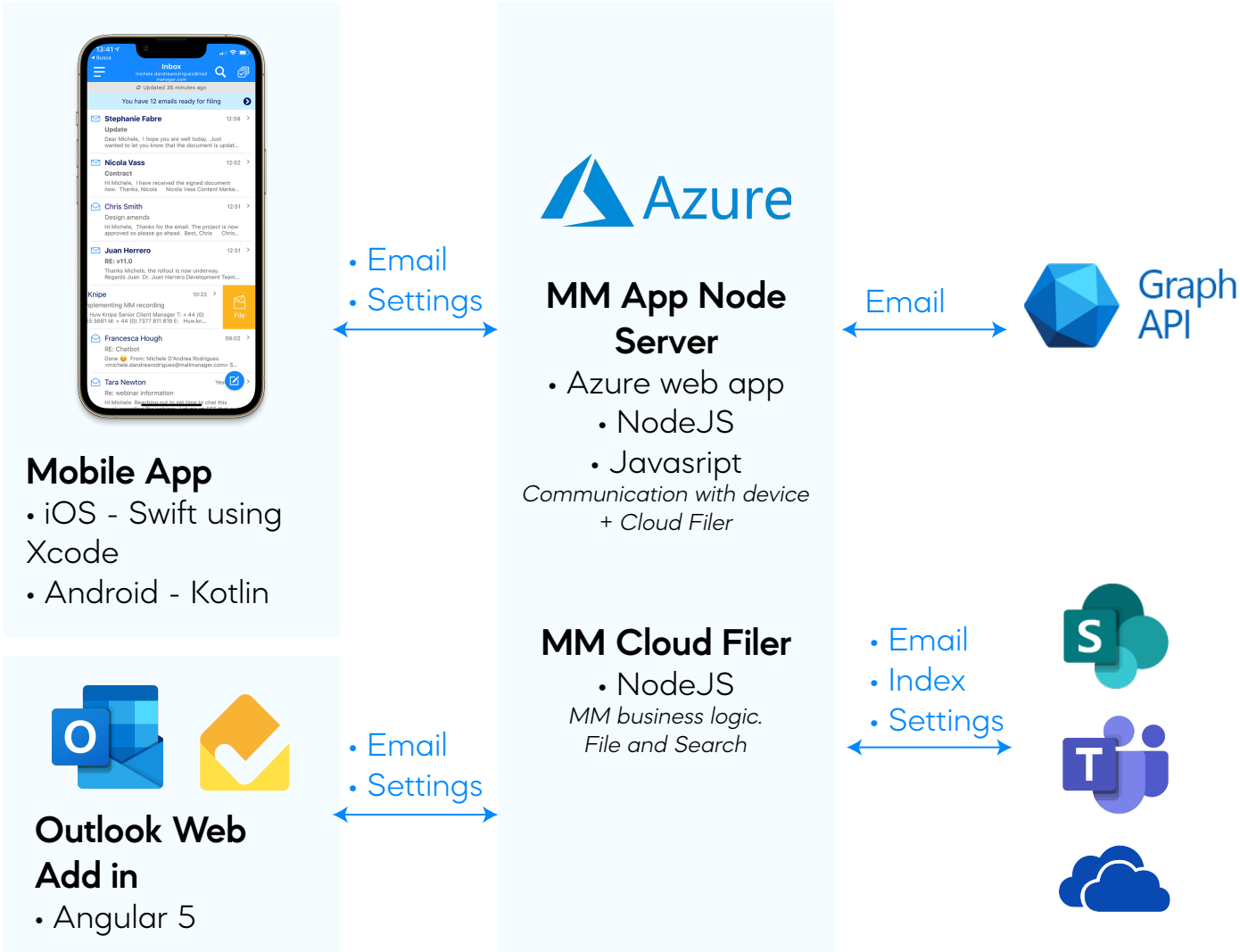
All cloud data storage operations, whether to the Mail Manager Azure cloud or SoftwareKey's systems, are encrypted using HTTPS.

The Mail Manager product end points are in UK South. We have some end points currently located in Australia to provide the latest version of the software to companies close to that location.

The SoftwareKey end points are in North America

Mobile Apps and Web Add-In

Architecture



Storage at Rest

No data is stored in this process on either the Mail Manager Azure cloud servers or the Microsoft cloud providing the Graph APIs.

Emails are stored only in their ultimate location, which is in the control of our clients. Again, the Microsoft suite of storage (SharePoint, OneDrive, and Teams) is encrypted and stored based on the setting in the customer's 365 organisation.

Data In Transit

Emails are retrieved by the mobile apps using an encrypted connection to the MS Graph API over HTTPS.

Emails transferred to cloud storage systems, e.g., SharePoint, OneDrive, Teams, are encrypted in transit using HTTPS. The Microsoft end points, are in the geographic region associated with the customer's 365 organisation.

All cloud data storage operations to the Mail Manager Azure cloud are encrypted using HTTPS.

The Mail Manager Azure end points are in the UK South Azure location (which is in London at the time of writing).

Data	Storage	Location	Encryption at Rest	Encryption in Transit
Desktop Settings and Data	Local PC	Local PC	Customer Policy	N/a
Shared Settings	Personal OneDrive	Customer 365 location	Yes	Yes
Cached Emails	Local PC	Local PC	Customer Policy	N/a
Stored Emails	Network Folders	Customer Network	Customer Policy	Customer Policy
	MS365 (SharePoint, OneDrive, Teams)	Customer 365 location	Yes	Yes
	Other systems	Depends upon system	Depends upon system	Depends upon system
Licence Data	SoftwareKey systems	North America	Yes	Yes
Mail Manager Usage Data	Azure PostgreSQL	Azure Europe North (Ireland)	Yes	Yes
Mail Manager Cloud Traffic	N/a	Azure UK South (London)	N/a	Yes
MS Graph API	N/a	N/a	N/a	Yes

Mail Manager

Personal Data

Emails contain personal data, and these are stored in a local cache folder on the PC in the user's profile as well as in the ultimate storage location. No interim storage of emails is undertaken when using the mobile apps or the web add-in. The emails, in this case, are transferred directly to their ultimate storage location.

No personal data is stored on the SoftwareKey licence system.

By default, no personal data is stored in the usage data that we gather (aka usage telemetry). User email addresses and device names are stored in an encrypted form that cannot be decrypted (by Mail Manager or any party).

If the customer grants permission to gather user email addresses and device names in the usage data, then these are sent in an encrypted form (Base64) that can be decrypted by any party. Note that this data is encrypted in transit and stored in a secure location only accessible to Mail Manager staff.

No other personal data is stored while using Mail Manager.