EBF Contacts Security Whitepaper

17/11/2023
public
version 1.5

VERSION	DATE	EDITOR	CHANGES
1.0	28/09/2022	Thomas Klütsch	First version
1.1	11/10/2022	Thomas Klütsch	Change document classification, move ISO certificate to first chapter
1.2	24/03/2023	Thomas Klütsch	Hubspot support
1.3	30/05/2023	Thomas Klütsch	Android support
1.4	25/08/2023	Thomas Klütsch	Added organizational contacts permission
1.5	17/11/2023	Thomas Klütsch	Support for CSV/JSON import

Table of Contents

01. General

This Whitepaper provides information about the EBF Contacts application focusing on security related aspects of the infrastructure, data processing and communication.

EBF GmbH is ISO 27001 certified. The certification is proof that EBF invests sufficiently in information and IT security, protect confidential data sufficiently against misuse, attacks, loss and disclosure and that we guarantee high availability of IT systems at the same time.

Certificate

Standard ISO/IEC 27001:2013

Certificate Registr. No. 01 153 1800745

Certificate Holder:

EBF

EBF-EDV Beratung Föllmer GmbH
Gustav-Heinemann-Ufer 120-122
50968 Köln
Germany

Scope: Consulting, development, implementation, hosting and support services for the Digital Workplace and relevant Enterprise Mobility Technologies

Statement of Applicability (SoA): dated 09.03.2022

Proof has been furnished by means of an audit that the requirements of ISO/IEC 27001:2013 are met.

Validity: The certificate is valid from 2022-06-21 until 2025-06-20.

2022-05-05

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

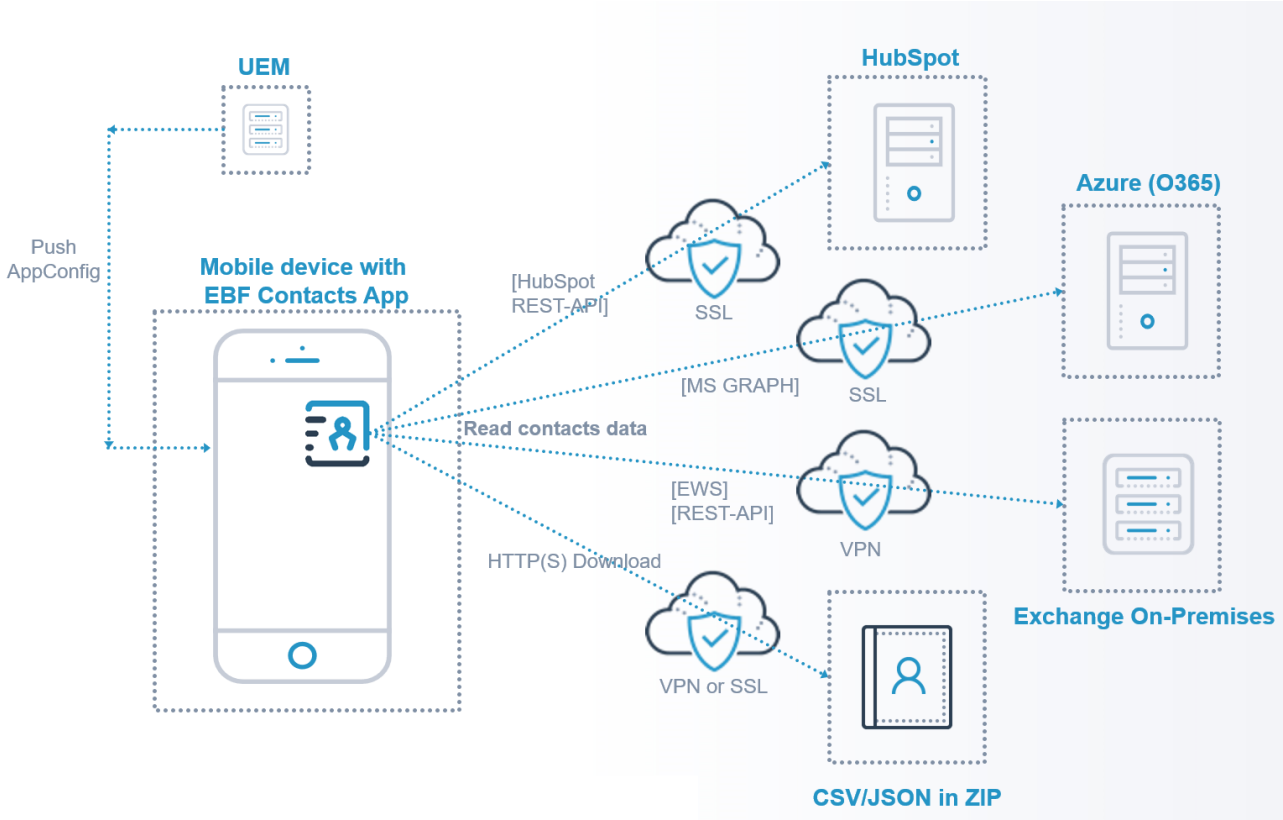
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Precisely Right.

02. System Architecture

The following picture gives an overview of the EBF Contacts app and communication flows:



03. Authentication and permissions

EBF Contacts allows user authentication via basic authentication and NTLM to Exchange On-Premises instance. For authentication to Exchange Cloud (O365) modern authentication (OAuth) is used. Users use their personal credentials for login.

On-Premises users need to have permission to access EWS (Exchange Web Services).

For Exchange Cloud (O365) an Azure Application ID needs to be created by the customer and provided to the application via parameter. Regarding Application ID mandatory permissions, all of type „delegated“ are:

- Contacts.Read
- User.Read
- User.ReadBasic.All
- User.Read.All

The Application ID may also require optional permissions, if filtering of contact data or additional endpoints/sources on reading from the Exchange instance is required (depending on configuration of the app):

- Group.Read.All (if you want to use the parameter „selectedGroups“)
- OrgContact.Read.All (if you want to use the parameter “readOrganizationContacts”)

The user performs a login with his personal O365 credentials.

For HubSpot a “private application” needs to be created in the HubSpot admin panel granting read access to contact data (crm.objects.contacts.read). A login to HubSpot with user credentials in EBF Contacts is not necessary.

For CSV/JSON data source the ZIP file can be encrypted using ZipCrypto. The password needs to be provided via AppConfig so EBF Contacts can decrypt the ZIP after downloading.

For Android the admin needs to make sure a browser app is installed in the device’s Work Profile to allow EBF Contacts to open a web view internally for the user to login to O365.

04. Data handling

EBF Contacts reads and stores contacts data from the customer’s Exchange/Hubspot instance on the device encrypted to have them available in offline scenarios. Contacts data will never be written back to the customer’s data source (readonly).

04.1. iOS

Contacts data is made available to the iOS phone app via official iOS CallDirectoryExtension interface to allow for identifying callers on incoming calls and show caller information in the calls list of iOS. No other applications have access to EBF Contacts data pool and data cannot be changed on the device.

04.2. Android

For Android devices EBF Contacts will store the contact data also in the system's contacts DB to allow for caller identification on incoming calls. The admin must make sure EBF Contacts is installed and used in an Android Enterprise Work Profile only to avoid leaking data to other unmanaged apps.

In the system's contact DB the user can change contact data but this is not intended because on next synchronization EBF Contacts will overwrite the data again.

Contacts data will be kept in the Work Profile also after uninstallation of EBF Contacts. To remove the contacts completely an admin either needs to remove the Work Profile or - before uninstall - the user must take the manual step of "Logout" from EBF Contacts to clean the system contact DB.

04.3. Personal data being stored

The EBF Contacts application stores contacts data on the device using encryption also containing the following personal data fields from Exchange:

- id
- displayName
- mail
- givenName
- surname
- userPrincipalName
- businessPhones (list of numbers)
- mobilePhone

Also, photos of contacts are stored encrypted on the device and shown in the application. This feature can be deactivated by the administrator on defining the EBF Contacts application parameters.

04.4. Data storage duration

Personal data is stored as long as the application is installed on the user's device. Data is deleted on uninstallation of the application for iOS.

For Android the user needs to do a manual logout from the App before uninstallation or the admin can remove the Work Profile from the device to force removing contact data completely.

05. Data transfer

A customer may need to implement a VPN solution on the device to secure access to the Exchange On-Premises server or a downloadable ZIP file. It is recommended to use an UEM system's VPN solution in that case.

For Exchange Cloud (O365) data transfer is secured by TLS (SSL) encryption.

For HubSpot data transfer is secured by TLS (SSL) encryption.

For CSV/JSON (ZIP file) data transfer is secured by TLS (SSL) encryption.

06. Data encryption

The EBF Contacts application is running in a sandbox (iOS) or in the work profile (Android). The configuration enforces encryption of data on the device until the user opens the device and authenticates himself. This is standard behavior of iOS. For Android the user explicitly needs to activate the Work Profile to get access to EBF Contacts.

Additionally, EBF Contacts encrypts the contacts data with a user defined encryption key with AES256. The user needs to enter this encryption key on every start of the application. For more comfort the user can also choose to use Touch-ID or Face-ID for login if available.

Encrypted data will be deleted if a user enters a wrong encryption key ten times in a row. Also, encrypted data will be deleted on logout from the application.

07. External APIs

Communication with related Microsoft Exchange instances and Hubspot is done using the official APIs. REST communication always uses port 443. SOAP-API ports may vary.

API	API TYPE
Exchange Webservice (EWS) (for Exchange On-Premises)	SOAP
Exchange REST-API (for Exchange On-Premises only when activating access to private address book)	REST
Microsoft Graph API (for Exchange Cloud O365)	REST
HubSpot API	REST

08. Logging

The EBF Contacts app stores a rolling logfile on the device containing information about error messages. The log files are kept for ten days and do not contain any personal data.