EBF Files
Security Whitepaper

17/10/2023
public
version 0.9

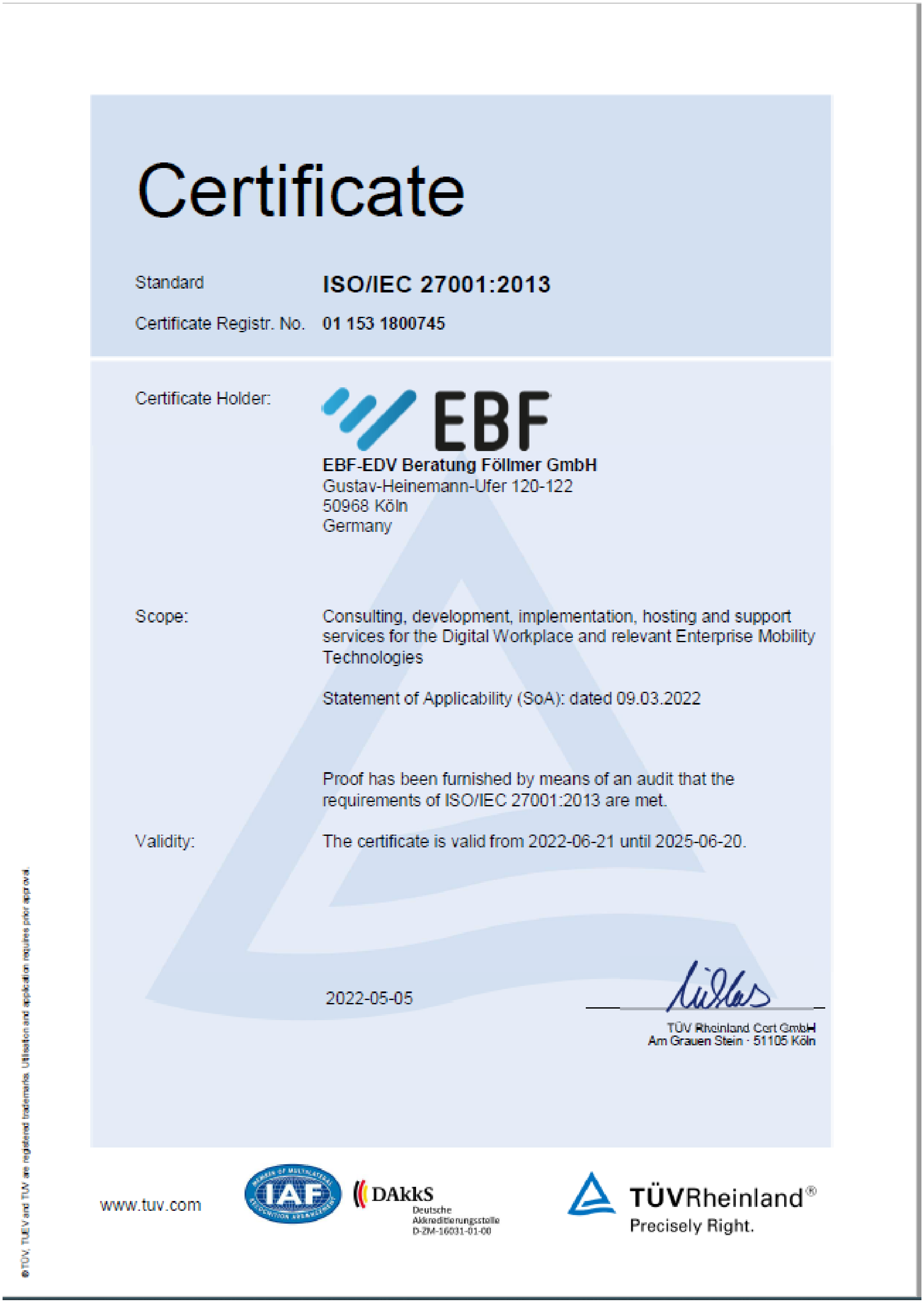
VERSION	DATE	EDITOR	CHANGES
1.0	13/12/2023	Thomas Klütsch	First version

Table of Contents

01. General

This Whitepaper provides information about the EBF Files 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

IAF

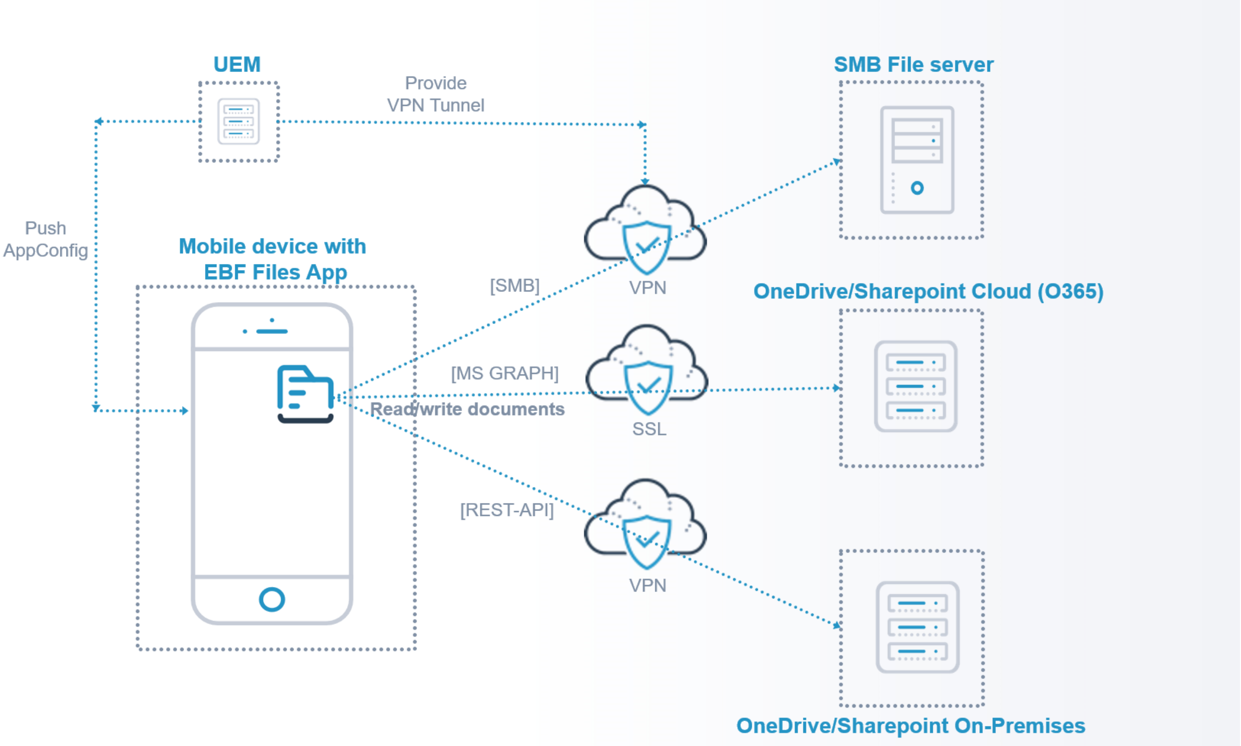
DAkkS
Deutsche
Akkreditierungsstelle
D-ZM-16031-01-00

TÜVRheinland®
Precisely Right.

© TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

02. System Architecture

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



03. Authentication and permissions

EBF Files allows user authentication via NTLM and Kerberos (SSOExtension by Ivanti) to Sharepoint and OneDrive4Business On-Premises instance. For authentication to Sharepoint Cloud (O365) modern authentication (OAuth) is used. Users use their personal credentials for login.

For authentication to SMB files shares NTLM must be used.

For OneDrive/Sharepoint 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
- Directory.AccessAsUser.All
- Directory.Read.All
- Files.Read
- Files.Read.All
- Files.ReadWrite
- Files.ReadWrite.All
- Group.Read.All
- GroupMember.Read.All
- People.Read
- People.Read.All
- User.Read
- User.Read.All
- User.ReadBasic.All
- Sites.FullControl.All
- Sites.Manage.All
- Sites.Read.All
- SitesReadWrite.All

The user performs a login with his personal O365 credentials.

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

04. Data handling

EBF Files reads and stores documents from the customer's OneDrive/Sharepoint and SMB file share instance on the device encrypted to have them available in offline scenarios. Changes to documents will be written back to the server after closing the internal document editor.
No other applications have access to EBF Files document pool. Data sharing can be de-/activated by the administrator per data source (container) to allow e.g., for sending documents via email attachments.

05. Personal data stored and storage duration

The EBF Files application stores documents from customer data sources on the device using encryption. Customer's documents may contain personal data.

Additionally, EBF Files stores and uses credentials for some data sources (OneDrive and Sharepoint On-Premises, SMB) to automate the login process.

Stored personal data include the following:

- Usernames for data sources
- Device-ID for office editor licensing

Credentials and documents are stored as long as the application is installed on the user's device. Data is deleted on uninstallation of the application. The user can delete all locally stored data by using the "Logout" button in the application's settings screen.

06. Data transfer

A customer may need to implement a VPN solution on the device to secure access to their On-Premises servers (OneDrive, Sharepoint and SMB file shares). It is recommended to use an UEM system's VPN solution in that case. If connecting to an SMB file share the app allows for using SMB3.0 which brings additional transport encryption on protocol level.

For OneDrive/Sharepoint Cloud (O365) data transfer is secured by TLS (SSL) encryption.

07. Data encryption

The EBF Files application is running in a sandbox (iOS) or in the work profile (Android) in managed environments. 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 Files.

Additionally, EBF Files encrypts the local 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 on uninstallation of the application. Also, encrypted data will be deleted on logout from the application.

08. External APIs and protocols

Communication with related Microsoft OneDrive and Sharepoint instances is done using the official APIs. REST communication always uses port 443. SMB protocol requires port 445.

DATA SOURCE TYPE	API / PROTOCOL	API TYPE / VERSIONS
OneDrive On-Premise	Sharepoint REST-API	REST
Sharepoint On-Premise	Sharepoint REST-API	REST
OneDrive Cloud (O365)	Microsoft Graph API	REST
Sharepoint Cloud (O365)	Microsoft Graph API	REST
SMB file share	SMB	SMB 2.x, SMB 3.0

09. Logging

The EBF Files 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. Logging can be deactivated completely by an admin.