Technical Documentation

empower® express architecture and security

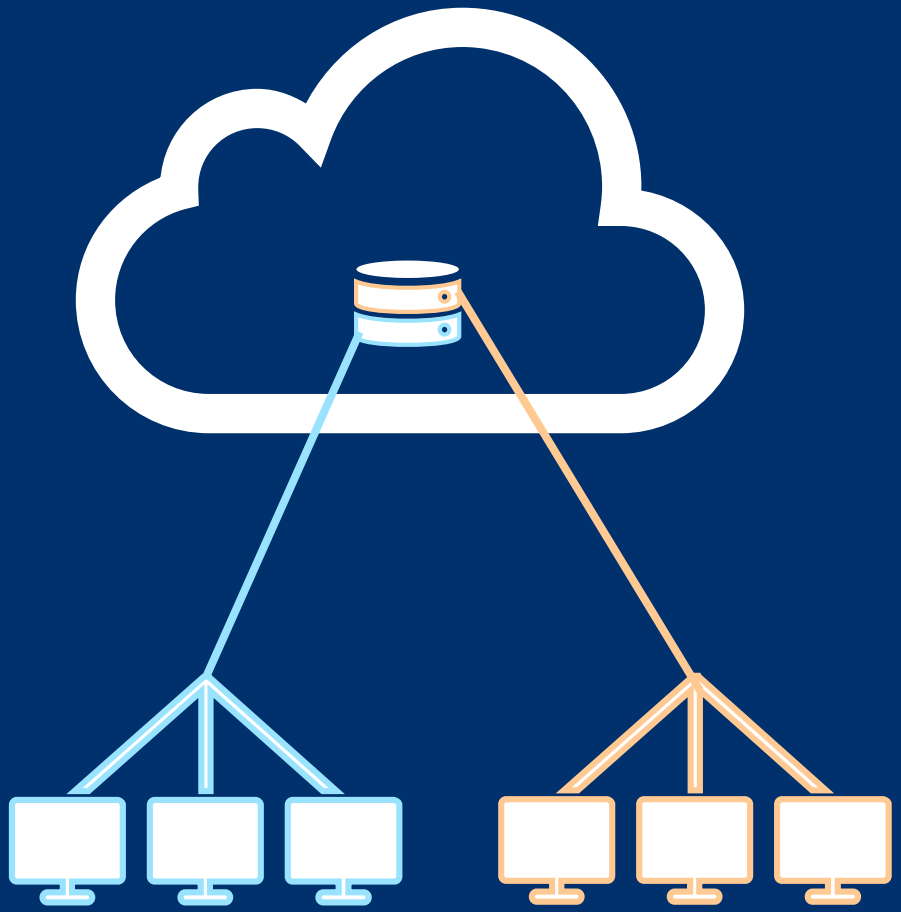
01

Introduction

IT Overview

empower® express is a software solution consisting of a cloud-based backend as well as several frontend applications (depending on the selected subscription). The empower express backend is a multi-tenant environment where each client has its own storage area that is isolated from other clients.

The frontend applications include (depending on the selected subscription) add-ins for Microsoft Office® on Windows or macOS, an offline synchronisation application used alongside the add-ins, as well as an additional web application.



empower® Client Applications

Client Installation Package

You get an exe (for Windows) / pkg (for macOS) installer package that can be installed by the user(s) or also through a software deployment system in a per user context. An MSI installer for PC is also available on request.

Update-Frequency & Auto-Updates

We release new versions of empower® 2-4 times per year. The software includes an auto updater component so that the software is updated automatically.

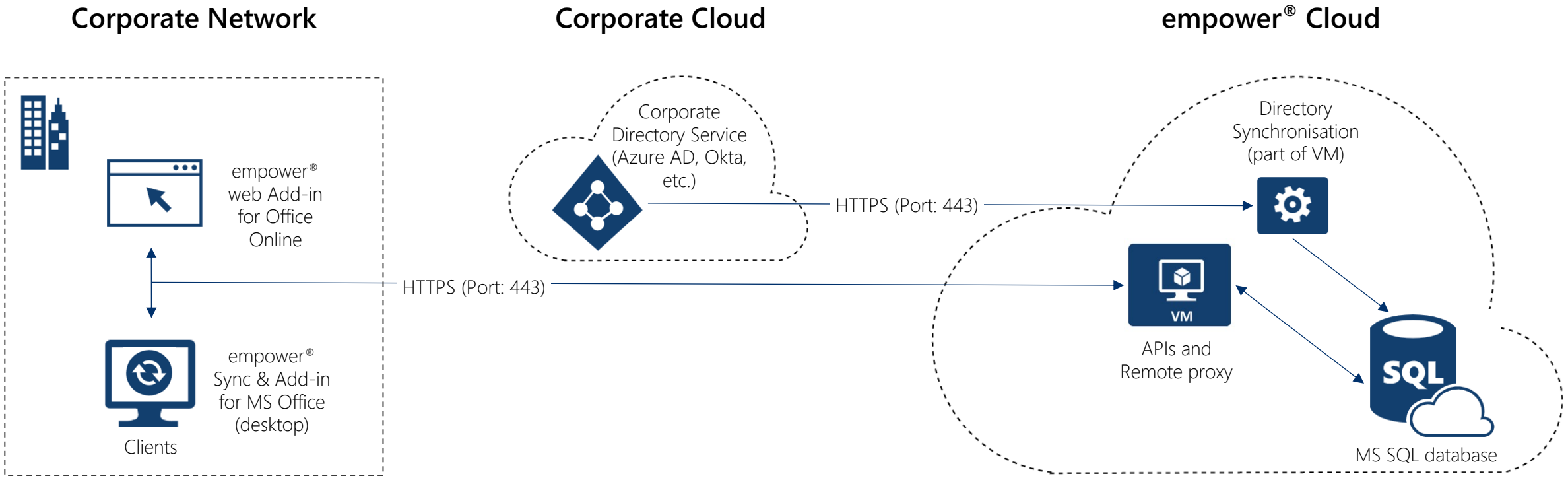
Web App

Web App can be accessed via any web browser allowing access to empower content even without access to PowerPoint (not relevant for the charts-only subscription).

02 Architecture

empower® Architecture (empower® Cloud)

(not relevant for the charts-only supscription)



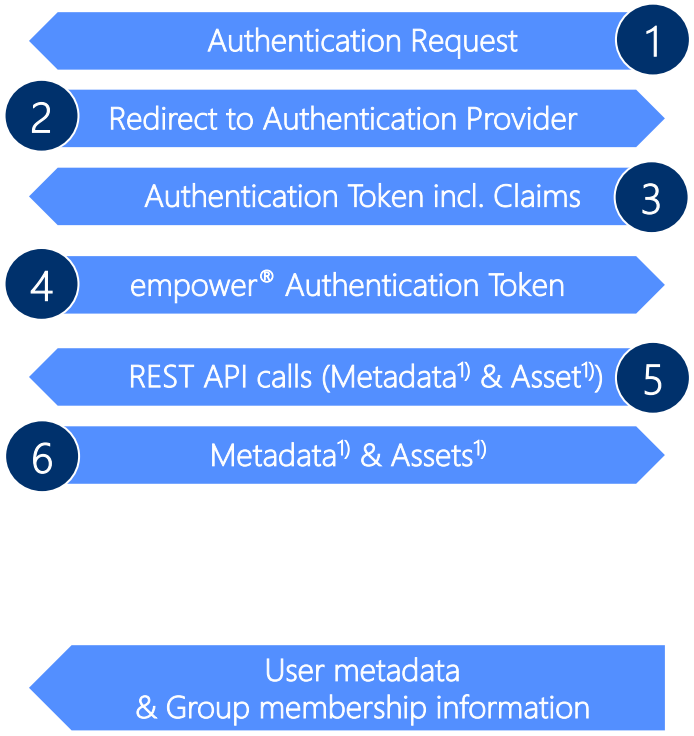
empower® Data Flow Diagram

(not relevant for the charts-only supscription)

empower® Backend

Hosted as a multi-tenant SaaS in the empower® Cloud based on Microsoft Azure

- Database (MS SQL Server)
  (primary asset and metadata storage)
- Backup
- empower® backend Web Services (REST APIs)
  (local filesystem cache for assets and in-memory cache for metadata)
- empower® Directory Sync
- Reverse Proxy (traefik)



All traffic is encrypted in transit (https (TLS) on port 443)

Customer Device Infrastructure

Windows or macOS-based devices
for desktop applications

- Microsoft Office® COM Add-Ins
  (local filesystem cache for all metadata accessible to current user and all offline-available assets)
- empower® Web App

Customer Identity Infrastructure

Hosting in Microsoft Azure's Cloud environment

- Identity Provider (Azure AD)

1) *Assets are uploaded content files, i.e. data files theoretically usable without empower® (Presentations, Documents, Images, etc.);*
Metadata is all structured data stored in empower®, e.g. element information (element author last modified date, …), folder structure, permission information, user data, etc.

03

Data Flow by Component

Data Flow by Component: empower® Backend

(not relevant for the charts-only supscription)

Type
Windows services hosted in the cloud on a Windows Server

Context
empower® Azure Subscription (cloud-hosted)

Type of Data	Direction	Protocol/port	Encrypted transfer/storage	Storage
User Profile Data & Identity Provider UIDs	In- / Outbound[1)]	HTTPS 443	yes/yes	SQL Server
Identity Provider Claims	Inbound	HTTPS 443	yes/yes	SQL Server
empower® REST API Requests	Inbound	HTTPS 443	yes/yes	SQL Server/n/a
Content (Metadata)	In- / Outbound	HTTPS 443	yes/yes	SQL Server
Content (Assets)	In- / Outbound	HTTPS 443	yes/yes	SQL Server, cached on AppServer
LetsEncrypt automatic certificate provisioning (optional)	In- / Outbound	HTTPS 443	yes/no	Application Server

1) Some user profile data is synchronized to clients for user-related functionality (user search, permission management, etc.).

Data Flow by Component: empower® Desktop Add-Ins

(not relevant for the charts-only supscription)

Type
COM-based add-Ins for the desktop versions of Microsoft Office® on Windows and macOS, including an out-of-process offline sync and data access application ("empower® sync")

Context
Customer-owned desktop devices

Type of Data	Direction	Protocol/port	Encrypted transfer/storage	Storage
Authentication Flow (Kerberos, NTLM or web-based)	In- / Outbound	HTTPS 443	yes/yes	Windows Credential Store, macOS Keychain
empower® REST API Requests	Outbound	HTTPS 443	yes/n/a	n/a
User Profile Data & empower® UIDs	Inbound	HTTPS 443	yes/partially	Device Storage
Content (Metadata)	In- / Outbound	HTTPS 443	yes/no	Device Storage
Content (Assets)	In- / Outbound	HTTPS 443	yes/no	Device Storage

04 Data Protection (GDPR) & Security

Security in the Azure based empower® Cloud

How secure is the empower® express Cloud?

- The empower® Cloud is based on the Microsoft Azure platform using the latest technologies and security standards to keep all client data safe.
- Each client has its own (isolated) space within the cloud based library and all client data is processed and stored solely in Microsoft Azure Data Centers within the EU.
- All content in the cloud is only accessible by secure authentication.
- All data that enters and leaves the cloud is transferred using TLS (*Transport Layer Security*) technology.
- All data that is stored in the cloud is encrypted at rest. And all data is backed up within the Azure cloud and region.

Who can access your data at empower®?

- Admins of Right Aligned (UK based) have access to client data to optimize client PPT templates and assign folder permissions.
- Very few technical empower admins also have access to the empower® cloud in order to perform important maintenance and support tasks. Microsoft admins have theoretical access as well.
- Right Aligned and empower take strong measures to help protect all client data from inappropriate access or use by unauthorized persons.
- All access by empower admins is protected via MFA and is logged.

How secure is the Microsoft Azure cloud?

- Microsoft has extremely high security standards and many security related certificates (as outlined on the next slide).
- It is very likely that your organization already approved the use of Microsoft Online Services which makes it easier to get internal approval for the empower® cloud.
- For further details on Microsoft Azure security, please visit the Microsoft Azure Trustcenter.

Azure global compliance

Microsoft Azure

The following compliance standards apply globally

CIS Benchmark | CSA-STAR attestation | CSA-STAR certification | CSA-STAR self-assessment
ISO 20000-1:2011 | ISO 22301 | ISO 27001 | ISO 27017 | ISO 27018 | ISO 27701 | ISO 9001
PCI DSS | SOC | WCAG | CDSA | PCI DSS | Shared Assessments | TruSight

Azure regions

Azure has more global regions than any other cloud provider—offering the scale needed to bring applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers.

over 60 regions worldwide

140 available in 140 countries

- Available region
- Announced region
- Availability zones

empower® Activation

empower® uses a built-in software activation to ensure that all users in your company are properly licensed. The activation works as follows:

- Each client (PC) activates itself against the empower® activation server in predefined intervals, e.g. every 30 days. A user can have multiple devices, but this is only counted as one license.
- The following information is stored on our activation server: SID (Active Directory ID), login name, product, version number, activation date of license, expiration date of license.
- If a client does not reactivate itself after one interval, the license will be freed up from the overall license volume. This way, it is no problem when employees leave the firm and new people can reuse these licenses.
- If the license volume is exhausted, the next client that tries to activate itself will receive a message that there are no more licenses available. In that scenario, please contact us to lease additional licenses.

Encryption

Encryption of data in transit

All flow of data between the client (the empower sync and add-ins on Windows and macOS or the web library and Teams bot) happens over an encrypted HTTPS connection. This includes authentication as well as the up- and download of all content data.

Encryption of data at rest

When hosted on-premise or in your own cloud environment, empower does not enforce any specific kind of encryption at rest. Any measures for *transparently* encrypting data at rest available withing your infrastructure (e.g. disk encryption) should be compatible with empower®.

When hosted in our empower cloud, all data is encrypted at rest using the database-level Service-Managed Transparent Data Encryption1 for the database and Azure Disk Encryption2 for the application server(s).

All encryption at rest happens at the database- or application server-level. empower currently does not support column-level encryption or bring-your-own key encryption scenarios. Because of the way the empower® backend works (e.g. transparently indexing, splitting and merging content data), these are technically not feasible or, if implemented, would not offer any additional security.

1 https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview

2 https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows


empower