CAPEXinsights
CAPITAL PROJECT DELIVERY MADE BETTER

Technical Factsheet

Overview

CAPEXinsights is a Project and Portfolio Management Software as a Service .NET Core Web Application hosted on the Azure Platform. An instance is comprised of a Net Core Web application presenting a single page application (SPA) based CRUD interface.

Data is stored in an Azure SQL database, making use of the temporal tables feature to allow full history tracking. Azure Storage enables users to upload files and documents, with Azure functions used for background processing. A second web application integrates to Microsoft Office for the Web so that users can view and edit documents online.

CAPEXinsights surfaces data through detailed dashboards through Power BI Embedded. Each instance comes with a standard set of dashboards and depending on the customer's requirements, additional customised dashboards can also be deployed.

Identity management and authentication is handled by Azure Active Directory (AAD), accessed using OpenID Connect. Authorisation is managed by the application and supports granularity down to a per project level.

Application lifecycle management (Planning, Source Code, Builds, Testing, Release Management) is managed through Azure DevOps.

Azure Application Insights is used for monitoring of performance metrics and logging faults.

Application Profiles

There are two user groups defined at the AAD application permission level:

- Administrator – users that can update system settings and configure supporting data taxonomies such as pick lists and document templates.
- Contributor – all other users with CRUD (Create, Read, Update, Delete) rights.

User permissions are further managed in the solution by administrators in a more granular way using the following permission levels:

- Full Control – can create new permission groups and manage custom permissions for a project.
- Edit – can create, read, update, and delete data.
- Read – can read data only, cannot create, update, or delete.

An open security model is applied. All authorised users are granted edit rights to all projects, except those projects for which permissions have been customised.

A full history is retained in the database as to the permissions changes that are applied to each project over time, as well as changes to group membership and access rights.

Organizational Access

The set of users who have access to CAPEXinsights is controlled by the customer's AAD management team.

CAPEXinsights uses Microsoft Azure's Application Gateway configured with Web Application Firewall V2 to provide a centralised protection from common exploits and vulnerabilities. Furthermore, CAPEXinsights Azure SQL Servers are configured to block access to the public endpoint to the server. Only Azure services/resources and specified Beca IP addresses have access to the server, and its databases.

Beca limits which of its own staff can access customer data. Beca staff that have access to customer data must complete work instructions and training on confidentiality and privacy.

Security and protection to access customer data is also managed through Azure Key Vault. This stores sensitive system configuration settings for application environments. A feature in Azure Key Vault gives Beca control over who has access to it and to what information.

All Beca staff use individual credentials to access the code base and customer data.

CAPEXinsights is hosted as a SaaS web-based solution and requires a modern browser to use. It integrates with AAD for Single Sign-On (SSO) and is hosted securely in Azure.

Password Policies

With the use of a customer's AAD, CAPEXinsights aligns to the customer's password policies.

Session Settings

CAPEXinsights uses the Microsoft identity platform for authentication. When a user authenticates with the Microsoft identity platform, SSO session is created with the user's browser and the Microsoft identity platform. The SSO session token is not bound specifically to CAPEXinsights.

The Microsoft identity platform uses two kinds of SSO session tokens: persistent and non-persistent. Non-persistent session tokens have a lifetime of 24 hours (these are destroyed when the browser is closed). Persistent tokens have a lifetime of 90 days. Anytime a SSO session

token is used within its validity period, the validity period is extended another 24 hours for non-persistent tokens or 90 days for persistent tokens.

If a SSO session token is not used within its validity period, it is considered expired and is no longer accepted.

Files

Files are stored in a private container in Azure Blob storage. There is no direct access to blob storage for any users. Access is only available via the web app. Files are encrypted at rest.

Database

The database is an Azure SQL database. It is only accessible via the web app and limited through IP address range restrictions in Azure. SQL data is encrypted at rest.

Business Continuity and Recovery

CAPEXinsights utilizes several Azure features to enable data backups, redundancy, failovers, and recovery.

CAPEXinsights Azure SQL Databases are backed up using Azures database platforms backup capability. CAPEXinsights Azure Storage Accounts are also backed up to a different storage account. All backups are backed up to another Azure Availability Zone within the Region it operates.

Authentication

The CAPEXinsights Web Application uses OpenID Connect to authenticate the current user. OpenID Connect is an identity layer that is built on top of the OAuth 2.0 protocol. This allows CAPEXinsights to verify the identity of the End-User based on the authentication performed by a configured authorization server.

CAPEXinsights uses its own credentials to access Power BI Embedded. Power BI Embedded is used for reporting purposes only. Access is secured through OpenID Connect in the same manner as the web application.

All web traffic is encrypted through TLS.

The authentication flow for project CAPEXinsights uses OpenID Connect, as depicted in the diagram below.

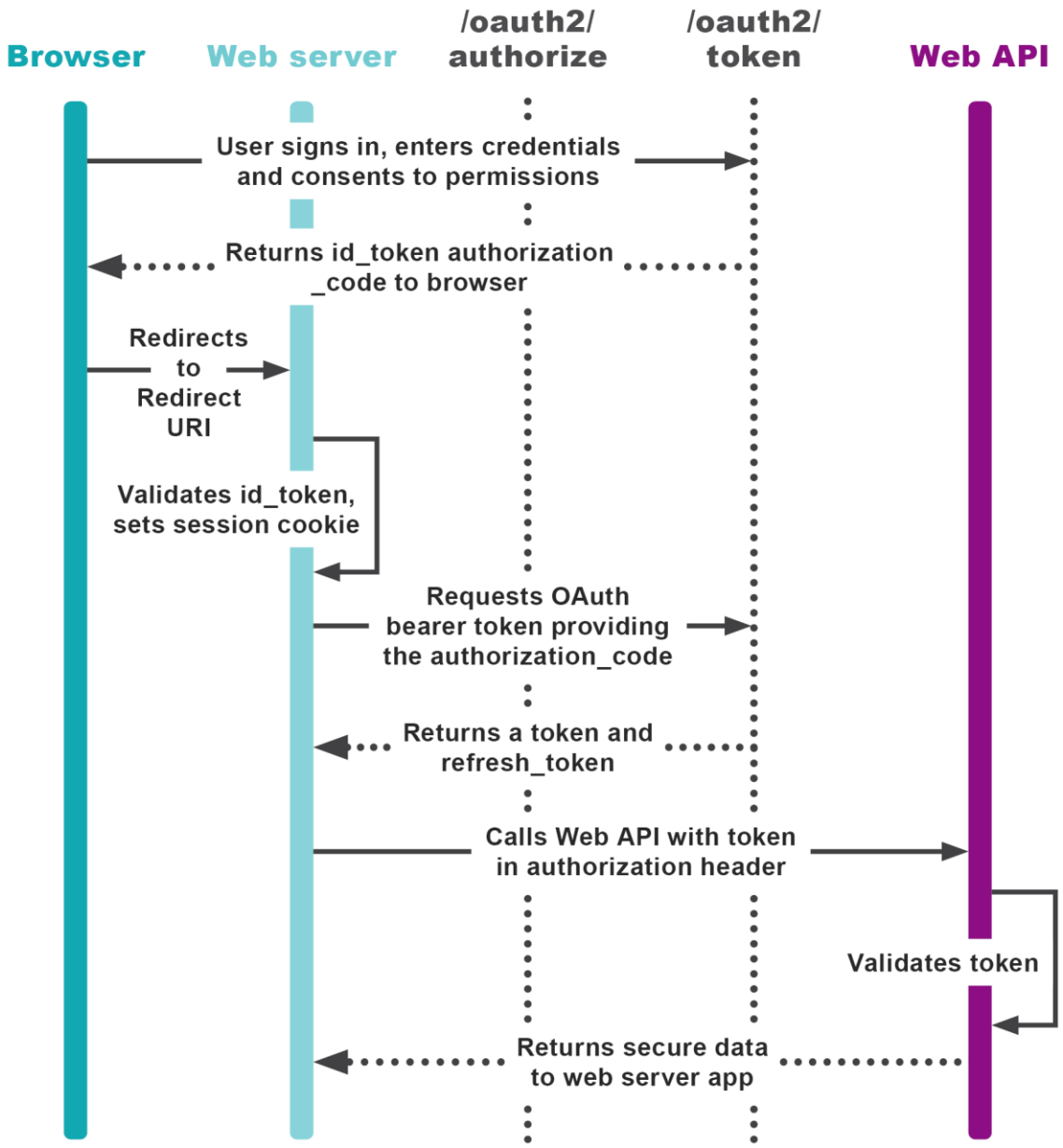

Figure 1 - OpenID Flow

The system can retrieve user roles (e.g., Admin) from AAD if configured by the customers AAD administrators.

Application Structure

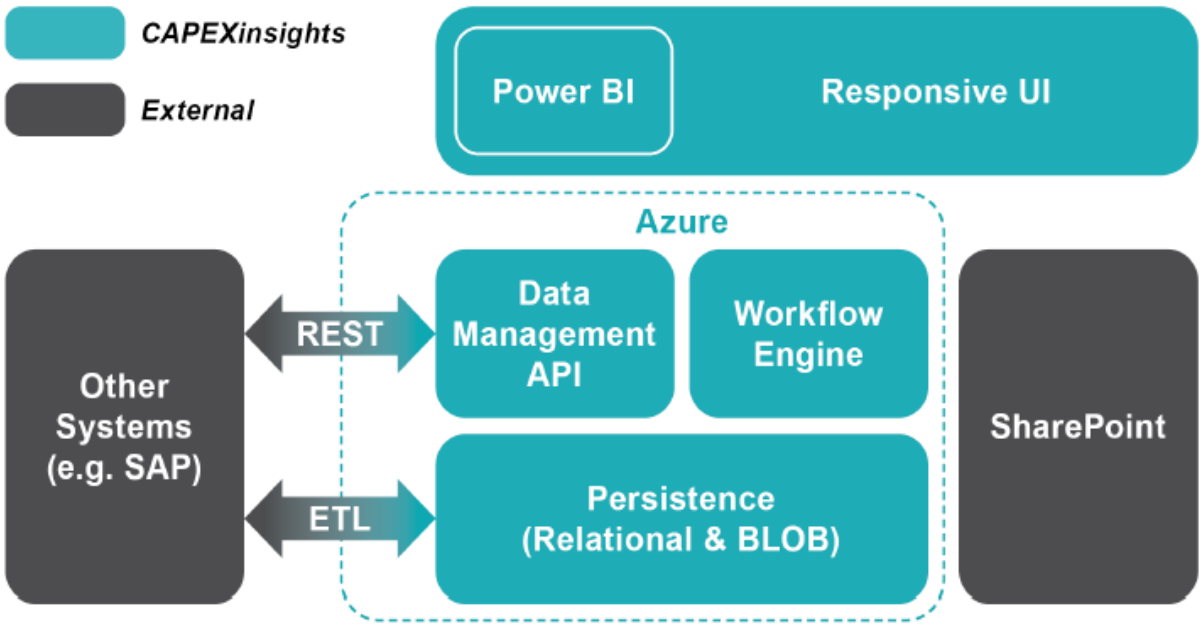

Figure 2 – Application Structure

Integration Methods

CAPEXinsights can be readily integrated with other applications.

Broadly, there are three categories of integration: manual, batch and automated. Beca recommends that initial system integrations take a staged approach. Starting with a manual approach to integration. Manual integration is simple, sufficiently robust for the initial phases of integration while all parties become familiar with the behaviour and technicalities of the systems involved and presents good value.

As an understanding of the data improves, data quality improves, data formats and standardisation become better, and integration governance is established, then we can consider a more sophisticated form of system integration. For clarity, a description of the three categories of integration is provided below.

Manual

The manual approach is useful at the beginning of system integrations where the data quality, quantity and format are uncertain or unfamiliar.

The manual approach is the simplest. The customer's team will manually provide Beca with data, in an agreed format and location, to ingest into CAPEXinsights as required and Beca will

upload this data load through a programmatic approach. This is usually done by following an ETL (Extract, Translate, Load) process. Going through the ETL process will provide the foundation for both parties to define the data format and standards required to enforce data quality. Generally, this method supports low frequency data transfers – typically monthly.

Batched

A batch integration approach is generally adopted after data quality, formats and governance processes are established through a more manual integration method.

Beca will set-up an automated system which receives data from the customer. The customer can provide that data using an automated approach themselves or manually. CAPEXinsights will then automatically process the data into the application at the required frequency.

While this remains a relatively low-cost integration approach, the data needs to be at a certain level of quality and in an agreed format so that it can be processed automatically, as not to generate too many errors. Generally, this method supports medium frequency data transfers – typically weekly or monthly.

Automated

An automated approach is where there is little to no human interaction with data being transferred between the integrated systems. This is achieved when data quality, data formats and standards and governance processes are established.

The customer's system(s) and CAPEXinsights are integrated with industry standard compliant data endpoints and connected through middleware.

If data quality, data formats, data standards and governance processes are already established prior to the customer systems and CAPEXinsights integration then going through the manual or batched phases may not be necessary.

The automated approach is the preferred long-term approach; however, it is important that the process for data sharing is mature, well tested and understood. Generally, this method supports high frequency data transfers – typically hourly or daily.

Solution Landscape

Integration between applications involved in capital project and portfolio delivery is critical. Integration creates transparency and makes it easier for people to deliver better capital project outcomes.

There are several applications where it is beneficial to apply these integrations. These are summarised in the following figure and listed in typical order of priority. Each customer is

different and may have a different priority and different application landscapes. Beca can work with each customer to integrate and configure CAPEXinsights to suit their business.

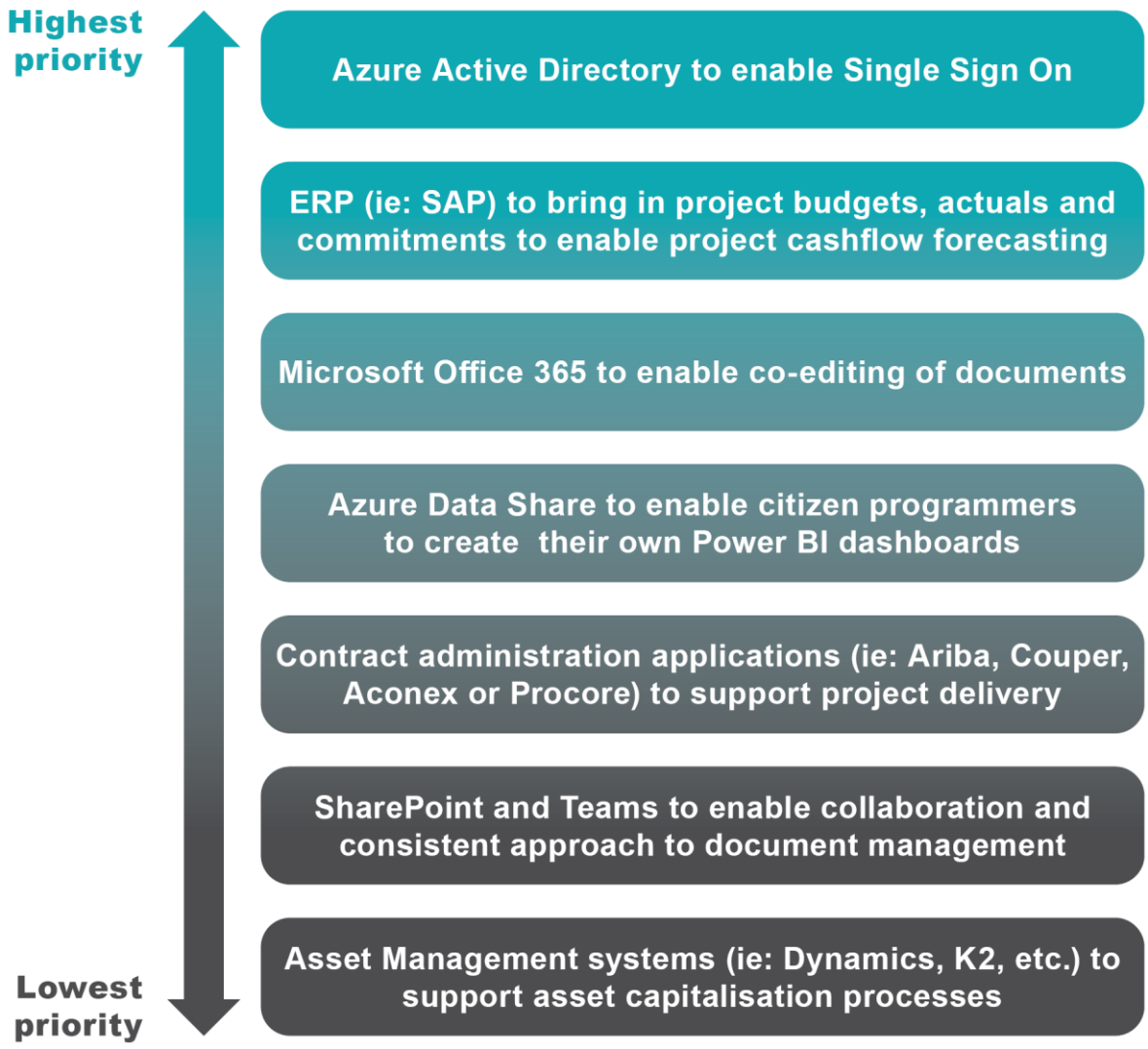

Figure 3 – Typical order of priority for system integration

General Architecture

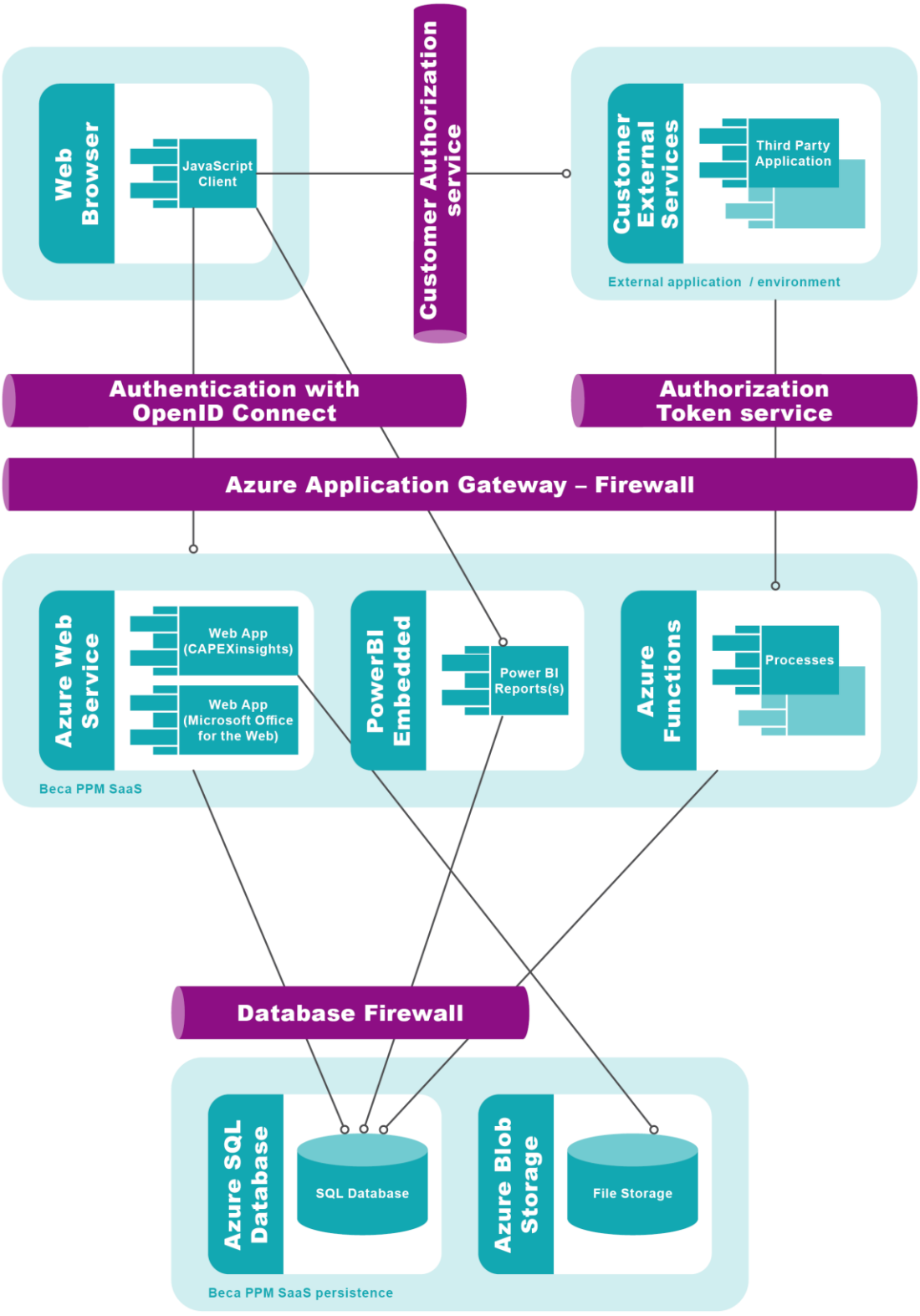

Figure 4 – Architecture