



SPFx App Technical Documentation

BPA Solutions

October 2022

1. BPA Applications on Office 365/SharePoint

BPA Apps (Quality, Medical, CRM, App Builder) are SharePoint apps to be installed in the client Office 365 environment, and developed with the SharePoint Framework (SPFx) technology.

2. Architecture Overview

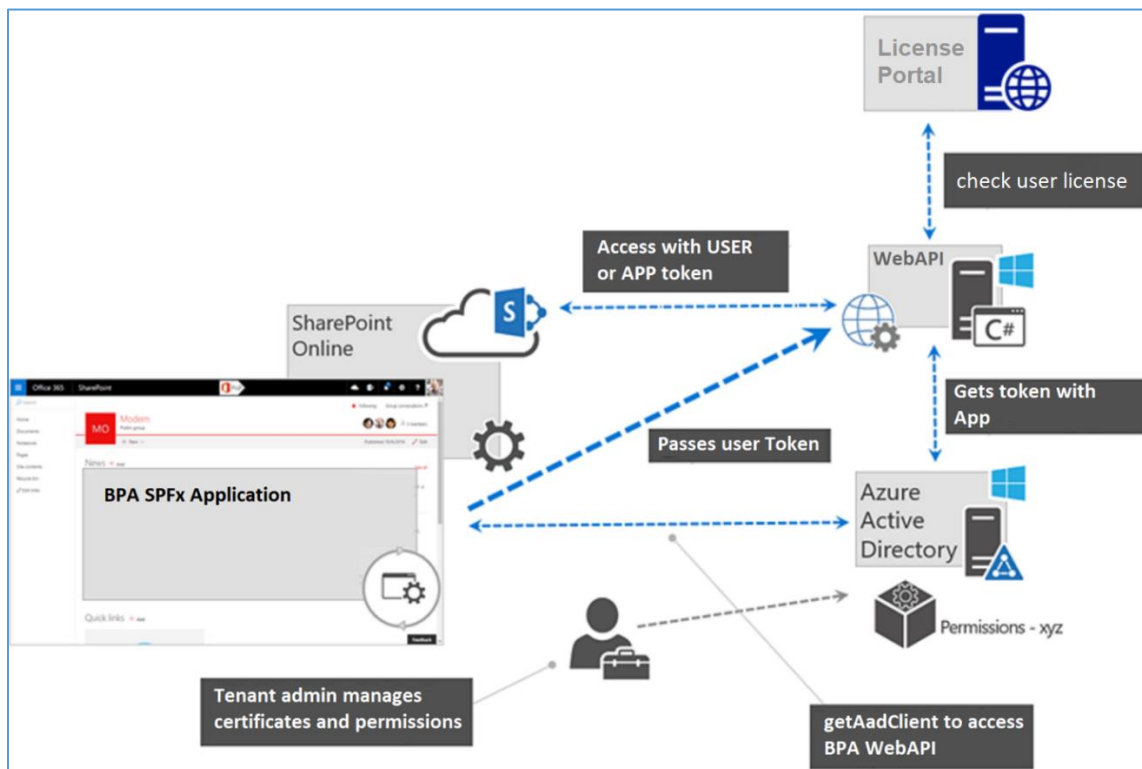
BPA SPFx applications are divided in 2 subcomponents:

- SPFx webparts, interacting with users, working with the permission token given by the current user session. Webparts are installed by the app in the client environment. SPFx active part is hosted in CDNs and only a non-changing part hosted in App Catalog. So, updates (usually monthly) can be done without to update all clients' sites.
- A multi-tenant WebAPI called by the SPFx client and interacting with SharePoint, using
 - the user token for operations to execute with user's permissions
 - the app token obtained thru an ACS client id/secret or an Azure Active Directory (AAD) secret for operations the user isn't allowed to execute. The clientsecret can be encrypted on the server.

The WebAPI runs in a Microsoft Azure environment maintained by BPA. Software updates are periodically done by BPA on the Azure backend with no impact on clients data and app configurations.

The WebAPI is used for:

- user actions with high level permissions
- remote event receivers like field replications when an item is created/updated
- batch actions



BPA SPFx Apps architecture scheme.

All communications between the systems are done under HTTPS protocol (WebAPI, License Portal, SharePoint Online, AAD).

Client Data Security

Data is stored in regular Microsoft SharePoint lists and libraries, in the client Office 365 environment. **BPA doesn't host any client data.** SharePoint security and protection apply and are fully respected.

All SharePoint features like versioning, recycle bin and backup/restore are fully available.

No client data is stored outside of SharePoint:

- No client data is stored in the BPA Azure server (WebAPI)
- No client data is stored in the BPA SPFx application
- No user password is stored anywhere

SharePoint and application permissions are under control of the client tenant administrator.

If requested, the client can host his own WebAPI server inside his own Azure tenant. In this case, the client is responsible to manage BPA software updates.

Main application components

BPA Application includes a variety of components. They change in each version with the new components or features. Here is a fair status end of 20201:

- On the SPFx client side
 - SPFx Webparts to CRWD data from SP lists. Current webparts are BPA MasterDetail, BPA DataViewer, BPA Form, BPA MailMerge, BPA eSignature and some BPA settings functions.
 - SPFx Extensions (e.g. to display the BPA Navigation)
 - One Client Side webpart to insert a client id/secret into SP to allow the WEBAPI to access to SP data without a user token. The installation indicates the requested permissions and asks for trust. Access by client id/secret can be changed to a AAD Permission file on custom WEBAPI server.
 - All the SPFx actions are done only with the current user Permission.
- On the WEBAPI side, one program
 - Serving information to itself and to the SPFx client about the site DDL (Data Definition Language) list the list of lists, their content types, views and fields
 - Answering to Sharepoint Remote Event Receivers (RER) (like OnUpdated event set up by BPA Reminder or BPA Fields Replication) and CRWD data from SP lists according to the task to achieve
 - Running batches, e.g. for Reminders or MailMerge.
 - Depending on the function to achieve, the action can be run with current user permission (with the SP token sent by SPFx) or with the App level permissions (e.g. RER or batches).

All data transfers are done under HTTPS protocol.

BPA Application Security

BPA SPFx applications can only execute SharePoint operations the current user token allows. When BPA WebAPI receives a request from a SPFx client, it

- checks for a user token in the request
- checks the token allows minimal access to the current SharePoint site
- works with SharePoint with the current user token (and with current user permissions) for most of the operations
- works with SharePoint with the rights given by the tenant administrator approved for high level operations or batch operations (batches, remote event receivers)

High level operation examples:

- Managing BPA settings lists
- Creating lists/Content types/Views/Columns
- Creating PDF via Graph

BPA application architecture was validated by a Microsoft MVP expert.

Azure Environment Security

The WebAPI runs in a Microsoft Azure environment maintained by BPA. This environment is protected by MFA for restricted administrators with restricted port access. State of the art security systems are in place. Backups are periodically done and prepared for high availability in case of issues.

3. BPA Application Permissions

The app needs the described below permissions to work normally, which is fully standard for such an add-in. Installation has to be performed by a Tenant Global Administrator to be able to grant all requested permissions.

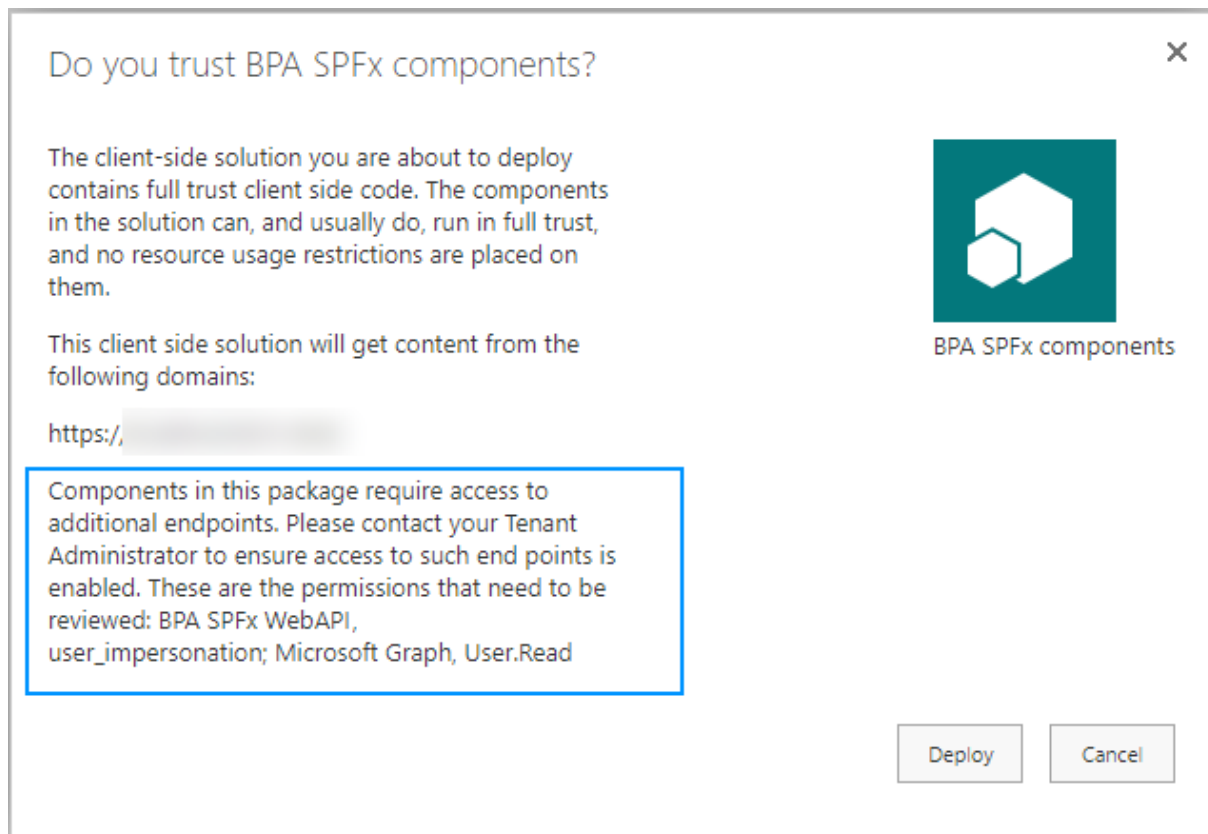
In addition, it requires these features to be activated:

- Custom Scripts have to be activated for the BPA Site Collection.
- App-Only access has to be allowed on tenant (ACS client id/secret). This requires SharePoint Online Management Shell.

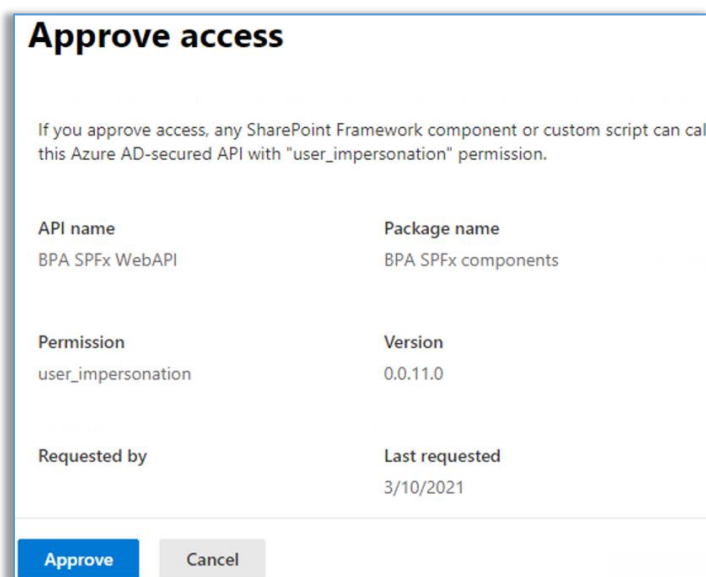
Client side (SPFx) permissions

The application requires these permissions to be granted for client-side part to be able to access AAD protected resources from JS code:

- **user_impersonation** – Delegated - to protect WebAPI backend with Azure AD (allow calls from only authorized users)
- **User.Read** - Delegated - get basic information about logged in user on client side



These permission requests need to be approved in SharePoint Admin Center:



Approve access

If you approve access, any SharePoint Framework component or custom script can call this Azure AD-secured API with "User.Read" permission.

API name	Package name
Microsoft Graph	BPA.SPFx.components
Permission	Version
User.Read	1.5.0.0
Requested by	Last requested
	9/28/2022


ACS WebAPI permissions

The Application needs the following permissions using ACS (to avoid requesting permission to all site collections) to perform app only actions on server side (WebAPI):

- **Site collection full control** - Delegated & Application - To have access to the BPA ONLY site collection to perform most of the tasks - first load, create & edit items/pages/lists. CSOM API

"bpasspfx.bpa-solutions.net" uses the following permissions

- Let it have full control of this site collection.
- Let it share its permissions with other users.
- Let it access basic information about the users of this site.



bpasspfx.bpa-solutions.net

Thus, we recommend 1 Site collection per BPA App.



AAD SharePoint and Graph WebAPI permissions

The application requires permission to Graph and SharePoint using AAD authentication for both app only and user to perform actions on server side:

- **Mail.Send** – Application - send email notification from the configured user using Graph API
- **Sites.Selected** – Application - have access to the ONLY site collection using Graph API (i.e. BPA Mail Merge conversion to PDF)
- **User.Read** – Delegated - get basic information about logged in user in WebAPI
- **AllSites.Read** – Delegated – Required for Export to Excel feature to read all items user has access to in a list/library in WebAPI using CSOM API.

Permissions requested

Review for your organization

 **BPA SPFx WebAPI**
BPA Solutions SA 

This app would like to:

- ^ Read items in all site collections
Allows the app to read documents and list items in all site collections on behalf of the signed-in user.
This is a permission requested to access your data in BPA Solutions SA.
- ^ Sign in and read user profile
Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
This is a permission requested to access your data in BPA Solutions SA.
- ^ Access selected site collections
Allow the application to access a subset of site collections without a signed in user. The specific site collections and the permissions granted will be configured in SharePoint Online.
This is a permission requested to access your data in BPA Solutions SA.
- ^ Send mail as any user
Allows the app to send mail as any user without a signed-in user.
This is a permission requested to access your data in BPA Solutions SA.

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Read the app installation procedure for more information about granting these permissions.

4. BPA Licensing System

The license portal is the most important part of the BPA licensing system. It's a BPA-hosted SharePoint site including the following information: the number of licensed users and readers, site URL(s), and the licensed users/readers accounts. The license portal does not store any sensitive user data – only user accounts (usually email address) and site URL(s) are stored. No user password is stored or used by the license portal. The license portal requires a named license manager(s) to get an access to the license portal with a password, and receive notifications. The licensing system features a scheduled job to process expiration notifications and a web service to securely communicate with the WebAPI to check

attributed licenses and manage licensed users (this part is protected by an auto-generated license password that is shared with the client license manager and is required to view/change licensed users).

There are 2 user roles in the licensing system:

- Reader – can only view items/documents
- Full user – can fully use the system

The BPA licensing system does not check user's permissions in SharePoint to define the current user role. The user license is automatically attributed at the first user connection to the site with the BPA App, based on the default user mode set in the licensing system. Clients can change the user mode and remove inactive user licenses directly from the licensing system in the BPA App settings, with no need to ask BPA. Note that the user role does not limit user actions in BPA apps (but that might be introduced later).

The licensing system verifies the license when each user connects to the site. Information is cached for 24 hours to keep good performance and reduce the number of server calls. It's possible to do a direct call and recheck the user license in case of an issue.

During the license verification, the following information is securely sent from the WebAPI to the License Portal web service:

- Site URL
- User account
- Product

The licensing system allows to register for a free 30-days trial, or to extend/change the license details.

5. BPA SPFx Strategy

BPA SPFx Apps is our last generation development using latest Microsoft development technologies, like Microsoft SPFx, PnP and React, and succeeding to previous on premises/cloud hybrid apps.

BPA's SPFx strategy is the following:

- The security of the application is ensured by all Microsoft SharePoint and Microsoft SPFx framework. We conform to all Microsoft recommendations and our decisions around data access were validated by experts
- We are using a unique architecture: SPFx/PH for 365/online
- SPFx Apps only supports SP365 modern pages
- SharePoint access is done with the CSOM Data Access Model
- It works with the current user permissions (JavaScript/React, on the client side) or with user or App permissions (C#, on the PH side)
- SharePoint lists, content types, views and fields caching is optimized (PH side)
- We store app configurations in hidden SP lists with unique identifier, sites synchronization capabilities and readability from C# and React/JavaScript
- Our reliable business components are optimized for CSOM
- Keeping the best App performance is our main goal