**CLM - SHP komponenta**

pro společnost

XXX a.s.

Verze 1

Obsah

[1. Cíl 3](#_Toc89349921)

[2. Komunikace 3](#_Toc89349922)

[2.1. Schéma 3](#_Toc89349923)

[2.1.1. Doplnění 4](#_Toc89349924)

[2.2. Vystavení dokumentu 4](#_Toc89349925)

[2.3. Stažení dokumentu 4](#_Toc89349926)

[3. Požadavky 5](#_Toc89349927)

[3.1. Dostupnost end-pointů 5](#_Toc89349928)

[3.2. Certifikáty 5](#_Toc89349929)

[3.3. TLS 1.2 5](#_Toc89349930)

[3.4. SNI 5](#_Toc89349931)

[3.5. SAP uživatel jako nositel tokenu 6](#_Toc89349932)

[3.6. Office 365 6](#_Toc89349933)

[3.7. Povolení SICF služeb 7](#_Toc89349934)

[4. Nastavení 7](#_Toc89349935)

[4.1. SAP oAuth klient 7](#_Toc89349936)

[4.2. Získání grantu 9](#_Toc89349937)

[4.3. Destinace 10](#_Toc89349938)

[4.4. Parametry 10](#_Toc89349939)

1. Cíl

Smyslem SHP komponenty je umožnit v CLM v rámci připomínkování využít možnosti Office 365 pro zpřístupnění připomínkovaného dokumentu připomínkujícímu. Komponenta umožňuje pro potřeby připomínkování nahrát připomínkovaný dokument do vyhrazeného prostoru na Sharepoint a zpřístupnit jej připomínkujícímu. Dle potřeb CLM následně komponenta umožňuje upravený dokument stáhnout zpět a ze Sharepointu opět odstranit.

1. Komunikace

Pro potřeby fungování SHP komponenty probíhá komunikace mezi CLM, SHP komponentou a Office 365. A to s využitím SAP oAuth klienta.

* 1. Schéma



1. CLM odešle požadavek do SHP komponenty
2. SHP komponenta vyžádá od SAP oAuth klienta získání oAuth autorizačního tokenu jméném SAP uživatele, který je nositelem tokenu (nikoliv jménem aktuálně přihlášeného uživatele).
3. SAP oAuth klient si vyžádá autorizační token skrze login.microsoftonline.com.
4. SAP oAuth klient získá autorizační token.
5. SHP komponenta získá možnost autorizace http požadavků na Office 365 příslušným autorizačním tokenem.
6. SHP komponenta odesílá http požadavek na Microsoft Graph API autorizovaný oAuth tokenem.
7. SHP komponenta získá výsledek volání Microsoft Graph API.
8. SHP komponenta odesílá požadavek na sharepoint.com autorizovaný autorizačním tokenem získaným z Microsoft Graph API.
9. SHP komponenta získá výsledek volání sharepoint.com
10. CLM získá odpověď – údaje k právě nahranému dokumentu nebo data staženého dokumentu.
	* 1. Doplnění

Komunikace se SAP oAuth klientem a Microsoft Graph API probíhá jménem vyhrazeného SAP uživatele, který je nositelem oAuth tokenu. Pro tyto účely volá SHP komponenta svá RFC zajišťující potřebnou komunikace skrze destinaci, která má tohoto uživatele přiřazeného. Název destinace je definován v parametrech.

Kroky 3 a 4 provádí SAP oAuth klient v situaci, kdy vypršela platnost stávajícímu tokenu a je potřeba jej obnovit. K tomu využívá refresh token. Provedení těchto kroků si v dané situaci vyžádá SHP komponenta.

Kroky 8 a 9 provádí SHP komponenta pouze v případě nahrávání dokumentů.

V rámci jednoho požadavku CLM v kroku 1 mohou kroky 2 až 9 proběhnout podle potřeby vícekrát.

* + 1. Princip zkráceně

Veškeré dokumenty se nahrávají na Sharepoint pod servisním uživatelem. Ten pak dává přístup přes email na uživatele, který edituje dokument. Editace probíhá kompletně pod účtem uživatele.

Pokud se při nahrávání zjistí, že expiroval token, servisní uživatel si vyžádá aktualizaci tokenu.

Servisní uživatel musí mít na Sharepoint stále přístup.

* 1. Vystavení dokumentu

Vystavení dokumentu je iniciováno žádostí CLM o vystavení dokumentu.

Obsah dokumentu je nejdříve dle schématu nahrán na Sharepoint.

Pro dokument na Sharepointu je vygenerován unikátní název, který je tvořen prefixem a unikátním klíčem. Prefix názvu je definován v parametrech.

Dokument je nahráván na Site, Drive a adresář, které jsou definovány v parametrech.

Kvůli limitům na velikost nahrávaného dokumentu u Microsoft Graph API je pro nahrání využito mechanismu UploadSession. V tomto případě se v krocích 6 a 7 nenahrává dokument samotný, ale pouze jeho definice a vytváří se UploadSession. Součástí vzniklé UploadSession je url na sharepoint.com, na které se nahrání dokumentu očekává. Toto URL obsahuje dočasný autorizační token. Při odesílání obsahu na toto URL v krocích 8 a 9 nelze využívat oAuth autorizace. Obsah nahrávaného dokumentu je rozdělen na části a je odesílán postupně opakováním kroků 8 a 9. Velikost těchto částí, chunků, je definována v parametrech.

Po úspěšném nahrání dochází k udělení přístupu (opět s využitím kroků 2 až 7) k dokumentu pro uživatele, jehož e-mail byl součásti žádosti CLM.

Informaci o nahraném dokumentu ukládáme do tabulky /MIBCON/SHPFREC.

SHP komponenta následně vrací do CLM identifikátor dokumentu a URL, skrze kterou je možné dokument editovat uživatelem, kterému byl udělen přístup. CLM poté zajistí otevření dokumentu připomínkujícím uživatelem.

* 1. Stažení dokumentu

Stažení dokumentů je iniciováno žádosti CLM o stažení dokumentu.

Při stahování dokumentu se po ověření existence provede ověření jeho přístupnosti. Dokument, který je otevřený a editovaný připomínkujícím uživatelem je na Sharepointu uzamčen. SHP komponenta takový dokument neumožní stáhnout a smazat a CLM na tento stav upozorní. SHP komponenta současně umožňuje tuto skutečnost ignorovat, pro možnost řešení výjimečných situací.

Pokud dokument existuje a je dostupný ke stažení, SHP komponenta dokument nejdříve stáhne pomocí kroků 2 až 7. Pokud bylo stažení CLM označeno jako finální, SHP komponenta následně dokument smaže opět pomocí kroků 2 až 7.

* 1. Expirace tokenu

Pokud se při nahrávání zjistí, že expiroval token, servisní uživatel si vyžádá aktualizaci tokenu.

Servisní uživatel musí mít na Sharepoint stále přístup.

**V Sharepointu se nastavuje doba expirace Tajemství klienta“ (Client Secret). Většinou je platnost 2 roky. Je nutné tuto dobu hlídat a před vypršením platnosti vystavit nové a přiřadit v SAP dle dokumentace.**

1. Požadavky

Pro správné fungování SHP komponenty je nutné zajistit splnění několika požadavků a současně přípravu potřebných údajů.

* 1. Dostupnost end-pointů

Z důvodu potřeby komunikace s cloudovým prostředím Office 365 je nutné zajistit a udržovat přístupnost následujících end-pointů:

* https://login.microsoftonline.com/\*
* https://graph.microsoft.com/\*
* https://\*.sharepoint.com/\*

Hvězdička (\*) zde slouží jako wildcard a není skutečnou součástí URL.

* 1. Certifikáty

Pro komunikaci je potřeba v STRUST nahrát a udržovat platné certifikáty pro domény:

* login.microsoftonline.com
* graph.microsoft.com
* sharepoint.com
	1. TLS 1.2

Komunikace vyžaduje povolení TLS 1.2 v systému SAP skrze nastavení ssl/client\_ciphersuites a ssl/ciphersuites v transakci RZ10.

Parametr: ssl/client\_ciphersuites

Hodnota: 150:PFS:HIGH:MEDIUM::EC\_P256:EC\_HIGH

Parametr: ssl/ciphersuites

Hodnota: 135:PFS:HIGH:MEDIUM::EC\_P256:EC\_HIGH

* 1. SNI

Pro spolehlivé fungování v cloudovém prostředí Office 365 je nutné mít v systému SAP aktivovánu TLS SNI extenzi. Viz note:

https://launchpad.support.sap.com/#/notes/2124480

* 1. SAP uživatel jako nositel tokenu

SHP komponenta pro komunikaci se SAP oAuth klientem používá k tomuto účelu vyhrazeného uživatele, který je nositelem oAuth tokenu. Tento uživatel musí mít oprávnění:

* volat potřebná RFC (/MIBCON/SHP\_RFC)
* konfigurovat SAP oAuth klienta
* využívat SAP oAuth klienta

Současně musí být dialogovým uživatelem při provádění grantu skrze oa2c\_grant transakci. Po úspěšném provedení grantu již nastavení dialogového uživatele není potřeba.

Potřebná oprávnění jsou shrnuta v roli ZCES\_SHP\_O365.



* 1. Office 365

Protože SHP komponenta využívá pro své fungování Office365, je potřeba zajistit údaje k Office365 aplikaci, která bude zprostředkovávat přístup. Dále pak vyhradit prostor, kam budou dokumenty nahrávány a uživatele, který bude mít v aplikaci oprávnění do vyhrazeného prostoru dokumenty nahrávat, udělovat přístupy dalším uživatelům, dokumenty stahovat a mazat.

* Název Site – Název site vyhrazené pro SHP komponentu (například: SP-CLM-SHP)
* Tenant Id
* Client Id
* Client Secret
* SiteId – Id site vyhrazené pro připomínkované dokumenty (příklad ve správném tvaru: 2C712604-1370-44E7-A1F5-426573FDA80A)
* DriveId – Id drive na site vyhrazené pro připomínkované dokumenty (příklad ve správném tvaru: b!t18F8ybsHUq1z3LTz8xvZqP8zaSWjkFNhsME-Fepo75dTf9vQKfeRblBZjoSQrd7)
* DirectoryId – Id adresáře na DriveId vyhrazeného pro připomínkované soubory (příklad ve správném tvaru: 01JDHW4JDU6NUJJRDJ2N9FLEAZUE3NYHEQ)

Údaje SiteId, DriveId a DirectoryId jsou dohledatelné skrze dotazy na Microsoft Graph API při znalosti názvu site a sharepoint domény.

Tyto údaje se využívají jak při konfiguraci skrze parametry, tak při zakládání SAP oAuth klienta.

* 1. Povolení SICF služeb

Konfigurace SAP oAuth klienta a získání grantu vyžaduje aktivaci následujících služeb v SICF:

* oa2c\_config
* oa2c\_grant\_app
* sec/oauth2/client/redirect
1. Nastavení
	1. SAP oAuth klient

Před získáním grantu je nutné založit SAP oAuth klienta ZAZURESHP, pokud tento už neexistuje. Pokud by bylo potřeba změnit nastavení Office365 aplikace do takové míry, kdy je nutná změna Client, je nutné SAP oAuth klienta odstranit a založit nového s aktualizovanými údaji (poté opět provést grant).

K založení a správě SAP oAuth klientů slouží transakce OA2C\_CONFIG, která spouští webdynpro na adrese SAP systému s cestou:

/sap/bc/webdynpro/sap/OA2C\_CONFIG?sap-client={klient id}#

V přehledu je potřeba kliknout na založení:



V novém okně se následně v profilu zvolí „ZAZURESHP1“ a doplní Client Id z Office365 údajů:



Po vyplnění a potvrzení se otevře detail nového klienta:



Zde je potřeba vyplnit vstup „Tajemství klienta“ (Client Secret). Poté se přejde na záložku rozsahy, kde je nutné přidat profil ZAZURESHP2:



Následně se vytvoření dokončí kliknutím na tlačítko „Uložení“:



Nově vytvořený záznam se objeví v přehledu:



* 1. Získání grantu

Získání grantu se provádí pod SAP účtem nositele grantu.

K provedení grantu slouží transakce OA2C\_GRANT, která spouští webdynpro na adrese SAP systému s cestou:

/sap/bc/webdynpro/sap/OA2C\_GRANT\_APP?sap-client={klient id}#

Po spuštění je potřeba zvolit odpovídající typ poskytovatele služeb (ZAZURESHP) a kliknout na tlačítko „Vyžádání tokenů OAuth 2.0“.



Vyžádání tokenů přesměruje na přihlášení, které dále probíhá podle nastavení organizace.

Po úspěšném získání grantu je u příslušného záznamu zobrazena aktuální informace o datumu přijetí a datumu expirace. Status je signalizován zeleně.



* 1. Destinace

Aby bylo možné komunikovat s Office365, aniž by bylo nutné s každým připomínkujícím uživatelem procházet grantem, volají se komunikační RFC skrze destinaci typu „Spojení ABAP“. Tato destinace je směřována do stejného klienta a v nastavení v tabu „Přihlášení a bezpečnost“ musí mít vyplněny přístupové údaje SAP uživatele, který slouží jako nositel oAuth tokenu. Tato destinace má obvykle název SHP\_CLM. Název destinace, kterou SHP komponenta využívá, je definován v parametrech.

* 1. Parametry

Některá nastavení chování SHP komponenty lze modifikovat skrze parametry v transakci /MIBCON/PARAM v oblasti SHP:



Tyto parametry jsou (název ve tvaru: Oblast / Proces / Parametr):

* SHP / GENERAL / SHP\_FILE\_PREFIX – Prefix názvu souboru, pod kterým je dokument při připomínkování uživatelem nahrán na Sharepoint.
* SHP / GENERAL / UPLOAD\_CHUNK\_SIZE – Velikost částí, na které je rozdělen soubor dokumentu pro jednotlivé kroky odeslání na Sharepoint. Velikost je bytech (B) a její vychozí hodnota je 1048576.
* SHP / GENERAL / REST\_DESTINATION\_NAME – Název destinace, která se používá při volání komunikačních RFC (například SHP\_CLM).
* SHP / API / TARGET\_SITE – Site Id pro Sharepoint Site, která je použita jako dočasné uložiště po dobu připomínkování dokumentu uživatelem.
* SHP / API / TARGET\_DRIVE – Drive Id pro site.
* SHP / API / TARGET\_DIRECTORY – Id adresáře na Drive Id, který je použit jako cíl pro nahrávání dokumentů.

Změna nastavení parametrů v SHP / API ve chvíli, kdy se na Sharepointu nalézají připomínkované dokumenty, způsobí jejich trvalou nedostupnost. Pokud je nutné provést tuto změnu, neměl by být v CLM žádný dokument vedený jako právě připomínkovaný na Sharepointu.