



dox42 Online Platform Description

Lisa Pulsinger

TABLE OF CONTENTS

Table of Contents	2
Document details	2
1. What is dox42 Online?	3
2. Security Information.....	3
3. Required Components for dox42 Online.....	3
4. Azure Active Directory authentication for dox42 Online for Microsoft Cloud Services	4
5. dox42 Template Design	4
6. dox42 Online with Azure Active Directory Impersonation.....	5
7. dox42 Online with AAD Application User with Client Secret or Certificate	6

DOCUMENT DETAILS

Version: dox42 Online Platform Description
Author: Lisa Pulsinger
Date: 23 July 2021

1. What is dox42 Online?

dox42 Online is a SaaS (Software as a Service) application for document generation. It is an Azure hosted Web service with an extensive API that allows the generation of documents via REST or SOAP calls and the integration of various data sources like Microsoft SharePoint, Dynamics 365, SAP, XML/JSON, data bases, etc...

2. Security Information

dox42 Online follows a token based authentication and it does not store any data or credentials on the Server. All security tokens that are obtained by dox42 Online from Azure Active Directory are only held in storage throughout a document generation call and are deleted in full afterwards. The process and prerequisites to obtain the necessary ID and access tokens are described in detail in chapter 4 and 5. Furthermore, all communication with dox42 Online is encrypted through https.

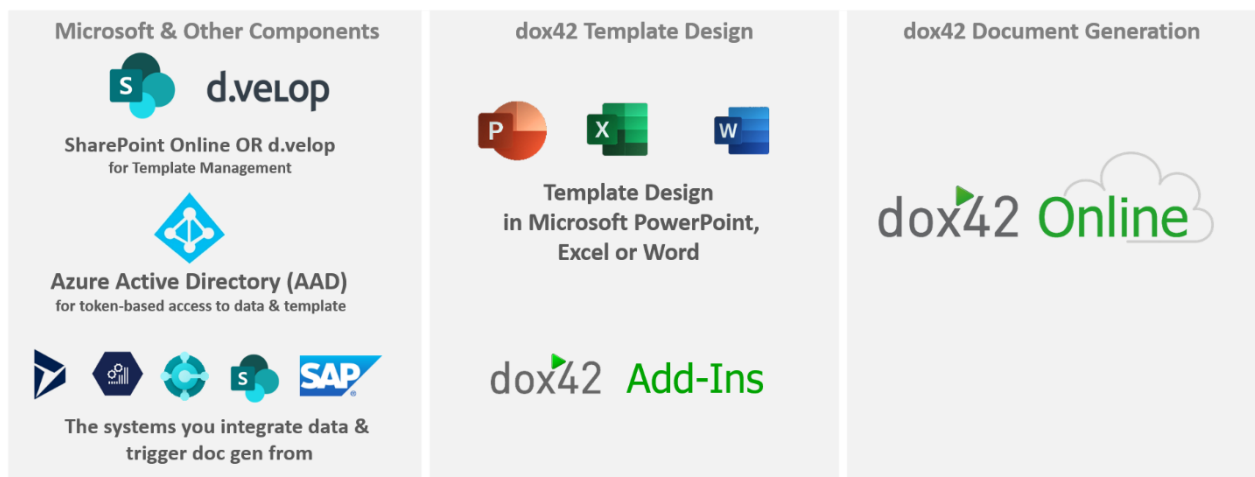
The hosting party, managing the dox42 Online platform, does in no case get access to customer data.

dox42 Online is fully GDPR compliant and all necessary documents can be found in the management application of your dox42 Online Server.

3. Required Components for dox42 Online

The requirements to use dox42 Online are listed below:

- ✓ SharePoint Online or d.velop Documents for d3 ECM for template management
- ✓ A dox42 Online tenant
- ✓ Azure Active Directory Application Registration for dox42 Online if SharePoint Online is used
- ✓ dox42 Add-ins for template design
- ✓ Any other system you connect your data from (e.g. Dynamics 365 CE, FO, BC, SAP, etc..)



4. Azure Active Directory authentication for dox42 Online for Microsoft Cloud Services

dox42 Online uses Azure Active Directory (AAD) authentication to obtain the necessary rights to generate documents in a Cloud environment.

An administrator needs to register a dox42 Online application within Microsoft Azure Active Directory with the following criteria:

- ✓ Azure Active Directory Web application
- ✓ Valid redirect URIs for dox42 Online Server + systems you will use AAD authentication from (e.g. D365 CE)
- ✓ A Client Secret
- ✓ Optional: a Certificate (see chapter 7 for applicable scenarios)
- ✓ Delegated API permissions for SharePoint Online (template management) + any other system you use dox42 Online with Azure Active Directory from (e.g. D365 CE or BC).

DELEGATED permissions: Allows the app to get access on behalf of the signed-in M365 user.

- ✓ A Mobile/Desktop platform + redirect URI (needed for template design)

The following information from the dox42 Online AAD app registration needs to be added to the Management UI of your dox42 Online Server:

- ✓ AAD App Registration ID
- ✓ M365 Tenant ID
- ✓ The provided client secret
- ✓ The SharePoint Online site you store your templates on

dox42 Online ONLY gets Access Tokens when ID Token is present and App ID, Tenant ID, Client Secret and Redirect URIs EXACTLY MATCH the information provided in the AAD app registration.

Please follow the [dox42 Online documentations](#) for further information on how to register a dox42 Online application within Azure Active Directory.

In case only d.velop Documents for d3 ECM is used, you don't need AAD.

5. dox42 Template Design

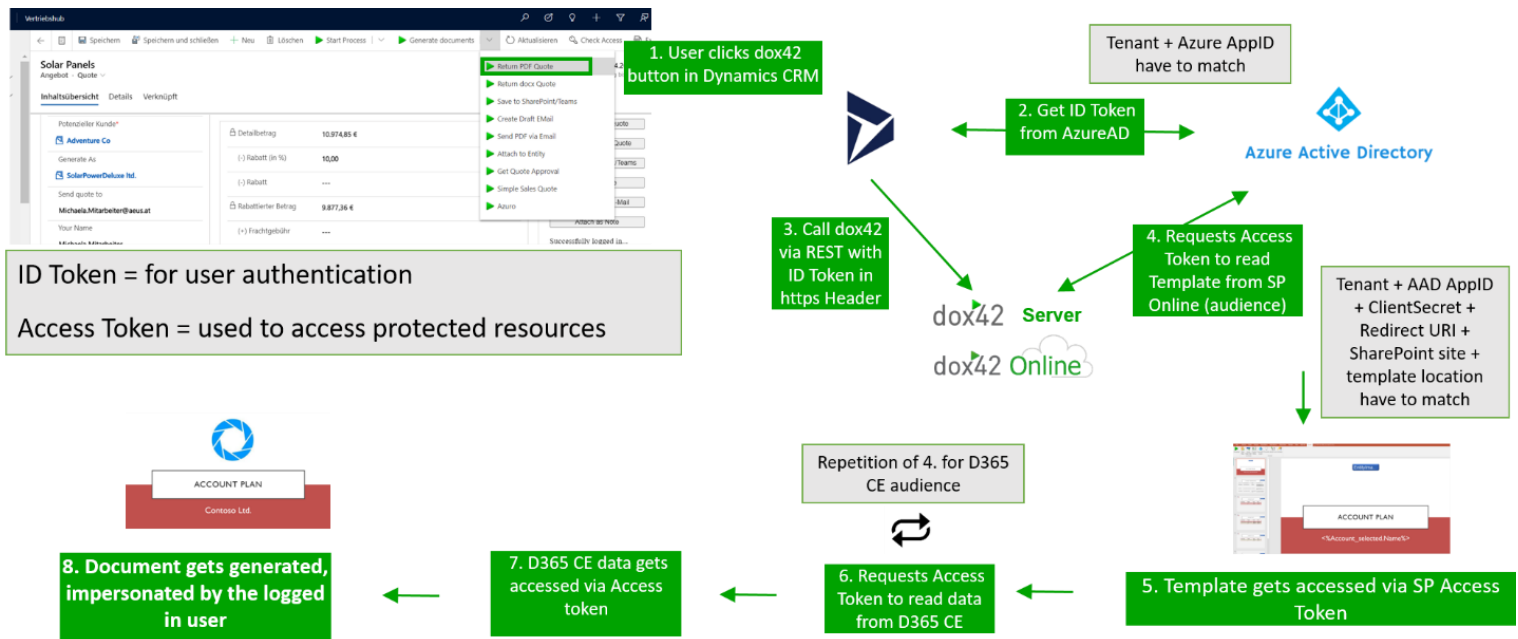
Every document that gets generated using dox42 Online, is based on a template, designed with the dox42 Add-ins in either Word, Excel or PowerPoint.

To integrate data into their template, the user needs to connect to their systems, within the dox42 Add-in. For a connection to SharePoint Online or Dynamics 365 the user connects via Azure Active Directory impersonation. For other systems, username/password or the specific authentication method required for that system may be used, e.g. AAD application user.

After the template design is complete, it needs to be uploaded and managed on SharePoint Online or d.velop Documents or d3 ECM. Managing your templates from SharePoint Online or d.velop is a requirement for dox42 Online, as one of those systems is needed to obtain the correct tokens.

6. dox42 Online with Azure Active Directory Impersonation

This chapter describes the authentication in a scenario where dox42 Online is used within Microsoft D365 CE with Azure Active Directory impersonation and the templates are managed on SharePoint Online.



(1) The logged in Microsoft 365 user triggers the document generation by clicking the dox42 button in Dynamics CRM. (Please see [dox42 D365 CE | Dynamics CRM documentation](#) on how to integrate dox42 into D365 CE.

(2) The request is sent to Azure Active Directory, and if the Tenant ID and AAD App ID provided in the set-up match, the user gets an ID Token from Azure Active Directory.

(3) This token is now included in the HTTPS Header of the REST Call sent to dox42 Server/Online.

(4 – 5) This ID token allows dox42 Online to request an Azure AD Access token for the audience SharePoint Online. It gives the registered dox42 app the permission to access the template from SP

Online. To obtain the Access Token, the provided Tenant ID, AAD App ID, the Client Secret, Redirect URIs, as well as the registered SharePoint site + trusted template locations have to match.

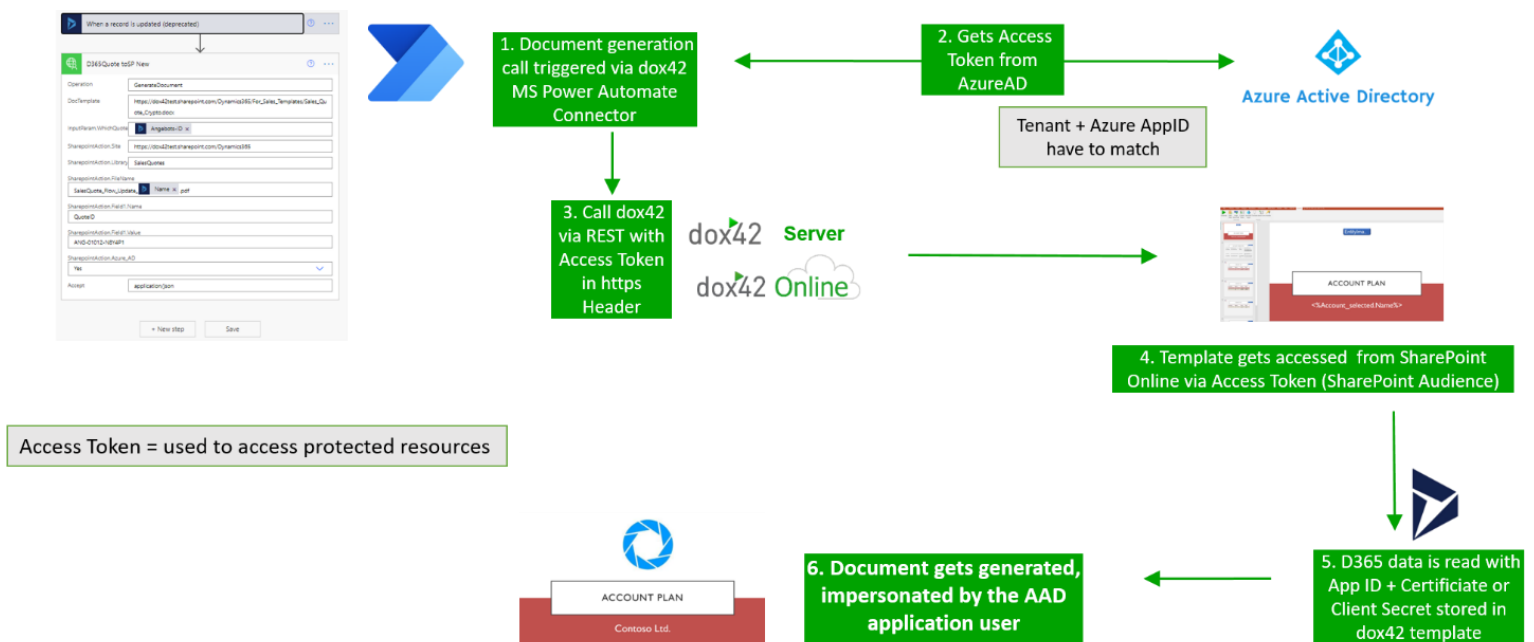
(6 – 7) An access token is always issued for one audience (e.g. SharePoint, or Dynamics CE). Therefore, the process of obtaining an Azure AD access token, is repeated for all data sources that use Azure Active Directory impersonation (e.g. D365 CE or BC).

(8) Now dox42 has the required all the necessary permissions of to read the template and data and generates the document impersonated.

7. dox42 Online with AAD Application User with Client Secret or Certificate

In certain scenarios, for example when a document gets generated via a Microsoft Power Automate flow, no ID tokens are generated, and hence the authentication for dox42 Online is structured a bit differently.

Note that if you generate D365 CE documents via Power Automate, you will need to connect to your D365 CE data sources with an Azure Active Directory App Registration + Client Secret or Certificate, rather than Azure Active Directory Impersonation. Please follow the instructions in the [dox42 D365 CE | Dynamics CRM documentation](#) for further information.



(1) The document generation gets triggered via an MS Power Automate workflow. For further information on how to set up a dox42 Power Automate flow, please follow the [dox42 Power Automate documentation](#).

(2) The dox42 MS Power Automate Connector obtains an Access Token from Azure Active Directory. **To obtain the Access Token, the provided Tenant ID, AAD App ID, the Client Secret, Redirect URIs, as well as the registered SharePoint site + trusted template locations have to match.**

(3) This token is now included in HTTPS Authorization Header of the REST Call sent to dox42 Online.

(4) This Access Token is generated for a SharePoint Online audience. It gives the registered dox42 AAD application the permission to load the template and data map from SP Online.

(5) Since in this scenario, no ID tokens are involved, no second Access Token can be generated and the connection to further data sources like D365 CE has to take place via an Azure Active Directory Application User + Client Secret/Certificate rather than Azure Active Directory User impersonation.

For the AAD application user, an application needs to be registered in Azure Active Directory including a Client Secret or a Certificate. Then, in order to obtain the correct user rights, this AAD application needs to be registered as an application user within D365 CE | Dynamics CRM. Make sure that you use the correct authentication method within your dox42 template (see [dox42 Dynamics CRM documentation for further details](#)).

(6) With these settings, dox42h as now obtained all necessary rights and generates the document impersonated as the AAD application user.