



WITH *Learn Smart Coding*
Topic

*What are OAuth 2.0
and OpenID Connect?*

*How it is used in Azure
AD B2C ?*



Learn Smart Coding

Everyone can
code !

Share
Like
Subscribe



<https://youtube.com/@learnsmartcoding>

What are OAuth 2.0 and OpenID Connect ?



OAuth 2.0 and OpenID Connect are both widely used protocols for authentication and authorization, and they play essential roles in Azure AD B2C. Let's break down what each of these protocols is and how they are utilized.



OAuth 2.0

What is OAuth 2.0?



OAuth 2.0 is a protocol that enables secure authorization of resources between different parties without sharing credentials. In simpler terms, it's a way for a user to grant limited access to their resources to another application or service without sharing their username and password.



How is OAuth 2.0 used in Azure AD B2C?

Azure AD B2C uses OAuth 2.0 as the underlying protocol to manage access to resources. When a user tries to access a protected resource, like a user's profile or certain functionalities in an application, OAuth 2.0 is used to grant access. This involves the issuance of access tokens that carry information about the permissions granted to the application



OpenID Connect



What is OpenID Connect?

OpenID Connect is an identity layer built on top of OAuth 2.0. It provides a standard way for applications to discover and verify information about users. While OAuth 2.0 focuses on authorization and access, OpenID Connect adds an authentication layer, allowing applications to obtain information about the identity of the user.



How is OpenID Connect used in Azure AD B2C?

In Azure AD B2C, OpenID Connect is used to authenticate users and obtain identity information in addition to the access tokens provided by OAuth 2.0. When a user logs in, OpenID Connect is responsible for verifying the user's identity and providing an ID token, which is a JSON Web Token (JWT) containing claims about the user.



The Relationship in Azure AD B2C

In Azure AD B2C, these protocols work hand in hand:

OAuth 2.0: Manages access to resources. When a user wants to perform an action that requires certain permissions, OAuth 2.0 facilitates the process of granting and validating access tokens

OpenID Connect: Adds the identity layer on top of OAuth 2.0. When a user logs in, OpenID Connect provides an ID token containing claims about the user, such as their name, email, and other profile information



Summary

OAuth 2.0 and OpenID Connect are integral to Azure AD B2C, working together to ensure secure access to resources and authentication of users in a way that's standardized and widely adopted in the industry



**OAuth 2.0
and OpenID
Connect in a
simple, real-
world story**



The Magical Library

Adventure:

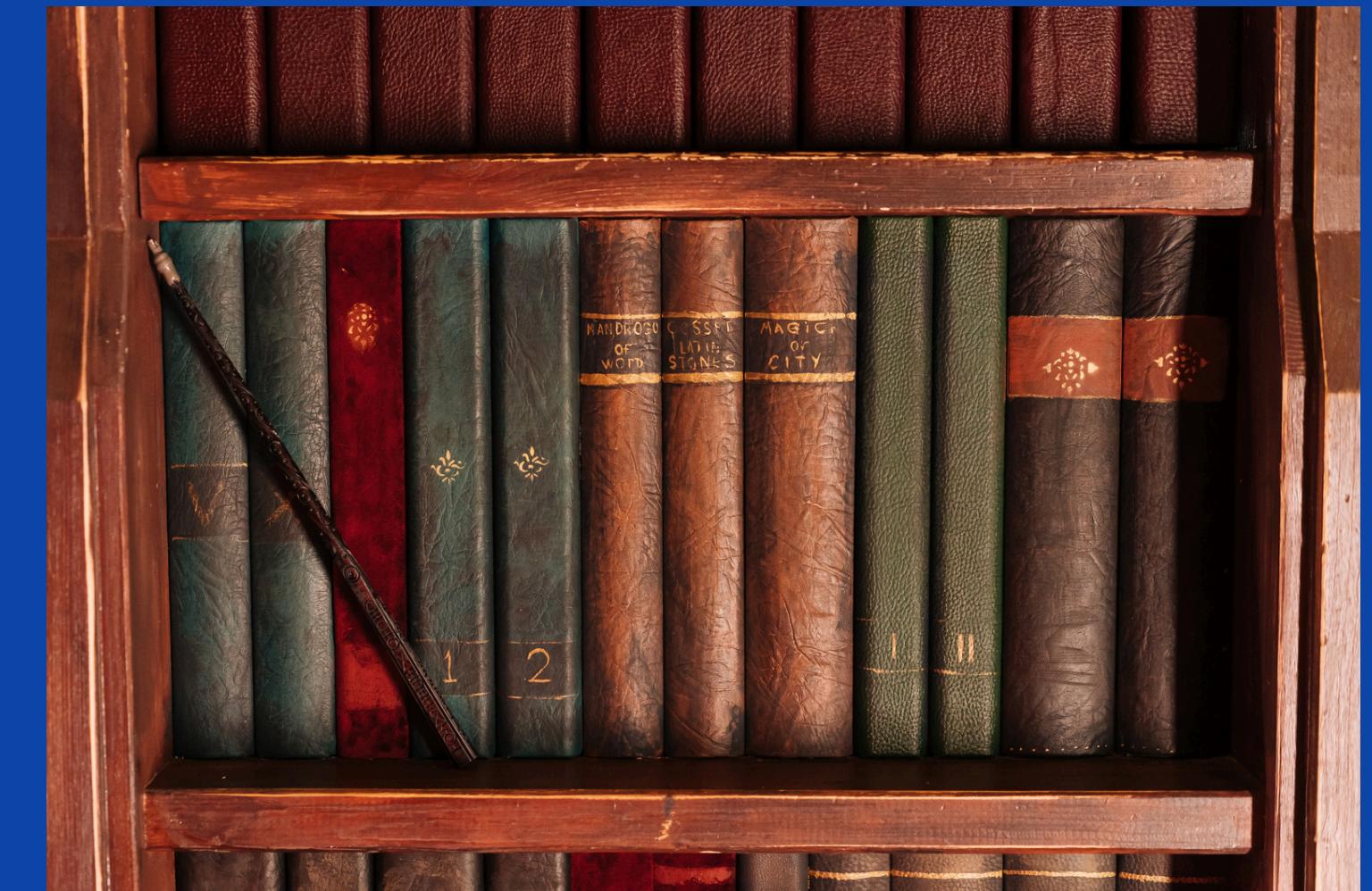
Once upon a time in the magical kingdom, there was a library filled with enchanted books that held secret knowledge. The librarian, who protected the books, wanted to allow wizards and witches to borrow these books but needed a secure way to control who could access them



<https://youtube.com/@learnsmartcoding>

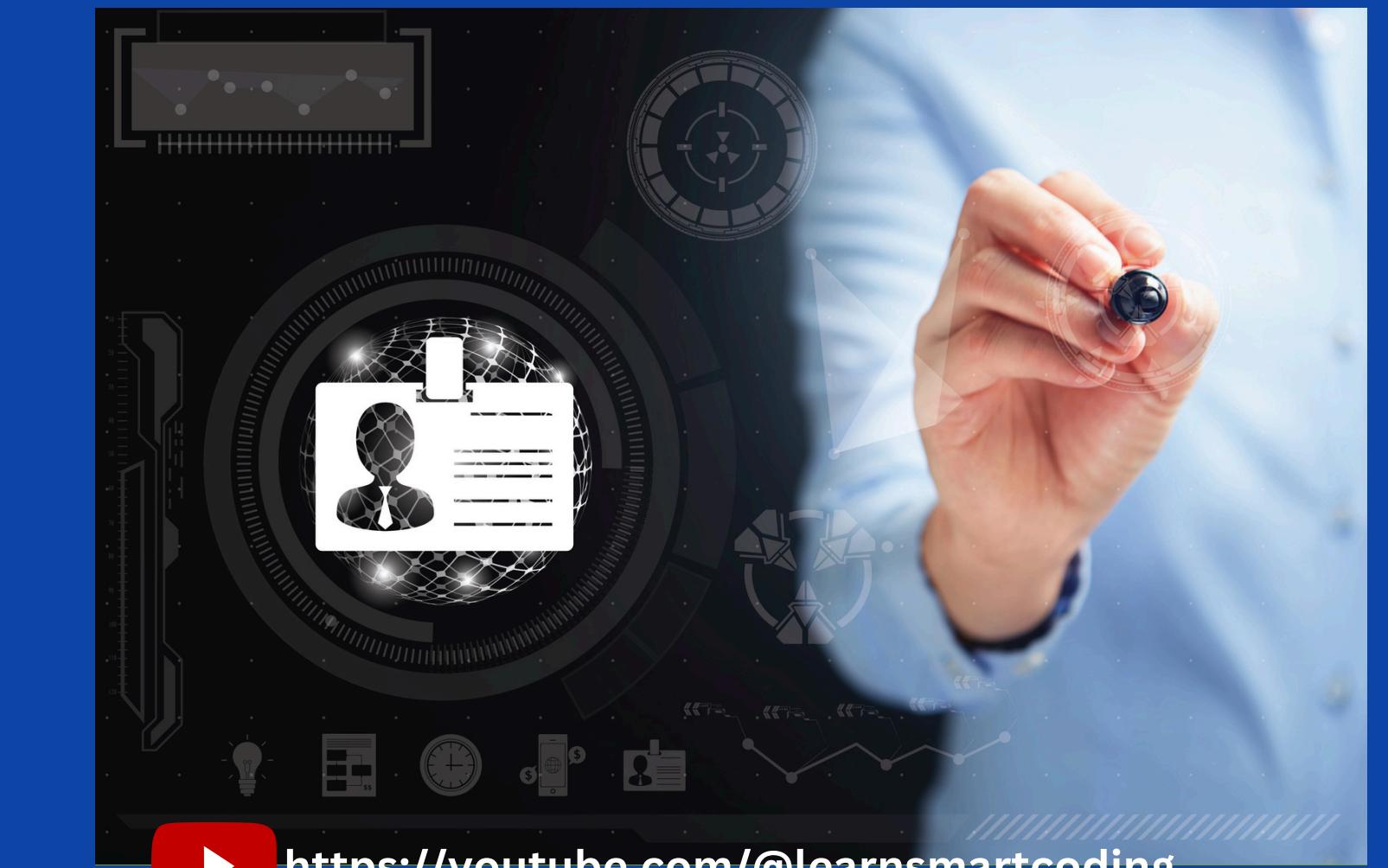
OAuth 2.0 - The Library Pass

Imagine you, a wizard named Alice, want to borrow a special spell book from the library. The librarian doesn't want your actual magical key but decides to give you a temporary "Library Pass" (OAuth 2.0 token).



Request for a Library Pass (Authorization Request)

- Alice asks the librarian for a Library Pass to borrow a book.
- The librarian, being cautious, asks Alice to show her magical ID card (Authentication) to make sure she's a known wizard.



<https://youtube.com/@learnsmartcoding>

Issuing the Library Pass (Access Token)

- Satisfied with Alice's identity, the librarian issues a Library Pass (OAuth 2.0 token).
- This pass contains information about what books Alice is allowed to borrow (scopes/permissions)



<https://youtube.com/@learnsmartcoding>

Using the Library Pass (Accessing Resources)

- Alice, with her Library Pass, can now enter the library and borrow the specific spell book she requested.
- The librarian checks the pass to ensure Alice has the right permissions.



<https://youtube.com/@learnsmartcoding>

OpenID Connect - The Wizard's Identity

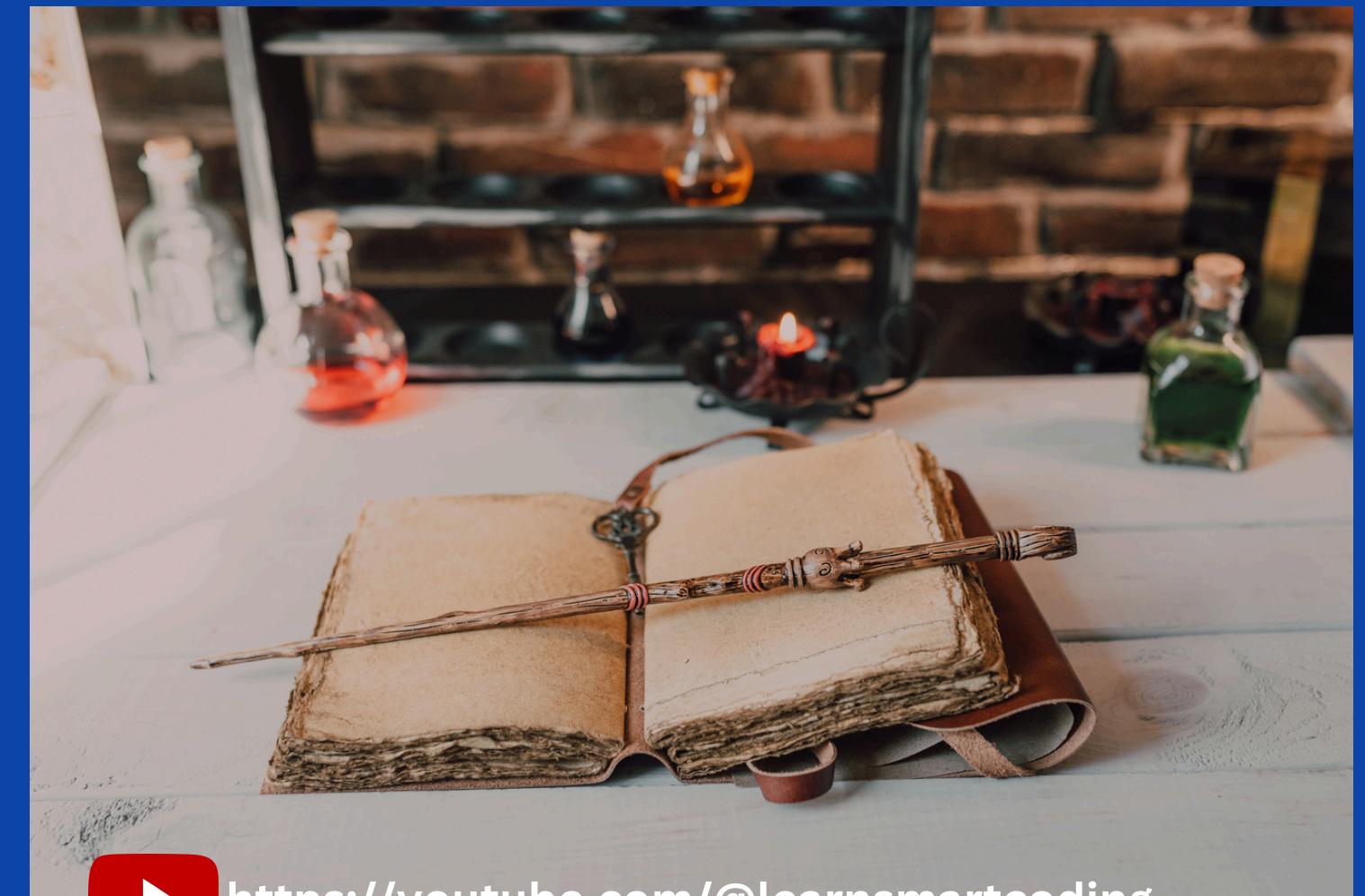
Now, let's add a layer to this magical adventure. Alice not only wants to borrow a book but also wants to tell the librarian her name and maybe even make a new wizard friend.



<https://youtube.com/@learnsmartcoding>

Introducing OpenID Connect (Adding an Identity Layer)

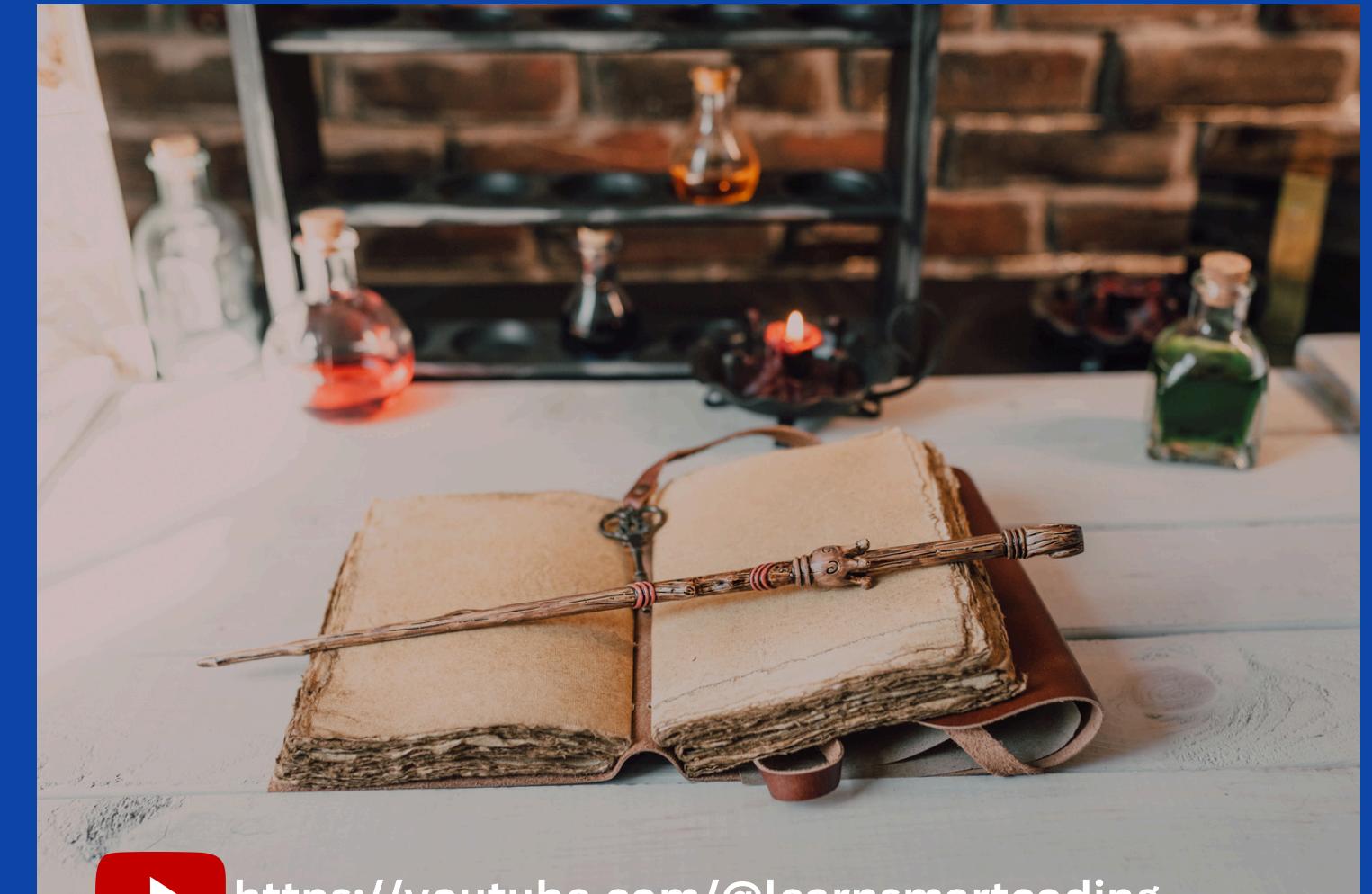
- When Alice asks for the Library Pass, she also asks the librarian if she can share her name and a bit about herself.
- The librarian, being friendly, agrees and adds an extra enchantment to the Library Pass, turning it into an "Identity Pass" (OpenID Connect ID token).



<https://youtube.com/@learnsmartcoding>

The Identity Pass (ID Token)

- This Identity Pass contains not only the permission to borrow books but also Alice's name and other information.
- Now, when Alice enters the library, the librarian not only knows she can borrow books but also greets her by name



Summary

- **OAuth 2.0 (Library Pass)**: Manages access to resources (books) by issuing temporary passes (tokens) with specific permissions.
- **OpenID Connect (Identity Pass)**: Adds an identity layer, allowing wizards like Alice to not only access resources but also share information about themselves securely.

So, in the magical kingdom of OAuth 2.0 and OpenID Connect, wizards and witches can not only borrow enchanted books but also share a bit of their magical identity along the way



<https://youtube.com/@learnsmartcoding>



—
Thank you for
watching!
Happy coding!



<https://youtube.com/@learnsmartcoding>