AuthN is "Who are you?"

AuthZ is "What can you do?"

OAuth is for AuthZ only by design.

OAuth is for AuthZ without sharing AuthN.

OAuth: Better Than Passwords

- Never had to share our password
- Revoke the access at any time
- Third-party website can only do what we granted
- We're training users to do silly things
- Never had to share our password

OAuth Vocabulary

- The exchange is called a **flow** or **grant type**
- The permissions are called **scopes**
- Access is granted via **tokens**

OAuth solves a major problem.

We can grant access without giving up control.

Some Challenges in OAuth

- OAuth is a framework—it doesn't solve every problem
- Specific solutions come through extensions
- Extensions vary from vendor to vendor
- Lots of things are open to interpretation

Why Not SAML?

- Defined in 2002–03
- SAML was designed primarily for SSO (AuthN)
- XML-based, so heavy payloads
- Not designed for delegated access
- Defined before mobile apps, and early in API history

So, how do we AuthN+AuthZ for APIs?

Approaches to API AuthN+AuthZ

- API keys

  Simple, common, easy to implement and use

  Hard to manage and rotate

- Account Identifier+Secret

  Very similar to API keys approach

  False sense of security

Approaches to API AuthN+AuthZ

- OAuth

  Easy to delegate selective access

  Easy to revoke access

  Common, well-supported in most tech stacks

  Not easy to implement

OAuth is for AuthZ.

OAuth doesn't specify payloads.

Though we often use JSON Web Tokens (JWTs).

OAuth doesn't specify AuthN.

That's up to the Identity Provider.

OAuth doesn't specify Identity.

We know someone AuthN+AuthZ, but not who.

OpenID Connect (OIDC)

- A simple identity extension on top of OAuth 2.0
- Defines specific fields (content and structure) for sharing profile information, such as address, phone number, email, and other fields
- This is done through an ID token
- Not part of the previous OpenID standard

OIDC is not for AuthZ.

But it builds on OAuth, which is for AuthZ.

OAuth 2.0	OpenID Connect
Designed for AuthZ	Designed for identity
Extensible	Structure+extension
User or devices/services	Only for users

OIDC is just a special case of OAuth.