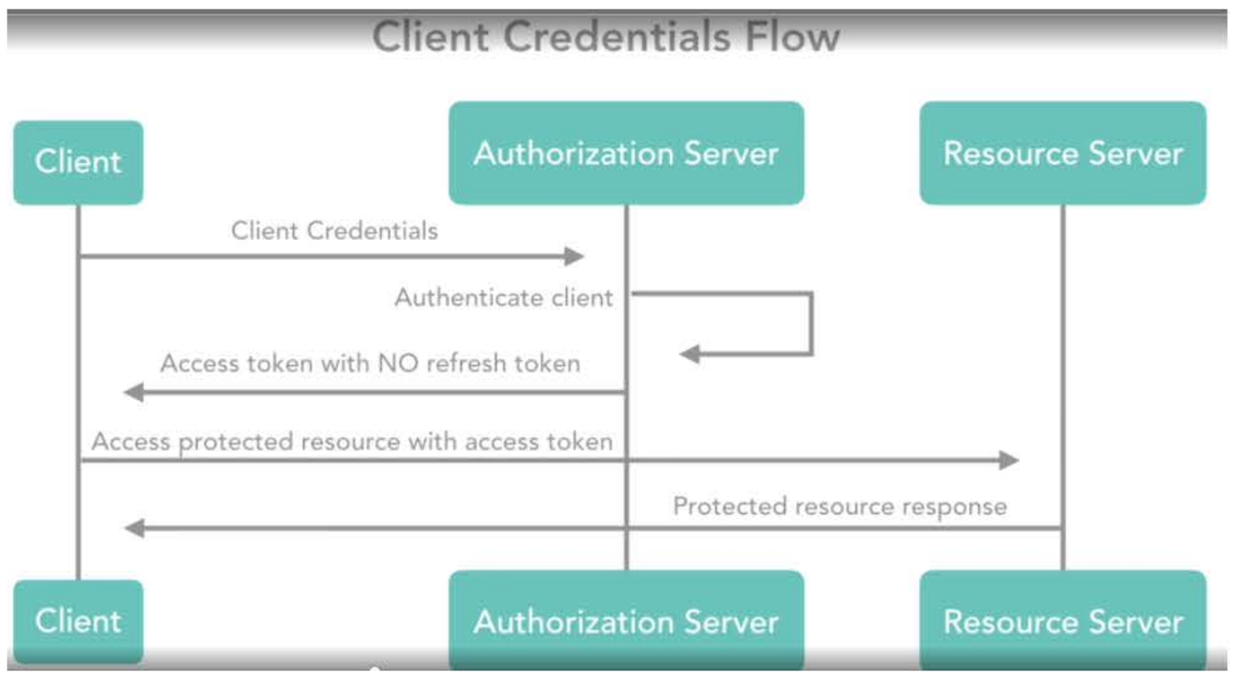
Client Credential Grant Type

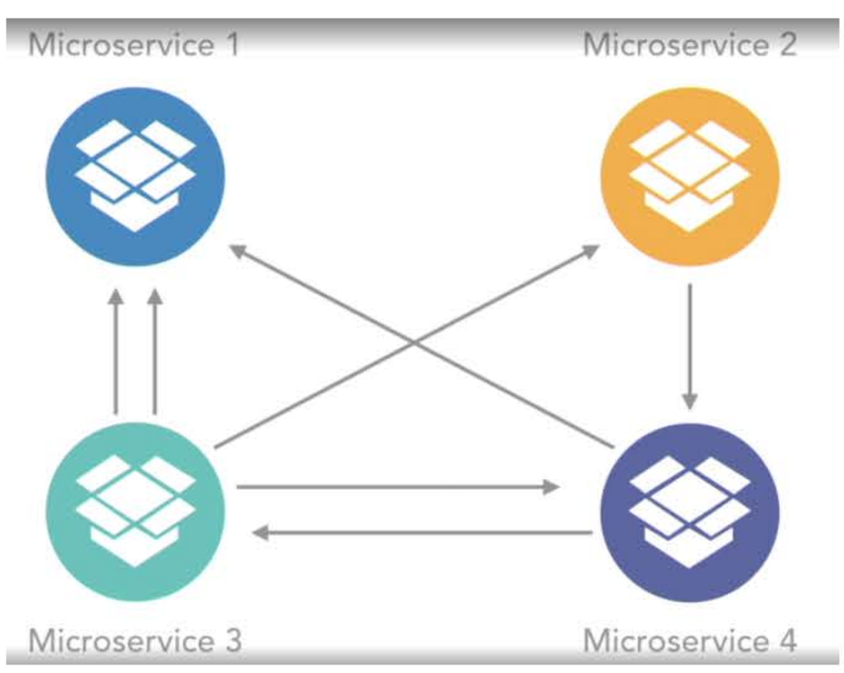
Designed specifically for server-to-server interactions, similar to "service accounts" from Active Directory and other backend services

No user involved (therefore not compatible with OIDC)



How the Client Credentials Flow Works

- I use task tracking system Trello
- I upload a file to a Trello task
- Trello uploads the file to Amazon S3
- I can download or view the file as I need



Why Client Credentials Flow?

- All the benefits of OAuth
- Easy onboarding

  I didn't need an S3 account to use Trello.

- Pluggable interfaces

  They can switch backend services as needed without my knowledge or involvement.

Important

The Client Credentials Grant Type is only for "private" clients where the interaction is handled by backed code.

Client Credential Flow Security Considerations

The Good News

Having no users means they can't compromise it!

Security Considerations

- Private clients only

  Secrets must be in backend code.

  Not appropriate for mobile apps or single page apps.

- Must use secure communications
- We don't have a user for logging or audit purposes

Security Consideration

- Validating our Access Tokens

  We could use the /introspect endpoint (if supported).

  We could use the token validation rules (RFC 7519).

  Either way, we'll likely cache the results—be careful.