OAuth 2.0 Incremental Auth

IETF 101 London, March 2018

William Denniss

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01

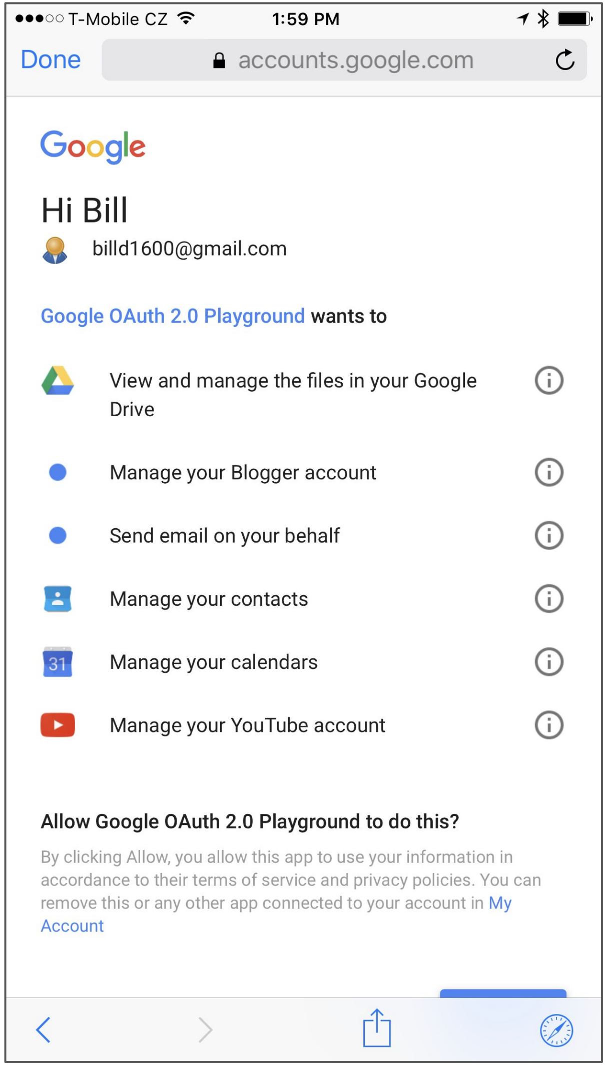
Recap: Incremental Auth Problem Statement

Asking for the kitchen sink of scopes up-front is a bad thing.

Users should have the *context* of the authorization request.

E.g. Granting a calendar scope only makes sense in the context of interacting with a calendar-related feature.

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01



Google

Hi Bill

billd1600@gmail.com

Google OAuth 2.0 Playground wants to

- View and manage the files in your Google Drive
- Manage your Blogger account
- Send email on your behalf
- Manage your contacts
- Manage your calendars
- Manage your YouTube account

Allow Google OAuth 2.0 Playground to do this?

By clicking Allow, you allow this app to use your information in accordance to their terms of service and privacy policies. You can remove this or any other app connected to your account in My Account

Incremental Auth Definition

The ability to request additional scopes in subsequent requests resulting in a single authorization grant representing all scopes granted so far.

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01

Typical Implementation

Consent screen should only display new scopes (or display new/existing scopes differently).

Single refresh token issued for the union of all granted scopes.

De-facto Incremental Auth for Confidential Clients

OAuth 2.0 doesn’t stop you returning an authorization grant with *more* scope, so many people have implemented this already for confidential clients.

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01

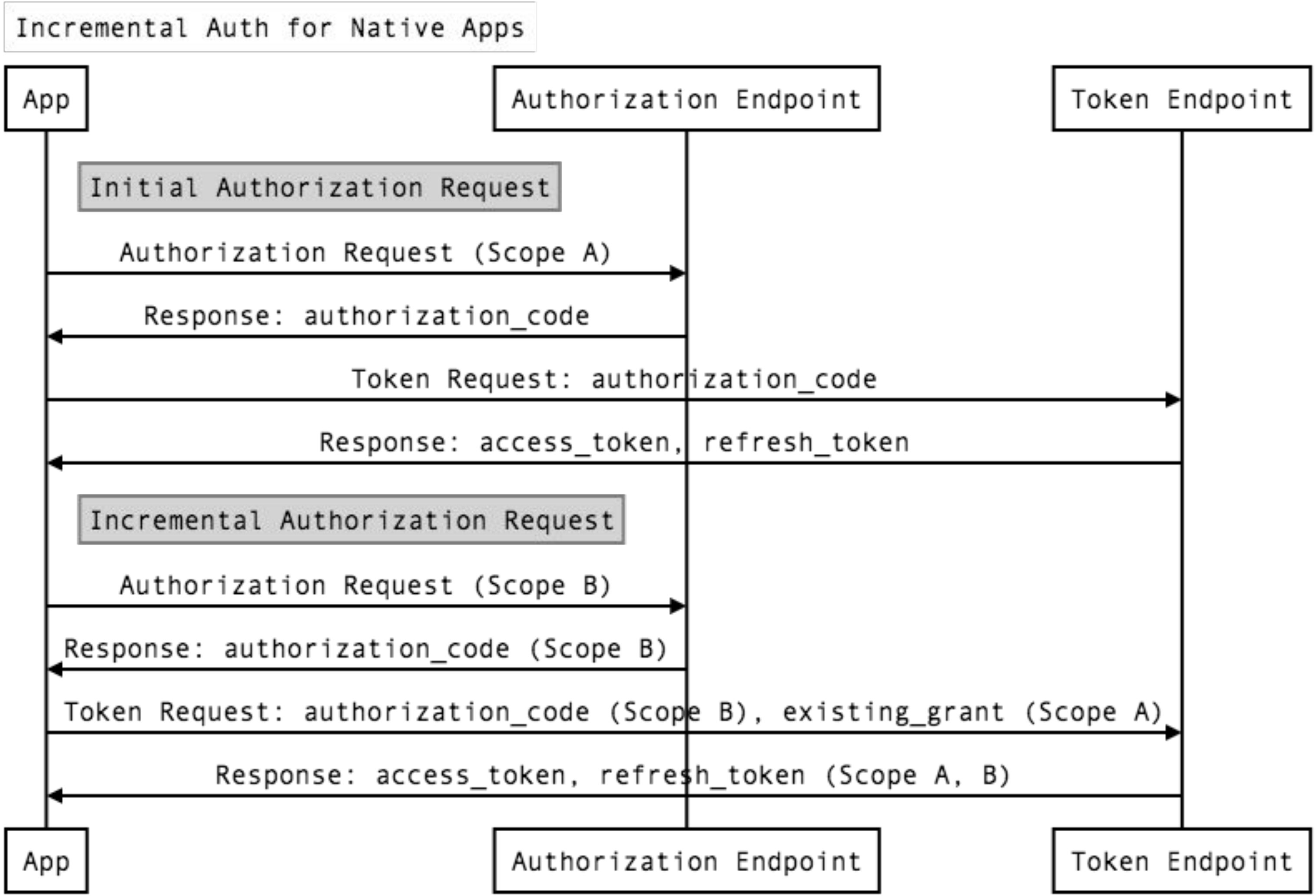
Public Client Protocol “Appcremental”

New token endpoint param: `existing_grant`.

When exchanging the authorization code from subsequent (i.e. incremental) requests, pass the previous refresh token in `existing_grant`.

Resulting access and refresh tokens will contain a union of the scope.

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01



Incremental Auth for Native Apps

App

Authorization Endpoint

Token Endpoint

Initial Authorization Request

Authorization Request (Scope A)

Response: authorization_code

Token Request: authorization_code

Response: access_token, refresh_token

Incremental Authorization Request

Authorization Request (Scope B)

Response: authorization_code (Scope B)

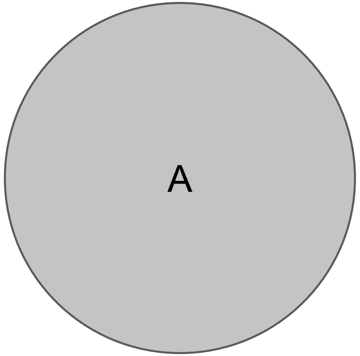
Token Request: authorization_code (Scope B), existing_grant (Scope A)

Response: access_token, refresh_token (Scope A, B)

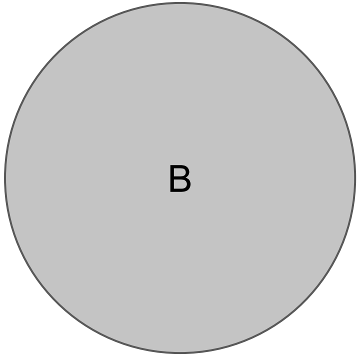
App

Authorization Endpoint

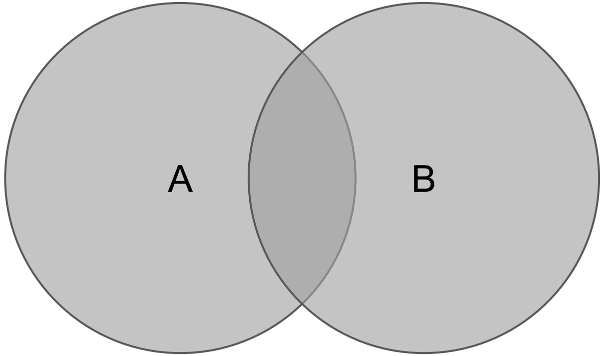
Token Endpoint



Grant A



Grant B



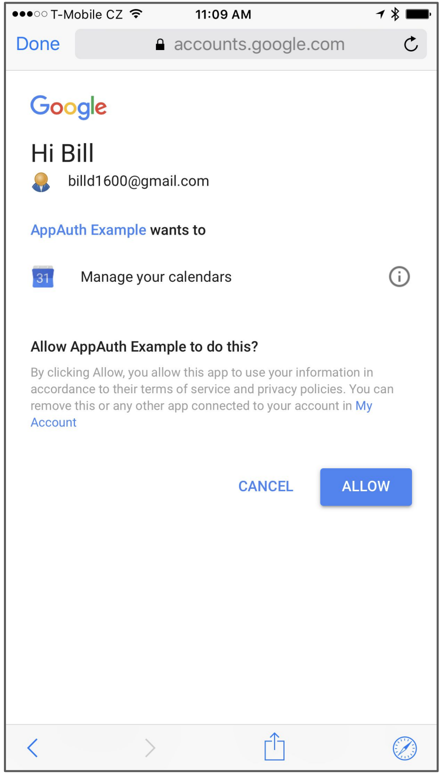
Combined Grant A ∪ B

OAuth 2.0 Incremental Auth Running Code

Google's OAuth server already supports incremental auth for public clients, as defined in this spec.

Try out my proof of concept:
https://github.com/WilliamDenniss/AppAuth-iOS/tree/appcremental

Demo



Hi Bill

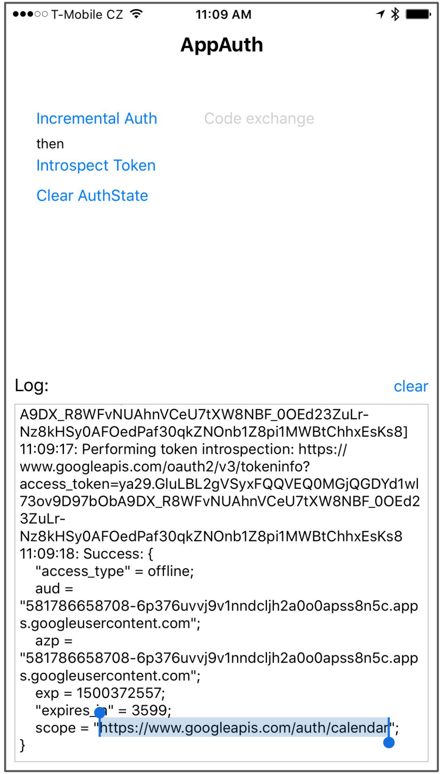
billd1600@gmail.com

AppAuth Example wants to

Manage your calendars

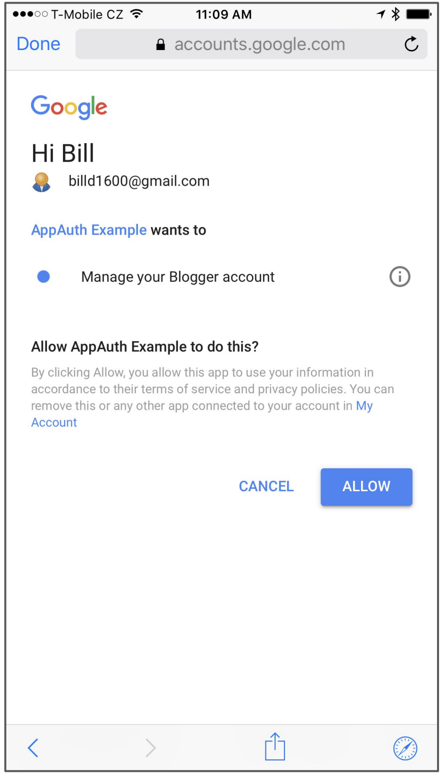
Allow AppAuth Example to do this?

By clicking Allow, you allow this app to use your information in accordance to their terms of service and privacy policies. You can remove this or any other app connected to your account in My Account



Log:

```
A9DX_R8WFvNUAhnVCeU7tXW8NBF_0OEd23ZuLr-
Nz8kHSy0AFOedPaf30qkZNOnb1Z8pi1MWBtChhxEsKs8]
11:09:17: Performing token introspection: https://
www.googleapis.com/oauth2/v3/tokeninfo?
access_token=ya29.GluLBL2gVSyxFQQVEQ0MGjQGDYd1wl
73ov9D97bObA9DX_R8WFvNUAhnVCeU7tXW8NBF_0OEd2
3ZuLr-
Nz8kHSy0AFOedPaf30qkZNOnb1Z8pi1MWBtChhxEsKs8
11:09:18: Success: {
   "access_type" = offline;
   aud =
"581786658708-6p376uvvj9v1nndcljh2a0o0apss8n5c.app
s.googleusercontent.com";
   azp =
"581786658708-6p376uvvj9v1nndcljh2a0o0apss8n5c.app
s.googleusercontent.com";
   exp = 1500372557;
   "expires_in" = 3599;
   scope = "https://www.googleapis.com/auth/calendar";
}
```



Hi Bill

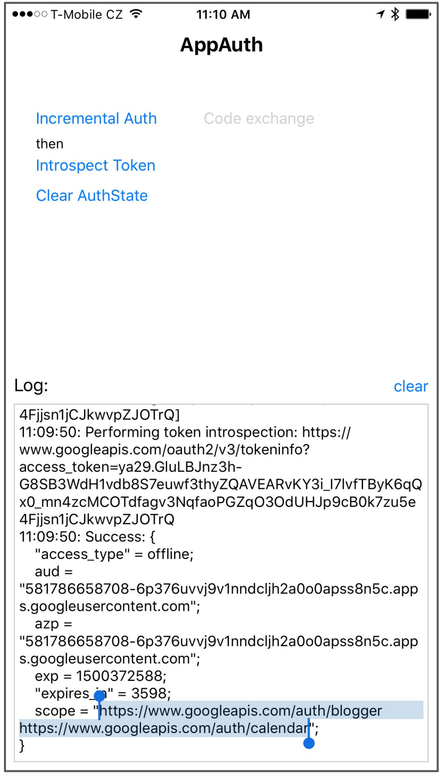
billd1600@gmail.com

AppAuth Example wants to

Manage your Blogger account

Allow AppAuth Example to do this?

By clicking Allow, you allow this app to use your information in accordance to their terms of service and privacy policies. You can remove this or any other app connected to your account in My Account



Log:

```
4FjjsnljCJkwvpZJOTrQ]
11:09:50: Performing token introspection: https://
www.googleapis.com/oauth2/v3/tokeninfo?
access_token=ya29.GluLBJnz3h-
G8SB3WdH1vdb8S7euwf3thyZQAVEARvKY3i_I7lvfTByK6qQ
x0_mn4zcMCOTdfagv3NqfaoPGZqO3OdUHJp9cB0k7zu5e
4FjjsnljCJkwvpZJOTrQ
11:09:50: Success: {
   "access_type" = offline;
   aud =
"581786658708-6p376uvvj9v1nndcljh2a0o0apss8n5c.app
s.googleusercontent.com";
   azp =
"581786658708-6p376uvvj9v1nndcljh2a0o0apss8n5c.app
s.googleusercontent.com";
   exp = 1500372588;
   "expires_in" = 3598;
   scope = "https://www.googleapis.com/auth/blogger
https://www.googleapis.com/auth/calendar";
}
```

https://youtu.be/SPSCW4NUooU

Confidential Client Specification Details

Documents best practices, security considerations, and:

New authorization endpoint parameter `include_granted_scopes`.

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01

Updates since IETF 99

Sections added:

- Security Considerations
- Privacy Considerations
- Usability Considerations
- Alternative Approaches

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01

OAuth 2.0 Incremental Auth

Discuss

https://tools.ietf.org/html/draft-wdenniss-oauth-incremental-auth-01