OAuth 2.0 Device Flow

IETF98 March 2017

William Denniss et al.

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Recap

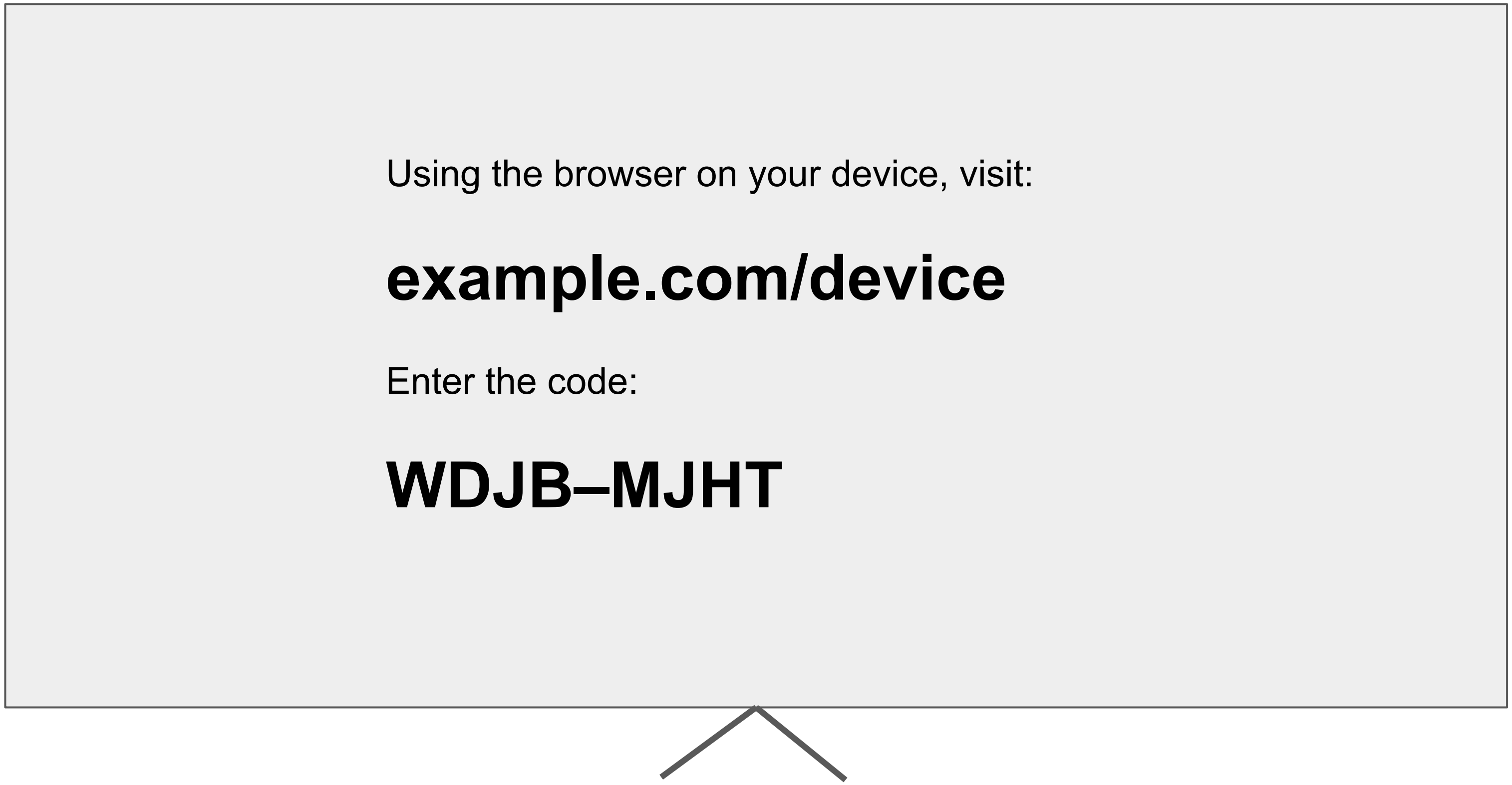
Authorization flow designed for devices that have an internet connection, but no browser and/or limited input.

The user will review the authorization request on a secondary device, like a mobile phone, or laptop.

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Recap



Using the browser on your device, visit:

example.com/device

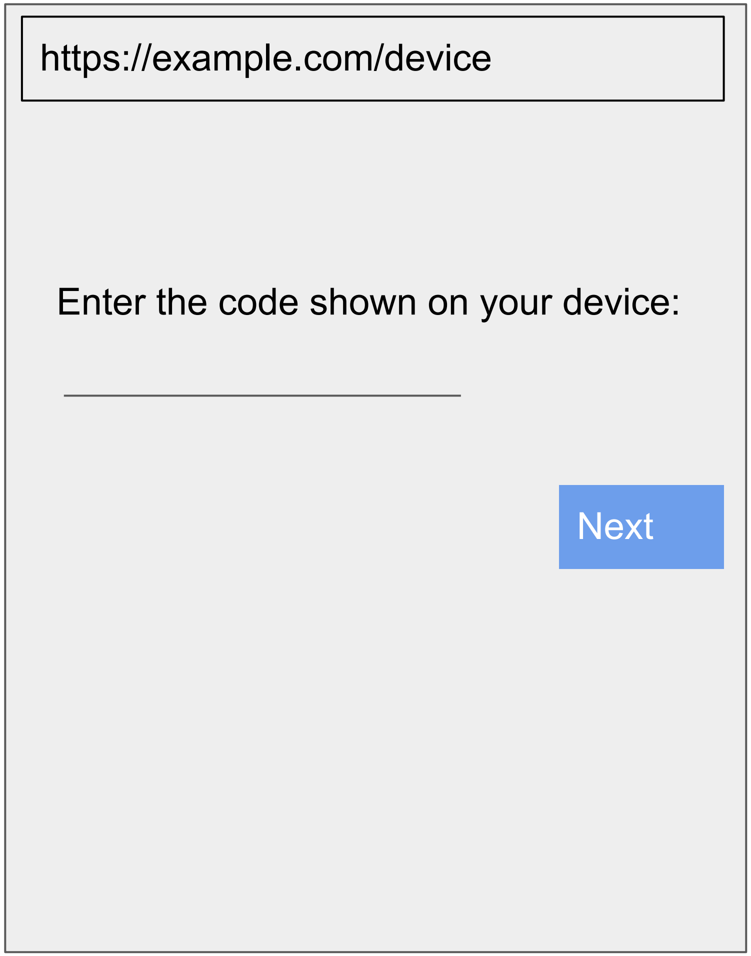
Enter the code:

WDJB–MJHT

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Recap



https://example.com/device

Enter the code shown on your device:

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Recap – Requirements

1. Internet connection (i.e. not for bootstrapping devices).

2. Display mechanism (visual, audio, etc).

DOES NOT NEED: Two-way connection to user’s device.

NOT FOR: Devices with browser + rich input

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Changes

New name!

OAuth 2.0 Device Flow for Browserless and Input Constrained Devices

If your device has a browser and a keyboard, then this isn't the OAuth flow you are looking for.

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Changes

`response_type` removed from the Device Authorization Endpoint.

NB. The Device Authorization Endpoint != OAuth Authorization Endpoint

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Changes

Specified a standard way to include the user code in the verification URI. For example:

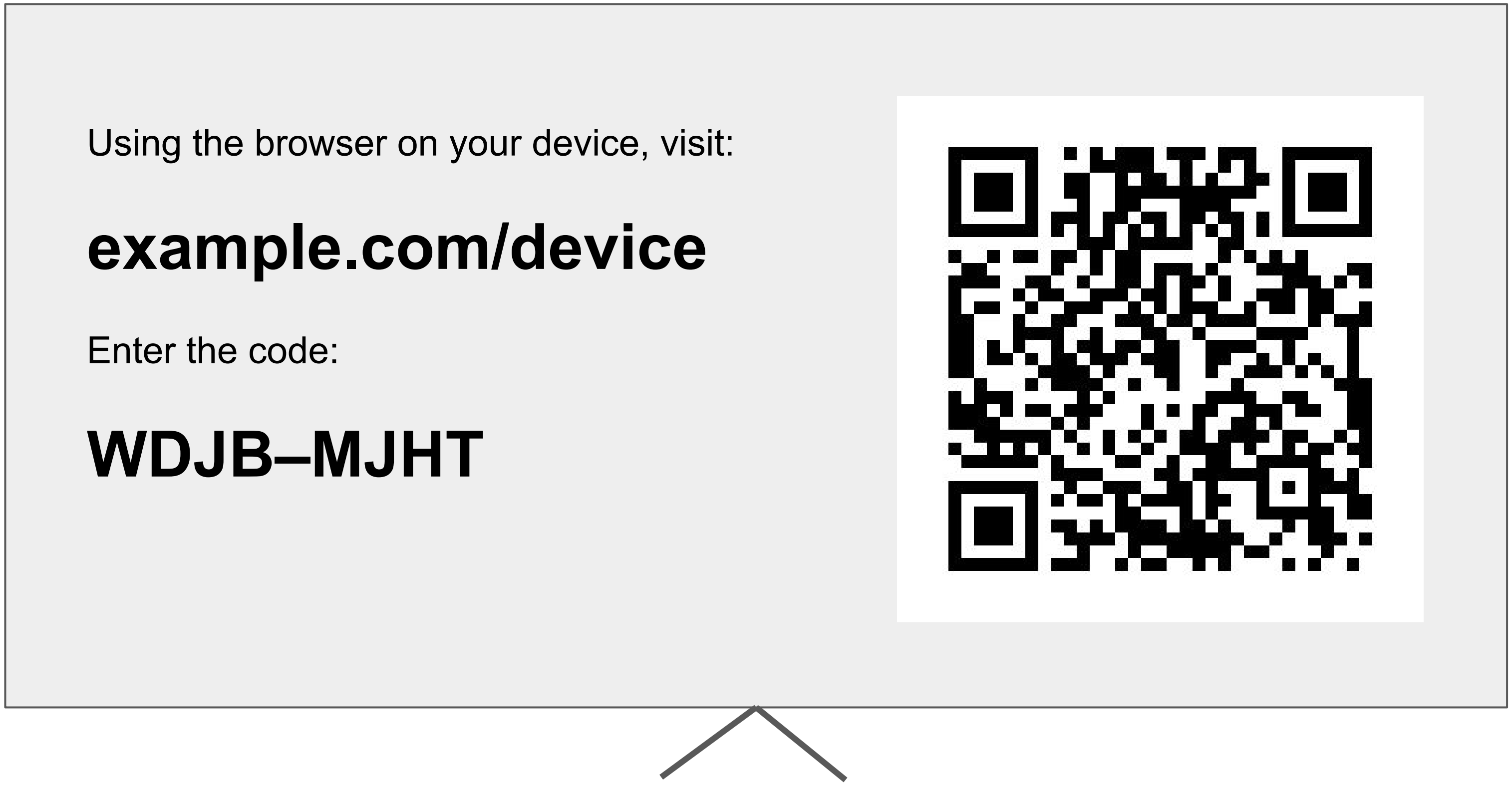
https://example.com/device?user_code=WDJB–MJHT

Optional enhancement, clients MUST still display the user_code.

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Example



Using the browser on your device, visit:

example.com/device

Enter the code:

WDJB–MJHT

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Changes

Security Considerations:

- User Code Brute Forcing
- Device Trustworthiness
- Remote Phishing
- Non-confidential Clients
- Non-Visual Code Transmission

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Changes

OAuth 2.0 Authorization Server Metadata

`device_authorization_endpoint`

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Clarification

Device authorization tokens should expire.

e.g. after 30 minutes

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Running Code – Google

Google's AS already supports the `urn:ietf…` grant type.

Never supported the now removed `response_type`.

No plans to support optional feature of including user code in the verification URI.

Only one non-compliant aspect with this draft: "`code`" rather than "`device_code`" on the token endpoint.

Example: https://youtube.com/tv

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Running Code

Open source server implementation:

MITREid 1.3 (coming soon, 1-2 weeks)

https://github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05

OAuth 2.0 Device Flow

Running Code

Open source, but Google-specific client example:

https://github.com/google/GTMAppAuth/tree/master/Example-tvOS

Code will be moved to the AppAuth for iOS, macOS (and tvOS!) project once the spec is stable.

OAuth 2.0 Device Flow

Questions?

https://tools.ietf.org/html/draft-ietf-oauth-device-flow-05