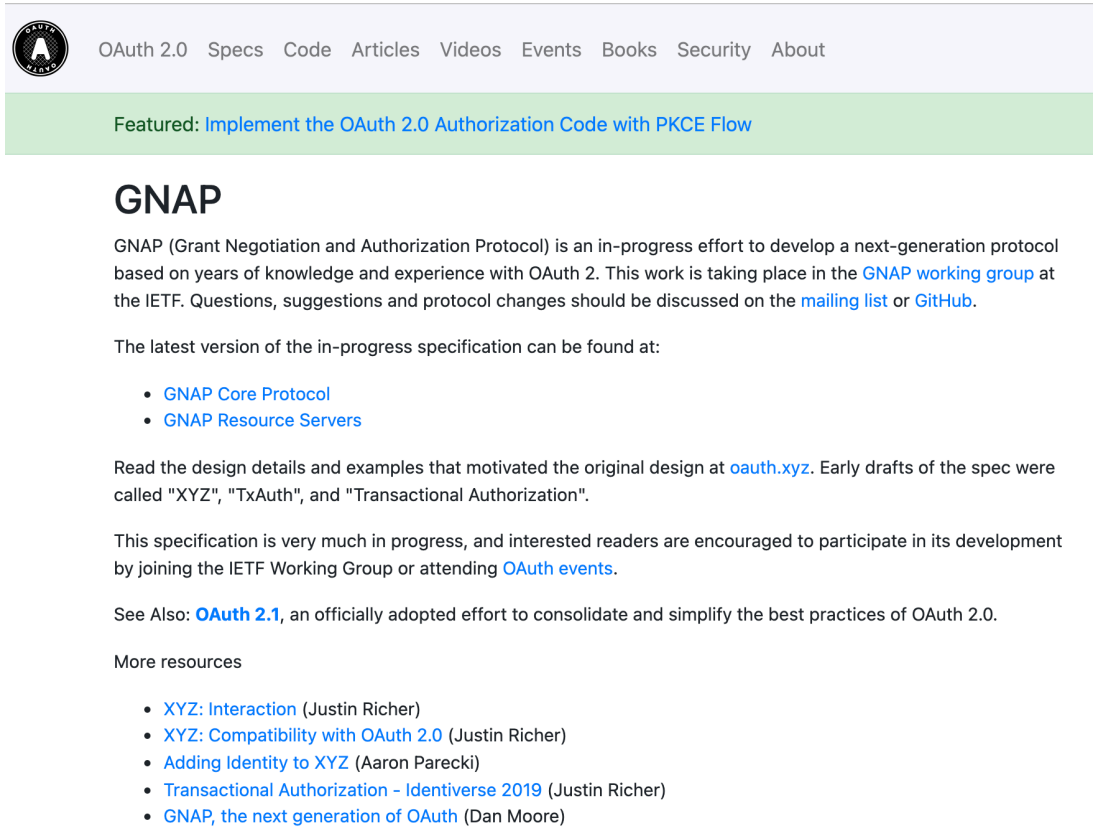
GNAP 超入門

- 伊東 諒
  - OpenID ファウンデーション・ジャパン
  - 株式会社ミクシィ

Grant Negotiation and Authorization Protocol



OAuth 2.0 Specs Code Articles Videos Events Books Security About

Featured: Implement the OAuth 2.0 Authorization Code with PKCE Flow

GNAP

GNAP (Grant Negotiation and Authorization Protocol) is an in-progress effort to develop a next-generation protocol based on years of knowledge and experience with OAuth 2. This work is taking place in the GNAP working group at the IETF. Questions, suggestions and protocol changes should be discussed on the mailing list or GitHub.

The latest version of the in-progress specification can be found at:

- GNAP Core Protocol
- GNAP Resource Servers

Read the design details and examples that motivated the original design at oauth.xyz. Early drafts of the spec were called "XYZ", "TxAuth", and "Transactional Authorization".

This specification is very much in progress, and interested readers are encouraged to participate in its development by joining the IETF Working Group or attending OAuth events.

See Also: **OAuth 2.1**, an officially adopted effort to consolidate and simplify the best practices of OAuth 2.0.

More resources

- XYZ: Interaction (Justin Richer)
- XYZ: Compatibility with OAuth 2.0 (Justin Richer)
- Adding Identity to XYZ (Aaron Parecki)
- Transactional Authorization - Identiverse 2019 (Justin Richer)
- GNAP, the next generation of OAuth (Dan Moore)

- OAuth 2.0の長年の経験とナレッジをベースとした次世代プロトコルを開発するための取り組み
- 現在策定中の仕様は2つ(IETF GNAP WG)
- ~~10分で解説するのはむr~~

本日の内容

- 現時点のGNAP概要
- OAuth 2.0との違い

策定中の仕様

- **Grant Negotiation and Authorization Protocol (Draft.08)**
  - **https://datatracker.ietf.org/doc/html/draft-ietf-gnap-core-protocol**
- Grant Negotiation and Authorization Protocol Resource Server Connections (Draft.01)
  - https://datatracker.ietf.org/doc/html/draft-ietf-gnap-resource-servers

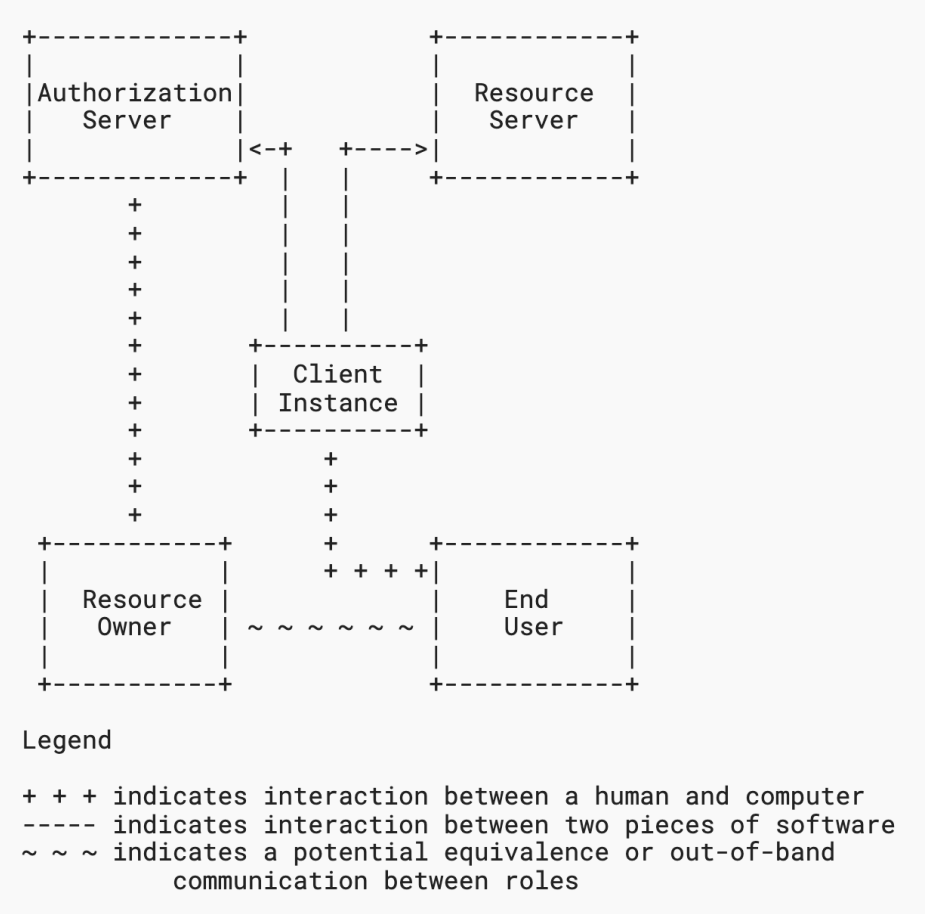
Table of Contents

Grant Negotiation and Authorization Protocol

Introduction

- This specification focuses on the portions of the delegation process facing the client instance. In particular, **this specification defines interoperable methods for a client instance to request, negotiate, and receive access to information facilitated by the authorization server.**
- The focus of this protocol is **to provide interoperability between the different parties acting in each role**, and is not to specify implementation details of each.

Roles



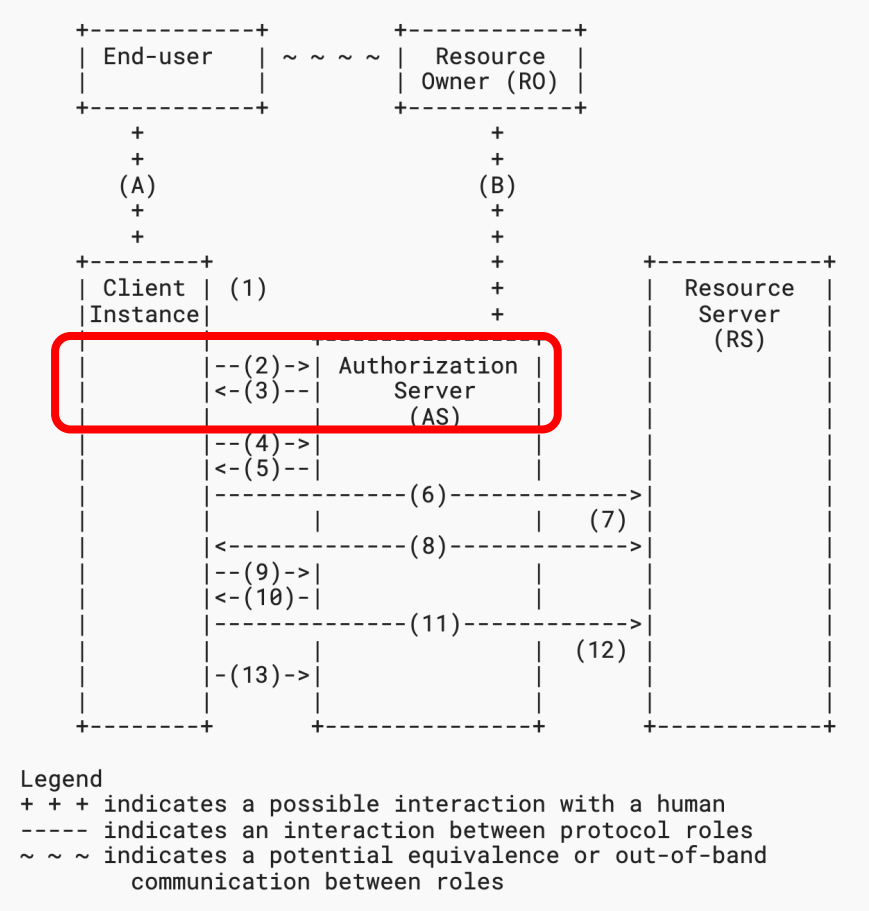
- Authorization Server (AS)
- Client
- Resource Server (RS)
- Resource Owner (RO)
- End User
  - クライアントを操作する人
  - **必ずしもROと同一ではない**

Trust relationships

GNAPの実装/運用にあたり重要になる信頼関係について、仕様内で言及されている

- **End User / RO** : 両者が異なる場合、
- **End User / Client** : Webアプリ、IoTデバイスなどの違い
- **End User / AS** : ブラウザなどでの対話
- **Client / AS** :
- **RS / RO** : 同意
- **AS / RS** : トークンのやりとりなど

Sequences



最初のClient/AS間のやりとりでその後のInteractionが決まる

- **Redirect-based Interaction** (≒AuthZ Code Grarnt)
- **User-code Interaction** (≒Device AuthZ Grant)
- **Asynchronous Authorization** (≒CIBA)
- **Software-only Authorization** (≒Client Cred Grant)
- **Refreshing an Expired Access Token** (≒Refresh Token)
- **Requesting User Information** (≒OIDC)

OAuth 2.0(2.1?) & GNAP

- 互換性：なし
- 対象となるユースケース
  - 重複する
  - OAuth 2.0で解決できない、複雑になってしまう課題への対応
- 移行
  - 考慮すべき点(client_id, AuthZ Request)について記載あり

OAuth 2.0との違い

- **Consent and authorization flexibility :** 柔軟で拡張可能なインタラクション定義
- **Intent registration and inline negotiation :** 共通のリクエストから必要に応じた処理の分岐
- **Client instances :** ClientID から key へ
- **Expanded delegation :** より構造化されたアクセス要求
- **Cryptography-based security :** Bearer Secretからの脱却
- **Privacy and usable security :** AS/RSの強力なBindからの解放

最新情報

- **IETF GNAP WG**
  - https://tools.ietf.org/wg/gnap/
- **Mailing List**
  - https://www.ietf.org/mailman/listinfo/txauth
- **GitHub Repository**
  - https://github.com/ietf-wg-gnap/gnap-core-protocol