HITACHI
Inspire the Next

Keycloak: The Open-Source IAM for Modern Applications
Part2: Conformance to API security profiles

Apr 19, 2023

Yuichi Nakamura
Hitachi, Ltd.

Self Introduction

HITACHI
Inspire the Next

Yuichi Nakamura, Ph.D.
Hitachi, Ltd. Director

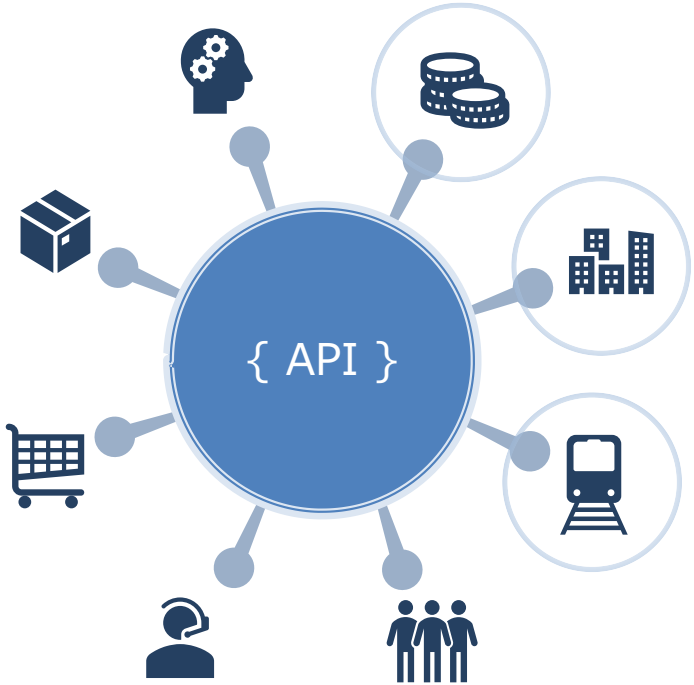
- Past: OSS activities around SELinux
  - Improvement of SELinux for embedded devices, and contribution to communities
  - Development of SELinux policy configuration tool as OSS (SELinux Policy Editor)
  - Presentations at various conferences (Ottawa Linux Symposium, CE Linux Forum, USENIX LISA etc.)
  - Academic papers, book about SELinux

- Now
  - A Board member of the Linux Foundation
  - Leading Keycloak consulting/contribution team in Hitachi
    - I am not a maintainer of Keycloak
    - Wrote Japanese Book about Keycloak
    - A Keycloak maintainer Takashi Norimatsu belongs to my team
      - He is leading development related to conformance to standards

Background: APIs everywhere

HITACHI
Inspire the Next

API is an interface for a service, currently REST API is widely used. APIs are opened to other applications and services as a trend of digital transformation.



Finance

OpenAPI is being enforced or strongly recommended by law in many countries.

Public

Services of governments and local governments are opening APIs. APIs are used by applications by 3rd party.

Industry

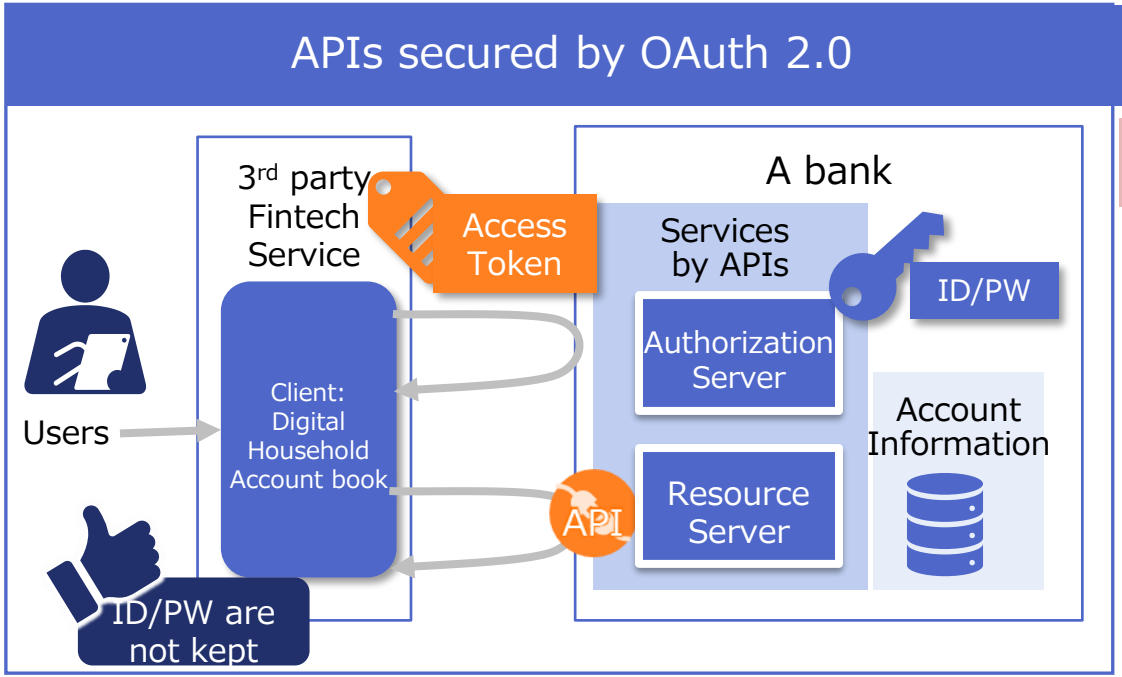
APIs are essential part of digital services as interfaces for 3rd party and mobile applications.

Moreover, API economy is being created among parties in different sectors.

Background: Security risks in API area

HITACHI
Inspire the Next

Security must be considered for APIs because they are opened to the Internet. As a first step of security, authorization is necessary. OAuth 2.0 is a de-facto standard of authorization of APIs. However, there are risks when we use the OAuth 2.0 improperly.



Example of risks

Leakage of access token
Replay attack, CSRF attack

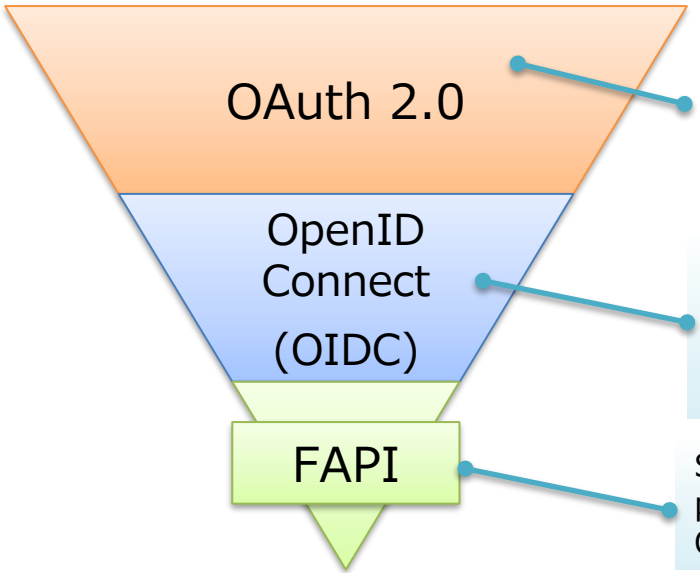
High-level security is required

APIs handling asset of users
APIs handling personal information

Toward high-level API security

HITACHI
Inspire the Next

For high-level API security, a specification called FAPI security profile is getting attention globally. FAPI is security profile describing secure usage of OAuth 2.0 and OpenID Connect(OIDC).



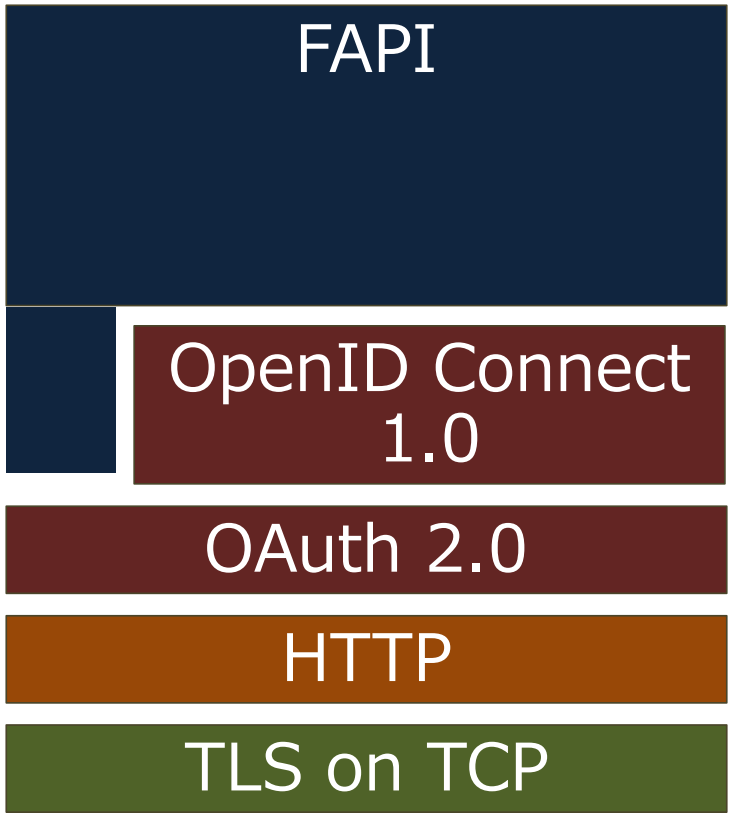
Specification for authorization by access token. It is a framework of authorization, but improper implementation often leads to vulnerabilities.

Some secure usage of OAuth 2.0 is introduced and OIDC can be used for authentication by ID token. However, improper implementation is still not restricted.

Secure usage of OAuth/OIDC is described across the protocol flow, including usage of optional specification of OAuth(e.g. PKCE) and lower layer protocol (SSL/TLS) usage.

Requirements specified by FAPI

HITACHI
Inspire the Next



[Main requirements]

* Usage of Proof Key for Code Exchange(PKCE)
* Holder-of-Key Token for access token by MTLS
* s_hash,c_hash parameter for authorization response
* Limiting signature/crypto algorithms

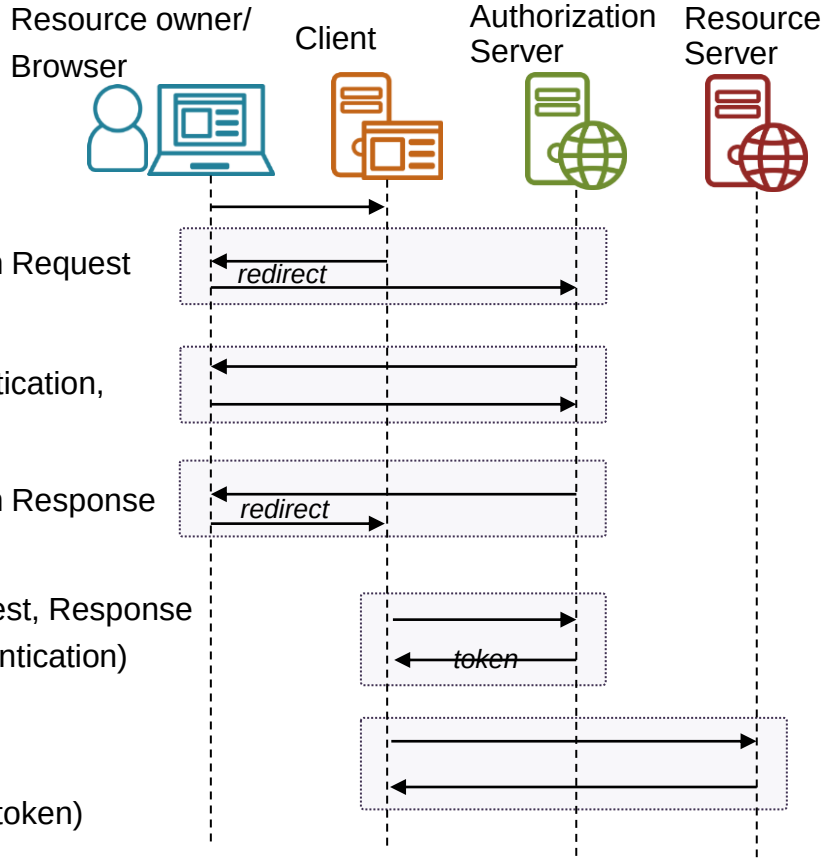
* Usage of signed Request Object
* Usage of nonce parameter for authorization request
* Usage of Hybrid Flow, ID token is used as a signature

* Usage of state parameter for authorization request

* Limitation of scheme(only HTTPS)、HTTP Strict Transport Security

* Limitation of version (1.2 or later)、Limitation of Cipher Suite、usage of RFC 6125

Sequence to call API using FAPI



[Step]

1. Authorization Request
2. User Authentication, Consent
3. Authorization Response
4. Token Request, Response
   (Client Authentication)
5. API call
   (with access token)

[Security checks specified in FAPI]

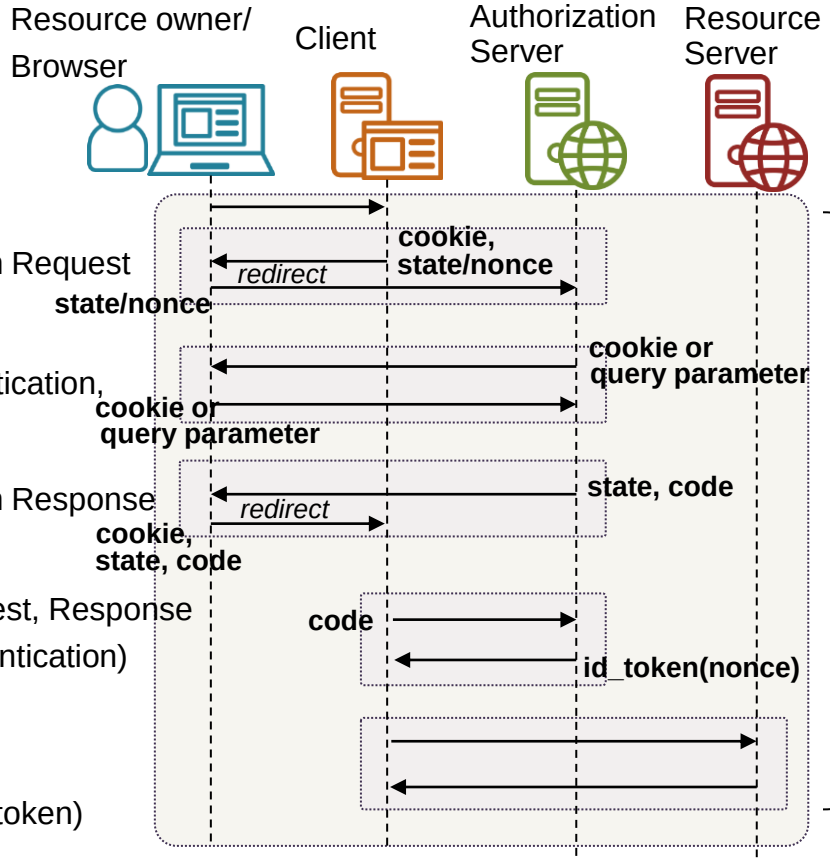
* Authorization request is not tampered/replayed
* Legitimate client generated the authorization request

* User is authenticated to an appropriate Level of Assurance
* Response is not tampered/replayed
* Legitimate server generated the response

* Sender of the request is the client who received authorization response

* Client is authenticated by appropriate way(not by client id/secret)
* Sender of the token is the client who received the token in the token request

Sequence to call API using FAPI



[Security checks specified in FAPI among steps]

- Each HTTP request/response belongs to one logical session

Various API security profiles

HITACHI
Inspire the Next

- There are various security profiles related to FAPI, they are not stable, often updated.
- Conformance tests and certification program are provided by OpenID Foundation, To prove compliance, it is important to pass conformance tests.

■ FAPI 1.0 family : specified by OpenID Foundation

- Financial-grade API Security Profile 1.0 - Part 1: Baseline
- Financial-grade API Security Profile 1.0 - Part 2: Advanced
- Financial-grade API: JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)
- Financial-grade API: Client Initiated Backchannel Authentication Profile (FAPI-CIBA)

■ Security profiles based on FAPI, specified by organizations in various countries

[UK : OpenBanking]

- OpenBanking Financial Grade API (FAPI) Profile
- OpenBanking CIBA Profile

[Australia : Consumer Data Right (CDR)]

- Consumer Data Right Security Profile

[Brazil : Open Banking Brasil]

- Open Banking Brasil Financial-grade API Security Profile
- Open Banking Brasil Financial-grade API Dynamic Client Registration

Collaboration: FAPI-SIG in Keycloak community

HITACHI
Inspire the Next

It is difficult to implement security profiles ...

- There are a lot of specifications to support security profiles.
- Specifications and conformance tests are often updated.
- Configuring Keycloak for security profiles is not easy.

Some people were interested in security profiles,
to accelerate collaboration FAPI-SIG was launched in Keycloak community in Aug 2020.
My colleague Takashi Norimatsu is leading.

- github - keycloak/kc-sig-fapi - https://github.com/keycloak/kc-sig-fapi
- Bi-weekly or Monthly webconf

Everyone can join and contribute !

Achievements of FAPI-SIG

HITACHI
Inspire the Next

In FAPI-SIG, development of features required for conformance to security profiles has been promoted.

<keycloak 13>

- Client Initiated Backchannel Authentication (CIBA) poll mode

<keycloak 14>

- FAPI 1.0 Baseline Security Profile
- FAPI 1.0 Advanced Security Profile
- Client Policies (Configuration framework)

<keycloak 15>

- Client Initiated Backchannel Authentication (CIBA) ping mode
- FAPI Client Initiated Backchannel Authentication Profile (FAPI-CIBA)
- FAPI JWT Secured Authorization Response Mode for OAuth 2.0 (JARM)
- OAuth 2.0 Pushed Authorization Requests (PAR)
- Brazil : Open Banking Brasil Financial-grade API Security Profile

Achievements of FAPI-SIG

HITACHI
Inspire the Next

- In order to prove conformance to security profiles, it is effective to pass conformance tests provided from OpenID Foundation. However, setting up environment and running tests in every version up of Keycloak is very hard work.We developed conformance test execution environment for Keycloak using Docker containers.

- Recent Keycloak can pass major conformance tests.

Keycloak version	FAPI 1.0 Advanced	FAPI-CIBA	Open Banking Brasil FAPI 1.0 (*1)	Open Finance Brasil FAPI 1.0 (*2,*3)	Australia Consumer Data Right (CDR)	UK Open Banking	OpenID Connect OP (*4)	OpenID Connect OP for Logout Profile
15.0.2	x	x	x	-	x	-	-	-
17.0.0	x	x	x	-	x	-	-	-
17.0.0-legacy	x	x	x	-	x	-	-	-
⋮								
20.0.0	x	x	x	x	x	x	x	x
20.0.1	x	x	x	x	x	x	x	x

Results are also available at https://github.com/keycloak/kc-sig-fapi

Contribution is welcomed

HITACHI
Inspire the Next

- API security profiles are evolving, Keycloak also should catch up the latest standards.
  - OIDC4IDA, FAPI 2.0, OAuth 2.1 etc…
- If you are interested in API security profiles for Keycloak, let's join FAPI-SIG meeting. Meeting schedule is announced in Keycloak-dev mailing list.
  https://groups.google.com/forum/#!topic/keycloak-dev/Ck_1i5LHFrE

Trademarks

- OpenID is a trademark or registered trademark of OpenID Foundation in the United States and other countries.
- Red Hat is trademark of Red Hat, Inc., registered in the United States and other countries.
- Other brand names and product names used in this material are trademarks, registered trademarks, or trade names of their respective holders.


Hitachi Social Innovation is
POWERING GOOD