

OpenID Certification Conformance Test ことはじめ

(苦労したこと、苦労しないために知っておきたいこと)

株式会社オージス総研

サービス事業本部 テミストラクトソリューション部

氏縄 武尊

自己紹介

氏縄 武尊(Ujinawa Takeru)



Work

株式会社オージス総研

テミストラクトソリューション部 3年目

ID管理・認証周りの開発

OpenID Connect, AWS



Private

滋賀県彦根市 出身

Twitter: @uji52

私の仕事 : ThemisStruct (テミストラクト)



ThemisStruct
テミストラクト

つくってます



ThemisStruct-WAM
テミストラクト

シングルサインオン
認証基盤

ThemisStruct-IDM
テミストラクト

ID管理

ThemisStruct-CM
テミストラクト

電子証明書発行・管理

IdentityPlatform AWS
対応版

サーバーレスで動く
統合認証基盤

Conformance Test

苦勞したポイント

Conformance Testの画面

Implicit, Hybrid] (OP-redirect_uri-NotP...

Discovery

-  Publishes openid-configuration di

Dynamic] (OP-Discovery-Config) ⓘ

  Keys in OP JWKs well formed [C

JWKs) ⓘ

-  Verify that claims_supported is published [Config, Dynamic] (OP

Discovery-claims_supported)

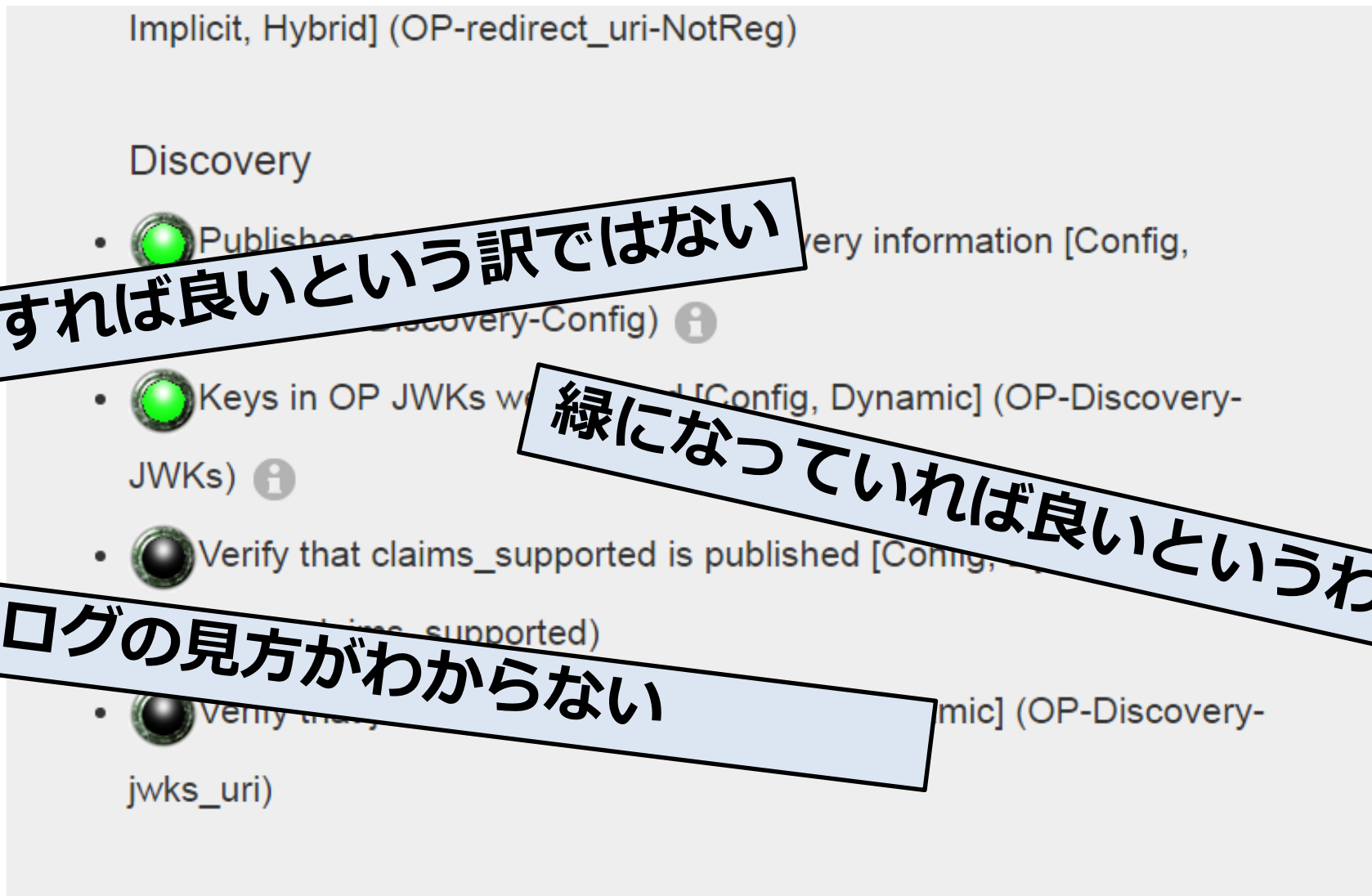
-  Verify that jwks_uri is published [Config, Dynamic] (OP-Discovery-

Legends

	The test has not be run
	Success
	Warning, something was not as expected
	Failed
	The test flow wasn't completed. This may have been expected or not
	Signals the fact that there are trace information available for the test

ボタンを押したらテストが走る
詳細なログも見られる→理解できれば修正も簡単

Conformance Testの画面



Conformance Testの画面

全部緑にすれば良いという訳ではない

**テスト自体は
事前知識があれば案外簡単**

ログの見方がわからない

わけでも無い

□ テストの進め方

- テスト項目の確認
- ログの確認方法・読み方

□ 失敗が分かりにくいテストケース

- 実例を挙げながらデモ形式で紹介

デモ

Conformance Testのコツ

□ テストケース毎に期待される結果を知る

- 既にCertifiedなOPのログを見る
- Conformance Profilesと実行ログをよく読む

□ ログとスペックを見比べて修正する

- リクエスト・レスポンス共に実行ログに出ている
- 不正な値の場合は大体スペックにそれっぽい記載がある

ご清聴ありがとうございました



ThemiStruct
テミストラクト

【お問い合わせ先】

株式会社オージス総研

TEL: 03-6712-1201 / 06-6871-7998

mail: info@ogis-ri.co.jp



Appendix(デモ中の画面)

テスト項目

[Home](#) » [OpenID Certification](#)

OpenID Certification

The OpenID Foundation enables implementations of [OpenID Connect](#) to be certified to specific conformance profiles to promote interoperability among implementations. The foundation's certification process utilizes self-certification and a conformance test suite developed by the foundation. Certified implementations can use the "OpenID Certified" certification mark. These resources are available to those considering or seeking certification:



- [OpenID Certification Frequently Asked Questions \(FAQ\)](#)
- [OpenID Connect Conformance Profiles](#)
- [OpenID Certification Terms and Conditions](#)
- [OpenID Certification of Conformance](#)
- [Attestation Statement \(used with Dynamic Client Registration\)](#)
- [How to run conformance tests and gather data](#)
- [How to request certification after successfully completing conformance testing for OPs](#)
- [How to run conformance tests and gather data demonstrating conformance for RPs \(in pilot phase\)](#)

認定されたConformance Profile
Conformance Testのログがダウンロードできる

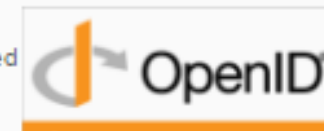
These implementations have been granted certifications for these conformance profiles:

Organization	Implementation	OP Basic	OP Implicit	OP Hybrid	OP Config	OP Dynamic
OGIS-RI	ThemiStruct Identity Platform v1.1.0	7-Oct-2016	7-Oct-2016		7-Oct-2016	
Dominick Baier & Brock Allen	IdentityServer3 v1.6			8-May-2015	8-May-2015	8-May-2015

[Home](#) » [OpenID Certification](#)

OpenID Certification

The OpenID Foundation enables implementations of **OpenID Connect** to be certified to specific conformance profiles to promote interoperability among implementations. The foundation's certification process utilizes self-certification and a conformance test suite developed by the foundation. Certified implementations can use the "OpenID Certified" certification mark. These resources are available to those considering or seeking certification:



- [OpenID Certification Frequently Asked Questions \(FAQ\)](#)
- [OpenID Connect Conformance Profiles](#)
- [OpenID Certification Terms and Conditions](#)
- [OpenID Certification of Conformance \(docx\) \(PDF\)](#)
- [Attestation Statement \(used with Dynamic OP profile only\) \(docx\) \(PDF\)](#)
- [How to run conformance](#)
- [How to request certification](#)
- [How to run conformance](#)
- [How to request certification](#)
- [OpenID Certified Mark](#)

Conformance Profileの確認ができる資料

These implementations have been granted certifications for these conformance profiles:

Organization		Implementation	OP Basic	OP Implicit	OP Hybrid	OP Config	OP Dynamic
Auth0		Auth0	24-May-2016			24-May-2016	
Dominick Baier & Brock Allen		IdentityServer3 v1.6	8-May-2015	8-May-2015	8-May-2015	8-May-2015	

3.1 OpenID Provider Conformance Profile Definitions

The following table specifies the protocol features included in the OpenID Provider conformance profiles defined above. It also lists the tests in the OpenID Provider test suite at <http://op.certification.openid.net/> that are used to test those features.

Conformance Feature Information			OP Conformance Profile			
Feature Name	Conformance Test Name	Test ID	Basic	Implicit	Hybrid	Full
Response Type & Response Mode						
Support code response_type	Request with response_type=code	OP-Response-code	y			
Support id_token response_type	Request with response_type=id_token	OP-Response-id_token		y		
Support id_token token response_type	Request with response_type=id_token token	OP-Response-id_token+token		y		
Support code id_token response_type	Request with response_type=code id_token	OP-Response-code+id_token			y	
Support code id_token token response_type	Request with response_type=code id_token token	OP-Response-code+id_token+token			y	

Conformance Profile毎に要求されるテストの内容

reached	restriction				
Ignore param Request	no err や SHOULD 等の要求もあることを頭に入れておく				
Support id_token_hint request parameter	Using prompt=none with user hint through id_token_hint	OP-Req-id_token_hint	SHOULD	SHOULD	SHOULD
Support login_hint request parameter	Providing login_hint	OP-Req-login_hint	no err	no err	no err
Support ui_locales request parameter	Providing ui_locales	OP-Req-ui_locales	no err	no err	no err
Support claims_locales request parameter	Providing claims_locales	OP-Req-claims_locales	no err	no err	no err
Support acr_values request parameter	Providing acr_values	OP-Req-acr_values	no err	no err	no err
OAuth Behaviors					
OAuth state request value returned in response		VerifyState()	y	y	y
Reject second use of Authorization Code	Trying to use authorization code twice should result in an error	OP-OAuth-2nd	Warning if under 30s		Warning if under 30s

事前準備

テストインスタンスの作成

<https://openid.net/certification/testing/>

OpenID® The Internet Identity Layer

OpenID Foundation - Current Working Groups - Specs & Dev Info - **OpenID® Certification** - OpenID Connect FAQ and Q&As

Home » [OpenID Certification](#) » Conformance Testing for OPs

Conformance Testing for OPs

This page describes how to run conformance tests and gather testing results.

Establishing Your Testing Configuration

The first step in using the OpenID Provider tests is to decide which conformance profiles you plan to test. Then you establish a testing configuration on the host op.certification.openid.net. You can do this in a self-service manner at <https://op.certification.openid.net:60000/>. If you have problems establishing your configuration, contact Roland Hedberg at roland.hedberg@umu.se.

Most OPs will test the Basic profile and many will also test the Implicit and Hybrid profiles. You can switch between the response_type values that these profiles use dynamically while testing.

Most OPs will also test the Config profile, which tests your discovery information published at your .well-known/openid-configuration endpoint. You can't switch whether to test this while testing, so you need to decide whether to do this up front.

Some OPs
You can't s

Most OPs w
Basic profile
dynamically

You need t
ui_locales -
WebFinger

Completing your configuration will give you a testing site using a port allocated for your use on op.certification.openid.net. Your testing site will be at a URL like <https://op.certification.openid.net:61234/>, but with a different port number.

Running Tests and Viewing Results

Search for:

Search

News Archives

News Archives

Select Month ▼

Categories

Categories

Select Category ▼

Recent Posts

Services

- Registration Open for OpenID Foundation Workshop on

OpenID Connect Provider Certification

This is a tool used for testing the compliance of an OpenID Connect Provider with the OpenID Connect specifications. In order to start testing you need to configure a test instance. Enter the issuer URL to the OpenID Connect Provider you want to test.

Issuer URL

Next

(without .well-known):

Issuer URLの設定

<https://op.example.com/oidc/.well-known/openid-configuration>

↑ 赤い部分だけ(末尾の"/"はあってもなくてもOK)

Issuer URL

https://

Next

(without .well-known):

New test instance

Enter a ID for the new test instance. When configured the test instance will appear in a list above which will contain all existing test instances. It will then be possible to continue using an existing test instance later on or reconfigure it if needed.

technight

Create new configurations

Upload configuration

**Test InstanceIDを入力
作成が完了するとインスタンスの初期設定画面に遷移**

Issuer URL

https://a

Next

(without .well-known):

Existing test instances

Instance ID

Port

technight

{

✎ Reconfigu

⬇ Download

🔄 Restart

Go to test instance →

New test instance

Enter a ID for the new test instance. When configured the test instance will appear in a list

**既に登録されている場合
設定の修正やテスト画面に遷移できる**

初期設定(Provider)

OpenID Connect Provider Certification - Test Instance Configuration

Provider configuration

Client configuration

Provider configuration:

Does the OP have a .well-known/openid-configuration endpoint?

Well-knowエンドポイントの有無を確認 yes/no

OpenID Connect Provider Certification - Test Instance Configuration

Provider configuration

Client configuration

Provider configuration:

Does the OP have a .well-known/openid-configuration endpoint?

What is the issuer path for this

configuration information? *

* Required fields

Previous

Next

**<Issuer URL>/.well-known/openid-configuration
で設定が完了(yesの場合)**

OpenID Connect Provider Certification - Test Instance Configuration

Provider configuration

Client configuration

Provider configuration:

Does the OP have a .well-known/openid-configuration endpoint?

Add static provider metadata field

authorization_endpoint *

New element:

Added elements:

id_token_signing_alg_values_supported

Add

**それぞれの項目を選択して値を入力
(noの場合)**

Open
Inst

Prov

Pro

Does

Add

auth

id_to

Static metadata fields



Mark the fields you want to show on the config page

- ☐ acr_values_supported
- ☒ authorization_endpoint *
- ☐ check_session_iframe
- ☐ claim_types_supported
- ☐ claims_locales_supported
- ☐ claims_parameter_supported
- ☐ claims_supported
- ☐ display_values_supported

**表示する項目の指定
(noの場合)**

初期設定(Client)

OpenID Connect Provider Certification - Test Instance Configuration

Provider configuration

Client configuration

Client configuration:

Do the provider support dynamic client registration?

Which subject type do you want to use by default?

Which response type should be used by default?

**Dynamic Client Registrationがある場合(yes)
特に入力は不要**

features

☐ Encrypted JWT

OpenID Connect Provider Certification - Test Instance Configuration

Provider configuration

Client configuration

Client configuration:

Do the provider support dynamic client registration?

Redirect uris

Client id *

Client secret *

**Dynamic Client Registrationが無い場合(no)
Client ID/Secretを発行して入力 Redirect URIは提供される**

Client id *

Client secret *

* Required info

Which subject type do you want to use by default?: public ▼

Which response type should be used by default? code ▼

 Select

supported

features:

☐ JWT signed with "None" algorithm (Unsigned)

☒ JWT signed with algorithm other than "none"

☐ Encrypted JWT

**デフォルトのsubject typeとresponse typeを設定
対応しているJWTの形式を設定**

supported

☒ JWT signed with algorithm other than "none"

テスト用のrequest parameterを設定

1 Test specific request parameters:

i Login hint

E.g. bob@example.com

i UI locales

E.g. en se

i Claims locales

E.g. en se

i Acr values

E.g. 2 1

i Webfinger url

https://example.com/bob

i Webfinger

E.g. bob@example.com

email

Previous

Submit

supported

☒ JWT signed with algorithm other than "none"

feat

 T

 L

 U

 C

 A

 V

 V

email

Previous

Submit

Save configurations

The configuration information will now be stored on the server. Do you want to continue?

Note: If the configurations are stored and the test server starts correctly you will be redirected to the test server.

No

Yes

実際にテストする

You are testing using:

- Basic (code)
- Dynamic discovery
- Static registration
- crypto support ['sign']

**Conformance Test用のインスタンス
RPとして動いて動作を確認してくれる**

If you want to change this you can do it [here](#)

Chose the next test flow you want to run from this list:

Response Type & Response Mode

-  Authorization request missing the response_type parameter [Basic, Implicit, Hybrid] (OP-Response-Missing)
-  Request with response_type=code [Basic] (OP-Response-code)

Discovery

-  Publishes openid-configuration discovery information [Config, Dynamic] (OP-Discovery-Config)
-  Keys in OP JWKs well formed [Config, Dynamic] (OP-Discovery-JWKs)
-  Verify that claims_supported is published [Config, Dynamic] (OP-Discovery-claims_supported)
-  Verify that jwks_uri is published [Config, Dynamic] (OP-Discovery-jwks_uri)

**Discoveryのテストが一番シンプルなので
初めてのテストの場合はオススメ**

request_uri Request Parameter

Discovery

-  Publishes openid-configuration discovery information [Config, Dynamic] (OP-Discovery-Config) ⓘ
-  Keys in OP JWKs well formed [Config, Dynamic] (OP-Discovery-JWKs) ⓘ
-  Verify that claims_supported is published [Config, Dynamic] (OP-Discovery-claims_supported) ⓘ
-  Verify that jwks_uri is published [Config, Dynamic] (OP-Discovery-jwks_uri) ⓘ

正常に動作すると緑になる
(※全部緑にするのが目的じゃないことに再度注意)

request_uri Request Parameter

Discovery

-  Publishes openid-configuration discovery information [Config, Dynamic] (OP-Discovery-Config) 
-  Keys in OP JWKs well formed [Config, Dynamic] (OP-Discovery-JWKs) 
-  Verify that claims_supported is published [Config, Dynamic] (OP-Discovery-claims_supported) 
-  Verify that jwks_uri is published [Config, Dynamic] (OP-Discovery-jwks_uri) 

このボタンを押すことでログが確認できる

request_uri Request Parameter

Test info

テストの情報(実行時間・テスト名等)

Profile: {'openid-configuration': 'config', 'response_type': 'code', 'crypto': 'sign', 'registration': 'static'}

Timestamp: 2016-12-12T08:42:08Z

Test description: Publishes openid-configuration discovery information [Config, Dynamic]

Test ID: OP-Discovery-Config

Issuer: https://a

Test output

テスト項目毎の結果一覧

__After completing the test flow:__

[check-http-response]

status: OK

description: Checks that the HTTP response status is within the 200 or 300 range

__X:==== END ====__

Trace output


```
0.000323 ----- DiscoveryRequest -----
0.000336 Provider info discover from 'https://[REDACTED]'
0.000342 --> URL: https://[REDACTED].well-known/openid-configuration
1.020230 ProviderConfigurationResponse: {
  "acr_values_supported": [
    "default"
  ],
  "authorization_endpoint": "https://[REDACTED]",
  "claims_parameter_supported": false,
  "claims_supported": [
    "email",
    "familyName",
    "givenName"
  ],
  "end_session_endpoint": "https://[REDACTED]",
  "grant_types_supported": [
    "authorization_code",
    "implicit"
  ],
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "issuer": "https://[REDACTED]",
  "jwks_uri": "https://[REDACTED]/.well-known/openid-configuration"
}
```

```
  ],
  "subject_types_supported": [
    "public"
  ],
  "token_endpoint": "https://[REDACTED]",
  "token_endpoint_auth_methods_supported": [
    "client_secret_basic",
    "client_secret_post"
  ],
  "userinfo_endpoint": "https://[REDACTED]",
  "version": "3.0"
}
1.999861 JWKS: {
  "keys": [
    {
      "alg": "RS256",
      "e": "AQAB",
      "kid": "FjZ6rLZ6SgF8jairlWgsyzkIY3gPcRTdoKDgxVZEx8Q",
      "kty": "RSA",
      "n": "OM9oijhWgV0iZZejFgeu5SdXC2SgA4hMGX8C_ET14-Lh3E2eWBPfjor3ST9T_cEgHiakRf3HovekA97dqpFR6Zo6NxVrwUyTt52aSUuLHoM1p",
      "use": "sig"
    }
  ]
}
2.012045 ==== END ====
```

Result

PASSED

テストの成否

実際のテスト

実際に叩いてみるテスト

□ OP-Discovery-Config

- Well-knownを実際に叩いてみる

□ OP-Discovery-JWKs

- Base64urlエンコード部分で実際にエラーを解消してみる

□ OP-Response-code

- 複数のエラーケースが存在する場合をしてみる

□ OP-scope-email, phone

- no errで良いケースをしてみる

□ OP-redirect_uri-NotReg

- レスポンスが返ってこないケースをしてみる

□ Well-knownエンドポイントを叩いて
実際にログを見してみる

➤ 結果は40-42ページの通り

□ Well-knownの後にjwks_uriを叩く テスト

- Base64urlエンコードしたkeyを返却すべき
- Base64エンコードで実装したものを修正する

Test output

(修正前)Base64エンコードしたkeyを返却

```
__After completing the test flow:__  
[verify-base64url]  
  status: ERROR  
  description: Verifies that the base64 encoded parts of a JWK is in fact base64url encoded and not just base64 encoded  
  info: 'n' not base64url encoded in key with kid 'FjZ6rLZ6SgF8jairIWgsyzkIY3gPcRTdoKDgxVZEx8Q'  
[check-http-response]  
  status: OK  
  description: Checks that the HTTP response status is within the 200 or 300 range  
__X:==== END ====__
```

Test output

(修正後)Base64urlエンコードしたkeyを返却

```
__After completing the test flow:__  
[verify-base64url]  
  status: OK  
  description: Verifies that the base64 encoded parts of a JWK is in fact base64url encoded and not just base64 encoded  
[check-http-response]  
  status: OK  
  description: Checks that the HTTP response status is within the 200 or 300 range  
__X:==== END ====__
```

□ エラー返却のパターンが2通り

(どちらで対応しても良い)

1. エラーをRPに返却する

- エラーレスポンスの形式をしっかりと守ること

2. End-Userにエラー画面を返す(スクショ必須)

- 他のOPのCertification結果が見れるので参考に

OpenID Certification OP Test

There are two acceptable outcomes: (1) returning an error response to the RP or (2) returning an error message to the End-User. In case (2), you must submit a screen shot of the error shown as part of your certification application.

To continue click this [link](#).

**(1)エラーをRPに送る or (2)End-Userにエラー画面を返す
(2)の場合はスクリーンショットも送ること**

エラーレスポンスがRPに返却されていることを確認

```
5.000487 ----- AuthorizationRequest -----
5.000952 --> URL: https://[REDACTED]?scope=openid&state=ziRdvRGA8QzCwID2&red
5.000961 --> BODY: None
5.509513 <-- error=invalid_request&error_description=response_type%20is%20not%20exists.&state=ziRdvRGA8QzCwID2
5.509862 AuthorizationErrorResponse: {
  "error": "invalid_request",
  "error_description": "response_type is not exists.",
  "state": "ziRdvRGA8QzCwID2"
}
5.510764 ==== END ====
```

Result

PASSED

□ OP-scope-email

- デモ環境で対応済みなScope

□ OP-scope-phone

- デモ環境では未対応なScope

こっち→

-  Scope requesting email claims [Basic, Implicit, Hybrid] (OP-scope-email) ⓘ
-  Scope requesting phone claims [Basic, Implicit, Hybrid] (OP-scope-phone) ⓘ

Test output

```
__AuthorizationRequest:pre__  
[check-response-type]  
    status: OK  
    description: Checks that the asked for response type are among the supported  
[check-endpoint]  
    status: OK  
    description: Checks that the necessary endpoint exists at a server  
__After completing the test flow:__  
[check-http-response]  
    status: OK  
    description: Checks that the HTTP response status is within the 200 or 300 range  
[verify-response]  
    status: OK  
    description: Checks that the last response was one of a possible set of OpenID Connect Responses  
[verify-scopes]  
    status: OK  
    description: Verifies that the claims corresponding to the requested scopes are returned  
__X:==== END ====__
```

こっち→

-  Scope requesting email claims [Basic, Implicit, Hybrid] (OP-scope-email) ⓘ
-  Scope requesting phone claims [Basic, Implicit, Hybrid] (OP-scope-phone) ⓘ

Test output

well-knownにてphone scopeが許可されていない

[-]

```
status: WARNING
info: OP is not supporting ['phone'] according to 'scopes_supported' in the provider configuration
__AuthorizationRequest:pre__
[check-response-type]
status: OK
description: Checks that the asked for response type are among the supported
[check-endpoint]
status: OK
description: Checks that the necessary endpoint exists at a server
__After completing the test flow:__
[check-http-response]
status: OK
description: Checks that the
[verify-response]
status: OK
description: Checks that the
[verify-scopes]
status: WARNING
description: Verifies that the claims corresponding to the requested scopes are returned
info: The following claims were missing from the returned information: ['phone_number', 'phone_number_verified']
__X:==== END ====__
```

**phone_number, phone_number_verified
が取得できない**

□ redirect_uriが間違っているケース

- レスポンスが無い状態でログが止まっている
- 結果はincompleteになる
- スクリーンショットを送る必要がある

OpenID Certification OP Test

This test should result in the OpenID Provider displaying an error message in your user agent. You should ignore the status of this test in the test tool, since it will be incomplete. You must submit a screen shot of the error shown as part of your certification application.

To continue click this [link](#).

To go back click this [link](#).

**ブラウザがエラー画面になっていることを確認
Conformance TestのStatusはIncompleteになる**

Incompleteになっている(正しい)

redirect_uri

-  Sent redirect_uri does not match a registered redirect_uri [Basic, Implicit, Hybrid] (OP-redirect_uri-NotReg) 

Test output

OKになっている

```
AuthorizationRequest:pre__  
[check-response-type]  
  status: OK  
  description: Checks that the asked for response type are among the supported  
[check-endpoint]  
  status: OK  
  description: Checks that the necessary endpoint exists at a server
```

レスポンスが返却されていないことを確認

```
}  
}  
21.154788 ----- AuthorizationRequest -----  
21.155223 --> URL: https://[redacted]?scope=openid&state=olr  
21.155232 --> BODY: None
```

Result

PARTIAL RESULT

ログの取得

<https://op.certification.openid.net:6xxxx/log>

OpenID Certification OP Test logs

A list of profiles that are saved on disk for this issuer:

- [code.config.static.sign](#) tar file: [Download logs](#)

OpenID Certification OP Test logs

A list of tests that are saved on disk for this profile:

- [OP-ClientAuth-Basic-Static](#)
- [OP-ClientAuth-SecretPost-Static](#)
- [OP-Discovery-Config](#)
- [OP-Discovery-JWKs](#)
- [OP-Discovery-claims supported](#)
- [OP-Discovery-jwks uri](#)
- [OP-IDToken-Signature](#)
- [OP-IDToken-kid](#)
- [OP-OAuth-2nd](#)
- [OP-OAuth-2nd-30s](#)
- [OP-OAuth-2nd-Revokes](#)
- [OP-Reg-NotUnderstood](#)
- [OP-Reg-acr values](#)
- [OP-Reg-claims locales](#)
- [OP-Reg-id token hint](#)
- [OP-Reg-login hint](#)
- [OP-Reg-max age=1](#)
- [OP-Reg-max age=10000](#)
- [OP-Reg-ui locales](#)
- [OP-Response-Missing](#)
- [OP-Response-code](#)
- [OP-UserInfo-Body](#)
- [OP-UserInfo-Endpoint](#)
- [OP-UserInfo-Header](#)
- [OP-claims-essential](#)