OpenID Connect Developer documentation

Introduction

Cleverbase offers IDentity Federation (IDF) through a HTTP interface based on the OpenID Connect specification.

Table of Contents

Hosts

Environment	Host
Pre-production	https://connect.acc.cleverbase.com
Production	https://connect.cleverbase.com

Client registration

Client registration is a manual process performed in collaboration with an account manager of Cleverbase. As input, the redirection URI(s) and client name (for displaying purposes) of the client is required. Client registration will lead to a confidential OAuth 2.0/ OpenID Connect Client with two parameters:

Parameter	Classification
OAuth 2.0 Client Identifier	Public Information
OAuth 2.0 Client Secret	Private information

This OAuth 2.0 Client can subsequently act as a client of the identity federation service of Cleverbase.

Technical specification

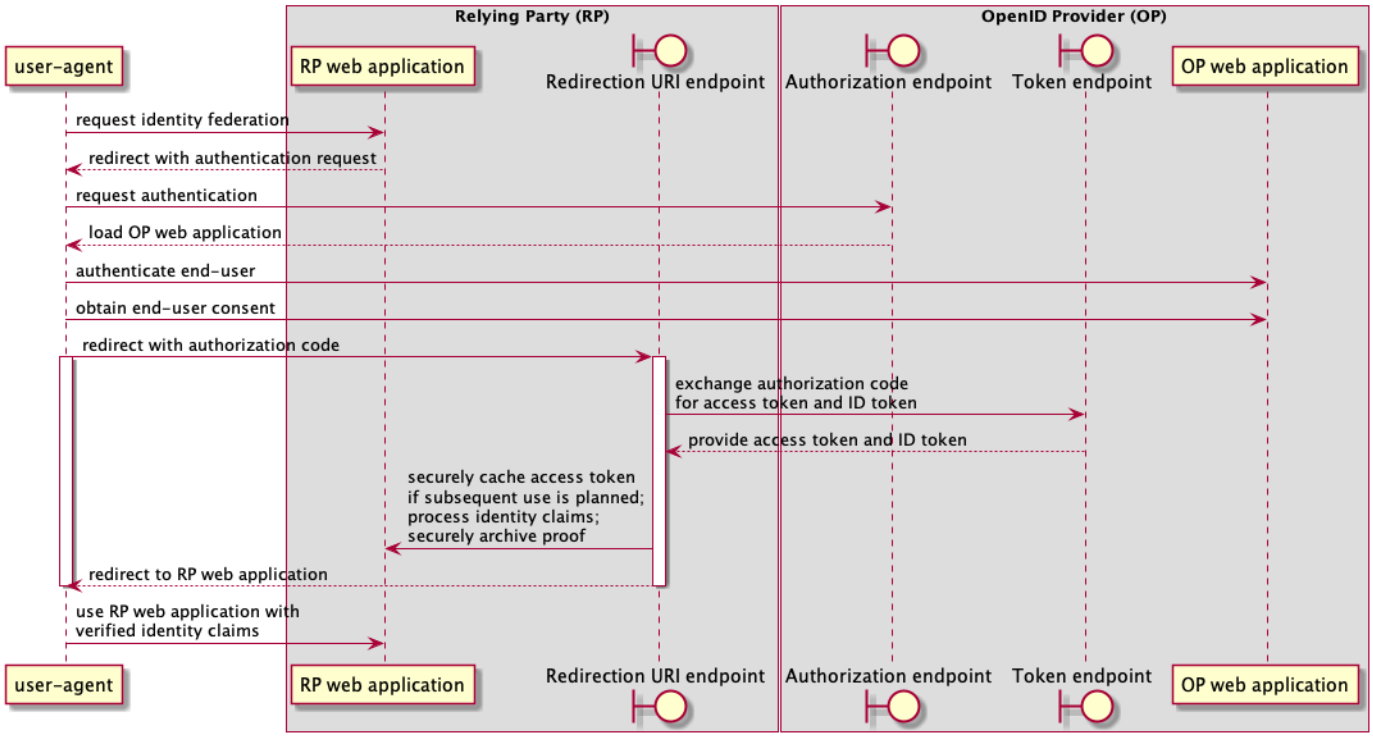
Framework

Cleverbase offers identity federation through an HTTP interface that complies with OpenID Connect Core 1.0 incorporating errata set 1 (OIDC), which complies to RFC 6749 The OAuth 2.0 Authorization Framework (OAuth 2.0). Relevant sections of the OIDC spec are: 1, 2, 3.1, 5, 8–10, 13–17.

Architecture

Cleverbase has the role of OpenID Provider towards organizations with the role of Relying Party.

Sequence diagram



Scopes and claims

See OIDC section 5 for full reference.

The OAuth 2.0 Client decides which claims to request. Currently, only requesting claims using scope values is supported. End-users may consent to a subset of requested claims, unless marked as essential claims.

The supported scopes and claims are:

Scope	Prescence	Claim	Description
openid	REQUIRED	sub	An identifier for the natural person. Can be correlated with subsequent requests by the relying party, for example to enable the end-user to log in back later to an previously created account.
com.cleverbase.proof	OPTIONAL	com.cleverbase.proof	A JSON array of JSON objects with id, content_type and base64_encoded_content fields. The content should be archived by the relying party and associated with the identifier and the provided content type. Example: `[ { "id": "consent", "content_type": "application/xml", "base64_encoded_content": "..." }, { "id": "assertion", "content_type": "application/xml", "base64_encoded_content": "..." } ]`
com.cleverbase.personal_info	OPTIONAL	given_name, com.cleverbase.last_name, birthdate, com.cleverbase.nationality, com.cleverbase.birthplace	Personal info of the end-user, as present in the identity document.

Scope	Prescence	Claim	Description
email	OPTIONAL	email, email_verified	End-user's preferred email address and if the email address is verified
com.cleverbase.id_number	OPTIONAL	com.cleverbase.id_number, com.cleverbase.document.type	Document number of the passport of id card used during registration and the type of document
com.cleverbase.authentication_certificate	OPTIONAL	com.cleverbase.authentication_certificate	The authentication certificate
com.cleverbase.signing_certificate	OPTIONAL	com.cleverbase.signing_certificate	The signing (content commitment) certificate
com.cleverbase.nl_brp_name	OPTIONAL	com.cleverbase.nl_brp_voornaam , com.cleverbase.nl_brp_voorvoegsel, com.cleverbase.nl_brp_geslachtsnaam, com.cleverbase.nl_brp_geslachtsnaam_zonder_voorvoegsel	Claim names based on BRP definitions

Requests

OAuth 2.0 Authorization endpoints

Cleverbase's Identity Federation service uses OAuth 2.0 for authorization.

GET /oauth2/authorize

- RFC 6749
- OpenID Connect

Description

Starts the OAuth 2.0 authorization server using an Authorization Code flow, as described in Section 1.3.1 of RFC 6749, to request authorization for the user to access the remote service resources. The authorization is returned in the form of an authorization code, which the signature application SHALL then use to obtain an access token with the oauth2/token method.

Input parameters

Parameter	Presence	Value	Description
response_type	REQUIRED	String	Must always be "code".
client_id	REQUIRED	String	unique Client Identifier.
redirect_uri	OPTIONAL	String	The URL to redirect to after the authorization process (defaults to registered redirect).
scope	REQUIRED	String	Space delimited string. Must contain "openid". May contain additional scopes like "com.cleverbase.proof" and "email".
state	REQUIRED	String	Up to 255 bytes of arbitrary data from the signature application that will be passed back to the redirect URI.
nonce	OPTIONAL	String	String value used to associate a Client session with an ID Token, and to mitigate replay attacks.

Response

Parameter	Presence	Value	Description
code	REQUIRED	String	The authorization code generated by the authorization server
state	REQUIRED	String	Should match state given in request
error	OPTIONAL	String	A single error code string
error_description	OPTIONAL	String	Human-readable text providing additional error information

Examples

Service Scope Request

In order to request authorization for the "openid" scope (login only):

```
GET /oauth2/authorize?
response_type=code&
client_id=<OAuth2_client_id>&
redirect_uri=<OAuth2_redirect_uri>&
scope=openid&
lang=en-US&
state=12345678&
nonce=54321
```

In order to request authorization for IDF scopes "openid email com.cleverbase.personal_info com.cleverbase.id_number":

```
GET /oauth2/authorize?
response_type=code&
client_id=<OAuth2_client_id>&
redirect_uri=<OAuth2_redirect_uri>&
scope=openid email com.cleverbase.personal_info com.cleverbase.id_number&
lang=en-US&
state=12345678&
nonce=54321
```

Service Scope Response

```
HTTP/1.1 302 Found
Location: <OAuth2_redirect_uri>?
code=FhkXf9P269L8g&
state=12345678
```

Error Response

```
HTTP/1.1 302 Found
Location: <OAuth2_redirect_uri>?error=invalid_request&
error_description=Invalid%20Authorization%20Code
```

POST /oauth2/token

- RFC 6749
- OpenID Connect

Description

Obtain an OAuth 2.0 bearer access token and id token from the authorization server by passing the authorization code returned by the authorization server after a successful user authentication, along with the used scope, the client ID and client secret in possession of the client application.

Input parameters

Parameter	Presence	Value	Description
grant_type	REQUIRED	String	Must always be "authorization_code"
code	REQUIRED	String	Code obtained from result oauth2/authorize
client_id	REQUIRED	String	Unique Client Identifier (see Prerequisites)
redirect_uri	REQUIRED	String	The URL where the user was redirected after the authorization process completed.

Input headers

Parameter	Presence	Value	Description
Authorization	REQUIRED	String	Must always be of type Basic Auth. e.g. Basic Y2xpZW50SUQ6cGFzc3dvcmQ (base64 encoded value of CLIENT_ID:CLIENT_SECRET -> RFC 6749)

Response

Parameter	Presence	Value	Description
access_token	REQUIRED	String	The short-lived access token to be used depending on the scope of the OAuth 2.0 authorization request.
expires_in	OPTIONAL	Int	The lifetime in seconds of the service access token.
id_token	REQUIRED	JWT	The ID Token is a security token that contains Claims about the Authentication of an End-User by an Authorization Server when using a Client. Can be parsed using tools like https://jwt.io/
scope	REQUIRED	String	Space delimited string containing the scope for which authorization was granted.
token_type	REQUIRED	String	Must be Bearer or SAD

Examples

Sample Request

```
POST oauth2/token HTTP/1.1
Authorization: Basic K3dfKT59SUD8gWghq1ghjuZ
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code&
code=<RESULT_FROM_/oauth2/authorize>&
client_id=<OAuth2_client_id>&
client_secret=<OAuth2_client_secret>&
redirect_uri=<OAuth2_redirect_uri>
```

Sample Response

Example response when original OAuth/authorize request only contains "openid":

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
{
    "access_token": "f0EigERuAYruavv2fwRc4ZJKn1x1Uef8ymarsCqKfJw.x4GXhb551nocByGDSd1-z5UX52ncGlo8ufSML8Xxc_k",
    "expires_in": 3600,
    "id_token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6InB1YmxpYzpiNDNhODFiNS0zNGU3LTRkOWYtYWRmNS0yNWFlZjdjYTJkNGYiLCJ0eXAiOiJKV1QifQ.eyJ
hdF9oYXNoIjoiZ0pHYzRyckI5YzR1ak5pc2hiNEdCZyIsImF1ZCI6WyJjZWIwMGVmYy1lNDI2LTRmNjgtODZhZS1mZmRkNjIxMTdiNDYiXSwiYX
V0aF90aW1lIjoxNjUwNDYyNTQ0LCJleHAiOjE2NTA0NjYxNjYsImlhdCI6MTY1MDQ2MjU2NiwiaXNzIjoiaHR0cHM6Ly9lc2lnbi5hY2MuY2xld
mVyYmFzZS5jb20vIiwianRpIjoiNzE2MTYxNTgtMzAwYS00NWYwLWI2NjctYTFlMWQ1ZWIxNmI4Iiwibm9uY2UiOiI4NzY1NDMyMSIsInJhdCI6
MTY1MDQ2MjUyNiwic2lkIjoiMTc0NGNiN2MtYzM4My00MTkzLWFkNmQtYWQxMjFlOWZjZDczIiwic3ViIjoiYmY3MGUyZGEtZmVmZi00YzZiLTg
2YzItNDdlZGExOTlhYjMwIn0.LTJumJu2oSTGfgC3I-
LRUmxHGEJt0Ky23MZcvWA8cRD_vd1wlI2DkJ_ZbhwGWng6uhxEMFs2XGOYzybkdKx7LEL3K53Lmcz43z6-bMnhlJkuWP46zdoDbML8DAF3DBze-
P8lafa2sTVVdrWEYtWrgJ9Wb9ZwwmNUbmkhFALvtuXPtRlmARvUQlJnHgzk-JNIMWOtrVcss8ZFfoipvdAefyQbVTZjzedK4imYdeTbOhuvF-
9HwV4gev75bsi2gXhAcGolxACuw1jKY9HwcEh7-aqUZjJr-
4pIPjfpoaQqXpy1Zbufj2ehKgADtVaXbIu7EBNXlLdQCQFJqjlGqcDflxxxJk4ZqZhNx1YxtxoASoLpHbyhOF_-
lFeXqvb2AeAVkQghxeQ7eCUhms9i_6OF9cHM41kRXkU--0ZjWAJHpJMQgjVWnLGOnGQc4YQXoeO3KWHlW7lOvKvP4l-
QoRwIQH6gL8GPEFArfhRvsSaxl70XLkkgO4L_qMecLzwErhP6qtxi75Lv-PFNZPU4TbtlrLLQV5mmFmgIUlJNED8WWJYn0F-I2qy0XxROcYN-
evG90V9TN9IbVg3MZHtVMBx2OUpo0XXpBokDOSf5FJVPNFgVXv8M5Y4zol0XMbdGrlDGUj1HVvIzuZavCAZ4V3DXQNelcnwdx79iVLRw_sdkekM
",
    "scope": "openid",
    "token_type": "bearer"
}
```

Example response when original OAuth/authorize request contained the following scopes "openid email com.cleverbase.personal_info com.cleverbase.id_number":

```
{
    "access_token": "rxdF-27ehy4LFSUsh32gVDfN9QpdwqDu-3ZtbVsx5J8.ZEv7ldfm5Y9GNLSYlrPe9p5__dzSem5UH1dCyrgRfno",
    "expires_in": 3600,
    "id_token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6InB1YmxpYzpiNDNhODFiNS0zNGU3LTRkOWYtYWRmNS0yNWFlZjdjYTJkNGYiLCJ0eXAiOiJKV1QifQ.eyJ
hdF9oYXNoIjoibG4tUGZBeDUyc2FKYjc0X19TVVlZUSIsImF1ZCI6WyJjZWIwMGVmYy1lNDI2LTRmNjgtODZhZS1mZmRkNjIxMTdiNDYiXSwiYX
V0aF90aW1lIjoxNjUwNDU5NDc4LCJiaXJ0aGRhdGUiOiIxOTkwLTEyLTIyIiwiY29tLmNsZXZlcmJhc2UuYmlydGhwbGFjZSI6IlJvbWUiLCJjb
20uY2xldmVyYmFzZS5kb2N1bWVudC50eXBlIjoiTkxEX1BBU1NQT1JUIiwiY29tLmNsZXZlcmJhc2UuaWRfbnVtYmVyIjoiWFdONzVJTTE2Iiwi
Y29tLmNsZXZlcmJhc2UubGFzdF9uYW1lIjoiRGUgQnJ1aWpuIiwiY29tLmNsZXZlcmJhc2UubmF0aW9uYWxpdHkiOiJOTEQiLCJlbWFpbCI6ImR
lbW8uYWNjLjE5MDQyMi4xMDI0NTlAY2xldmVyYmFzZS5jb20iLCJlbWFpbF92ZXJpZmllZCI6dHJ1ZSwiZXhwIjoxNjUwNDYzMTI5LCJnaXZlbl
9uYW1lIjoiV2lsbGVrZSBMaXNlbG90dGUiLCJpYXQiOjE2NTA0NTk1MjksImlzcyI6Imh0dHBzOi8vZXNpZ24uYWNjLmNsZXZlcmJhc2UuY29tL
yIsImp0aSI6ImFjOGRjMjQ0LWY4OGMtNGQyZC1hNDI3LTMzYjZkMGVmMzc3MSIsIm5vbmNlIjoiODc2NTQzMjEiLCJyYXQiOjE2NTA0NTk0NjIs
InNpZCI6IjVjZTlkN2U0LTUxNTAtNGZmOS05ODRiLWUzNTgyZTAxNDdhNyIsInN1YiI6ImJmNzBlMmRhLWZlZmYtNGM2Yi04NmMyLTQ3ZWRhMTk
```

```
5YWIzMCJ9.mpvCyfWv7909aJwh3a-
4O4FolTbx2Zkj_ICAQCu_QEIwRlYNdod4Oet5VXdlCtMg4Rer8c47QKv_6dZNeEuE44yDXvt57q0RJG9ArQzIvQHs0cwvDECoAmduCuU8Uq64SU
ZwEGycxPHNqFCjvHN3B_6GyxW72-
rXWbszpVxwOOINV9ODTAY3MixIqLEJsOeHfv5mTGrxCYZ8Lsd3DSZJo34w3zX2xdUSFRVugTZbjfafvopGBZ4MS72Rsu9BF1vuEb00rFv2hWLNR
jXpRDL5QSKApjkiKSYs7WKc14-nUVv1J5LjC5SpAtf22CoPu-Kt3hdtjZlR1XrwZn-MLWcB9qdaBrfo0wyk_n7gJHcph5ihk5ql4VHsYeXB-
NubCRPcyyxDuXknr5yzPmFWy6xctiYcBEXuACFjlqn_bTKy7JO4cls16cJ0YLK6f6QvIaNHZQnq-AxI_yDSa9KtjYa5HK2UgHPT2J-
9f1f2TmZpH22TVF6SWF7ZUENF7nbGgTlIrXv9ex55lMDaHZC4mU04HA1MkXza3E52DVkJM4_1IkXYk6KyPIe7kFrGX8oUQlWihBenv405nmxUsG
CrQgzwNAwrMx6nIzBHQDRxRsWMVcbLwVNf6Vo64ETdDE_9i8zaSe1Gi-JSwDAhUchjAGpp6ml_ReG-FYyCDq7jKi1XoY0",
    "scope": "openid email com.cleverbase.personal_info com.cleverbase.id_number",
    "token_type": "bearer"
}
```


Error Response on the Authorize Endpoint

Case	Displayed to User	Error	Error Description
`ChallengeExpired`	De QR code is vervallen. De QR code heeft een beperkte levensduur. Probeer het nog een keer en scan het binnen de 10 minuten.	`access_denied`	authentication challenge expired
`EmailUnverified`	`'Uw email is niet geverifieerd', 'Activeer uw e-mail adres om verder te gaan. Om uw e-mail adres te valideren zoek naar "Verifieer je e-mailadres" in uw inbox en volg de instructies daar.'`	`access_denied`	user email is unverified
`ConsentExpired`	`'Pincode niet op tijd hebt ingevoerd', 'Wacht niet te lang om de pincode in te voeren, hier staat een tijdslimiet op.'`	`access_denied`	consent request expired
`ConsentRejected`	`'U ging niet akkoord met het delen van uw gegevens'`	`access_denied`	Resource owner rejected consent
`ProcessExpired`	`'Tijdslimiet bereikt', 'Deze handeling heeft een beperkte levensduur. Probeer het nog een keer en voer je pincode in binnen de 10 minuten.'`	`access_denied`	process expired
`NonPkioCertificate`	Kan niet verbinden met onze systemen. Er was een technisch probleem aan onze kant, probeer het nog een keer.	`server_error`	n/a
`VerificationFailed`	Kan niet verbinden met onze systemen. Er was een technisch probleem aan onze kant, probeer het nog een keer.	`server_error`	n/a
`SystemError`	Kan niet verbinden met onze systemen. Er was een technisch probleem aan onze kant, probeer het nog een keer.	`server_error`	n/a
`ConsentInvalidated`	Kan niet verbinden met onze systemen. Er was een technisch probleem aan onze kant, probeer het nog een keer.	`server_error`	n/a
`AuthenticationFailure`	Kan niet verbinden met onze systemen. Er was een technisch probleem aan onze kant, probeer het nog een keer.	`server_error`	n/a

Userinfo endpoint

The UserInfo Endpoint is an OAuth 2.0 Protected Resource that returns Claims about the authenticated End-User. To obtain the requested Claims about the End-User, the Client makes a request to the UserInfo Endpoint using an Access Token obtained through OpenID Connect Authentication. These Claims are represented by a JSON object that contains a collection of name and value pairs for the Claims.

Note: when this endpoint is used for IDF then optional scopes are required otherwise only a pairwise pseudonymous identifier for the natural person user is returned. See scopes and claims for details

Warning: Currently this feature is only available on the legacy "https://idf.acc.cleverbase.com" host.

OpenID Connect

GET /userinfo

Input headers

Parameter	Presence	Value	Description

Parameter	Presence	Value	Description
Authorization	REQUIRED	String	Must always be of type Bearer. Obtained from the "openid" scope OAuth flow. e.g. Bearer 4/CKN69L8gdSYp5_pwH3XlFQZ3ndFhkXf9P2_TiHRG-bA

Response

Parameter	Presence	Value	Description
sub	REQUIRED	String	Subject - Identifier for the End-User at the Issuer.
com.cleverbase.proof	OPTIONAL	JSON	A JSON array of JSON objects with id, content_type and base64_encoded_content fields. The content should be archived by the relying party and associated with the identifier and the provided content type. See the Knowledge Base for more context.
com.cleverbase.last_name	OPTIONAL	String	Last name of the end-user, as present in the identity document.
given_name	OPTIONAL	String	Given name(s) of the end-user, as present in the identity document.
birthdate	OPTIONAL	String	Birthdate of the end-user, as present in the identity document.
com.cleverbase.birthplace	OPTIONAL	String	Birthplace of the end-user, as present in the identity document.
com.cleverbase.nationality	OPTIONAL	String	Nationality of the end-user, as present in the identity document.
com.cleverbase.document.type	OPTIONAL	String	Document type used by the end-user to identify.
com.cleverbase.id_number	OPTIONAL	String	Unique number of the the identity document used during client registration.
email	OPTIONAL	String	End-user's preferred email address.
email_verified	OPTIONAL	Boolean	True if the end-user's email address has been verified.
com.cleverbase.authentication_certificate	OPTIONAL	String	PEM encoded x.509 Certificate
com.cleverbase.signing_certificate	OPTIONAL	String	PEM encoded x.509 Certificate
com.cleverbase.nl_brp_voornaam	OPTIONAL	String	First name(s)
com.cleverbase.nl_brp_voorvoegsel	OPTIONAL	String	Prefix
com.cleverbase.nl_brp_geslachtsnaam	OPTIONAL	String	Family name
com.cleverbase.nl_brp_geslachtsnaam_zonder_voorvoegsel	OPTIONAL	String	Family name without prefix
aud	REQUIRED	String	Audience - (for who or what the token is intended for)
auth_time	REQUIRED	Int	Time when authentication occurred - Unix timestamp
iat	REQUIRED	Int	Token issued at - Unix timestamp
iss	REQUIRED	String	Issuer (who created and signed this token)
rat	REQUIRED	Int	Unkown - Unix timestamp

Sample request

```
GET /userinfo HTTP/1.1
Authorization: Bearer 4/CKN69L8gdSYp5_pwH3XlFQZ3ndFhkXf9P2_TiHRG-bA
Content-Type: application/json
```

Sample response

Example response when the original oauth/authorize request only contained the "openid" scope (login functionality only)

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
{
    "aud": [
        <client_id>
```

```
    ],
    "auth_time": 1650458268,
    "iat": 1650458274,
    "iss": "https://esign.acc.cleverbase.com/",
    "rat": 1650458253,
    "sub": "bf70e2da-feff-4c6b-86c2-47eda199ab30"
}
```

Example response when the original oauth/authorize request contained the scopes "openid email com.cleverbase.personal_info com.cleverbase.id_number":

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
{
    "aud": [
        <client_id>
    ],
    "auth_time": 1650459478,
    "birthdate": "1990-12-22",
    "com.cleverbase.birthplace": "Rome",
    "com.cleverbase.document.type": "NLD_PASSPORT",
    "com.cleverbase.id_number": "XWN75IM16",
    "com.cleverbase.last_name": "De Bruijn",
    "com.cleverbase.nationality": "NLD",
    "email": "demo.acc.190422.102459@cleverbase.com",
    "email_verified": true,
    "given_name": "Willeke Liselotte",
    "iat": 1650459485,
    "iss": "https://esign.acc.cleverbase.com/",
    "rat": 1650459462,
    "sub": "bf70e2da-feff-4c6b-86c2-47eda199ab30"
}
```