

Guide to LSA SSO (Yeti) Services

DATE	Dec-2024
VERSION	2.3
PREPARED BY	Team

Table of Contents

1	Introduction and Purpose	3
2	References	3
2.1.1	Terminology	3
3	Use Cases	4
3.1	General Approach	4
4	Technical Overview	6
4.1	Language Considerations	6
5	Service Reference	6
5.1	Redirect to Authorization Endpoint	7
5.1.1	Input Parameters	7
5.1.2	Success Output Parameters	9
5.1.3	Failure Output Parameters	10
5.2	Call to Token Endpoint with Authorization Code	10
5.2.1	Input Parameters	10
5.2.2	Success Response	11
5.2.3	Failure Response	12
5.3	Call to Token Endpoint with Refresh Token	12
5.3.1	Success Response	13
5.3.2	Failure Response	14
5.4	Call to User Info	14
5.4.1	Input Parameters	14
5.4.2	Success Response	15
5.4.3	Failure Response	16
5.5	Call to Openid Configuration	16
5.5.1	Input Parameters	16
5.5.2	Success Response	17
5.5.3	Failure Response	18
5.6	Call to JWK Endpoint	18
5.6.1	Input Parameters	18
5.6.2	Success Response	18
5.6.3	Failure Response	19
5.7	Call to Login	20

5.7.1	Success Response	21
5.7.2	Failure Response.....	21
5.8	Frontchannel Call to Logout.....	22
5.8.1	Input Parameters	22
5.8.2	Success Response	22
5.8.3	Failure Response.....	22
5.9	Backchannel Call to SSO Logout	23
5.9.1	Input Parameters	23
5.9.2	Success Response	23
5.9.3	Failure Response.....	24
5.10	Call to User Registration	24
5.10.1	Input Parameters	24
5.10.2	Success Response	26
5.10.3	Failure Response.....	27
5.11	Call to Modify User Profile	27
5.11.1	Input Parameters	27
5.11.2	Success Response	29
5.11.3	Failure Response.....	30
5.12	Call to Delete User Profile	30
5.12.1	Input Parameters	30
5.12.2	Success Response	31
5.12.3	Failure Response.....	31
5.13	Call to Password Update	32
5.13.1	Input Parameters	32
5.13.2	Success Response	33
5.13.3	Failure Response.....	33
5.14	Call to Resend Double Opt-In Email.....	33
5.14.1	Input Parameters	34
5.14.2	Success Response	34
5.14.3	Failure Response.....	35
5.15	Call to Reset Password	35
5.15.1	Input Parameters	35
5.15.2	Success Response	36
5.15.3	Failure Response.....	36
5.16	Call to Social Signin	37
5.16.1	Success Response	37
5.16.2	Failure Response.....	38
5.17	Call to Facebook Signin	39
5.17.1	Success Response	39

5.17.2	Failure Response.....	40
5.18	Call to Fetch Short-lived Signed Id Token.....	40
5.18.1	Input Parameters	41
5.18.2	Success Response	41
5.18.3	Failure Response.....	42
6	Client Configuration	43

1 Introduction and Purpose

LSA SSO is a Single-Sign-On and Identity Management system, henceforth referred to as **"Yeti"**.

Yeti is based on the Openid Connect standard, which as of today is the main reference standard in user authentication, and which in turn uses OAuth 2.0, which is the main reference standard in the area of authorization between applications.

The purpose of this document is:

- To facilitate the adoption of Yeti by client web and mobile applications
- To document in detail the single services

2 References

Description	Refernce
Openid Connect Core Specifications	https://openid.net/specs/openid-connect-core-1_0.html
Android libraries for Openid	https://github.com/openid/AppAuth-Android
IOS Libraries for Openid	https://github.com/openid/AppAuth-iOS

2.1.1 Terminology

Openid Connect terminology is often used in this document. Further details can be found in the Openid Connect official specifications in the "Terminology" chapter. The most important are:

Term	Meaning
Adopting application	The client application which uses Yeti
Relying Party (RP)	Synonym of "Adopting Application"
Client	Synonym of "Adopting Application"
SSO	Single-Sign-On
OpenId Provider (OP)	Yeti itself
Claim	User profile attribute
Id Token	User Identity Token
Access Token	Token to access Yeti services

Refresh Token	Token to refresh access to Yeti services
SSO Domain	Un set of "Clients" which share the same set of users
JWT	JSON Web Token
Backchannel	Server to server, or backend channel
Frontchannel	Front-end channel, i.e involving the browser (for example a redirect is frontchannel)
Confidential client	A client to which a "client secret" is supplied by y-tech. Typically web applications are confidential and mobile applications are not

3 Use Cases

3.1 General Approach

Yeti allows adopting applications (RPs) to know the identity of their users and to obtain their attributes. It allows multiple applications to share the same user base, and to share a single access via username and password between multiple applications, thereby avoiding separate logins for each application (SSO).

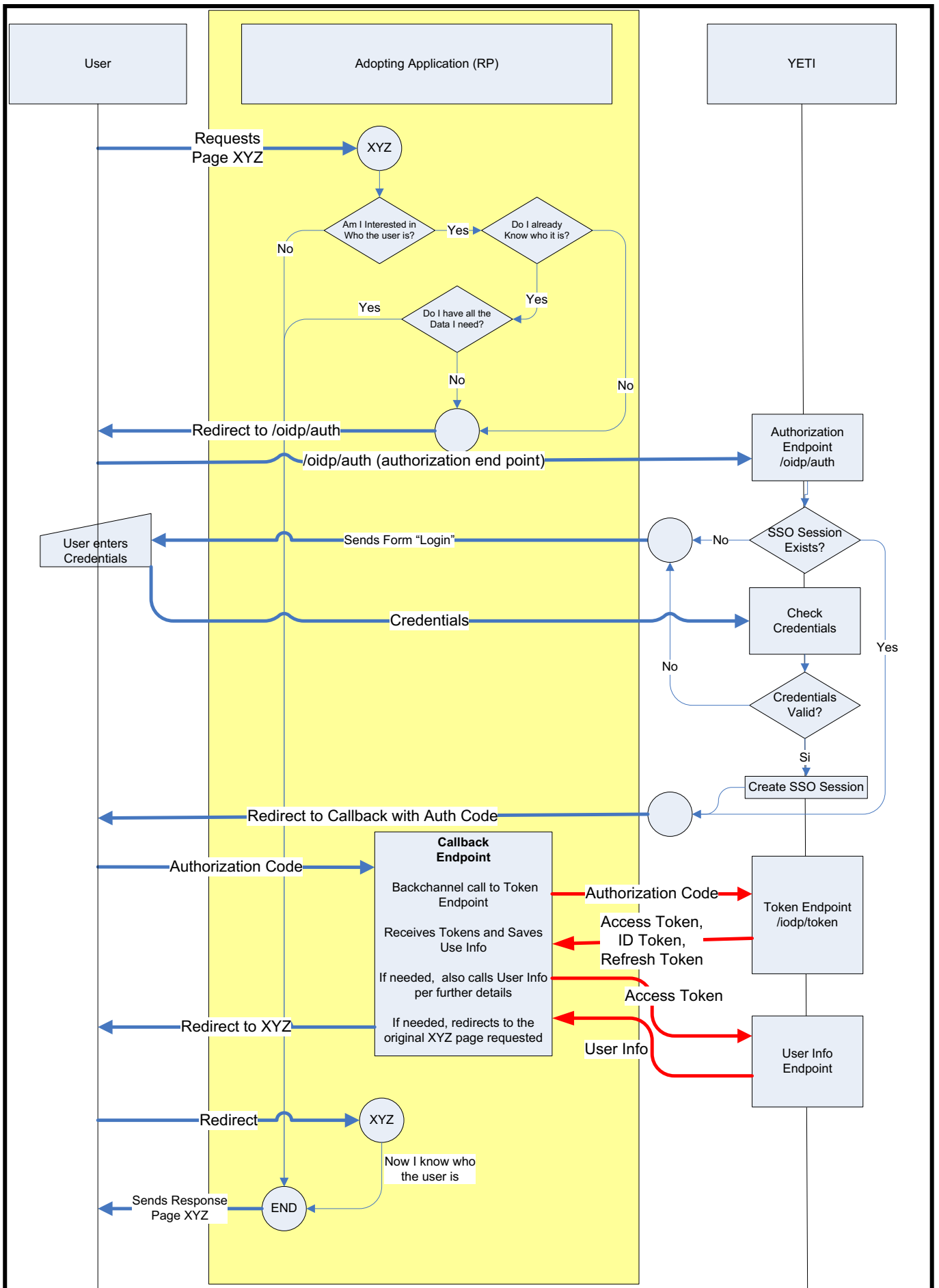
The adopting application is free to manage the information received from Yeti as it deems best: such as keeping it's own local copy of user attributes, such as to have it's own way of recognizing who is interacting with it, for example via a classic "session" in a web application, or device storage in a mobile application.

As well as allowing adopting applications to know the identity of their users, Yeti provides various functionalities for registering users, modifying their profile, and managing their credentials.

The diagram which follows represents the high-level reasoning which an adopting application would apply in using Yeti.

For native mobile applications, the flow is substantially the same: the "redirects" initiated by the app leverage the system browser, and invoke the /oidp/auth endpoint with the system browser embedded in the app, whereas the redirects initiated by Yeti will use special URLs which the IOS and Android operating systems are able to recognize as belonging to that app, hence triggering the app itself. These URLs are not "classic" web urls, here is an example:

it.example.mobileapp://callback?code=123456



4 Technical Overview

Yeti is a web-based system, using a technology stack with:

- Linux operating system
- Load balanced web servers with separate database server
- Oracle Database
- Javalite web development framework running under Tomcat servlet engines
- Freemarker templates for the front-end pages (eg. the user profile page)

4.1 Language Considerations

Yeti is bilingual, providing English and Italian.

Messages from the backend are either in Italian or English.

In any request, a parameter "hl" may be added to change the language of the backend messages:

Parameter	Values
Hl	Allowed values: "it"/"en" (Italian/English)

A client can have a default language. (See "Client Configuration" paragraph, "cd_lang_default")

A client can be multi-lingual. (See "Client Configuration" paragraph, "fl_multi_lang"). In this case, the Freemarker templates will have an Italian and an English version, with suffix _it or _en.

A user can have a preferred language.

The addition of the "hl" request parameter has priority over the default language of the client and the preferred language of the user.

5 Service Reference

This chapter contains reference details on the services exposed by Yeti. The majority are REST web services, except for the "Redirect to Authorization Endpoint", which is an http redirect.

The root endpoints are:

Environment	Root Endpoint
Staging	https://obelix.y-tech.it
Production	<p>Normally, each SSO domain will have a dedicated host name on the domain "yeti-sso.it", for example:</p> <p>https://genoa.yeti-sso.it</p> <p>Else, if the client prefers to use his own domain, he can also choose it freely. The name chosen must have a DNS record pointing to the production IP address of yeti, which coincides with the IP address of www.yeti-sso.it</p> <p>Please note that in this user guide, many "Input Parameters" paragraphs in this document, contain the line "Host: www.yeti-sso.it</p>

	sso.it ” for example purposes. This line should be replaced by “Host: <the hostname assigned to the client>” It is mandatory that the protocol be HTTPS
--	--

In the documentation which follows this root endpoint is referred to as: `{{root endpoint}}`

5.1 Redirect to Authorization Endpoint

This is invoked by the adopting application via an http redirect to the authorization endpoint with a set of parameters as described below.

The redirect is compliant to the Openid specifications.

Endpoint
<code>{{root endpoint}}/oidp/auth</code>

5.1.1 Input Parameters

These are passed to the endpoint via a classic http redirect query string, for example:

```
HTTP/1.1 302 Found
Location: https://www.yeti-sso.it/oidp/auth?
    response_type=code
    &scope=openid
    &client_id=s6BhdRkqt3
    &state=af0ifjsldkj
    &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
```

Field Name	Type	Mandatory	Description
scope	String	Yes	Set to “openid profile” or “openid”
response_type	String	Yes	For the Openid Code Flow Set to “code” For the Openid Implicit Flow Set to “id_token” or “id_token token”
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has it’s own client_id
redirect_uri	String	Yes	This is the url encoded callback endpoint of the adopting application, to which Yeti will redirect after authenticating the user. The redirect will pass the authorization code, which is subsequently to be used in the token call. Example: <code>https%3A%2F%2Fclient.example.org%2Fcb</code> Which is the url encoded value of:

			https://client.example.org/cb
state	String	No	Opaque value to be passed back to the redirect_uri callback, which should check that the value passed to the authorization endpoint coincides with the value passed back to the callback.
nonce	String	No	Opaque value to be passed back in the id token.
prompt	String	No	<p>This parameter controls what user interaction the authorization server should undertake. In its absence, the authorization server prompts the user to enter his credentials if not already authenticated and does not prompt if already authenticated (normal behaviour). Should the client application need to force a reauthentication, the it can pass this parameter with value "login".</p> <p>Possible values:</p> <p>"none":</p> <p>Yeti will not display any authentication or consent user interface pages. An error is returned if an End-User is not already authenticated</p> <p>"login"</p> <p>Yeti prompts the End-User for reauthentication. If it cannot reauthenticate the End-User, it returns an error "login_required".</p> <p>"consent"</p> <p>The Authorization Server prompts the End-User for consent before returning information to the Client. If it cannot obtain consent, it returns an error "consent_required"</p> <p>"login consent"</p> <p>require both login and consent</p>
max_age	Integer	No	Maximum Authentication Age. Specifies the allowable elapsed time in seconds since the last time the End-User was actively authenticated by Yeti. If the elapsed time is greater than this value, Yeti will attempt to actively re-authenticate the End-User by prompting for credentials.
code_challenge	String	No	Required if the client application is configured to require it. Mobile application clients should require it for increased

			<p>security. Web clients can require it for increased security.</p> <p>This should contain the encrypted SHA256 hash of a "code verifier", which is defined as:</p> <p>a random high entropy cryptographic STRING, using the Unreserved Characters [A-Z] / [a-z] / [0-9] / "-" / "." / "_" / "~" from Sec 2.3 of [RFC3986], with a minimum length of 43 characters and a maximum length of 128 characters</p> <p>The client application should temporarily store the value of the code_verifier (not the code_challenge!). The code_verifier must subsequently be passed as an input parameter to the token endpoint calls.</p> <p>The Android and IOS libraries for Openid mentioned in the "References" chapter provide methods for generating both the code_verifier and the code_challenge.</p>
code_challenge_method	String	No	<p>Required if the client application is configured to require it. Mobile application clients should pass it for increased security.</p> <p>Set to "S256"</p>

5.1.2 Success Output Parameters

These are passed back to the adopting application's callback endpoint specified in the "redirect_uri" input parameter via a classic http redirect query string, for example:

```
HTTP/1.1 302 Found
Location: https://client.example.org/cb?
  code=Splxl0BeZQQYbYS6WxSbIA
  &state=af0ifjsldkj
```

Field Name	Type	Mandatory	Description
code	String	Yes	This is the short-lived authorization code which the adopting application should store in order to subsequently invoke the Yeti token endpoint
state	String	No	This is set to the same value as in the input parameter "state". If present, the adopting application must check that it contains the same value as the input parameter of the same name.

5.1.3 Failure Output Parameters

These are passed to the endpoint via a classic http query string, for example:

```
HTTP/1.1 302 Found
Location: https://client.example.org/cb?
  error=invalid_request
  &error_description=
    Unsupported%20response_type%20value
  &state=af0ifjsldkj
```

Field Name	Type	Mandatory	Description
error	String	Yes	Possible values: invalid_request login_required consent_required
error_description	String	No	URL encoded string with a human understandable description of the error
state	String	No	This is set to the same value as in the input parameter "state". If present, the adopting application must check that it contains the same value as the input parameter of the same name.

5.2 Call to Token Endpoint with Authorization Code

This is invoked by the adopting application via the backchannel (server to server), usually a small number of seconds after the redirect to the authorization endpoint (see previous paragraph). Typically the token endpoint would be invoked by the logic residing inside the adopting application's callback which the authorization endpoint redirects to.

Endpoint	Http Method	Content Type
{{root_endpoint}}/oidp/token	POST	application/x-www-form-urlencoded

5.2.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /oidp/token HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant_type=authorization_code&code=Sp1xl0BeZQQYbYS6WxSbIA
```

The `client_id` and the `client_secret` are combined with a colon (`client_id:client_secret`). The resulting string is base64 encoded (eg. `YWxhZGRpbjpvGVuc2VzYW1ldhjsiaktT`).

5.2.2 Success Response

Example response:

Version: 2.3

Field Name	Type	Mandatory	Description
access_token	String	Yes	Value of the access token assigned
refresh_token	String	Yes	Value of the refresh token assigned
scope	String	No	Same value as supplied to the authorization endpoint.
id_token	String	Yes	Value of the id token assigned
token_type	String	Yes	Set to "Bearer"
expires_in	String	No	Expiration time of the Access Token in seconds since the response was generated

5.2.3 Failure Response

If the request is not successful, a 400 or 401 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "error_description": "Non risulta (o e' scaduto) authorization code:
ffG58oNVxbeVxAazDOgQVQ4RgEUUtm7LQEzco_7wvTI",
  "error": "invalid_token"
}
```

Field Name	Type	Mandatory	Description
error	String	Yes	Code of the error. Values: "invalid_token" – token not valid (usually because it has expired) "invalid_request" – other issues other values possible.
error_description	String	Yes	Human readable description of the error. In the case of access token expiry, it is: "L'access_token fornito in questa request risulta scaduto. Occorre fare refresh"

5.3 Call to Token Endpoint with Refresh Token

This call is needed when the access token is expired, it will respond with a new access and a new refresh token. Please note that the new refresh token in the response invalidates the previous refresh token.

Endpoint	Http Method	Content Type
{{root_endpoint}}/oidp/token	POST	application/x-www-form-urlencoded

The input parameters are passed to the endpoint via POST a query string, for example:

POST /oidp/token HTTP/1.1

Host: www.yeti-sso.it

Content-Type: application/x-www-form-urlencoded

client_id=s6BhdRkqt3

&refresh_token=some_refresh_token_value

&client_secret=some_secret12345

&grant_type=refresh_token

&scope=openid

Field Name	Type	Mandatory	Description
grant_type	String	Yes	Set to "refresh_token"
refresh_token	String	Yes	Value of the refresh token previously assigned in a call to token endpoint with authorization code (see previous paragraph)
client_secret	String	No	Required if the client is confidential. Set to the values of the client secret assigned by y-tech to this client
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has it's own client_id
scope	String	No	Set to same value as original authorization request (usually "openid")

5.3.1 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "access_token": "AtGh8OpCnqFACKMrtzX9JoCubNvo4FPRgAC-Q1thlU0",
  "refresh_token": "V0gzNcoLBN4eMynj4BQtnM0v40lYuGtDiYN4tKBk9Hw",
  "id_token": "eyJhbGciOiJSUzI1NiJ9.eyJz. snip ..emEPvM965LrA"

  "scope": "openid",
  "token_type": "Bearer",
  "expires_in": 86400
}
```

Field Name	Type	Mandatory	Description
access_token	String	Yes	Value of the access token assigned
refresh_token	String	Yes	Value of the refresh token assigned

scope	String	No	Same value as supplied to the authorization endpoint.
token_type	String	Yes	Set to "Bearer"
expires_in	String	No	Expiration time of the Access Token in seconds since the response was generated

5.3.2 Failure Response

If the request is not successful, a 400 or 401 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "error_description": "Non risulta il refresh token:
058pAkIztcDCP3tPSfdDYTsRelSLuP9RXPnR78jsYo",
  "error": "invalid_token"
}
```

Field Name	Type	Mandatory	Description
error	String	Yes	Code of the error. Values: "invalid_token" – token not valid (usually because it has expired) "invalid_request" – other issues other values possible.
error_description	String	Yes	Human readable description of the error

5.4 Call to User Info

This call is needed to fetch the full user profile attributes, when the attributes present in the id token are insufficient (the id token only contains the subject identifier (sub) and the email address).

Endpoint	Http Method	Content Type
{{root_endpoint}}/oidp/userinfo	GET	Not applicable (get request without parameters)

5.4.1 Input Parameters

This endpoint does not need input parameters, just a bearer authorization header with the access token value, example:

```
GET /oidp/userinfo HTTP/1.1
Host: www.yeti-sso.it
Authorization: Bearer SlAV32hkKG
```

5.4.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "sub": "1",
  "email_verified": true,
  "birthdate": "27/11/1962",
  "address": {
    "street_address": "Via Manzoni, 18",
    "country": "Italy",
    "locality": "Milano",
    "region": "MI",
    "postal_code": "20100"
  },
  "gender": "male",
  "name": "Jeremy Coleman",
  "phone_number": "+393287906000",
  "given_name": "Jeremy",
  "family_name": "Coleman",
  "email": "jj.coleman@y-tech.it"
}
```

Field Name	Type	Mandatory	Description
sub	String	Yes	Subject identifier (User identifier)
email_verified	Boolean	No	Indicates whether the email address has been verified (typically via a confirmation email (double opt-in)) True if verified, else false.
birthdate	String	No	Date of birth in dd/mm/yyyy format
gender	String	No	"male" or "female"
name	String	No	Full name (given + family)
phone_number	String	No	
given_name	String	No	
family_name	String	No	
email	String	Yes	
address	Object	No	See indented members below
street_address	String	No	
country	String	No	
locality	String	No	Name of the town

region	String	No	In Italy, this is the code of the province, for example "MI" (for Milan province)
postal_code	String	No	

5.4.3 Failure Response

If the request is not successful, a 400 or 401 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "error_description": "Non risulta l'access_token fornito in questa request",
  "error": "invalid_token"
}
```

Access token expiry can be recognized by 401 http status and error_code "invalid_token"

Field Name	Type	Mandatory	Description
error	String	Yes	Code of the error. Values: "invalid_token" – token not valid (usually because it has expired) "invalid_request" – other issues other values possible.
error_description	String	Yes	Human readable description of the error. In the case of access token expiry, it is: "L'access_token fornito in questa request risulta scaduto. Occorre fare refresh"

5.5 Call to Openid Configuration

This call is useful for discovery of the Openid configuration details

Endpoint	Http Method	Content Type
{{root_endpoint}}/.well-known/openid-configuration	GET	Not applicable (get request without parameters)

5.5.1 Input Parameters

This endpoint does not need input parameters, just a bearer authorization header with the access token value, example:

GET /.well-known/openid-configuration HTTP/1.1

Host: www.yeti-sso.it (or relevant hostname for Relying Application)

5.5.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "response_types_supported": [
    "code",
    "code id_token",
    "id_token",
    "token id_token"
  ],
  "end_session_endpoint": "https://www.yeti-sso.it/utente/logout",
  "scopes_supported": [
    "openid",
    "email",
    "profile"
  ],
  "issuer": "https://www.yeti-sso.it",
  "authorization_endpoint": "https://www.yeti-sso.it/oidp/auth",
  "userinfo_endpoint": "https://www.yeti-sso.it/oidp/userinfo",
  "claims_supported": [
    "sub",
    "email",
    "given_name",
    "family_name",
    "gender",
    "phone_number",
    "birthdate",
    "locality",
    "region",
    "postal_code",
    "country",
    "lang",
    "street_address",
    "fl_consenso_cond_generali",
    "fl_informativa_privacy_letta",
    "fl_consenso_comunicazione",
    "fl_consenso_profilazione",
    "fl_consenso_cessione_terzi"
  ],
  "httpStatus": 200,
  "jwks_uri": "https://www.yeti-sso.it/oidp/jwk",
}
```

```

"subject_types_supported": "public",
"id_token_signing_alg_values_supported": [
    "HS256",
    "RS256"
],
"token_endpoint_auth_methods_supported": [
    "client_secret_basic"
],
"token_endpoint": "https://www.yeti-sso.it/oidp/token",
"status": "ok"
}

```

5.5.3 Failure Response

Theretically there should not be any errors

5.6 Call to JWK Endpoint

This call is needed when the client is configured to use the RS256 id token signing mechanism. It should be used by the client application to check the validity of the id token returned by the token endpoint.

Endpoint	Http Method	Content Type
{{root_endpoint}}/oidp/jwk/<client_id>	GET	Not applicable (get request without parameters)

5.6.1 Input Parameters

The only input "parameter" is the client id, which needs to be appended to the URL, example (with client id: "123456"):

```

GET /oidp/jwk/123456 HTTP/1.1
Host: www.yeti-sso.it

```

5.6.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```

{
  "keys": [
    {
      "kty": "RSA",
      "e": "AQAB",
      "use": "sig",
      "kid": "3",

```

```

    "alg": "RS256",
    "n":
    "q92cFkXYSOT4viQeyKMbz1TG2M4ob_xUBIJrggSAINxrjmVeMphS8xaG5UNdGTvv7YVpg41b173ImUs
    FJSuLh5m3bsct5LDtf3jxJvGZw-FoQATKinOmBly-r0RRTH213w90kU7v_KgKNiSijZGrR8uIJB_u-
    nMGZdJvs7EZL6IOOhlTnF0SGoixIxVDNTjz2QkSPArLNymSk11kdiVS1Zs8Ac6nGG2j_7vk6Z7E_7d0
    hDZvb3SyV_D6I7Cnvd6M0BfKIxfyv-
    UF0k5VCIKeRQ1pJpTgbS7AE_aVPyp3vezbANMK_0gAO22PVN7ays8e4YVjUT7e08AoF44un3pTQ"
  }
],
  "status": "ok",
  "httpStatus": 200
}

```

Field Name	Type	Mandatory	Description
keys	Object	Yes	See indented members below
kty	String	Yes	Key type currently only value is "RSA"
e	String	Yes	The "e" (exponent) parameter contains the exponent value for the RSA public key. It is represented as a Base64urlUInt-encoded value. For instance, when representing the value 65537, the octet sequence to be base64url-encoded MUST consist of the three octets [1, 0, 1]; the resulting representation for this value is "AQAB".
use	String	Yes	Purpose the key is used for: Values: sig - signing enc - encryption
kid	String	Yes	Key unique identifier
alg	String	Yes	Key signing algorithm. currently only "RS256"
N	String	Yes	The modulus value for the RSA public key. It is represented as a Base64urlUInt-encoded value.
status	String	Yes	set to "ok"
httpStatus	String	Yes	set to 200

5.6.3 Failure Response

If the request is not successful, a 400 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 400,
  "message": "Non trovo un organizzazione con client id: 123456",
  "status": "ko"
}
```

5.7 Call to Login

This call is typically not used by adopting applications, since the redirect to the authorization endpoint takes care of asking for the user credentials, and has the advantage of setting up a SSO session. However, if the adopting application is not interested in SSO, it may invoke this service directly, thereby getting an access token (to use subsequently to invoke the user info endpoint), a refresh token, and optionally an id token and an sso session id value.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/do_accedi	POST	application/x-www-form-urlencoded

The input parameters are passed to the endpoint via POST a query string, for example:

```
POST /utente/do_accedi HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
client_id=s6BhdRkqt3
&email=some_email_address
&pwd=some_password
&response_type=access_token
```

Field Name	Type	Mandatory	Description
pwd	String	Yes	The user's password
email	String	Yes	The user's email address
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has its own client_id
response_type	String	No	Can be used if the login service is invoked without a prior authorization request, and access and/or id tokens are required in the response. Possible values: "access_token" to receive access and refresh token or to "access_token id_token" to receive access, refresh and id tokens

			"access_token id_token sso_session_id" to receive access, refresh, id tokens and a sso session id value
--	--	--	---

5.7.1 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "access_token": "1kqtAHAsSgRVJAjAYNkNJs88II0KLShdcswikbuOHXk",
  "refresh_token": "vE6ipWlmpvY8idlquKsW0s2U-m1u2EyEVt789ZA0_Vc",
  "httpStatus": 200,
  "message": "Utente autenticato con successo",
  "token_type": "Bearer",
  "expires_in": 345600,
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Utente autenticato con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success
access_token	String	Yes	Value of the access token assigned
refresh_token	String	Yes	Value of the refresh token assigned
token_type	String	Yes	Set to "Bearer"
expires_in	String	No	Expiration time of the Access Token in seconds since the response was generated

5.7.2 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Combinazione di email e password non valida",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure

message	String	Yes	For success: "Utente autenticato con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 both for success and failure

5.8 Frontchannel Call to Logout

This call is used to end the SSO session, for example when the user wants to switch to another account, or simply if he wants to terminate the SSO session for security reasons.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/logout	GET	Not applicable

5.8.1 Input Parameters

Field Name	Type	Mandatory	Description
redirect	String	No	Post logout Redirect URL

This endpoint can also have an "Accept" header specifying "application/json", in which case the response will be in JSON, example:

```
GET /utente/logout HTTP/1.1
Host: www.yeti-sso.it
Accept: application/json
```

5.8.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Logout effettuato",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Logout effettuato", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success

5.8.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Logout effettuato", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.9 Backchannel Call to SSO Logout

This call is needed to end the SSO session, for example when the user wants to switch to another account, or simply if he wants to terminate the SSO session for security reasons. This is the "server to server" version of the logout, typically used in conjunction with the client application logout (first logout from client application, then invoke this server to server).

Endpoint	Http Method	Content Type
{{root_endpoint}}/oidp/logout	GET	Not applicable

5.9.1 Input Parameters

This endpoint does not need input parameters, just a bearer authorization header with the access token value, example:

```
GET /oidp/logout HTTP/1.1
Host: www.yeti-sso.it
Authorization: Bearer SlAV32hkKG
```

5.9.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Logout effettuato",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Logout effettuato", for failure, the reason for the failure

httpstatus	Integer	Yes	200 for success
------------	---------	-----	-----------------

5.9.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Logout effettuato", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.10 Call to User Registration

This is the backchannel call to user registration, which may be needed if the adopting application wants to develop its own UI for user registration. It is not needed if the client is happy with the registration front-end supplied and tailored in terms of look and feel by Yeti.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/do_registra	POST	application/x-www-form-urlencoded

5.10.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /utente/do_registra HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded

email=someuser@somedomain.com
&given_name=Datonomme
&family_name=De Family
&gender=female
&birthdate=01/01/1998
&secret=kTWIi7wsj5am0ptTNmtK6rpZp8tPMF39inbvwC0qJGc
&clientId=12345
```



```

&pwd=bbb
&pwd2=bbb
&fl_consenso_cond_generali=1
&fl_informativa_privacy_letta=1
&fl_consenso_comunicazione=0
&fl_consenso_profilazione=0
&fl_consenso_cessione_terzi=0

```

The list of user attributes below is not exhaustive, as it is still in development.

Field Name	Type	Mandatory	Description
Email	String	No	Mandatory if tp_auth empty or equal to "upwd"
tp_auth	String	No	If set to "otp", will require country_code and n_cell. This is for OTP authentication via SMS
given_name	String	No	
family_name	String	No	
gender	String	No	"male" or "female"
birthdate	String	No	Format dd/mm/yyyy
secret	String	Yes	
clientId	String	Yes	
Pwd	String	Yes	Password
pwd2	String	Yes	Password (same again)
fl_consenso_cond_generali	String	Yes	Must be set to "1" if no "secret" parameter present. If secret present, can be either "0" or "1"
fl_informativa_privacy_letta	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
fl_consenso_comunicazione	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
fl_consenso_profilazione	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
fl_consenso_cessione_terzi	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
street_address	String	No	
locality	String	No	
region	String	No	
postal_code	String	No	
country	String	No	

address_country_code	String	No	Country code of address, either 2 character or 3 character (eg: "IT" or "ITA")
n_cell	String	No	Mandatory if tp_auth = 'otp', must be a valid mobile phone number
country_code	String	No	Mandatory if tp_auth = 'otp', must be a valid telephone country_code (eg. "+39")
cod_cliente_legacy	String	No	Legacy system user identifier or originating system reference for the user.
opt_in	String	No	Can be added as a hidden parameter in the registration form. If set to "Y", and email confirmation opt-in is active, the user, on clicking the confirmation opt-in email link, will be redirected to the redirect_uri of his authorization request, instead of "/utente/opt_in" (default behaviour)
birth_country	String	No	
birth_province	String	No	
birth_comune	String	No	
string1 to string10	String	No	"User" fields of type String for custom purposes
num1 to num5	String	No	"User" fields of type Number (Integer) for custom purposes
date1 to date5	String	No	"User" fields of type Date for custom purposes. Format dd/mm/yyyy

5.10.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "redirect": "no",
  "httpStatus": 200,
  "message": "Registrazione effettuata con successo",
  "sub": 437,
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
Status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Registrazione effettuata con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success

redirect	String	No	Has value "no"
sub	Integer	No	In case of successful registration, this contains the unique identifier of the user created

5.10.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	The reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.11 Call to Modify User Profile

This is the backchannel call to user profile update, which may be needed if the adopting application wants to develop it's own UI for user profile update. It is not needed if the client is happy with the profile update front-end supplied and tailored in terms of look and feel by Yeti.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/do_modifica_profilo	POST	application/x-www-form-urlencoded

5.11.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /utente/do_modifica_profilo HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
Authorization: Bearer SlAV32hkKG
```

```
sub=100100
&email=someuser@somedomain.com
```

```

&given_name=Datonomme
&family_name=De Family
&birthdate=01/01/1998
&clientId=12345
&fl_consenso_cond_generali=1
&fl_consenso_profilazione=0
&fl_consenso_cessione_terzi=0

```

The below list of user attributes below is not exhaustive, as it is still in development.

The optional parameters need not be passed if their values does not need changing.

The http authorization header must contain a valid access token, unless the "secret" parameter is passed.

Field Name	Type	Mandatory	Description
sub	String	Yes	User identifier
email	String	No	This should not be updated
tp_auth	String	No	This is for OTP authentication via SMS/Email or Push. It must be set to "otp" if the client uses OTP authentication instead of email / password authentication.
given_name	String	No	
family_name	String	No	
gender	String	No	"male" or "female"
birthdate	String	No	
clientId	String	Yes	
pwd	String	No	Password
pwd2	String	No	Password (same again)
fl_consenso_cond_generali	String	No	Must be set to "1" if no "secret" parameter present. If secret present, can be either "0" or "1"
fl_informativa_privacy_letta	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
fl_consenso_comunicazione	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
fl_consenso_profilazione	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
fl_consenso_cessione_terzi	String	No	Possible values "1" (consent granted) or "0" (consent NOT granted)
street_address	String	No	
locality	String	No	
region	String	No	

postal_code	String	No	
address_country_code	String	No	Country code of address, either 2 character or 3 character (eg: "IT" or "ITA")
country	String	No	
n_cell	String	No	Mandatory if tp_auth = 'otp', must be a valid mobile phone number without country code
country_code	String	No	Mandatory if tp_auth = 'otp', must be a valid telephone country_code (eg. "+39")
cod_cliente_legacy	String	No	Legacy system user identifier or originating system reference for the user.
redirect	String	No	Post update redirect url
birth_country	String	No	
birth_province	String	No	
birth_comune	String	No	
string1 to string10	String	No	"User" fields of type String for custom purposes
num1 to num5	String	No	"User" fields of type Number (Integer) for custom purposes
date1 to date5	String	No	"User" fields of type Date for custom purposes. Format dd/mm/yyyy
secret	String	No	Client secret. This is needed to modify a profile without passing an access token.

5.11.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Modifica profilo effettuata con successo",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Modifica profilo effettuata con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success

5.11.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	The reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.12 Call to Delete User Profile

This is the backchannel call to user profile deletion. The http authorization header must contain a valid access token, unless the "secret" parameter is passed.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/do_cancella_profilo	POST	application/x-www-form-urlencoded

5.12.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /utente/do_cancella_profilo HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
Authorization: Bearer SLAV32hkKG
```

```
sub=100100
&email=someuser@somedomain.com
&clientId=12345
```

Field Name	Type	Mandatory	Description
Sub	String	Yes	User identifier
Email	String	No	Mandatory tor clients using email/password authentication
clientId	String	Yes	

secret	String	No	Client secret. This is needed to modify a profile without passing an access token.
tp_auth	String	No	Must be set to "otp" if the client uses OTP authentication instead of email / password authentication.

5.12.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Cancellazione profilo effettuata con successo",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Cancellazione profilo effettuata con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success

5.12.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	The reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.13 Call to Password Update

This is the backchannel call to user password update, which may be needed if the adopting application wants to develop it's own UI for user password update. It is not needed if the client is happy with the password update front-end supplied and tailored in terms of look and feel by Yeti.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/do_cambia_password	POST	application/x-www-form-urlencoded

5.13.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /utente/do_cambia_password HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
```

```
sub=100100
&clientId=12345
&email=someuser@somedomain.com
&pwdOld=someOldPassword
&pwdNew=someNewPasword
&pwdNew2=someNewPassword
```

Field Name	Type	Mandatory	Description
sub	String	Yes	User identifier
email	String	Yes	Must exist
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has it's own client_id
pwdOld	String	Yes	Old password (must be valid for the above email)
pwdNew	String	No	Password
pwdNew2	String	No	Password (same again)
redirect	String	No	Post update redirect url

5.13.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Password modificata con successo",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Password modificata con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success

5.13.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	The reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.14 Call to Resend Double Opt-In Email

This call resends the registration confirmation email. It is needed by users if their email address still needs confirmation, and they have mislaid the original email.

This is the backchannel call to the functionality, which may be needed if the adopting application wants to develop it's own UI for it. It is not needed if the client is happy with the relevant front-end supplied and tailored in terms of look and feel by Yeti.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/do_reinvio_mail_conferma	POST	application/x-www-form-urlencoded

5.14.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /utente/do_reinvio_mail_conferma HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
```

```
clientId=12345
&email=someuser@somedomain.com
&pwd=someValidPassword
```

Field Name	Type	Mandatory	Description
email	String	Yes	Must exist
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has it's own client_id
pwd	String	Yes	Password (must be valid for the above email)

5.14.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Email di conferma registrazione reinviata con successo",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Email di conferma reinviata con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success

5.14.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	The reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.15 Call to Reset Password

This call sends an email which contains a link which allows the user to set his password to a new value, even if he does not know his current password.

This is the backchannel call to the functionality, which may be needed if the adopting application wants to develop it's own UI for it. It is not needed if the client is happy with the relevant front-end supplied and tailored in terms of look and feel by Yeti.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/do_send_reset_password_email	POST	application/x-www-form-urlencoded

5.15.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /utente/do_send_reset_password_email HTTP/1.1
Host: www.yeti-sso.it
```

Content-Type: application/x-www-form-urlencoded

clientId=12345

&email=someuser@somedomain.com

Field Name	Type	Mandatory	Description
email	String	Yes	Must exist
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has it's own client_id

5.15.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "Email per il reset della password inviata con successo",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Email per il reset della password inviata con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success

5.15.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	The reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

5.16 Call to Social Signin

This call is used by the "signin with google/apple/etc" functionality embedded in the Yeti provided credentials page. It is invoked by front-end javascript. However, if the adopting application opts to develop its own credentials page, they can use this call to sign-in and/or sign-up an authenticated user with a valid id token obtained from google/apple/etc. Please note that this call is not valid for facebook. The facebook signin is the subject of the next paragraph.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/social_signin	POST	application/x-www-form-urlencoded

The input parameters are passed to the endpoint via POST a query string, for example:

```
POST /utente/social_signin HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
client_id=s6BhdRkqt3
&id_token=<id token obtained from google>
&cdSocial=google
```

Field Name	Type	Mandatory	Description
id_token	String	Yes	Id token obtained from google
cdSocial	String	Yes	Possible values: google apple microsoft
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has it's own client_id

5.16.1 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "redirect": "no",
  "httpStatus": 200,
  "message": "Utente autenticato con successo",
  "ssoSessionId": "eb491e24-f0d9-42ff-96cb-da410d3f2979",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Utente autenticato con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success
ssoSessionId	String	Yes	Single Sign-on session id. If this is stored in a cookie with name "yetiSsoSession" an SSO session can be established.

5.16.2 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "ID token bad: Expired JWT",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Utente autenticato con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 both for success and failure

5.17 Call to Facebook Signin

This call is used by the "signin with facebook" functionality embedded in the Yeti provided credentials page. It is invoked by front-end javascript. However, if the adopting application opts to develop its own credentials page, they can use this call to sign-in and/or sign-up an authenticated user with a valid id token obtained from google/apple/etc.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/facebook_signin	POST	application/x-www-form-urlencoded

The input parameters are passed to the endpoint via POST a query string, for example:

```
POST /utente/facebook_signin HTTP/1.1
Host: www.yeti-sso.it
Content-Type: application/x-www-form-urlencoded
client_id=s6BhdRkqt3
&id_social=<user id obtained from facebook>
&cdSocial=facebook
&email=<some email>
&given_name=john
&family_name=smith
```

Field Name	Type	Mandatory	Description
id_social	String	Yes	Id obtained from Facebook. This is the unique identifier of the facebook user.
cdSocial	String	Yes	Possible values: facebook
client_id	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has its own client_id
given_name	String	No	
family_name	String	No	
email	String	Yes	

5.17.1 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "redirect": "no",
  "httpStatus": 200,
  "message": "Utente autenticato con successo",
```

```

    "ssoSessionId": "eb491e24-f0d9-42ff-96cb-da410d3f2979",
    "status": "ok"
}

```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	For success: "Utente autenticato con successo", for failure, the reason for the failure
httpstatus	Integer	Yes	200 for success
ssoSessionId	String	Yes	Single Sign-on session id. If this is stored in a cookie with name "yetiSsoSession" an SSO session can be established.

5.17.2 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```

{
    "httpStatus": 200,
    "message": "Manca il parametro idSocial in chiamata da front-end",
    "status": "ko"
}

```

Field Name	Type	Mandatory	Description
Status	String	Yes	"ok" for success, "ko" for failure
Message	String	Yes	For success: "Utente autenticato con successo", for failure, the reason for the failure
HttpStatus	Integer	Yes	200 both for success and failure

5.18 Call to Fetch Short-lived Signed Id Token

This call fetches a short-lived, signed, id token for the user identified by the access token supplied in the authorization header of the request; the lifetime of this token is defined by the configuration parameter "short_lived_jwt_seconds", which typically should be about 5 minutes. This call was introduced to enable other applications to obtain trusted user information from a yeti application, thus allowing them to do an "implicit sign-up / sign-in" without asking for credentials. The signing of the id token is done with an RSA private key, owned by Y-Tech, whose public key must be shared to the owners of the application wishing to use the implicit sign-up.

Endpoint	Http Method	Content Type
{{root_endpoint}}/utente/get_signed_id_token	POST	application/x-www-form-urlencoded

5.18.1 Input Parameters

These are passed to the endpoint via POST a query string, for example:

```
POST /utente/get_signed_id_token HTTP/1.1
```

```
Host: www.yeti-sso.it
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Authorization: Bearer SlAV32hkKG
```

```
sub=100100
```

```
&clientId=372831321
```

The http authorization header must contain a valid access token.

Field Name	Type	Mandatory	Description
Sub	String	Yes	User identifier
clientId	String	Yes	Set to the client_id value assigned by y-tech to the adopting application. Each adopting application has it's own client_id

5.18.2 Success Response

If the request is successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "id_token":
"eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiI5NjIiLCJhdWQiOiJHRU5PQSIsImVtYWlsX3Z1cm1maWVkJj
p0cnVlLCJiaXJ0aGRhdGUiOiIxO..snip..F49k9Yp3_glGZZPp7luhYljkpLCJZ1s7rZGPcc8jQ_oxS
kINxOQjT4Sz9vaXE_OkYskvs5md08k3DudHsMp5HVdlwTAa6KTCHidug",
  "status": "ok"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure

id_token	String	Yes	The id token of the user identified by the access token provided in the authorization header
httpstatus	Integer	Yes	200 for success

5.18.3 Failure Response

If the request is not successful, a 200 Http Status is returned, with a JSON Payload.

Example response:

```
{
  "httpStatus": 200,
  "message": "human readable error message",
  "status": "ko"
}
```

Field Name	Type	Mandatory	Description
status	String	Yes	"ok" for success, "ko" for failure
message	String	Yes	The reason for the failure
httpstatus	Integer	Yes	200 for success and for failure

6 Client Configuration

Each adopting application needs have a client-id assigned and to be configured in the Yeti system. The table below is a reference list of the configurable parameters managed by Yeti. It is not necessary to have a deep knowledge of this: a suitable client configuration will be suggested by Y-tech to the owner of the adopting application.

Field Name	Type	Mandatory	Description
cd_org	String	Yes	For Yeti internal use
ds_org	String	Yes	Description of the adopting application. Used in emails and error messages.
ds_sito	String	Yes	Description of the adopting application's web site. Used in emails and error messages.
cd_sso_domain	String	Yes	User domain code Multiple applications which share the same user base, will share the same code here
client_id	String	Yes	The openid client identifier
client_secret	String	No	The openid client secret. Mandatory for confidential clients. Typically not needed by native mobile apps
callback_uri	String	No	Contains a " " separated list of valid callback uris. The callback_uri passed to the authorization request must be present in this list, else an error is returned.
tp_double_opt_in	String	No	Type of double opt-in (email confirmation procedure). Possible values: null: none NONE: none RELAX: relaxed double opt-in STRICT: strict double opt-in VSTRICT: Very strict double opt-in
num_days_relaxed_double_opt_in	Float	No	Number of days of "relaxation" in relaxed double opt-in. This is the number of days Yeti will allow the user to access without confirming his email address by clicking on the link of the confirmation email.
fm_layout	String	Yes	Freemarker template layout to be used in the UI front-end pages (for example the login page, the registration page, and others).

fm_template_prefix	String	Yes	Freemarker template prefix for this client.
auth_code_lifetime_seconds	Integer	Yes	The validity lifetime in seconds of the code sent by Yeti in response to an authentication request. For greater security, this should be set to a small value, such as 30
access_token_validity_days	Float	Yes	The validity lifetime in days of the access token. Can have decimals. This configures how long an access token is valid for before a refresh request needs to be invoked.
refresh_token_validity_days	Float	No	The validity lifetime in days of the refresh token. Can have decimals. This configures how long aa refresh token is valid for before a new interactive user authentication needs to take place. If empty, the refresh token never expires. Typically the lifetime of the refresh token should be much longer than the access token.
id_token_validity_days	Float	Yes	The validity lifetime in days of the id token. Can have decimals. This configures how long an id token is valid for.
sso_cookie_lifetime_days	Float	Yes	The validity in days of the Yeti single sign-on session. Can have decimals.
alg	String	Yes	The algorithm to use in signing the id token JWT Possible values: RS256 – use asymmetric public / private key pair. The public key is available via the yeti JWK endpoint HS256 – use symmetric cryptography with the client secret
short_lived_jwt_seconds	Integer	No	Lifetime in seconds of the signed id token obtained via /utente/get_signed_id_token
fl_pkce_obbligatorio	Integer	Yes	Indicates if PKCE code challenge and verifier are mandatory (1) or not (0) for this client.
fl_implicit_flow_allowed	Integer	Yes	Configures whether the openid implicit and hybrid flows are allowed. Values: 1 (allowed), 0 (Not allowed)
backchannel_logout_url	String	No	Not implemented

accedi_url	String	No	
consent_url	String	No	
tp_autenticazione_migrazione	String	No	This is the type of authentication the client is using. Can be: Null: Email and password authentication "UPWD": Email and password authentication "OTP": Mobile phone number and one time password via SMS, Push or Email
double_opt_in_email_subject	String	No	Double opt in email subject
double_opt_in_email_from	String	No	Double opt in email "from" value
reset_password_email_subject	String	No	Password reset email subject
reset_password__in_email_from	String	No	Password reset email "from" value
fl_google_signin	Integer	No	Indicates whether or not the "Signin with Google" button should be shown. Values: 1 (Yes), 0 (No)
fl_facebook_signin	Integer	No	Indicates whether or not the "Signin with Facebook" button should be shown. Values: 1 (Yes), 0 (No)
fl_apple_signin	Integer	No	Indicates whether or not the "Signin with Apple" button should be shown. Values: 1 (Yes), 0 (No)
fl_microsoft_signin	Integer	No	Indicates whether or not the "Signin with Microsoft" button should be shown. Values: 1 (Yes), 0 (No)
fl_whitelist	Integer	No	Indicates whether or not access to certain services (eg. update user profile) should be restricted to a list of ip addresses. This is applicable when the adopting application chooses to invoke the service from the backchannel. If the service is invoked from the front-channel via the Yeti provided UI, this is not applicable (i.e. there is no restriction to the ip addresses) Values: 1 (Yes), 0 (No)

list_of_whitelist_ips	String	No	Comma separated list of ip addresses
cd_crm	String	No	CRM system code This will be provided by Yeti if the adopting application requires a CRM integration
google_client_id	String	No	Google client id Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
google_jwk_url	String	No	Google jwk url Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
facebook_app_id	String	No	Facebook app id Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
facebook_apiversion	String	No	Facebook API Version Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
microsoft_client_id	String	No	Microsoft Client Id Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
microsoft_authority	String	No	Microsoft Authority Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
microsoft_jwk_url	String	No	Microsoft jwk url Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
microsoft_secret	String	No	Microsoft Secret Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
apple_client_id	String	No	Apple Client Id

			Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
apple_jwk_url	String	No	Apple JWK url Please refer to the relevant (Google/Apple/Microsoft/Facebook) developer instructions on how to setup a social sign in.
fl_multi_lang	Integer	No	Indicates whether or not the pages should be multilingual. Default is No. Values: 1 (Yes), 0 (No)
cd_lang_default	String	No	2 character default language code. Example values: "it" (Italian), "en" (English)
privacy_expiry_days	Float	No	Indicates the number of days which need to elapse for the privacy acceptance flags to be considered expired. It is used to set a user attribute "privacy expiry date". It is included in the output of the "userinfo" endpoint.
short_lived_jwt_seconds	Integer	No	Indicates the validity lifetime of the id token produced by the "Call to Fetch Short-lived Signed Id Token" in number of seconds
otp_type	String	No	If the authentication type chosen is "OTP" (see above "tp_autenticazione_migrazione"), indicates the channel used for the OTP. Possible values: sms email push
otp_provider	String	No	Possible values: aws (Amazon Web Services) ... others to be implemented
otp_access_key	String	No	Access key to otp_provider
otp_secret_key	String	No	Secret key to otp_provider
otp_attr1	String	No	Depends on otp_provider and otp_type. In the case of Amazon, SMS, this contains the "Region" of the amazon servers used to send the SMSs
otp_attr2	String	No	Depends on otp_provider and otp_type

otp_mess_prefix	String	No	This is the text which should precede the OTP itself in the OTP message. Example: "Welcome to <web site name>! This is your One Time Password: "
post_userinfo_endpoint	String	No	If this contains a URL, such a URL will be invoked each time the user profile is changed, with http method POST, and containing a JSON payload like the payload returned by the /oidp/userinfo request.
min_age	Integer	No	Minimum age for sign-up (relevant only in presence of user's "birthdate")
warning_age	Integer	No	Warning age for sign-up(relevant only in presence of user's "birthdate")
fl_check_phone_unique	Integer	No	Indicates if the system should check for the uniqueness of a confirmed phone number. Values: 1 (Yes), 0 (No)
<u>fl_check_profile_compl on sso</u>	Integer	No	Indicates if the system should check for profile completeness on sso client switch. Values: 1 (Yes), 0 (No)

Further configuration options are available via the appropriate population of a "LOOKUP" table. An example is the opt_in email subject and sender (OPT_IN_SUBJECT, OPT_IN_EMAIL_FROM).