Piekuves talona(token) saemšana

Piekuves talona(token) saemšana

Description

This operation obtains an *OAuth 2.0* access token. This operation can be invoked as part of an OAuth 2.0 authorization code grant flow or via an OAuth 2.0 Service provider's credentials grant flow.

End-user access token

When the authorization code grant flow is used, the obtained access token represents the authorization granted by a end-user to the Service provider's application making the call for accessing certain resources or services on this end-user's behalf (identity data, signature identities, etc.). To obtain the token, the Service provider's application must present the authorization code obtained with the Obtain authorization operation.

This type access token is used to receive end-user's:

- Electronic identification;
- signing identities;
- eParaksts Mobile related signing and authentication certificates;
- PKSC#1 signature

Introspect access token

When the Service provider's credentials grant flow is used, the obtained access token demonstrates the administrative authorization of the Service provider's application making the call for accessing certain resources or services (i.e., without direct intervention of the resource's owner), or for accessing resources of the Service provider's application. Token is issued when the authorization server that processes the request is not associated to an identity provider. A token of this type can be used for accessing resources not associated to end-users or to end-user resources of any domain.

This type of access token is used to get access to Signature creation and validation service API's

Request

To obtain the token, the Service provider's application must send a request like the following to authorization server using TLS. This request is sent directly from the Service provider’s application to authorization server and does not go via the browser.

```
POST /trustedx-authserver/oauth/{as}/token
```

Parameter

Title	Type	Field	Description
as	path	mandatory	Identifier of the authorization server from which the token is requested available "**as**":

Content-Type Header

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

In HTTP POST request is necessary to incorporated the following main attribute: *Authorization* – API access token.

```
Authorization: Basic <API-Key>
```

Body

The content of the request varies according to the type of OAuth 2.0 flow in which the token is requested:

Content in the Case of the Authorization Code Grant Flow (used for electronic identification/signing requests)

Property	Usage	Description
`grant_type`	mandatory	Must have the **`authorization_code`** value.
`code`	mandatory	The authorization code received in the previous authorization response.
`redirect_uri`	mandatory	URI where the authorization response was received with the authorization code. Must match the **`redirect_uri`** parameter of the API authorization code request (see API authorization code request), and must be omitted if it is also omitted in the authorization request.

Content in the Case of the Client Credentials Grant Flow - Introspect access token (used for access SignAPI service)

Property	Usage	Description
`grant_type`	mandatory	Must have the **`client_credentials`** value .
scope	mandatory	Must have the **`urn:safelayer:eidas:oauth:token:introspect`** value

Introspect access token

Introspect piekuves talona (token) saemšana

Description

This operation obtains an *OAuth 2.0* access token. This operation can be invoked as part of an OAuth 2.0 Service provider's credentials grant flow.

Introspect access token

When the Service provider's credentials grant flow is used, the obtained access token demonstrates the administrative authorization of the S ervice provider's application making the call for accessing certain resources or services (i.e., without direct intervention of the resource's owner), or for accessing resources of the Service provider's application. Token is issued when the authorization server that processes the request is not associated to an identity provider. A token of this type can be used for accessing resources not associated to end-users or to end-user resources of any domain.

⚠ This type of access token is used to get access to Signature creation and validation service API's

Request

To obtain the token, the Service provider's application must send a request like the following to authorization server using TLS. This request is sent directly from the Service provider's application to authorization server and does not go via the browser.

```
POST /trustedx-authserver/oauth/{as}/token
```

Parameter

Title	Type	Field	Description
as	path	mandatory	Use "lvrtc-eipsign-as"

⚠ Host:

Test environment: eidas-demo.eparaksts.lv

Production: eidas.eparaksts.lv

Content-Type Header

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

In HTTP POST request is necessary to incorporated the following main attribute: *Authorization* – API access token.

```
Authorization: Basic <API-Key>
```

How to generate API Access Key

Before Service provider access Integration platform API, LVRTC shall register Service provider as customer of Integration platform. After signing a contract with LVRTC (Test of Production environment) LVRTC generates Service Provider's application identifier – (*client_id*) and shared secret (*client_secret*), intended for the customer usage.
API Access Key (API Key) is generated from the Service provider's application identifier (*client_id*), a secret shared with the platform (*client_secret*) on the following basis:

Service provider's application identifier *client_id* are converted using the UTF-8 character encoding and URL encoding conditions.

⚠ For example, value "Portls" conversion result is "port%C4%81ls".

Service provider's application password *client_secret* is converted by using the UTF-8 character encoding and URL encoding conditions.

⚠ For example, value "drošba" conversion result is "dro%C5%A1%C4%ABba".

Both values of the previous two steps must be combined with separator colon ":" between them.

⚠ For example, by using previous examples, the result will be "port%C4%81ls:dro%C5%A1%C4%ABba".

Obtained value must be converted using base 64 encoding without line breaks.

⚠ For example, values "port%C4%81ls:dro%C5%A1%C4%ABba" conversion result is "CG94ydCVDNCUMWxzOmRybyVDNSVBMSVDNCVBQmJh".

"MIME Tools" tool in "Notepad + +" can be used for this purpose.

```
API-Key = base64[url_encode(utf8(<client_id>)) ':' url_encode(utf8(<client_secret>))]
```

Body

The content of the request for Introspect access token (used for access SignAPI service):

Property	Usage	Description
`grant_type`	mandatory	Must have the *client_credentials* value .
scope	mandatory	Must have the *urn:safelayer:eidas:oauth:token:introspect* value

Example (Introspect access token)

The following example shows a situation in which the Service provider's application with the identifier "*Portal*" and the password "*drošba*" authority shall transmit the request to the server with the identifier "*lvrtc-eips-as*":

```
POST /trustedx-authserver/oauth/lvrtc-eipsign-as/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Authorization: Basic CG94ydCVDNCUMWxzOmRybyVDNSVBMSVDNCVBQmJh
Host: eidas-demo.eparaksts.lv
grant_type=client_credentials&
                        scope=urn%3Asafelayer%3Aeidas%3Aoauth%3Atoken%3Aintrospect
```

Response

In response, Integration platform authorization server issues a bearer-type OAuth 2.0 access token and returns it in a JSON structure.

```
{
"access_token" : {string},
"token_type" : "Bearer",
"expires_in" : {number}
}
```

Parameter

Property	Description
`access_token`	Access token generated by Authorization server. The token has the characteristics specified in the configuration of the authorization server that processed the request and consists of a random string of the number of bytes specified in the **Access token number of random bytes** (by default, 32), encoded in hexadecimal.
`token_type`	Type of access token. Always has the "*bearer*" value. (Bearer type OAuth 2.0 access token).
`expires_in`	Lifetime (in seconds) of the access token. The Service provider's application must perform the access the token authorizes before the token expires. This value can be configured in the **Token timeout** option of the authorization server (by default, 120 seconds). Once this timeout has expired, the token becomes invalid, and the Service provider's application must obtain another one if it wants to continue invoking the protected services.

Example

Introspect access token:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=utf-8
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
{
 "scope": "urn:safelayer:eidas:oauth:token:introspect",
 "access_token": "dfffb0d7f90bed142464750cacad5e4b9e23f58ecb1d77e3bdf706ba208ad16a",
 "token_type": "Bearer",
 "expires_in": 600
}
```

Example (end-users access token)

```
POST /trustedx-authserver/oauth/lvrtc-eipsign-as/token HTTP/1.1
Host: eidas-demo.eparaksts.lv
Authorization: Basic cG9ydCVDNCU4MWxzOmRybyVDNSVBMSVDNCVBQmJh
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

grant_type=authorization_code&
   redirect_uri=https%3A%2F%2Fwww.portals.lv%2Foauth%2Fback&
   code=4515...e0ba
```

Example (Introspect access token)

The following example shows a situation in which the Service provider's application with the identifier "**`Portal`**" and the password "**`drošba`**" authority shall transmit the request to the server with the identifier "**`lvrtc-eips-as`**":

```
POST /trustedx-authserver/oauth/lvrtc-eipsign-as/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Authorization: Basic cG9ydCVDNCU4MWxzOmRybyVDNSVBMSVDNCVBQmJh
Host: eidas-demo.eparaksts.lv
grant_type=client_credentials&
                        scope=urn%3Asafelayer%3Aeidas%3Aoauth%3Atoken%3Aintrospect
```

Response

In response, Integration platform authorization server issues a bearer-type OAuth 2.0 access token and returns it in a JSON structure.

```
{
"access_token" : {string},
"token_type" : "Bearer",
"expires_in" : {number}
}
```

Parameter

Property	Description
`access_token`	Access token generated by Authorization server. The token has the characteristics specified in the configuration of the authorization server that processed the request and consists of a random string of the number of bytes specified in the **Access token number of random bytes** (by default, 32), encoded in hexadecimal.
`token_type`	Type of access token. Always has the "**`bearer`**" value. (Bearer type OAuth 2.0 access token).
`expires_in`	Lifetime (in seconds) of the access token. The Service provider's application must perform the access the token authorizes before the token expires. This value can be configured in the **Token timeout** option of the authorization server (by default, 120 seconds). Once this timeout has expired, the token becomes invalid, and the Service provider's application must obtain another one if it wants to continue invoking the protected services.

Example

Access token with end-user authentication:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=utf-8
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
{
"access_token" : "a2b4...6daf",
"token_type" : "Bearer",
"expires_in" : 120
}
```

Introspect access token:

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=utf-8
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
{
 "scope": "urn:safelayer:eidas:oauth:token:introspect",
 "access_token": "dfffb0d7f90bed142464750cacad5e4b9e23f58ecb1d77e3bdf706ba208ad16a",
 "token_type": "Bearer",
 "expires_in": 600
}
```