POUŽÍVATEĽSKÁ PRÍRUČKA
EKS OAUTH

EKS OAuth príručka	verzia: č. 1.1
	dátum: 5.6.2018

História revízií

Verzia	Popis zmien	Dátum
1.0	Úvodný návrh príručky	7.8.2017
1.1	Doplnenie informácie o EKS prostredí pre vyžiadanie pridelenia oprávnenia správcu klientskych aplikácii	5.6.2018

OBSAH

1 ÚVOD

Účelom dokumentu je popis spôsobu a potrebných krokov pre využívanie služieb EKS OAuth pre prácu s API v EKS.

1.1 UPOZORNENIE

Obrázky znázornené v tejto príručke sa nemusia úplne zhodovať s obrazovkami, ktoré uvidíte pri práci s reálnym systémom. Rozdiely, ktoré môžete zaregistrovať vplývajú z toho, že v reálnom systéme sa priebežne jednotlivé obrazovky aktualizujú.

1.2 POJMY A POUŽITÉ SKRATKY

Skratka/Pojem	Význam
EKS	Elektronický kontraktačný systém
API	Skratka pre pojem : Application Programming Interface (rozhranie pre programovanie aplikácií)
Klientska aplikácia	Aplikácia požadujúca prístup k službám EKS API v mene používateľa EKS s jeho autorizáciou (third-party aplikácia). (V zmysle RFC6749 sa jedná o „Client“)
Správca klientskej aplikácie	Registrovaný používateľ s oprávnením evidencie registrovaných klientskych aplikácií v EKS
EKS používateľ	Registrovaný používateľ EKS.
Autorizačný server	Server poskytujúci služby autorizácie pre third-party aplikácie
API server	Server poskytujúci API služby EKS
OAuth	Reprezentuje autorizačný framework v zmysle odporúčania RFC6749
RFC6749	Štandard definujúci autorizačný framework pre získanie prístupu third-party aplikácii k http službám; https://tools.ietf.org/html/rfc6749

2 EKS OAUTH2

EKS poskytuje používateľom EKS a aplikáciám tretích strán štandardizované rozhranie pre autentifikáciu a autorizáciu aplikácie pre volanie EKS API služieb – EKS OAuth.

Pri príprave potrebných funkcionalít EKS OAuth bol dodržaný štandard RFC6749, ďalej len „štandard“.

V zmysle spomenutého štandardu vznikli v EKS podporné služby a funkcionality popísané v nasledujúcich kapitolách.

2.1 REGISTRÁCIA KLIENTSKEJ APLIKÁCIE

Pre prístup ku službám EKS API je nutné registrovať klientsku aplikáciu prostredníctvom nasledujúcich krokov:

2.1.1 OPRÁVNENIE SPRÁVCU KLIENTSKÝCH APLIKÁCII

Registrovaný používateľ EKS ako prvý krok musí požiadať Centrum podpory prevádzky EKS o pridelenie prístupu ku funkcionalite správy klientskych aplikácií. Žiadosť je potrebné podať vo forme mejlovej správy na mejlovú adresu Centra podpory EKS: podpora@eks.sk a v rámci ktorej je potrebné uviesť nasledovné informácie:

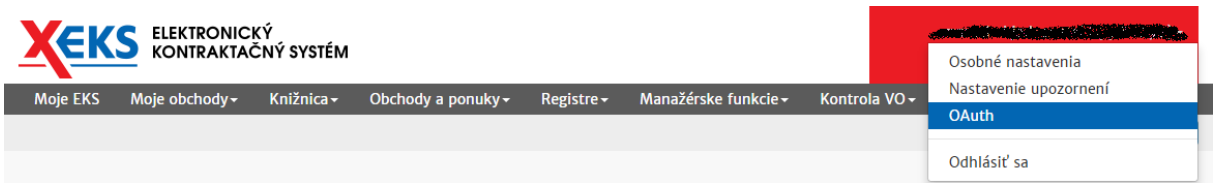
- Prostredie, na ktorom žiada o pridelenie prístupu: EKS produkčné prostredie alebo EKS test prostredie alebo oboje (odporúčané je žiadať o pridelenie prístupu na oboje prostredia)
- meno a priezvisko žiadateľa,
- identifikáciu používateľského účtu, ktorému je požadované pridelenie oprávnenia
- telefonický kontakt a mejlový kontakt žiadateľa

Po odoslaní žiadosti o pridelenie prístupu ku funkcionalite správy klientskych aplikácií a po jej preverení a vybavení centrum podpory EKS bude požívateľ o pridelení oprávnenia informovaný.

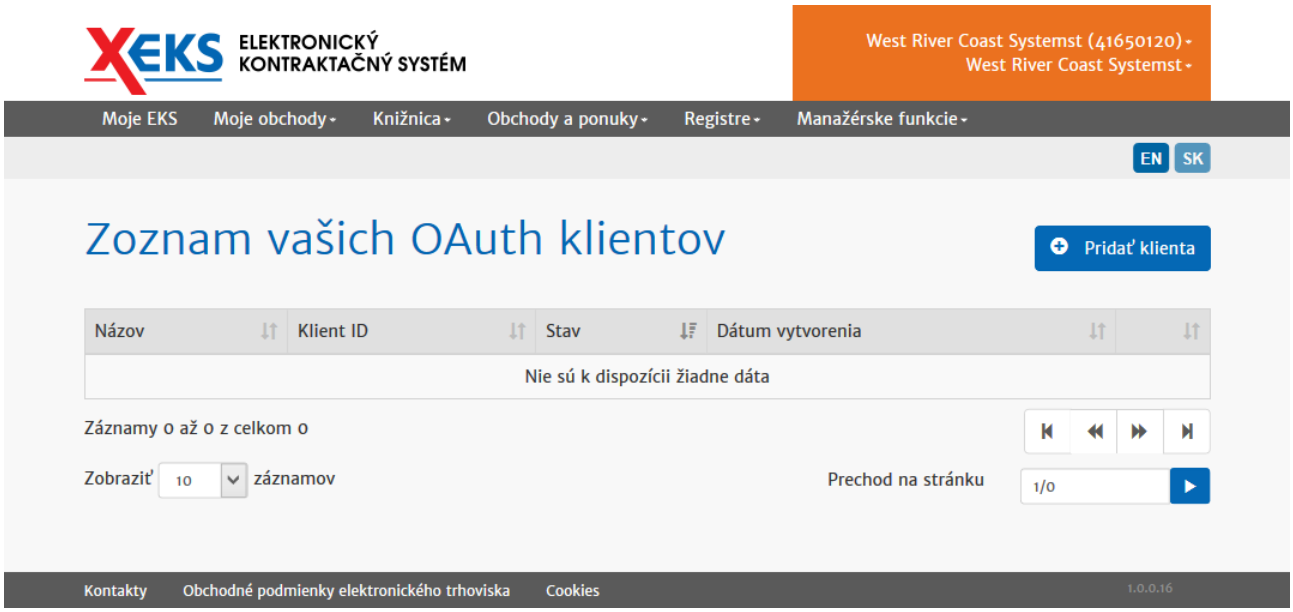
V prípade, ak má registrovaný používateľ už pridelený prístup k funkcionalite správy klientskych aplikácií, tento krok vynecháva.

2.1.2 REGISTRÁCIA KLIENTSKEJ APLIKÁCIE OAUTH

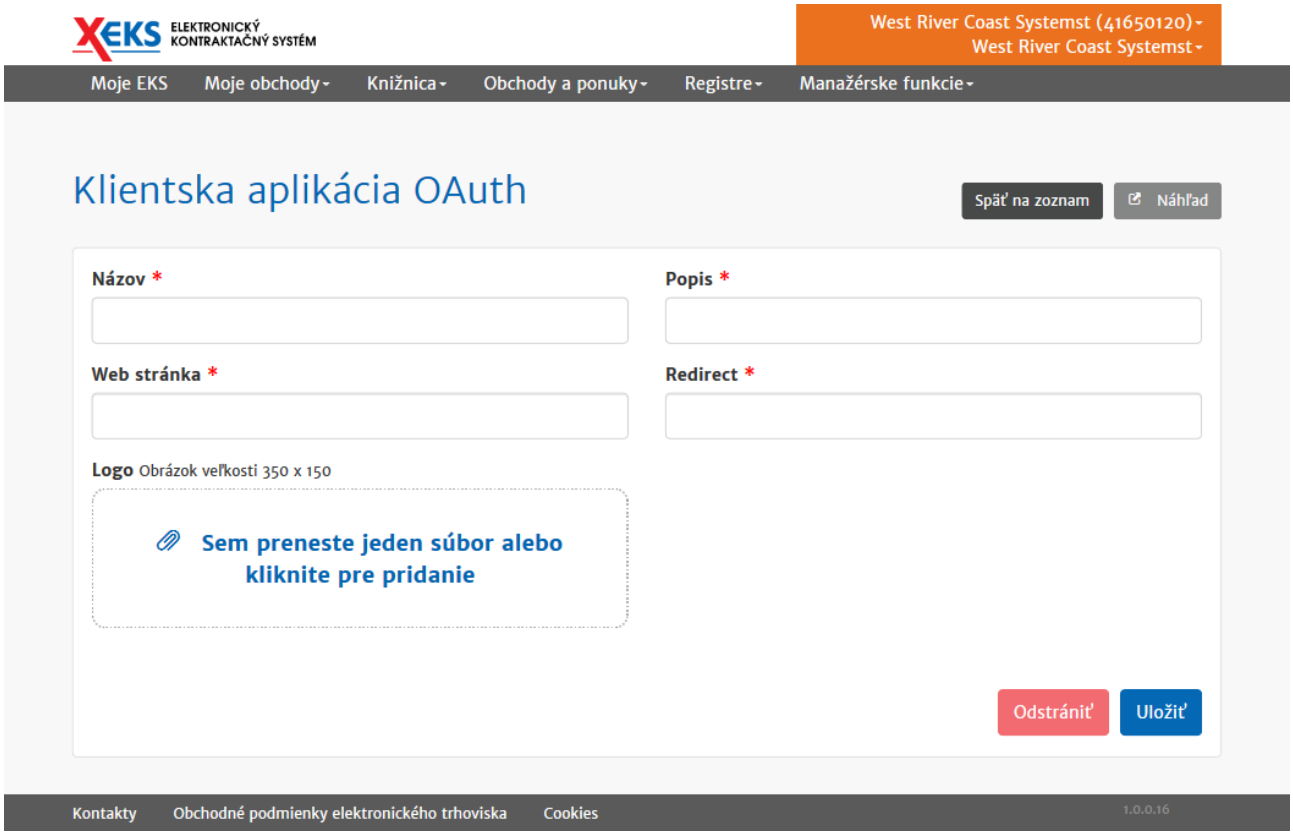
Pre zobrazenie prehľadu registrovaných klientskych aplikácií zvoľte položku menu OAuth v pravom hornom rohu:



Následne systém zobrazí zoznam vami registrovaných klientskych aplikácií OAuth:



Pre registrovanie novej klientskej aplikácie OAuth kliknite na tlačidlo „Pridať klienta“. A následne uveďte požadované údaje do zobrazeného formulára:



Nasledovne:

- Názov – názov vašej klientskej aplikácie
- Popis – popis vašej klientskej aplikácie
- Web stránka - URL odkaz na ďalšie informácie o vašej klientskej aplikácii
- Redirect – URL pre OAuth callback s informáciou o výsledku autentifikácie a autorizácie používateľom EKS, nezobrazuje sa v autorizačnej výzve používateľom EKS.
- Logo – obrázok s logom vašej klientskej aplikácie.

Po registrácii novej klientskej aplikácie systém vygeneruje ID a heslo, ktoré sú jedinečné pre každú klientsku aplikáciu (clientId a clientSecret v zmysle „štandardu“). Heslo je tajné a je prístupné len pre správcu klientskej aplikácie. Po zaregistrovaní klientskej aplikácie je možné okamžite využívať EKS API služby.

Pri zadávaní požadovaných údajov v tomto formulári berte na vedomie fakt, že tieto sú **zobrazované vo výzve používateľa EKS na autorizáciu vašej aplikácie pre prístup k údajom a volanie služieb API v EKS**. Z uvedeného dôvodu je nutné uvádzať korektné a správne informácie.

V prípade uvedenia nesprávnych alebo zavádzajúcich údajov môže správca EKS ukončiť platnosť vašej klientskej aplikácii.

2.2 AUTENTIFIKÁCIA A AUTORIZÁCIA KLIENTSKEJ APLIKÁCIE

Autentifikačný a autorizačný flow je spísaný v rámci „štandardu“.

2.2.1 AUTORIZÁCIA KLIENTSKEJ APLIKÁCIE

Klientska aplikácia musí pred použitím API služieb požiadať o pridelenie prístupového tokenu (access token v zmysle „štandardu“) . EKS OAuth podporuje spôsob pre získanie prístupového tokenu „Autorizačný request“ v zmysle „štandardu“.

2.2.1.1 Autorizačný kód request

- Klientska aplikácia požiada v mene používateľa o autorizačný kód.
- S autorizačným kódom požiada klientska aplikácia o pridelenie prístupového tokenu.
- S prístupovým tokenom môže klientska aplikácia používať API služby.

Klientska aplikácia presmeruje používateľa EKS prostredníctvom webového prehliadača (user agent-a v zmysle „štandardu“) a iniciuje požiadavku o pridelenie autorizačného kódu nasledovným requestom:

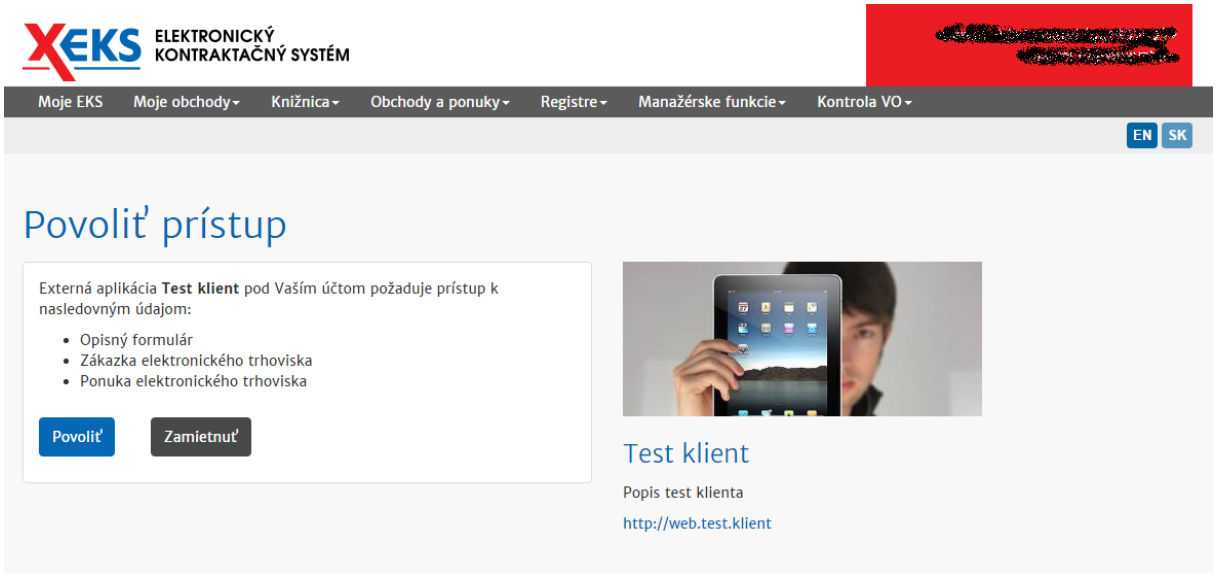
```
Request method: GET

https://oauth.eks.sk/authorize?response_type=code&client_id=__&redirect_uri=__&
scope=__&state=__
```

, kde význam jednotlivých parametrov je nasledovný:

Request Parameter	Význam
response_type	V zmysle „štandardu“, článok 4.1 je požadovaná hodnota „code“ pre vyžiadanie autorizačného kódu
client_id	Identifikátor, ktorý bol vygenerovaný systémom EKS pri registrácii klientskej aplikácie
redirect_uri	URI adresa, ktorú zadal správca klientskej aplikácie pri registrácii určená pre callback s informáciou o pridelenom autorizačnom a prístupovo kóde alebo o chybovom výsledku spracovania requestu
Scope	Rozsah služieb a údajov, ku ktorým klientska aplikácia požaduje získanie povolenia. Jednotlivé služby sú oddelené medzerou. Prípustné hodnoty sú: *OpisnyFormular* – pre prístup ku API službám opisného formulára *ZakazkaElektronickehoTrhoviska* – pre prístup k API službám správy zákaziek elektronického trhoviska *PonukaElektronickehoTrhoviska* – pre prístup k API službám správy ponúk elektronického trhoviska

Autorizačný server požiadavku spracuje nasledovne:

- Presmeruje EKS používateľa na stránku prihlásenia sa do EKS v prípade, ak ešte nie je prihlásený do EKS
- Následne zobrazí používateľovi výzvu na potvrdenie povolenia (autorizáciu) klientskej aplikácie pre prístup k údajom EKS a k službám EKS v mene prihláseného používateľa:



2.2.1.2 Autorizačný kód response

V prípade, ak používateľ v predchádzajúcom kroku potvrdil povolenie pre klientsku aplikáciu, tak autorizačný server vygeneruje autorizačný kód a odovzdá ho klientskej aplikácii prostredníctvom https requestu na URL uvedenú v registrácii klientskej aplikácie v poli „Redirect“:

```
https request method GET
redirect_uri?state=___&code=CODE
```

, kde význam jednotlivých vrátených parametrov je nasledovný:

Request Parameter	Význam
Redirect_uri	URI adresa, ktorú zadal správca klientskej aplikácie pri registrácii určená pre callback s informáciou o pridelenom autorizačnom a prístupovo kóde alebo o chybovom výsledku spracovania requestu
state	Identifikátor, ktorý poslala klientska aplikácia v predošlom requeste; z bezpečnostných dôvodov by nemala klientska aplikácia akceptovať reqest s nekorešpondujúcim údajom state.
code	Pridelený autorizačný kód

2.2.1.3 Prístupový kód request

Klientska aplikácia po obdŕžaní autorizačného kódu požiada o pridelenie prístupového kódu nasledovným requestom:

```
REQUEST POST method
https://oauth.eks.sk/token?grant_type=authorization_code&code=CODE
&redirect_uri=__&client_id=__&client_secret=__
```

, kde význam jednotlivých parametrov je nasledovný:

Request Parameter	Význam
grant_type	V zmysle „štandardu“, článok 4.1 je požadovaná hodnota „authorization_code“ pre vyžiadanie prístupového kódu
client_id	Identifikátor, ktorý bol vygenerovaný systémom EKS pri registrácii klientskej aplikácie
code	Pridelený autorizačný kód
redirect_uri	URI adresa, ktorú zadal správca klientskej aplikácie pri registrácii určená pre https callback s informáciou o pridelenom autorizačnom a prístupovo kóde alebo o chybovom výsledku spracovania requestu
client_id	Identifikátor, ktorý bol vygenerovaný systémom EKS pri registrácii klientskej aplikácie
client_secret	Tajný identifikátor, ktorý bol vygenerovaný systémom EKS pri registrácii klientskej aplikácie

2.2.1.4 Prístupový kód response

Autorizačný server vráti prístupový token:

```
RESPONSE:
{ "access_token":TOKEN }
```

V prípade spracovania s chybou, je táto vrátená vo forme response s http kódom 400 s popisom chyby v tele response:

```
RESPONSE:
{ "error": "popis chyby" }
```

2.3 VOLANIE SLUŽIEB EKS API

Pri každom volaní API služieb EKS je potrebné do http requestu pridať nasledovný header:

```
Authorization: Bearer TOKEN
```

, kde TOKEN predstavuje hodnotu prideleného prístupového tokenu (viď kapitola 2.2.1.4).