Сквозная авторизация на партнерском портале ООО “СкайДНС”

Для кого эта документация

Документация написана для партнеров ООО "СкайДНС". Описывает механизм создания ссылки на партнёрский портал, для обеспечения прозрачной авторизации пользователей.

Принцип действия

Принцип основан на безопасной передаче данных через небезопасную среду, проще говоря с помощью криптографической подписи.

Рассмотрим на примере: Допустим есть партнер "Рога и Копыта", который предоставляет услуги доступа в интернет. Есть кабинет партнера, через который клиенты партнера управляют услугами. Есть кабинет партнерского портала, через который пользователь может управлять сервисом ООО "СкайДНС". Требуется организовать бесшовную авторизацию на партнерском портале из кабинета партнера для его клиентов.

Для этого с помощью ключей доступа формируется подписанный URL, ведущий на партнерский портал. После перехода по URL пользователь авторизуется без ввода пароля. При этом, если неавторизованный пользователь попадает на партнерский портал, он перенаправляется на кабинет партнера для получения ссылки для авторизации.

Требования

1. Ключи доступа к API ООО "СкайДНС" и доменное имя портала. Ключи и доменное имя можно получить связавшись с отделом продаж;
2. Передать в ООО "СкайДНС" URL, где неавторизованный пользователь может получить ссылку для авторизации на партнерском портале;
3. Идентификатор пользователя на партнерском портале ООО "СкайДНС", его можно получить при создании пользователя, с помощью Provider Api ООО "СкайДНС";
4. Библиотека для криптографической подписи, см. далее.

Есть готовые реализации библиотеки криптографической подписи:

1. python - в фреймворке Django "django.core.signing";
2. python - библиотека "itsdangerous";
3. php - библиотека "itsdangerous-php";
4. javascript - библиотека "nobi".

Если используемый вами язык программирования не перечислен выше, вам необходимо самостоятельно найти или написать аналог вышеописанных библиотек.

Создание URL

Для создания URL вам потребуется private_key и доменное имя портала. Далее пример кода для формирования URL. Так же потребуется идентификатор пользователя, для которого мы генерируем ссылку.

Далее следует код на python:

```
from django.utils.crypto import get_random_string
from django.core import signing

key = 'private key'
domain = 'skydns.example'
username = 'user@partner'

data = {'ident': username, 'token': get_random_string()}
signer = signing.Signer(key, salt='skydns')
json = signing.JSONSerializer().dumps(data)
b64 = signing.b64_encode(json)
token = signer.sign(b64)

print 'https://%s/welcome?%s' % (domain, token)
```

Где key это приватный ключ, domain доменное имя портала, username это идентификатор пользователя. Полученный URL можно разместить в месте доступном пользователю.

Данным URL можно воспользоваться только один раз, и в течение некоторого времени, после этого данный токен становится не валидным.

Использование URL

Далее полученный URL нужно отобразить пользователю, что бы он перешел по нему на портал.

Так же необходимо передать нам URL, по которому пользователь, не авторизованный на нашем портале, мог бы авторизоваться. Как правило это URL личного кабинета партнера.

Пример кода на php

При возможности заменить функцию generateRandomString на криптографически безопасную random_bytes из модуля CSPRNG.

```
<?php
require("itsdangerous.php");

function generateRandomString($length = 10) {
    $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $charactersLength = strlen($characters);
    $randomString = '';
    for ($i = 0; $i < $length; $i++) {
        $randomString .= $characters[rand(0, $charactersLength - 1)];
    }
    return $randomString;
}

$key = "private key";
$domain = "skydns.example";
$username = "user@partner";
$complex = array(
    "ident" => $username,
    "token" => generateRandomString(10)
);
$ser = new ItsDangerous\Signer\Serializer($key);
$c = $ser->dumps($complex);



$url = sprintf("https://%s/welcome?%s", $domain, base64_encode($c));

print $url;
```

Revision #3
Created 8 December 2023 13:12:11 by Виктор
Updated 8 October 2024 06:25:33 by Виктор