CMS.IO, Authentication

Dominik Pinter, dominikp@kentico.com

Kentico

Agenda

CMS.IO:

- Implementation details
- Pitfalls

Authentication:

- HTTP basic authentication
- ASP.NET Forms authentication
- OAuth

CMS.IO implementation details

- How to start?
- Provider registration
- REST API vs. Client SDK vs. Own wrapper
- Recommended object model
- Storage features and characteristics
  - Root directory object
  - Flat structure
  - Default properties
  - Shared storage between servers

CMS.IO – Writing a provider - pitfalls

- Authentication and authorization
- How to create directory?
- Where to store file metadata?
- Datacenter time zone
- What to do if
  - File does not exist? (AKA System.IO related stuff)
  - Connection to storage service is lost? (AKA storage related stuff)

Kentico

CMS.IO - demos

- Provider registration
- Working with CMS.IO
- File creation/deletion
- Directory creation/deletion

HTTP basic authentication

- Support in HTTP protocol
- HTTP response 401
- User name and password encoded in Base64
- Not safe without SSL (HTTPS)

```
GET http://localhost/page HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 …
Accept: text/html,application/xhtml+xml,application …
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Authorization: Basic dXNlcjpwYXNzd29yZA==
```

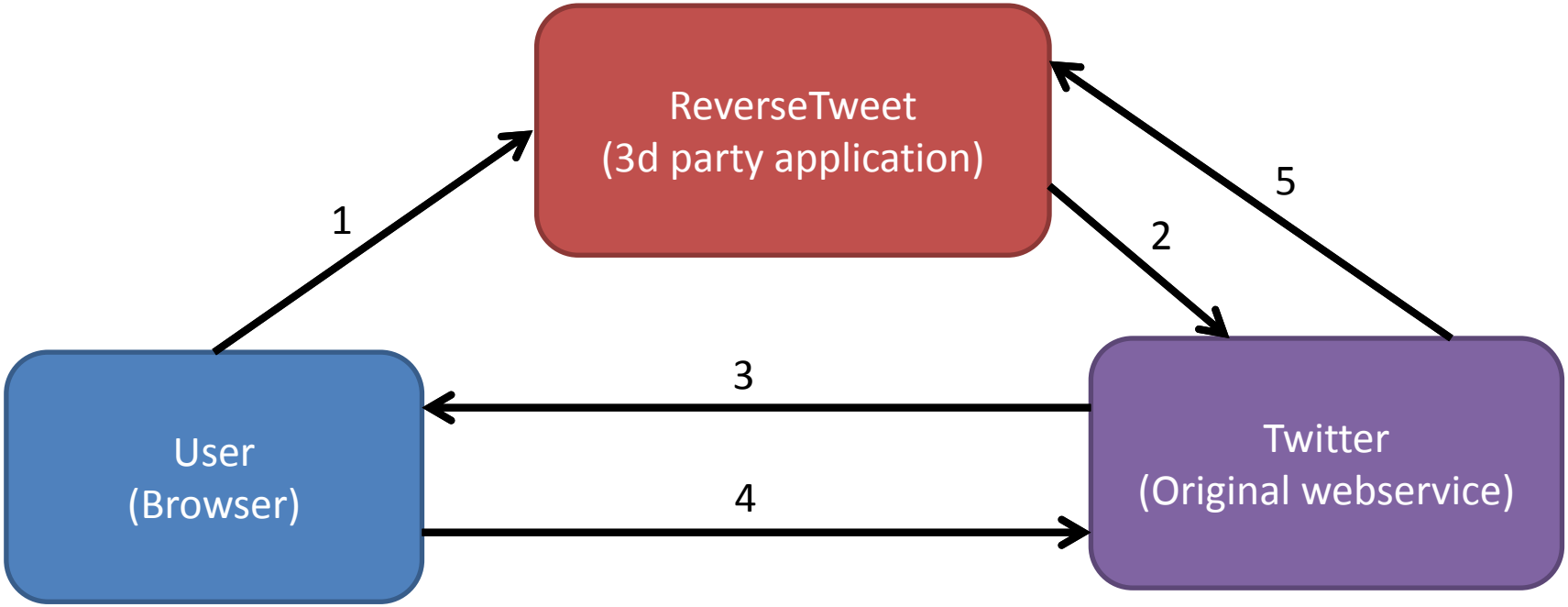
ASP.NET Forms authentication

- Built in ASP.NET
- Uses forms and HTTP POST
- Cookie based
- Configurable through web.config
- Integrated with ASP.NET membership provider

OAuth - basics

- An authentication mechanism for web applications/web services
- **Problem**: 3rd applications built upon existing web services, for example social networks need access to your an user account. The use doesn‘t want to give them an user name and password.
- **Solution**: The original web service can give them a temporary token for accessing the use account.
- OAuth 1.0 - RFC 5849 http://tools.ietf.org/html/rfc5849
- OAuth 2.0 – draft http://tools.ietf.org/html/draft-ietf-oauth-v2-31

OAuth – how it works



1. User sends request to 3rd party application
2. 3rd party application requests access token
3. User is redirected to original web service
4. User authenticates by user name and password to original web service
5. 3rd party application gets the access token

Kentico

OAuth - demo

ReverseTweet

Kentico

Homework

File manipulation

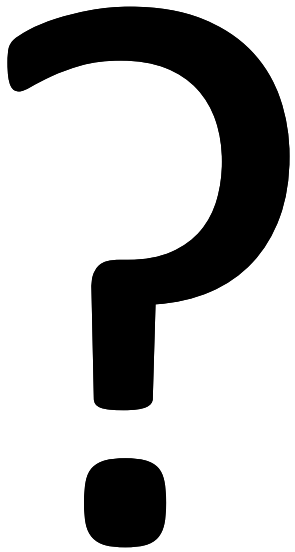
CMS.IO

Create file

Delete file

Kentico

Q&A



Kentico

Thank you

http://www.kentico.com
http://devnet.kentico.com
dominikp@kentico.com