

 <https://beyondj2ee.wordpress.com/2013/03/21/당신의-api가-restful-하지-않은-5가지-증거/>

오늘은

HTTPS와 REST

먼저 HTTPS

HTTP

+

Secure Socket Layer

SSL이 정보를
암호화 하는 방법

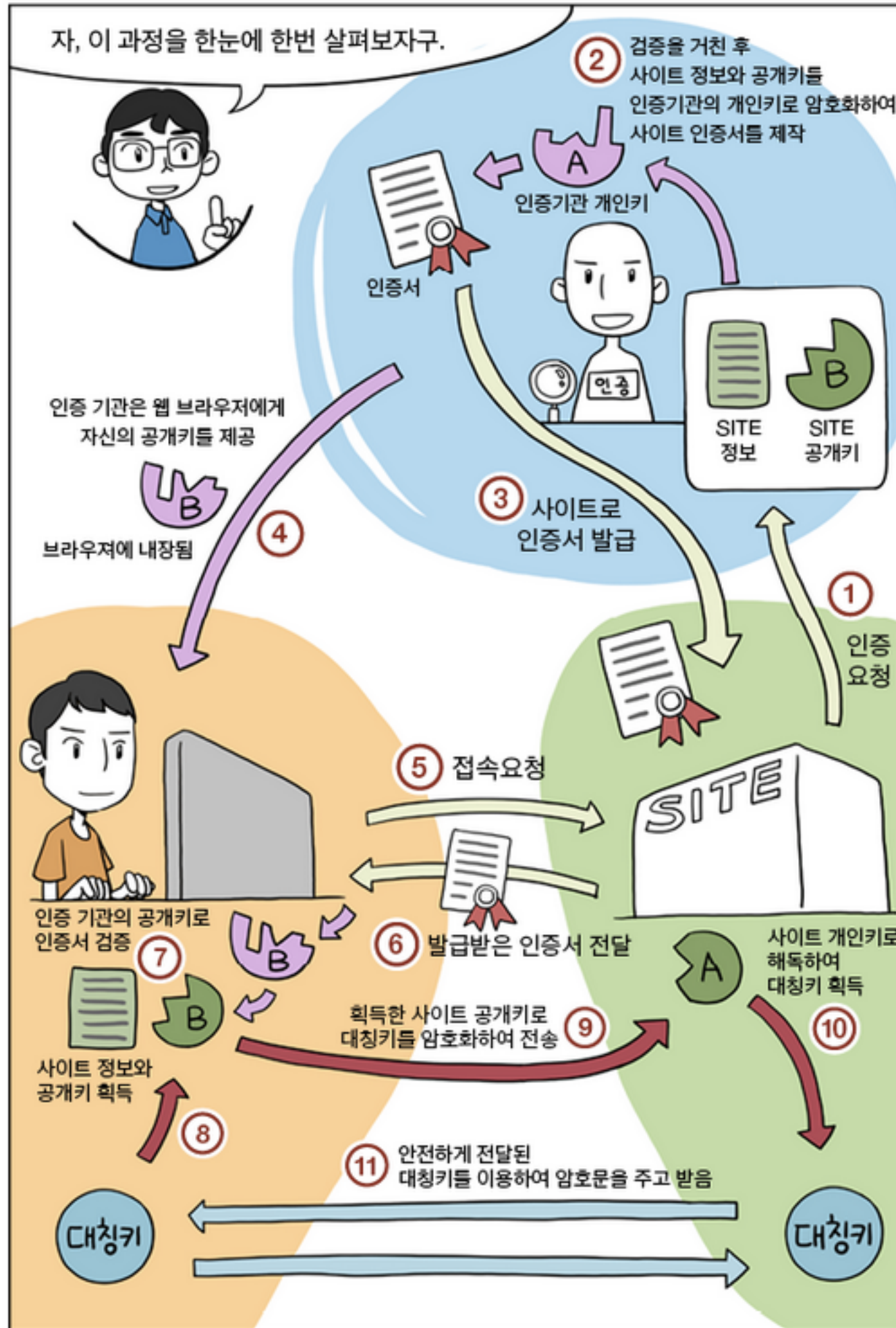
Symmetric-key Algorithm

- 시저암호 같은 건데 대칭키 없이는 풀기 어려움
- 꽤 안전한데 문제는 대칭키만 있으면 쉽게 풀어버림
- 복호를 해야하는 사람에게 대칭키를 줘야만 함
- 주다가 중간에 뺏기면 망함
- 그래도 빨라서 아직도 데이터를 이 방식으로 암호화함
- 그래서 대신에 RSA로 대칭키자체를 암호화함

RSA

- 암호키가 2개
- A로 암호화하면 B로 복호화, B로 암호화하면 A로 복호화가능
- A키는 모든 사용자에게 뿌림, B키는 서버 혼자만 가지고 있음
- 사용자가 A로 암호화해서 서버만 복호화 가능
- 정보 자체를 RSA키로 암호화,복호화하기에는 CPU가 부담됨

자, 이 과정을 한눈에 한번 살펴보자구.

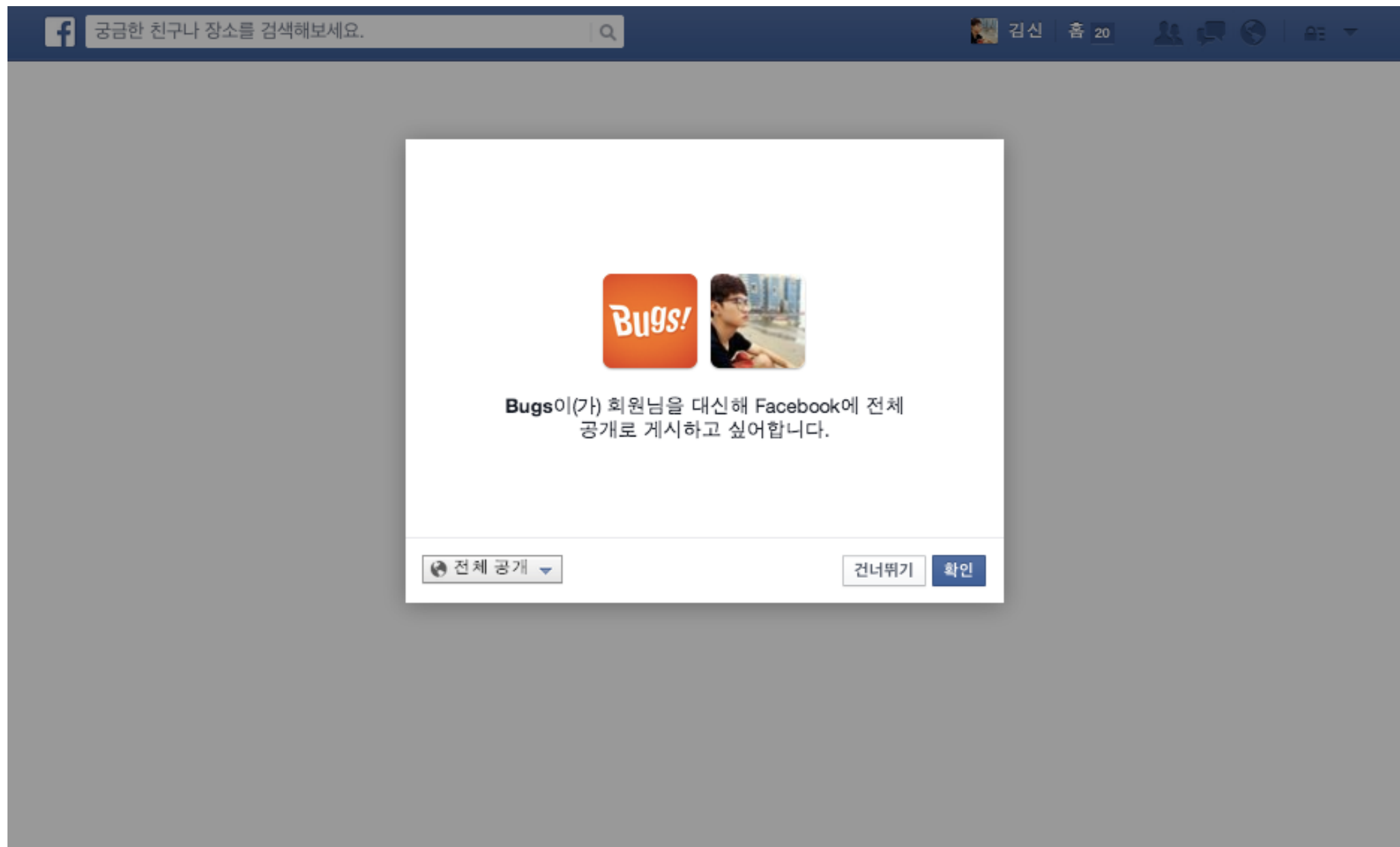


출처 링크

그래도 서버 개발자가
나쁜 사람이면 망함

OAUTH

보안하던 김에 마저 해봅시다



이게 OAuth.

원래는 많았는데 다 합침

- 구글의 AuthSub
- AOL의 OpenAuth
- 야후의 BBAuth
- 아마존의 웹서비스 API

용어정리만 한번하고 넘어가겠음

- User: 사용자
- Service Provider: 로그인 API 제공하는 곳
- Consumer: 로그인 API를 사용하는 사이트
- Request Token:
 - 어디서 로그인 시도하는지 consumer-service provider
- Access Token: 로그인 됨. 어디까지 접근되는지.

인증방식

- 소비자가 서비스제공자에게 요청토큰을 요청한다.
- 서비스제공자가 소비자에게 요청토큰을 발급해준다.
- 소비자가 사용자를 서비스제공자로 이동시킨다. 여기서 사용자 인증이 수행된다.
- 서비스제공자가 사용자를 소비자로 이동시킨다.
- 소비자가 접근토큰을 요청한다.
- 서비스제공자가 접근토큰을 발급한다.
- 발급된 접근토큰을 이용하여 소비자에서 사용자 정보에 접근한다.

REST

Representational State Transfer

식별자로 할 수 있는 유일한 일은 대상을 나타내는 것이다. 역참조를 할 때가 아니라면 다른 정보를 얻기 위해서 URI의 내용을 들여다보지 말아야 한다.

– 팀 버너스리(<http://www.w3.org/DesignIssues/Axioms.html>)

URI를 아름답게



URI는 리소스와 메소드

URI는 리소스와 메소드

- User 리스트 보기: Get /users/
- User 생성 폼: /user/new
- User 생성 : POST /user/93403
- User 수정 : PUT /user/93403
- User 조회 : GET /user/93403
- User 취소 : DELETE /user/93403

리소스는 명사
메소드는 동사

꼭 알아둬야 할 URL 규칙

- 슬래시(/)는 계층구조일때만 쓴다.
- ex) <https://examplecom/2013/03/21/bobobobo>
- 동사가 쓰고 싶을 때는 다시 한번 생각해보자
- _보다는 -를 추천

응답상태코드

- 1XX 조건부 응답
- 2XX 성공
- 3XX 리디렉션 완료
- 4XX 요청 오류
- 5XX 서버 오류

알아둬야 할 응답 상태 코드

- 200 OK
- 304 Not Modified
- 400 Bad Request
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

그 밖의 응답 상태 코드들

REST가 완전 답은 아니다

HEAD에 담아야 할 Meta Data

```
HTTP/1.1 200 OK
Date: Mon, 30 Jun 2014 09:24:16 GMT
Server: Apache
Last-Modified: Sat, 01 Sep 2012 18:32:44 GMT
ETag: "149-4c8a82265cb00"
Accept-Ranges: bytes
Content-Length: 329
Vary: Accept-Encoding
Content-Type: text/html
```

자잘한 규칙들은
곧 정리해서 올리겠음

지난번에 한 거 복습합시다