OAuth2 Criticism & Concerns

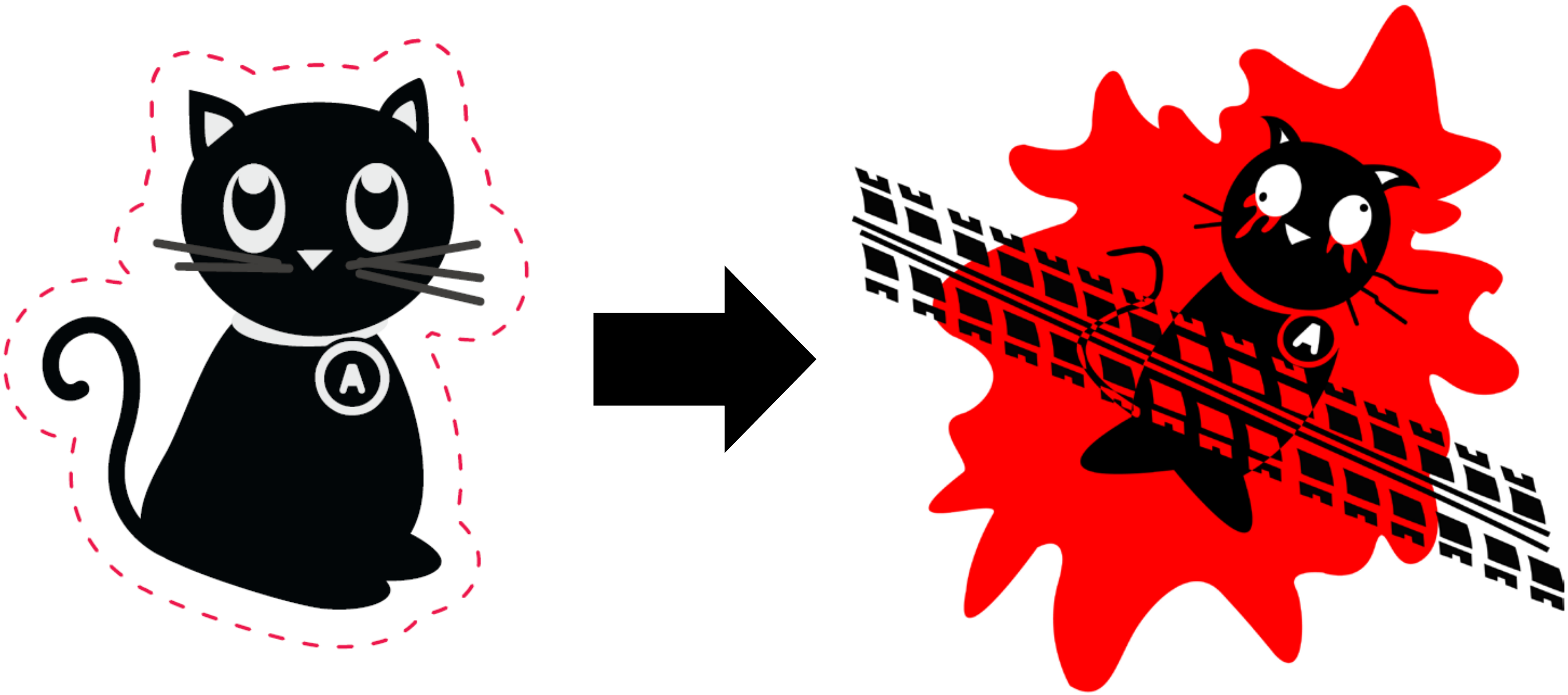
Dominick Baier

http://leastprivilege.com

@leastprivilege

pluralsight
hardcore developer training

Criticism & Concerns



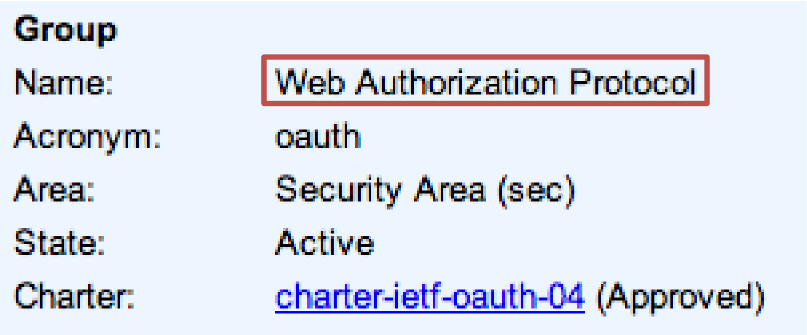
artwork by **@ChrisMCarrasco**

Eran Hammer

- **http://hueniverse.com/2010/09/oauth-bearer-tokens-are-a-terrible-idea/**
- **http://hueniverse.com/2010/09/oauth-2-0-without-signatures-is-bad-for-the-web/**

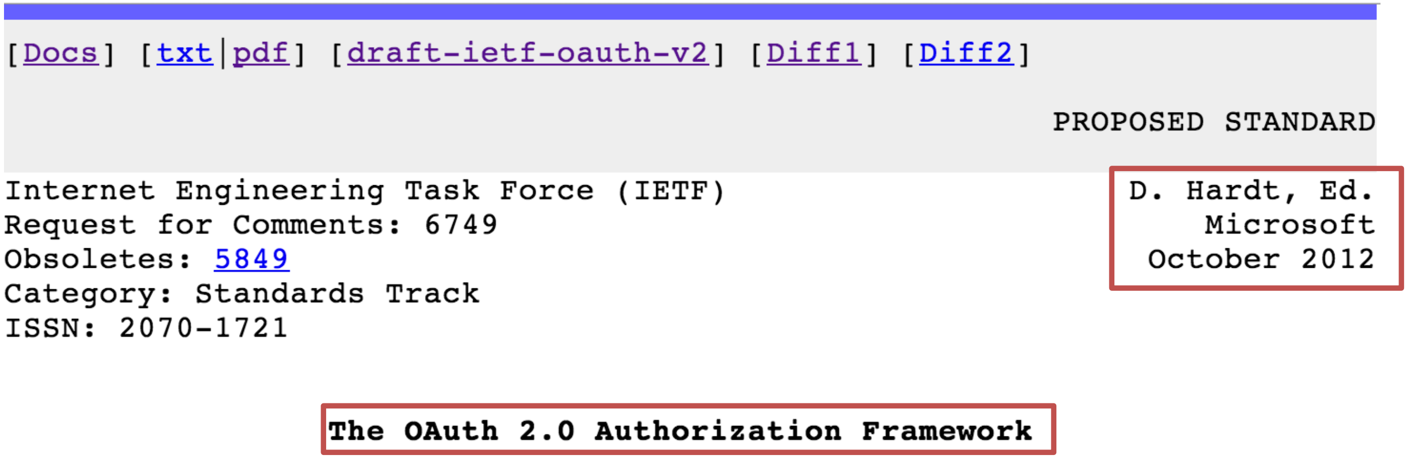
- **http://hueniverse.com/2012/07/oauth-2-0-and-the-road-to-hell/**

- **OAuth2: Looking back and moving on**
  - https://vimeo.com/52882780



Group

Name:	Web Authorization Protocol
Acronym:	oauth
Area:	Security Area (sec)
State:	Active
Charter:	charter-ietf-oauth-04 (Approved)



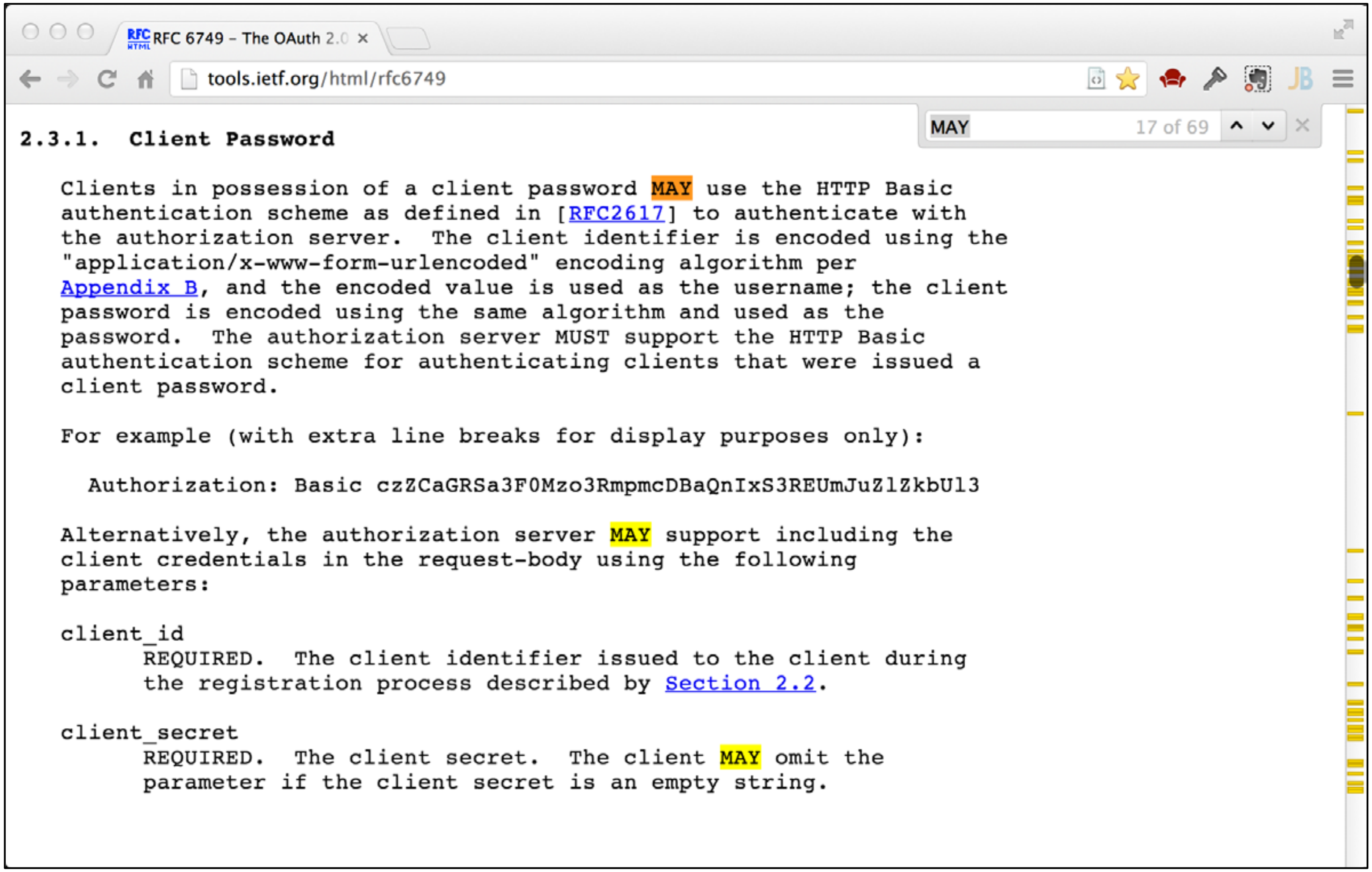
[Docs] [txt|pdf] [draft-ietf-oauth-v2] [Diff1] [Diff2]

PROPOSED STANDARD

```
Internet Engineering Task Force (IETF)                    D. Hardt, Ed.
Request for Comments: 6749                                    Microsoft
Obsoletes: 5849                                            October 2012
Category: Standards Track
ISSN: 2070-1721
```

The OAuth 2.0 Authorization Framework

"A Framework to build Protocols"



```
2.3.1.  Client Password

   Clients in possession of a client password MAY use the HTTP Basic
   authentication scheme as defined in [RFC2617] to authenticate with
   the authorization server.  The client identifier is encoded using the
   "application/x-www-form-urlencoded" encoding algorithm per
   Appendix B, and the encoded value is used as the username; the client
   password is encoded using the same algorithm and used as the
   password.  The authorization server MUST support the HTTP Basic
   authentication scheme for authenticating clients that were issued a
   client password.

   For example (with extra line breaks for display purposes only):

     Authorization: Basic czZCaGRSa3F0Mzo3RmpmcDBaQnIxS3REUmJuZlZkbUl3

   Alternatively, the authorization server MAY support including the
   client credentials in the request-body using the following
   parameters:

   client_id
         REQUIRED.  The client identifier issued to the client during
         the registration process described by Section 2.2.

   client_secret
         REQUIRED.  The client secret.  The client MAY omit the
         parameter if the client secret is an empty string.
```

JSON Web Token (JWT)

JSON Web Encryption (JWE)
JSON Web Signatures (JWS)
JSON Web Algorithms (JWA)

Assertion Framework for OAuth2
JWT Bearer Token Profiles
SAML 2.0 Bearer Token Profiles
Token Revocation
MAC Tokens

The OAuth2
Authorization Framework
(RFC 6749)

OAuth2
Bearer Token Usage
(RFC 6750)

Threat Model and
Security Considerations
(RFC 6819)

Core (proposed standards)

Informational

OAuth2 Resource Set Registration
Dynamic Client Registration
User-Managed Access
Chaining and Redelegation
Metadata & Introspection

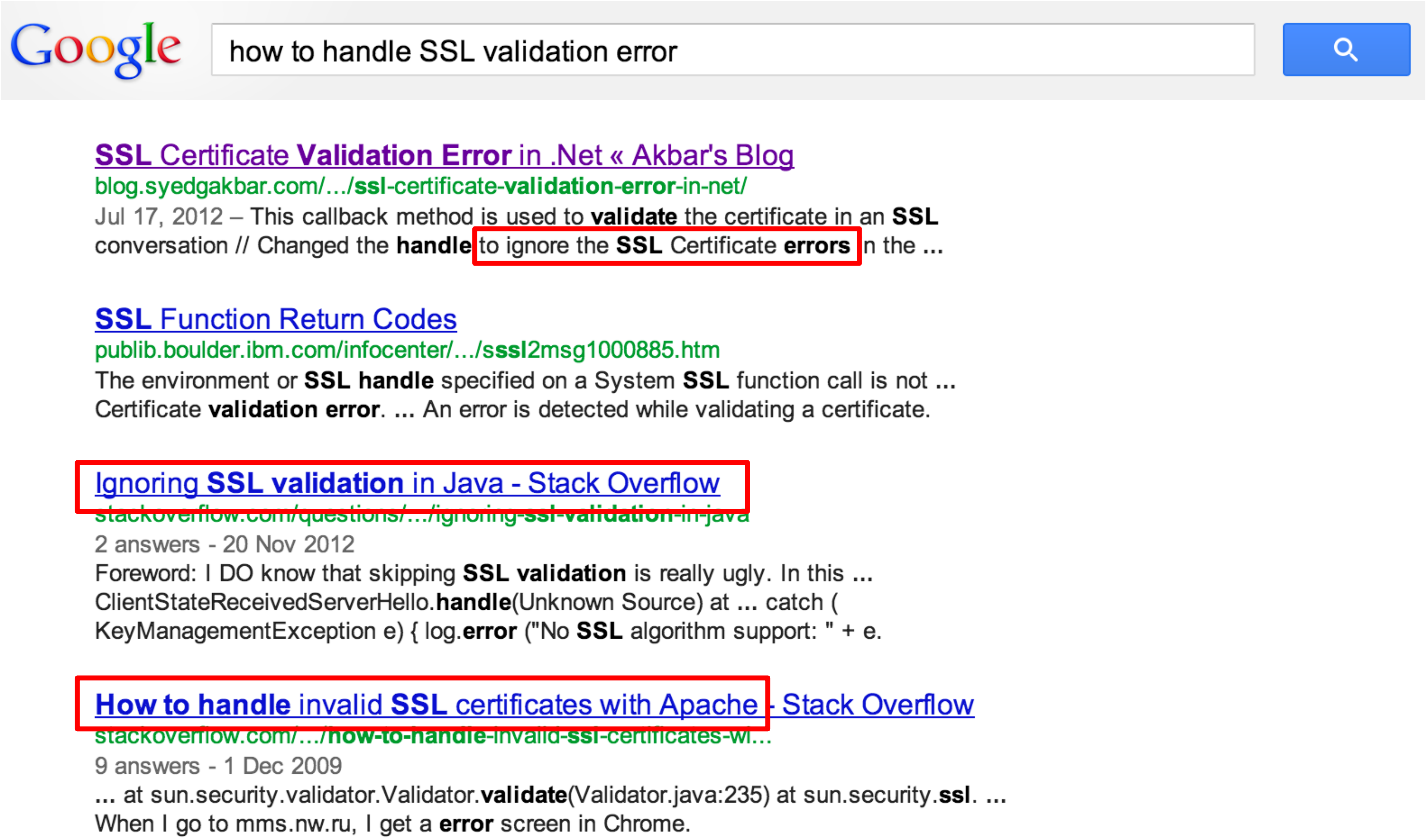
http://openid.net/specs/openid-connect
basic-1_0-23.html
implicit-1_0-06.html
messages-1_0-15.html
standard-1_0-16.html
discovery-1_0-12.html
registration-1_0-14.html
session-1_0-11.html

http://datatracker.ietf.org/wg/oauth/

Bearer Token

A security token with the property that any party in possession of the token (a "bearer") can use the token in any way that any other party in possession of it can. Using a bearer token does not require a bearer to prove possession of cryptographic key material (proof-of-possession).

Developers & SSL



how to handle SSL validation error

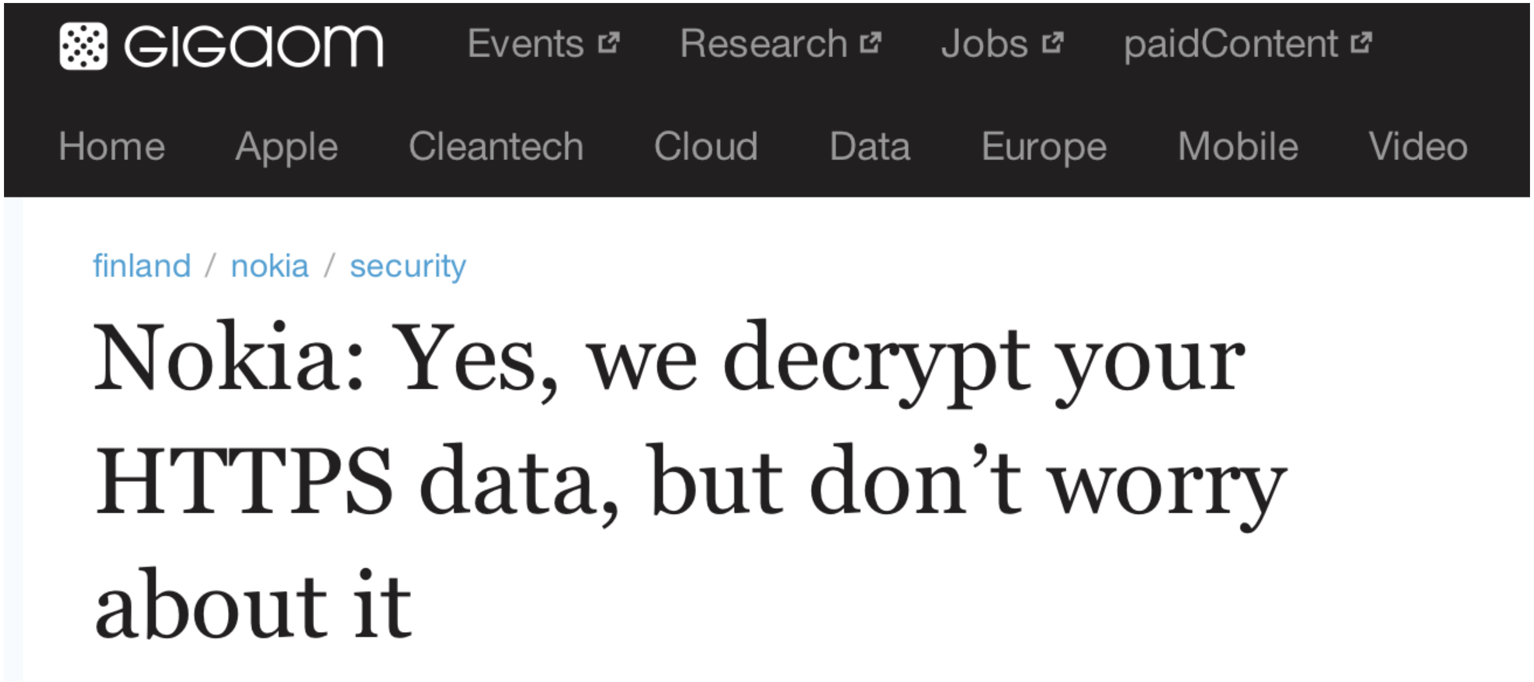
SSL Certificate **Validation Error** in .Net « Akbar's Blog
blog.syedgakbar.com/.../**ssl**-certificate-**validation**-**error**-in-net/
Jul 17, 2012 – This callback method is used to **validate** the certificate in an **SSL** conversation // Changed the **handle** to ignore the **SSL** Certificate **errors** in the ...

SSL Function Return Codes
publib.boulder.ibm.com/infocenter/.../s**ssl**2msg1000885.htm
The environment or **SSL handle** specified on a System **SSL** function call is not ... Certificate **validation error**. ... An error is detected while validating a certificate.

Ignoring **SSL validation** in Java - Stack Overflow
stackoverflow.com/questions/.../ignoring-**ssl**-**validation**-in-java
2 answers - 20 Nov 2012
Foreword: I DO know that skipping **SSL validation** is really ugly. In this ... ClientStateReceivedServerHello.**handle**(Unknown Source) at ... catch (KeyManagementException e) { log.**error** ("No **SSL** algorithm support: " + e.

How to handle invalid **SSL** certificates with Apache - Stack Overflow
stackoverflow.com/.../**how-to-handle**-invalid-**ssl**-certificates-wi...
9 answers - 1 Dec 2009
... at sun.security.validator.Validator.**validate**(Validator.java:235) at sun.security.**ssl**. ... When I go to mms.nw.ru, I get a **error** screen in Chrome.

Infrastructure & SSL

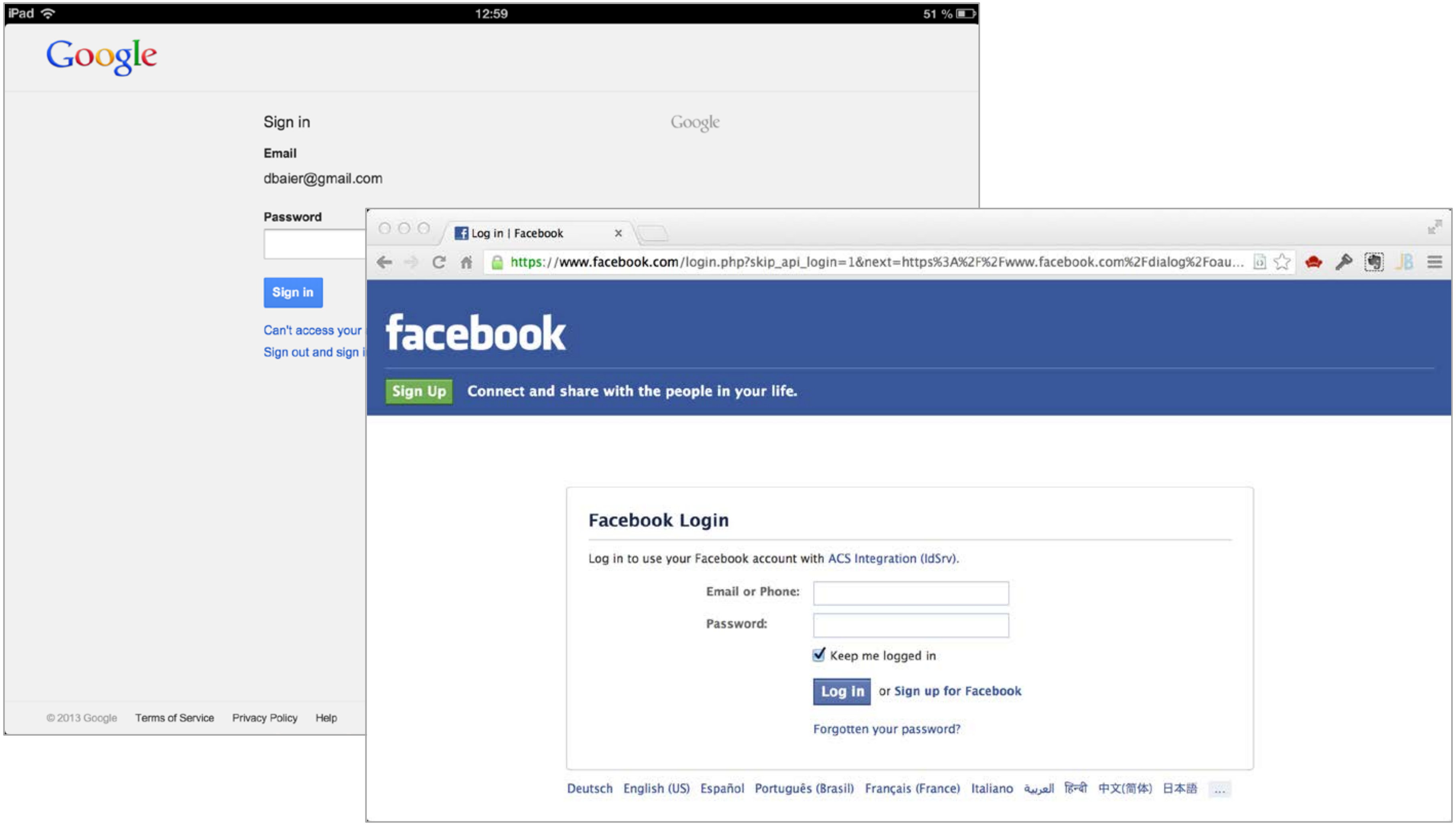


finland / nokia / security

Nokia: Yes, we decrypt your HTTPS data, but don't worry about it

http://gigaom.com/2013/01/10/nokia-yes-we-decrypt-your-https-data-but-dont-worry-about-it/

Security Theater



iPad 12:59 51 %

Google

Sign in

Google

Email

dbaier@gmail.com

Password

Sign in

Can't access your

Sign out and sign i

© 2013 Google Terms of Service Privacy Policy Help

Log in | Facebook

https://www.facebook.com/login.php?skip_api_login=1&next=https%3A%2F%2Fwww.facebook.com%2Fdialog%2Foau...

facebook

Sign Up Connect and share with the people in your life.

Facebook Login

Log in to use your Facebook account with ACS Integration (IdSrv).

Email or Phone:

Password:

☑ Keep me logged in

Log in or Sign up for Facebook

Forgotten your password?

Deutsch English (US) Español Português (Brasil) Français (France) Italiano العربية हिन्दी 中文(简体) 日本語 ...

OAUTH2
ATTACK SURFACE EVERYWHERE

Attack Surface

```
GET /authorize?
  client_id=nativeapp&
  redirect_uri=http://localhost/cb&
  scope=resource&
  response_type=token&
  state=123
```

http://leastprivilege.com/2013/03/15/common-oauth2-vulnerabilities-and-mitigation-techniques/
http://leastprivilege.com/2013/03/15/oauth2-security/
http://homakov.blogspot.de/2012/08/saferweb-oauth2a-or-lets-just-fix-it.html

Some Facebook Hacks

- http://www.darkreading.com/blog/240148995/ the-road-to-hell-is-authenticated-by-facebook.html
- http://homakov.blogspot.no/2013/02/hacking-facebook-with-oauth2-and-chrome.html
- www.nirgoldshlager.com/2013/03/ how-i-hacked-any-facebook-accountagain.html

Summary

- **The OAuth2 "approach" is useful for many typical applications scenarios**

- **Spec needs some refinement**
  - "basic profile"
  - MAC tokens
- **Current implementations are lacking**
  - even by the big guys
  - let alone the myriad of DIY implementations

- **Very good & balanced view**
  - https://www.tbray.org/ongoing/When/201x/2013/01/23/OAuth