

API Security

PHP|Tek 2012

Rob Richards
r-richards@mashery.com



Who am I?

Rob Richards

Mashery

Email: rrichards@mashery.com

Twitter: [@mashery](https://twitter.com/mashery)

Slides: www.cdatazone.org



WWW



Danger! Danger!



Traditional Web Site



- Browser based
- Tightly controlled ecosystem
 - UI
 - Data
 - Interaction



Chrome



Firefox



Internet Explorer



Konqueror



Opera



Safari

APIs



- Accessed by any number of apps, devices, browsers
- Increased threat exposure
 - Direct attack on API
 - End-user deception attack
 - Inadvertent attack



Apps Gone Wild!



I'm Under Attack!

(A True Story)



- Customer becoming flooded

I'm Under Attack!

(A True Story)



- Customer becoming flooded
- Looks like a DDoS



I'm Under Attack!

(A True Story)



- Customer becoming flooded
- Looks like a DDoS
- Identify Attacker

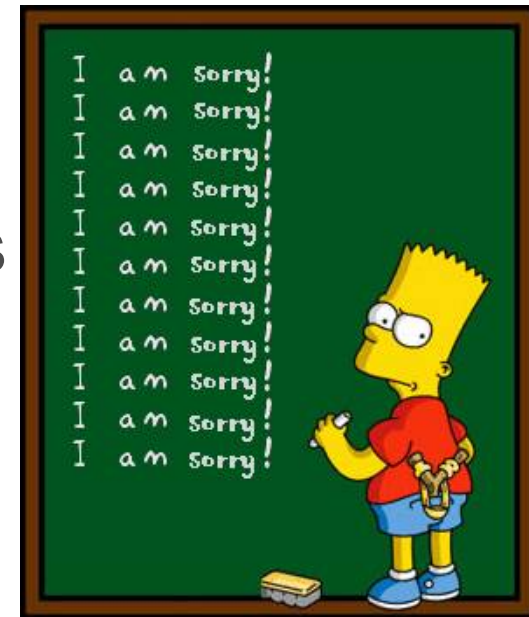


I'm Under Attack!

(A True Story)

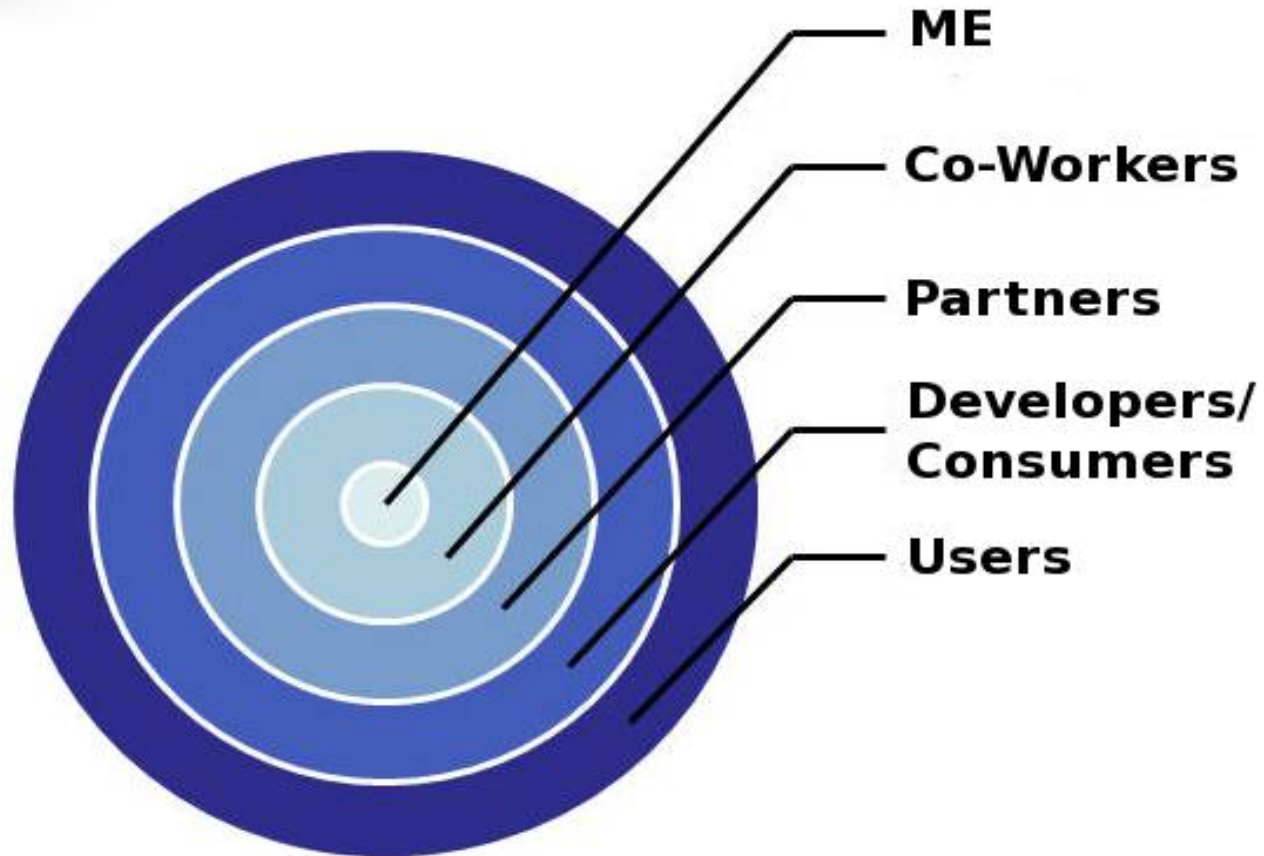


- Customer becoming flooded
- Looks like a DDoS
- Identify Attacker
- Poorly coded app
 - distributed to tens of thousands of devices



TRUST NO ONE

Threat Zones



iPhone App



```
ASCII Find f lash
Replace

Replace All Replace Replace & Find Previous Next

:173 682E7574 696C7305 616C6961 7310666C 6173685F etAliasName.f lash.utils.alias.f lash_
:03A 2F2F6164 6F62652E 636F6D2F 4153332F 32303036
:E65 76656E74 730D666C 6173682E 64697370 6C61790C
:174 6976651D 466C6173 68557469 6C536372 6970743A f lash.system.native.F lashUtilScript:
:765 74446566 696E6974 696F6E42 794E616D 6524466C :getAliasName.getDefinitionByName$Fl
:A67 65744465 66696E69 74696F6E 42794E61 6D650867 ashUtilScript::getDefinitionByName.g
:469 6C536372 6970743A 3A676574 54696D65 720F6573 etTimer.F lashUtilScript::getTimer.es
:66C 61736855 74696C53 63726970 743A3A65 73636170 capeMultiByte F lashUtilScript::escap
:363 6170654D 756C7469 42797465 22466C61 73685574 eMultiByte.unescapeMultiByte"F lashUt
:361 70654D75 6C746942 79746505 74726163 6516466C ilScript::unescapeMultiByte.trace.Fl
:A74 72616365 09666C61 73682E6E 65740A55 524C5265 ashUtilScript::trace.f lash.net.URLRe
:769 73746572 436C6173 73416C69 61732246 6C617368 quest.Class.registerClassAlias"F lash
:973 74657243 6C617373 416C6961 730F6765 74436C61 NetScript::registerClassAlias.getCla
:84E 65745363 72697074 3A3A6765 74436C61 73734279 ssByAlias.F lashNetScript::getClassBy
:A6F 55524C1D 466C6173 684E6574 53637269 70743A3A Alias.navigateToURL.F lashNetScript::
:365 6E64546F 55524C19 466C6173 684E6574 53637269 navigateToURL.sendToURL.F lashNetScri
:66C 6173682E 64656275 67676572 0D656E74 65724465 pt::sendToURL.f lash.debugger.enterDe
:275 67676572 53637269 70743A3A 656E7465 72446562 bugger"F lashDebuggerScript::enterDeb
:164 6F62652E 7574696C 73094D4D 45786563 7574651F ugger.Boolean.adobe.utils.MMExecute.
:363 72697074 3A3A4D4D 45786563 7574650C 4D4D456E MacromediaUtilScript::MMExecute.MMEn
:065 64696155 74696C53 63726970 743A3A4D 4D456E64 dCommand"MacromediaUtilScript::MMEnd
:E02 31300475 696E740E 666C6173 682E7072 6F66696C Command.Version.10.uint.f lash.profil
:368 50726F66 696C6572 53637269 70743A3A 70726F66 er.profile.F lashProfilerScript::prof
:50B 656E7669 726F6E6D 656E740A 6E6F6E65 1173686F ile.Inspectable.environment.none.sho
:646 6C617368 50726F66 696C6572 53637269 70743A3A wRedrawRegions&F lashProfilerScript::
:1F6E 7322666C 6173682E 6572726F 72733A49 6C6C6567 showRedrawRegions"f lash.errors:Illeg
:1F72 0C666C61 73682E65 72726F72 7315496C 6C656761 alOperationError.f lash.errors:Illega
:205 4572726F 7214666C 6173682E 6572726F 72733A49 lOperationError.Error.f lash.errors:IO
:866 6C617368 2E657272 6572733A 4D656D6F 72794F72 OError.IOException.f lash.errors:MemoryEx
s)
5 bytes selected at offset 9322956 out of 10067808 bytes
```

Charles Proxy



Your Friendly Neighborhood Application Spy Tool!

<http://www.charlesproxy.com/>

Charles CA Root Certificate:
<http://www.charlesproxy.com/ssl.zip>

Charles Proxy

A screenshot of the Charles Proxy 3.6.5 application window. The title bar reads "Charles 3.6.5 - Session 1 *". The interface is divided into several sections. On the left, a "Structure" pane shows a tree view of the proxy's virtual server hierarchy: "http://fizzer" (expanded) contains "v1/" (expanded) which contains "user/" (expanded) containing "index5.php" (with a warning icon). Below this are "http://safebrowsing.clients.google.com" and "http://safebrowsing-cache.google.com". The main area is titled "Response" and shows the following text:

```
HTTP/1.1 403 Forbidden
X-Powered-By: PHP/5.3.13
Content-type: text/html
Transfer-Encoding: chunked
Date: Tue, 22 May 2012 01:53:43 GMT
Server: Mashery Proxy

{"error":{"code":403,"message":"Not Authorized"}}
```

At the bottom of the response pane, there are tabs for "Headers", "Text", "Hex", "HTML", "JSON", "JSON Text", and "Raw", with "Raw" selected. The status bar at the bottom left shows "CONNECT https://na3.salesforce.com:443" and the bottom right shows "Map Local" and "Recording".

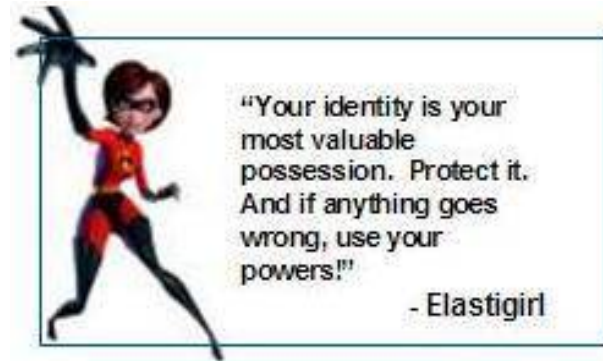
SSL



Digital Identity



"a set of claims made by one digital subject about itself or another digital subject"

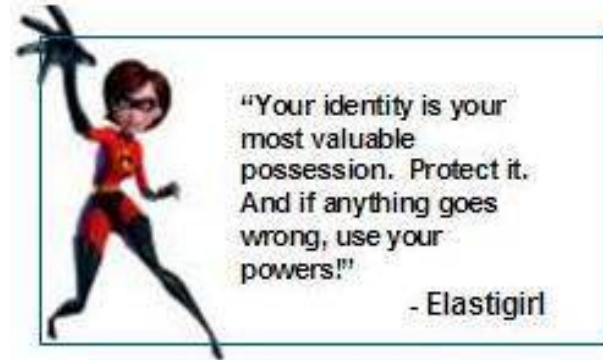


Application Identity



apikey=2745529bacf89590115d3657ac9d0442

Use Strong Keys



Authentication (AuthN)



"Authentication is the process of confirming a claimed identity."



Authentication (AuthN)



- Username/password
- TLS
- HMAC (Hash-based Message Authentication Code)
- WS-Security
- External to API



Authorization (AuthZ)



"Authorization is the act of granting permission for someone or something to conduct an act. Even when identity and authentication have indicated who someone is, authorization may be needed to establish what he or she is allowed to do."

Authorization (AuthZ)



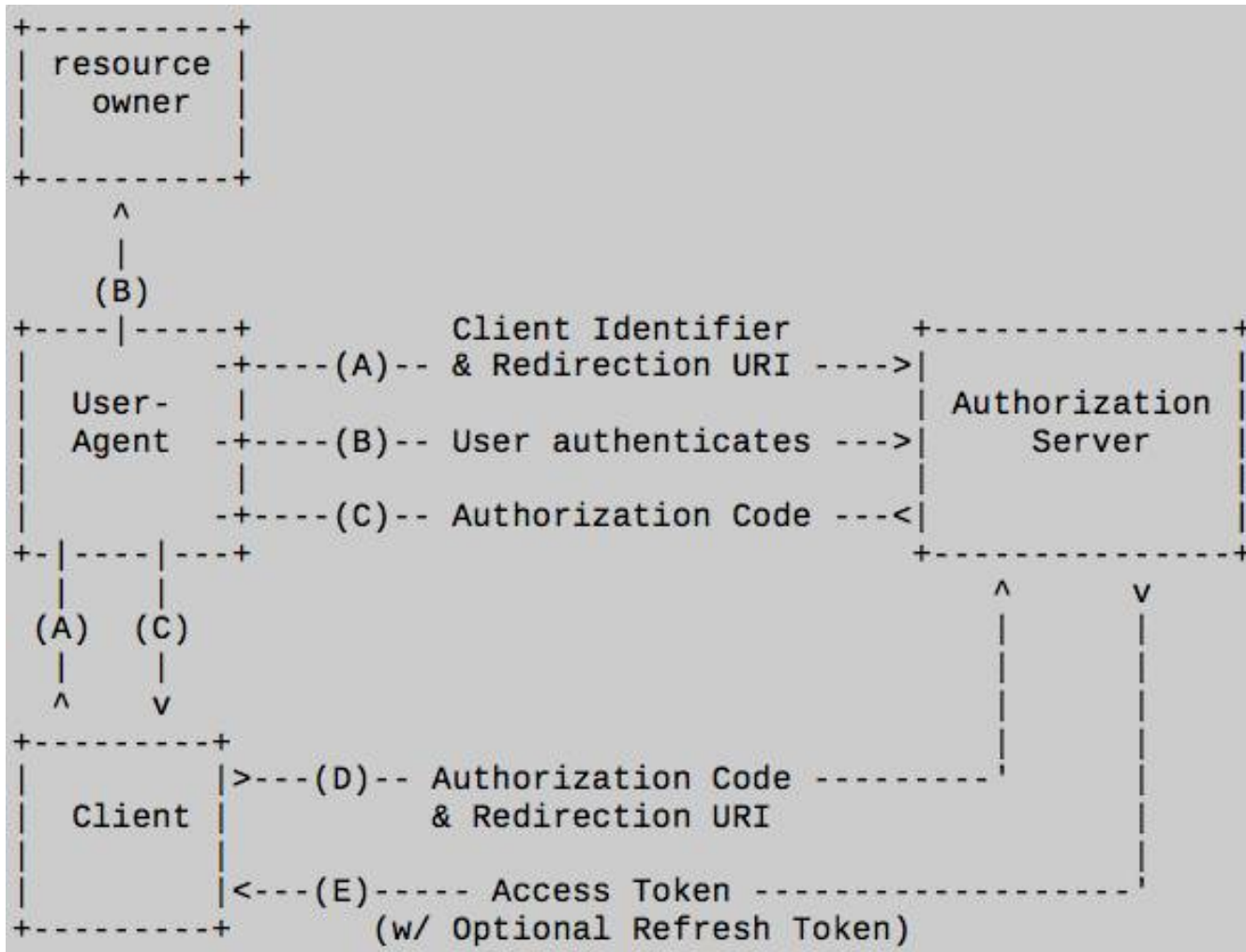
- OAuth
- Security Assertion Markup Language (SAML)

OAuth



Oauth

Authorization Code Flow



Oauth

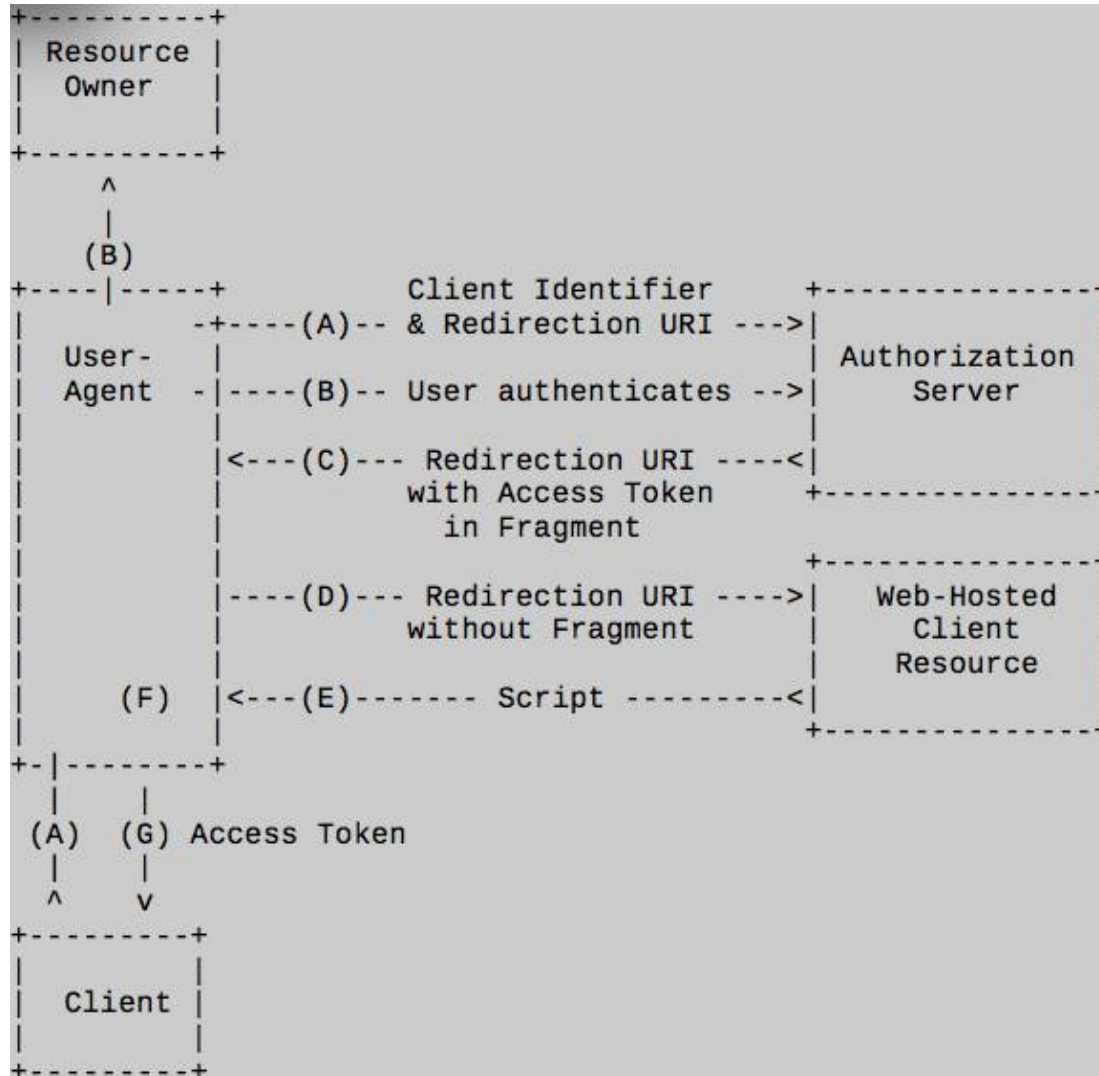
iPhone Custom Schemes



Key	Type	Value
Localization native development region	String	en
Bundle display name	String	\${PRODUCT_NAME}
Executable file	String	\${EXECUTABLE_NAME}
Icon file	String	
Bundle identifier	String	com.tutsplus.mobile.\${PRODUCT_NAME}
InfoDictionary version	String	6.0
Bundle name	String	\${PRODUCT_NAME}
Bundle OS Type code	String	APPL
Bundle versions string, short	String	1.0
Bundle creator OS Type code	String	????
▼ URL types	Array	(1 item)
▼ Item 0	Diction...	(2 items)
URL identifier	String	com.tutsplus.mobile.Receiver
▼ URL Schemes	Array	(1 item)
Item 0	String	readtext
Bundle version	String	1.0
Application requires iPhone environme	Boolean	YES
Main nib file base name	String	MainWindow
▶ Supported interface orientations	Array	(3 items)

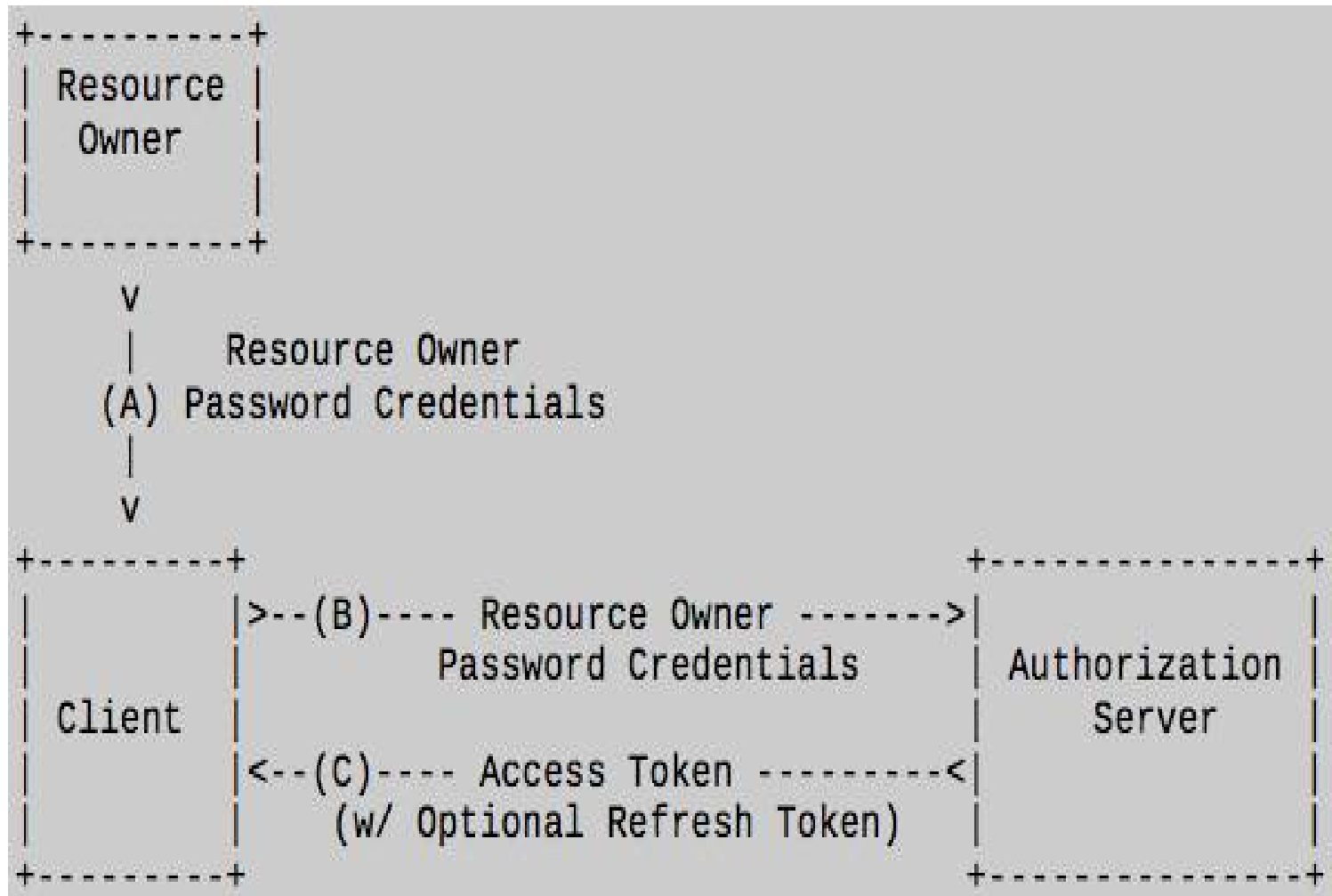
Oauth

Implicit Grant Flow



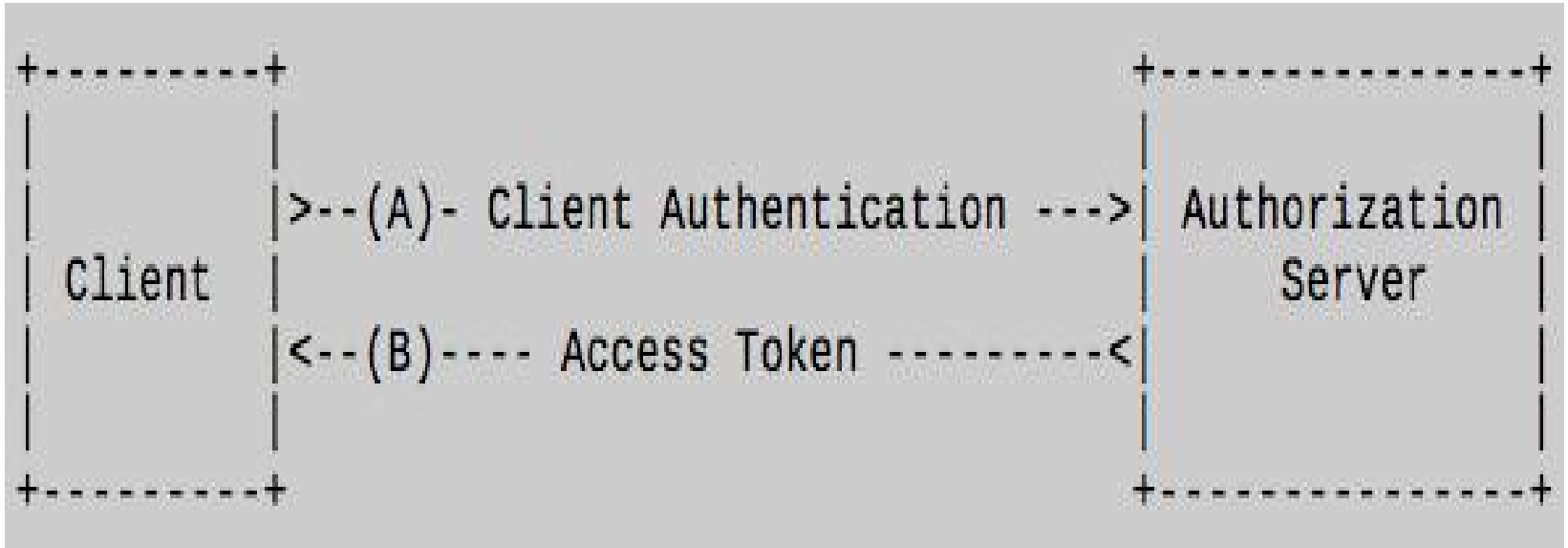
Oauth

Resource Owner Password Credentials Grant



Oauth

Client Credentials Grant



Oauth Extensions



<http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer-19>

<http://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-01>

<http://tools.ietf.org/html/draft-ietf-oauth-saml2-bearer-12>

Cryptography



- Digital Signatures
 - Authenticate
 - Message Integrity
 - Non-repudiation
- Data Encryption

XML Encryption



```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <EncryptedData
Type='http://www.w3.org/2001/04/xmlenc#Element'
  xmlns='http://www.w3.org/2001/04/xmlenc#'>
    <CipherData>
      <CipherValue>A23B45C56</CipherValue>
    </CipherData>
  </EncryptedData>
</PaymentInfo>
```

XML Digital Signature



```
<Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmlsig#">
<SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmlsig#rsa-sha1" />
  <Reference URI="">
    <Transforms>
      <Transform Algorithm="http://www.w3.org/2000/09/xmlsig#enveloped-signature" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlsig#sha1" />
    <DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK.../DigestValue>
  </Reference>
</SignedInfo>
  <SignatureValue>...</SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509Certificate>MIIB9zCCAWCgAwIBAgIERZwdkzANBgkqhk...</X509Certificate>
    </X509Data>
  </KeyInfo>
</Signature>
```

Crypto with JSON



Upcoming standards for using signatures and encryption with JSON data structures.

<http://self-issued.info/docs/draft-jones-json-web-signature-json-serialization-01.html>

<http://tools.ietf.org/html/draft-ietf-jose-json-web-signature-02>

<http://tools.ietf.org/html/draft-ietf-jose-json-web-encryption-02>

JSON Web Signature (JWS)



Payload

```
{  
  "iss": "joe",  
  "exp": 1300819380,  
  "http://example.com/is_root": true  
}
```

```
eyJpc3MiOiJqb2UiLA0KICJleHAiOiJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlIjM9PC19yb290Ij09cnVlQ
```

JSON header describing structure and algorithm to use:

```
{  
  "typ": "JWT",  
  "alg": "HS256"  
}
```

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9
```

JSON Web Signature (JWS)



JWS Secured Input:

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogIj0h0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290ljp0cnVlfQ
```

Base64 encoded HMAC SHA-256 JWS Secured Input:

```
dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk
```


JSON Web Signature (JWS)



JSON Web Signature JSON Serialization (JWS-JS):

```
{  
  "headers":  
  [ "eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9" ],  
  "payload":  
  "eyJpc3MiOiJqb2UiLA0KICJleHAiOiJlZMDA4MTkzODAsD  
  QogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnV  
  lfQ" ,  
  "signatures": [ "dBjftJeZ4CVP-  
  mB92K27uhbUJU1p1r_wW1gFWFOEjXk" ]  
}
```

JSON Web Encryption (JWE)



Payload: {"iss":"joe",
"exp":1300819380,
"http://example.com/is_root":true}

eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlMnVsS9pc19yb290Ijp0cnVlFQ

Header: {"alg":"RSA1_5",
"enc":"A256GCM",
"iv":"__79_Pv6-fj39vX0",
"x5t" : "7noOPq-hJ1_hCnvWh6IeYI2w9Q0" }

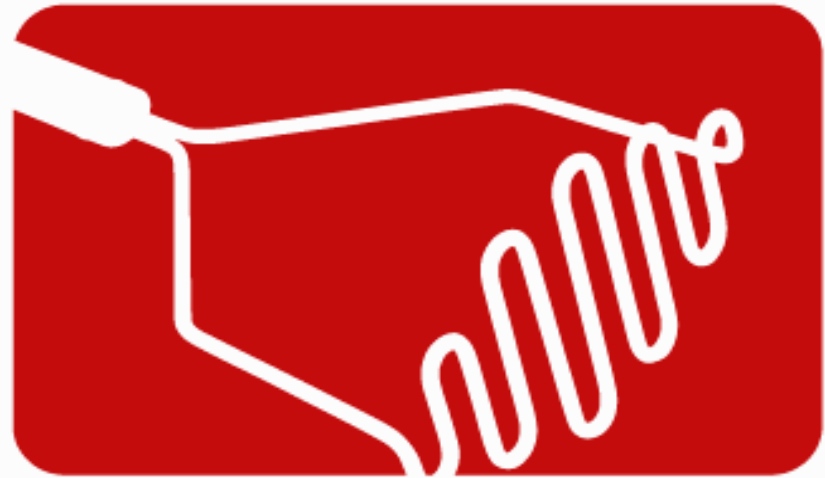
eyJhbGciOiJSU0ExXzU1LA0KICJlbmMiOiJBMjU2R0NNIiwNCiAiaXYiOiJfXzU1LA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlMnVsS9pc19yb290Ijp0cnVlFQ

JSON Web Encryption (JWE)



```
{
  "headers":
  [ "eyJhbGciOiJSU0ExXzUiLA0KICJlbnMiOiJBMjU2R0NNIiwNCiAiaXYiOiJfXzc5X1B2Ni1mZyIsDQogIng1dCI6Ijdub09QcS1oSjFfaENudldoNkllWUkydzlRMCMJ9" ],
  "encrypted_keys": [
    "TBD_key_1_value_TBD",
    "TBD_key_2_value_TBD" ],
  "ciphertext": "TBD_ciphertext_value_TBD"
}
```

Questions?



MASHERY

We're Hiring!

