



JavaOne™

java.sun.com/javaone

Building Secure Mashups With OpenAjax

Jon Ferraiolo
IBM and OpenAjax Alliance

TS-5030

OpenAjax
alliance



You will learn:

- Mashups - the promise and challenges
- OpenAjax Alliance mashup initiatives

You will see:

- OpenAjax Mashups in action

GOAL

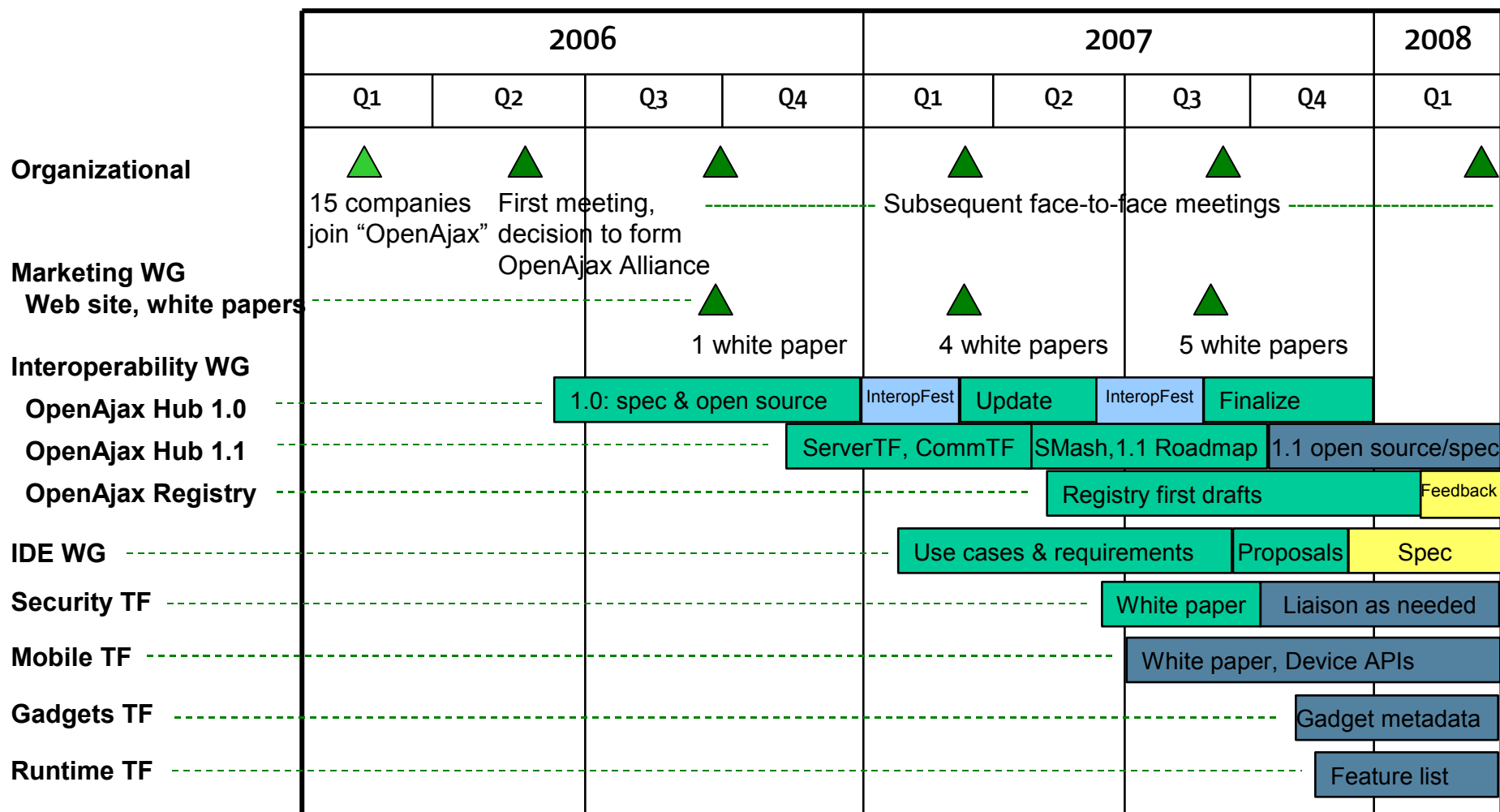
Agenda

- Introducing OpenAjax Alliance
- Secure Mashup Initiatives Overview
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

Why did the industry form OpenAjax Alliance?

- Interoperability problems across Ajax toolkits
 - Sometimes toolkits step on each other
 - Almost never do toolkits integrate with each other
 - Interoperability/integration is necessary for mashups to work
- Education
 - For IT managers and Web developers, Ajax can be complex and confusing – tyranny of choice
- Help drive the future of the Ajax ecosystem

OpenAjax Alliance – Today



OpenAjax Hub 1.0

➤ What is it?

- Small bit of standard JavaScript™ technology (< 3K after compaction)
- Enables multiple Ajax runtimes to work together

➤ Version 1.0 features

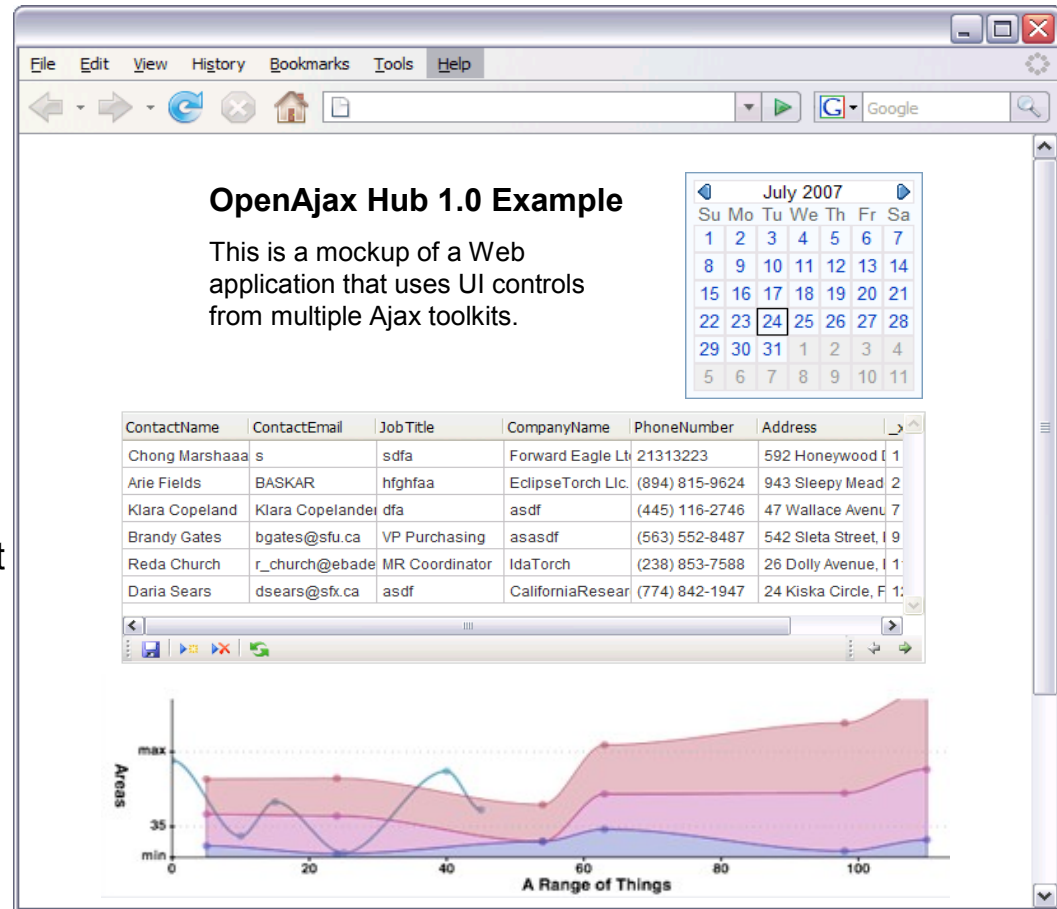
- Ajax library registration
 - `OpenAjax.hub.registerLibrary()`
- Simple publish/subscribe engine (the pub sub hub)
 - `OpenAjax.hub.publish(topicName, payload)`
 - `OpenAjax.hub.subscribe(topicName, callbackFunction)`

OpenAjax Hub 1.0 – an example

Assume multiple Ajax toolkits:

- UTILS.js – Various utils, inc. XHR
- CALENDAR.js – Calendar control
- DATAGRID.js – Powerful tables
- CHARTS.js – Charting utilities

The visual controls need to react to new server data and to each other and update their views appropriately



Example – under the hood

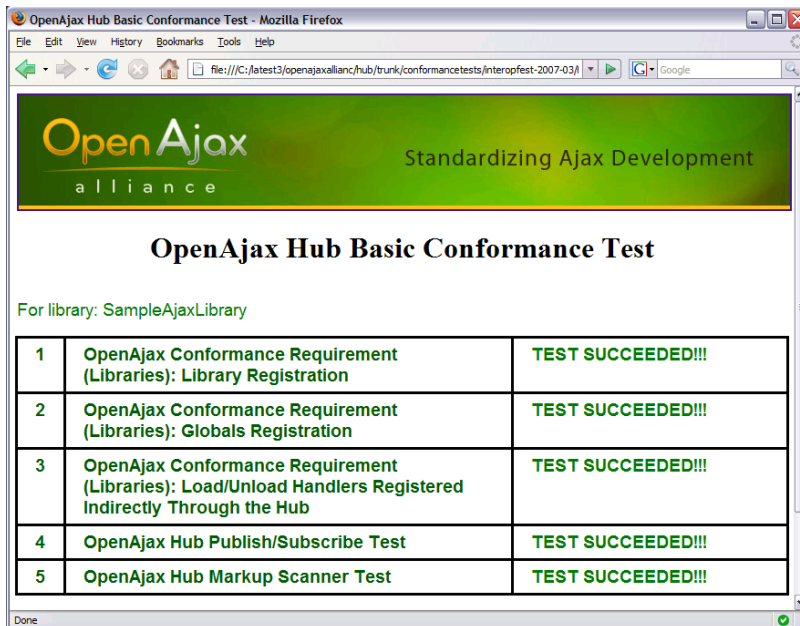
```
<html>
  <head>
    <script src="OpenAjax.js"/>
    <script src="UTILS.js"/>
    <script src="CALENDAR.js"/>
    <script src="CHARTS.js"/>
    <script src="DATAGRID.js"/>
    <script>
function MyCalendarCallback(...) {
  OpenAjax.hub.publish("myapp.newdate", newdate);
}
function NewDateCB(eventname, pubData, subData) {...}
OpenAjax.hub.subscribe("myapp.newdate", NewDateCB);
    </script>
  </head>
```


OpenAjax InteropFests

➤ Objectives:

- Verify that OpenAjax Hub is reliable, performant, and suitable
- Allows members to check if they are OpenAjax Conformant

Jan-March 2007



OpenAjax Hub Basic Conformance Test - Mozilla Firefox

file:///C:/latest3/openajaxalliance/hub/trunk/conformancetests/interopfest-2007-03/

OpenAjax alliance Standardizing Ajax Development

OpenAjax Hub Basic Conformance Test

For library: SampleAjaxLibrary

1	OpenAjax Conformance Requirement (Libraries): Library Registration	TEST SUCCEEDED!!!
2	OpenAjax Conformance Requirement (Libraries): Globals Registration	TEST SUCCEEDED!!!
3	OpenAjax Conformance Requirement (Libraries): Load/Unload Handlers Registered Indirectly Through the Hub	TEST SUCCEEDED!!!
4	OpenAjax Hub Publish/Subscribe Test	TEST SUCCEEDED!!!
5	OpenAjax Hub Markup Scanner Test	TEST SUCCEEDED!!!

Done

12 toolkits participated

http://www.openajax.org/member/wiki/InteropFest_2007_March



July-Sept 2007



InteropFest 1.0 Example Web Page - Mozilla Firefox

file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/private/InteropFest%20Index.html

OpenAjax alliance Standardizing Ajax Development

OpenAjax Alliance InteropFest 1.0 Template

About this template

This page is a template for InteropFest 1.0 that culminates at the OpenAjax Alliance face-to-face meeting on Sept 27, 2007. To participate in the InteropFest, you need to customize this template per the instructions that begin with the Readme.txt file that accompanies this template.

The only part of this template that must be preserved after your customization is the results table that you see in the lower-left corner. It is OK to re-use the results table and/or put it in a different location.

Your customizations can also remove/replace the OpenAjax banner at the top of the page, but you must preserve the smaller-size banner that sits on top of the test results.

No matter how you customize, remove or replace this section.

Data generation component

(NOTE: This template uses a client-side JavaScript component to generate random stock value change events. As the Readme.txt file explains, there are many options for customizing this template. Among the options: (1) you can use this datagen component, (2) you can replace the datagen component, or (3) you can customize in more radical ways. Whatever you decide, as part of your customization effort, remove this paragraph.)

Click the button below to pause or resume the continuous feeds of simulated stock market price changes.

Pause

Data visualization component

(NOTE: This template uses a client-side JavaScript component to use an HTML table to present the stock value change events. As the Readme.txt file explains, there are many options for customizing this template. Among the options: (1) you can use this simple datavis component, (2) you can replace the datavis component, or (3) you can customize in more radical ways. Whatever you decide, as part of your customization effort, remove this paragraph.)

OpenAjax InteropFest 1.0 Test Results

Library registration test	TEST SUCCESSFUL
Pubsub test	TEST SUCCESSFUL
# Registered libraries	3
# Messages published	1518
# Messages received	1518
# Unique topics received	3

East Bay Electric	EBEL	93 12
Hall Systems	HSLS	89 12
Larsen Circuits	LATR	87 14
Yeastian Executive Search	YOOP	114 14
Strawberry Computers	STRA	67 12
Titan Power	TITA	90 14
Chisoff Systems	CSLS	104 12
Open Ajax	OPAJ	94 12

14 organizations, 20 toolkits participated

http://www.openajax.org/member/wiki/InteropFest_1.0

InteropFest Participants

Participating organizations	Participating toolkits
24SevenOffice Apache XAP Dojo Foundation IBM ILOG DWR/Getahead IT Mill Lightstreamer Microsoft Nexaweb OpenLink SW Open Spot Software AG Sun Microsystems TIBCO	AjaxEngine Apache XAP Dojo Toolkit Ext ILOG JViews IT Mill Toolkit jMaki jQuery Lightstreamer Microsoft Ajax Library Nexaweb Ajax Client OAT: OpenLink AJAX Toolkit OpenSpot CalcDesk Prototype script.aculo.us Software AG's webMethods/CAF TIBCO General Interface 24SevenOffice Vili YUI

OpenAjax Hub 1.0 status

> Status

- *Approved*

> Specification

- http://www.openajax.org/member/wiki/OpenAjax_Hub_1.0_Specification

> Reference implementation at SourceForge

- <http://openajaxallianc.sourceforge.net>

Agenda

- Introducing OpenAjax Alliance
- Secure Mashups Overview
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

Mashups – the self-service business pattern



Opportunity

assemble mash-up

start design from data

data

find, transform into remixable content

catalog, share widgets feeds in atom and RSS

business mash-up ecosystem

- 

Mashup software



• Mashup tools

- Widget and feed discovery
- Application assembly
- Instant deployment

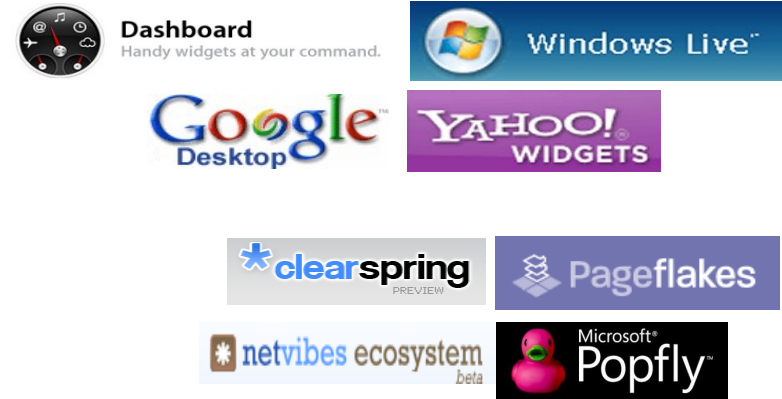
• Widgets

- Pre-packaged, remixable mini-applications
- Usually tied to a back-end web service
 - Sometimes leveraging previous investment in SOA
- Public or company-private
- Key enabler of the long tail

Widget innovation – no shortage



Industry challenges



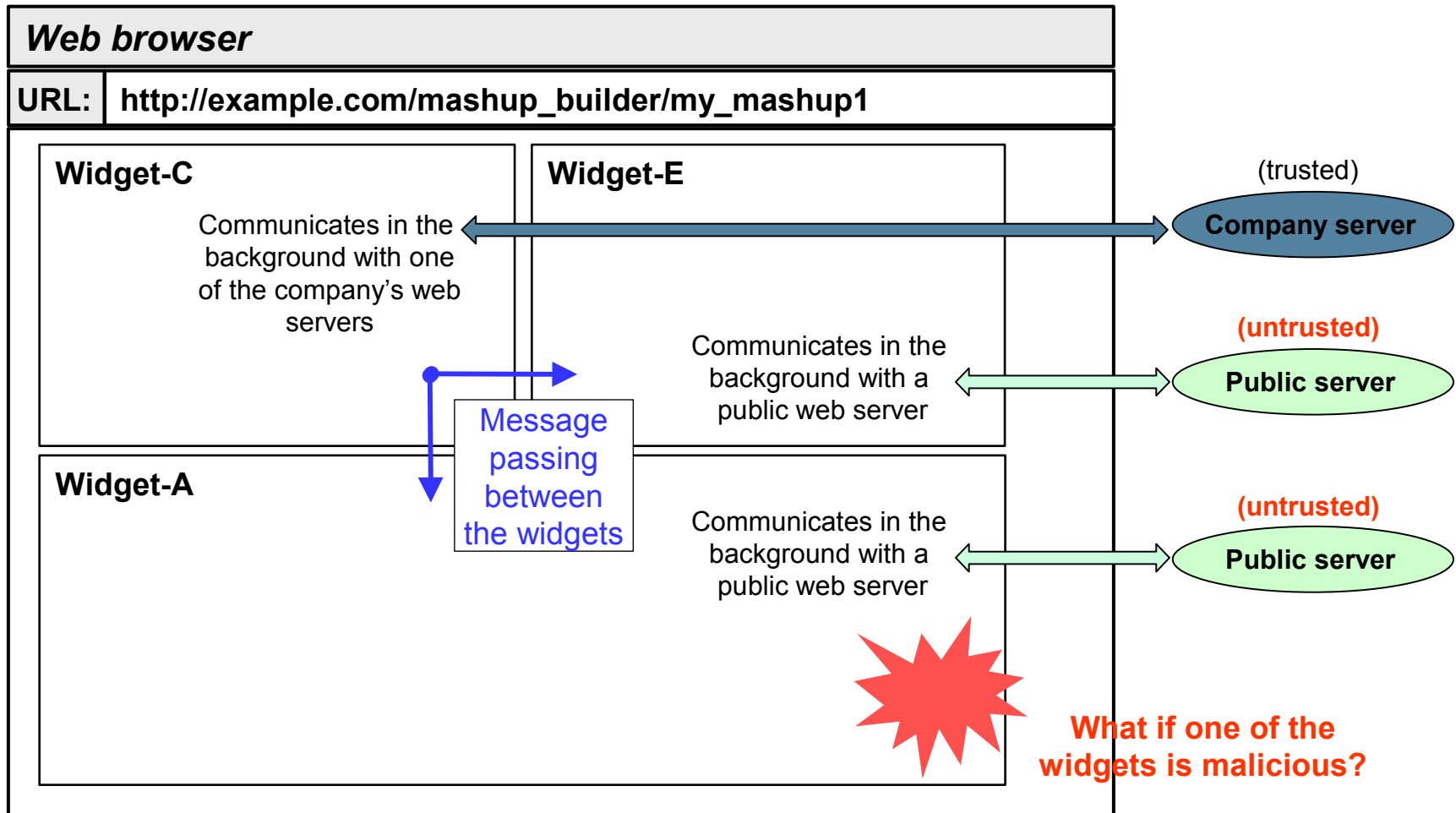
➤ Interoperability

- Dozens of proprietary technologies
- *Good news: many use the “Web Runtime” (i.e., Ajax)!*
- Bad news: even when using the Web Runtime, widgets are not interoperable

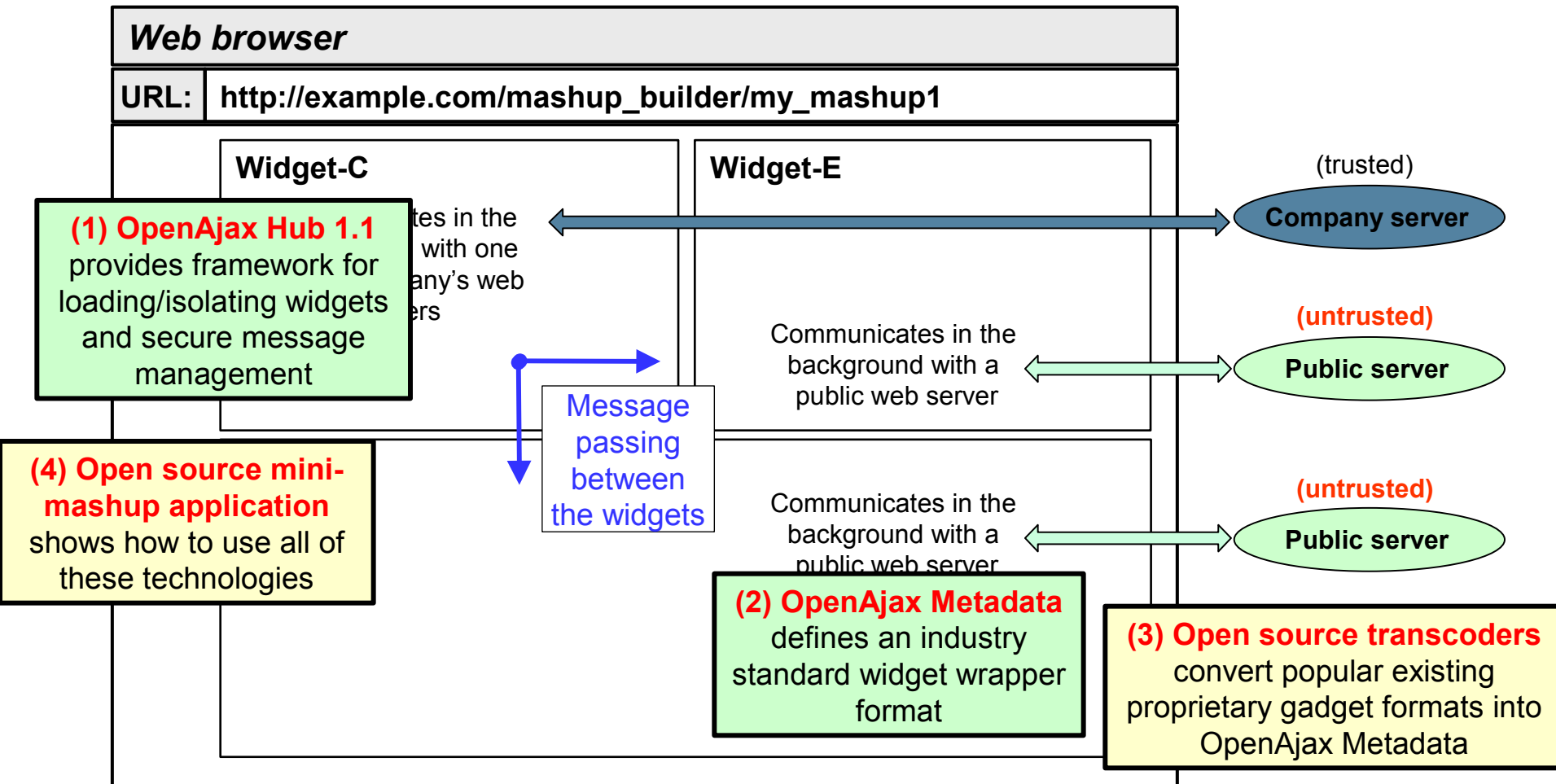
➤ Security

- The power of mashups – comes largely from discovering and integrating great widgets from 3rd parties
- But 3rd party widgets might be malicious

Security vulnerabilities



OpenAjax – Addressing the challenges



Agenda

- Introducing OpenAjax Alliance
- Secure Mashup Initiatives Overview
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

OpenAjax Hub 1.1 – New features

- OpenAjax Hub 1.0 addresses pub/sub within a single browser frame

- OpenAjax Hub 1.1 adds the following:
 - Pub/sub across frames
 - Framework for secure mashups
 - Pub/sub between clients and servers (i.e., Comet)

Mashups: security issues

- Browser same-origin policy prevents interaction across origins
- Typical Solution: bypass same-origin policy by
 - Dynamic SCRIPT tag to another server (client-side)
 - Proxying content (server-side mashups)
 - “IFrame proxy” (window.location fragment identifier)

SMash

- SMash stands for “Secure Mashups”
 - Secure handling of 3rd party mashup components
 - Runs in today’s browsers (without plugins)
- Designed and implemented at IBM™ Research (beginning of 2007)
 - Open-sourced (openajaxallianc.sourceforge.net) in August 2007
 - Research Paper describing SMash in WWW 2008 Conference
- High-level APIs, independent of implementation technology
 - Fragment communication, HTML5 postMessage, Java™ platform, Flash etc.
 - Will still work when browsers add native support for secure cross-frame messaging

OpenAjax Hub 1.1: Concepts

➤ Managed hub-instances

- A frame/window can have multiple managed hub-instances
- Hub-instance has one manager, multiple clients

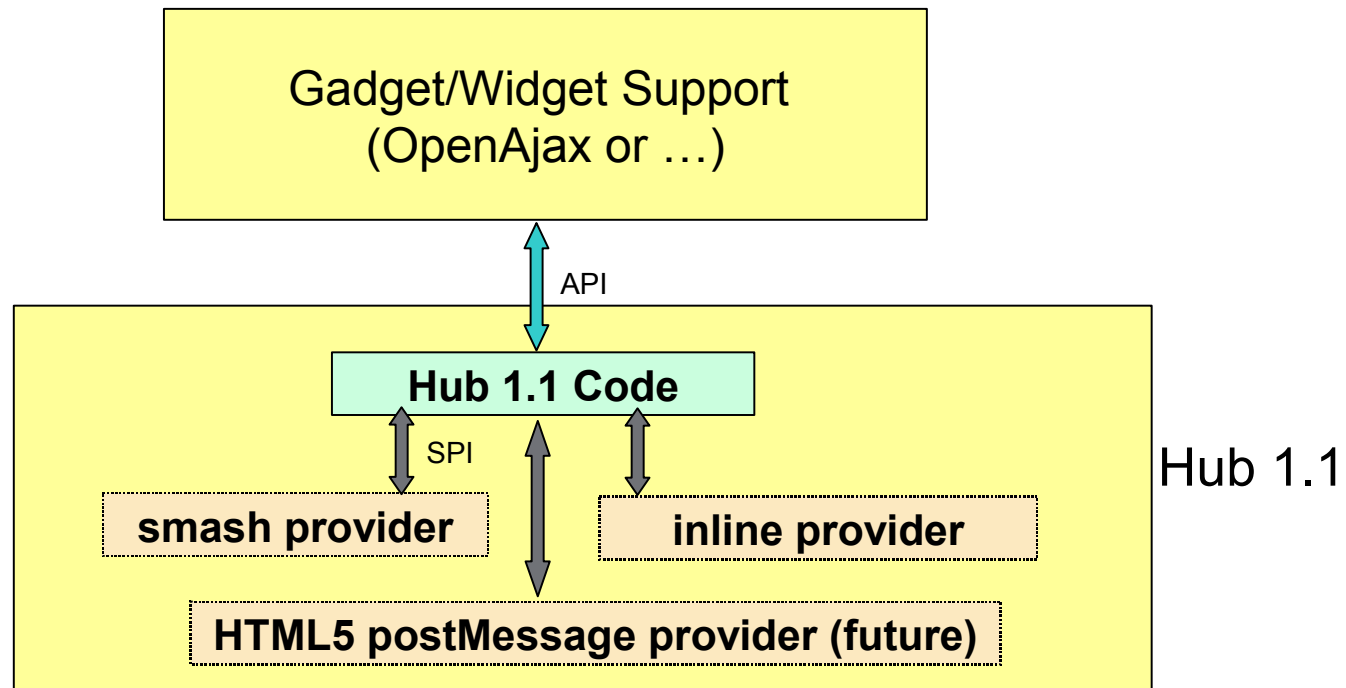
➤ Fine-grained policy hooks for manager

- For security policy, mediation between incompatible clients etc.
- No policy encoded in hub

➤ Providers: Multiple communication providers for client to hub-instance communication

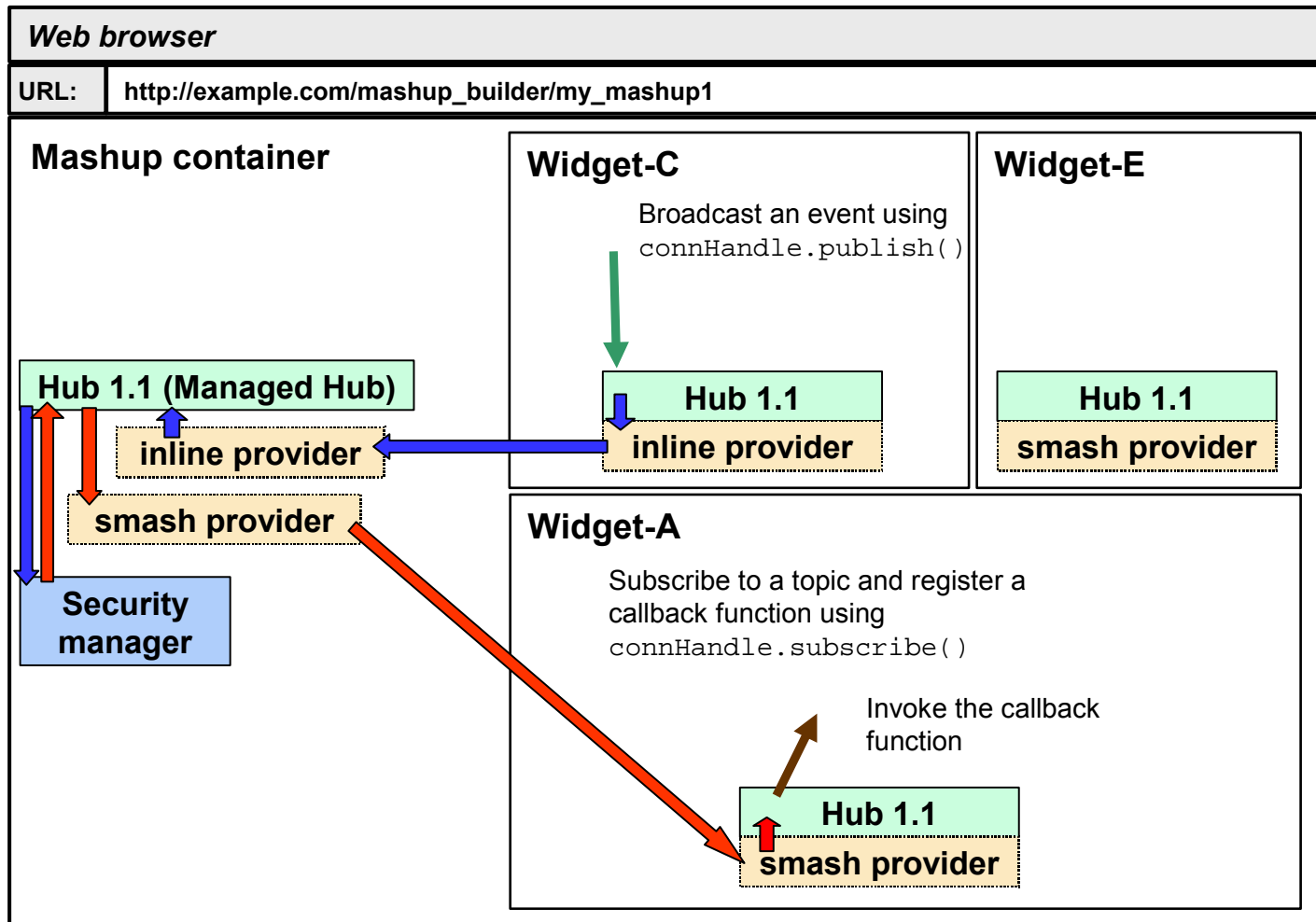
- Provider and Hub SPI
- Current providers: inline, smash (using code from SMash)

OpenAjax Hub 1.1: Architecture

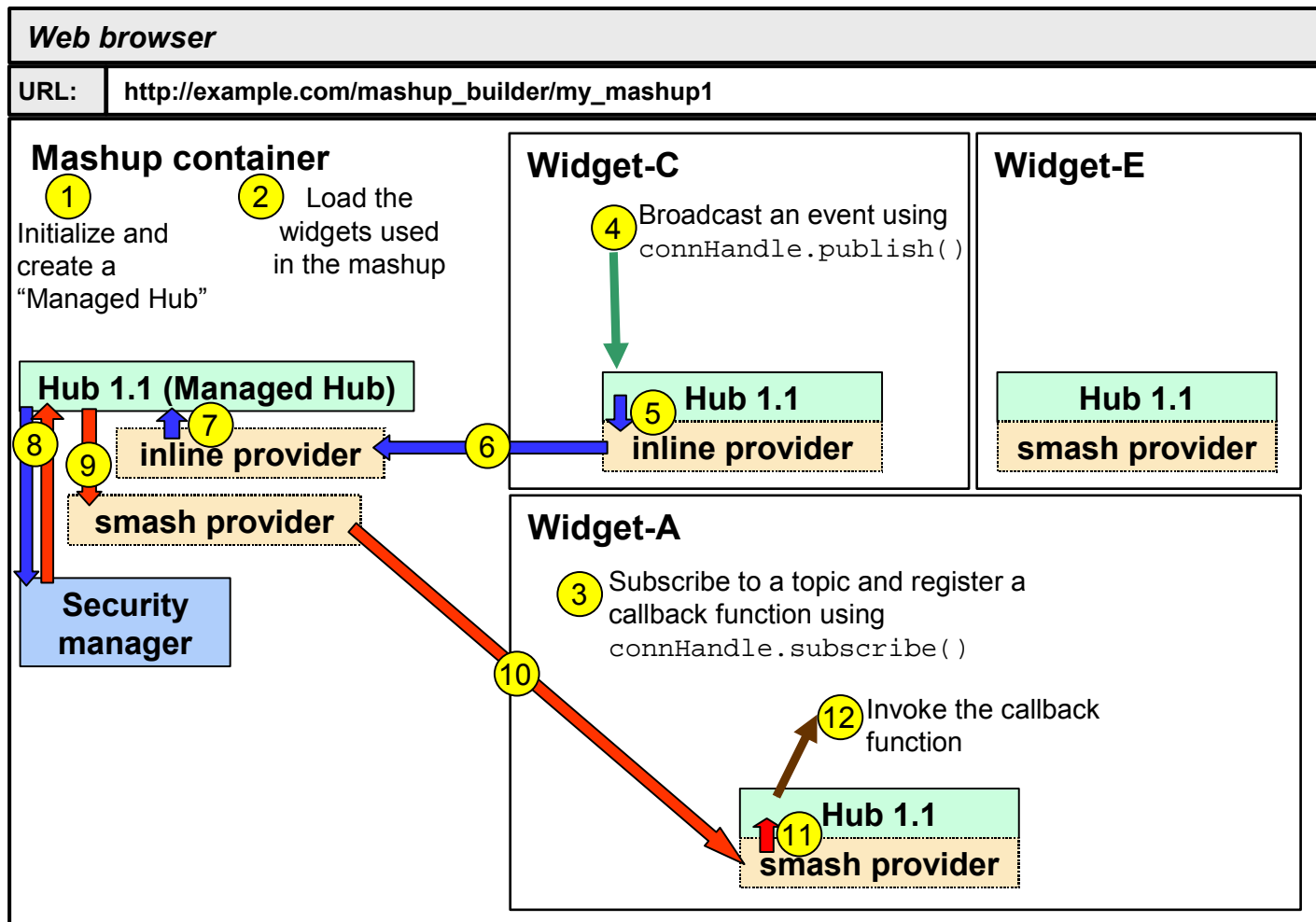


- Gadget/Widget layer sits on top of OpenAjax Hub 1.1
- Hub supports composite gadgets with
 - any level of nesting
 - any combination of gadget types (inline, iframe, ...) e.g. inline gadget-foo composed of iframe gadget-bar and inline gadget-baz

OpenAjax Hub 1.1: Simple example



OpenAjax Hub 1.1: the steps



Hub 1.1 status

➤ Specification

- First draft spec – far along
- http://www.openajax.org/member/wiki/OpenAjax_Hub_1.1_Specification

➤ Reference implementation at SourceForge

- First implementation (far along)
- <http://openajaxallianc.sourceforge.net>

➤ Timeline for Hub 1.1

- **Now:** Detailed review within Interoperability Working Group
- **Spring 2008:** Stable, complete spec
- **July-September 2008:** InteropFest (with OpenAjax Metadata)
- **Fall 2008:** Finalize and approve

Agenda

- Introducing OpenAjax Alliance
- Secure Mashup Initiatives Overview
- OpenAjax Hub 1.1
- OpenAjax Metadata for Widgets
- Demo
- Summary

Widget innovation – no shortage



OpenAjax Metadata – industry problems

➤ IDE interoperability problem

- Countless Ajax libraries
- Each library has its own approach to documenting
 - JavaScript APIs
 - UI controls
- *As a result, difficult to deliver visual authoring tools that integrate with the full set of Ajax libraries in the industry*

➤ Mashup interoperability problem

- Dozens of widget formats (Google, Yahoo, Apple, Microsoft...)
- Current industry situation:
 - Widgets developers provide multiple versions of their widgets
 - To do a mashup, you usually need a programmer
- *As a result, difficult to deliver visual mashup tools that integrate with the full set of widgets in the industry*

OpenAjax Metadata – what it provides

➤ (IDE WG) Ajax library metadata “intermediary” standard

- Standard XML for describing
 - JavaScript APIs
 - Widgets
- Committee includes
 - Adobe, Aptana, Dojo, Eclipse, IBM, Microsoft, Sun, TIBCO, and Zend

➤ (Gadgets TF) Mashup gadgets “intermediary” standard

- Standard XML for describing a mashup component
- But mashup gadgets have special needs
 - List of topics that they produce and consume (i.e., pub/sub)
 - Security issues related to secure mashups

OpenAjax Metadata sample code

```
<widget xmlns="http://ns.openajax.org/widgets">

  <properties>
    <property name="Addr" type="Loc" listen="true" />
  </properties>

  <content>
    <!-- HTML+JavaScript go here -->
  </content>

</widget>
```

OpenAjax Metadata status

> Specification

- First draft spec - far along
- http://www.openajax.org/member/wiki/OpenAjax_Metadata_Specification

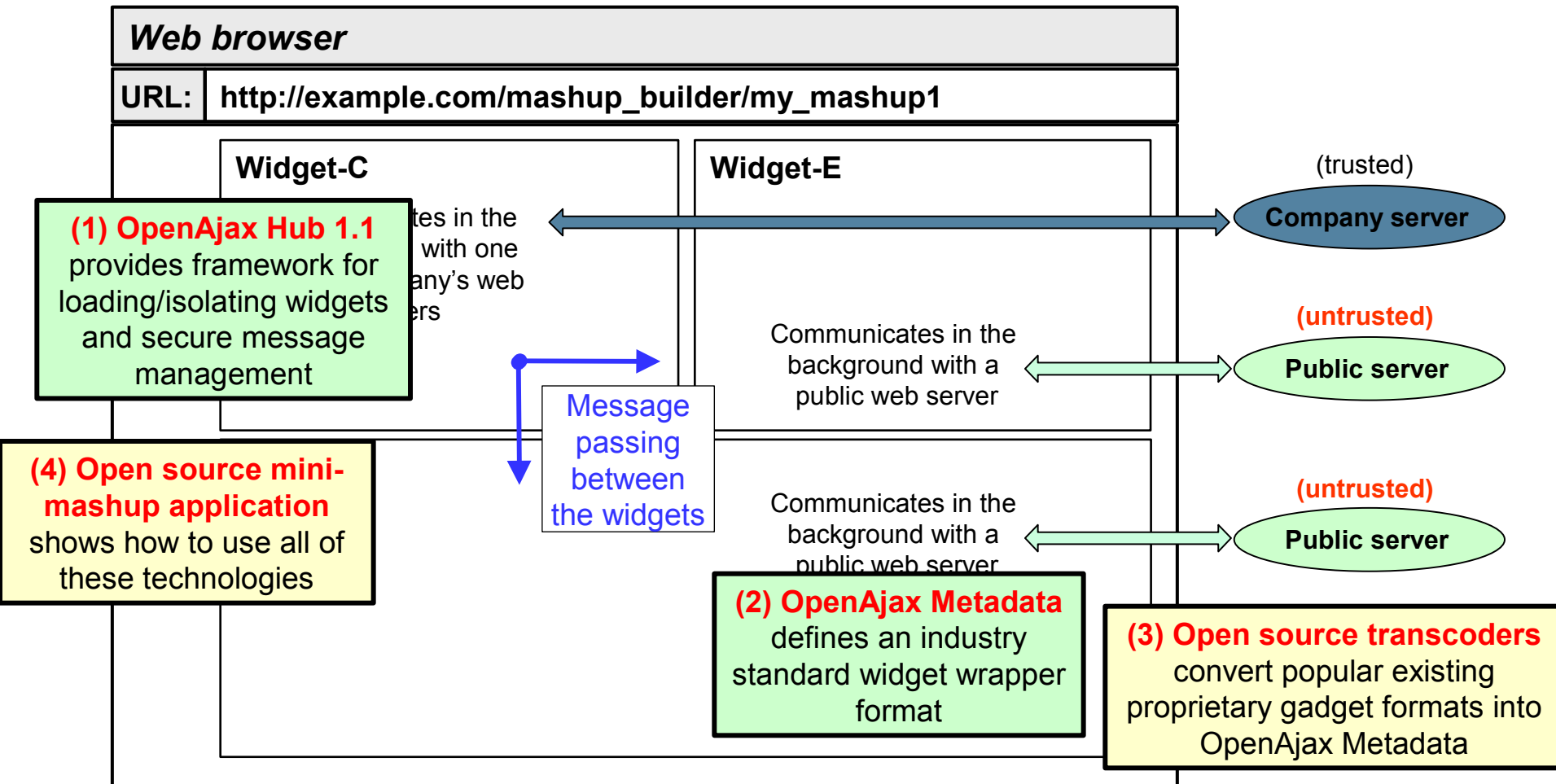
> Open source

- Gadget transcoders
- Mini mashup application

> Timeline for OpenAjax Metadata

- **Now:** Finishing spec within IDE Working Group
- **Spring 2008:** Stable, complete spec
- **July-September 2008:** InteropFest (with OpenAjax Hub 1.1)
- **Fall 2008:** Finalize and approve

OpenAjax – Addressing the challenges



OpenAjax Mashups in action

A large, light blue arrow pointing to the right, positioned behind the word "DEMO".

DEMO

Summary

- Mashups offer both promise, but have challenges
 - Security
 - Interoperability
- OpenAjax Alliance is addressing the challenges
 - OpenAjax Hub 1.1
 - OpenAjax Metadata

For More Information

- **Web site:** <http://www.openajax.org>
- **Wiki:** <http://www.openajax.org/member/wiki>
- **Blog:** <http://www.openajax.org/blog>
- **Mail list:** public@openajax.org
- **Email:** Jon Ferraiolo <jferrai@us.ibm.com>

THANK YOU



Jon Ferraiolo, IBM & OpenAjax Alliance

TS-5030

