

ORACLE



SECURING THE NEW DIGITAL EXPERIENCE

Dr Steffo Weber, Oracle

May, 2014

~~Bridg~~Filling the UX gap for
mobile enterprise
applications.

Latest Entries

Protecting IDPs from malformed SAML requests

[Read more](#)

Write secure code, don't write security code.

[Read more](#)

Fine-grained authorization and XACML.

[Read more](#)

Tuning the industry's most trusted directory server.

[Read more](#)

Hands-On SOA and Web Security.

[Read more](#)

Harnessing Sun's OpenSSO Authentication and Authorization.

[Read more](#)

Overview

Motivation

- ▶ What for?
- ▶ UI vs UX vs Security
- ▶ Channels

Foundation

- ▶ WebSSO limits
- ▶ OAuth
- ▶ XCode

Experience

- ▶ How long?
- ▶ How complicated?
- ▶ Alternatives

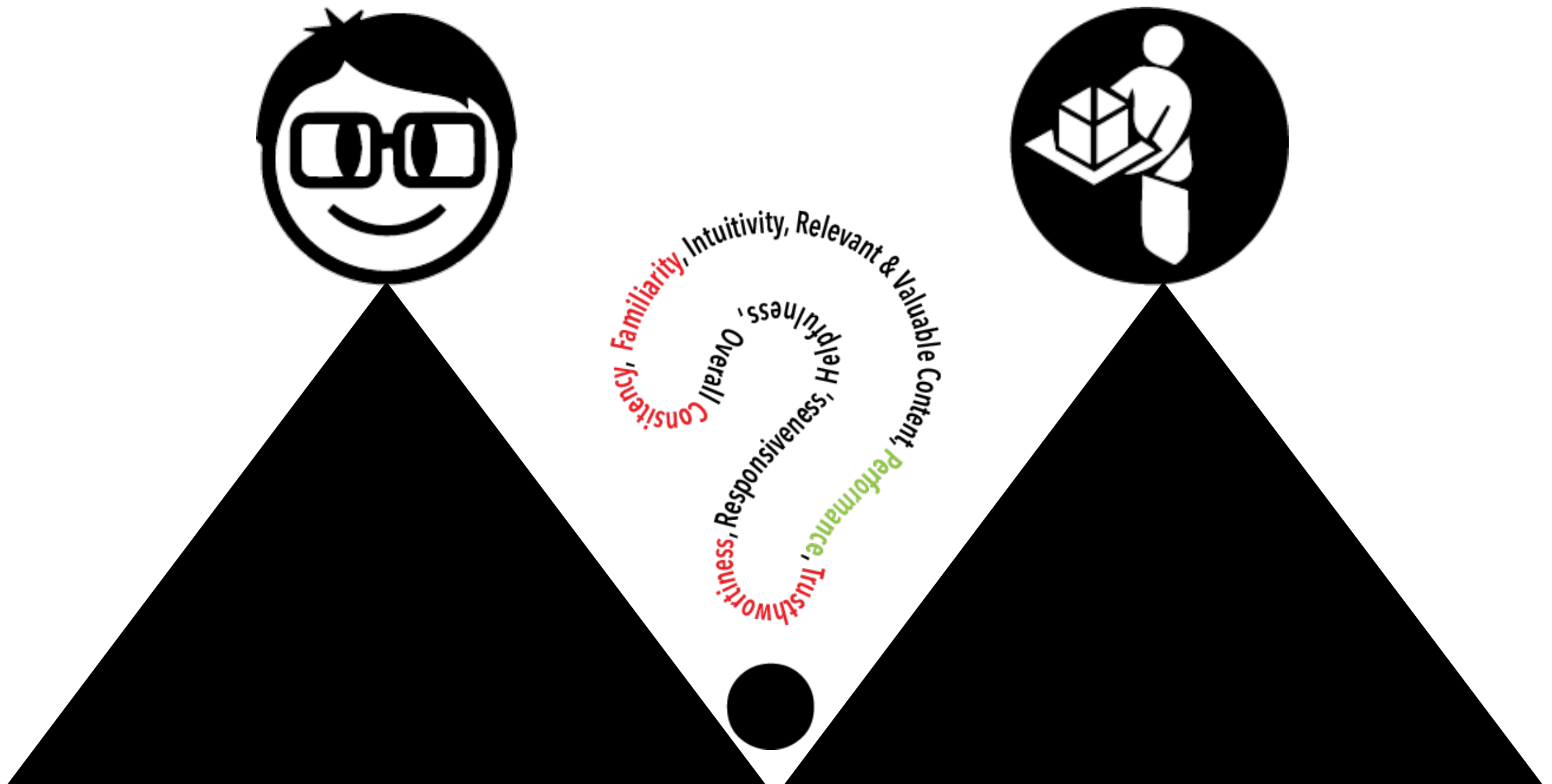


Motivation

Importance of mobile access
management

The UX gap varies

depending on your objectives



Motivation

Evolution of UX

Pro

Information &
Data Design

Prosumer

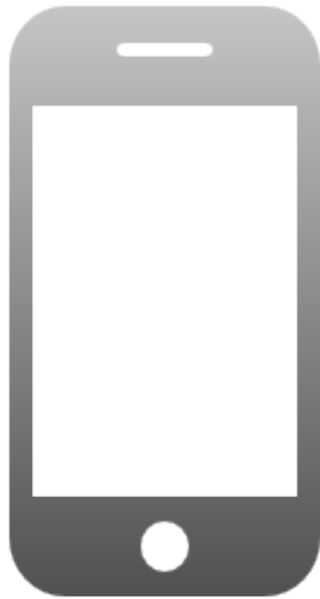
Graphical UI

Consumer

User Experienced
Design

Motivation

Why UX is **not** UI



- ▶ Touchscreen with GUI
- ▶ Application (MVC)
- ▶ Background Services (REST)

Motivation

Some findings (hypothesis first)

13.6 million tablets shipped to enterprises (2011)

96.3 million tablets shipped to enterprises (2016)

Motivation

Some findings (hypothesis first)

85% prefer mobile apps over mobile websites

79% will not retry an app if the failed once or twice

48% will delete an app if it is too slow

Consumer

Don't make me think.

Consumer

Now what the relationship to identity? Why can't I use Facebook/Twitter login?

Buying process

and corresponding identity.

1. Problem/Need Recognition
2. Information Search
3. Evaluation of Alternatives
4. Purchase Decision
5. Post-purchase Behaviour

?



Social ID



Social ID
Web Trail



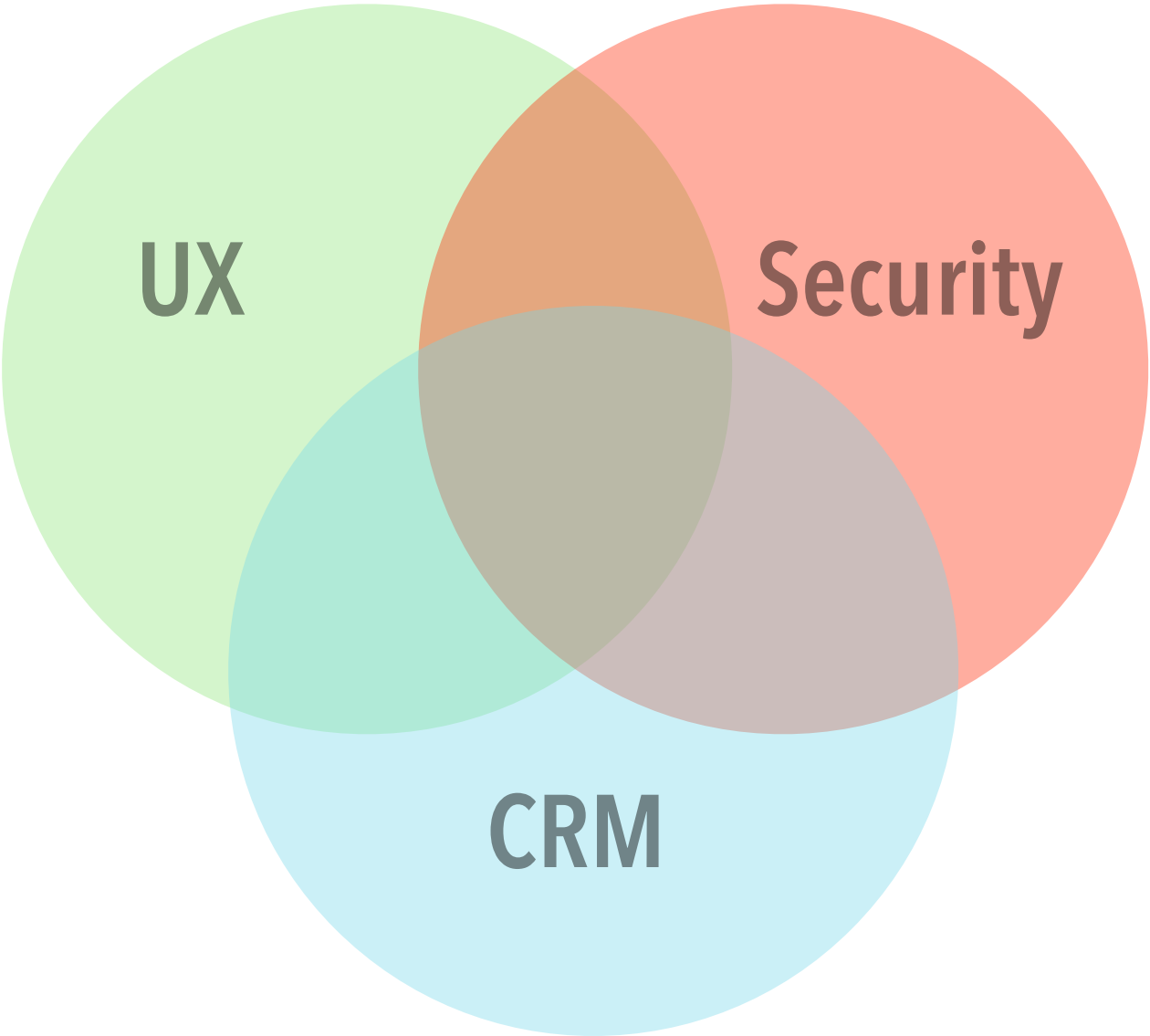
Social ID
Web Trail
Address
Billing Rel



Social ID
Web Trail
Address
Billing Rel
Customer ID

This is where real identity comes into play.

Customer Loyalty



Customer Loyalty

Advice: all channels are equal.

mobile **sites**,
mobile **apps**,
traditional channels.

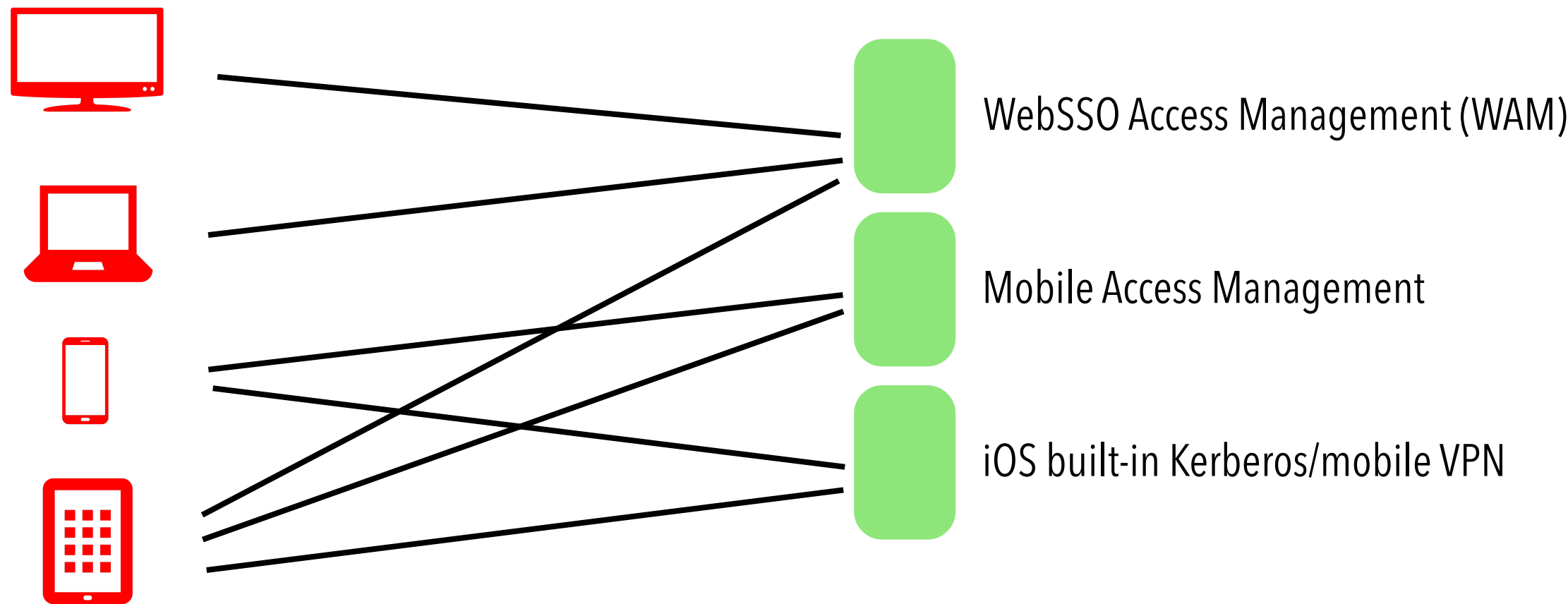
Cookies, web SSO

Multiple apps...

Cookies, web SSO

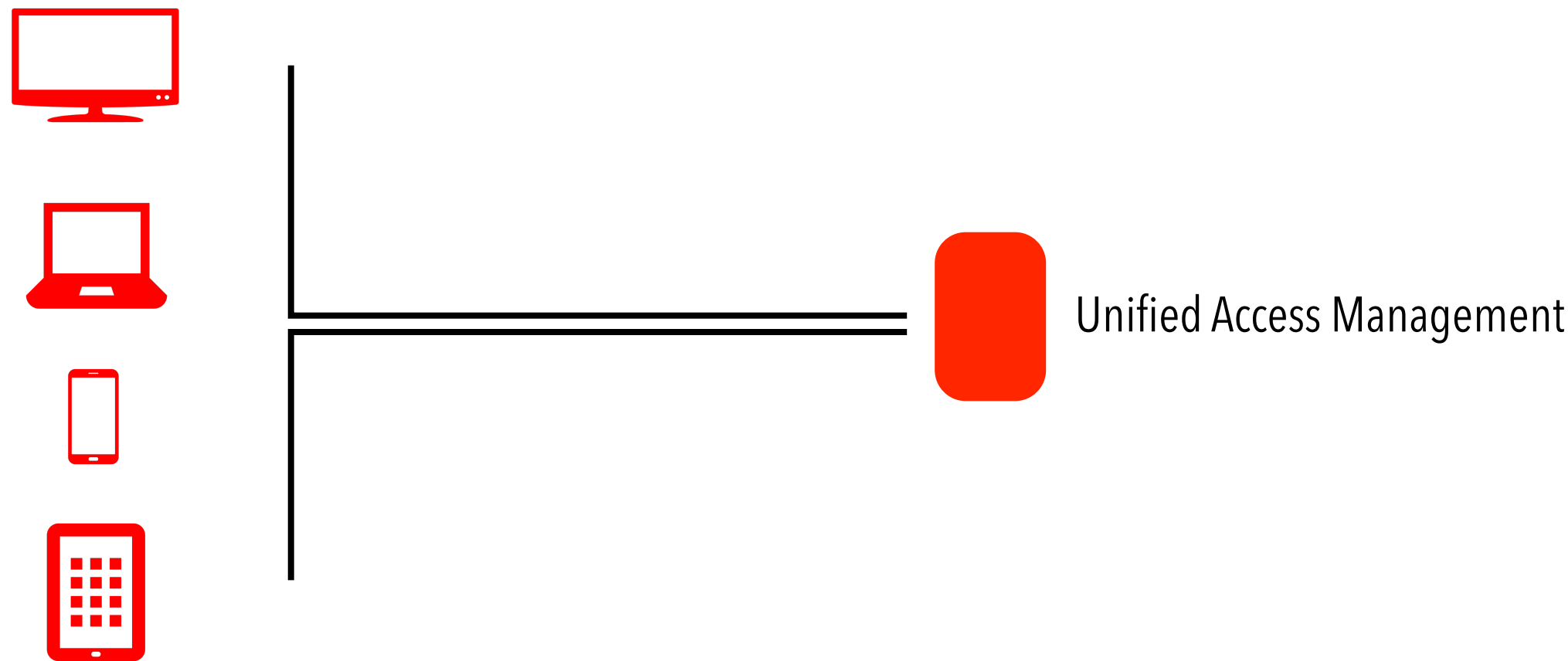
Customer Loyalty

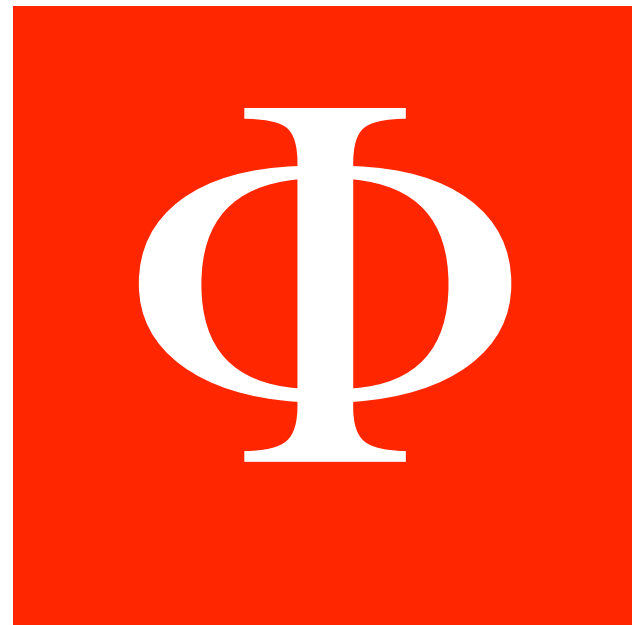
Advice: all channels are equal.



Customer Loyalty

Advice: all channels are equal.

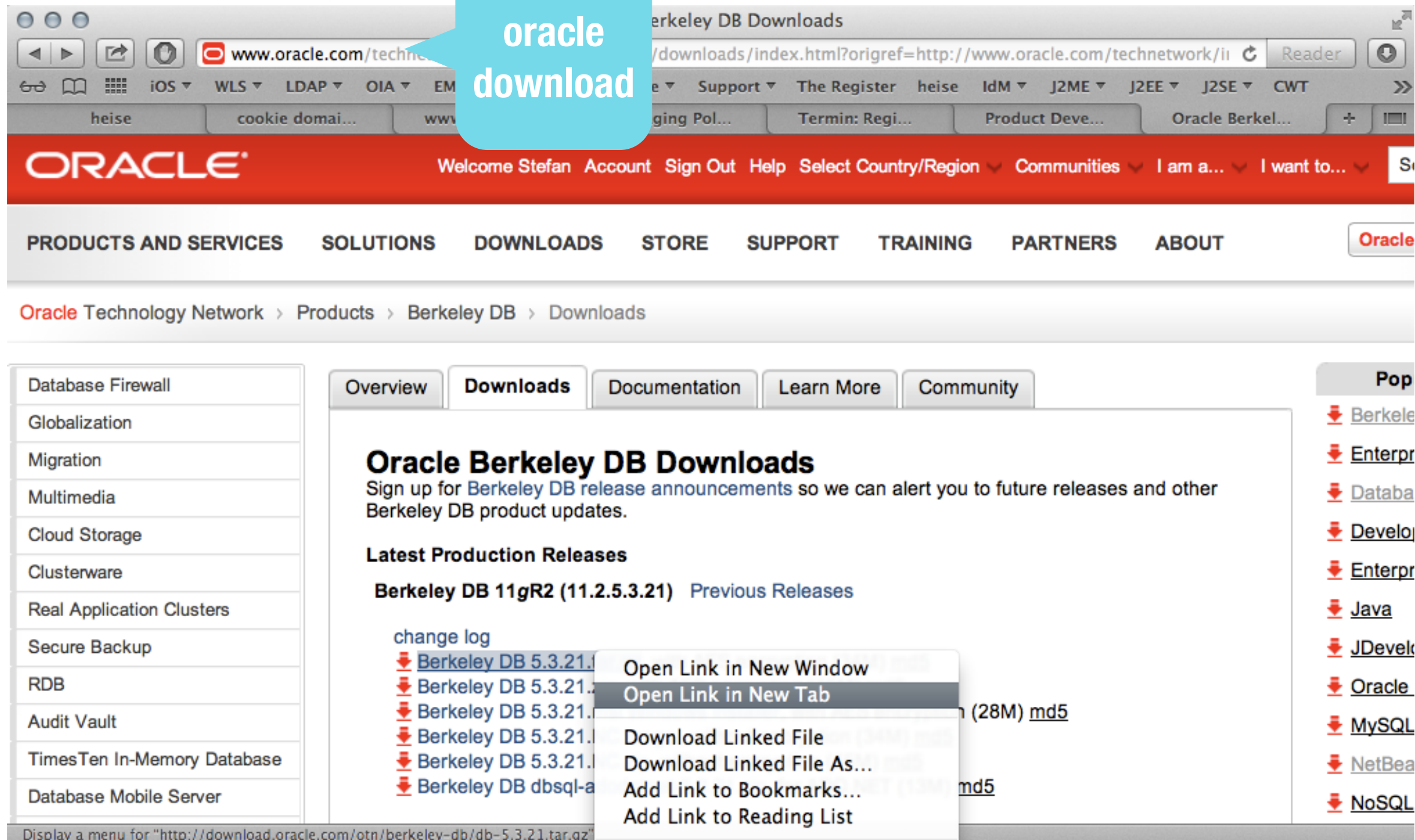




Foundation

How to achieve SSO for multiple apps?

If you want to download...



WebSSO (recap)

...you have to log on;...

Please click here to sign in

Single Sign On - Login

https://login.oracle.com/mysso/signon.jsp

Reader

heise cookie domai... www.ietf.org... Managing Pol... Termin: Regi... Product Deve... Single Sign O...

ORACLE

sign-in first

Sign In

Username

steffo.weber@oracle.com

Password

Lost Password? Reset your password via APS or by calling the Oracle Helpdesk

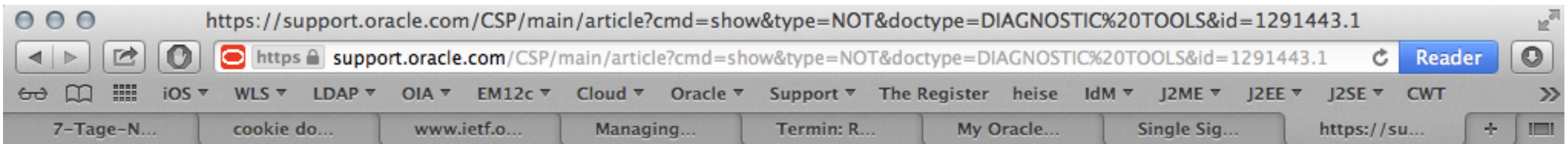
Sign In

Powered by Oracle Access Manager 11g

Display a menu for "javascript:doLogin(document.LoginForm);"

WebSSO (recap)

... and you're logged on site-wide.



Using DirTracer to Gather Debug Data for DSEE or ODSEE Directory Servers. [ID 1291443.1]

Modified 03-DEC-2012 Type DIAGNOSTIC TOOLS Status PUBLISHED

Applies to:

Oracle Directory Server Enterprise Edition - Version 5.1 and later
Information in this document applies to any platform.

Main Content

DT7 (DirTracer) version 7.1.2

Always consult this document to make sure you have the latest DT version "each" time you log a new DSEE/ODSEE service request.

Attachments:

(see the Downloads section of this doc near the bottom)

- DirTracer 7.1.2 Solaris
- DirTracer 7.1.2 Linux

 [Rate this document](#)

support

SSO for mobile apps

A challenge.



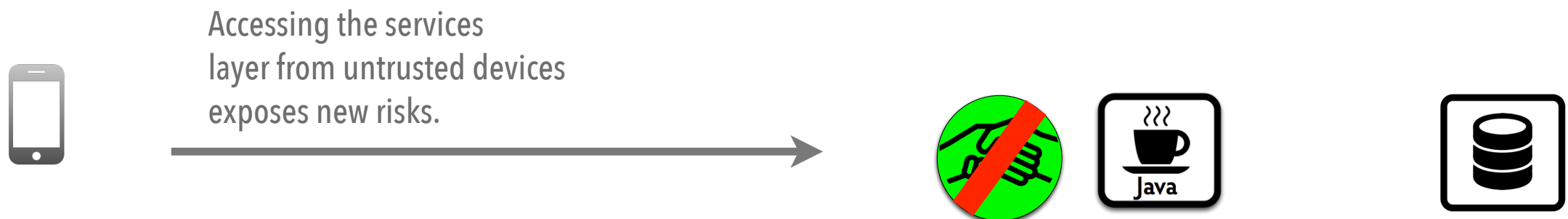
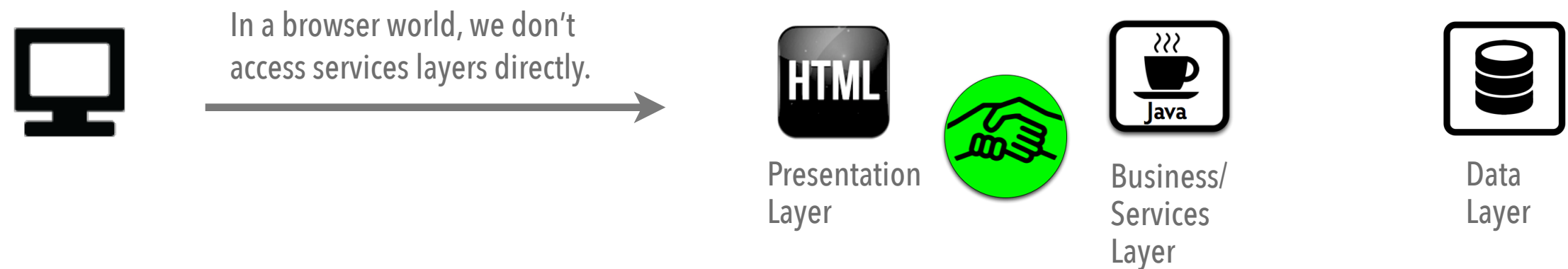
Options

What you _can_ do.

- ▶ Store credentials
- ▶ Use iOS builtin Kerberos
- ▶ Embedded browser (HTML-5 apps)
- ▶ Adopt real SSO protocols (OAuth, Open ID Connect, SAML...)
- ▶ Inject security services into unsigned apps (mobile app management)

Analysis

New security situation.



iPhone is the new presentation layer

No trust between ext DMZ and service zone.

Mobile SSO

Three issues to solve.

- ▶ **Token store**
 - we have to simulate a cookie cache
 - ideally part of mobile OS – but isn't
- ▶ **Account for different services**
 - different tokens for different services
 - buying tickets for different concerts with the same credit card
- ▶ **Token insertion mechanism**
 - magically sending a token with a REST request

Inter-process
communication

Adopting OAuth

Providing REST
libraries

Foundation

OAuth concepts

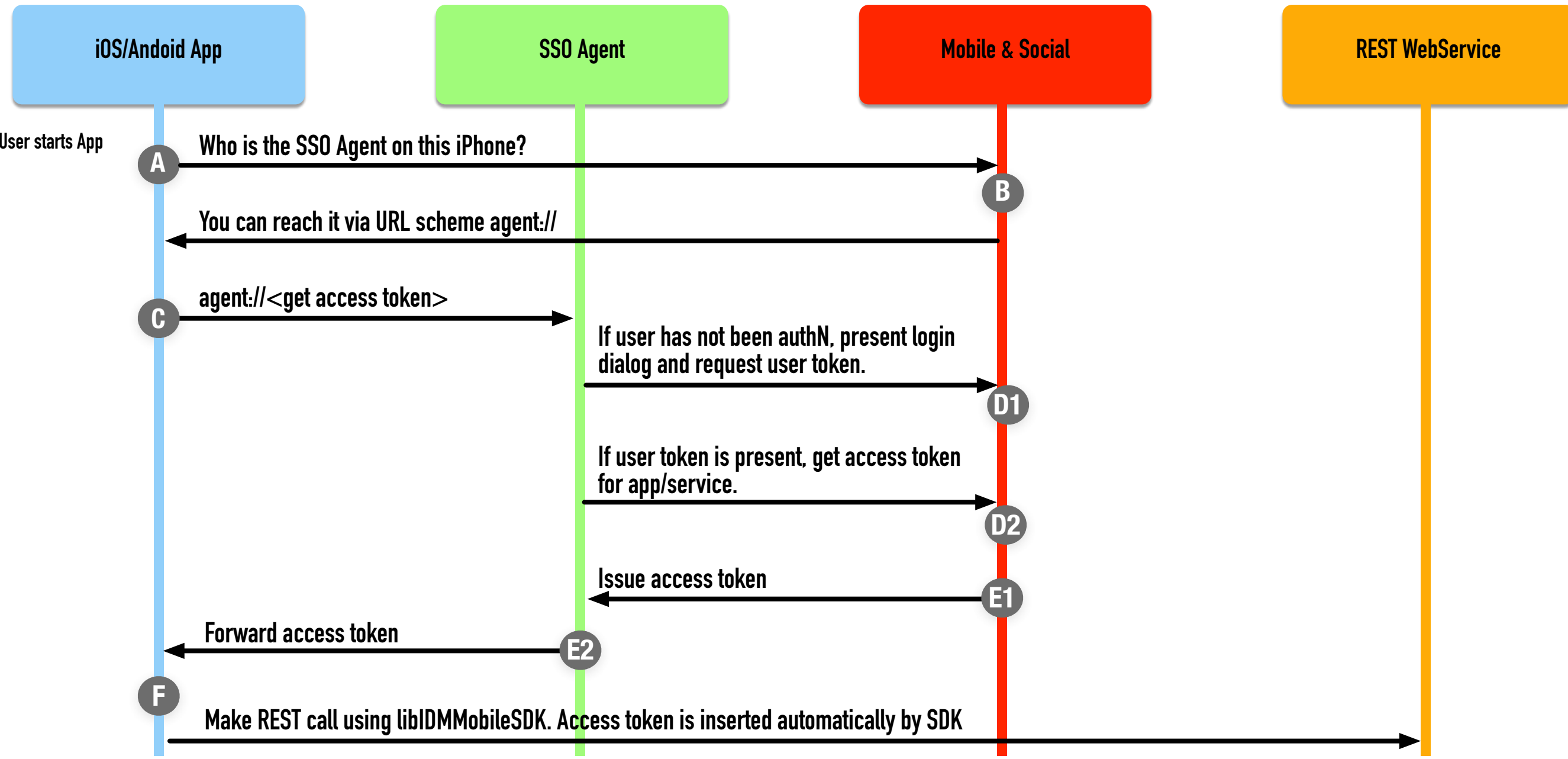
one **user token**

VS.

multiple **access tokens**

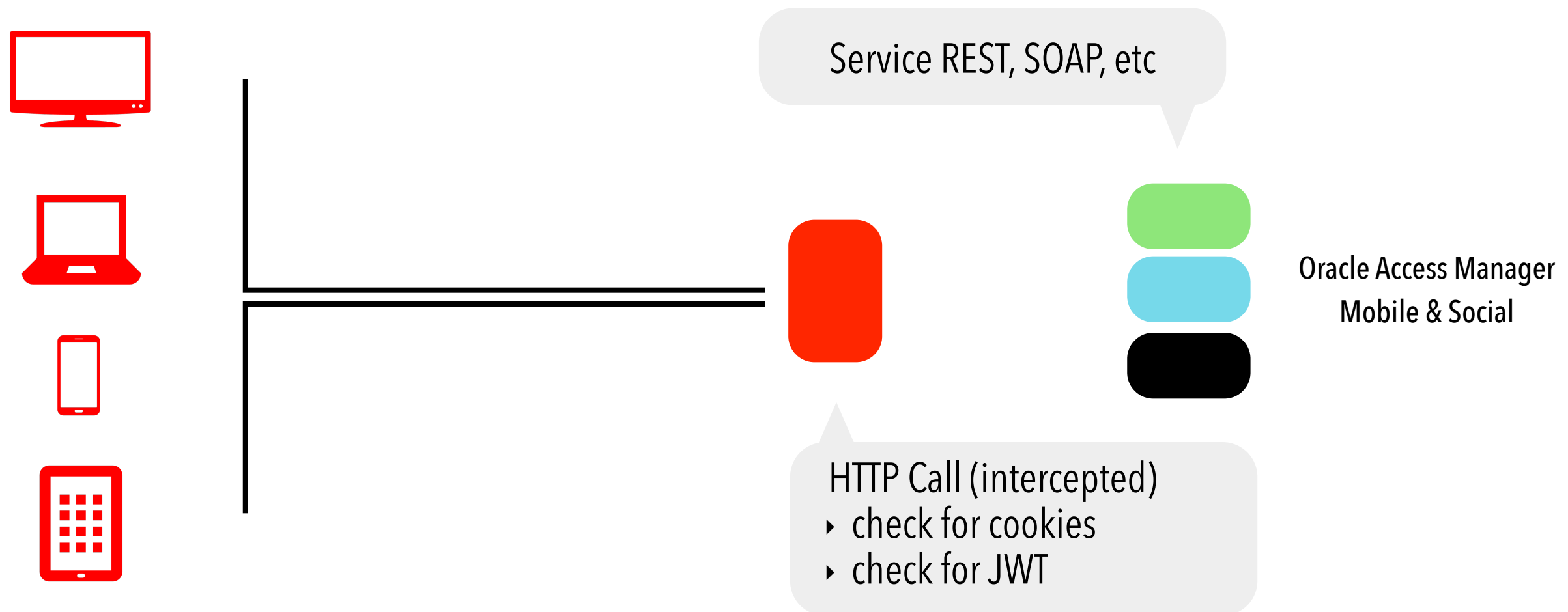
Foundation

Ok, here comes OAuth...



Foundation

All channels are equal.



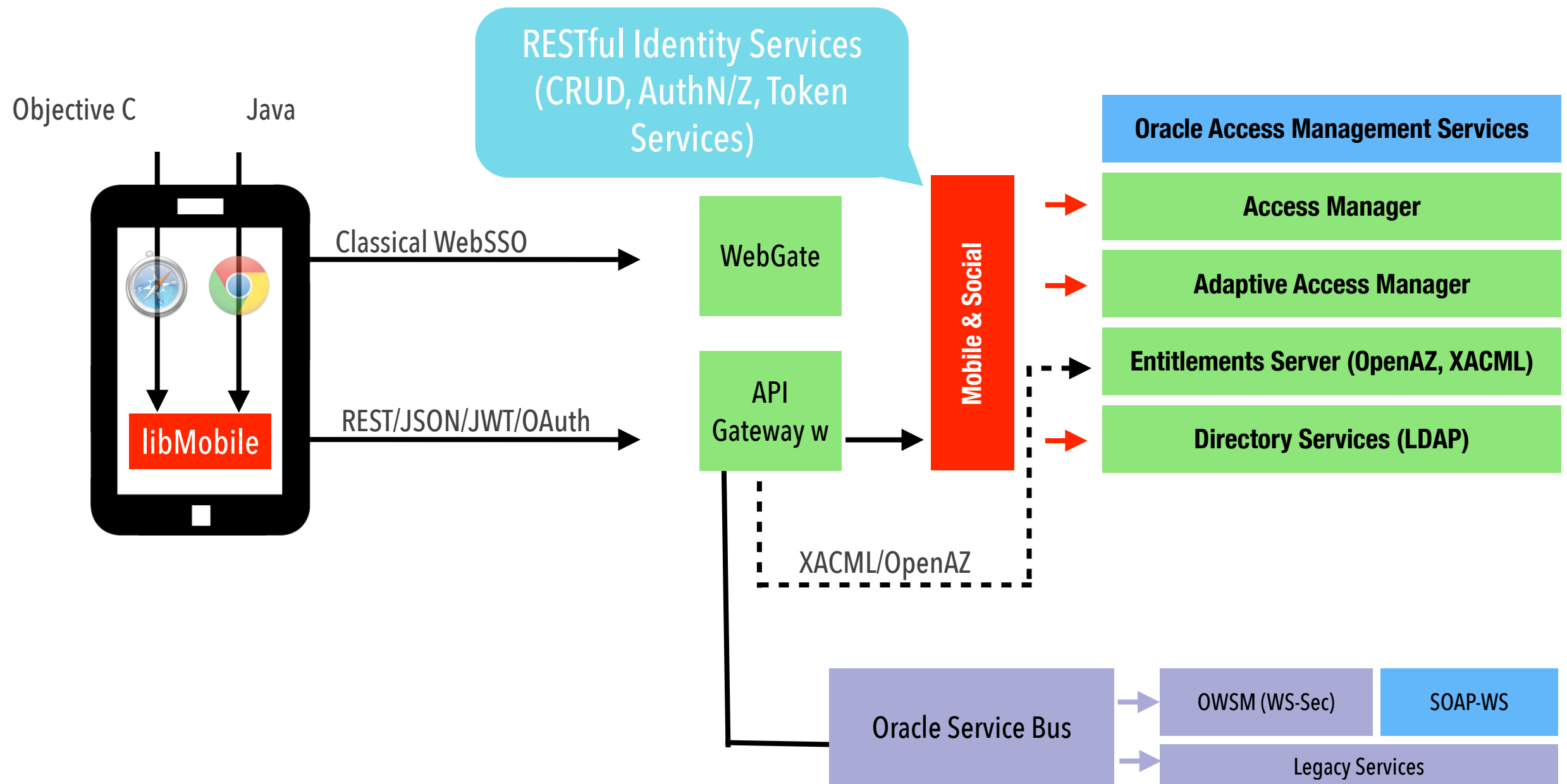
GET <http://oracle:7777/hello/steffo>

User-Agent: OIC-Authentication

Authorization: OAM-Auth rcfPxHcF1EywCq

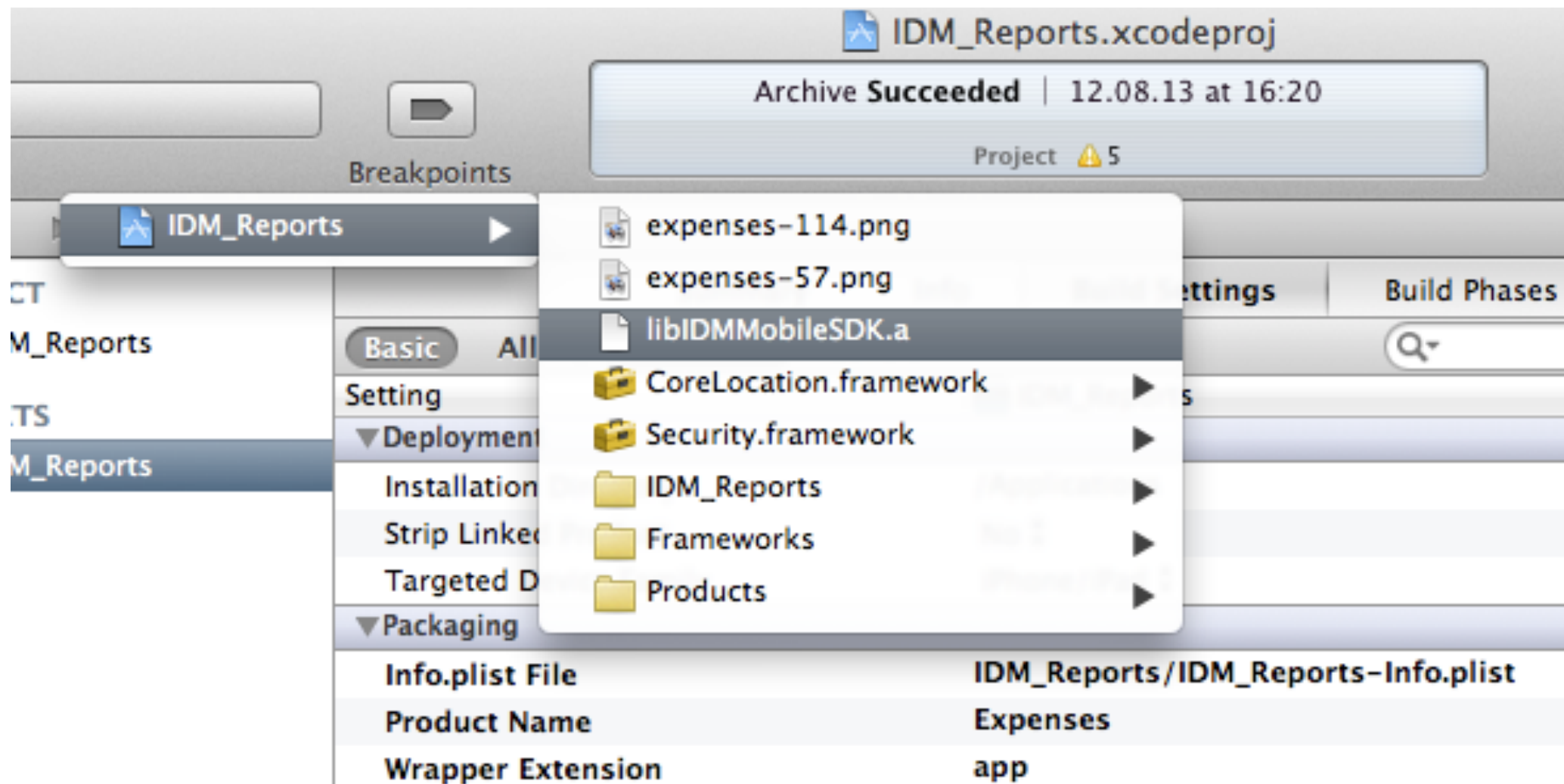
Foundation

Access management architecture.



Foundation

Import libIDMMobileSDK.a



Foundation

Register a URL scheme

Key	Type	Value
Information Property List	Dictionary	(18 items)
Localization native development region	String	en
Bundle display name	String	\$(PRODUCT_NAME)
Executable file	String	\$(EXECUTABLE_NAME)
Icon files (iOS 5)	Dictionary	(1 item)
Bundle identifier	String	com.sun.steffo.\$(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	Dictionary	(2 items)
URL identifier	String	com.sun.steffo.SimpleMobile
URL Schemes	Array	(1 item)
Item 0	String	simplemobile
Bundle version	String	1.0
Application requires iPhone environment	Boolean	YES
Main storyboard file base name	String	MainStoryboard
Icon already includes gloss effects	Boolean	YES
Required device capabilities	Array	(1 item)
Status bar tinting parameters	Dictionary	(1 item)
Supported interface orientations	Array	(3 items)

Foundation

SSO relevant code in iOS app

```
#import "IDMMobileSDK.h"
/* we have @property (nonatomic,retain) OMMobileSecurityService *mobileServices; from header */

- (void)connectToOICServerAndSetup {
    .....
    OMMobileSecurityService *mss = [[OMMobileSecurityService alloc]
        initWithURL:self.oicURL // e.g. http://token.net:14100/
        appName:self.applicationName // e.g. SampleApp or Art
        domain:self.oicServiceDomainName // e.g. MagServiceDomain
        delegate:self];
    self.mobileServices = mss;
    .....
    UIBarButtonItem *rightButton = [[UIBarButtonItem alloc]
        initWithTitle:@"Login"
        style:UIBarButtonItemStyleBordered
        target:self
        action:@selector(doLogin:)]; }

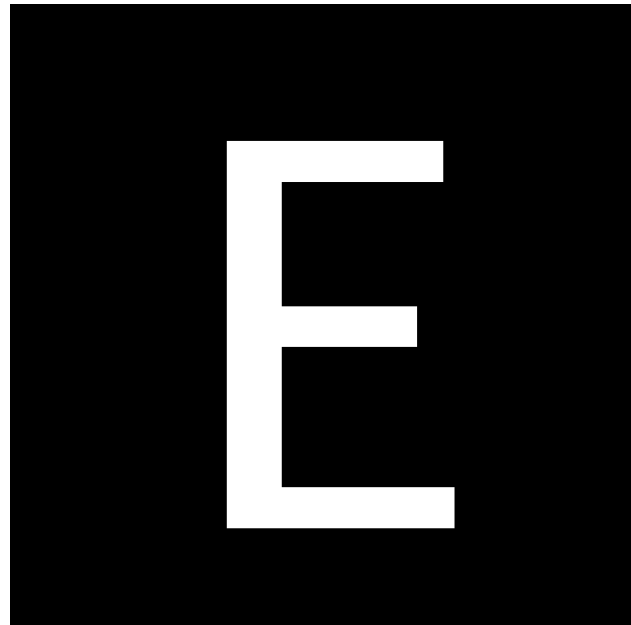
- (IBAction)doLogin:(id)object {
    .....
    NSError *error = nil;
    error = [self.mobileServices startAuthenticationProcess:nil
        presentViewController:self];}

- (void)didFinishAuthentication:(OMAuthenticationContext *)context
    error:(NSError *)error
{
    .....
    username = context.userName;
}
```

**Initialize app & load profile
from central server**

Login button & event config

Event handler



Experience

How long?

How complex?

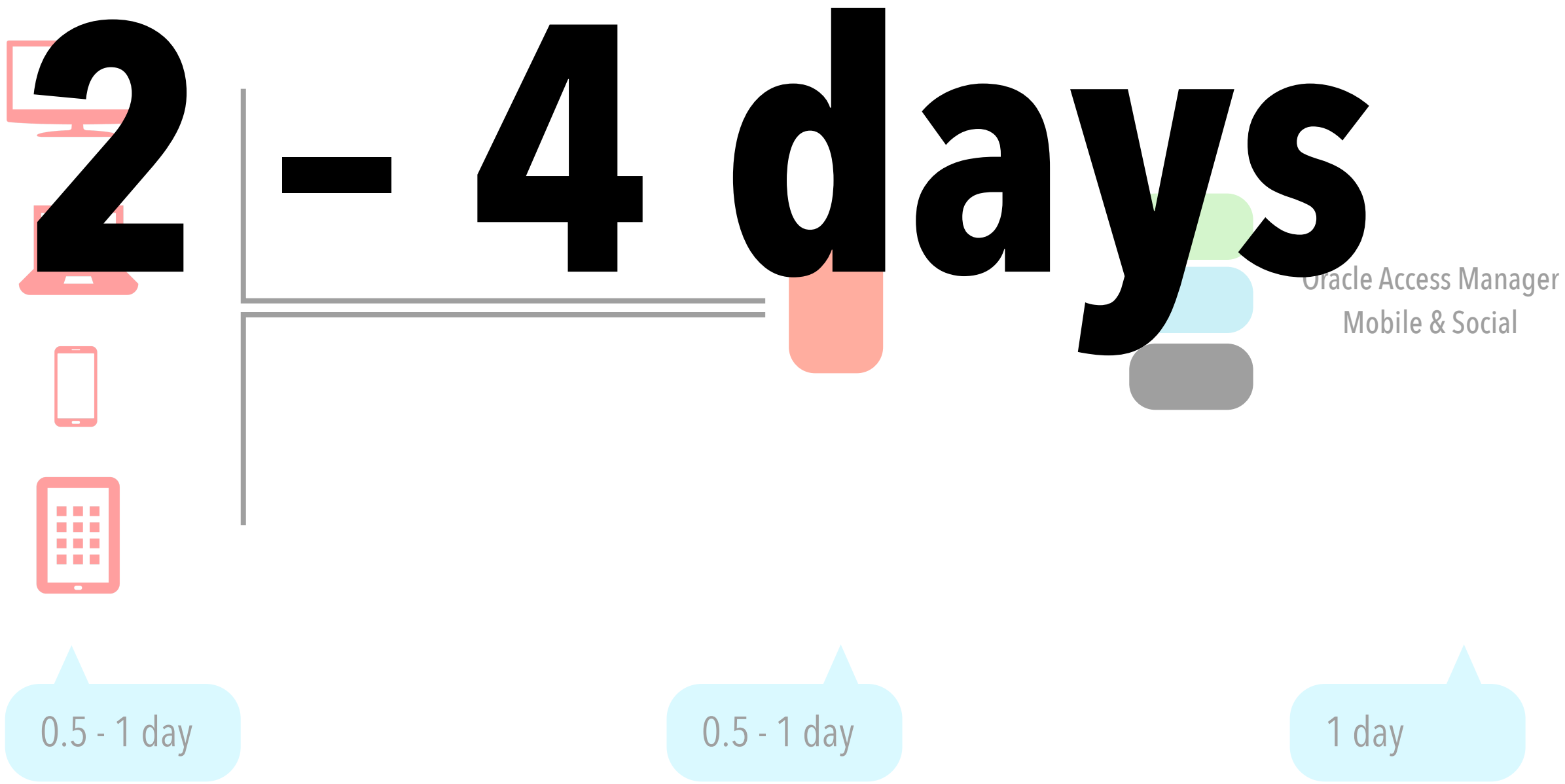
Experience

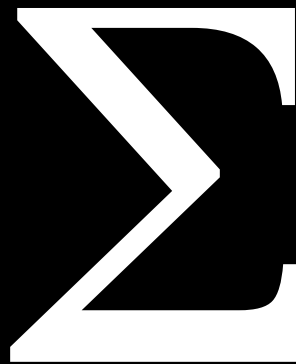
How long did it take?

- ▶ Good
 - Easy iOS integration (SSO is transparent to the developer)
 - Complete service protection
 - No hassle with Apple app store
- ▶ Suggested enhancements
 - Currently uses old app delegate pattern

Experience

How long did it take?





- ▶ Mobile SSO increases usability and customer loyalty
- ▶ OAuth eco-system can transform WebSSO into mobile SSO
- ▶ Don't think channel and avoid silos.



Identity
Culture

<http://flip.it/caxRa>

Will IoT be the
new mobile?