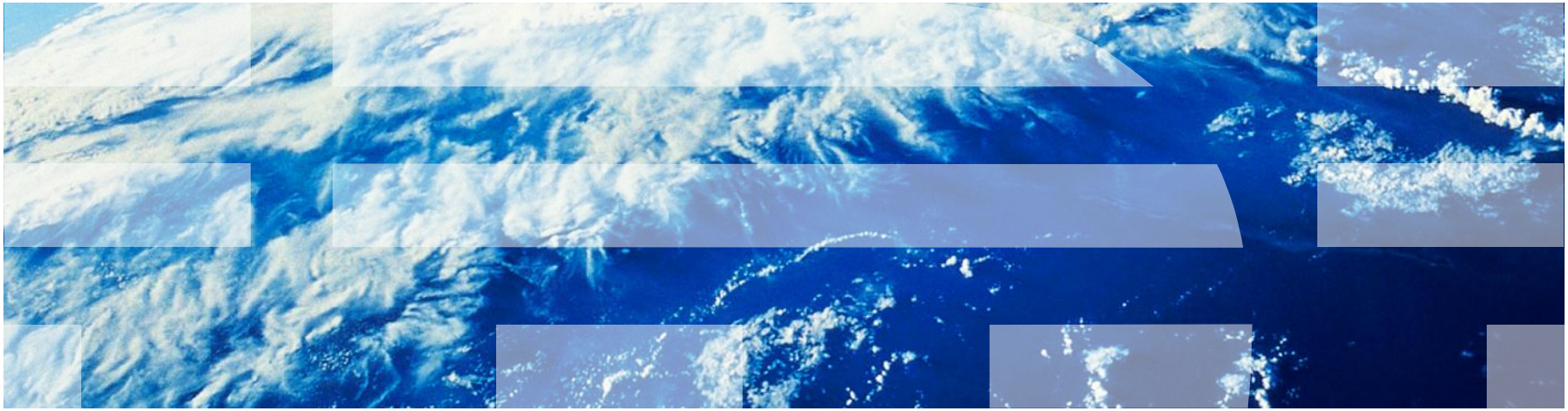
IBM Worklight Foundation V6.2.0 Getting Started

Application Authenticity Protection



Trademarks

- IBM, the IBM logo, ibm.com, and Worklight are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.
- Other company products or service names may be trademarks or service marks of others.
- This document may not be reproduced in whole or in part without the prior written permission of IBM.

About IBM®

- See http://www.ibm.com/ibm/us/en/

Agenda

- Overview
- Enabling application authenticity check – Hybrid
- Enabling application authenticity check – Native
- Controlling application authenticity from Worklight Console

Overview (1 of 5)

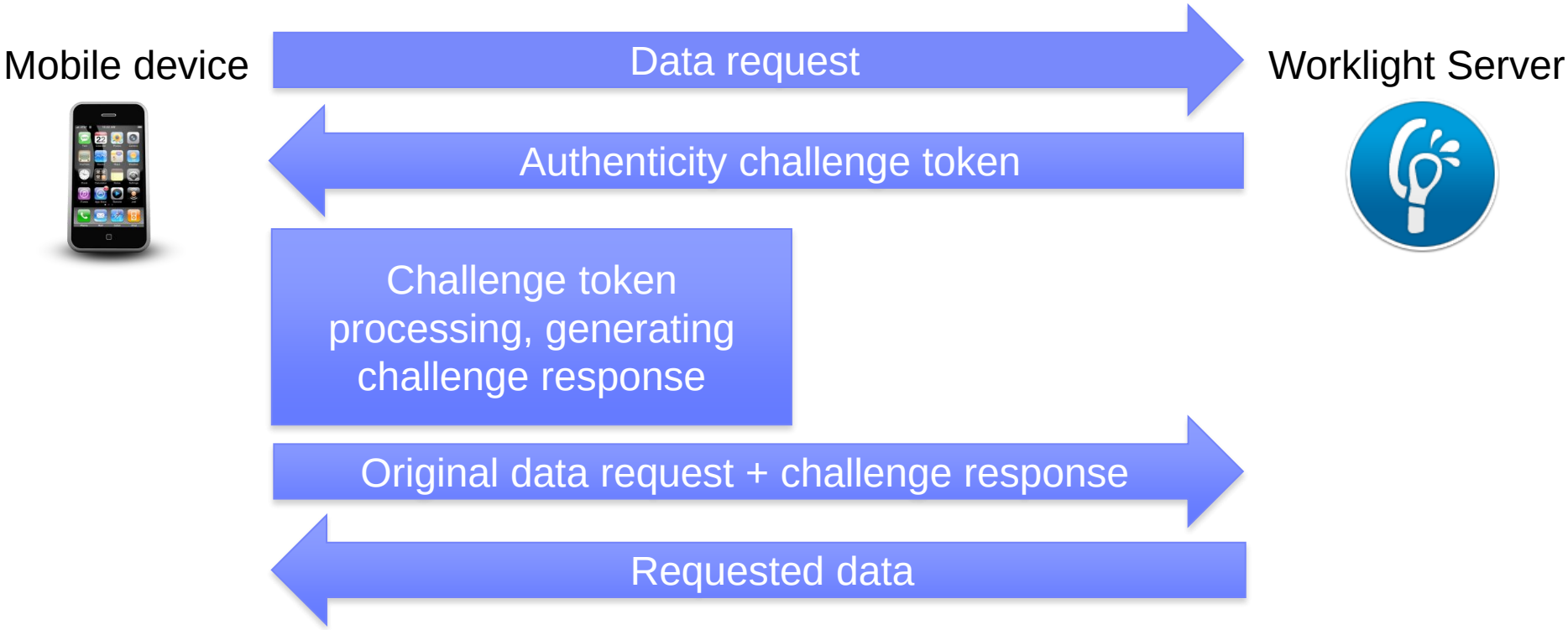
- The HTTP services (APIs) that Worklight® Server offers can be accessed by any entity by issuing an HTTP request.
- As described in previous modules, it is possible to protect relevant services with various security tests.
- The application authenticity check ensures that the application that tries to connect to a Worklight Server is the authentic one and was not tampered with or modified by some third-party attacker.
- Application authenticity is available for iOS and Android platforms.

Overview (2 of 5)

- **Important:**
  - Application authenticity protection is not available in the Worklight Development Server. To test, deploy the application to a Worklight Server on a remote application server.
  - Application authenticity protection is available only to licensed installations of Worklight Server.

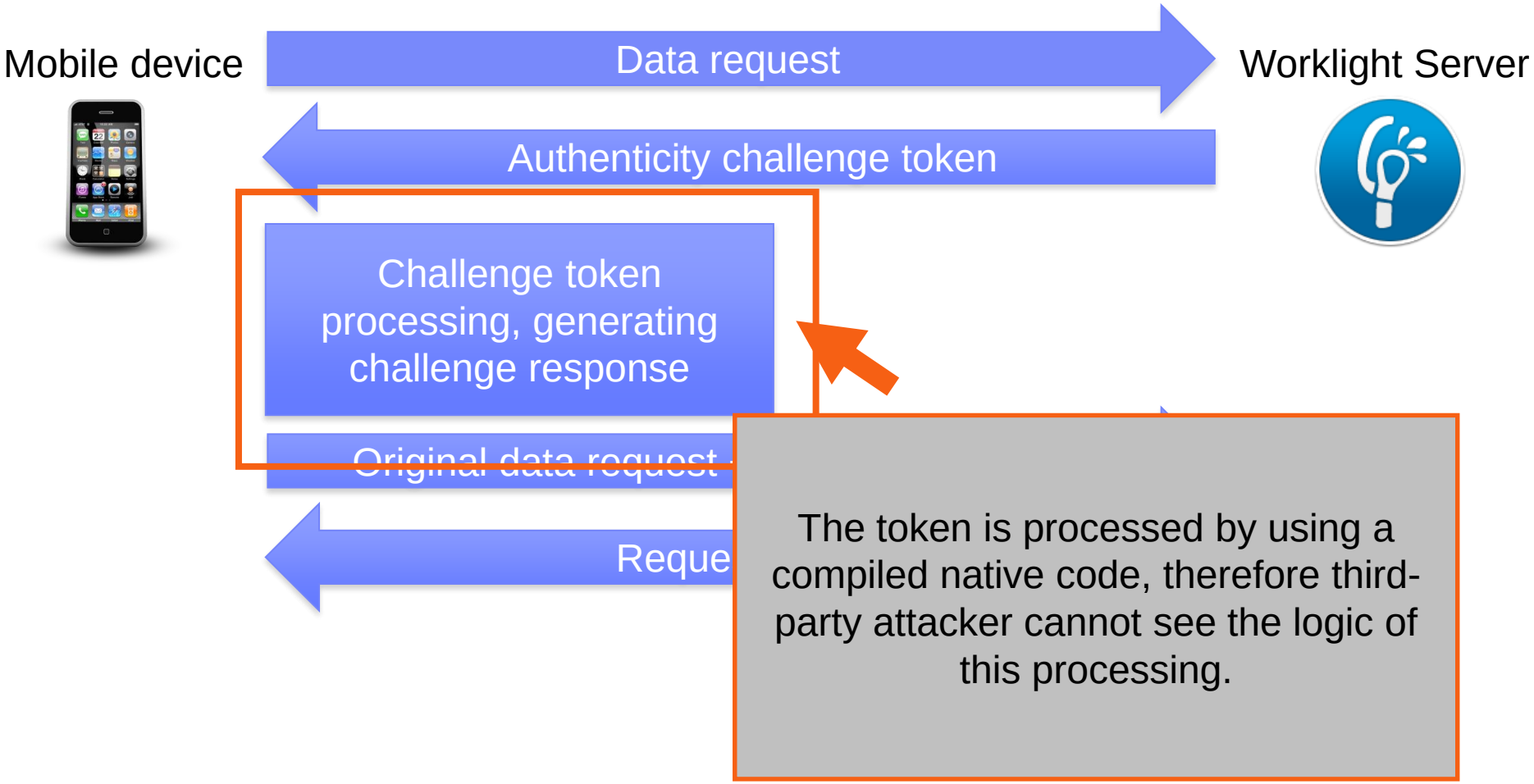
Overview (3 of 5)

- Authenticity check flow



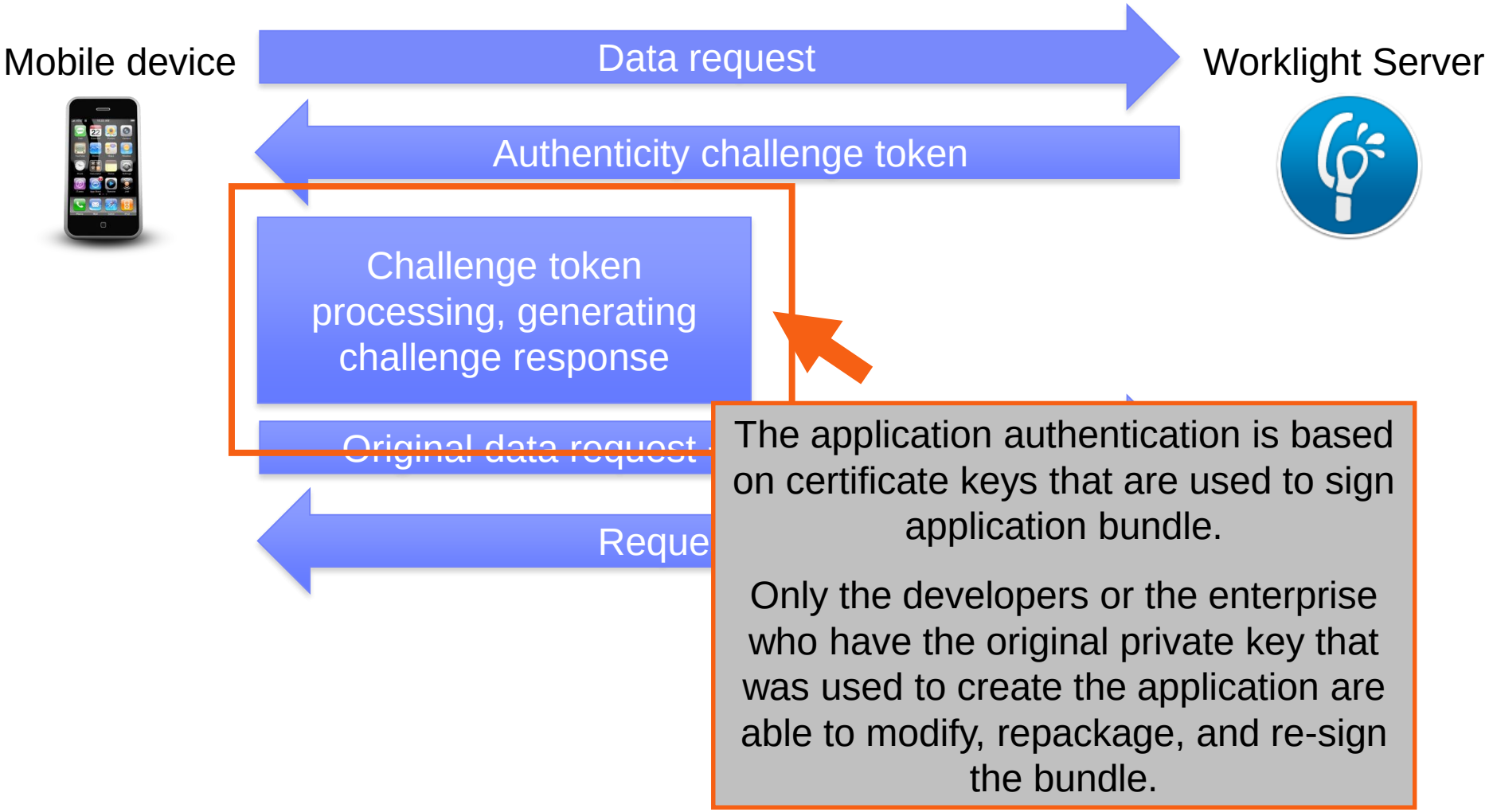
Overview (4 of 5)

- Authenticity check flow



Overview (5 of 5)

- Authenticity check flow



Agenda

- Overview
- Enabling application authenticity check – Hybrid
- Enabling application authenticity check – Native
- Controlling application authenticity from Worklight Console

Enabling application authenticity check – Hybrid (1 of 9)

- To enable application authenticity, start by modifying your `authenticationConfig.xml` file.
  - Add the relevant authentication realm to your security tests.
  - If you use `<mobileSecurityTest>`, you must add the `<testAppAuthenticity/>` child-element to it.
  - If you use `<customSecurityTest>`, you must add the `<test realm="wl_authenticityRealm"/>` child-element to it.

```
<mobileSecurityTest name="mobileTest">
    <testAppAuthenticity/>
    <testUser realm="MyUserAuthRealm"/>
    <testDeviceId provisioningType="auto" />
</mobileSecurityTest>
```

==

```
<customSecurityTest name="mobileTest">
    <test realm="wl_authenticityRealm" step="1"/>
    <test realm="wl_antiXSRFRealm" step="1"/>
    <test realm="wl_remoteDisableRealm" step="1"/>
    <test realm="MyUserAuthRealm" isInternalUserID="t
    <test realm="wl_deviceAutoProvisioningRealm" isIn
</customSecurityTest>
```

Enabling application authenticity check – Hybrid (2 of 9)

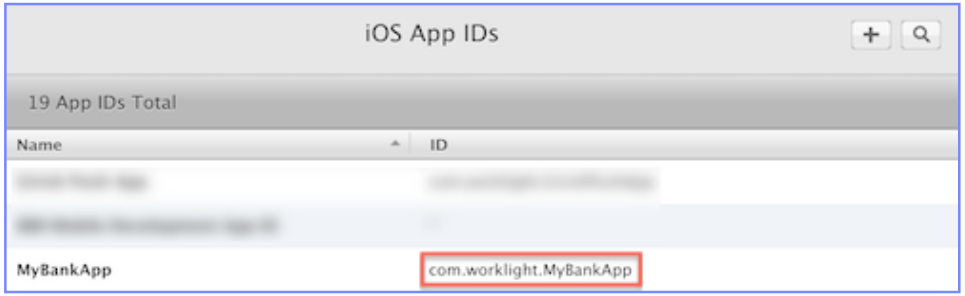
- Next, modify the `application-descriptor.xml` file of your application.
  - Add the `securityTest` attribute to the Android or iPhone/iPad environment element. For example:

```
<android version="1.0" securityTest="customTests">
```

Enabling application authenticity check – Hybrid (3 of 9)

- To enable application authenticity check for the **iPhone/iPad environment**:

  1. Specify the `bundleId` of your application exactly as you defined it in the Apple Developer portal. For example:

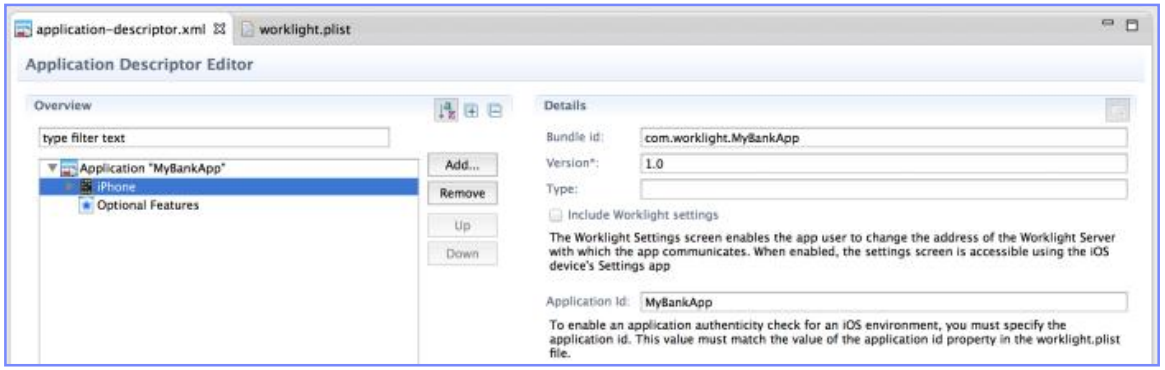



```
<iphone bundleId="com.worklight.MyBankApp" version="1.0">
    <worklightSettings include="false"/>
    <security>
        <encryptWebResources enabled="false"/>
        <testWebResourcesChecksum enabled="false" ignoreFileExtensions="png, jpg, jpeg, gif, mp4, mp3"/>
    </security>
</iphone>
```

Enabling application authenticity check – Hybrid (4 of 9)

- To enable application authenticity check for the **iPhone/iPad environment**:

  2. Add the **Application Id** by using the Application Descriptor Editor (design view):



  - The Application Id value must match the value of the `application id` property, which is located in the `worklight.plist` file.

Enabling application authenticity check – Hybrid (4 of 9)

- You can also directly edit `application-descriptor.xml` and add an `applicationId` attribute to the `iphone` element:

```
<iphone
    bundleId="com.worklight.MyBankApp"
    applicationId="MyBankApp"
    securityTest="customTests"
    version="1.0"
>
```

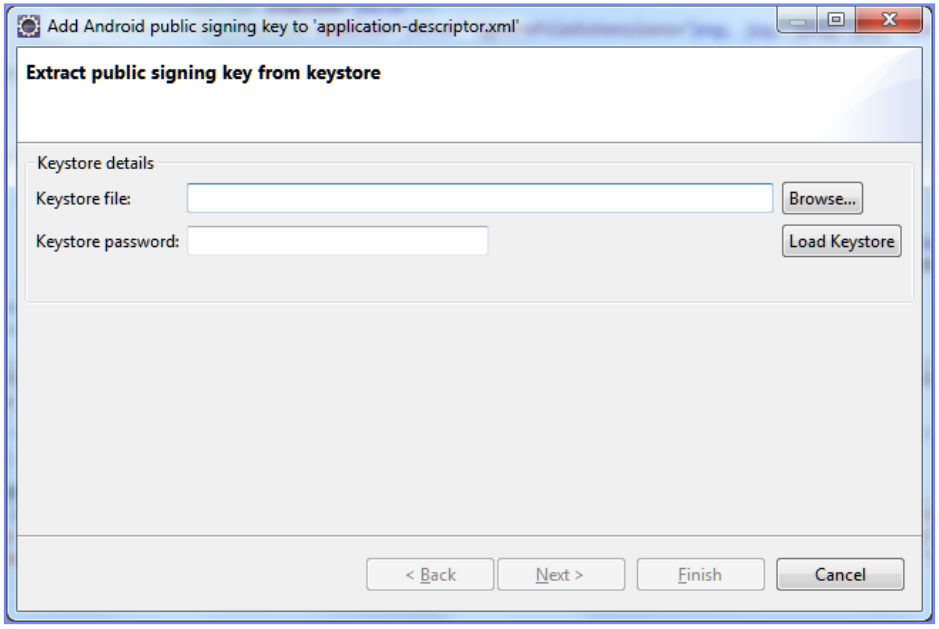
Enabling application authenticity check – Hybrid (5 of 9)

- To enable application authenticity check for the **Android environment**:

  1. Extract the public signing key of the certificate that is used to sign application bundle (`.apk` file).
     - Worklight Studio provides tools to simplify this process.
     - If you are building an application for distribution (production), you must extract the public key from the certificate that you are using to sign your production ready application.
     - If you are building an application in the development environment, you might use the public key from a default development certificate that is supplied by the Android SDK.
     - The development certificate can be found in a keystore that is in a **{user-home}/.android/debug.keystore** file.

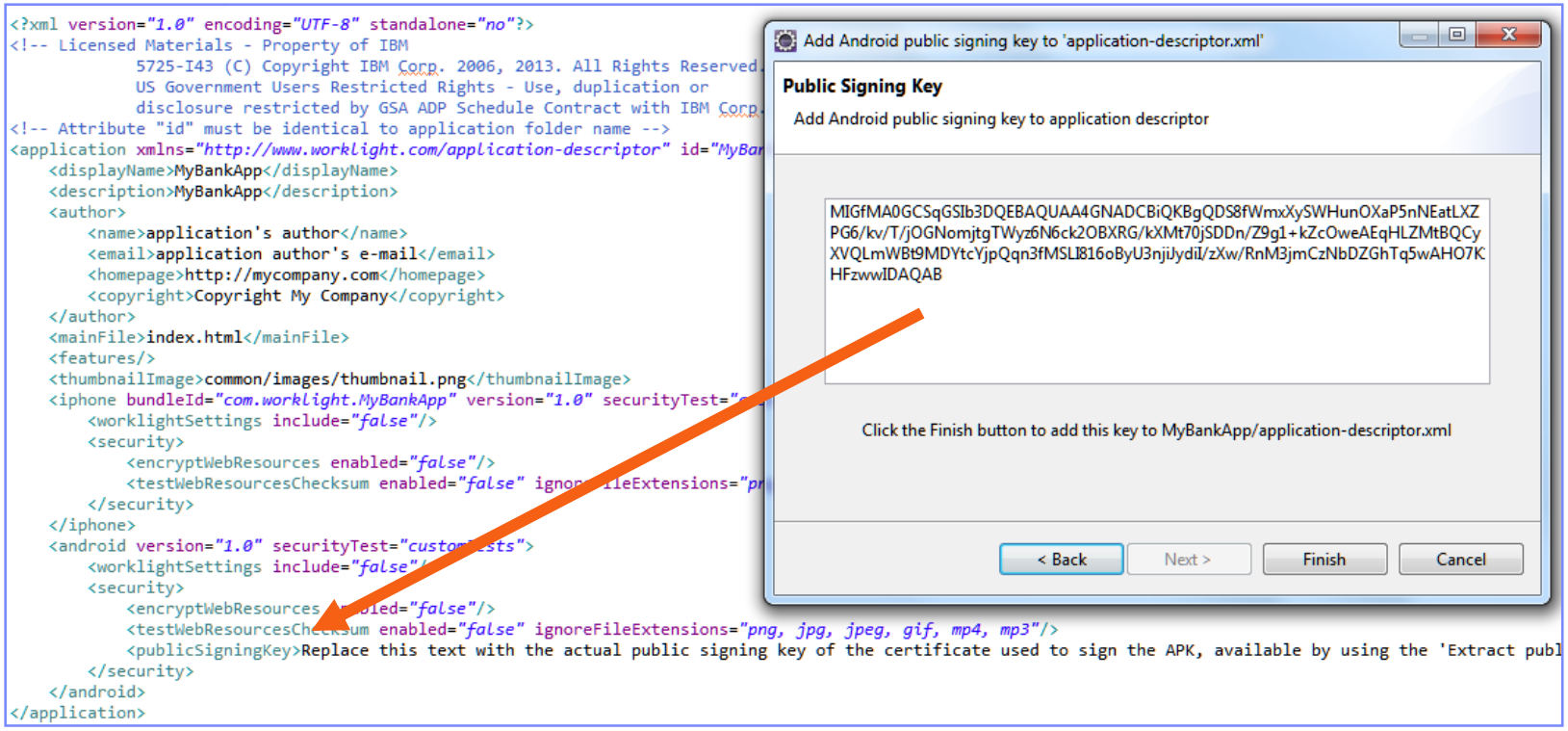
Enabling application authenticity check – Hybrid (6 of 9)

- You can either extract the public key manually or use the wizard that is Worklight Studio provides.
- To use the wizard:
  1. Right-click your Android environment folder and select **Extract public signing key**.
  2. Specify the location and the password of a keystore file, and click **Load Keystore**.
  3. The default password for **debug.keystore** is “android”.
  4. Set the **Key alias** and click **Next**.



Enabling application authenticity check – Hybrid (7 of 9)

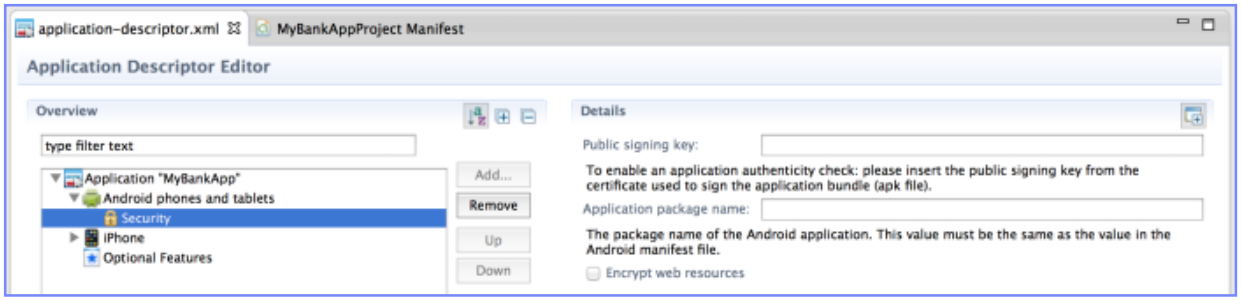
- A dialog opens that displays the public key.
- After you click **Finish**, the public key is automatically pasted to the relevant section of the `application-descriptor.xml` file.



Enabling application authenticity check – Hybrid (8 of 9)

- To enable application authenticity check for the **Android environment**:

  2. Add the **Application package name** by using the Application Descriptor Editor (design view):



  - Take the **Application package name** value from the `package` attribute of the `<manifest>` node in the `AndroidManifest.xml`.
  - If you decide to change the value to another, verify that you change it in both locations.

Enabling application authenticity check – Hybrid (9 of 9)

- You can also directly edit `application-descriptor.xml` and add a `packageName`:

```
<android version="1.0" securityTest="customTests">
    <worklightSettings include="false"/>
    <security>
        <encryptWebResources enabled="false"/>
        <testWebResourcesChecksum enabled="false"
            ignoreFileExtensions="png, jpg, jpeg, gif, mp4, mp3"/>
        <publicSigningKey>MIGfM …</publicSigningKey>
        <packageName>com.MyBankApp</packageName>
    </security>
</android>
```

Agenda

- Overview
- Enabling application authenticity check – Hybrid
- Enabling application authenticity check – Native
- Controlling application authenticity from Worklight Console

Enabling application authenticity check – Native

- When you enable App Authenticity in a native application:
  - For the **iOS environment:**
    1. In Eclipse, the steps to follow are the same as done in the previous slides.
    2. In Xcode, verify that the following value exists in the **Other Linker Flags** field: `-ObjC`
  - For the **Android environment:**
    1. In Eclipse, the steps to follow are the same as done in the previous slides.
    2. From the Worklight project Native API folder, copy the following folders to your native project `lib` folder: `armabi, armabi-v7a, mips, x86`.

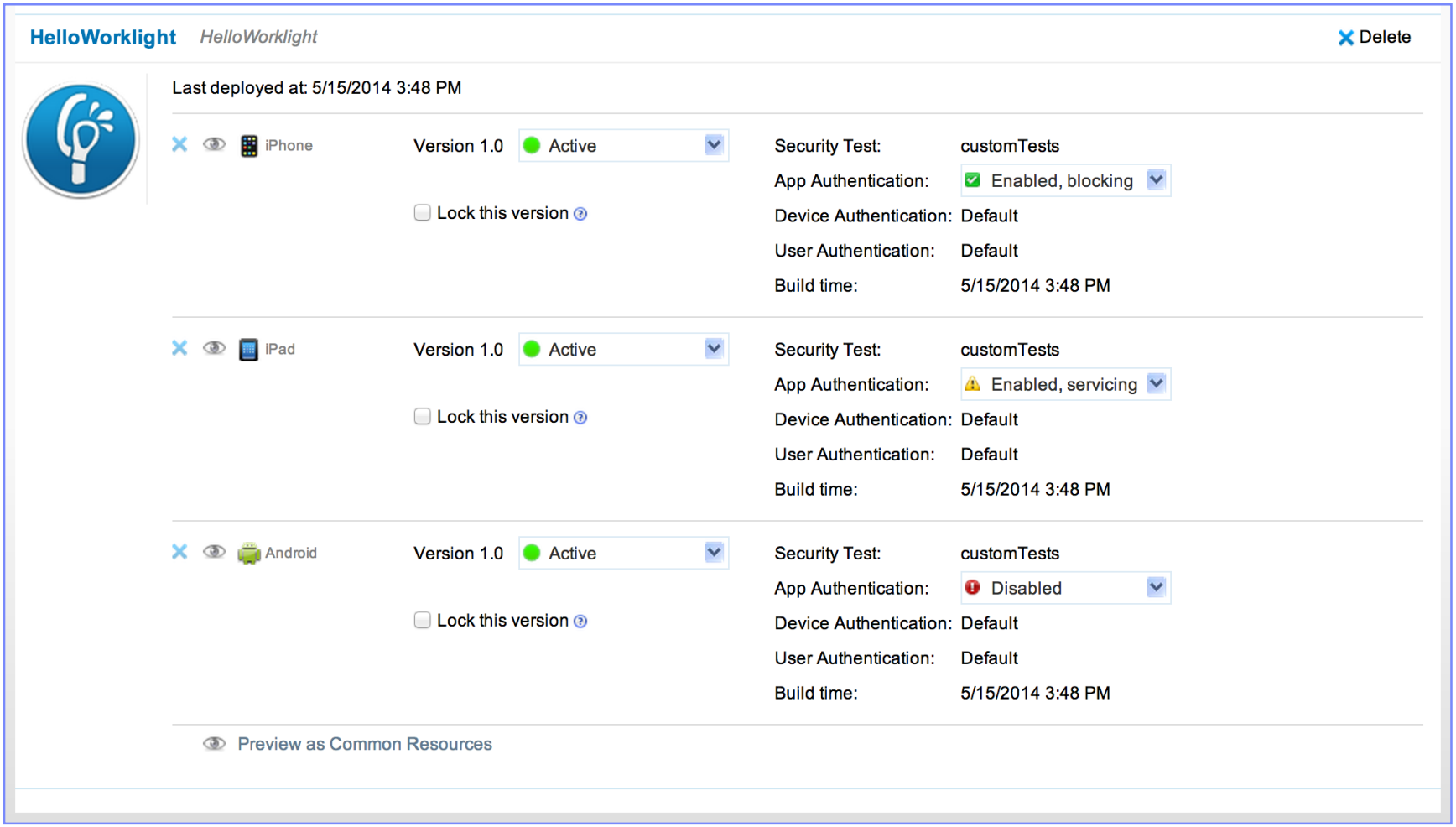
Agenda

- Overview
- Enabling application authenticity check – Hybrid
- Enabling application authenticity check – Native
- Controlling application authenticity from Worklight Console

Controlling Application Authenticity from Worklight Console (1 of 2)

- Worklight Console provides means for enabling and disabling application authenticity realm.
- You can set three modes:
  - **Enabled, blocking** – This mode means that the application authenticity check is enabled. If the application fails the check, it will not be served by a Worklight Server.
  - **Enabled, serving** – This mode means that the application authenticity check is enabled. If the application fails the check, it will still be served by a Worklight Server.
  - **Disabled** – This mode means that application authenticity check is disabled.

Controlling Application Authenticity from Worklight Console (2 of 2)



Controlling Application Authenticity from Worklight Console (3 of 3)

- Worklight Console provides means for enabling and disabling application authenticity realm.
- You can set three modes:
  - **Enabled, blocking** – This mode means that the application authenticity check is enabled. If the application fails the check, it will not be served by a Worklight Server.
  - **Enabled, serving** – This mode means that the application authenticity check is enabled. If the application fails the check, it will still be served by a Worklight Server.
  - **Disabled** – This mode means that application authenticity check is disabled.

Notices

- Permission for the use of these publications is granted subject to these terms and conditions.
- This information was developed for products and services offered in the U.S.A.
- IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.
- IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
  - IBM Director of Licensing
    IBM Corporation
    North Castle Drive
    Armonk, NY 10504-1785
    U.S.A.
- For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:
  - Intellectual Property Licensing
    Legal and Intellectual Property Law
    IBM Japan Ltd.
    1623-14, Shimotsuruma, Yamato-shi
    Kanagawa 242-8502 Japan
- **The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.
- This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.
- Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
- IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.
- Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:
  - IBM Corporation
    Dept F6, Bldg 1
    294 Route 100
    Somers NY 10589-3216
    USA
- Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.
- The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.
- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

- This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.
- Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:
  - © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

Privacy Policy Considerations

- IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.
- Depending upon the configurations deployed, this Software Offering may use session cookies that collect session information (generated by the application server). These cookies contain no personally identifiable information and are required for session management. Additionally, persistent cookies may be randomly generated to recognize and manage anonymous users. These cookies also contain no personally identifiable information and are required.
- If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent. For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the sections entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Support and comments

- For the entire IBM Worklight documentation set, training material and online forums where you can post questions, see the IBM website at:
  - http://www.ibm.com/mobile-docs
- **Support**
  - Software Subscription and Support (also referred to as Software Maintenance) is included with licenses purchased through Passport Advantage and Passport Advantage Express. For additional information about the International Passport Advantage Agreement and the IBM International Passport Advantage Express Agreement, visit the Passport Advantage website at:
    - http://www.ibm.com/software/passportadvantage
  - If you have a Software Subscription and Support in effect, IBM provides you assistance for your routine, short duration installation and usage (how-to) questions, and code-related questions. For additional details, consult your IBM Software Support Handbook at:
    - http://www.ibm.com/support/handbook
- **Comments**
  - We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this document. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.
  - For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.
  - When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state.
  - Thank you for your support.
  - Submit your comments in the IBM Worklight Developer Edition support community at:
    - https://www.ibm.com/developerworks/mobile/worklight/connect.html
  - If you would like a response from IBM, please provide the following information:
    - Name
    - Address
    - Company or Organization
    - Phone No.
    - Email address

Thank You