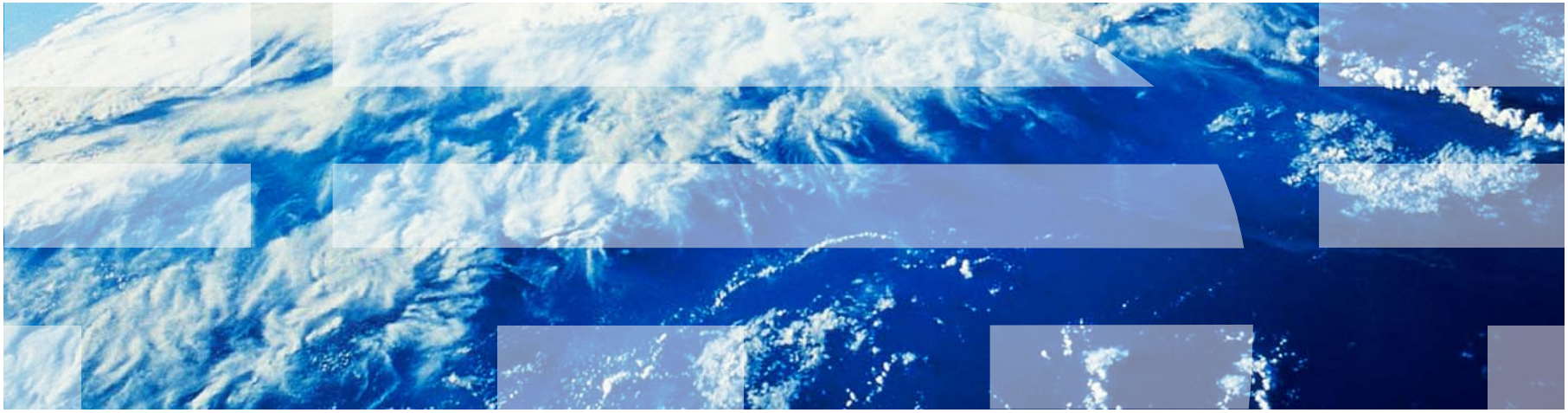
IBM Worklight V6.1.0
Getting Started

Device provisioning concepts



7 March 2014

Trademarks

- IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Worklight is a trademark or registered trademark of Worklight, an IBM Company. 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
- Device ID
- Understanding device provisioning
- No provisioning
- Auto provisioning
- Custom provisioning

Overview (1 of 2)

- Device provisioning is one of the most advanced and complex security features that IBM Worklight® provides.
- Device provisioning is a process of attaching a certificate to the device identity.
- Device identity (or in short – device ID) is similar to user identity, but is used to uniquely identify a specific device.
- Device identity is essential for various features. For example:
  - Push notifications – you want to know which device you are sending the notification to.
  - Reports – you want to know how many devices are using your server.
- Knowing the device identity opens a wide array of security integration possibilities, for example you can decide which devices are allowed to communicate with the Worklight Server.
- In this training module you learn what device provisioning is, what types of device provisioning are supported by IBM Worklight and what are the artifacts that are involved in a process of device provisioning.

Overview (2 of 2)

- IBM Worklight supports three types of device provisioning:
  - No provisioning
  - Auto provisioning
  - Custom provisioning
- This training module focuses on the first two types.
- For more information about custom provisioning, see the **Custom Provisioning** module and the IBM Worklight product documentation.

Agenda

- Overview
- Device ID
- Understanding device provisioning
- No provisioning
- Auto provisioning
- Custom provisioning

Device ID

- Device ID is automatically obtained (generated) by a client side framework, when it is requested by the Worklight Server.
- It is used to uniquely identify a specific device with the Worklight Server.
- Similar to the way the user ID is used for user authentication, the device ID is used for device authentication.
- Device provisioning is based on the device ID and supported on iOS and Android platforms.

Agenda

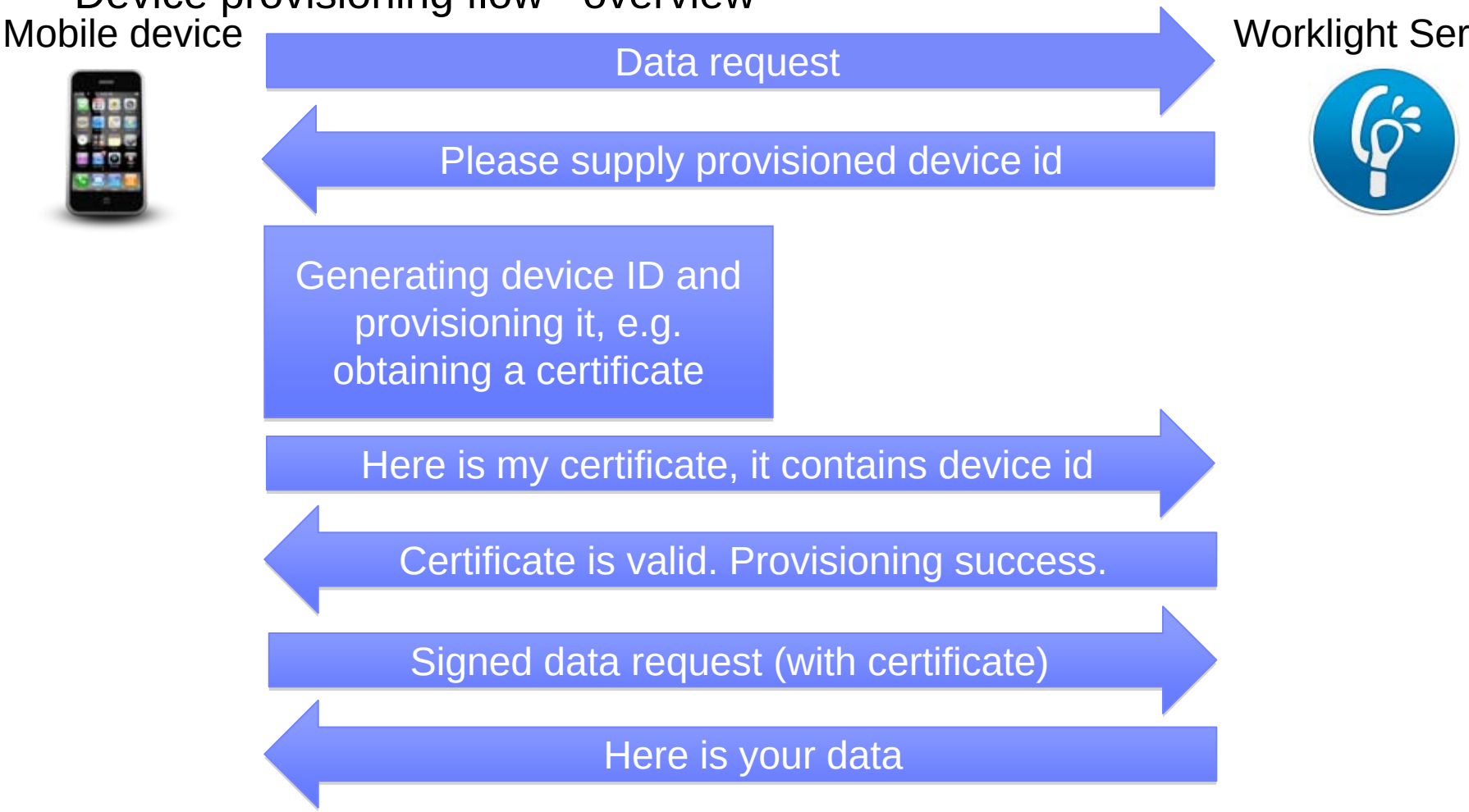
- Overview
- Device ID
- Understanding device provisioning
- No provisioning
- Auto provisioning
- Custom provisioning

Understanding device provisioning (1 of 2)

- Device provisioning is a process where a certificate is issued by the Worklight Server for a specific device.
- The issued certificate contains device information that is obtained during the provisioning process.
- Before issuing a certificate to a specific device, the Worklight Server can perform extra validations on received device credentials.
- It is possible to configure your own CA keystore to be used for device provisioning certificate generation.

Understanding device provisioning (2 of 2)

- Device provisioning flow - overview



Agenda

- Overview
- Device ID
- Understanding device provisioning
- No provisioning
- Auto provisioning
- Custom provisioning

No provisioning (1 of 2)

- **No provisioning** is appropriate for the development environment.
- Using **No provisioning** means that the provisioning process is not triggered (requested) by the Worklight Server.
- Application obtains the device ID and sends it to the Worklight Server as-is.
- The Worklight Server does not perform any validation, whether this device is allowed to communicate with it or not.
- The certificate is neither issued or requested on any stage.
- **No provisioning** is a default option for mobile applications.
- You are not required to manually enable **No provisioning** if you are using default security settings.

No provisioning (2 of 2)

- If you use **customSecurityTest** to protect a resource that requires device identity and want to use **No provisioning**, add the realm, as illustrated here, to your security test.

```
  <test realm="wl_anonymousUserRealm" isInternalUserID="true"/>
  <test realm="wl_deviceNoProvisioningRealm" isInternalDeviceID="true"/>
customSecurityTest>
```

Agenda

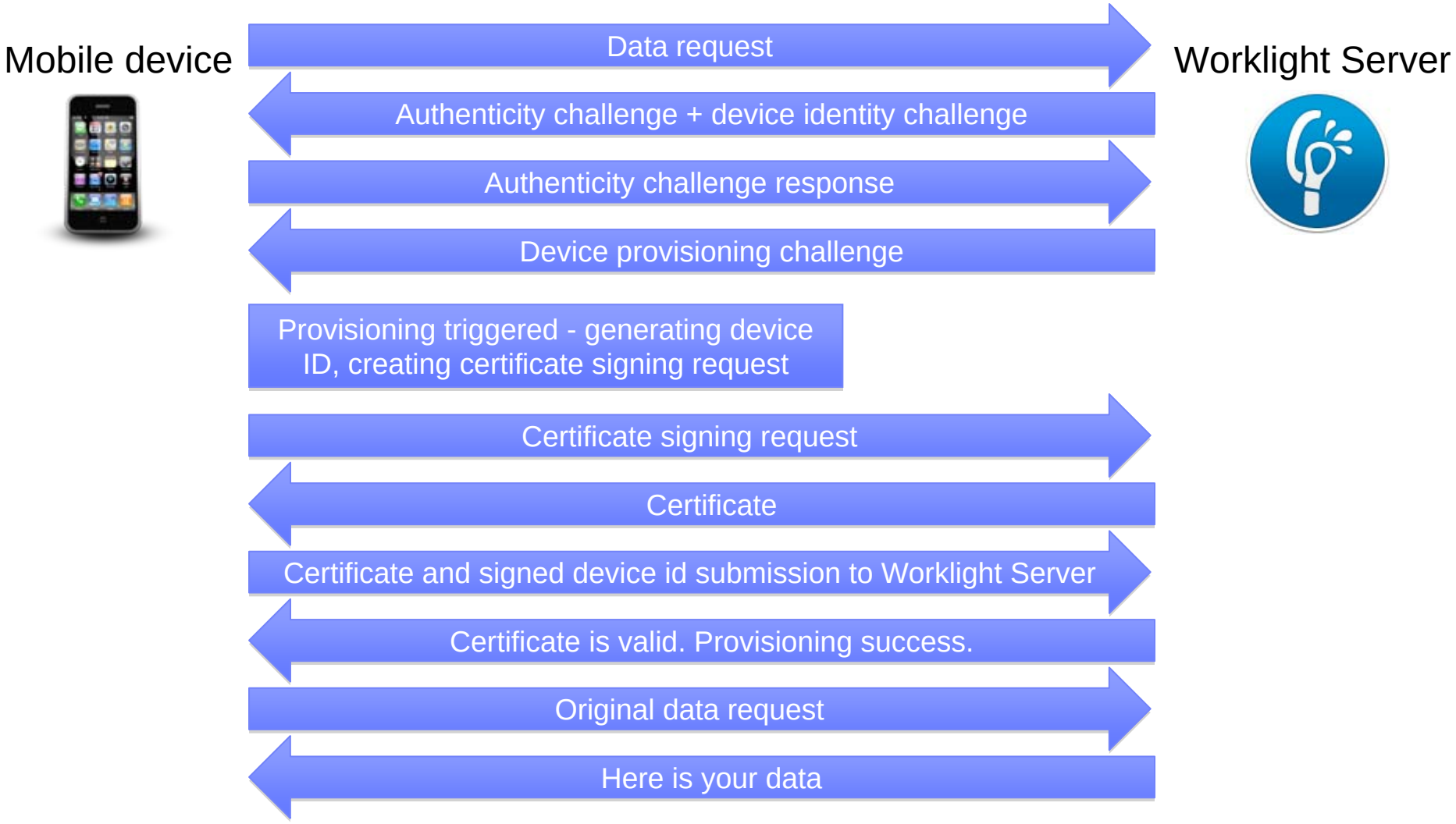
- Overview
- Device ID
- Understanding device provisioning
- No provisioning
- Auto provisioning
- Custom provisioning

Auto provisioning (1 of 7)

- **Auto provisioning** is an automated one-time process during which a certificate is issued by Worklight Server and sent to client.
- **Auto provisioning** is triggered by a Worklight Server when it requests a provisioned device identity.
- The application obtains the device ID and starts an automated provisioning process.
- The Worklight Server collects supplied device information and issues a certificate by using the server-side CA keystore.
- The certificate will be issued to any device that requests it, therefore **Auto provisioning** makes sense only when it is used after a successful authenticity check.
- See following slides for the **Auto provisioning** flow.

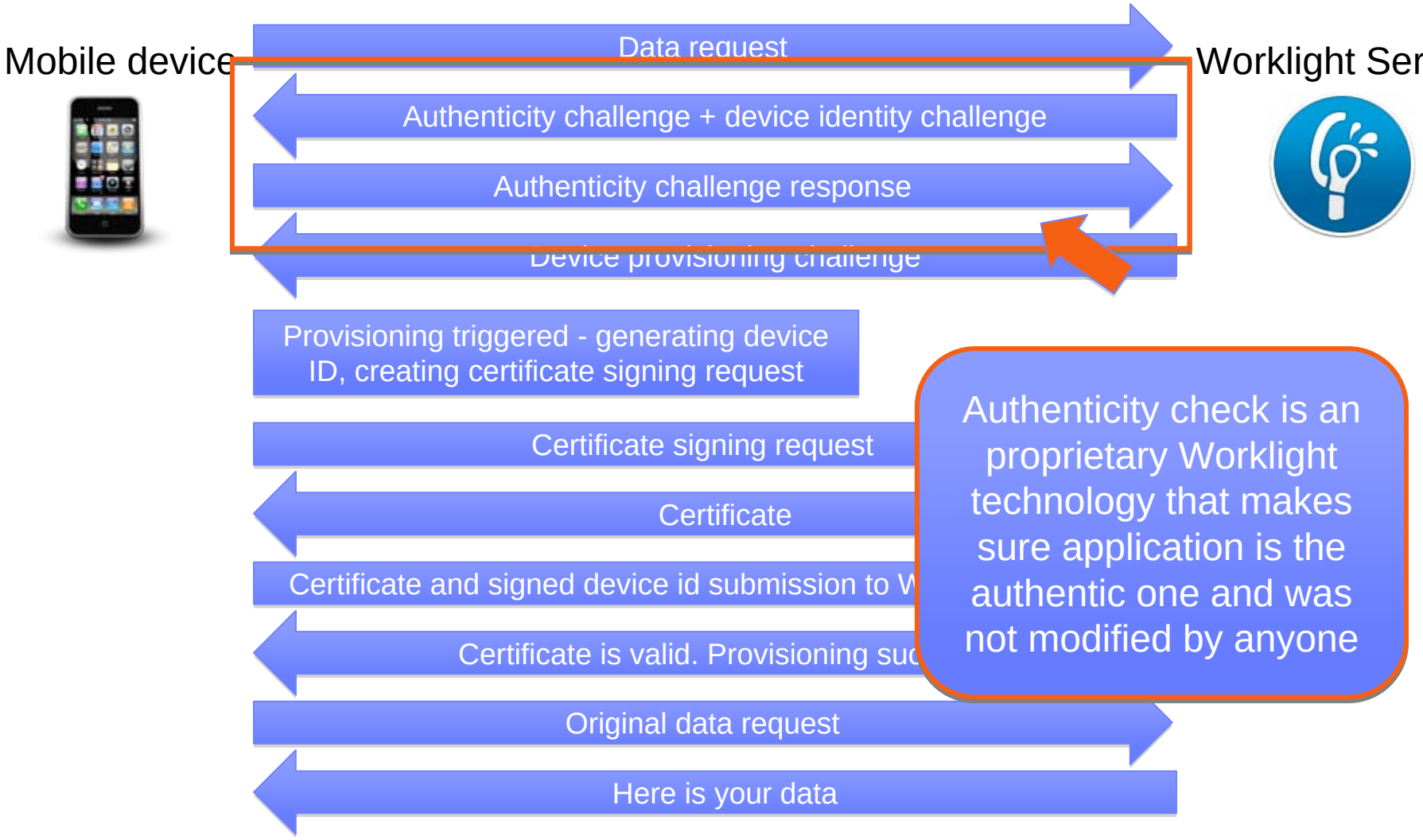
Auto provisioning (2 of 7)

- Auto provisioning during first application start:



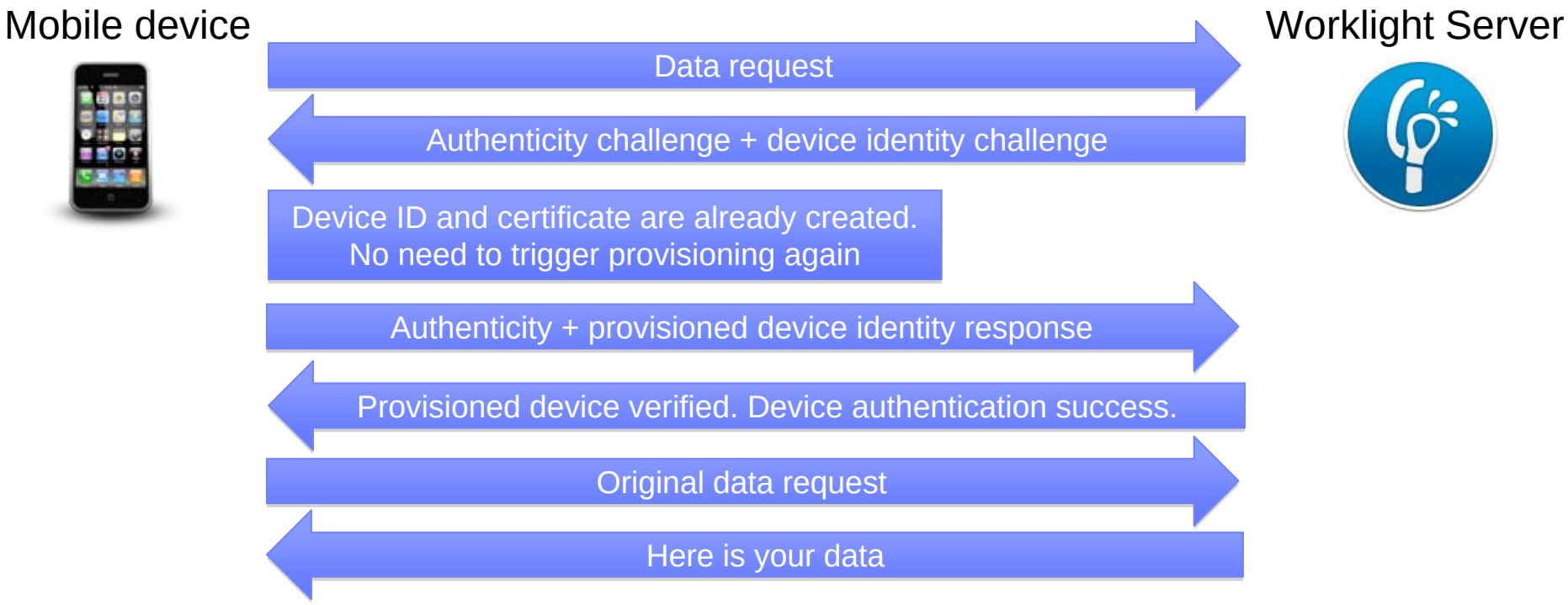
Auto provisioning (3 of 7)

- Auto provisioning during first application start:



Auto provisioning (4 of 7)

- Subsequent start up of a provisioned application:



Auto provisioning (5 of 7)

- To enable **Auto provisioning** add the following realms to your **authentication-config.xml** file.
  - If you use custom security test:

```
    <test realm="wl_authenticityRealm"/>
    <test realm="wl_deviceAutoProvisioningRealm" isInternalDeviceID="true"/>
</customSecurityTest>
```

  - If you use mobile security test:

```
<mobileSecurityTest name="mobileTests">
    <testAppAuthenticity/>
    <testDeviceId provisioningType="auto" />
</mobileSecurityTest>
```

Auto provisioning (6 of 7)

- By default the Worklight Server uses its internal keystore to issue a certificate.
- You can tell the Worklight Server to use your own keystore by adjusting the **worklight.properties** file.

```
#################################################################################################################
#    Worklight Default Certificate (For device provisioning)
#################################################################################################################
# You can change the default behavior with regard to CA certificates. You can also implement custom provisioning.
# If you want to change the auto-provisioning mechanism to use different granularity (application, device or group) or a
# different list of pre-required realms, you can create your own customized authenticator, login module and challenge handler.
# For more information, see the "Custom Authenticator and Login Module" Getting Started training module.

#The path to the keystore, relative to the server folder in the Worklight Project, for example: conf/my-cert.jks
#wl.ca.keystore.path=
#The type of the keystore file. Valid values are jks or pkcs12.
#wl.ca.keystore.type=
#The password to the keystore file.
#wl.ca.keystore.password=
#The alias of the entry where the private key and certificate are stored, in the keystore.
#wl.ca.key.alias=
#The password to the alias in the keystore.
#wl.ca.key.alias.password=

#################################################################################################################
#    Worklight SSL keystore
#################################################################################################################
#SSL certificate keystore location.
ssl.keystore.path=conf/default.keystore
#SSL certificate keystore type (jks or PKCS12)
ssl.keystore.type=jks
#SSL certificate keystore password.
ssl.keystore.password=worklight
```

- Note **wl.ca.keystore.path** property value can be both relative to the Worklight project ***/server/*** folder and absolute to the file system.

Auto provisioning (7 of 7)

- **Auto provisioning** must be used together with the application authenticity protection.
- For more information, see the **Application Authenticity Protection** module.

Agenda

- Overview
- Device ID
- Understanding device provisioning
- No provisioning
- Auto provisioning
- Custom provisioning

Custom provisioning

- **Custom provisioning** is an extension of **Auto provisioning**.
- With **Custom provisioning,** you can add custom CSR and certificate validation functions to define custom device provisioning rules.
- For more information, see the **Custom Device Provisioning** module and the IBM Worklight product documentation.

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