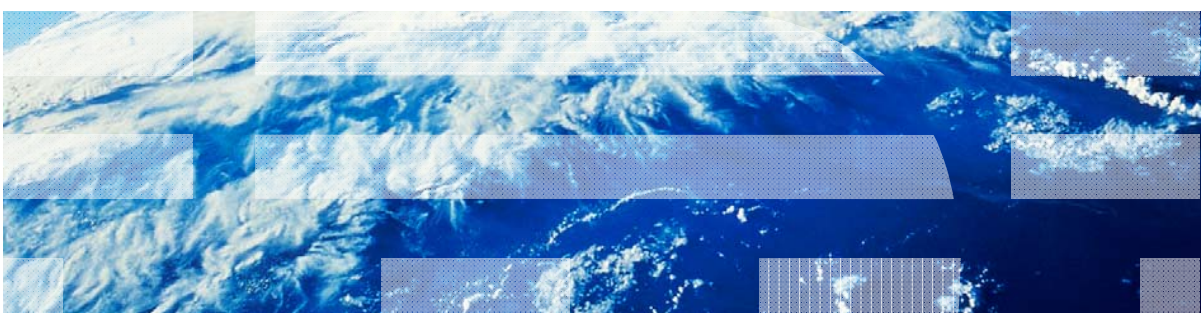
IBM Worklight V5.0.6
Getting Started

JSONStore – Encrypting sensitive data with FIPS 140-2



15 March 2013

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.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
- 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

- FIPS overview
  - What is FIPS 140-2?
  - JSONStore FIPS compliance
  - Supported Architectures
  - Procedure overview
- Configuration for FIPS on Android
- Configuration for FIPS on iOS
- Enabling FIPS mode in JSONStore
  - Validating FIPS mode

What is it FIPS 140-2?

- Federal Information Processing Standards (FIPS) are standards and guidelines that are issued by the United States National Institute of Standards and Technology (NIST) for federal government computer systems.
- FIPS Publication 140-2 is a security standard that is used to accredit cryptographic modules.
- FIPS 140-2 applies to cryptographic modules that are used to protect sensitive but unclassified information by United States federal government agencies and government contractors.

- **Note**: In this module, **FIPS** refers to the **FIPS Publication 140-2**.

JSON Store FIPS Compliance

- JSONStore uses OpenSSL to securely encrypt data.
- OpenSSL is an open source library that implements various cryptography and utility functions that are used by JSONStore.
- For JSONStore to run in a FIPS-compliant mode, use a version of OpenSSL that is FIPS-compliant.
- **Note**: The sample that accompanies this module uses *OpenSSL FIPS 2.0.2*, which is a version of OpenSSL that is validated as compliant with FIPS 140-2. Then, to ensure that JSONStore runs in a FIPS-compliant mode, you must also follow the instructions in this module.

Supported Architectures

- FIPS-compliant JSONStore is supported only on the following architectures for iOS and Android:
  - iOS:
    - armv7
    - i386
  - Android:
    - armv7
    - x86

Note: Although IBM Worklight® and JSONStore supports armv5 for Android, FIPS compliance mode for armv5 is not supported.

Procedure Overview – Android

- Procedure overview:
  - Copy the FIPS-compliant version of OpenSSL to your IBM Worklight application.
  - Replace the necessary IBM Worklight libraries that are used by JSONStore.
  - Implement functions to load the new libraries.
  - Validate that your application is now running in a FIPS-compliant mode.
- You learn the details of this procedure in later sections of this module.

Procedure Overview – iOS

- Procedure overview:
  - Replace the existing framework with a framework that contains the FIPS-compliant version of OpenSSL.
  - Copy the source file that is necessary for build-time fingerprint validation.
  - Add the binary file and script that are necessary to run the build-time fingerprint validation.
  - Validate that your application is now running in a FIPS-compliant mode.
- FIPS requires a build-time validation check. This check is done automatically on Android. For iOS, more steps are necessary for this check.
- You learn the details of this procedure in later sections of this module.

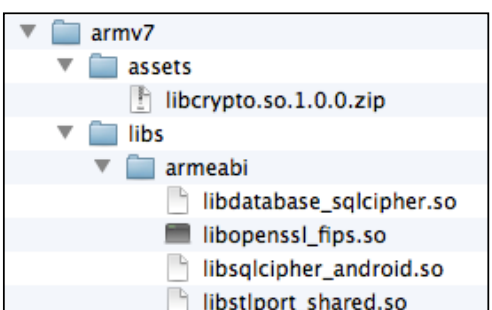
Agenda

- FIPS overview
  - What is FIPS 140-2?
  - JSONStore FIPS compliance
  - Supported Architectures
  - Procedure overview
- Configuration for FIPS on Android
- Configuration for FIPS on iOS
- Enabling FIPS mode in JSONStore
  - Validating FIPS mode

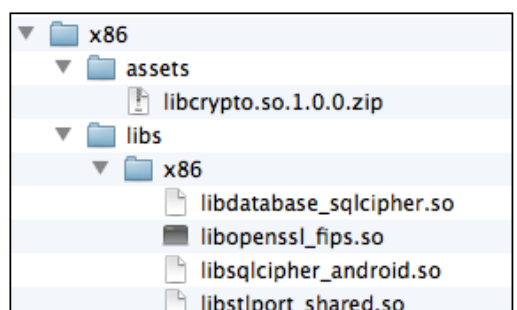
Selecting an architecture

- The necessary files are available in the sample for this module under the **fips-config** folder.
- Both armv7 and x86 are supported for FIPS compliance, however you have to follow the steps for *only* the architecture that you want your application to support.
- This module shows the steps and uses images for armv7. The steps for x86 are identical.

Hierarchy for armv7 in **fips-config/Android**

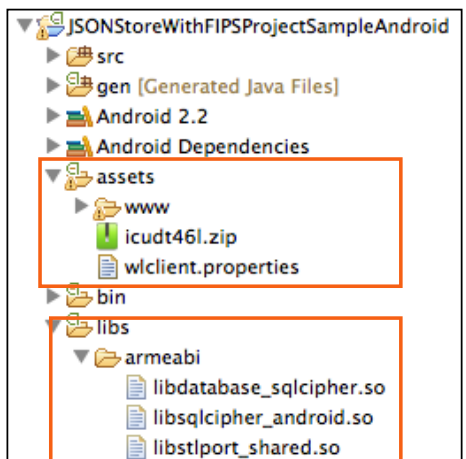


Hierarchy for x86 in **fips-config/Android**



Locating the correct directories

- Import the provided sample project.
- Locate the **assets** folder and the **libs/armeabi** folder of the Android project.



Copy the files

- Copy **fips-config/Android/armv7/assets/libcrypto.so.1.0.0.zip** into the corresponding **assets** folder of your Android project.
- Replace the following library files in your **libs/armeabi** folder with the corresponding files that are in **fips-config/Android/armv7/libs/armeabi**:
  - libdatabase_sqlcipher.so
  - libsqlcipher_android.so
  - libstlport_shared.so
  - libopenssl_fips.so

Add code to load OpenSSL Library

- Locate the **onWLInitCompleted** method in the main source file that is generated with your IBM Worklight Android application.
- Add the following code before the **super.loadUrl(...)** call, as shown here:

```
public void onWLInitCompleted(Bundle savedInstanceState){

    String library = "libcrypto.so.1.0.0";
    try{
            File localStorage = new File(getLocalStorageRoot());
            InputStream pathStream = this.getApplicationContext().getAssets().open(library +
".zip");
            WLUtils.unpack(pathStream, localStorage);
            System.load(super.getLocalStorageRoot() + "/" + library);
    }catch(IOException e){
            // Handle failed loading of files
    }

    super.loadUrl(getWebMainFilePath());
}
```

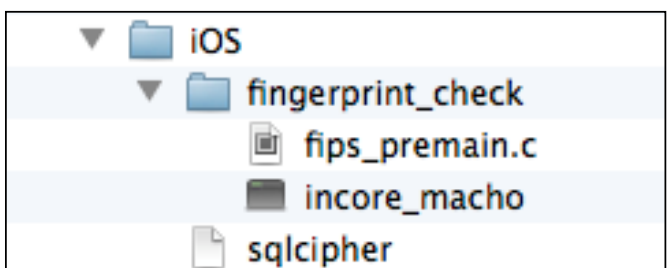
- This step completes the native configurations that are necessary to configure FIPS-compliant OpenSSL on Android.

Agenda

- FIPS overview
  - What is FIPS?
  - JSONStore FIPS compliance
  - Supported Architectures
  - Procedure overview
- Configuration for FIPS on Android
- Configuration for FIPS on iOS
- Enabling FIPS mode in JSONStore
  - Validating FIPS mode

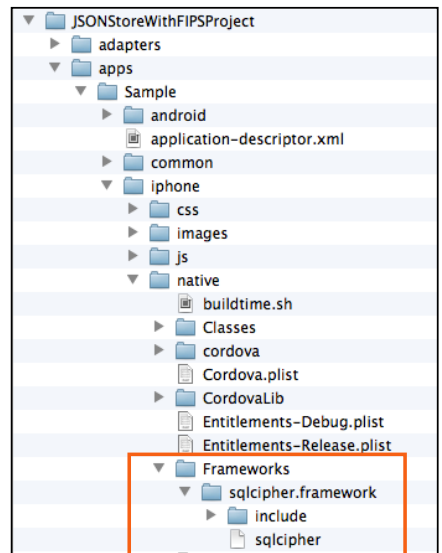
Selecting an architecture

- For iOS, the FIPS-compliant version of OpenSSL for both supported architectures are combined into a single framework file.
  - You do not have to copy files for multiple architectures.



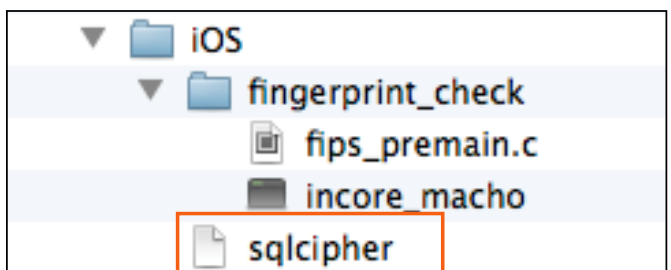
Locating the correct directories

- Import the provided sample project.
- Locate the folder: **{PROJECT_HOME}/apps/{APP_NAME}/iphone/native/Frameworks/sqlcipher.framework**
- The figure shows the location for the provided sample.



Copying the files (1 or 2)

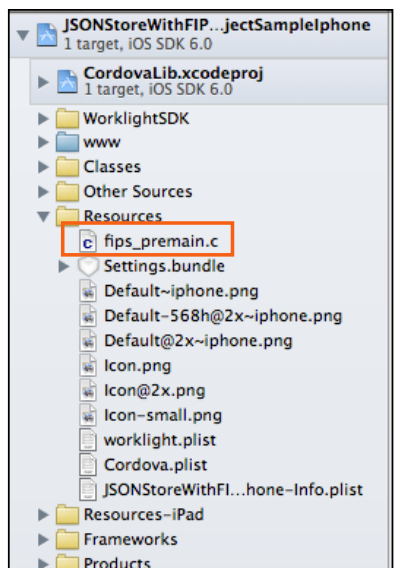
- You must replace only the file that is named **sqlcipher**.
- Replace the existing **sqlcipher** file, as you located it in the previous slide, with the one that is in **config/iOS**.



- Copy the **incore_macho** file to a directory that Xcode can access.
  - Consider copying it in the **/usr/local/bin/** directory.

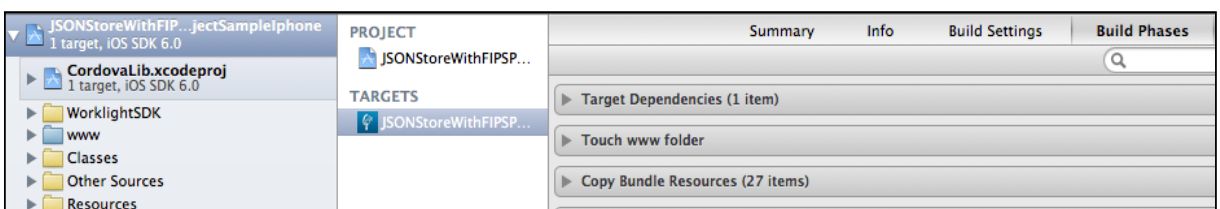
Copying the files (2 of 2)

- Copy the **fips_premain.c** file into your project.
  - Consider copying it in to the **Resources** folder.

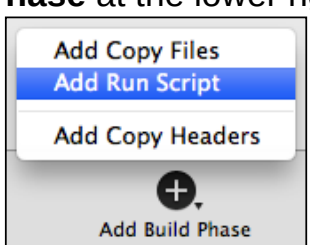


Build-time fingerprint check – Running the script

- Instruct Xcode to run the fingerprint check upon each build:
  - Select the Project and target for your application.
  - Select the **Build Phases** tab.

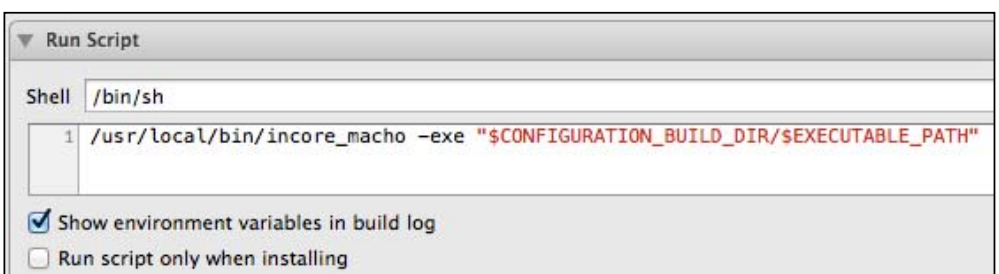


  - Click **Add Build Phase** at the lower right, and then select **Add Run Script**.



Running the fingerprint check script

- In the space that is provided for the script, add the following line:
  - **{INSTALL_PATH}/incore_macho -exe "$CONFIGURATION_BUILD_DIR/$EXECUTABLE_PATH"**
    - *where **{INSTALL_PATH}** is the location where you installed the **incore_macho** file*
- For example, if **{INSTALL_PATH}** is **/usr/local/bin**, the line to add is as shown here:



Agenda

- FIPS overview
  - What is FIPS 140-2?
  - JSONStore FIPS compliance
  - Supported Architectures
  - Procedure overview
- Configuration for FIPS on Android
- Configuration for FIPS on iOS
- Enabling FIPS mode in JSONStore
  - Validating FIPS mode

Enabling FIPS mode in JSONStore

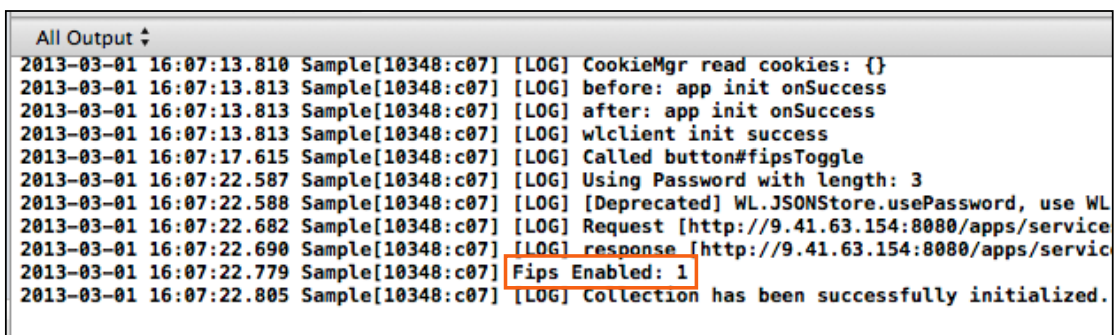
- After you completed the steps in the previous slides, your application can now run by using a FIPS-**capable** version of OpenSSL, meaning that it can now enable or disable FIPS mode for OpenSSL.
- To enable FIPS mode for JSONStore, add the **fipsEnabled** flag with the value **true** to your **initCollection** call:

```
usersCollection = WL.JSONStore.initCollection(
  "users",
  usersSearchFields,
   {
    adapter: usersAdapterOptions,
    fipsEnabled: true,
    onSuccess: initCollectionSuccessCallback,
    onFailure: genericFailureCallback,
    load:true
  })
```

- To ensure that your program is using FIPS-compliant OpenSSL, you **must** pass this flag with a value of **true** for each **initCollection** call that you make.

Verifying FIPS mode

- When you run your project and a call to **initCollection** with the **fipsEnabled** flag set to **true** is done, the standard log (logcat for Android, built-in log for Xcode) displays whether you are running with FIPS mode enabled:



- The trace "**Fips mode: 0**" means that, although the program is running correctly, FIPS mode is not properly enabled. Check to make sure that all files are properly copied to the correct locations.

Check yourself questions

- FIPS mode **cannot** be enabled for the architecture:
  - i386
  - armv5
  - x86
  - armv7
- The name of the flag that is needed to enable FIPS 140-2 in JSONStore is:
  - fipsFlag
  - enhanceSecurity
  - No flag is necessary
  - fipsEnabled
- The purpose of the fingerprint check in iOS is:
  - To let the application know that you are enabling FIPS mode
  - To protect the application from any future security tampering
  - To validate that the FIPS-compliant OpenSSL was not tampered with
  - There is no purpose; it is not necessary

Check yourself questions

- FIPS mode **cannot** be enabled for the architecture:
  - i386
  - armv5
  - x86
  - armv7
- The name of the flag that is needed to enable FIPS 140-2 in JSONStore is:
  - fipsFlag
  - enhanceSecurity
  - No flag is necessary
  - fipsEnabled
- The purpose of the fingerprint check in iOS is:
  - To let the application know that you are enabling FIPS mode
  - To protect the application from any future security tampering
  - To validate that the FIPS-compliant OpenSSL was not tampered with
  - There is no purpose; it is not necessary.

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/en/us sections entitled "Cookies, Web Beacons and Other Technologies" and "Software Products and Software-as-a-Service".

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 forums at:
    - https://www.ibm.com/developerworks/mobile/mobileforum.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