Application Authenticity Protection

Overview

By issuing an HTTP request, any entity can access the HTTP services (APIs) that IBM MobileFirst Platform Foundation Server offers.
The Application Authenticity Protection feature ensures that an application that tries to connect to a MobileFirst Server instance is the authentic one and was not tampered with or modified by a third-party attacker.

TODO: Add information about the Security Check

Application Authenticity Protection is available for:

- Cordova applications (iOS, Android, Windows 8, Windows 10)
- Native applications (iOS, Android, Windows 8, Windows 10)

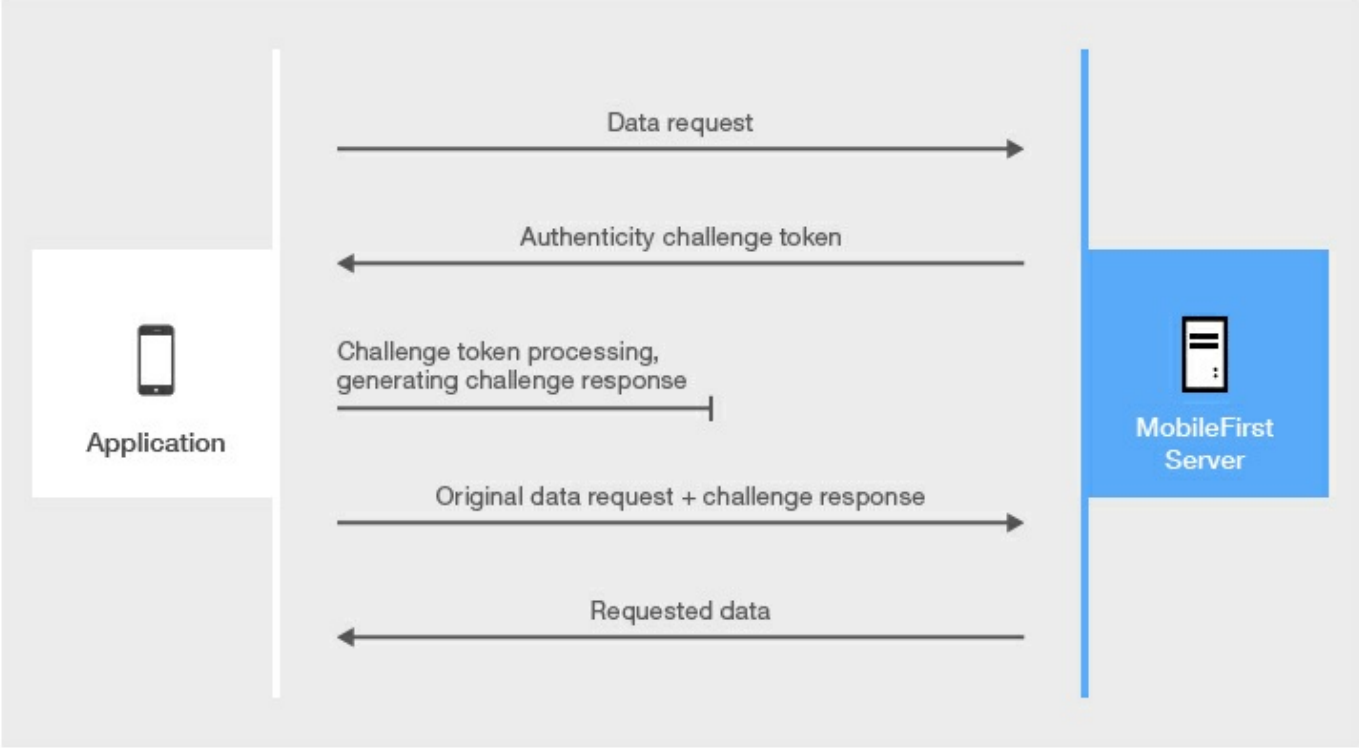
> **Note:** Application Authenticity Protection is **not available** in the MobileFirst Development Server. To test, follow the below instructions in a remote application server, such as a QA, UAT or Production server.

Jump to:

Authenticity Flow

Application Authenticity Protection is based on certificate keys that are used to sign the application bundles. Only the developer or the enterprise who have the original private key that was used to create the application are able to modify, repackage, and re-sign the bundle.

TODO: Verify correctness of diagram



> The challenge token in the diagram is processed by compiled native code, so that third-party attackers cannot see the logic of this processing.

Enabling Application Authenticity Protection

In order to enable Application Authenticity Protection for your Cordova or Native application, the application's binary file needs to be signed using the MobileFirst-supplied command line tool. Eligible binary files are: `ipa` for iOS, `apk` for Android and `appx` for Windows 8 Universal & Windows 10 UWP.

1. Open **Terminal** and run the command: `java -jar path-to-mfp-server-authenticity-tool.jar path-to-binary-file`

   For example:

   ```
   java -jar /Users/idanadar/Desktop/mfp-server-authenticity-tool.jar /Users/idanadar/Desktop/MyBankApp.ipa
   ```

   The result of the command above is a `.data` file generated next to the `MyBankApp.ipa` file called `MyBankApp.appAuthenticity.data`.

2. Open the MobileFirst Operations Console in your browser of choice.
3. Select your application from the left-side pane and click on the Authenticiy menu item.
4. Click on "Upload File" to upload the `.data` file.

After uploading the `.data` file Application Authenticity Protection will be enabled for the application.

TODO: add image of where to upload .properties file

Disabling Authenticity

In order to disable Application Authenticity Protection, remove the previously uploaded `.data` file.

TODO: add image of where to remove .properties file

Configuring Authenticity

Application Authenticity Protection has two available properties:

TODO: add missing property description

- `expirationInSec`:
- `inactivityTimeoutInSec`:

To configure these properties, in the MobileFirst Operations Console navigate to the ... screen.

TODO: add image of where to edit the properties