

Receipt Validation Programming Guide



Developer

Smartflash - Exhibit 2013

Apple v. Smartflash

CBM2014-00112

Contents

About Receipt Validation 5

At a Glance 5

Validating Receipts Locally 5

Validating Receipts With the App Store 5

Validating Receipts Locally 6

Locate and Parse the Receipt 6

Compute the Hash of the GUID 8

Validate the Receipt 9

Respond to Receipt Validation Failure 9

Exit If Validation Fails in OS X 10

Refresh the Receipt If Validation Fails in iOS 10

Set a Minimum System Version for Mac Apps 10

Don't Localize Your Version Number 10

Protect Your Validation Check 10

Test During the Development Process 11

Validate In-App Purchases 11

Implementation Tips 13

Get the GUID in OS X 13

Parse the Receipt and Verify Its Signature 15

Validating Receipts With the App Store 19

Verifying an App Receipt 19

Verifying an Auto-Renewable Subscription Receipt 20

Receipt Fields 22

App Receipt Fields 22

Bundle Identifier 22

App Version 22

Opaque Value 23

SHA-1 Hash 23

In-App Purchase Receipt 23

Original Application Version 23

Receipt Expiration Date 24

In-App Purchase Receipt Fields	24
Quantity	24
Product Identifier	25
Transaction Identifier	25
Original Transaction Identifier	25
Purchase Date	26
Original Purchase Date	26
Subscription Expiration Date	26
Cancellation Date	27
App Item ID	27
External Version Identifier	27
Web Order Line Item ID	28
 Document Revision History	 29

Figures, Tables, and Listings

Validating Receipts Locally 6

- Figure 1-1 Structure of a receipt 7
- Listing 1-1 ASN.1 definition of the payload format 8
- Listing 1-2 ASN.1 definition of the in-app purchase receipt format 12
- Listing 1-3 Get the computer's GUID 13
- Listing 1-4 Verify the signature using OpenSSL 15
- Listing 1-5 Parse the payload using asn1c 16
- Listing 1-6 Extract the receipt attributes 17
- Listing 1-7 Compute the hash of the GUID 17

Validating Receipts With the App Store 19

- Table 2-1 Status codes for auto-renewable subscriptions 21

About Receipt Validation

Note: This book was previously titled *Validating Mac App Store Receipts*.

The receipt for an application or in-app purchase is a record of the sale of the application and of any in-app purchases made from within the application. You can add receipt validation code to your application to prevent unauthorized copies of your application from running. Refer to the license agreement and the review guidelines for specific information about what your application may and may not do to implement copy protection.

Receipt validation requires an understanding of cryptography and a variety of secure coding techniques. It's important that you employ a solution that is unique to your application.

At a Glance

There are two ways to validate receipts: locally and with the App Store. Compare both approaches and determine which is a better fit for your app and your infrastructure. You can also choose to implement both approaches.

Validating Receipts Locally

Validating locally requires code to read and validate a PKCS #7 signature, and code to parse and validate the signed payload.

Relevant Chapters: [“Validating Receipts Locally”](#) (page 6), [“Receipt Fields”](#) (page 22)

Validating Receipts With the App Store

Validating with the App Store requires a secure connection between your app and your server, and code on your server to validate the receipt with the App Store.

Relevant Chapters: [“Validating Receipts With the App Store”](#) (page 19), [“Receipt Fields”](#) (page 22)

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.