



Whole Home Sign In (a.k.a. Silent Sign In)

Version 1.3

13th June 2023

Table of Contents

1	Purpose of this document.....	3
2	Technical Implementation	3
2.1	Overview	3
2.2	Whole Home Sign In authentication materials (authRefreshToken)	3
2.3	subscriptionToken Format	4
2.3.1	subscriptionToken JWT header	4
2.3.2	subscriptionToken JWT payload.....	4
2.4	Use of Firebolt's SecureStorage module	4
2.4.1	authRefreshToken	4
2.4.2	subscriptionToken	4
2.5	Partner application Sequence Flows.....	5
2.5.1	Non Apps Marketplace Application	5
2.5.2	Apps Marketplace Application	6
	Appendix A: Example subscriptionToken.....	7



1 Purpose of this document

This document outlines the technical solution that Partners need to implement within their application in order to support Whole Home Sign In.

2 Technical Implementation

2.1 Overview

The technical solution for implementing the Whole Home Sign In functionality is based around the Firebolt SecureStorage module. It allows a Partner application to securely store/update/delete a data object and share it between all Sky devices with the Sky Household. This data object contains the authentication materials required by the application to automatically sign in the user into the application and is referred to as the authRefreshToken.

When a user launches the Partner application, which does not currently have a logged in user, the Partner application will check to see if the authRefreshToken is available. If it is, the Partner application will use this authRefreshToken to sign the user in. If it is not available, the normal sign in process will take place, after which the Partner application will store the Whole Home Sign In authentication materials within the authRefreshToken, for use on other devices within the household.

If the user logs out of the Partner application, it shall delete the authRefreshToken.

If a Partner application operates within Sky's Apps Market Place, an additional token is made available to the app which contains the MarketOne partnerSubscriptionId value via a subscriptionToken. This enables Silent Sign In on the first usage of the app on any device within the home, by means of matching the household subscription to the user's partner application account. Subsequently, the application can store the authentication materials within the authRefreshToken, to enable whole home sign-in on other devices within the household.

2.2 Whole Home Sign In authentication materials (authRefreshToken)

Sky does not mandate any specific format or approach to what authentication materials are stored to enable the Partner application to automatically sign in the user. However, we do issue the following guidelines:

- The materials are long lived
- The materials do not contain sensitive data
- The materials can be used to retrieve shorter lived bearer tokens used by the Application
- The materials can be invalidated server side by the Partner applications back office
- The materials are limited in scope to devices operated by Sky

2.3 subscriptionToken Format

The subscriptionToken will be pre-seeded into the Secure Storage when a user subscribes to the partner application via Sky's Apps Marketplace. It will be in the form of a signed JSON Web Token (JWT) as defined below. See Appendix A for an example.

2.3.1 subscriptionToken JWT header

Name	Value
"alg"	"RS256"
"typ"	"JWT"

2.3.2 subscriptionToken JWT payload

Name	Value
"iss"	"Sky"
"appld"	"<Application Identifier>"
"pSubId"	"<Market One PartnerSubscriptionId>"

2.4 Use of Firebolt's SecureStorage module

Sky mandates that the Partner application SHALL use the following values for the parameters of the Firebolt's SecureStorage APIs, when using them for Whole Home Sign In.

2.4.1 authRefreshToken

Parameter	Value
scope	"account"
key	"authRefreshToken"

2.4.2 subscriptionToken

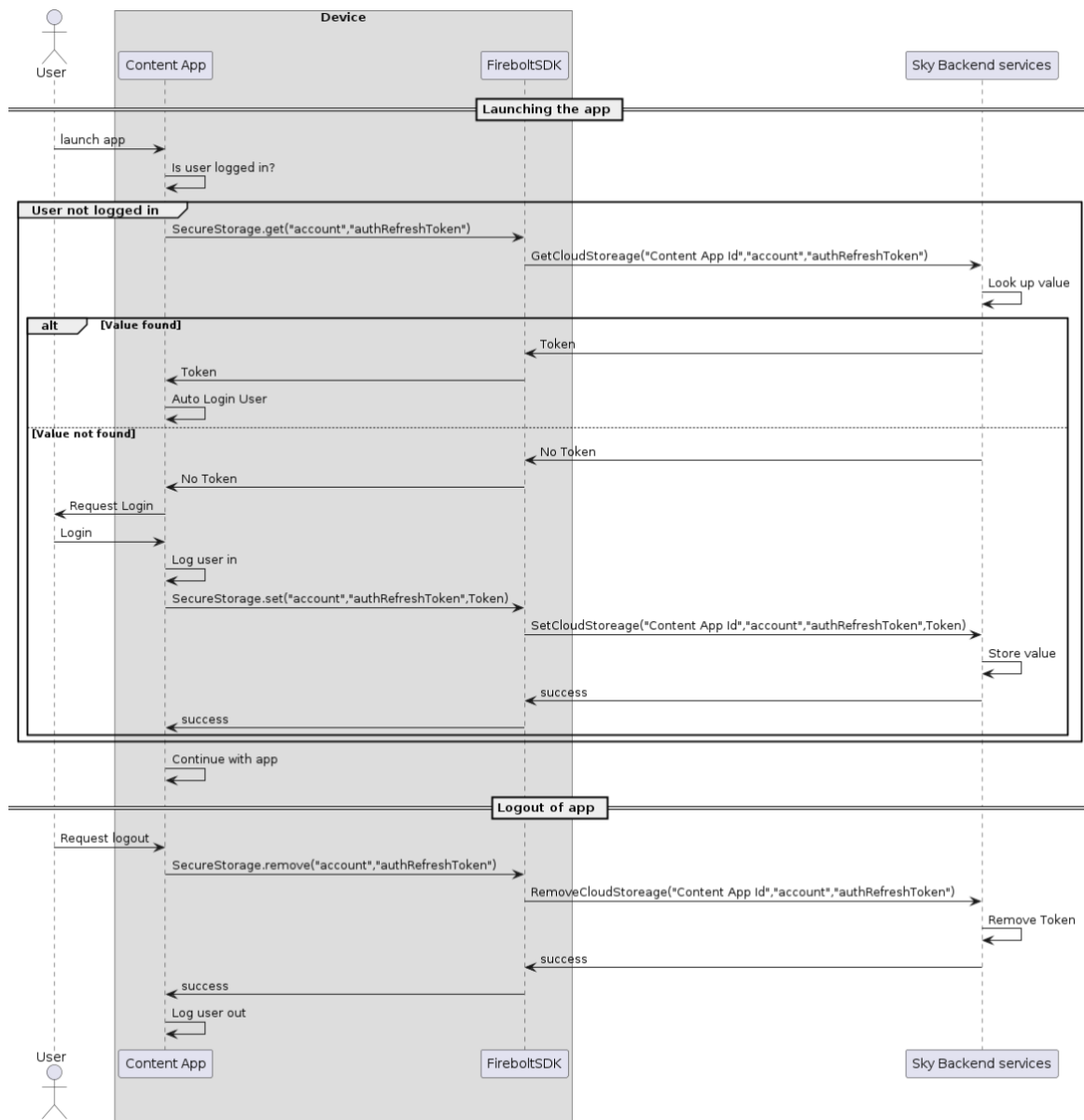
Parameter	Value
scope	"account"
key	"subscriptionToken"



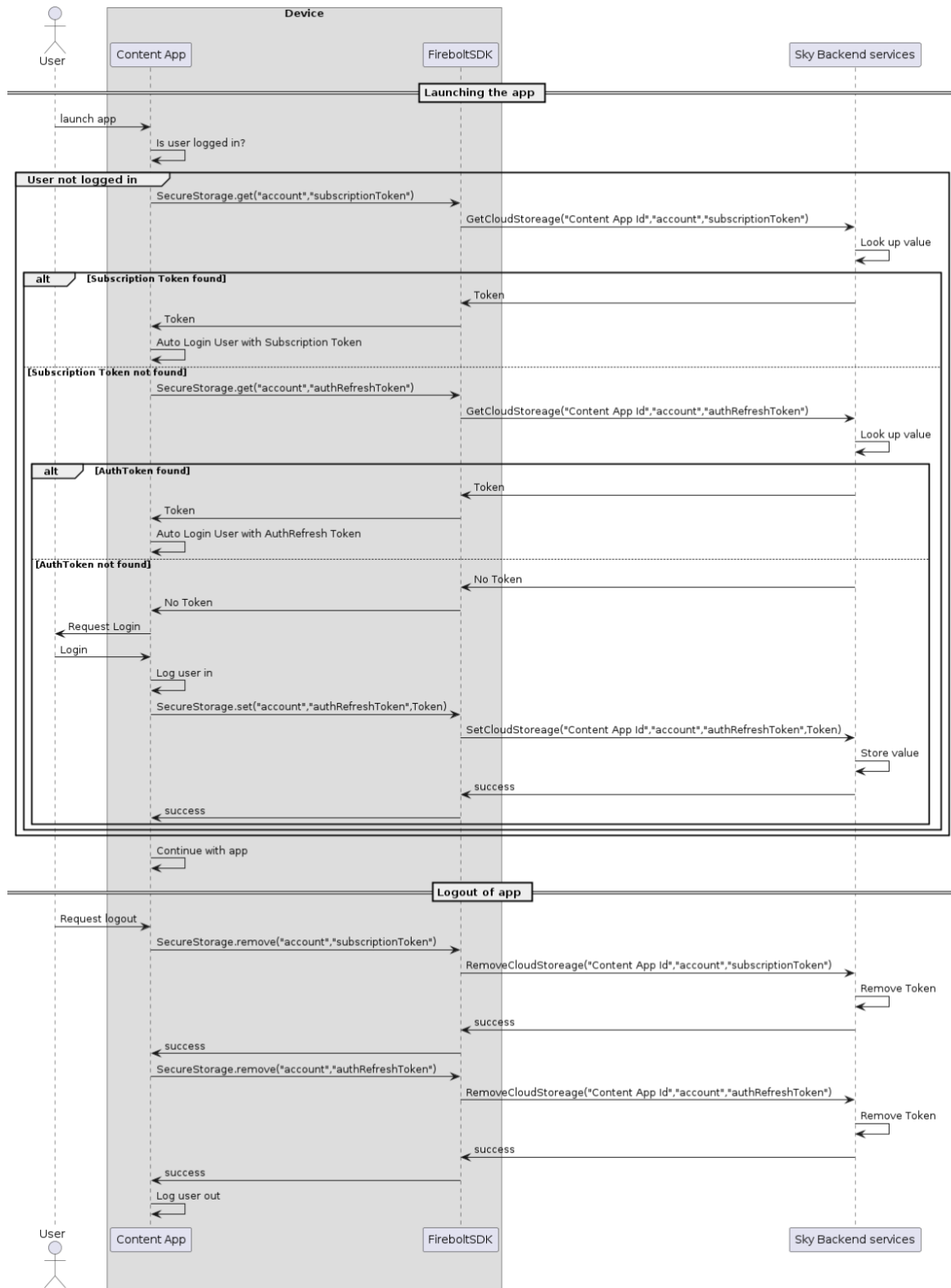
2.5 Partner application Sequence Flows

The following sequence diagram shows how the Partner application SHALL make use of the Firebolt SecureStorage module to implement Whole Home Sign In.

2.5.1 Non Apps Marketplace Application



2.5.2 Apps Marketplace Application



Appendix A: Example subscriptionToken

Given the follow header and payload JSON values of the token:

Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

Payload

```
{
  "iss": "Sky",
  "appId": "GreatVideoApp",
  "pSubId": "d0ae3e15-e8f3-4896-b382-f7e8d7d72849"
}
```

Using a sample RSA key pair, the signed JWT created is:

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJTa3kiLCJhcHBzI6Ikd5ZWVmlkZW9BcHAiLCJwU3ViS
WQiOiJkMGFIM2UxNS1IOGYzLTQ4OTYtYjM4Mi1mN2U4ZDdkNzI4NDkifQ.xVXFxE7o3trUR8OSIPikK99f6C_iL
ChjIGWulphihOp6z3ZLaFCMusL2WkWY3H06BY-AWeyYLIL4aQU_xCJMxoF40dwwHRmt-
qoBfoiuVf5qa67XsHASSVwtLKZigyXN3rUtpNrnEHdQnI2b4nDSNFCWq70L1Hli1nYHhxOAmZzIzS-
tjCLThSCxSdB0wOFCOV-
hXHulXZhCM9MnOS3uYP8PVSHnIBasJMkYyAuZhSsE8MTFj6MxfslTEgezrgbieLgkAkZF0h45zOU7ZsUAsyu6JS
U5CZgUvQMzP4hGmxAWUPc8LTMpT5h_NWaLxKRuhlcQCOE6UDrYERkZ9Zw
```

This token can be validated using the following sample RSA public key

-----BEGIN PUBLIC KEY-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyoCWNdOtD2ZMHMZ8r/Rs
rxSpZ20YuWRlaFO/tpiJMfoda1x5CgGtNm1iK2nYpVAbo54P/3D5ptFbzVb0ZJkx
CxNDoMqh4o8hDjeKVZ9Nas2BtXONMFfi+sW2dzUDhrpo1F3/mHDlc67BWwh+CecC
o4clzfGxCmAihQsIQJ+pwKp7n+iCk7kdonOGqGGd8DFiEr1SeZNRXU8lZ5tmyXLf
q1tBv1EAY4QBQq16YNS3ZnP+jPOASnsVlIME+rklBKqkvKxfX7yDRgAkINXnm/L
PR5JBbPQKwTt492G3YHPqE1MoiKUpSLnxK+dBALEZ68Zx7wfJhj16ln7sYNegBu+
dwIDAQAB
```

-----END PUBLIC KEY-----

Note: This is just a sample public key and not the key that will be used in the live environment

