cBRAIN™

F2 Security Description

F2 Touch and F2 Manager

Updated: April 2021

Responsible: Norman Schreiber

Table of contents

Introduction

In the following document we provide a technical introduction to F2 Touch and F2 Manager. The document will especially focus on the transport of data, how the applications communicate with the database server and if there is a possibility to store data, how the storage is supported.

For functional information please see the user handbooks for both applications.

Questions and comments to this documentation may be addressed to:

Norman Schreiber: nos@cbrain.com
Product Manager - cBrain Germany

HTTPS encrypted Communication between F2 applications and database

Find below the traditional setup of server infrastructure and how the mobile applications communicate with the database server via the mobile server.

Technical setup and infrastructure

In the technical setup the customer will normally ensure that communication between clients and mobile devices are and the F2 Database is encrypted via HTTPS.

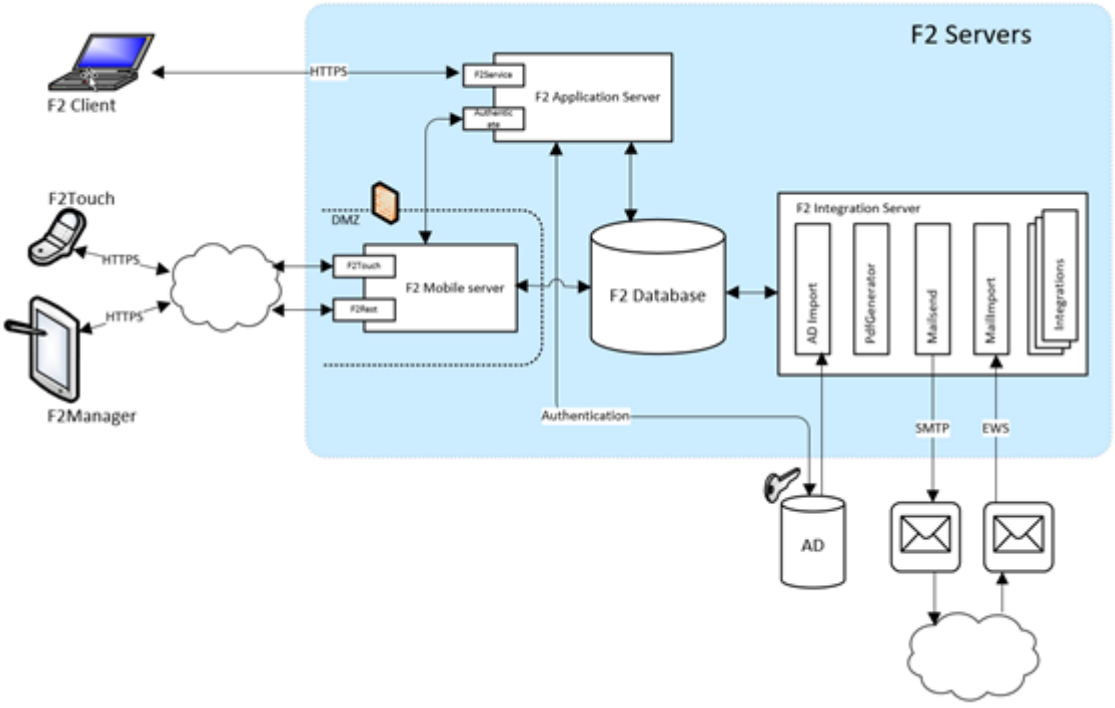

Figure 1: F2 Standard-systems architecture

Push notifications

The server can handle notifications via a central service. From this service the information is transferred to either the Android or iOS device.

Notifications are marked in the "counter" on the F2 Touch icon, so the user can see, how many unread items exist and the notification transfers contains a small part of the text for the user to review in his notification center.

The push notifications are sent via Firebase.

Authentication is done against Firebase using a private key file included with the PushService.

To send notifications to MDM apps, we will need:

- Bundle-ID for the apps
- An APNs Authentication Key.

If an authentication key is not available, we can use an APNs certificate instead, but it will need to be renewed once a year.

Alternatively, customers can choose to set up a Firebase project themselves and add their apps. In that case, we will need a private key-file for the Firebase project, which can be downloaded from the "Service accounts" tab in the Firebase console.

Via configuration the content of the notification can either be very limited e.g. you have a chat, you have a mail, you have an approval. Or the content can be rich with information e.g. "From Norman Schreiber. Hello Robert, can we meet on Wednesday. We…".

F2 Touch - Technical specifications

F2 Touch consists of 2 products. The F2 web-application which is an HTML5 application on the one hand. And F2 Touch which is designed to support handling F2 from mobile either Android or iOS based devices.

The web application runs on various browsers. When using a browser, the application will not store data on the device.

To use the F2 Touch optimized for mobile use, the user can download the F2 Touch application via Apple App Store or Google Play Store. After successful download, the user will have to add a server URL and login with his login code as part of the application's setup.

The mobile Touch application wraps the F2 Web application thus provides the same functionality and some extra features.

The extra features are e.g., the possibility to swipe, the possibility to have notifications, and the possibility to work offline.

F2 Touch and data on the device

With F2 Touch on the mobile device, the mobile application can store data on the devices. The purpose of the data storage is to allow the user to work on selected data in the inbox when working from locations with not effective or not existing network.

The user can perform several actions on the data like answer a chat or mail, delete and archive. These actions are piled up in an action list which then is performed when the device has access to the network again.

Data is transferred and synchronized to F2 Touch. The database is based on iOS's most secure fileclass *NSFileProtectionComplete for all data on the device*. And when the device is secured with access login on the data, the device will be AES256-encrypted.

F2 Manager - Technical specifications

F2 Manger is a native X-Code application designed to support top management, like ministers, by handling meeting materials and approvals.

In relation to meeting material, the standard is that the material will only be present on the iPad for a predefined period. This period is configurable in the F2 Desktop client.

In relation to approval material, the standard is that the material for approval only is present, until the approval is conducted. Please notice that a setting exists, where specific users can have access to their approval history also for a specific and configurable period.

F2 Manager and data on the device

Data is transferred and synchronized to F2 Manger. The database is based on IOS most secure fileclass *NSFileProtectionComplete for all data on the device*. And when the device is secured with access login on the data, the device will be AES256-encrypted.