LoChat

Backend Documentation

Authentication Proccess

Domenik Irrgang
February 15, 2018

Summary

This document is written to describe the authentication process on the backend using the frontend. It is supposed to give a general overview of the process itself, but how it affects the requests send after the authentication has been completed. It is going to describe which step is taken with its reasoning.

Contents

List of figures **i**

1 Introduction **1**

2 Workflow **2**

2.1 First Time Authorization 2

2.2 Changing Device 2

2.3 Using Device with no SIM card 2

3 Details **3**

3.1 Request Verification Code 3

3.2 Send SMS with Verification Code 4

3.3 Request Private Key 4

3.4 Requesting a Resource 4

List of Figures

1 Activation of Device 3
2 Valid request 4
3 Invalid Request 5

1 Introduction

To be able to control who is accessing which resource on the backend, some form of authentication needs to be in place. This authentication should be a once time setup for the user and should only be worried with again if the user is switching his device. Authentication on multiple devices at the same time shall not be possible.

2 Workflow

This section is going to describe how the authentication process in the users point of view takes place.

2.1 First Time Authorization

The user has just downloaded the application on his device and is now asked to enter some personal information (gender, year of birth). Once that is done he clicks the register button. He now receives a SMS on his device and is prompted to enter the code in the SMS to the application (will be processed automatically by the application if the application has the rights to read SMS). Now is authorized and can use the application.

2.2 Changing Device

When changing the device the same process of the "First Time Authorization" is done with the difference that the user does not need to enter the personal information anymore and instead skips that, because he already has an existing account.

2.3 Using Device with no SIM card

If now SIM card is present during the authorization process, the application will ask for a phone number. As the SMS can not be received on that device the code contained in the SMS needs to be entered manually and will be received on the device with the SIM card of the given phone number.

3 Details

This section is going to describe how the authentication process takes place in detail. The picture below gives a general overview of the process. Each step of the diagram is getting described in detail.

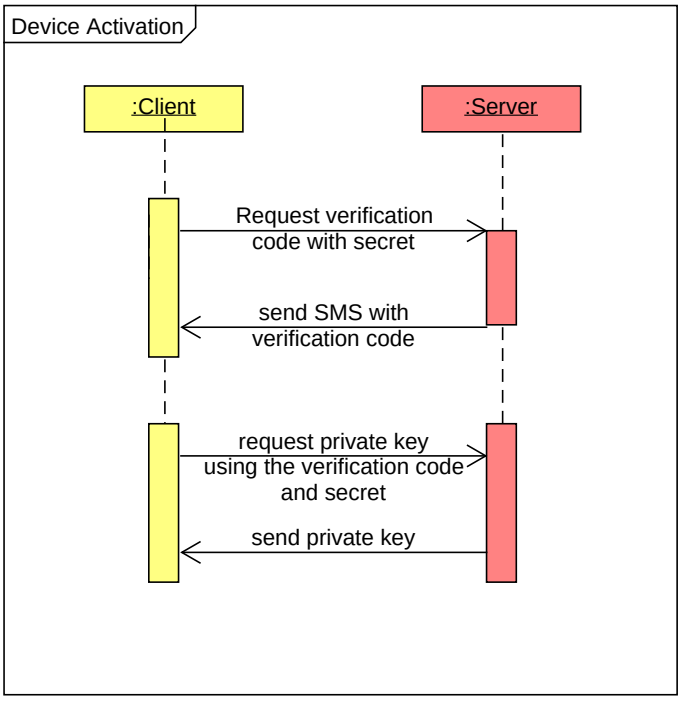

Figure 1: Activation of Device

3.1 Request Verification Code

In this step the request to receive a SMS with the verification code is send. The request contains the personal information of the user, the phone number and a secret. If it is not the first time for the user to use this phone number, no personal information needs to be send. The secret is simply a randomly generated 32 characters long string. The use for this string is explained in a later part. In the database a new user is created or updated with the newly given information (phone number, personal information and secret).

3.2 Send SMS with Verification Code

Once the backend has processed the previous request, a SMS is send to the given phone number containing a randomly generated six digit number. This number is then stored with a reference to the user in the database.

3.3 Request Private Key

A new request is send to the backend containing the six digit verification code and the secret from the first step. Here the secret becomes important. A attacker could have intercepted the SMS and could now validate his device with the verification code, but because he does not know the secret from the first step he can not complete this step. When the verification code request is send SSL encryption is used so the secret can not be read.
If the verification code and the secret are the same as in the database this step sends back a private key. This key is then used by the user to make any requests to any resource to the backend and needs to be locally encrypted and stored on the device.

3.4 Requesting a Resource

If any resource is requested the private key needs to be provided in the request header in the "X-Auth-Token" field. If the key is missing a response with the code 403 is send.

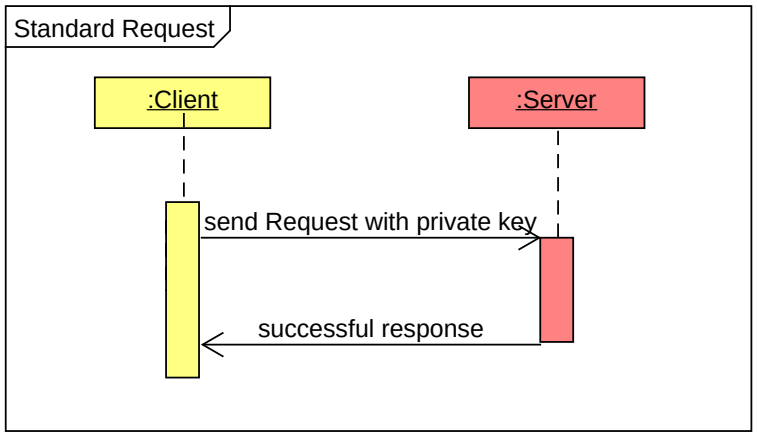

Figure 2: Valid request

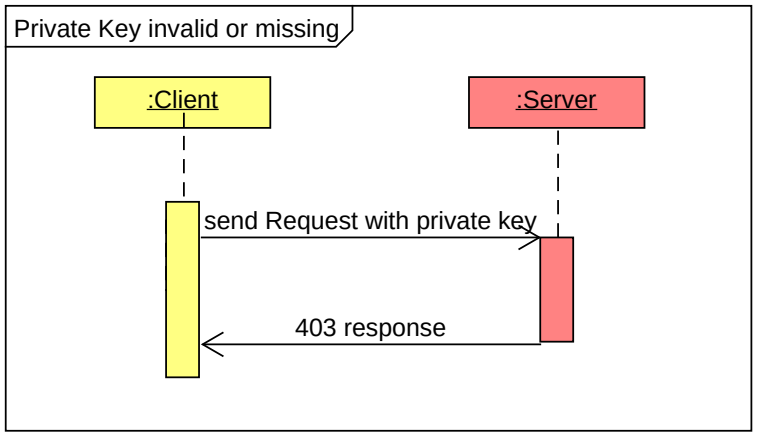

Figure 3: Invalid Request