CSL (Client Side Logging) Phase I – Requirements Document

**Version**: 0.4

**Authors**: Dmitry Kudryavtsev, Alex Arkhipov

# Contents

[1. Contents 2](#_Toc433647869)

[2. Revision history 3](#_Toc433647870)

[3. Purpose of this document 4](#_Toc433647871)

[4. Requirements 5](#_Toc433647872)

[4.1 CSL-REQ1 Mobile Application requirements 5](#_Toc433647873)

[4.1.1 CSL-REQ1.1 Login to log storage server 5](#_Toc433647874)

[4.1.2 CSL-REQ1.2 Feature enable/disable in Mobile app 5](#_Toc433647875)

[4.1.3 CSL-REQ1.3 Sending logs to server 5](#_Toc433647876)

[4.1.4 CSL-REQ1.4 Mobile application local log and event storage 5](#_Toc433647877)

[4.1.5 CSL-REQ1.4 Log and event upload failure 5](#_Toc433647878)

[4.1.6 CSL-REQ1.4 Log and event local storage rotation 5](#_Toc433647879)

[4.2 CSL-REQ2 Database requirements 5](#_Toc433647880)

[4.2.1 Scalability 5](#_Toc433647881)

[4.2.2 Capacity 5](#_Toc433647882)

[4.2.3 Data storage maintenance 6](#_Toc433647883)

[4.2.4 CSL-REQ3 Handling errors 6](#_Toc433647884)

[4.3 CSL-REQ2 Data transmission requirements 6](#_Toc433647885)

[4.3.1 CSL-REQ3 Secure data transfer 6](#_Toc433647886)

[4.3.2 CSL-REQ3 Data compression 6](#_Toc433647887)

[5. Open Questions 7](#_Toc433647888)

[5.4 Log server name 7](#_Toc433647889)

[5.5 Log storage server capacity 7](#_Toc433647890)

[6. Limitations 7](#_Toc433647891)

[6.1 Authorization limitation 7](#_Toc433647892)

# Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Summary of changes** |
| 0.1 | 16/10/2015 | Dmitry Kudryavtsev | First draft |

0.2 16/10/2015 Dmitry Kudryavtsev Internal review

0.3 20/10/2015 Dmitry Kudryavtsev, Alex Arkhipov Modification after review

0.4 23/10/2015 Dmitry Kudryavtsev, Alex Arkhipov Changes on external review

# Purpose of this document

This document describes the requirements for the Client Side Logging feature. It also covers limitation and open questions topics.

# Requirements

## CSL-REQ1 Mobile Application requirements

### CSL-REQ1.1 Login to log storage server

There should be simple authentication mechanism implemented on both mobile and server sides to authenticate to log storage server during sending logs and events. Logs and Events can be stored in MongoDB only if authentication is successful. See limitation section.

### CSL-REQ1.2 Feature enable/disable in Mobile app

The user will not be able to to enable/disable feature in Mobile app. However, the enable/disable functionality should be implemented as part of mobile application development and saved in mobile application settings.

### CSL-REQ1.3 Sending logs to server

Mobile application must be able to send logs and events to server and server stores them in MongoDB.

### CSL-REQ1.4 Mobile application local log and event storage

Mobile application must implement local storage of logs and events. Every 10 minutes or when there are 1Mb of local storage space is occupied mobile application connects to the log storage server and uploads all information from local storage to log storage server.

### CSL-REQ1.4 Log and event upload failure

If there are any issues with uploading logs and events to backend server (no internet connection, log storage server error, etc…), application must keep all logs and events data locally with ability to send them, when connection is reestablished.

### CSL-REQ1.4 Log and event local storage rotation

If logs or events in the local mobile storage are occupied 1Mb (and log storage server is not available for writing) there must be a rotation mechanism that deletes oldest logs and events and writes new ones.

## CSL-REQ2 Database requirements

### Scalability

The solution should provide the way to extend number of logs saved in MongoDB by adding new servers/disks.

### Capacity

Standard HW server with 10Tb of disk space must provide the ability to store data from all OOMA users for at least 1 month (the longer the better).

### Data storage maintenance

There must be a limitation of days, how long mongoDB stores data. It depends on capacity and user activity. When mongoDB disk free space becomes less than 20%, monitoring tool (script) will delete one week of oldest data

### CSL-REQ3 Handling errors

If application crashes while loading log data to log storage server it must perform a recovery check to avoid data duplication on server

## CSL-REQ2 Data transmission requirements

### CSL-REQ3 Secure data transfer

Log storage server must provide HTTPS access only.

### CSL-REQ3 Data compression

GZIP compression must be implemented for HTTPS data transmission to save mobile traffic.

# Open Questions

## Log server name

Need to define name since it will be hardcoded in mobile application

## Log storage server capacity

Capacity of MongoDB is based on average activity of mobile application users.

For approximate calculation following parameters are used:

Number of active users = 90 000

Average size of 1 event/log = 500 bytes

Average number of events per month for one user = 150 (about 5 calls per month)

1. For events :

Number of events per month for ONE user = 150

Number of events per month for ALL user = 150 \* 90 000 = 13 500 000

1. For logs (no exact data here – need to measure during application testing)

Average size of LOGs per User for ONE month is about 10 Mb

Each month it will take: 90 000 \* 10 / 1024 = 900 Gb of Log DATA per month

Based on this calculation there will be **900** Gb of DATA per month

# Limitations

## Authorization limitation

Since there is no access to production servers planned for Log Storage server it will be impossible to implement authorization and authentication functionality. It will be very painful for the user to maintain separate username/password specifically for logging feature. That is way it was decided to implement simple but unreliable authorization method. Due to this attacker can potentially know this method and be able to send fake logs and events to log server. The risk is understood and accepted. More information about authorization method is available in design documentation.