**Design Document of ABE-based ABAC Demo**

**(For NRL Project)**

Zian Zhang, Qiuxiang Dong, and Dijiang Huang

**Version:** 1.0

**Date:** 01/30/2020

**Design Overview**

The project is going to convert Attribute-Based implementation scheme which are written in python code into java file so that attribute-Based implementation can be ran in Android platform. The main task of this design will be conversion of the setup of Attribute-Based scheme. There are seven python files which are used to setup Attribute-Based scheme. The original python files use Charm-Crypto library. After conversion of the code, the application will be developed by using Android Studio.

1. Convert the python’s files
2. Develop Android Application (Android Studio)
3. (Optional) Might use other crypto libraries as

**Background Information**

While using this application, the user requests an attribute certificate and pass it to key generation center. The key generation center will verify and pass private key back to the application. The application will use Attributed-Based implementation scheme to protect user data.

If the user wants to store a file, the user needs to encrypt the file and upload to a file system (etc. IPFS). Then the application will use Attributed-Based scheme to encrypt the hash value which is generated by the file system, and the password which is generated by the user. The application will upload the encrypted file to a blockchain system. Also, the application is able to decrypt the file from blockchain system by using private key.

**The process of design**

1. Convert IDABE.py into some java files

**Estimated time:** 7 days **Expected finished time:** TBA

1. Convert gp\_setup.py and ferderated\_setup.py

**Estimated time:** 2 days **Expected finished time:** TBA

1. Convert federated\_keygen.py

**Estimated time:** 3 days  **Expected finished time:** TBA

1. Convert internal\_delegation.py

**Estimated time:** 3 days **Expected finished time:** TBA

1. Convert external\_delegate.py

**Estimated time:** 3 days **Expected finished time:** TBA

1. Develop Android application(Android Studio)

**Estimated time:** 15 days **Expected finished time:** TBA

1. (Optional)Use other library or figure out another way if Charm library cannot support Android platform

**Estimated time:** 15 days **Expected finished time:** TBA

**Future Development(Optional)**

To be decided in the process of the design.

**Tentative Software Architecture**

