PublicKeyInfrastructure - Design Document

Lior Ashkenazi | 315533059

June 11, 2022

1 Preface

This project consist of Public Key Infrastructure, PKI, where a user can generate entities in this ecosystem of the following types:

- Root Certificate Authority Entity - a CA which signs it self, has no predecessor.
- Certificate Authority Entity - an intermediate entity which is a CA but signed by another Root CA / Intermediate CA.
- Certificate Entity - an intermediate entity, which is not a CA, therefore it is not authorised to sign other entities.

Moreover, there is a Validation Authority, which more details on it will be shown next.
Now, we describe next the modules of the project.

2 Certification

Responsible for certificates generation, caching and validation, where the pythonic module pyOpenSSL, using SSL/TLS technology, is used and is in fact the base of the entire project where is wrapped by this module. Therefore, all the basic technologies and certificates are real-life certificates and objects. Moreover, generation under this module involves generating cryptographic tools for signing and validating certificates, which are X509 certificates under SSL. Furthermore, CRL system is also implemented, where each CA has a CRL. Finally, The caching system is also part of this module, where it is necessitated because of the SSL Networking module, where communication under SSL.

3 Entities

Incoporates the generation of "Entities" with all sorts of authorised levels and responsible for linking this generation to an actual generation of certificates, meaning that every entity has a real certificate and the relevant cryptographic objects. Also, it responsbile for the communication between entities, which is done safely, thanks to the Validation Authority. This entity is distinct and uniqe. Through this entity, before communicating with another entity, every entity can request validation of the other entity. In particular, revocation mechanism is implemented, as requested, in this module. Therefore, any authorised entity can revoke an entity which is issued, and only an issued entity. The VA thus can validate that an entity is not revoked and it is safe for communication. Finally, all of those operations is done by “controller.py” file which operates the entire entities ecosystem and virtually operates the entire project. Any action involving entities goes through this file.

4 SSL Networking

Network infrastrucure used for communication between entities. Entities in this version of the project can communicate with each other through text. The protocol of the network is TCP wrapped by SSL network for safety reasons. Before communication, entities has to validate their addressee.

5 Instructions

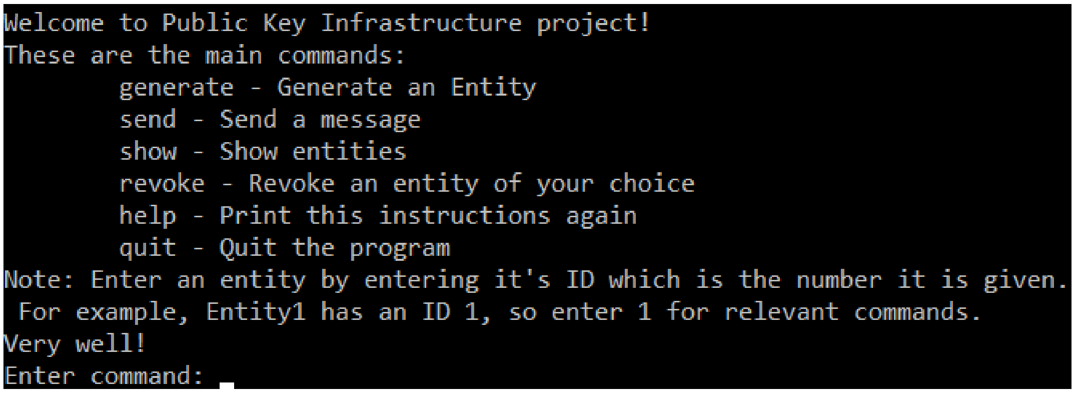
For activating the program, please create a python virtual environment in the program’s folder. Then, install the requirements by entering the following command in a terminal open in the project’s folder:

```
pip install −r requirements.txt
```

(Actually, installing the most recent version of pyOpenSSL is enough)
Then, activate the program by entering this command:

```
python main.py
```

(python3 or python, depends on your OS)
and you should the instructions for operating the program:



```
Welcome to Public Key Infrastructure project!
These are the main commands:
        generate - Generate an Entity
        send - Send a message
        show - Show entities
        revoke - Revoke an entity of your choice
        help - Print this instructions again
        quit - Quit the program
Note: Enter an entity by entering it's ID which is the number it is given.
 For example, Entity1 has an ID 1, so enter 1 for relevant commands.
Very well!
Enter command: 
```

Figure 1: Instructions

Good Luck :)