List of Tables

List of Figures

Contents

I. Introduction

In this project, we are suppose to implement a distribution processsecure electronic certificate of success for CertifPlus company.

Objectives

- An user can:
  - request to create a certificate with their information
  - download their certificate
  - verify an existing certificate
- The authenticity of the certificate issued electronically in the form of an image must be guaranteed:
  - The image contains visible information :
    - The name of the person receiving the certificate of achievement
    - The name of the successful certification
    - A QRcode containing the signature of this information
  - The image contains hidden information :
    - tamper-proof information is concealed by steganography in the image. This information includes the visible information of the certificate as well as the guaranteed delivery dateby a *timestamp* signed by a time stamping authority freetsa
- Verification
  - extract and the stamp concealed in the image by steganography and verify signature and timestamp
  - checks the signature encoded in the QRcode

II. Programs, Materials, Methodologies

2.1 Programs and Materials

- Python 3.8
- bottle - For Web Services
- qrcode, numpy, Pillow, zbarlight for qrCode creation, verification and image modification
- a stenography library provided in this project
- socat - multipurpose relay tool

2.2 Methodologies

A. Creating certficate

An user will request CertifPlus for creating a certificate by providing his/her informations containing Last name and First name, Institue and a signature data (more details while be described in the analysis risk part)