HW05

Riccardo Zucchelli 1984963

October 2024

1 Introduction

This homework centers on the practical use of the CieSign application, which has been developed by the Public Administration to facilitate secure online interactions. The CieSign app operates in conjunction with CieID, an innovative digital system that leverages an individual's electronic ID card to authenticate users online. This approach enhances security and simplifies access to various online public services, ensuring that only verified individuals can perform sensitive operations.

This document will be using part of the informations discovered in the previous homework to get the necessary tools needed to verify the strengths and limitations on this free tool provided by the government.

2 Digitally signing a file

The process of signing a PDF document is more or less similar to what other (paid) services ask. The application asks the PDF that we want to sign, optionally appending an actual physical signature of the person -which per se hasn't any legal binding, since it's a digital one- and then asking for proof of identity, which is done by providing the physical ID card to the NFC Reader and confirming its PIN. As a test, a PDF will be provided and will be digitally signed by the aforementioned mean.

2.1 Verifying the contents

After a quick verification of the file integrity with `openssl smime` suite of commands, we can analyze better what the certificate grants us to do. We'll use openssl to show x509 certificate contents, and specifically we're interested in x509v3 extensions to see if something is missing from the digital signature provided by TIM.

```
X509v3 extensions:
    X509v3 Authority Key Identifier:
        F9:2E:E9:08:64:9F:A2:B8:2B:A8:32:95:41:73:E9:7D:9D:0C:15:18
    Authority Information Access:
```

```
        OCSP - URI:https://ocsp.cie.interno.gov.it/
    X509v3 Certificate Policies:
        Policy: 1.3.76.47.4
        User Notice:
            Explicit Text: X.509 authentication certificate issued by the Italian
        CPS: http://www.cartaidentita.interno.gov.it/policy/cittadini_cps.pdf
    X509v3 Extended Key Usage:
        TLS Web Client Authentication
    X509v3 CRL Distribution Points:
        Full Name:
        URI:http://ldap.cie.interno.gov.it/ciesubca002.crl
    X509v3 Subject Key Identifier:
        ED:95:C6:F1:83:6D:33:3A:CF:07:F8:CA:F4:1E:76:57:75:BA:04:A6
    X509v3 Key Usage: critical
        Digital Signature
```

Generally speaking we can't see many differences between this certificate and the one contained in the previous homework. We can get more information by searching on internet about the type of certificate that this is, and by explaining what it's the main difference between **QCert** and **Gen** e-Signatures. In the context of the European Union, **QCert for ESIG** and **Gen for ESIG** refer to different types of electronic signatures and related certification systems, which are used to ensure the security and legal validity of electronic transactions.

QCert for ESIG

- **QCert** refers to a **Qualified Certificate** used for electronic signatures (ESIG). A Qualified Certificate is a certificate issued by a trusted Certification Authority (CA) that complies with strict requirements set by EU regulations (eIDAS regulation) for electronic signatures.
- It ensures that the signature is legally binding and has the highest level of security, offering strong authentication and integrity.
- The key difference with QCert is that it is specifically linked to the creation of **qualified electronic signatures**, which have the same legal standing as handwritten signatures in the EU. This type of signature is issued by a **Qualified Trust Service Provider** (QTSP) and must meet additional criteria such as being issued with a secure signature creation device.

Gen for ESIG

- **Gen for ESIG** typically refers to **general certificates** used for electronic signatures. These certificates may not meet the higher standards set by the EU for qualified signatures, and they might be used for less critical applications or in situations where the highest level of security is not required.

- **Gen certificates** can be issued by a broader range of Certification Authorities (CAs) and do not have the same stringent regulatory framework as Qualified Certificates. This makes them suitable for situations where legal equivalence to handwritten signatures is not required, and a more flexible, less costly option is acceptable.

The main key difference between the two is their **Legal Standing**: Qualified Certificates (QCert) provide the highest level of legal certainty under EU law, while general certificates (Gen) are typically used for less critical purposes and may not be recognized in all legal contexts. Generally, Gen certificates are legally recognized only in the national level, while QCerts are internationally recognized.

source: https://eidas.ec.europa.eu/efda/trustservices/browse/eidas/tls/tl/IT