Cybersecurity - Homework 8

Vlad Turno (1835365)

December 14, 2025

1) Introduction

A digital signature is a cryptographic value that is calculated from a private key and it serves as a verification tool to confirm the authenticity and integrity of the data (private key is used to sign, and the public key is used to verify the signature).
Digital signatures often rely on hashing algorithms (such as SHA-256) to hash the message before signing. The signature verification process involves checking whether the signature matches the original data and verifying that the signer's public key corresponds to the private key that was used for signing.

2) Checklist

- **Obtain the public key**: the signed document must be available along its digital signature and the public key since its required for the verification process. It can be typically retrieved from a certificate or a public key infrastructure.
- **Extract the signature**: separate the digital signature from the original message (is usually appended to the message or provided in a separate file). Compute the hash value of the original message using the same algorithm adopted by the signer, and decrypt the signature using the aforementioned public key (the decrypted value should expose the hash value of the original message).
- **Hash comparison**: compare the decrypted hash with the one calculated from the message and if they match it means that the signature is valid and/or the message have not been altered in any way.

3) Verification

The signature validation is performed automatically in Adobe Acrobat Reader and it tells if the signature is valid, expired, or invalid (due to reasons like certificate issues, CRL/OCSP problems, etc.) but I have to manually carry the analysis because otherwise this homework would be way too easy and the professor (who won't read it anyway) does not want it to happen.

3.1) PAdES Signature

To extract the PAdES signature and its related certificate I'll use PDFSig API tool and the certificate analysis will be carried via OpenSSL tools.
The following command outputs information about the PAdES signature in the pdf file, including name, possible certificate and validity:

```
$ pdfsig test_signed.pdf

Digital Signature Info of: test_signed.pdf
Signature #1:
  - Signature Field Name: Signature1
  - Signer Certificate Common Name: Fabrizio d'Amore
  - Signer full Distinguished Name: dnQualifier=WSREF-94746602542849,CN=Fabrizio d
      'Amore,serialNumber=TINIT-DMRFRZ60P04H501I,givenName=Fabrizio,SN=d'Amore,C=
      IT
  - Signing Time: Dec 08 2025 15:49:26
  - Signing Hash Algorithm: SHA-256
  - Signature Type: ETSI.CAdES.detached
  - Signed Ranges: [0 - 11238], [30184 - 47765]
  - Total document signed
  - Signature Validation: Signature is Valid.
  - Certificate Validation: Certificate issuer is unknown.
```

3.2) Certificate

Cool but as far as i see the certificate issuer is unknown and I have to try something else to get the full chain. With the Adobe Acrobat pdf editor I managed to view and download the certificate in .p7c format and I am able to extract the full certificate chain:

```
$ openssl pkcs7 -inform DER -in CertExchange.p7c -print_certs -out extracted_certs.pem

subject=C = IT, SN = d'Amore, GN = Fabrizio, serialNumber = TINIT-DMRFRZ60P04H501I, CN =
    Fabrizio d'Amore, dnQualifier = WSREF-94746602542849
issuer=C = IT, L = Arezzo, O = ArubaPEC S.p.A., organizationIdentifier = VATIT-01879020517, OU
     = Qualified Trust Service Provider, CN = ArubaPEC EU Qualified Certificates CA G1
-----BEGIN CERTIFICATE-----
MIIHMjCCBRqgAwIBAgIQYH6I/ODzxQB8EREtkCBGpTANBgkqhkiG9w0BAQsFADCB
sjELMAkGA1UEBhMCSVQxDzANBgNVBAcMBkFyZXp6bzEYMBYGA1UECgwPQXJ1YmFQ
RUMgUy5wLkEuMRowGAYDVQRhDBFWQVRJVC0wMTg3OTAyMDUxNzEpMCcGA1UECwwg
UXVhbGlmaWVkIFRydXN0IFNlcnZpY2UgUHJvdmlkZXIxMTAvBgNVBAMMKEFydWJh
UEVDIEVVIFF1YWxpZmllZCBDZXJ0aWZpY2F0ZXMgQ0EgRzEwHhcNMjQxMTA1MTMy
NDE4WhcNMjcxMTA1MTMyNDE4WjCBjTELMAkGA1UEBhMCSVQxEDAOBgNVBAQMB2Qn
QW1vcmUxETAPBgNVBCoMCEZhYnJpemlvMR8wHQYDVQQFExZUSU5JVC1ETVJGUlo2
MFAwNEg1MDFJMRkwFwYDVQQDDBBGYWJyaXppbyBkJ0Ftb3J1MR0wGwYDVQQuExRX
U1JFRi05NDc0NjYwMjU0MjgOOTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBALkbg52kRGZDn6fFXDCXj4nR1qwfuU2ytumKABZPtVHVGjtlL2S/OfJnhHGA
UiOblji/7W6H44Yhds9TX6PKRqV9jSvgvYa4RZ91h7ZyVv6s4JJNIwK4cnwmRvVx
7YmPlkhu+EsfQd0C8LS2Q44ioFlyBeyhF0smj6CUcsmblnJG0EAzS8k1VeuJAMYm
0L3jEyJvfaI5JxfmAA8IQ91i5i00aCGTfgJxghAgzUjZxP7g0kGq2Cw3oebGneQL
r/OssE9eszWj6JLoXQG+lQe8+3MuCY4mDmqkN2sO7D5c+7Ledh2PZx0IeH1J+9uC
oTXvBMut8hKMuvBnc5aiwT8tqmsCAwEAAaOCAmUwggJhMB8GA1UdIwQYMBaAFMZv
O4V70SaxeJpCpCVpDPb/eqBnMH8GCCsGAQUFBwEBBHMwcTA4BggrBgEFBQcwAoYs
aHR0cDovL2NhY2VydC5wZWMuaXQvY2VydHMvYXJ1YmFwZWMtZWlkYXMtZzEwNQYI
KwYBBQUHMAGGKWh0dHA6Ly9vY3NwMDEucGVjLml0L3ZhL2FydWJhcGVjLWVpZGFz
HRRh4sW+Ch70AXem6v/wlXX1QdsIlsE2aSFuqjDpBwEQj/VM/0EACSIvA7HQsWGK
GEta+AI3j6+cva3Emc3A21mGs0N60xlG2R+kgYJK4kQxo7f5TkNDowhZlaN3+bom
H1En4NK6WvvC89DuIROObMlVNH4GfgS0pcR2r/0FqbRuN8RVoJE0f4PT8xxBBPjL
EZBbLR7w/wom5Au6VdQheC/L76QatxqheZso2ygF/GJ3HOJy5QKZLPNpuiyjs5qg
oN9lZNDqNyP2SN+4RRNO5YjuMywf/VUmcb3mpGjbvt4HR9hbWwcxxio7K7KxOYkn
6xYHfrbQhxSueP/XoyMUIXyKhWuPVA==
-----END CERTIFICATE-----
```

3.3) Examination

```
$ openssl x509 -in extracted_certs.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:7e:88:fc:e0:f3:c5:00:7c:11:11:2d:90:20:46:a5
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IT, L = Arezzo, O = ArubaPEC S.p.A., organizationIdentifier = VATIT
             -01879020517, OU = Qualified Trust Service Provider, CN = ArubaPEC EU Qualified
             Certificates CA G1
        Validity
            Not Before: Nov  5 13:24:18 2024 GMT
            Not After : Nov  5 13:24:18 2027 GMT
        Subject: C = IT, SN = d'Amore, GN = Fabrizio, serialNumber = TINIT-DMRFRZ60P04H501I,
             CN = Fabrizio d'Amore, dnQualifier = WSREF-94746602542849
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b9:1b:83:9d:a4:44:66:43:9f:a7:c5:5c:30:97:
                    8f:89:d1:d6:ac:1f:b9:4d:b2:b6:e9:8a:00:16:4f:
                    b5:51:d5:1a:3b:65:2f:64:bf:39:f2:67:84:71:80:
                    52:23:9b:96:38:bf:ed:6e:87:e3:86:21:76:cf:53:
                    5f:a3:ca:46:a5:7d:8d:2b:e0:bd:86:b8:45:9f:75:
                    87:b6:72:56:fe:ac:e0:92:4d:23:02:b8:72:7c:26:
                    46:f5:71:ed:89:8f:96:48:6e:f8:4b:1f:41:dd:02:
                    f0:b4:b6:43:8e:22:a0:59:72:05:ec:a1:17:4b:26:
                    8f:a0:94:72:c9:9b:96:72:46:d0:40:33:4b:c9:35:
                    55:eb:89:00:c6:26:d0:bd:e3:13:22:6f:7d:a2:39:
                    27:17:e6:00:0f:08:43:dd:62:e6:2d:34:68:21:93:
                    7e:02:71:82:10:20:cd:48:d9:c4:fe:e0:d2:41:aa:
                    d8:2c:37:a1:e6:c6:9d:e4:0b:af:f3:ac:b0:4f:5e:
                    b3:35:a3:e8:92:e8:5d:01:be:95:07:bc:fb:73:2e:
                    09:8e:26:0e:6a:a4:37:6b:0e:ec:3e:5c:fb:b2:de:
                    76:1d:8f:67:1d:08:78:7d:49:fb:db:82:a1:35:ef:
                    04:cb:ad:f2:12:8c:ba:f0:67:73:96:a2:c1:3f:2d:
                    aa:6b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                C6:6F:3B:85:7B:D1:26:B1:78:9A:42:A4:25:69:0C:F6:FF:7A:A0:67
            Authority Information Access:
                CA Issuers - URI:http://cacert.pec.it/certs/arubapec-eidas-g1
                OCSP - URI:http://ocsp01.pec.it/va/arubapec-eidas-g1
            X509v3 Issuer Alternative Name:
                email:info@arubapec.it
            X509v3 Certificate Policies:
                Policy: 0.4.0.194112.1.2
                Policy: 1.3.6.1.4.1.29741.1.7.2
                  CPS: https://www.pec.it/repository/arubapec-qualif-cps.pdf
                Policy: 1.3.76.16.6
            qcStatements:
                0..0......F..0......F.....0......F..0.......F..0..0>.8https://www.pec.it/
                     repository/arubapec-qualif-pds-it.pdf..it0>.8https://www.pec.it/
                     repository/arubapec-qualif-pds-en.pdf..en
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl01.pec.it/va/arubapec-eidas-g1/crl
            X509v3 Subject Key Identifier:
                25:60:64:8E:3E:5D:07:11:36:E3:91:34:6C:02:1B:95:CA:E5:8E:5F
            X509v3 Key Usage: critical
                Non Repudiation
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        71:b8:42:c0:34:3e:41:7e:89:64:ef:7d:a7:fe:c8:fe:9b:9d:
        f3:96:bf:04:01:a3:3b:7a:05:d3:fe:23:50:79:a2:c3:eb:4f:
        19:34:fc:c2:96:a0:13:9e:55:3e:2f:b5:a6:77:43:68:c8:1c:
        ff:8b:ff:6f:77:32:90:15:7b:e8:d1:f4:be:9f:40:ba:45:8e:
        ce:92:f5:94:d5:26:91:18:57:ea:c4:63:9f:0f:9c:68:e3:ca:
        bb:2b:ed:e8:a3:3c:97:ad:b8:66:ae:d9:38:f7:01:91:5e:29:
        5a:5c:8c:03:a0:6b:86:b2:85:2a:f8:a7:56:80:a4:bd:6d:1b:
        5d:9b:40:04:67:4f:da:56:06:9c:09:19:e7:d9:63:7d:d9:e8:
        0f:dc:59:03:6f:66:97:3a:f8:a2:4b:02:63:ec:53:ee:e2:88:
        6e:37:c4:55:a0:91:34:7f:83:d3:f3:1c:41:04:f8:cb:11:90:
        5b:2d:1e:f0:ff:0a:26:e4:0b:ba:55:d4:21:78:2f:cb:ef:a4:
        1a:b7:1a:a1:79:9b:28:db:28:05:fc:62:77:1c:e2:72:e5:02:
        99:2c:f3:69:ba:2c:a3:b3:9a:a0:a0:df:65:64:d0:ea:37:23:
        f6:48:df:b8:45:13:74:e5:88:ee:33:2c:1f:fd:55:26:71:bd:
        e6:a4:68:db:be:de:07:47:d8:5b:5b:07:31:c6:2a:3b:2b:b2:
        b1:39:89:27:eb:16:07:7e:b6:d0:87:14:ae:78:ff:d7:a3:23:
        14:21:7c:8a:85:6b:8f:54
```

3.4) Update Interval

Now we look into the certificate for any information about the certificate revocation list and see if the certificate has been revoked before expiration or something like that.
When a certificate is revoked, it's added to the CRL so that users and systems can check whether a certificate is still valid.
A CRL is typically published by the CA at regular intervals and is referenced by systems that need to verify the validity of certificates. If a system encounters a certificate that's on the CRL, it will treat that certificate as invalid, even if it hasn't expired yet.

```
X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl01.pec.it/va/arubapec-eidas-g1/crl
            X509v3 Subject Key Identifier:
                25:60:64:8E:3E:5D:07:11:36:E3:91:34:6C:02:1B:95:CA:E5:8E:5F
            X509v3 Key Usage: critical
                Non Repudiation

$ curl -O http://crl01.pec.it/va/arubapec-eidas-g1/crl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 2006k    0 2006k    0     0  2267k      0 --:--:-- --:--:-- --:--:-- 2267k

$ openssl crl -in crl -text -noout

...
Serial Number: 5DBA8D117B364B69
        Revocation Date: Oct 13 07:07:18 2022 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Superseded
    Serial Number: 64D3DD154EB21B741F6C3A7BE0F1424D
        Revocation Date: Aug  7 08:29:33 2025 GMT
    Serial Number: 37C00EAA262BBADF8178D47748D1FB56
        Revocation Date: Jul 24 12:49:07 2025 GMT
    Serial Number: 6C40E26245EAEEA7FACB1A4C6AC0C004
        Revocation Date: May 26 10:37:33 2025 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Superseded
    Serial Number: 3BB8F0E7E57B91D8304B13DE4EE9EAC4
        Revocation Date: Dec  3 10:56:19 2024 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Superseded
    Serial Number: 2499383D636A00D2A51A50B125C337DC
        Revocation Date: May  9 14:24:21 2025 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Superseded
...
    Serial Number: 4DD94A6F626FAB56
        Revocation Date: Mar 31 16:40:18 2023 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Superseded
    Serial Number: 48E0041F8854C2BDB07D34FB43319595
        Revocation Date: Jun 15 14:37:03 2025 GMT
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        1b:13:49:89:bb:30:a7:73:47:31:47:e8:c8:77:89:fa:8f:11:
        ed:28:da:f4:6e:5e:2b:de:a5:d6:04:32:fc:9e:3f:f9:44:10:
        27:62:e3:46:44:cf:6c:b4:b3:cd:dc:01:25:22:65:c7:2d:9c:
        bc:02:cd:10:88:29:ec:20:a3:16:6b:7b:74:5c:e1:4d:96:99:
        91:9c:28:21:0a:8c:d1:f4:fd:5e:b2:64:99:36:ae:8f:d0:cc:
        fb:f9:17:ba:5c:fe:dc:43:9c:82:cc:d6:5a:19:1d:b1:f0:39:
        c8:ce:5d:c5:03:98:b0:6a:52:89:d1:9d:46:54:00:19:5e:e1:
        26:97:46:d4:d3:8a:90:09:51:a3:f0:00:1f:d0:33:33:c5:09:
        6a:c9:ba:36:8a:25:6e:1b
```

3.5) Online Status

Finally we check the Online Certificate Status Protocol (OCSP) using OpenSSL OCSP Responder, a server run by the Certificate Authority that verifies digital certificate validity in real time, answering with the certificate status in respinse to the API call.
Is basically a more efficient version of the previous seen certificate revocation list (CRL):

```
X509v3 Authority Key Identifier:
                C6:6F:3B:85:7B:D1:26:B1:78:9A:42:A4:25:69:0C:F6:FF:7A:A0:67
            Authority Information Access:
                CA Issuers - URI:http://cacert.pec.it/certs/arubapec-eidas-g1
                OCSP - URI:http://ocsp01.pec.it/va/arubapec-eidas-g1

$ openssl ocsp -issuer issuer_certs.pem -cert extracted_cert.pem -url http://
    ocsp01.pec.it/va/arubapec-eidas-g1

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:7e:88:fc:e0:f3:c5:00:7c:11:11:2d:90:20:46:a5
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IT, L = Arezzo, O = ArubaPEC S.p.A., organizationIdentifier =
            VATIT-01879020517, OU = Qualified Trust Service Provider, CN =
            ArubaPEC EU Qualified Certificates CA G1
        Validity
            Not Before: Nov  5 13:24:18 2024 GMT
            Not After : Nov  5 13:24:18 2027 GMT
        Subject: C = IT, SN = d'Amore, GN = Fabrizio, serialNumber = TINIT-
            DMRFRZ60P04H501I, CN = Fabrizio d'Amore, dnQualifier = WSREF
            -94746602542849
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b9:1b:83:9d:a4:44:66:43:9f:a7:c5:5c:30:97:
                ...
                    04:cb:ad:f2:12:8c:ba:f0:67:73:96:a2:c1:3f:2d:
                    aa:6b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                C6:6F:3B:85:7B:D1:26:B1:78:9A:42:A4:25:69:0C:F6:FF:7A:A0:67
            Authority Information Access:
                CA Issuers - URI:http://cacert.pec.it/certs/arubapec-eidas-g1
                OCSP - URI:http://ocsp01.pec.it/va/arubapec-eidas-g1
            X509v3 Issuer Alternative Name:
                email:info@arubapec.it
            X509v3 Certificate Policies:
                Policy: 0.4.0.194112.1.2
                Policy: 1.3.6.1.4.1.29741.1.7.2
                  CPS: https://www.pec.it/repository/arubapec-qualif-cps.pdf
                Policy: 1.3.76.16.6
            qcStatements:
                0..0......F..0......F.....0......F..0.......F..0..0>.8https://www.
                    pec.it/repository/arubapec-qualif-pds-it.pdf..it0>.8https://
                    www.pec.it/repository/arubapec-qualif-pds-en.pdf..en
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl01.pec.it/va/arubapec-eidas-g1/crl
            X509v3 Subject Key Identifier:
                25:60:64:8E:3E:5D:07:11:36:E3:91:34:6C:02:1B:95:CA:E5:8E:5F
            X509v3 Key Usage: critical
                Non Repudiation
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        71:b8:42:c0:34:3e:41:7e:89:64:ef:7d:a7:fe:c8:fe:9b:9d:
       ...
        b1:39:89:27:eb:16:07:7e:b6:d0:87:14:ae:78:ff:d7:a3:23:
        14:21:7c:8a:85:6b:8f:54
```