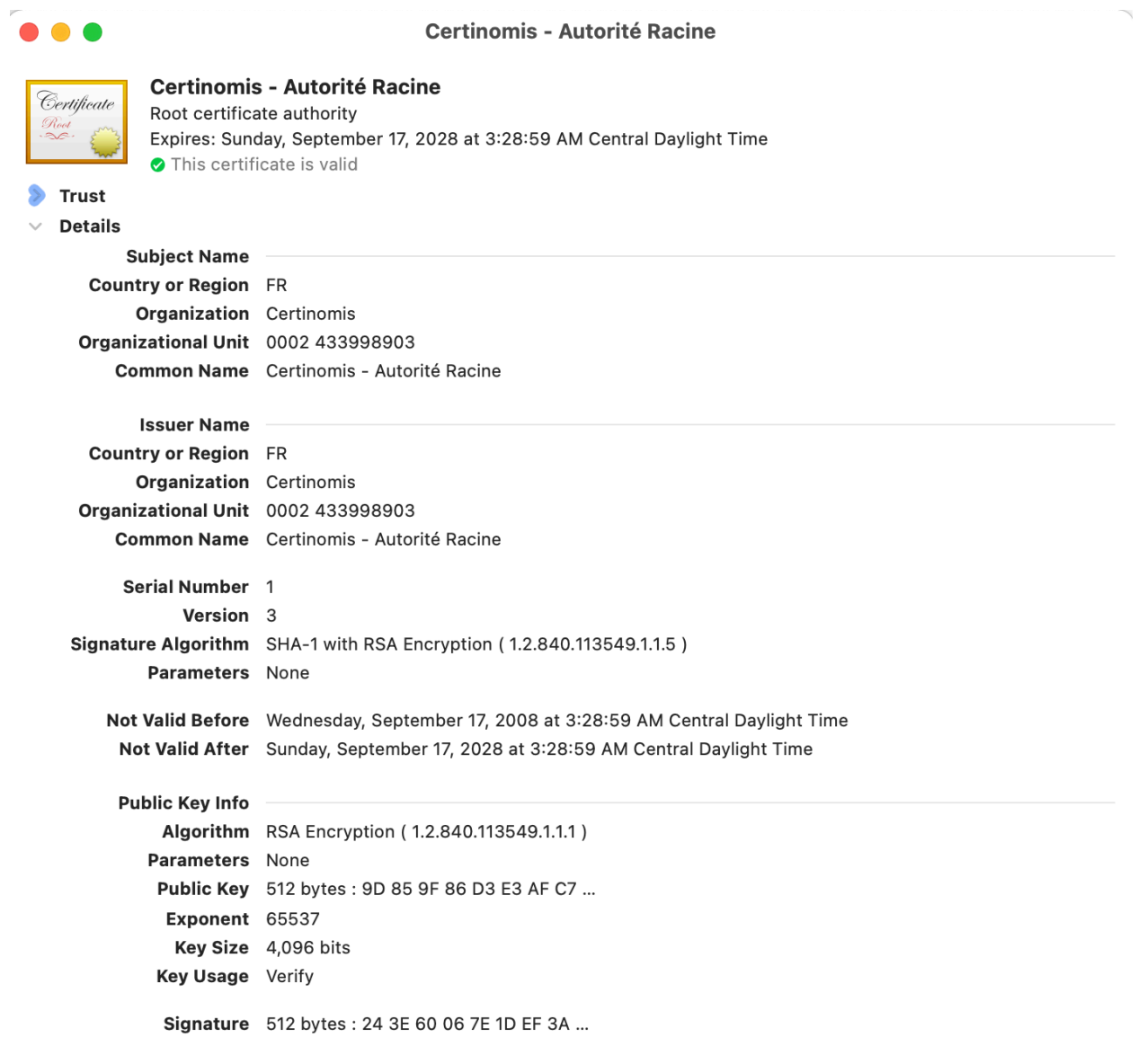


Homework 8 – Networking

Pick your favorite browser, the one that you use more often. Find the root CA certificates that are currently installed. (Since there are many different browsers, you probably need to do a web-search. For example, on Mac, you will have to go through the “Keychain Access tool”. Determine roughly the number of root CA. Then screen-capture one certificate.

Hand-in: A **PDF** with a description of what you did, the rough number of installed CAs, and the capture of one certificate.



The screenshot shows a window titled "Certinomis - Autorité Racine" with a standard Mac OS title bar (red, yellow, green buttons). The main content area displays the details of a root certificate authority. At the top left is a small icon of a certificate. The text reads: "Certinomis - Autorité Racine", "Root certificate authority", and "Expires: Sunday, September 17, 2028 at 3:28:59 AM Central Daylight Time". A green checkmark icon indicates "This certificate is valid". Below this, there are two expandable sections: "Trust" (with a blue arrow icon) and "Details" (with a downward arrow icon). The "Details" section is expanded and shows the following information:

- Subject Name** (Section Header)
- Country or Region** FR
- Organization** Certinomis
- Organizational Unit** 0002 433998903
- Common Name** Certinomis - Autorité Racine
- Issuer Name** (Section Header)
- Country or Region** FR
- Organization** Certinomis
- Organizational Unit** 0002 433998903
- Common Name** Certinomis - Autorité Racine
- Serial Number** 1
- Version** 3
- Signature Algorithm** SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
- Parameters** None
- Not Valid Before** Wednesday, September 17, 2008 at 3:28:59 AM Central Daylight Time
- Not Valid After** Sunday, September 17, 2028 at 3:28:59 AM Central Daylight Time
- Public Key Info** (Section Header)
- Algorithm** RSA Encryption (1.2.840.113549.1.1.1)
- Parameters** None
- Public Key** 512 bytes : 9D 85 9F 86 D3 E3 AF C7 ...
- Exponent** 65537
- Key Size** 4,096 bits
- Key Usage** Verify
- Signature** 512 bytes : 24 3E 60 06 7E 1D EF 3A ...