

heig-vd

Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Applications et Services Internet

SSL - JSSE (Java Secure Socket Extension)

RAPPORT DE LABORATOIRE

Romain de Wolff

IL2008

19 janvier 2008

Table des matières

1	Introduction	1
2	Réponses aux questions	1
2.1	En examinant le certificat du serveur, comment pouvez-vous en déduire que celui-ci est auto-signé ?	4
2.2	Pourquoi serait-il intéressant de faire signer le certificat par une entité comme Verisign ?	4
3	Clé publique	4
4	Conclusion	4
5	Références	4

1 Introduction

2 Réponses aux questions

Lors de la connexion sur notre serveur HTTPS à l'aide du navigateur Firefox, le serveur nous affiche une alerte comme le montre la figure 1

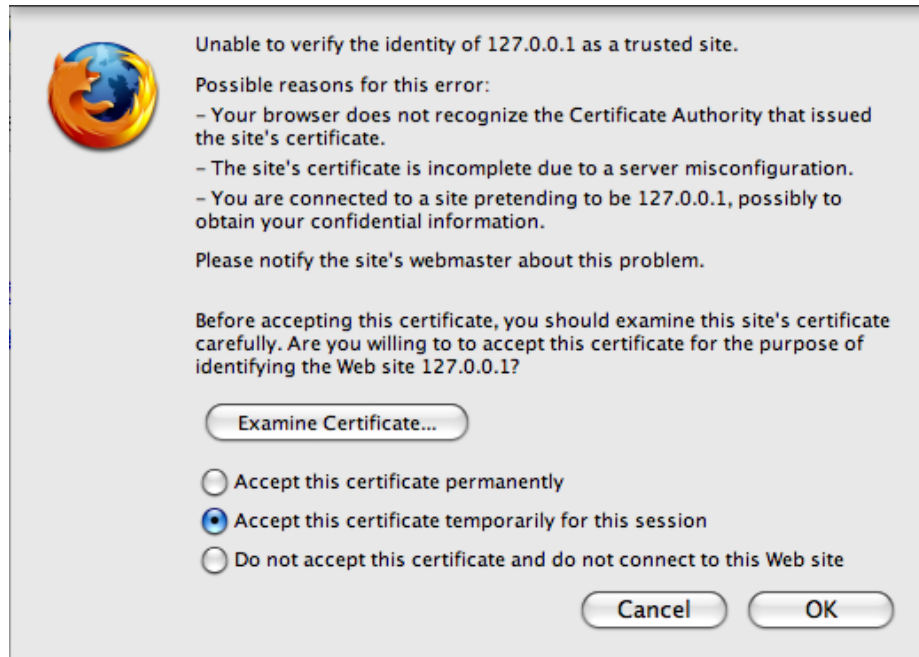


FIG. 1 – Alerte affichée lors de la connexion sur le site sécurisé.

Nous acceptons ce certificat et nous allons voir le site s'afficher. On remarque que le site est sécurisé grâce à l'icone représentant un cadenas (en bas à droite dans Firefox) que l'on peut voir sur la figure 2.

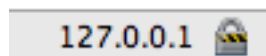


FIG. 2 – Icone dans la barre des tâches du navigateur Firefox.

En cliquant sur le cadenas on peut afficher les informations relatives à la sécurité et donc du certificat que l'on a accepté. La figure 3 nous montre à quoi ressemble cette fenêtre.



FIG. 3 – Information sur la sécurité du site.

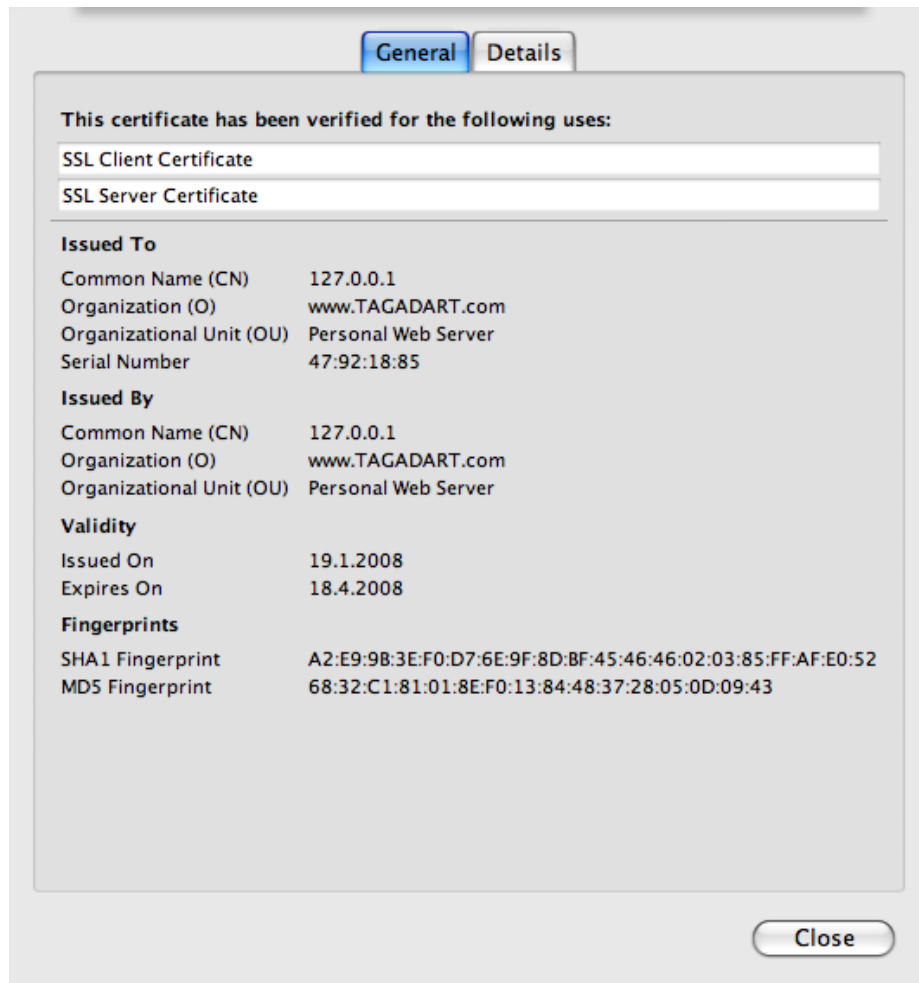


FIG. 4 – Affichage détaillée des informations sur le certificats que nous avons créé.

- 2.1 En examinant le certificat du serveur, comment pouvez-vous en déduire que celui-ci est auto-signé ?
- 2.2 Pourquoi serait-il intéressant de faire signer le certificat par une entité comme Verisign ?

3 Clé publique

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBujCCASMAQAwEjELMAkGA1UEBhMCQ0gxChZBbnVBAgTAlZEMREwDwYDVQQHEwhMYXVzYW5u
ZTEZMBcGA1UEChMQd3d3L1RBR0FEQVJULmNvbTEcMBoGA1UECxMTUGVyc29uYWwgV2ViIFNlcnZl
cjsESMBAGA1UEAxMJMTI3LjAuMCA4xMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCjcLrCV1/h
50CuSHjNevhTrRS0bCQ1oCN27c3hTLdDbLVjDNqUJqziTXpowFTUXmM/hrbKwVzM5+I4krwx/6dW
oVVhaGywXkQwN4mQ2rgFvkdM8xIpPKfyVMTLYRQLfd89qLYC8C0SUR3MqzuNRpT71nlalRB9A6Mg
IIx53mf8UQIDAQABoAAAwDQYJKoZIhvcNAQEEBQADgYEAhT/hvwHd1Qb5ZPe6EmBbMJe6VozqQT
yzaA2q6+4Y+FzuQ0PT7oePyg22e6HTiEtXRiHNGiCXVlceeNxKYFBGoBGVSGOHvauWFGRntErntQ
X7vYKW5XCjHfEpsMwKsj42b4zMFN743IT/LmiC/NsghW3q+UD7AUs1ld4+XaX68=
-----END NEW CERTIFICATE REQUEST-----
```

4 Conclusion

5 Références

<http://jquery.com/> Site officiel de jQuery.

<http://www.jquery.info/> Site francophone sur jQuery.

<http://docs.jquery.com/Tutorials> Tutoriels officiels.

<http://www.gotapi.com/html> Description de l'API jQuery ainsi que HTML. Très utile comme référence rapide et disponibles pour une grande variété de langages courants.

http://developer.mozilla.org/fr/docs/Le_DOM_et_JavaScript Explication du DOM et JavaScript.

<http://www.yoyodesign.org/doc/w3c/dom2-core/introduction.html> Documentation DOM.

http://fr.wikipedia.org/wiki/Document_Object_Model Documentation DOM.

<http://fr.wikipedia.org/wiki/Javascript> Documentation JavaScript.