Partie II : infrastructure à clés publiques et certificats X.509

#1

En résumé , le certificat X.509 sert à valider l'identité et l'intégrité de l'entitée certifiée à l'aide d'une clé publique. De ce fait, l'utilisateur pourra identifier le serveur comme celui qu'il cherche à obtenir (uqav.ca). Celui-ci pourra alors demander son propre certificat aux l'autorité de certification et d'enregistrement qui pourront confirmer à l'utilisateur que ceci est bien le site « uqav.ca ». Dans ce cas, le fait de certifier le site uqac.ca ne protègera pas l'utilisateur d'aller sur ce site. Or, si l'utilisateur ne prend pas la peine de vérifier si le site est bel et bien le site désiré, malheureusement le site malicieux obtiendera ses informations.

#2

a)

Non , il s'agit d'un certificat signé (sa propre clé publique est vérifié par d'une autorité de certification)

b)

Le 2 Février 2015 (2015-02-02)

c)

SHA-1

d)

256 bits