

Tiers de confiance, PKI & Certificat

■ ■ ■ **Mot de passe et authentification**

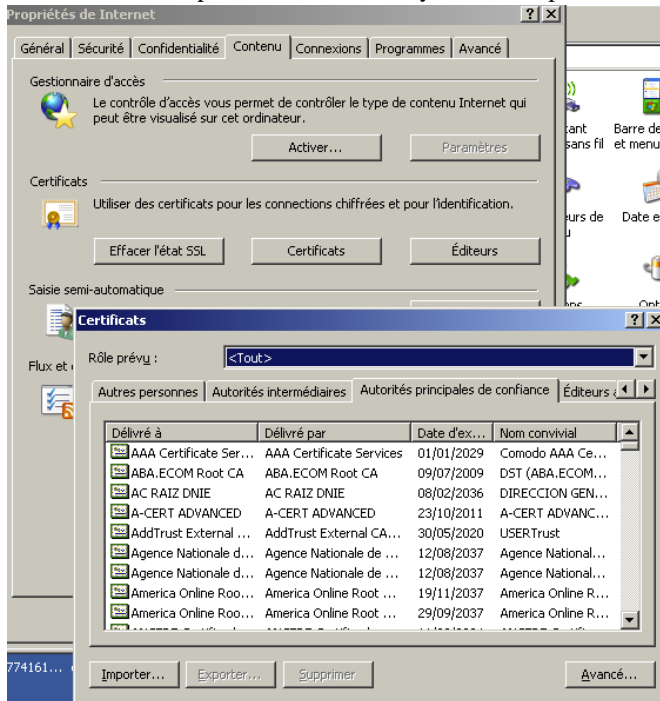
- 1 – Allez sur le site <http://www.passwordmeter.com/> et testez des *mots de passe*.
 - a. Est-ce que le mot de passe que vous utilisez habituellement est aussi robuste que vous le pensez ?
 - b. Essayez le mot de passe « Sécurité ». Quelle est sa robustesse ?
Est-il facilement trouvable ? Comment ?
 - c. Que pensez vous des règles d'évaluation proposées par ce site ?
 - d. Allez construire un mot de passe sur <http://www.testyourpassword.com/>
 - e. Allez évaluer votre mot de passe contre les attaques « brute-force » sur:
<https://howsecureismypassword.net/>

■ ■ ■ **Certificats : chaîne et constitution**

- 2 – a. Allez sur l'infrastructure de gestion de la confiance de l'administration, dite « IGC/A », sur
<https://www.ssi.gouv.fr/administration/services-securises/igca/>
Quelle taille de clés sont proposées pour le certificat racine ?
Pourquoi en existe-t-il deux versions ?
Existe-t-il d'autre(s) différence(s) concernant les opérations cryptographiques ?
 - b. Allez sur le lien « modalités de vérification » : comment vérifier que vous avez le « bon » certificat racine ?
Quel serait le risque sinon ?
- 3 – a. Qu'est-ce que la dématérialisation ?
 - b. Télédéclaration de la TVA : quelle différence entre EFI et EDI ?
Vous pourrez trouver des informations sur :
<http://www.expert-comptable-tpe.fr/posts/view/declarations-edi-efi-les-differences>
La référence depuis les « Finances Publiques » :
<https://www.impots.gouv.fr/portail/professionnel/teleprocedures-efi-ou-edi>
 - c. Quel rôle joue le certificat électronique ?
- 4 – a. Allez sur <https://www.certinomis.fr/nos-solutions/lidentite-personnelle/>
Comment est délivré une « Offre profil 2 étoiles » ?
 - b. Allez sur
<https://www.certinomis.fr/nos-solutions/horodatage-et-cachets-electroniques-de-la-poste>
Qu'est-ce que « l'horodatage » ?
Comment est-il sécurisé ?
 - c. Allez voir l'offre offerte par Certinomis en « identité professionnelle », « offre entreprises & associations » et en « Téléprocédures » :
<https://www.certinomis.fr/nos-solutions/lidentite-professionnelle>
Quel est le coût des différentes offres proposées ?
Sous quelle forme peut être fourni le certificat ?
Qu'apporte l'utilisation d'une carte à puce ?
 - d. Allez sur <https://www.certinomis.fr/cartes-teleprocedures>
Permet-elle la télédéclaration de la TVA ?
 - e. Allez sur <https://www.certinomis.fr/informations-pratiques/revoquer-votre-certificat>
Quelles sont les raisons possibles d'une demande de révocation ?

- 5 – Regardez le certificat protégeant l'accès au site sécurisé <https://webmail.unilim.fr/>.
- quel algorithme est utilisé pour réaliser la signature électronique ?
 - quel algorithme est utilisé pour calculer l'empreinte du certificat ?
 - quelle est la date d'expiration du certificat ?
 - donnez la chaîne de confiance du site ;
 - quelle est la CA, « *Certificate Authority* », de ce certificat ?
 - allez sur <https://www.amazon.fr/>, est-ce que la chaîne de certificat est la même ?

- 6 – Regardez les certificats présents dans votre système d'exploitation :



Existe-t-il des AC françaises ?

Des ressources fournies par l'ANSSI, « Agence nationale de la sécurité des systèmes d'information »

- 7 – Allez sur le site de l'ANSSI, <http://www.ssi.gouv.fr/> et consultez les documents suivants :
- « Principes généraux » :
 - ◇ <http://www.ssi.gouv.fr/administration/bonnes-pratiques/>
 - « Mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques »
 - ◇ <https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/>
 - ◇ https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf
 - ◇ *Quelle est la taille recommandée des clés de chiffrement ?*
 - « Guide d'hygiène informatique » :
 - ◇ <http://www.ssi.gouv.fr/administration/guide/guide-dhygiene-informatique/>
 - ◇ *Lire certaines règles : 6, 14, 15, 23, 40*
 - Le choix d'un mot de passe :
 - ◇ <http://www.ssi.gouv.fr/administration/guide/mot-de-passe/>
 - « Outils méthodologiques »
 - ◇ <http://www.ssi.gouv.fr/administration/bonnes-pratiques/methodologie>
 - ◇ *pour référence*
 - « Typologie de la menace »
 - ◇ <http://www.ssi.gouv.fr/administration/principales-menaces/>
 - ◇ *pour référence*