tetaneutral.net - Evolution #39

certificat https officiel

18/07/2011 10:26 - Laurent GUERBY

Statut:	Résolu	**Début:**	18/07/2011
Priorité:	Normal	**Echéance:**	
Assigné à:	Raphaël Durand	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:			

Description

Choisir un fournisseur, doit marcher si possible sur tout les navigateurs

Historique

#1 - 06/08/2011 22:14 - Laurent GUERBY

Discussion interessante :

http://ask.slashdot.org/story/11/08/06/1841210/Ask-Slashdot-Does-SSL-Validation-Matter

http://perspectives-project.org/
"Notaries" => surveillance distribuée des changements de certificat SSL

#2 - 05/07/2012 17:11 - Laurent GUERBY

http://wiki.cacert.org/FAQ/BrowserClients
http://www.ilico.org/faq/#erreursecuritenaviguateurssl

#3 - 26/05/2013 22:17 - Raphaël Durand

J'ai parlé à Laurent de fabriquer des certificats SSL sur Cacert.
Je l'ai déjà fait pour mon serveur perso Ultrawaves.fr
Avantages : C'est gratuit et militant
Inconvénient : le certificat racine n'est pas reconnu par défaut sur les navigateurs et les OS (sauf Debian).

Je propose de faire un test avec ces certificats.

#4 - 09/06/2013 11:52 - Matthieu Herrb

Le principe de CA-Cert c'est de certifier (on dit par anglicisme "assurer") les identités de personnes et indirectement de domaines DNS associés pour produire des certificats x509.

La démarche c'est:

1. créer un compte sur cacert.org
2. rencontrer des "assureurs" de cacert à qui on montre 2 documents d'identité avec photo. En fonction de la confiance que fait l'assureur à ces documents et donc à cette identité, l'assureur attribue des points (entre 1 et 35).
3. à partir d'un certain nombre de points on peut faire certifier un certificat x509 par l'autorité de certification de cacert. Collatérallement, on peut faire signer sa clé PGP si on veut à ce niveau.
4. on peut aussi enregister des domaines dont on est admin (en prouvant via messages envoyés à l'adresse de contact, ou via infos ajoutées dans le DNS ou sur une page web) et faire signer des certificats pour ces domaines.
5. quand on a assez de points, on devient soi-même assureur et on peut à son tour distribuer des points à d'autres.

Les seuils sont expliqués sur cette page: http://wiki.cacert.org/FAQ/Privileges

(AP c'est les "Assurance Points" dont je parle ci-dessus, EP c'est les "Experience Points" que les assureurs accumulent en fonction des assurances qu'ils font.)

#5 - 22/06/2013 20:27 - Raphaël Durand

guerby a ouvert un compte sur CAcert, c'est lui qui fera l'émission des certificats pour les serveurs.
Matthieu l'a certifié en lui donnant 35 points, mais il en faut 50 pour fabriquer des certificats bien reconnus. (selon les explications de Matthieu)
Je monte sur Paris le 7 juillet, je tâcherais de trouver des accréditeurs pour gagner des points et pouvoir en donner à guerby.

#6 - 23/07/2013 14:44 - Laurent GUERBY

Je devrai avoir 35+35 = 70 points grace a Benjamin d'Octopuce

#7 - 23/07/2013 14:51 - yannick deroche

Et concrètement? ça permettrait de générer des cert en *.tetaneutral.net pour les hosting des adhérents?
A quoi d'autre?

#8 - 23/07/2013 15:06 - Thomas Pedoussaut

Je (Thomas Pedoussaut) peux aussi assurer (pour un faible nombre de points).

#9 - 23/07/2013 23:39 - Raphaël Durand

J'ai pas mal avancé sur le sujet, je pourrais vous en parler de vive voix demain mercredi 24 juillet.

-A partir de 50 points sur CAcert on peut créer un certificat serveur.
J'ai réussi à créer un certificat class 1 wildcard (**.*.exemple.com), mais pour rajouter d'autres niveaux (exemple.com, *.**.*.exemple.com) il faut modifier la conf de OpenSSL et je n'arrive pas à faire fonctionner la modif.
On peut aussi créer un certificat class 3 plus sécurisé, mais ça nécessite des modifs dans Apache ou nginx et je ne l'ai pas encore testé.

Je ramènerais des formulaires pour ceux qui veulent se faire assurer.

#10 - 26/07/2013 22:51 - Raphaël Durand

C'est bon j'ai trouvé toutes les configs nécessaires à la fabrication de certificats corrects.
Il faut fabriquer des certificats de classe 3, la classe 1 n'étant encore disponible que pour la compatibilité avec des systèmes plus anciens.
(explications : ici http://wiki.cacert.org/FAQ/TechnicalQuestions#CA)

J'ai trouvé un tuto pour rajouter des subjectAltName et donc mettre plusieurs noms de domaines dans le certificat.
http://langui.sh/2009/02/27/creating-a-subjectaltname-sanucc-csr/

Un certificat de ce type est installé sur mon serveur, vous pouvez tester en allant sur https://ultrawaves.fr ou https://www.ultrawaves.fr et regarder les détails du certificat.
Je vais pouvoir mettre tout cela au propre dans un tutorial.

On va pouvoir fabriquer un certificat correct pour le serveur web (tetaneutral.net et www.tetaneutral.net)
Si ça marche on pourra l'étendre à d'autre services xxxx.tetaneutral.net et notamment aux adhérents qui utilisent des sous-domaines.

#11 - 26/07/2013 22:57 - Raphaël Durand

Je vous linke également ce document qui liste les OS qui incluent ce certificat par défaut : http://wiki.cacert.org/InclusionStatus

#12 - 03/10/2013 09:26 - Raphaël Durand

Un certificat SSL CACert a été mis en place sur la homepage de Tetaneutral.
Vous pouvez le voir en allant sur https://tetaneutral.net ou https://www.tetaneutral.net

Si c'est concluant on pourra l'étendra aux autres VM (chiliproject,lg, etc...)

#13 - 01/07/2015 22:36 - Raphaël Durand

- % réalisé changé de 50 à 100

- Statut changé de En cours à Fermé

Un certificat Wildcard a été pris chez Gandi et installé sur les services qui en ont besoin.
Evolution réalisée.

#14 - 01/07/2015 22:37 - Raphaël Durand

- Statut changé de Fermé à Résolu