Evolutions du service TCS de RENATER (Trusted Certificate Service)

Ludovic Auxepaules

Évolutions du service TCS de RENATER (*Trusted Certificate Service*)

Ludovic Auxepaules
GIP RENATER
23-25 rue Daviel
75 013 Paris

Résumé

Dans cette proposition nous revenons tout d'abord sur un bref historique de l'évolution du service TCS. Nous exposons notamment plus en détails le bilan du service TCS opéré avec Digicert entre 2015 et 2020. Nous décrivons ensuite les fonctionnalités et les principaux changements depuis le lancement de TCS avec Sectigo en mai 2020. Dans une dernière partie, nous nous focalisons sur les difficultés croissantes qui touchent la gestion des certificats serveur depuis quelques années. Dans ce contexte il est nécessaire d'être de plus en plus organisé et réactif ; nous évoquons enfin les différentes solutions permettant de centraliser et/ou d'automatiser la gestion des certificats.

Mots-clefs

TCS, certificats, SSL, TLS, sécurité, ACME, API.

1 Introduction

Depuis plus d'une quinzaine d'années, le service de certificats TCS (*Trusted Certificates Service*) mis à disposition par RENATER pour la communauté Éducation/Recherche, permet d'obtenir des certificats électroniques de sécurisation pour les applications en ligne. Ces certificats électroniques sont reconnus par défaut par la plupart des logiciels (navigateurs internet, clients de messagerie électronique, smartphones…) et ne nécessitent aucune configuration préalable sur les postes clients.

Le service TCS de RENATER est la déclinaison française du contrat signé entre *GÉANT Association* [1] et un prestataire de certification commercial, au bénéfice de plus d'une trentaine de Réseaux Nationaux d'Enseignement et Recherche en Europe (NREN, *National Research and Education Network*), dont RENATER. Au fil des renouvellements de marchés, ce service évolue pour s'adapter aux demandes et aux attentes de la communauté européenne Éducation/Recherche. En mai 2020, lors du dernier renouvellement du marché géré par l'association GÉANT, la société *Sectigo* a été retenue pour succéder à *Digicert* dans la quatrième mouture du service TCS.

2 Historique de l'évolution du « service TCS »

2.1 De SCS à TCS entre 2005 et 2015

Dès le début des années 2000, des IGC (Infrastructures de Gestion de Clés) ont commencé à être opérées dans la communauté Éducation-Recherche française notamment par l'Unité Réseau du Cnrs (UREC) et par le Comité Réseau des Universités (CRU) [2]. Même si ces IGC permettaient de proposer des certificats de confiance et garantissaient l'authentification, la confidentialité et

l'intégrité dans les échanges, elle ne couvraient pas tous les besoins grandissant de la communauté et notamment ceux de pouvoir mettre en place des certificats serveurs reconnus par les navigateurs internet sans avoir une fenêtre « *pop-up* » d'avertissement de vérification du certificat (sans installation préalable d'une autorité de certification sur les postes clients).

En avril 2005, l'initiative « *Pop-free low cost certificates* » portée par TERENA (*Trans-European Research and Education Networking Association*), à laquelle 8 NREN européens se sont associés, a permis de lancer un premier appel d'offre auprès des autorités de certification (AC) commerciales et d'en retenir une, *GlobalSign*, afin de délivrer des certificats serveur à un prix bien plus abordable que ceux du marché. Le service, nommé TERENA SCS (*Server Certificate Service)* [3] est ainsi né pour être déployé dès avril 2006 : il a été adopté et proposé conjointement en France par le CRU et RENATER jusqu'à la fin 2009. Le service SCS a été un succès avec la délivrance d'environ 4 500 certificats serveur. Néanmoins les délais d'obtention des certificats étaient longs et le fonctionnement était très exigeant pour l'autorité d'enregistrement (le NREN de chaque pays).

Fin 2009, un nouvel appel a été mené et *Comodo CA Limited* a cette fois été retenu ; il proposait des certificats plus largement reconnus par des clients : des certificats de serveur (avec la validation du contrôle du domaine DCV et ensuite la validation de l'organisation « OV » à partir de février 2013), des certificats de personne et des certificats de signature de code (dès mai 2014 pour ces derniers). Des portails, dont le développement était géré de manière centralisé, ont été hébergés et opérés par chaque NREN afin de gérer leurs demandes de certificats : respectivement le portail « Djangora » pour les certificats serveurs et le portail « Confusa » pour les certificats personnels. Une vingtaine de NREN ont adhéré à ce nouveau service nommé dorénavant TCS pour *TERENA Certificate Service*[1]. En France, le service TCS a été proposé à la communauté par RENATER, le CRU et l'UREC[2]. 338 établissements ont adhéré au service TCS auprès de RENATER, après signature d'une lettre d'engagement[3]. 7 000 certificats ont été délivrés entre 2010 et 2015.

Les portails opérés directement par les NREN se sont révélés très coûteux en ressources et limités en possibilités, c'est pourquoi les marchés suivants de TCS ont été adaptés pour que les prochains partenaires commerciaux retenus opèrent directement tous les portails.

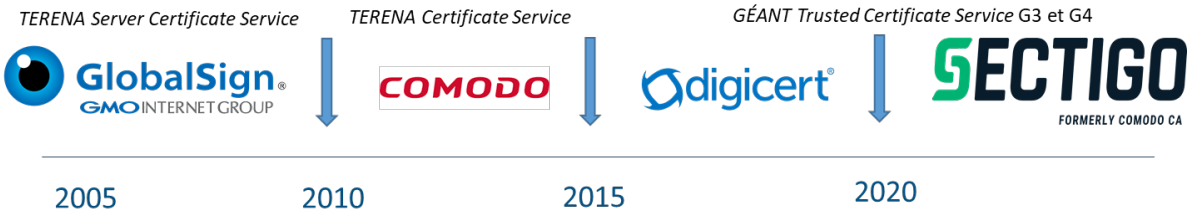

Figure 1 – Historique du service TCS [1]

1 Le service SCS est devenu TCS à partir du moment où les certificats délivrés n'étaient plus seulement des certificats de serveur.

2 Depuis l'intégration en 2011 [4] des missions du CRU et de l'UREC au sein de RENATER, le service TCS n'est plus fourni à la communauté française que par RENATER.

3 Jusqu'en 2020, il était nécessaire pour chaque établissement de signer au préalable un accord de souscription au service TCS (autrement appelé lettre d'engagement). Cet accord fixait les conditions d'utilisation et définissait également le nom officiel de l'établissement ainsi que la liste des personnes autorisées à valider les demandes de certificats et de révocation, la déclaration des organisations et des domaines.

2.2 Bilan de TCS opéré avec *Digicert* entre 2015 à 2020

En 2015, la troisième version du service TCS devient *Trusted Certificate Service* et est gérée dorénavant par l'association GÉANT, issue de la fusion en 2014 de TERENA et de DANTE (*Delivery of Advanced Network Technology to Europe*). L'opérateur *Digicert*, un des leaders sur le marché des certificats et acteur majeur du ***Certification Authority Browser Forum (****CA/Browser Forum)* [5], a été retenu pour une durée de 5 ans par GÉANT. L'autorité de certification *Digicert* propose une large gamme de certificats, un service de validation rapide et de nombreuses fonctionnalités au sein d'un portail unique : *CertCentral* (tableau de bord, rapports, outils d'aide à la gestion des certificats, API...). Ce portail *CertCentral* de *Digicert* est simple d'utilisation, sécurisé (authentification à deux facteurs par OTP ou certificat, restriction par adresses IP) :

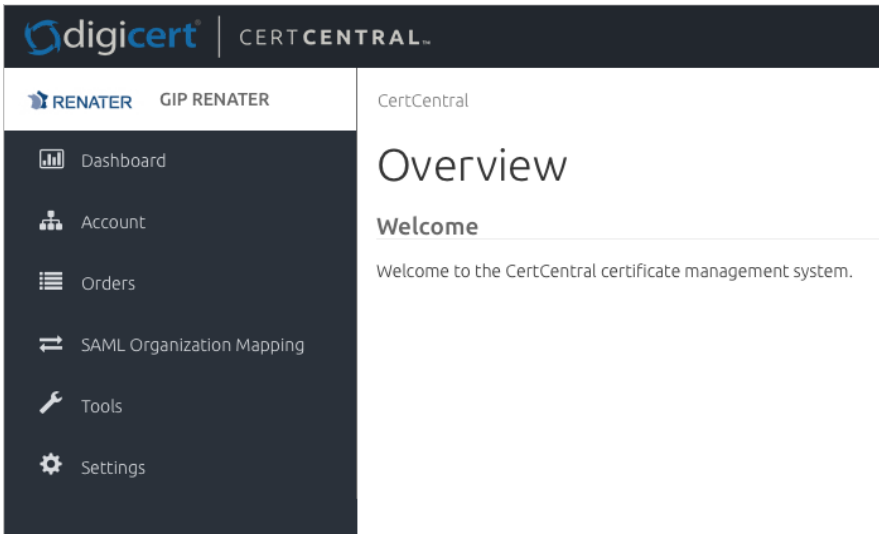

Figure 2 – Portail CertCentral de Digicert

Après la réception de la lettre d'engagement et validation des informations par RENATER, une division et les comptes d'administrateur déclarés de l'établissement sont créés manuellement dans le portail de *Digicert*. Les administrateurs sont ensuite autonomes pour gérer leurs organisations, leurs domaines, leurs utilisateurs et leurs certificats. Ils ont en responsabilité de :

- vérifier les informations légales des organisations qu'ils déclarent et de les soumettre pour validation à *Digicert* (obligatoire pour demander des certificats OV ou EV) ;
- ajouter les domaines qu'ils possèdent et de lancer la procédure de « validation du contrôle des domaines » (DCV pour *Domain Control Validation*) ;
- modérer les demandes de certificats.

Les administrateurs de chaque établissement ont la possibilité d'inviter et de créer des comptes « Utilisateurs » qui sont habilités seulement à réaliser des demandes de certificats serveur dans le portail *CertCentral*. Ces demandes sont ensuite modérées par les administrateurs.

Concernant les certificats clients, les administrateurs ont la possibilité d'activer des portails en *self-service* avec SAML pour gérer les demandes de certificat de personnes des utilisateurs finaux dans leurs établissements.

Le service TCS avec *Digicert* proposé par RENATER [6] a eu un succès encore plus important que les deux précédentes versions : 380 divisions et 475 organisations[4] ont été créées sur une période de 5 ans avec un total de 1 200 administrateurs et de 700 utilisateurs. 4 700 domaines ont été enregistrés et plus de 69 000 certificats ont été délivrés de 2015 à 2020 :

- Certificats serveur : plus de 60 000 ;
- Certificats de personnes : plus de 8 900 ;
- Certificats de grille de calcul : 46 ;
- Certificats de signature de code : 161 ;
- Certificats de signature de documents : 49.

Malgré ce succès, des « dégradations du service TCS avec *Digicert* » ont pu être constatées à la fin du marché : des difficultés n'ont cessé de croître dans la validation des organisations pour la délivrance des certificats EV et en majeure partie avec le renforcement des procédures de contrôle (validation rendue infructueuse après des échecs d'appel sur le numéro de téléphone public de l'organisme au lieu d'appeler directement le demandeur ou l'administrateur habilité déclaré dans le portail). Les campagnes d'audits aléatoires à la demande du *CA/Browser Forum*, les changements de procédures par l'autorité de certification ont pu également susciter des incompréhensions chez les administrateurs des organisations, par exemple lorsque des demandes de certificats restent suspendues sans raison apparente et aucune notification de la part de *Digicert*.

Concernant les certificats de personne, suite à la fin du support progressif de la fonctionnalité « <keygen[5]> » dans les navigateurs, il a été de plus en plus difficile de générer des certificats de personne avec *Digicert*. Ce problème généralisé a affecté également les administrateurs eux-mêmes lors de l'expiration de leur certificat demandé lors de l'authentification renforcée mise en place très majoritairement au lancement de TCS en 2015 sur le portail *CertCentral :* l'impossibilité de régénérer leur certificat bloque l'accès de l'administrateur au portail de *Digicert* et nécessite l'intervention d'un autre administrateur pour débloquer la situation en changeant notamment la méthode d'authentification.

Depuis mai 2020, il n'est plus possible de réaliser de nouvelles demandes de certificats TCS avec *Digicert* mais les révocations des certificats émis restent accessibles jusqu'à leur fin de validité[6].

3 TCS avec Sectigo depuis mai 2020

Après deux cycles de passation de marché menés en 2019 par l'association GÉANT, la société *Sectigo* a été retenue en fonction de la qualité et du prix de sa proposition. L'accord commercial est

4 Toutes les divisions et organisations dans *Digicert* n'étaient plus actives avant la migration de TCS vers *Sectigo* en avril 2020 : en effet, certaines organisations pouvaient correspondre à des organismes ou établissements qui ont plusieurs dénominations ou ont « fusionné », changé de nom, ou encore cessé d'exister légalement, ... Il a ainsi été identifié entre 340 et 400 organisations à accompagner vers le nouveau service TCS.

5 La balise HTML <keygen> permet via un formulaire HTML de générer un jeu de clés dont la clé privée est stockée dans le navigateur et la clé publique est signée à l'issue du processus et installée également le porte-clés du navigateur. Cet élément a été rendu obsolète à partir de 2016 pour des raisons de sécurité et de protection des données ; les navigateurs ont ainsi retiré les uns après les autres le support de cette fonctionnalité. Dorénavant l'utilisation de la *Web Cryptography API* [7] est recommandée pour générer une paire de clés de certificat et l'exporter facilement pour permettre une installation manuelle du certificat signé par l'utilisateur.

6 Pour les certificats serveur demandés en avril 2020 avec une validité de 2 ans, les révocations sont accessibles jusqu'à fin avril 2022. Pour les certificats de personne demandés avec une validité de 3 ans, ils pourront être révoqués dans *CertCentral* de *Digicert* jusqu'en avril 2023.

convenu dorénavant pour une durée allant jusqu'à 10 ans avec des cycles annuels allant de mai à mai d'une année sur l'autre. Comme dans les marchés précédents, une redevance annuelle est versée à GÉANT par les NREN qui adhèrent à TCS. RENATER, tout comme les NREN italien, anglais et allemand, se voient appliquer la redevance annuelle correspondant à la catégorie la plus haute (le montant des redevances varie de 1 à 10 fois par rapport à la catégorie la plus basse).

Les établissements et organismes qui adhèrent au service TCS proposé par RENATER n'ont pas de coût répercuté de cette redevance sur leurs demandes de certificats.

RENATER fournit et maintient à jour une documentation du service TCS en France [8] à destination des administrateurs des établissements ayant choisi d'adhérer au service.

En France, depuis mai 2020, 358 établissements ont choisi d'adhérer ou de renouveler leur adhésion au service TCS avec *Sectigo* auprès de RENATER. Plus de 75 000 certificats[7] ont déjà été délivrés en 2 ans d'utilisation du service TCS avec *Sectigo*.

3.1 Certificats proposés dans TCS

Différents types de certificats sont proposés dans le service TCS de RENATER avec *Sectigo* :

- **les certificats serveur** (*SSL/TLS Certificates*) à validation d'organisation (*OV - Organization Validation*) et à validation étendue (*EV - Extended Validation*) pour authentifier les serveurs et établir des sessions sécurisées avec les clients. Ces certificats ont une durée de validité d'un an.

- **les certificats de personne** (*Client Certificates*) pour l'authentification de l'usager, la signature d'e-mails… Ces certificats ont une durée de validité de 1 à 3 ans maximum ;

- **les certificats de signature de code** (*Code Signing Certificates*) pour la vérification de la source et de l'intégrité de l'application par la signature numérique d'un programme afin de prouver qu'il n'a pas été altéré ou compromis ;

- **les certificats de signature de document** (*Document Signing Certificates*) pour signer numériquement des documents de bureautiques à partir d'Adobe PdF, MS Office, LibreOffice… Ces certificats sont accessibles uniquement par une procédure spécifique de demande en dehors du portail SCM et le coût des *tokens* physiques est à prendre en compte par le demandeur. Ces certificats sont présents dans l'*Adobe Approved Trust List* [9] mais n'ont pas vocation à être utilisés dans le contexte où des certificats de signature électronique qualifiée sont nécessaires[8] ;

- **les certificats de grilles de calcul** (*Grid certificates)* pour les infrastructures distribuées de calcul : ces certificats sont présents au sein de l'IGTF (*Interoperable Global Trust Federation*). Ils ne sont pas à l'heure actuelle proposée par défaut à la communauté Éducation/Recherche française. En effet, il est recommandé aux participants français d'utiliser le service historique GRID-FR opéré par RENATER [11][9].

7 Début mai 2022, 39 700 certificats sont actifs dont 34 300 certificats serveur, 5 300 certificats de personne et 81 certificats de signature de code.

8 *Sectigo* propose depuis août 2021, des certificats conformes au règlement européen eIDAS [10]. Ces certificats ne sont pas compris dans le service TCS mais ils peuvent être commandés par les organismes demandeurs à leur frais directement auprès de *Sectigo*.

9 D'ici 2023, le service GRID-FR devrait migrer progressivement vers le service TCS. Les certificats dédiés aux grilles de calcul seront ainsi disponibles à ce moment-là dans le service TCS de RENATER.

3.2 Différents rôles dans le portail SCM de *Sectigo*

Le service TCS de RENATER avec *Sectigo* proposent 3 niveaux de comptes d'administrateurs :

- **MRAO** (*Master Registration Authority Officer*) : ce rôle est le plus haut niveau d'administration dans le portail SCM de *Sectigo*. Il est réservé uniquement aux administrateurs des NREN de chaque pays adhérant à TCS. Les MRAO gèrent l'ensemble des organisations habilitées à demander des certificats. Pour cela, les MRAO sont amenés à créer, renseigner et valider toutes les organisations, créer les administrateurs des organisations (RAO) et les accompagner… En plus de ces responsabilités, ils sont les points de contact avec GÉANT et *Sectigo* et ont pour ces derniers un accès dédié au support Premier de *Sectigo* ;

- **RAO** (*Registration Authority Officer*) : ce rôle est le niveau d'administration d'une organisation[10]. Il est réservé aux correspondants du service TCS d'un organisme. Les RAO gèrent les domaines, les certificats et les administrateurs locaux (DRAO)… qui appartiennent à cette organisation. Ils ont par délégation la possibilité de d'ajouter des domaines et de lancer la procédure de validation du contrôle du domaine (DCV). Ils peuvent ajouter des notifications spécifiques et personnaliser des modèles d'e-mail envoyés automatiquement pour leur organisation. Les RAO ont accès au support TCS de RENATER et également au support *Sectigo* de niveau 2. Les RAO peuvent créer des départements « si nécessaire » dans leur organisation : les départements sont utiles pour déléguer la gestion d'un ou plusieurs domaines/sous-domaines et les certificats associés à des administrateurs locaux d'une organisation DRAO (qui ne sont pas correspondants TCS pour l'ensemble de l'établissement) ;

- **DRAO** (*Department Registration Authority Officer*) : ce rôle correspond au niveau administrateur d'un département[11]. Les DRAO ne peuvent gérer que des domaines, certificats… qui appartiennent à ce département et ils ont gérés complètement par les RAO.

Avec *Sectigo*, certaines opérations de validation nécessitent l'intervention d'un autre administrateur pour qu'elles soient prises en compte (règle de validation « *four eyes principle* ») : c'est le cas notamment lors des demandes de certificat EV qui ne peuvent pas être validées directement par l'administrateur « demandeur ».

Dans le contexte de TCS avec *Sectigo*, les NREN ont un rôle de contrôle accru qui se positionne entre *Sectigo* et les établissements pour certaines opérations : les MRAO lancent et suivent la validation des organisations (*Triggering OV Anchor*) auprès de *Sectigo* afin que l'organisation puisse demander ensuite des certificats serveur OV et si besoin de l'approbation des demandes d'ancres EV (*Triggering EV Anchor*) afin que l'organisation puisse demander ensuite des certificats serveur EV. Toutes les validations et les contrôles sont réalisés par l'opérateur de certification *Sectigo* en suivant les recommandations du *CA/Browser Forum*.

En comparaison avec le service TCS de *Digicert*, les administrateurs des établissements ont un peu moins d'autonomie mais ils sont libérés d'une partie des processus de validation et de contrôle de leur organisation dont les processus peuvent se révéler complexes et changeants. Les administrateurs RAO peuvent ainsi gagner en efficience dans la gestion courante des demandes de

10 Le nom d'une organisation correspond au champ O « *Organization* » dans les certificats émis.

11 Le département est un concept purement interne à une organisation ou une entreprise. Le nom d'un département d'une organisation correspond au champ OU « *Organization Unit* » dans les certificats émis.

certificats en fonction des besoins de leur organisme mais ils ont toujours à gérer les demandes et le renouvellement annuel des DCV de leurs domaines.

3.3 Nouvelle procédure d'activation du service TCS pour un organisme

Dorénavant avec le nouvel accord signé entre GÉANT et *Sectigo*, il n'est plus nécessaire pour chaque établissement de signer un accord de souscription au service TCS. La nouvelle procédure d'activation du TCS se révèle ainsi être plus simple et rapide : l'activation du service et la déclaration des administrateurs du service au sein de l'établissement sont réalisés directement via le portail PASS (Portail d'Accès et de Suivi des Services) comme pour tout autre service de RENATER. Pour cela, il est nécessaire qu'un « contact référent » de l'établissement se connecte et active le service TCS dans le portail PASS (dans l'onglet « Service » puis « Services activables ») et qu'il définisse au moins un correspondant TCS. Les correspondants du service TCS sont les administrateurs « RAO » de l'organisation correspondant à leur organisme dans le portail SCM de *Sectigo*.

Dès le lancement de TCS avec Sectigo fin avril 2020, nous avons automatisé la création des organisations et des administrateurs RAO à l'aide des API de *Sectigo* : les créations et modifications sont ainsi réalisées le jour ouvré suivant de l'activation du service TCS ou de l'ajout d'un correspondant TCS dans le portail PASS. Seuls les organismes dont le service TCS a un statut « en demande » ou « actif » et dont le contrat n'est pas en cours de traitement sont ajoutés ou modifiés dans le portail SCM de *Sectigo*. Un organisme correspond toujours à une seule organisation dans *Sectigo*. La validation de l'organisation par les administrateurs MRAO de RENATER ne sera lancée que si l'organisme a bien une « existence légale », c'est à dire qu'il est possible de valider ses informations (nom, adresse, code postal, ville) depuis une source en ligne officielle (SIRENE, infogreffe…). Dans le cas de figure d'un organisme ne pouvant être validé pour utiliser directement le service TCS, ce dernier devra adhérer au service TCS via une autre organisation ou bien après correction des informations le concernant : par exemple, les laboratoires sont le plus souvent amenés à utiliser le service TCS via leur tutelle de rattachement (Université, CNRS…) car ils n'ont pas de SIREN propre.

3.4 Fonctionnalités offertes par le portail SCM de *Sectigo*

Tous les administrateurs du service TCS peuvent accéder à toutes les fonctionnalités offertes par TCS depuis le portail SCM (*Sectigo Certificate Manager*) :

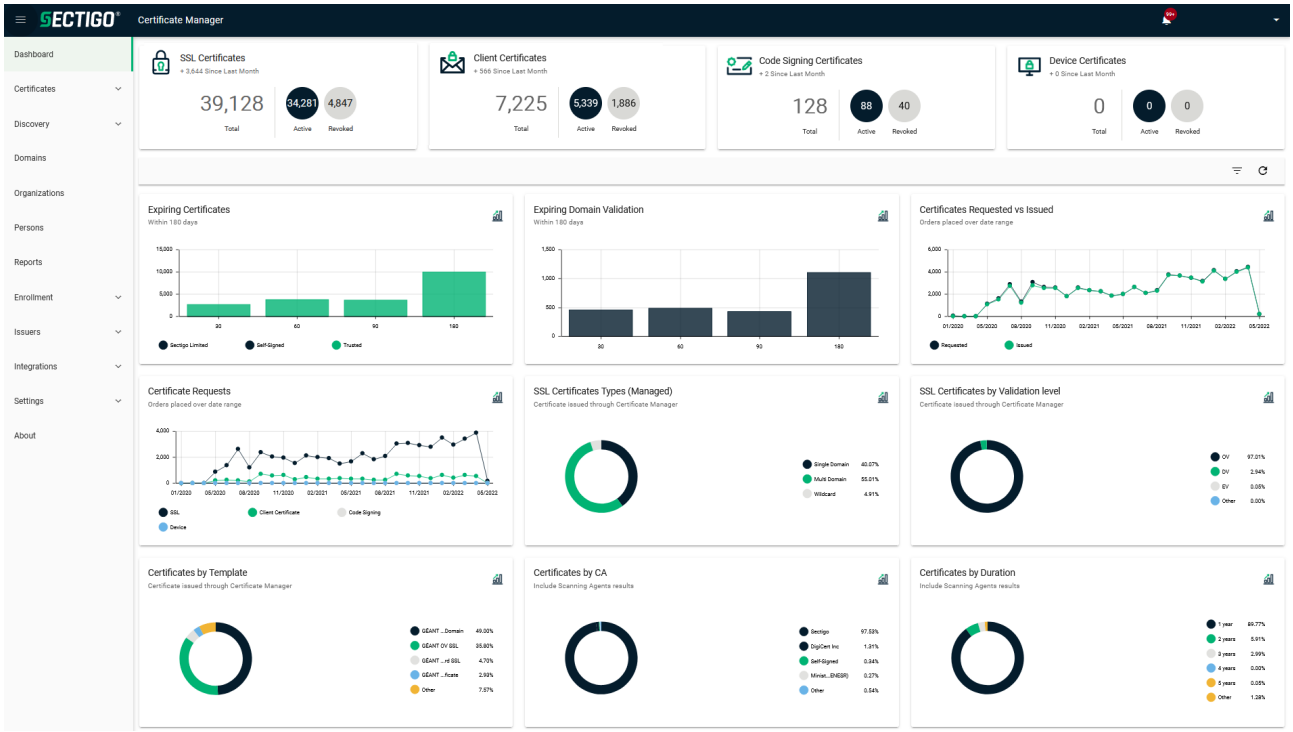

Figure 3 – Portail SCM (Sectigo Certificate Manager)

Ce portail unique est riche et simple d'utilisation ; *Sectigo* l'améliore et le fait évoluer régulièrement et il maintient des documentations et bases de connaissances détaillées pour faciliter sa prise en main. Des notifications annoncent les principaux changements au moment de la connexion de l'administrateur et également par e-mail (sur inscription). Les administrateurs ont accès dans le portail SCM à des tableaux de bord, des rapports, des outils de découverte des certificats installés, à la gestion complète de leurs organisations, départements, domaines, certificats… Ils peuvent personnaliser les notifications reçues par e-mail et paramétrer des filtres de recherche… *Sectigo* propose également des API REST, des agents à installer sur différentes plateformes et il supporte le protocole ACME (*Automatic Certificate Management Environment*) qui a été créé à l'origine et démocratisé par *Let's Encrypt* [12].

Dans le portail SCM, les MRAO peuvent « tout voir » et agir au besoin sur chacune des organisations existantes alors que les RAO et les DRAO ne voient et peuvent agir respectivement que sur leur organisation ou département.

Contrairement au portail de *Digicert* où il était possible de créer des comptes « utilisateur » ayant les seuls droits de demandes de certificats, *Sectigo* ne permet que de définir des administrateurs avec des droits de gestion avancés. Néanmoins plusieurs possibilités sont offertes aux administrateurs RAO pour permettre à leurs utilisateurs finaux de réaliser eux-mêmes des demandes de certificats TCS :

- concernant la délivrance des certificats de personne, un premier portail en *self-enrollment* avec une authentification SAML est accessible pour l'ensemble des organisations liées à RENATER ; il est utilisable par configuration dans chaque organisation[12]. En l'absence d'IdP inscrit dans la fédération eduGain, il est également possible pour les administrateurs d'inviter directement les utilisateurs depuis le portail SCM après avoir créé une « personne » et renseigné son nom, prénom et son adresse e-mail (dont le domaine est obligatoirement possédé et géré par l'organisation). Ensuite l'utilisateur pourra recevoir une invitation par e-mail qui sera valide pour demander un certificat selon le type et la durée retenue par l'administrateur.

- concernant la délivrance des certificats de serveur, les administrateurs RAO ont la possibilité d'activer un ou plusieurs portails en s*elf-enrollment* pour autoriser des demandes de certificats SSL/TLS à des utilisateurs qui ne sont pas des administrateurs RAO ou DRAO. L'authentification de l'utilisateur peut être réalisée avec SAML ou avec un code d'accès unique propre au portail créé. Une fois la demande réalisée par l'utilisateur final, elle devra approuver par un administrateur de l'organisation concernée.

4 Difficultés et solutions pour gérer les certificats

Au fil du temps, l'usage des certificats « SSL » s'est généralisé et est devenu incontournable notamment sur les serveurs pour sécuriser les échanges chiffrés via http(s), imap(s), ldap(s)… De plus en plus en de certificats sont émis chaque année. Cependant, des difficultés croissantes touchent la gestion du grand nombre de certificats et se sont accentuées ces 5 dernières années.

4.1 Des exigences de plus en plus nombreuses édictées par les « navigateurs »

Dès 2011, des incidents répétés au niveau de certaines autorités de certification publiques ont conduit les navigateurs à être de plus en méfiants et à renforcer progressivement les règles édictées aux AC publiques. Ces règles sont exprimées sous forme de recommandations définies et votées par le *CA/Browser Forum*[13] où sont représentés les principaux acteurs du marché (autorités de certification et navigateurs) [5]. Nous reportons ici quelques évolutions notables qui ont eu des effets sur les AC et par conséquent sur le service TCS avec *Digicert* ou *Sectigo* :

- depuis 2015, le protocole ***Certificates Transparency*** [13], à l'initiative de Google et adopté ensuite par Apple, a progressivement[14] été « imposés » aux AC afin qu'elles publient « au grand jour » tous les certificats publics qu'elles émettent. En surveillant les journaux de

12 Le portail SAML de délivrance des certificats clients est accessible à l'adresse https://cert-manager.com/customer/renater/idp/clientgeant. L'IdP utilisé par une organisation devra être enregistré dans la fédération eduGain et être configuré pour renvoyer les attributs *mail*, *eduPersonPrincipalName*, *eduPersonEntitlement* et *schacHomeOrganisation* au SP de Sectigo. La valeur *urn:mace:terena.org:tcs:personal-user* doit être présente dans l'attribut *eduPersonEntitlement* pour les utilisateurs autorisés à demander un certificat de personne. La valeur de l'attribut *schacHomeOrganization* correspond de préférence à un domaine de l'établissement (celui du *Scope*). Le champ *Academic code* doit être renseigné dans l'organisation concernée avec la valeur renvoyée par votre IdP dans l'attribut *schacHomeOrganization*.

13 La première version des directives applicables aux certificats EV a été définie en juin 2007 dans le document « *Guidelines for the issuance and management of extended validation certificates* ». En novembre 2011, le *CA/Browser Forum* adopte ensuite la première version des recommandations destinées à fournir des normes de sécurité minimales pour tous les certificats SSL/TLS approuvés par les navigateurs : « *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* ».

14 En octobre 2015, Google exige que les AC enregistrent les certificats dans les journaux CT publics. En avril 2018, cette exigence est généralisée par le *CA/Browser Forum* est étendue à l'ensemble des certificats OV et DV.

publication des certificats (*CT logs*), il est ainsi plus simple de vérifier si une autorité n'émet pas un certificat sans autorisation pour un domaine donné.

- en septembre 2017, le contrôle des enregistrements **DNS *Certification Authority Authorization – CAA*** [14] devient obligatoire pour les AC avant toute émission de certificat serveur[15].
- depuis 2017, les navigateurs ont annoncé deux fois une réduction de la durée de confiance des certificats serveurs publics qui était jusque-là de 3 ans maximum :
  - à partir de mars 2018, tous les nouveaux certificats serveurs sont ainsi limités à une validité de 2 ans. *Digicert* commence à mettre en place cette mesure dès 2017 ;
  - à partir du 1er septembre 2020, tous les nouveaux certificats serveurs émis sont limités à une validité de 1 an. *Sectigo* applique cette mesure le 19 août 2020.
- les procédures de validation des contrôles des domaines (DCV) avant toute délivrance d'un certificat ont également été renforcées au fil du temps et certaines méthodes de validation sont modifiées ou deviennent prohibées : par exemple, la méthode de validation HTTP/HTTPS par dépôt d'un fichier spécifique sur un serveur web devient prohibée pour la validation de domaine destiné à délivrer des certificats *wildcard*. *Sectigo* applique cette dernière mesure dès fin novembre 2021.
- les contenus des différents champs d'un certificat sont méticuleusement contrôlés : liste des noms de domaine, nom de l'organisation, ville, code postal, état, pays… Pour être en adéquation avec les dernières recommandations, *Sectigo* annonce notamment que :
  - dès septembre 2021, les informations du champ *Locality – L* (ville) ne seront plus renseignée et le champ s*tate* (état/province) sera renseigné à la place pour l'ensemble des certificats serveur nouvellement émis ;
  - dès avril 2022, le champ *Organization Unit – OU* (nom du département) va commencer à ne plus être renseigné dans certaines demandes de certificats serveur. Le 1er septembre 2022, le *CA/Browser Forum* exige que le champ *OU* soit inutilisé et obsolète pour tous les certificats nouvellement émis. Cette modification peut avoir des conséquences sur tout processus ou système qui dépend de la présence d'informations dans le champ *ou.*
- la règle « des 5 jours du *CA/Browser Forum* » impose une contrainte forte pour renouveler les certificats avant leur révocation effective si un problème a été constaté sur un certificat lors d'un audit.

Il est important de comprendre que toutes les autorités de certification publiques sont concernées par ces « règles ». Dans le contexte du service TCS de RENATER avec *Sectigo*, les MRAO veillent à ce que les validations concernant les organisations respectent bien les recommandations courantes du *CA/Browser Forum* : ils centralisent la gestion et renseignent directement les informations liées aux organisations. Concernant les validations des contrôles des domaines, elles sont déléguées aux RAO ; néanmoins les MRAO sont amenés à vérifier si les domaines déclarés par une organisation

15 La définition d'un enregistrement DNS CAA permet au propriétaire d'un nom de domaine d'autoriser une ou plusieurs autorités de certification à émettre des certificats pour le domaine concerné (toutes les autres seront exclues). Si aucun enregistrement n'est défini pour un domaine alors toutes les autorités sont autorisées tacitement à émettre des certificats pour ce domaine.

sont effectivement possédés légalement par elle (en consultant les bases *whois* notamment). En cas d'enfreinte à cette règle, la délégation de gestion des DCV peut être retirée à l'organisation.

4.2 Des conséquences en cas de non-respect des « recommandations »

Le non-respect des recommandations fixées par le *CA/Browser Forum* conduit a des conséquences allant de la simple demande de **révocation d'un ou plusieurs certificats jusqu'au « bannissement » de l'autorité de certification** dans un ou l'ensemble des navigateurs si la chaîne de confiance de l'AC[16] est remise en cause. Pour cela, les « représentants des navigateurs » mènent directement des audits ou demandent également aux AC des audits de plus en plus réguliers et stricts : ces audits peuvent conduire à la revalidation des informations des organisations, des domaines, des contacts habilités mais également à des révocations de certificats plus fréquentes en cas de manquements. A titre d'exemples, nous reportons quelques évènements marquants ayant touché le service TCS ou d'autres autorités ces dernières années :

- fin 2018, le *CA/Browser Forum* vote la fin de la confiance des certificats serveur contenant le caractère « _ » dans les noms de domaine. Dès début 2019, *Digicert* commence à appliquer cette mesure et à révoquer tous les certificats concernés ;
- en juin 2019, *Digicert* se voit contraint par le *CA/Browser Forum* de mener une campagne de revalidation des organisations et des domaines liés à la délivrance de certificats EV. Le renforcement des contrôles de validation des demandes de certificats EV conduit alors à de nombreuses demandes qui restent bloquées pour les organisations utilisant TCS si la procédure « EV » n'est pas menée complètement : elle est le plus souvent bloquée au moment de l'étape de vérification de l'identité du demandeur via un appel téléphonique sur le numéro public de l'organisme ;
- en mars 2020, *Let's Encrypt* révoque 3 millions de certificats suite à des problèmes de sécurité dans la validation des domaines (un bug dans l'implémentation de CAA) ;
- en juillet 2020, suite à différentes campagnes d'audit insatisfaisantes, tous les certificats EV de certaines AC dont celle opérée par *Digicert* pour TCS jusqu'à avril 2020 (chaîne de certification intermédiaire *TERENA SSL High Assurance CA 3*) sont à révoquer. Les certificats concernés, s'ils sont toujours nécessaires, doivent être renouvelés en moins d'une semaine chez *Sectigo*[17] au lieu de *Digicert*. Plus de milles certificats ont été concernés pour les organisations utilisant TCS en France.
- de l'été 2020 à début 2021, plusieurs campagnes d'audits sont menées sur les contenus des champs renseignés dans les certificats émis par différentes AC dont *Sectigo* : des erreurs « mineures » d'enregistrement majoritairement dans les champs *State* ou *Locality* ont été

16 Suite à un piratage et à l'émission de certificats frauduleux *wildcard* ciblant Google, Yahoo, Wordpress., AOL… l'autorité de certification *DigiNotar* a été bannie définitivement des principaux navigateurs et l'opérateur a cessé d'exister à partir de là. En 2015, Google bannit certaines autorités de Symantec (héritée de Thawte) car elles n'étaient pas conformes au protocole *Certificate Transparency* : les autorités de certification doivent se soumettre à un système auditable et public d'enregistrement de tous les certificats. Les activités de certification de Symantec ont été revendues en 2017 et elles sont gérées depuis par *Digicert*.

17 Il a été recommandé par RENATER de demander en priorité des certificats OV en premier lieu car les demandes de certificats EV peuvent « être bloquées » par la procédure EV plus contraignante et plus longue à mener avant la délivrance d'un certificat. De plus, la différenciation entre certificats OV et EV dans les navigateurs est ténue pour un utilisateur final depuis la suppression progressive de tous les éléments « visuels » dans les principaux navigateurs (le « nom de l'organisation », le « petit cadenas vert » dans la barre de navigation ont été supprimés avant 2020).

identifiées et ont conduit à différentes vagues de revalidation/réémission avant la révocation des certificats concernés par ces erreurs d'enregistrement (quelques centaines pour TCS).

- en janvier 2022, *Let's Encrypt* révoque 2 millions de certificats en 2 jours suite à un problème dans le code implémentant la méthode de validation « *TLS Using ALPN* ».

4.3 Des changements et expirations des certificats des chaînes de certification

Une dernière difficulté dans la gestion et l'utilisation des certificats provient des **changements ou expirations des certificats racines ou intermédiaires des chaînes de certification** qu'il convient d'anticiper sur les serveurs ou clients utilisant des certificats. Un premier cas de figure est relatif à chaque renouvellement du service TCS[18] avec un nouvel opérateur : la chaîne de certification est amenée nécessairement à changer et peut avoir des spécifications différentes « plus récentes et plus sécurisées » (par exemple, l'utilisation de signature avec l'algorithme *SHA384WITHRSA* dans TCS avec *Sectigo* au lieu de *SHA256WITHRSA*[19] avec *Digicert*).

Les certificats racines ou intermédiaires ont comme tout certificat une durée de validité (jusqu'à plusieurs dizaines d'années) ; leur expiration a un effet sur l'ensemble de la chaîne de certification : si un certificat de la chaîne est expiré, les certificats signés avec ne sont plus de confiance. Les AC doivent anticiper l'expiration en mettant en place des mécanismes de publication de nouveaux certificats en bien amont de l'expiration et en recourant également à la certification croisée (*Cross Signing*) qui consiste à signer un certificat selon des chaînes de confiance alternatives : les certificats intermédiaires et ou racines y ont donc « plusieurs versions avec un même nom » mais sont signés avec des certificats différents. Ces mécanismes permettent de limiter les impacts lors de l'expiration mais ils peuvent induire également des incompréhensions (certificats portant le même nom et plusieurs chaînes de confiance différentes).

Malgré ces précautions, au moment de l'expiration d'un certificat racine, certains systèmes anciens non mis à jour ou qui possèdent leur propre base de certificats peuvent rencontrer des problèmes car ils ne « connaissent » pas le nouveau certificat racine et ainsi ils ne sont plus capables de continuer à valider les signatures des certificats. Ce problème a été rencontré notamment fin septembre 2021 avec l'expiration du certificat racine *IdentTrust DST Root CA X3*[20] utilisé par *Let's Encrypt* qui a posé des problèmes d'accès internet sur des dispositifs anciens non mis à jour et également à moindre échelle en mai 2020 avec l'expiration de la racine *AddTrust External CA Root*[21] héritée de *Comodo* et utilisée par *Sectigo*.

Idéalement il est conseillé de veiller à maintenir à jour les différentes plateformes de son parc, surveiller les expirations des certificats utilisés (feuille, intermédiaire et racine) et le cas échéant

18 Par exemple, lors du passage de *Digicert* à *Sectigo* en 2020, les certificats serveur OV émis avec *Digicert* sont signés par « *TERENA SSL CA 3* » (signée elle-même par « *DigiCert Assured ID Root CA* ») alors que ceux émis par *Sectigo* sont signés par « *GEANT OV RSA CA 4* » (signée elle-même par « *USERTrust RSA* »).

19 Ce changement a nécessité la mise à disposition d'un profil de certificat alternatif, « *Elite SSL (SHA256*) » de Sectigo, afin que les organisations ayant des systèmes trop anciens pour supporter l'algorithme *SHA384WITHRSA* puissent continuer à réaliser des demandes de certificats de serveur avec TCS le temps de les remplacer.

20 Pour continuer à fonctionner, les anciens systèmes nécessitent l'installation du certificat racine *DST Root CA X3* (renommée ensuite en *TrustID X3 Root*) prévu pour rétrocompatibilité ; les systèmes plus récents peuvent utiliser le certificat racine plus récent *ISRG Root X1*.

21 Les anciens systèmes utilisent pour continuer à fonctionner le certificat racine *Comodo CAA Certificate Services* signant le certificat intermédiaire *USERTrust RSA CA* ; les systèmes plus récents peuvent utiliser *USERTrust RSA CA* en tant que certificat racine.

installer les certificats manquants afin de ne pas subir d'interruption de service ou « d'alertes de sécurité » dans les navigateurs.

4.4 Vers une automatisation de la gestion des certificats

Dans ce contexte où les renouvellements des certificats sont à mener de plus en plus rapidement, il est nécessaire d'être organisé, réactif et d'avoir une bonne visibilité tout au long du cycle de vie des certificats. Différentes solutions permettant de centraliser et/ou d'automatiser la gestion et le traitement des certificats peuvent limiter les actions humaines et conduire à réagir plus efficacement afin de renouveler un grand nombre de certificats rapidement.

Une première piste consiste à centraliser la gestion de ces certificats sur des systèmes dédiés ou/et à concentrer le traitement et le support sur des équipements de *SSL Offloading*[22] et en veillant par la même occasion à contrôler le nombre de certificats serveur demandés : par exemple, en utilisant des certificats *wildcard* ou multi-domaines.

Une seconde piste est d'industrialiser et d'automatiser la gestion des certificats. *Sectigo* supporte différentes solutions pour faciliter et automatiser la gestion des certificats :

- **Utilisation des API REST de *Sectigo*** : ces API permettent de réaliser la majorité des opérations du portail SCM et notamment la gestion et la demande de certificats. Pour réaliser une demande pour un nouveau certificat SSL en ayant généré la CSR au préalable, il suffit d'envoyer une requête POST à l'API /api/*ssl/v1/enroll* de *Sectigo* et ensuite de récupérer le certificat signé via une requête GET à */api/ssl/v1/collect/{sslId} ;*
- **Intégrations dédiées ou spécifiques** : agents dans le monde Microsoft, intégration des constructeurs (F5, *ServiceNow*...), support des principaux outils de *DevOps* (*Chef*, *HashiCorp Vault*, *Jenkins*, *Ansible*, *Kubernetes*, *Puppet*, *Docker*...), SCEP (*Simple Certificate Enrollment Protocol*)…
- **Utilisation du protocole ACME**.

Le protocole ACME (*Automatic Certificate Management Environment*) [15] a été créé à l'origine pour le service *Let's Encrypt* [12] en 2015 afin d'automatiser les relations entre une machine et l'autorité de certification chargée de lui délivrer des certificats. Ce protocole a largement été adopté et est maintenant la solution la plus répandue pour automatiser la gestion des certificats serveur. Le client le plus connu est *certbot* [16] ; un exemple complet de configuration est décrit dans la documentation du service TCS de RENATER [11]. À la différence de *Let's Encrypt* qui délivre des certificats conformes au standard DV (*Domain Validation*) et valides quelques mois, le protocole a été implémenté par *Sectigo* afin de délivrer également des certificats OV (*Organization Validation*) et EV (*Extended Validation*) dont la durée de validité est d'un an. De plus, *Sectigo* permet de gérer la création de comptes ACME, la liste des domaines autorisés directement depuis le portail SCM. Des cas d'usage concrets de l'utilisation d'ACME avec *Sectigo* dans le contexte de TCS ont été exposés lors d'un *Webinar* organisé par GÉANT le 13 avril 2021 [17].

Actuellement entre 15 et 30 % des certificats SSL émis par les organisations avec le service TCS de RENATER le sont avec le protocole ACME.

22 Le *SSL Offloading* est un processus de suppression du chiffrement basé sur SSL au niveau du trafic entrant afin de soulager un serveur web de la charge de traitement du déchiffrement et/ou du chiffrement du trafic envoyé via SSL. En général, le traitement est déchargé sur un système distinct conçu spécifiquement pour l'accélération SSL ou la terminaison SSL.

Bibliographie

[1] GÉANT Association, Trusted Certificates Service Wiki, https://wiki.geant.org/display/TCSNT/Trusted+Certificate+Service+Home.

[2] Aumont S., Gross C. et Leca P. Infrastructures de Gestion de Clés et Certificats X500. Dans tutoriels du congrès JRES2001, Lyon, décembre 2001 ; https://2001.jres.org.

[3] Guezou J.-F., Launay D. et Aumont S. SCS est mort, vive TCS !. Dans Actes du congrès JRES2009, Nantes, décembre 2009 ; https://2009.jres.org/soumission/papers/render/pdf/76.pdf.

[4] Gydé L. Tour d'horizon des services de RENATER. Dans Actes du congrès JRES2011, Toulouse, novembre 2011 ; https://2011.jres.org/archives/191/paper191_article.pdf.

[5] Certification Authority Browser Forum (CA/Browser Forum), Certification Authorities, Web Browsers, and Interested Parties Working to Secure the Web ; https://cabforum.org.

[6] Turpin M. Trusted Certificate Service - Le service de certificats de RENATER. Dans Actes du congrès JRES2015, Montpellier, décembre 2015 ; https://conf-ng.jres.org/2015/document_revision_2426.html?download.

[7] W3C, Web Cryptography API, W3C Recommendation. 26 janvier 2017 ; https://www.w3.org/TR/WebCryptoAPI/.

[8] RENATER, Documentation du service TCS de RENATER ; https://services.renater.fr/tcs.

[9] Membres Adobe Approved Trust List ; https://helpx.adobe.com/ch_fr/acrobat/kb/approved-trust-list1.html.

[10] ANSSI, Le règlement « eIDAS » ; https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas.

[11] RENATER, Documentation du service Grid-FR de RENATER ; https://services.renater.fr/ssi/grid-fr.

[12] Let’s Encrypt, https://letsencrypt.org.

[13] IETF, RFC 6962 - Certificate Transparency. juin 2013 ; https://tools.ietf.org/html/rfc6962

[14] IETF, RFC 6844 - DNS Certification Authority Authorization (CAA) Resource Record. janvier 2013 ; https://datatracker.ietf.org/doc/html/rfc6844.

[15] IETF, RFC 8555, Automatic Certificate Management Environment (ACME). mars 2019 ; https://datatracker.ietf.org/doc/html/rfc8555.

[16] EFF, certbot ; https://certbot.eff.org.

[17] GÉANT Association, TCS Webinar: ACME. 13 avril 2021 ; https://wiki.geant.org/display/TCSNT/TCS+Training.