Impacts organisationnels du déploiement des certificats de personne TCS

Jean-François Guezou
RENATER
CRI campus de Beaulieu
263 ave Général Leclerc
CS 74205
35 042 RENNES Cedex

Résumé

Le service Terena Certificate Service (TCS) délivre aux établissements d'enseignement supérieur et aux organismes de recherche européens des certificats électroniques reconnus par la majorité des navigateurs sans configuration spécifique.

Ce service est déployé en France par RENATER depuis octobre 2009 dans sa version certificats serveur et depuis novembre 2010 dans sa version certificats de personne. Ces derniers ont pour vocation la couverture des besoins en signature et chiffrement de courriels ou d'authentification des usagers.

L'infrastructure et l'organisation mises en place pour délivrer ces certificats visent à simplifier au maximum les démarches de l'utilisateur final pour les obtenir. De cette simplicité naissent non seulement des responsabilités pour les établissements qui déploient ce service, mais aussi des contraintes. Techniques de prime abord, ces contraintes ne sont pas sans conséquence organisationnelle plus ou moins importantes. Elles méritent quelque attention.

Lors de la souscription au service, l'établissement s'engage formellement sur les procédures qu'il va mettre en place pour assurer le maintien du niveau de confiance que l'on peut accorder aux certificats. Celles-ci ont des répercussions organisationnelles plus ou moins importantes selon les usages choisis, authentification, signature ou chiffrement.

Cette contribution met en lumière des points d'attention à prendre en considération dans un projet de déploiement du service.

Mots clefs

TCS, IGC, PKI, certificats

1 Introduction

TERENA Certificate Service (TCS)[1] est un service européen délivrant des certificats électroniques reconnus par la majorité des clients sans configuration spécifique. Déployé en France par RENATER[2], ce service connaît un grand succès dans sa version certificats serveurs. On dénombre aujourd'hui près de 10 000 certificats délivrés dans notre communauté pour 340 établissements ou organismes différents. Ce succès s'explique, en premier lieu, par la réponse apportée à un réel besoin, par sa gratuité et la simplicité d'accès au service, mais aussi par la facilité d'obtention des certificats par les administrateurs de serveurs.

Depuis novembre 2010, TCS propose en plus de délivrer des certificats de personne utilisables pour la signature ou le chiffrement des courriels ou encore l'authentification[3]. Ici aussi, la facilité avec laquelle l'utilisateur final obtient son certificat est privilégiée. Cependant, le déploiement du service dans un établissement nécessite quelque attention.

Comme dans toute infrastructure de gestion de clés (IGC), les processus sont distribués et les intervenants multiples. L'ensemble est décrit dans un document regroupant la politique de certification (CP) et la Déclaration des Pratiques de Certification (DPC) [4] que tous les intervenants s'engagent à respecter, créant par là même un cadre de confiance. La confiance naît notamment de la

[1] TERENA : association européenne des réseaux nationaux pour l'éducation et la recherche (NREN) dont RENATER est l'un des membres. http://www.terena.org/

[2] http://www.renater.fr/spip.php?rubrique275

[3] http://www.renater.fr/spip.php?rubrique330

vérification d'un certain nombre de prérequis directement ou indirectement imposés par la DPC. Techniques de prime abord, ces prérequis peuvent engendrer des conséquences organisationnelles plus ou moins contraignantes pour l'établissement souscrivant au service, selon le mode d'alimentation du référentiel d'identité et le type d'usage retenu pour les certificats.

Pour chaque engagement, formellement pris par l'établissement souscripteur, il convient d'en cerner les répercussions organisationnelles et, selon les usages choisis, authentification, signature ou chiffrement, de détailler les mesures à mettre en place pour s'assurer du maintien du niveau de confiance que l'on accorde à ces certificats.

2 La hiérarchie de confiance

La hiérarchie de confiance, définie dans la DPC, prévoit qu'un établissement souscrivant au service TCS certificats de personne assume la responsabilité d'Autorité d'Enregistrement (AE). Cela signifie que l'établissement désigne lui-même les personnes habilitées à demander un certificat et en garantit l'identité. Cette garantie passe par le contrôle en face à face d'une pièce d'identité de la personne et la validation du courriel qui lui est associé. Simple à respecter, si ce contrôle est effectivement opéré, et a toujours été systématiquement opéré lors de l'arrivée d'une nouvelle personne dans l'établissement, cette clause risque fort, dans le cas contraire, de restreindre la population visée. Difficile en effet d'organiser ce contrôle d'identité à grande échelle. Si le contrôle ne couvre pas toutes les personnes, se pose alors la question de la manière de distinguer les personnes dont on a vérifié l'identité de celles pour lesquelles cela n'a pas été fait. Le référentiel d'identité de l'établissement est un bon candidat pour accueillir cette information à condition d'accorder une grande attention à l'efficience des procédures de retrait des personnes ayant quitté l'établissement. Un contact local, responsable du déploiement de ce service et désigné opérateur d'autorité d'enregistrement, s'assure du bon déroulement de ces opérations.

De la délégation d'autorité d'enregistrement découle la confiance placée dans le fournisseur d'identité de l'établissement, lui-même impérativement inscrit à la Fédération Education-Recherche[5]. C'est en effet le fournisseur d'identité qui qualifie l'usager se connectant au portail de gestion des certificats. À cet effet, le fournisseur d'identité propage, en plus des attributs d'identification classiques[6], un attribut dynamique[7] indiquant formellement l'autorisation accordée à la personne d'obtenir un certificat. L'autorisation ne doit être accordée que sous conditions, notamment la vérification d'identité en face à face et la validation du courriel.

Il est par conséquent impératif, quel que soit le type d'usage prévu des certificats, de s'intéresser au mode d'alimentation du référentiel d'identité. Il faut s'assurer qu'il pourra être un bon support pour l'autorisation donnée aux personnes de demander un certificat.

3 Le processus de distribution

Les certificats distribués sont des certificats de type X509 d'une durée de validité de 3ans[8]. Ils peuvent être installés dans différents clients (navigateurs ou clients de messagerie) afin d'être utilisés pour signer des messages électroniques ou s'authentifier auprès des applications prévues à cet effet (des serveurs web par exemple).

Les certificats sont délivrés depuis un portail mutualisé opéré par TERENA (Confusa[9]). La procédure d'accès au portail demande une authentification via la fédération Education-Recherche, puis analyse la valeur de l'attribut dynamique propagé par le fournisseur

[4] Plus connues sous le terme anglais CP/CPS. Le document est accessible en ligne : http://www.terena.org/tcs/repository

[5] http://fedaration.renater.fr

[6] EduPersonPrincipalName, DisplayName, Organization, Email.

[7] EduPersonEntitlement. Pour son utilisation, consulter : https://federation.renater.fr/docs/fiches/entitlement

[8] L'autorité de certification « *TERENA personal CA* » signe les certificats. C'est une autorité fille de *« UTN-USERFirst-Client Authentication and Email* », autorité de certification de COMODO, elle-même signée par l'autorité racine « *AddTrust External CA Root* ».

[9] https://tcs-personal-portal.terena.org/

d'identité du visiteur. C'est sur la valeur de cet attribut que le portail discrimine les utilisateurs autorisés ou non à demander un certificat.

La valeur de l'attribut dynamique est soit affectée directement dans les fichiers de configuration du fournisseur d'identité soit calculée sur la base du résultat d'une requête effectuée par le fournisseur d'identité auprès du référentiel d'identité. Sous le contrôle de l'opérateur d'enregistrement, une intervention du gestionnaire du fournisseur d'identité est donc nécessaire.

4 L'assistance aux usagers

Le portail de distribution des certificats facilite l'obtention des certificats. La demande et l'installation du certificat s'opèrent automatiquement depuis le navigateur du demandeur. Cependant, selon le système d'exploitation du poste utilisé, des complexités peuvent naitre des outils logiciels dans lesquels les certificats doivent être installés. En outre, pour un même logiciel, les procédures ou messages affichés peuvent différer d'une version à l'autre. Dans d'autres cas, notamment celui de la suite logicielle Mozilla[10], le logiciel s'affranchit du magasin de certificats du système d'exploitation utilisant son propre magasin. Ces complexités peuvent dérouter les utilisateurs non familiarisés avec ces technologies.

Le support aux usagers est du ressort des établissements. Au-delà de l'information sur le service, il convient donc de bien appréhender les besoins d'assistance à la configuration des logiciels clients utilisés. Selon les populations cibles, des formations peuvent aussi s'avérer nécessaires. Il est tout aussi important de veiller à la sensibilisation aux bonnes pratiques d'usage des certificats, notamment aux règles de protection, de conservation et d'archivage de ceux-ci. A minima une documentation en ligne facilement accessible et un courriel de support sont à déployer.

5 Le chiffrement

Parmi les usages techniquement autorisés des certificats TCS, figure le chiffrement. Favoriser leur usage dans ce cadre peut sembler une bonne alternative au déploiement d'un produit spécifique de gestion du chiffrement. Cependant, par nécessité interne, mais aussi pour se conformer à la législation française, le chiffrement oblige à la mise en place d'un séquestre pour garantir les possibilités de recouvrement. Or, le séquestre n'est organisé ni par TERENA ni par RENATER. Cette charge revient donc à l'établissement. Celui-ci se heurtera à une difficulté liée à leur mode de distribution dit décentralisé : l'utilisateur obtient lui-même, directement, ses certificats depuis le portail Confusa mis en œuvre par TERENA à cet effet. Pour alimenter un séquestre, il faut donc, en premier lieu, être informé de l'obtention d'un nouveau certificat, éventuellement par une démarche volontaire du détenteur. Il faut ensuite obtenir les bi-clés auprès de celui-ci dans le cadre d'une procédure sécurisée. Reste, bien entendu, la gestion du séquestre à organiser.

Il ne faut pas occulter la facilité avec laquelle il est possible de chiffrer un message dans la plupart des clients de messagerie, bien souvent une simple case à cocher. On en revient ici à la bonne information des utilisateurs qui, sauf si un séquestre est organisé, devront soit détruire après lecture les messages reçus chiffrés, soit veiller à ne les conserver qu'en clair.

6 Conclusion

Autant le déploiement du service TCS certificats serveur ne pose pas véritablement de difficultés, autant le service TCS certificats de personne demande une approche en mode projet. Au vu des contraintes organisationnelles générées, il est sans doute préférable de l'envisager uniquement dans le cadre d'un projet nécessitant ce déploiement et d'en limiter la portée en ciblant les usages. La limitation des usages peut avoir pour effet de restreindre la population concernée, réduisant ainsi les contraintes organisationnelles inhérentes. Le portail Confusa simplifie les démarches de l'utilisateur légitime pour obtenir un certificat. Il ne faut pas faire perdre de vue que cette simplicité provient de la grande attention portée, en amont, aux procédures d'autorisation.

[10] Thunderbird, Firefox.

Le service TCS certificats de personne n'a pas vocation à répondre à l'ensemble des besoins de notre communauté. Il a le mérite de proposer une solution opérationnelle distribuant des certificats reconnus sans configuration spécifique. l'IGC/A [11], autorité racine gouvernementale, ne pourra répondre à nos besoins que si se déploie, à l'instar d'autres Ministères, une autorité de certification pour le Ministère de l'Enseignement Supérieur et de la Recherche signée par elle.

[11] Autorité racine opérée par l'ANSSI. HTTP://www.ssi.gouv.fr/igca