Autorité de certification (pour une IGC) CNRS-Test administrée par l'UREC

Jean-Luc Archimbaud

Autorité de certification CNRS-Test administrée par l'UREC

Jean-Luc Archimbaud Directeur technique de l'UREC
Chargé de mission sécurité réseaux CNRS
16/3/2000

Cet article expose les raisons qui ont conduit à la mise en service d'une plate-forme de test d'une autorité de certification pour le CNRS (http://www.services.cnrs.fr/ca/), d'un mode opératoire de celle-ci et des conclusions que l'on est susceptible d'en tirer.

On se reportera à l'article de Nicole Dausque «Infrastructures de gestion de clefs » qui sera prochainement en ligne à l'URL http://www.urec.fr/securite/articles/IGC.pdf, pour une présentation générale de ces infrastructures.

Les besoins de certificats au CNRS

Un certificat est l'équivalent électronique d'une carte d'identité ou d'un passeport qu'un utilisateur peut fournir comme preuve de son identité. Il contient aussi les informations nécessaires pour envoyer des données chiffrées à cet utilisateur, donc apporte un service de confidentialité. Il peut aussi être utilisé par un serveur Web pour prouver son identité et pour chiffrer les échanges avec ce serveur.

Les besoins d'utilisation de certificats existent déjà au CNRS comme le montrent les exemples suivants.

Si le Directeur Général du CNRS et chaque Délégué régional avaient un certificat, **toutes les notes administratives pourraient être signées électroniquement de manière fiable et donc diffusées par messagerie électronique**, sans ambiguïté ni sur leur origine, ni sur leur intégrité. Cela pourrait être étendu à tous les responsables de l'organisme, donc toutes les notes officielles pourraient être envoyées dans le courrier électronique. Je vous rappelle qu'actuellement l'origine d'un message électronique (le « From ») ne prouve rien, il est très facile de la falsifier, et donc que toute diffusion officielle ne peut pas se faire sur ce media dans l'état actuel de son utilisation.

Dans la communauté de la recherche, les demandes commencent à arriver. **Certains chercheurs** nous ont déjà réclamé un certificat pour communiquer avec leurs homologues étrangers.

Bernard Perrot, responsable sécurité de l'**IN2P3**, prévoit que les chercheurs de l'Institut vont très prochainement avoir besoin de certificats dans le cadre de collaborations internationales. Il craint que les chercheurs français ne s'adressent alors à des organismes étrangers - en tout cas extérieurs au CNRS - pour obtenir ces cartes d'identité, et qu'ainsi l'IN2P3 n'ait plus aucune maîtrise de cette autorité dont l'indépendance vis-à-vis de critères nationaux ne sera pas garantie. Il projette la mise en service d'une infrastructure de certification au sein de l'IN2P3 avant l'été 2000, cohérente avec les initiatives du CNRS dans le domaine et en collaboration étroite avec l'UREC.

L'**INIST** a signé un accord avec l'éditeur ELSEVIER pour permettre aux laboratoires d'un Département CNRS d'accéder aux revues scientifiques en ligne de cet éditeur. Pour identifier l'utilisateur autorisé à accéder aux revues électroniques, un mécanisme basé sur les adresses IP et des couples nom-mot de passe a été mis en oeuvre. Souhaitant faire évoluer ce mécanisme, l'INIST nous a contacté pour essayer de trouver une solution plus évolutive,

pérenne et pouvant être étendue à l'ensemble des laboratoires pour les services qu'il souhaite mettre à disposition du CNRS. Pour nous, l'utilisation de certificats est une solution évidente.

A moindre échelle, dès à présent certains groupes qui l'on coordonne à l'UREC auraient besoin d'échanges sécurisés : **les coordinateurs régionaux sécurité** - 30 personnes environ - chargés entre autres de la diffusion du produit Internet Scanner d'ISS, qui reçoivent par courrier électronique classique les clés d'activation de ce produit, clés qui devraient être confidentielles ; et le groupe des **correspondants sécurité laboratoire** CNRS (170 personnes environ) qui reçoivent les avis des CERTs sans aucune garantie ni sur l'origine, ni sur l'intégrité de ces messages.

Certaines applications de gestion mises en place par la DSI ont déjà des mécanismes de sécurisation. Mais elles ne sont pas basées sur des certificats (faute de produits disponibles lors de la mise en œuvre) et il y a souvent autant de mécanismes (donc de mots de passe…) que d'applications. **Il faudrait maintenant étendre cette sécurisation à toutes les applications de gestion et arriver à une approche globale pour avoir une manière unique d'authentifier les utilisateurs et les serveurs, utilisable par toutes les applications actuelles ou futures**. Anticipant peut-être une démarche nationale, la Délégation d'Aquitaine a d'ailleurs déjà mis en place une diffusion de certificats de personnes pour une communauté d'agents administratifs restreinte.

Ces besoins ne sont pas spécifiques au CNRS : tous les acteurs commerciaux de l'Internet, par exemple, sont demandeurs et poussent à la mise en place de certificats à tous les niveaux. Il n'y a qu'à feuilleter la presse informatique - et même grand public - pour trouver de nombreux articles sur la question.

La sécurisation des applications Internet

La demande de sécurisation n'est pas récente au CNRS. De plus, depuis plusieurs années, des logiciels permettent d'avoir des communications électroniques (messagerie, Web) avec une authentification et une confidentialité fortes. Nous avons néanmoins attendu avant de faire des recommandations car aucun produit ne répondait à nos deux contraintes : reposer sur les logiciels clients que l'on utilise (Netscape, Internet Explorer ou Eudora) et permettre de communiquer avec d'autres personnes extérieures à l'organisme (c'est-à-dire avec des produits concurrents). Ceci les disqualifiait d'office, la recherche ne travaille pas en vase clos.

Aujourd'hui **un ensemble cohérent de standards Internet existe qui permet d'utiliser des couples de clés privée-publique associés à des certificats pour assurer l'authentification, l'intégrité et la confidentialité des principales applications et modes de transports d'information de l'Internet**. Ainsi les protocoles **IPsec** permettent de chiffrer tout le trafic réseau entre deux équipements de communication ; le protocole **S/MIME** dans la messagerie électronique peut garantir l'origine et l'intégrité d'un courrier avec une signature infalsifiable et permet de chiffrer le texte du message ; les protocoles **HTTPS** et **SSL** permettent de limiter l'accès à des pages Web à certains utilisateurs (sans besoin de gestion de mots de passe et de procédures complexes) et peuvent garantir la confidentialité lors du transfert des pages,…

Ces standards sont implémentés dans les outils que nous utilisons comme Netscape et Internet Explorer. Cliquez sur l'icône *Security* de Netscape pour en avoir la preuve. A noter que cela ne veut pas dire que ces fonctions sont faciles d'emploi pour un utilisateur non spécialiste, ni que les produits fassent vraiment ce qu'ils prétendent faire dans leurs fonctions de sécurité !

Les mécanismes mis en jeu reposent sur l'utilisation du chiffrement asymétrique avec des certificats. Concrètement, **il faut au moins un certificat par utilisateur et par serveur Web**.

Quelle autorité de certification ?

Un certificat, comme une carte d'identité ou un passeport, est délivré par une autorité (de certification) qui garantit sa validité.

Techniquement, cette autorité peut être n'importe quelle société ou organisme. Sur l'Internet, il n'existe pas de gouvernement qui délivre des certificats, ni d'organisations structurées et indépendantes comme celles qui affectent les numéros IP ou les noms de domaine. De nombreuses sociétés commerciales se sont déjà lancées dans ce business qui va être très lucratif. On voit très bien le risque encouru par un organisme dont la carte d'identité des agents aurait été attribuée par une autorité ni habilitée, ni contrôlée par lui-même. **Il faut donc bien choisir son autorité de certification**.

Plusieurs solutions sont (et seront) possibles :

- **Utiliser les autorités commerciales** qui existent déjà comme Verisign, GlobalSign, American Express, … Les navigateurs sont déjà configurés en standard pour « faire confiance » à certaines. Déroulez les menus *Security-Certificates-Signers* pour avoir la liste des autorités reconnues par Netscape (rassurez vous, si vous ne voulez plus les agréer un menu Netscape permet de les supprimer). En s'appuyant sur ces sociétés :
  - On devient dépendant d'une structure commerciale. Qui plus est, cette structure a des chances d'être étrangère. Dans la soixantaine d'autorités « reconnues » par Netscape, listées avec les menus ci-dessus, aucune n'est française par exemple.
  - On doit acheter chaque certificat, avec une redevance annuelle. Le coût est loin d'être négligeable (de l'ordre de 200 F / an pour une personne par exemple).
- **Attendre la mise en place d'une autorité au niveau du ministère**. Aucune autorité opérationnelle pour le CNRS n'est annoncée à court terme. A notre connaissance, des projets existent, mais pour les rectorats.
- **Décider dès à présent de mettre en place ce service au CNRS**, avec nos moyens propres, ou en sous-traitant tout ou partie de ce service à une société externe. Hormis les problèmes de financement et/ou de moyens humains, nous n'avons aucune expérience dans la réalisation d'un tel service, ce qui va rendre périlleuse l'écriture d'un cahier des charges. Côté utilisateur, nous ne savons pas si les produits grand public cités ci-dessus sont vraiment utilisables facilement, ni si on peut leur faire confiance. Il semble donc prématuré de lancer l'opération dès aujourd'hui.

Quelque soit l'autorité de certification choisie, il faut résoudre un autre problème. Comme il existe un circuit de procédures pour délivrer des cartes d'identité, il faut mettre en place l'équivalent. Il faut ainsi décider qui va recueillir et vérifier les informations données par un agent CNRS lorsqu'il va demander un certificat, qui va créer le certificat, qui va le lui délivrer, pour quelle durée, où va-t-il être stocké, où va-t-on pouvoir récupérer les certificats des autres agents, … **Il faut définir ce que l'on appelle une architecture de gestion de ces certificats** (PKI Public Key Infrastructure ou IGC Infrastructure de Gestion de Clés).

CNRS-Test

La démarche suivie par l'UREC a été de monter une autorité de certification pour le CNRS sur le modèle d'une plate-forme de tests. Depuis plusieurs mois, nous avons assemblé les briques logicielles nécessaires pour installer ce service, avec des produits du domaine public. Cela nous a pris du temps pour comprendre théoriquement les mécanismes de gestion de ces clés, ainsi que les fonctions des logiciels malheureusement très peu

documentés. Nous avons appelé cette autorité de certification CNRS-Test. Nous avons aussi défini une méthode de création, d'obtention, de stockage des certificats et avons rédigé un petit guide utilisateur (http://www.services.cnrs.fr/ca/). A noter que techniquement la publication des certificats se fait au moyen d'annuaires LDAP (Light Directory Access Protocol, standard d'accès à un annuaire, annuaire au sens large), sujet sur lequel nous travaillons aussi en parallèle.

Nous avons dans un premier temps ouvert cette plate-forme pour les deux groupes sécurité pilotés par l'UREC cités précédemment (celui de 30 personnes, puis celui de 170), Les certificats sont utilisés avec les outils de messagerie Netscape et Outlook (Internet Explorer). Pour l'instant nous n'avons pas réussi à utiliser Eudora, malgré des tests avec des plug-in différents ; nous continuons d'investiguer. Début mars, il est difficile de faire un premier bilan de l'utilisation, l'ouverture ayant eu lieu il y a quelques jours. Si le test est positif, nous pourrions ouvrir cette plate-forme à d'autres communautés d'utilisateurs non informaticiens. Contactez nous si vous avez une demande spécifique. Vous pouvez aussi essayer la mécanique pour obtenir et utiliser un certificat en vous connectant sur l'URL http://www.services.cnrs.fr/ca/, mais il faut en avoir l'utilité car la mise en œuvre n'est pas immédiate et nous demande un travail d'assistance personnalisée à chaque demande.

Nous travaillons maintenant sur les possibilités d'ouvertures et d'architectures. Nous souhaitons ainsi tester les interconnexions possibles avec d'autres autorités de certification (il faut que chacune reconnaisse l'autre …) en priorité d'organismes d'enseignement et de recherche. Notre population de chercheurs ne peut pas restée isolée, la communication sécurisée avec l'extérieur est donc une priorité. Nous avons fait un appel à nos collègues des universités mais pour l'instant, il n'y a pas de plate-forme opérationnelle chez eux.

Nous voulons aussi tester certaines possibilités de décentralisation de la délivrance des certificats. Nous avons ainsi certifié avec CNRS-Test, une autorité de certification « fille » pour une délégation régionale. L'administrateur dans la délégation régionale va délivrer les certificats localement en utilisant les mêmes procédures que nous.

Malgré la notion de plate-forme de tests, **notre méthode de travail est d'essayer de se mettre dès le départ dans des conditions de production**, c'est à dire avec des procédures sécurisées, contrôlées et une utilisation à la portée de non-informaticien.

Comme on peut le comprendre dans cette présentation, une sécurité forte telle que celle offerte par une lettre recommandée n'est pas l'objectif de ces tests. Il faudrait dans ce cas étudier le source de tous programmes utilisés dans la chaîne. L'objectif est de s'assurer que le courrier sera simplement bien cacheté (pas lisible par n'importe quelle personne) et que la signature ne sera pas falsifiée. Néanmoins parallèlement à cette expérience il faudra contacter les personnes compétentes en France - comme le SCSSI - pour avoir leur avis sur le niveau de sécurité des produits utilisés.

Le nom de l'autorité CNRS-Test n'est pas anodin. L'UREC n'a ni la mission, ni les moyens de gérer une autorité de certification. Ainsi nous considérons que les certificats délivrés par CNRS-Test ont but de test, pour une durée limitée, et nous ne garantissons pas la sécurité assurée par ceux-ci (néanmoins un message signé avec un certificat de CNRS-Test apporte une authentification nettement supérieure à celle d'un message non signé). A terme, les certificats CNRS-Test seront remplacés par des certificats définitifs et officiels lorsque les choix auront été fait au CNRS et qu'une autorité de certification pour l'organisme sera en place.

Cette plate-forme doit nous permettre d'acquérir une compétence dans ce domaine (ne serait-ce déjà que pour comprendre les fonctions des produits commerciaux pour les comparer et évaluer la justesse de leur coût) et devrait répondre aux questions suivantes (ou au moins proposer des éléments de réponse) :

- Les fonctions de sécurité des produits répandus dans notre communauté comme Netscape et Internet Explorer sont elles utilisables aujourd'hui ? Par tous ? Si non, peut-on les configurer pour rendre leur emploi plus facile ?
- Ce service de certificats est il généralisable à tous les agents CNRS ou doit on le restreindre à certains groupes (selon le besoin, la fonction, l'application, la compétence, …) et l'architecturer de manière différente selon les groupes ?
- Quelle architecture de gestion des clés au CNRS ? Une autorité de certification centralisée et des autorités d'enregistrement décentralisées dans les délégations, dans les laboratoires, dans les départements ? Plusieurs autorités de certification ? Quelles procédures faut il mettre en place pour la gestion de ces certificats ?
- A quel coût peut-on estimer le travail pour délivrer un certificat ? Est-ce préférable de sous-traiter totalement ou en partie ce service ? Suivant quel cahier des charges ?
- Pour les certificats, quelles informations doivent ils contenir (laboratoire, numéro d'agent, …) ? Comment gérer et mettre à jour ce qui permet d'annuler la validité de certains certificats, les listes de révocations ?
- Techniquement en cryptographie, faut il assurer un séquestre de tout ou partie des clés privées ? Quelle longueur de clé choisir ?

Au terme de cette expérimentation, un rapport devrait répondre à ces questions en vue d'éclairer les décisions que le CNRS aura à prendre. **La décision de la mise en place d'une autorité de certification et d'un mode opératoire sont des choix très stratégiques pour un organisme**.