

Désignation, rôle et devoirs des Autorités d'Enregistrement de l'Autorité de Certification CNRS2-Standard

17 février 2014

S'il existe une version plus récente de ce document, celle-ci est déposée dans l'espace <http://igc.services.cnrs.fr>

Ce document doit être :

- Diffusé à chaque Directeur d'unité avant la désignation de l'autorité d'enregistrement pour cette unité.
- Lu, accepté et suivi par chaque autorité d'enregistrement CNRS2-Standard.

Désignation des autorités d'enregistrement

Dans chaque unité ou service CNRS, l'autorité d'enregistrement pour l'autorité de certification CNRS2-Standard, appelée AE, est par défaut le directeur de l'unité. Celui-ci peut déléguer cette fonction à une ou plusieurs personnes. Cette délégation est similaire à une délégation de signature.

Pour désigner l'autorité d'enregistrement de son unité (qui peut être lui-même), le directeur d'unité doit envoyer un courrier postal spécifiant les coordonnées de l'autorité d'enregistrement (prénom, nom, adresse électronique, numéro de téléphone) ainsi que l'adresse IP de la machine de son (ses) AE. Un modèle de lettre est disponible dans la page <http://igc.services.cnrs.fr>.

Le délégué régional a généralement confié le rôle de gestion des autorités d'enregistrement de laboratoire de sa délégation à une personne appelée autorité d'enregistrement CNRS2-Plus de la délégation. La liste de ces autorités est disponible dans le document « Liste des autorités d'enregistrement CNRS2-Plus dans les délégations régionales » dans la page <http://igc.services.cnrs.fr>.

Les changements (fin de fonction ou nouvelles nominations) d'AE doivent être demandés suivant cette même procédure.

Certificats CNRS2-Standard

Deux types de certificats CNRS2-Standard peuvent être créés pour une unité : des certificats de personnes et des certificats de services (machines ou applications serveurs).

Ces certificats sont destinés à un usage professionnel.

Un certificat de personne CNRS2-Standard est une carte d'identité professionnelle qui permet à son possesseur de prouver son identité professionnelle, lorsqu'il signe ses messages électroniques, accède à des applications, à des pages Web...

Les certificats de services permettent aux machines ou aux applications serveurs de prouver leur identité aux utilisateurs qui y accèdent et de mettre éventuellement en place un transport chiffré entre les machines clientes et le serveur.

Si des certificats sont nécessaires dans le cadre d'expérimentation de logiciels dans des projets (exemple grilles de calcul), à cause des risques encourus alors par les certificats et clés privées

(exposés sur des machines moins sûres que des machines d'exploitation), il est nécessaire d'utiliser d'autres certificats que CNRS2-Standard, sous l'autorité de certification CNRS2-Projets.

Rôle de l'AE

Le rôle de l'AE est, pour son unité, de :

- Valider ou rejeter les demandes de nouveaux certificats électroniques venant des personnes travaillant dans l'unité, ainsi que les demandes de renouvellement d'anciens certificats. Ceci après un certain nombre de vérifications.
- Révoquer les certificats quand nécessaire.

Devoirs de l'AE

Les requêtes de création et de renouvellement sont effectuées électroniquement par les utilisateurs. L'AE en prend connaissance avec son outil de messagerie et son navigateur.

Avant d'accepter une requête de certificat de personne l'AE doit s'assurer que :

- Le demandeur travaille dans l'unité. Il n'y a pas de restriction sur le statut du demandeur (agent CNRS ou non, permanent ou temporaire, stagiaire, ...). Par contre, le personnel extérieur (par exemple d'une entreprise extérieure intervenant dans le laboratoire) n'a pas droit à un certificat CNRS2-Standard.
- Les informations fournies (prénom, nom, adresse électronique, code unité) sont exactes. L'adresse électronique doit être l'adresse professionnelle du demandeur et doit être exacte, c'est à dire correspondre à celle qui apparaît dans le champ « From » des messages.
- La demande provient bien de la bonne personne. Lors de la création d'un nouveau certificat, un contact face à face ou éventuellement téléphonique est obligatoire. Lors du renouvellement, ce contact direct n'est pas obligatoire.

L'AE doit aussi choisir la durée de validité du certificat. Celle-ci doit correspondre à la présence de la personne dans le laboratoire. Si le certificat est destiné à un stagiaire par exemple, la durée de validité à choisir devra être la durée du stage.

Le certificat CNRS2-Standard a une durée maximum de validité de 2 ans (durée par défaut).

Les certificats électroniques CNRS2-Standard sont destinés à une utilisation professionnelle et ils doivent être créés uniquement quand les personnes en ont besoin pour leurs activités professionnelles. Il est très fortement déconseillé de créer un certificat qui ne va pas être utilisé rapidement par son possesseur.

Avant d'accepter une requête de certificat de service l'AE doit s'assurer que :

- L'unité est bien propriétaire ou gestionnaire de la machine ou de l'application serveur.
- L'adresse électronique indiquée dans la demande. bien celle de l'administrateur de la machine ou de l'application serveur.

L'AE doit révoquer un certificat de personne lorsque :

- Son propriétaire quitte le laboratoire.
- Les informations dans le certificat ne sont plus exactes : changement de nom, d'adresse électronique...
- Le propriétaire ne peut plus l'utiliser : perte de la clé privée associée.

- La clé privée associée de l'utilisateur a des risques d'avoir été compromise (divulgaration, machine piratée...).
- L'utilisateur fait un usage abusif de son certificat.

L'AE doit révoquer un certificat de service lorsque :

- La machine ou l'application serveur disparaît.
- Les informations dans le certificat ne sont plus exactes : changement de nom, d'adresse électronique de l'administrateur...

La clé privée associée a été perdue ou risque d'avoir été compromise (divulgaration, machine piratée...).

L'AE doit prévenir l'utilisateur de la révocation de son certificat par message électronique signé, si ceci est possible.

Seuls les certificats en cours de validité peuvent être révoqués. Les certificats périmés sont rejetés systématiquement par toutes les applications donc inutilisables.

Outils techniques pour l'AE

Pour son travail d'AE, l'autorité d'enregistrement utilisera la station dont le numéro IP a été spécifié dans le courrier de désignation, avec le navigateur Firefox (<https://www.mozilla.org/fr/firefox/>).

De plus, il utilisera un certificat CNRS2-Plus. Ce certificat CNRS2-Plus ne pourra être demandé qu'une fois les formalités de désignation par le directeur de l'unité accomplies et enregistrées auprès de la délégation Régionale.

Pour obtenir ce certificat CNRS2-Plus l'AE se connectera sur la page : <http://igc.services.cnrs.fr/CNRS2-Plus/>

En cas de problème dans ses fonctions, l'AE contactera l'autorité d'enregistrement CNRS2-Plus de la délégation régionale dont dépend le laboratoire.

Rappel sur la procédure de demande et de création d'un certificat de personne CNRS2-Standard

- Le demandeur avec son navigateur se connecte sur la page : <http://igc.services.cnrs.fr/CNRS2-Standard/>.
- Il remplit le formulaire électronique de demande de certificat.
- Ce formulaire est récupéré par le serveur IGC (Infrastructure de Gestion de Clés) qui envoie un message électronique à l'utilisateur lui demandant de confirmer sa demande.
- Celui-ci confirme par messagerie électronique.
- Le serveur IGC reçoit cette confirmation et envoie un message électronique à l'AE de l'unité de l'utilisateur en indiquant qu'une demande de certificat est arrivée.
- L'AE se connecte sur le serveur de validation de l'IGC. Il effectue les vérifications décrites dans le paragraphe « Devoirs de l'AE ». Si tout est correct, il valide la requête en utilisant son certificat CNRS-Plus.
- Le demandeur reçoit un message électronique indiquant où il peut récupérer son certificat.
- Le demandeur récupère son certificat avec son navigateur. Il doit utiliser obligatoirement la même machine, le même compte et le même navigateur avec lesquels il a fait sa demande.

Documentations

Toutes les documentations sur les certificats électroniques au CNRS utiles pour les autorités d'enregistrement, incluant une FAQ, sont disponibles sur la page : <http://igc.services.cnrs.fr/Doc/>.