Politique de certification et procédures de l'autorité de certification CNRS

V2.1 – 1 juin 2001

Jean-Luc Archimbaud CNRS/UREC
Directeur technique de l'UREC
Chargé de mission sécurité réseaux informatiques au CNRS

Ce document décrit les choix de services, d'organisation et techniques de l'autorité de certification CNRS. Il sera complété au fur et à mesure de la mise en place de cette autorité.

En février 2000 a été mise en place une autorité de certification CNRS-Test. Les buts (tests) sont décrits dans l'article http://www.urec.fr/securite/articles/CA.CNRS-Test.pdf et le mode opératoire dans les pages en ligne http://www.services.cnrs.fr/ca/.

En juin 2000 le CNRS a pris la décision de créer une autorité de certification et d'en confier la mise en place à l'UREC :
http://www.urec.cnrs.fr/securite/certifications/decision_creation_AC_cnrs.pdf.

Depuis cette date, un **comité de pilotage** animé par C. Michau Directeur de l'UREC et un **comité technique** animé par moi-même travaillent pour définir la politique de certification et les procédures. Ce qui a été mis en place et ce qui est décrit dans ce document découlent des décisions de ces comités.

En parallèle, le **développement d'un logiciel IGC** (Infrastructure de Gestion de Clé) pour les besoins du CNRS s'adaptant à la structure de l'organisme a été réalisé à partir d'outils du domaine public, OpenSSL en particulier. Une première version de ce développement est opérationnelle.

En mai 2001, a débuté la mise en place de sites pilotes utilisant les logiciels développés et les procédures définies pour délivrer des certificats : délégations de Bordeaux et Toulouse, laboratoire LAAS, fédération IMAG, projet européen de calcul distribué datagrid, groupe des coordinateurs et des correspondants sécurité, comités d'organisation et de programme de la conférence JRES2001. Actuellement des certificats ont déjà été distribués sur ces sites et commencent à être utilisés principalement pour le contrôle d'accès à des serveurs Web (authentification de l'utilisateur, accès en lecture ou écriture à certaines pages, ...) et à des listes de diffusion ainsi que pour la signature de messages électroniques.

1 Des certificats pour qui ?

Des certificats pour les personnes, des certificats pour les services (serveur Web, routeur, …) et des certificats pour signer du code de programme (applet JAVA par exemple) seront délivrés. **Dans la phase pilote seuls des certificats de personnes et de services sont délivrés, dans les sites et projets pilotes ainsi qu'à quelques entités pour des tests**.

1.1 Pour les personnes

Toute personne :

- qui travaille dans un laboratoire ou service CNRS (agents CNRS ou non, permanents, temporaires, stagiaires, thésards, invités, …),
- qui est agent CNRS mais ne travaille pas dans une unité CNRS,
- d'un organisme partenaire et qui a besoin de certificat dans le cadre de ses collaborations avec le CNRS,

peut obtenir un certificat de l'autorité de certification CNRS.

1.2 Pour les services

Tout service et tout équipement dans un laboratoire CNRS ou fonctionnant pour le compte du CNRS ou utilisé par de nombreux utilisateurs CNRS peut obtenir un certificat CNRS. La demande doit être validée et faite par l'autorité d'enregistrement de l'unité propriétaire ou gestionnaire.

2 Des certificats pour quel usage ?

Par défaut **les certificats délivrés ne sont pas réservés à une application ou à un ensemble d'applications bien délimité**. Ils pourront être utilisés pour la messagerie électronique, le contrôle d'accès à des pages Web et à des applications, la diffusion électronique de notes administratives signées, …

Coté utilisateur, **les certificats sont conçus pour être utilisable au moins par les versions récentes des clients Netscape et Internet Explorer (et Outlook)**.

La DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) recommande 2 types de certificats :

- Pour la signature (authentification et intégrité). Dans ce cas l'utilisateur est seul à connaître sa clé privée ;
- Pour le chiffrement (confidentialité). Dans ce cas il est recommandé que l'autorité de certification (ou un service) assure le séquestre des clés privées de tous les utilisateurs pour en particulier pouvoir les restituer en cas de perte.

L'autorité de certification CNRS délivrera donc à terme les 2 types de certificats recommandés par la DCSSI, avec des procédures différentes et des options de séquestre différentes. **Dans la phase pilote ne seront délivrés que des certificats pour l'authentification et l'intégrité, sans séquestre de clé privée**.

3 Autorités et certificats

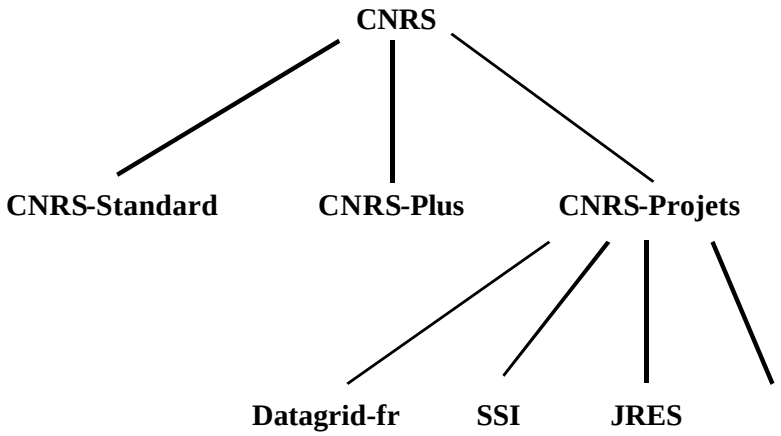
3.1 Autorités de certification

Il n'existe pas actuellement d'autorité de certification française gouvernementale qui pourrait certifier l'autorité CNRS. Celle-ci est donc **auto-signée** dans un premier temps. Si cette configuration changeait, ce choix pourrait être modifié.

L'arborescence d'autorités suivante est mise en place

Une autorité racine « CNRS » est créée et au second niveau, **plusieurs autorités filles** :

- Une autorité **CNRS-Standard** (signée par l'autorité CNRS) : délivre des certificats utilisateurs, des certificats de services et de codes pour des utilisations courantes. **Dans la phase pilote des certificats CNRS-Standard sont délivrés aux utilisateurs du LAAS, de l'IMAG et des laboratoires des délégations de Bordeaux et Toulouse.**
- Une autorité **CNRS-Plus** (signée par l'autorité CNRS) : délivre des certificats utilisateurs pour des « actes importants » aux personnes ayant une fonction de direction. **Dans la phase pilote, les autorités d'enregistrement des sites pilotes ont des certificats CNRS-Plus**.
- Une autorité **CNRS-Projets** (signée par l'autorité CNRS) dont de but est de pouvoir délivrer des certificats (utilisateurs, services ou codes) pour des projets. Ces projets ont pour la plupart une durée de vie limitée, avec éventuellement la participation d'autres organismes que le CNRS. Sous cette autorité on créera autant de sous autorités que de projets. **Dans la phase pilote ont été créés 3 sous arborescences** (signées par l'autorité CNRS-Projets) **: Datagrid-fr pour le projet Datagrid, SSI** (comme Sécurité des Systèmes d'Information) pour les coordinateurs et correspondants sécurité et **JRES**.



L'autorité CNRS-Test continue d'exister pour les mêmes besoins de tests mais en utilisant le nouveau logiciel IGC et les nouvelles procédures pour délivrer et gérer les certificats.

3.2 Les certificats de personnes

Ils sont au format X509V3. Ils utilisent un **algorithme de chiffrement RSA avec des clés de 1024 bits par défaut** (512 ou 2048 éventuellement).

Ils sont **délivrés par défaut pour une période de 1 an dans le cas de personnel permanent**. Dans le cas de personnel temporaire la durée est limitée à la durée du contrat pour les contrats inférieurs à un an.

Le champ CN (Canonical Name) contient **le prénom, le prénom et l'adresse électronique de la personne.**

Les autres champs du **DN (Distinguished Name)** sont remplis différemment selon les caractéristiques de la personne et selon l'autorité de certification.

Pour les certificats émis par les autorités CNRS-Standard et CNRS-Plus :

- Si la personne travaille dans une unité ou un service CNRS (même si elle n'est pas agent CNRS) : C=FR, O=CNRS, OU=Code unité
- Si la personne est agent CNRS mais travaille dans un service d'un autre organisme : C=FR, O=CNRS, OU= Code Labintel du service
- Si la personne n'est pas agent CNRS et travaille chez un partenaire : C=Vide, O=EXTERNE, OU=Vide

Pour les certificats émis par les autorités sous l'autorité CNRS-Projets, le contenu des différents champs se fait en accord avec le responsable du projet. Dans la phase pilote :

- Datagrid-fr : C contient le code pays (pas uniquement FR, si la personne n'est pas française), O le nom de l'organisme (CNRS ou CEA ou CS ou …), OU le code ou le nom du laboratoire ou du service.
- SSI : C=FR, O=CNRS, OU=Code unité

3.3 Les certificats de services

Le DN contient le **nom de la machine** sous forme de domaines, en utilisant un alias de la machine pour faire apparaître le nom du service **(**Exemples : www.urec.cnrs.fr pour un service Web, abintel.cnrs.fr pour un serveur labintel national) et **l'adresse électronique de l'administrateur du service**.

3.4 Autorités d'enregistrement pour CNRS-Standard

Pour chaque unité ou service, une personne a autorité pour valider les demandes de certificat CNRS-Standard du personnel (mais aussi des services et des codes de programmes) de cette unité ou de ce service. Elle est autorité d'enregistrement. Cette personne est par défaut le directeur. Celui-

ci peut déléguer cette fonction à une personne de confiance de son unité qui agira en son nom pour ces procédures.

Chaque autorité d'enregistrement a un certificat CNRS-Plus qui est utilisé pour ces procédures.

3.5 Autorités d'enregistrement des sous-autorités de CNRS-Projets

Pour chaque projet, une personne a autorité pour valider les demandes de certificat pour les personnes travaillant dans le projet, ainsi qu'éventuellement les services et les codes de programmes du projet. Cette autorité d'enregistrement est par défaut le responsable du projet (pour le CNRS). Celui-ci peut déléguer cette fonction à une autre personne pour ces procédures**.**

Chaque autorité d'enregistrement a un certificat CNRS-Plus qui est utilisé pour ces procédures.

4 Procédures pour délivrer un certificat

4.1 CNRS-Standard ou de sous-autorité de CNRS-Projets de personne, sans séquestre de clé privée

Ces certificats sont destinés à l'authentification et à la signature (authentification et intégrité). Ils peuvent être utilisés pour la confidentialité (chiffrement) si l'utilisateur prend soin de sauvegarder de manière très fiable sa clé privée.

Pour chaque unité ou service ou projet, il existe une autorité d'enregistrement. Cette autorité d'enregistrement possède un certificat CNRS-Plus. La chronologie de la création de certificat pour un utilisateur est la suivante :

- L'utilisateur avec Netscape ou Internet Explorer accède à un formulaire électronique en ligne. Ce formulaire lui demande son nom, prénom, adresse électronique, … toutes les données qui vont figurer dans son certificat. Le formulaire rempli, la création d'un couple de clés privée-publique est provoquée sur le poste utilisateur. Le poste utilisateur conserve la clé privée, la clé publique est « récupérée » par le serveur.
- Un message électronique, pour confirmation et vérification d'adresse électronique, est envoyé à l'utilisateur, qui l'acquitte.
- Le formulaire (avec la clé publique de l'utilisateur) est stocké dans un spool. L'autorité d'enregistrement est avertie par messagerie électronique qu'une demande de certificat est arrivée.
- L'autorité d'enregistrement accède à cette demande avec son navigateur et son certificat CNRS-Plus. Elle vérifie les informations contenues dans la demande, contacte le demandeur pour vérifier qu'il a bien fait cette demande (et possède la clé privée associée). Si tout est bon, elle acquitte la demande. Celle-ci est transmise à l'autorité de certification.
- L'autorité de certification (un automate) crée le certificat , le dépose sur un serveur Web et dans l'annuaire LDAP des certificats CNRS, puis envoie un message électronique à l'utilisateur.
- L'utilisateur récupère son certificat sur le serveur Web.

Les différentes demandes et toutes les opérations sont archivées.

Cette procédure sera affinée après le bilan de la phase pilote.

4.2 CNRS-Standard de service, sans séquestre de clé privée

La procédure est identique à celle utilisée pour les personnes. L'utilisateur demandeur doit être l'administrateur du service et il doit déjà posséder un certificat de personne.

5 Révocation des certificats

Dans la phase pilote les certificats peuvent être révoqués uniquement par l'autorité d'enregistrement.

6 Service de séquestre et de recouvrement de clés privées

Dans la phase pilote ce service n'est pas assuré. L'UREC n'a connaissance à aucun moment de la clé privée des utilisateurs. Ce sont à eux de sauvegarder leurs clés privées.

7 Accès aux formulaires, certificats …

Pour demander un certificat, obtenir le certificat et la liste de révocation de l'autorité de certification, rechercher les certificats d'autres utilisateurs :

CNRS/CNRS-Standard : http://igc.services.cnrs.fr/CNRS-Standard/

CNRS/CNRS-Plus : http://igc.services.cnrs.fr/CNRS-Plus/

CNRS/CNRS-Projets/Datagrid-fr : http://igc.services.cnrs.fr/Datagrid-fr/

CNRS/CNRS-Projets/SSI : http://igc.services.cnrs.fr/SSI/

CNRS-Test : http://igc.services.cnrs.fr/CNRS-Test/