L’utilisation de l’IGC du CNRS dans le système d’information régional

Roland Dirlewanger
CNRS- Délégation Aquitaine et Poitou-Charentes
Esplanade des Arts et Métiers - BP 105
33405 TALENCE CEDEX
rd@dr15.cnrs.fr

Introduction

- Le besoin
  - Particularités du CNRS :
    - Forte déconcentration : 1600 unités, 20 délégations, 2 instituts
    - Moins de 30% des personnels de ces unités sont agents CNRS
    - Infrastructures réseaux partagées avec les partenaires
    - Des centaines de serveurs WWW et messagerie
  - Besoins en terme de sécurité :
    - Authentification, confidentialité de la messagerie
    - Authentification pour les services WWW
    - Simplification de procédures administratives

IGC du CNRS - principes

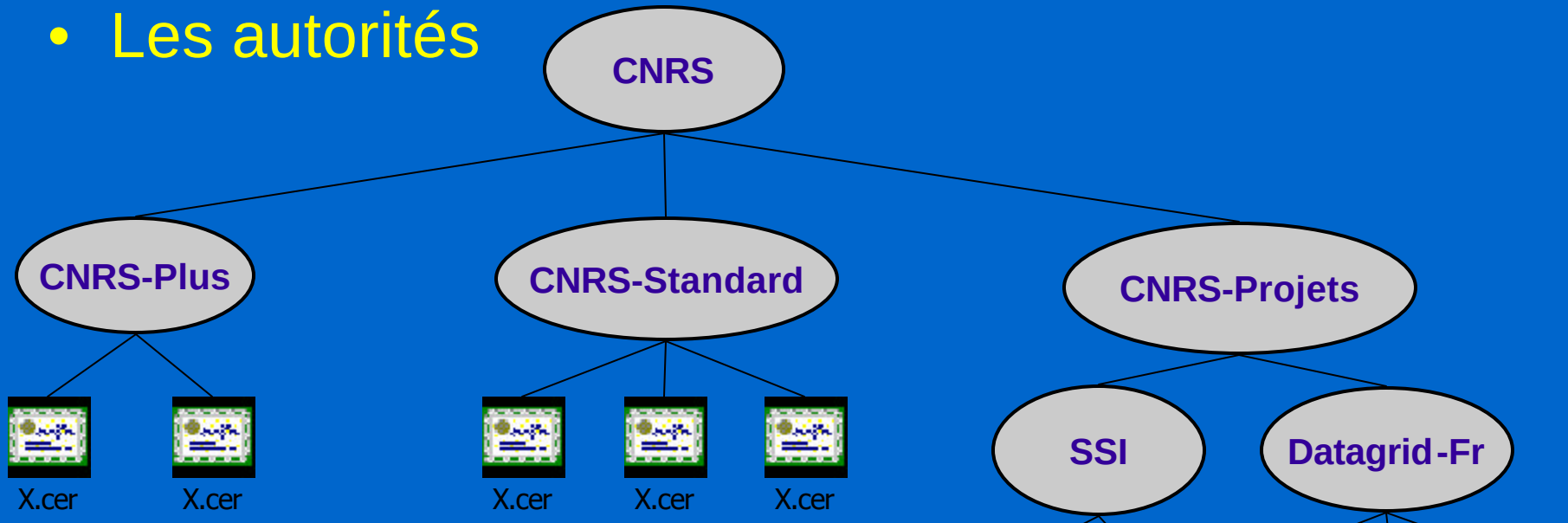
- Les grands principes
  - Diffusion de certificats pour toute personne en ayant besoin
  - Prise en compte de besoins particuliers
    - Projets communs avec des partenaires externes au CNRS (grilles de calculs, …)
  - Des autorités d ’enregistrement (AE) au plus près des utilisateurs

IGC du CNRS – organisation (1)

- Les autorités de certifications
  - Une autorité racine CNRS
  - Une autorité CNRS-Standard :
    - Délivre les certificats d'utilisateurs pour les personnes travaillant dans les unités du CNRS.
  - Une autorité CNRS-Plus
    - Délivre des certificats aux autorités d'enregistrement pour les certificats CNRS-Plus
  - Une autorité CNRS-Projets
    - Délivre des certificats d'autorité de certification pour les projets (grilles de calculs, coordinateurs de sécurité, etc.)

IGC du CNRS – organisation (2)

- Les autorités



Signature, authentification,
AE pour CNRS-Plus
• pour les délégations
AE pour CNRS-Standard,
• pour les laboratoires

Signature, authentification,
Demande de certificats pour des serveurs SSL (HTTPS, IMAPS, SMTP/TLS, …)

Usages spécifiques aux projets

IGC du CNRS – organisation (3)

- La confiance
  - Chaque Délégation nomme une ou deux AE
    - Reçoivent un certificat CNRS-Plus permettant de valider les demandes de certificat CNRS-Plus provenant des AE des unités de la Délégation
  - Chaque directeur/ice d'unité nomme une ou deux AE
    - Reçoivent un certificat CNRS-Plus validé par l'AE de la Délégation
    - Permet de valider les demandes de certificats CNRS-Standard provenant des personnels de l'unité

IGC du CNRS – déploiement (1)

- Différentes phases de tests (1999, 2000)
  - UREC, Délégation de Bordeaux
- Choix d'un logiciel de gestion de l'IGC (2001)
  - Développement propriétaire
- Deux délégations pilotes pour le déploiement
  - Bordeaux (2001), Toulouse (2002)
  - Autres régions à partir de 2003
- Actions au niveau régional :
  - Formation des AE : sensibilisation
  - Assistance aux utilisateurs

IGC du CNRS – déploiement (2)

- Principaux enseignements
  - Choix initiaux (autorités, confiance, …) validés
  - Logiciel de gestion de l'IGC opérationnel
  - Difficultés techniques dues aux clients utilisés :
    - Avec MS Internet Explorer : impossible sur Mac
    - Avec Netscape : problèmes avec des certificats ayant le même sujet (Distinguished Name) mais émis par des autorités différentes, dysfonctionnements avec Netscape 6
    - Possibilité de signer des formulaires limités à Netscape 4
  - Organisation dans les labos
    - À terme : AE fait partie de l'équipe de direction, support et assistance effectués par l'équipe informatique
    - En pratique : AE = informaticien du laboratoire

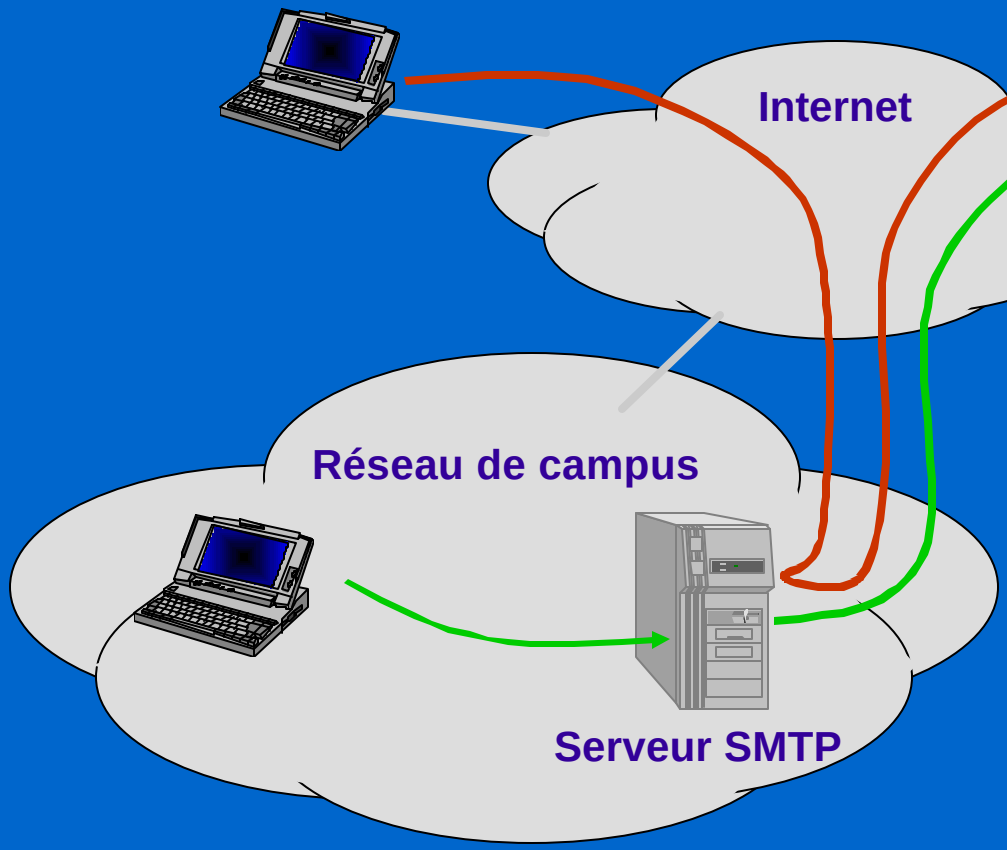
IGC du CNRS – politique de certification

- Actuellement :
  - La politique de certification est intra-CNRS
  - Décrite de façon informelle dans http://www.urec.cnrs.fr/securite/articles/PC.CNRS.pdf
- Objectif mi-2003 :
  - Rédaction des politiques de certification (PC) et des déclarations de pratiques de certifications (DPC) selon le RFC 2527
  - Collaboration avec la DCSSI pour signature de la racine du CNRS par l'IGC-A

Utilisation – messagerie et mobilité

- L'accès à la messagerie depuis des postes de travail portables est indispensable, mais
  - Besoin de l'utilisateur viole parfois la politique de sécurisation des laboratoires ou campus
    - Exemple : accès interdit aux ports POP ou IMAP
  - Constat : fuite des boîtes à lettres vers des fournisseurs externes
- Problèmes :
  - Protection du patrimoine scientifique
  - Difficultés pour l'envoi des messages selon l'endroit où l'on est connecté (anti-relais)

Le problème de l'anti-relais



Le même poste de travail localisé à deux endroits différents à un comportement différent vis-à-vis de l'envoi de messages

Trafic SMTP interdit

Trafic SMTP autorisé

Utilisation – messagerie et mobilité

- La solution pour l'anti-relais : SMTP/TLS
  - Authentification de l'utilisateur via son certificat
    - Il devient autorisé à utiliser le serveur en relais
    - Toute la session d'envoi de message est chiffrée
  - Pour la première fois : la sécurisation d'un service apporte un confort à l'utilisateur !

- Solutions mises en œuvre
  - Serveur : Unix : sendmail, postfix
    - Exemple : camus.dr15.cnrs.fr accepte de relayer tout trafic SMTP authentifié par un certificat CNRS
  - Client :
    - **Windows : MS Outlook**
    - **MacOS, Unix, Windows : Netscape, Mozilla**

Utilisation – messagerie et mobilité

- La solution pour les accès : IMAP/SSL
  - Nécessite un certificat pour le serveur
  - Toute la session est chiffrée : mot de passe, contenu des messages échangés
  - Éventuellement, l'accès au serveur IMAP lui même peut-être authentifié par le certificat de l'utilisateur

- Solutions mises en œuvre :
  - Serveur : Unix : wu-imapd, stunnel
  - Client :
    - **Windows : MS Outlook**
    - **MacOS, Unix, Windows : Netscape, Mozilla**

Utilisation – serveurs WWW

- Exemple de services avec authentification et confidentialité :
  - Transmission d'informations confidentielles à depuis/vers les laboratoires
    - Informations financières (direction, service de gestion)
    - Gestion des risques (direction, responsable hygiène et sécurité)
    - Informations personnalisées (remboursement de frais de mission)
  - Transmission de formulaires administratifs
    - Demandes d'inscription à la formation permanente
    - Demandes de billets de transports
- Solutions mises en œuvre
  - Unix : Apache ; Windows : IIS

Utilisation – gestionnaire de profil (1)

- Les réalisations montrent qu'il existe différents types de profils d'utilisateurs :
  - Des groupes identifiables par des attributs contenus dans le certificat :
    - tous les titulaires d'un certificat CNRS,
    - toutes les personnes d'un laboratoire,
    - telle personne, …
  - Des groupes non identifiables par les attributs contenus dans le certificat :
    - telle fonction : directeur, gestionnaire, correspondant fonctionnel

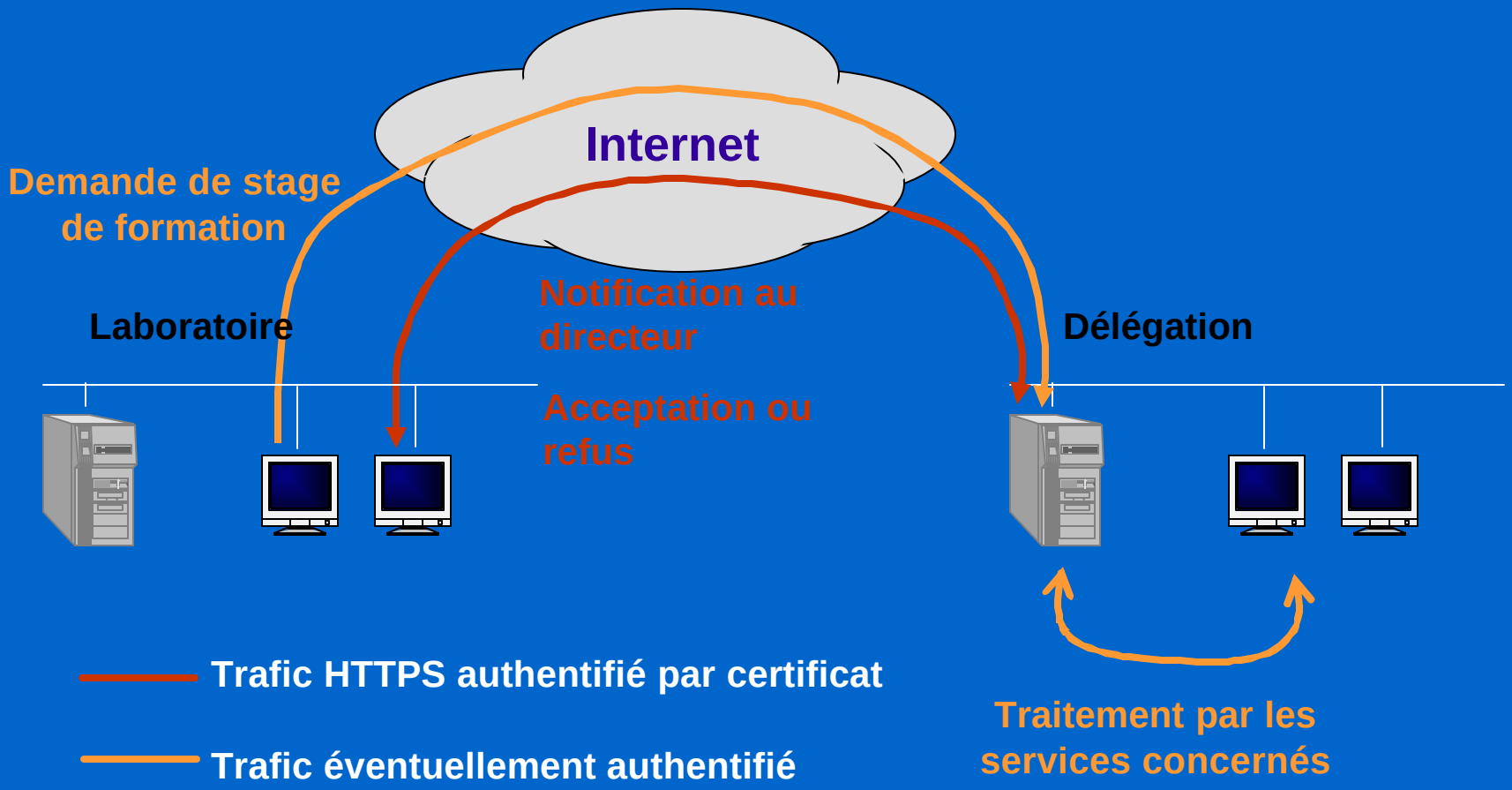
Utilisation – gestionnaire de profil (2)

- Nécessité d'un gestionnaire de profil
  - Associe à un certificat les autorisations pour un système d'information
  - Permet de dissocier le système d'information ou l'application de l'authentification
  - En pratique : interface WWW avec annuaire LDAP
    - Côté applicatif : fonction qui retourne vrai ou faux en fonction d'une application et d'un certificat
    - Côté utilisateur :
      - Demande d'accès via un formulaire WWW
      - Validation/refus de cet accès par une personne autorisée en fonction de l'application

Utilisation – et la signature ?

- La signature électronique est peu utilisée
  - Peu de solutions techniques pour garantir la validité de la signature dans le temps :
    - Problème de l'archivage des messages signés reçus dans les boites des utilisateurs
    - Vérification de la signature à long terme (Cour des comptes, reconstitution de carrières, retraites, …)
  - Les outils de messagerie sont mal adaptés pour des processus de type « *workflow* » impliquant des signataires multiples pour un même document.
  - C'est rarement le signataire qui prépare les courriers

Exemple d'une procédure administrative
(Demande de stage de formation, DR de Toulouse)



Utilisation – formulaires signés

- Exemple précédent a montré :
  - Suppression des formulaires papier dans un processus administratif
  - Fonctionnement très bien accepté par les utilisateurs
  - Peut-être étendu à des processus plus complexes, notamment dans le cas de signataires multiples
- Mais …
  - Ce n'est pas une signature électronique => notion de visa électronique
  - En cours de développement : parapheur électronique

Conclusion

- Déploiement de l'IGC dans la Délégation :
  - Projet initial (1999-2000):
    - Mise en œuvre de la signature électronique dans les unités
    - Sensibilisation des utilisateurs, assistance pour l'installation des certificats
  - Constat :
    - L'assistance aux utilisateurs est continue, elle demande une forte expertise sur les clients utilisés
    - On ne remplace pas un parapheur papier par des messages signés
    - La gestion des profils est indispensable pour les applications WWW
  - Bilan :
    - La quasi-totalité des laboratoires des Délégations pilotes ont une autorité d'enregistrement opérationnelle.