Certificats X509
&
Infrastructure de Gestion de

Claude Gross

urec

Confiance et Internet

Comment établir une relation de confiance indispensable à la réalisation de transaction à distance entre personnes qui ne se connaissent pas ?

Services de base en sécurité

- **Authentification**
  - Assurance de l'identité d'une personne, d'un objet
- **Intégrité**
  - Garantie de non modification par un tiers d'un message
- **Non-répudiation**
  - Pour que l'émetteur ne puisse pas nier l'envoi
- **Confidentialité**
  - Protection contre la « lecture » non autorisée par un tiers

Chiffrement à clefs symétriques

- clef de chiffrement = clef de déchiffrement
  - ⇨ clef secrète
    - DES : Data Encryption Standard
    - 3DES : 3 passes dans DES en utilisant 2 ou 3 clefs distinctes (112 ou 168 bits)
    - RC2, RC4, RC5 : clef de 1 à 1024 bits
    - IDEA (International Data Encryption Algorithme)
    - AES (Advanced Encryption Standard)
- Chiffrement et déchiffrement rapide

Chiffrement à clefs symétriques

- Problèmes
  - Comment se partager les clefs secrètes ?
  - Connaissance à priori des correspondants
  - Nombre de clefs

Chiffrement à clefs asymétriques

- Clef de chiffrement ≠ clef de déchiffrement
- Couple de clefs (créées ensemble) : bi-clef
- L'une des clés est secrète, l'autre est publique
- Impossible de découvrir une clef à partir de l'autre
- Tout texte chiffré avec une clef est déchiffré avec l'autre et uniquement avec celle-ci
- RSA (Rivest, Shamir, Adelman): 1976
- Si annuaire des clefs publiques : permet une utilisation du chiffrement de manière planétaire

- Problème : temps de chiffrement et de déchiffrement

Algorithmes symétriques/asymétriques

Algorithmes symétriques

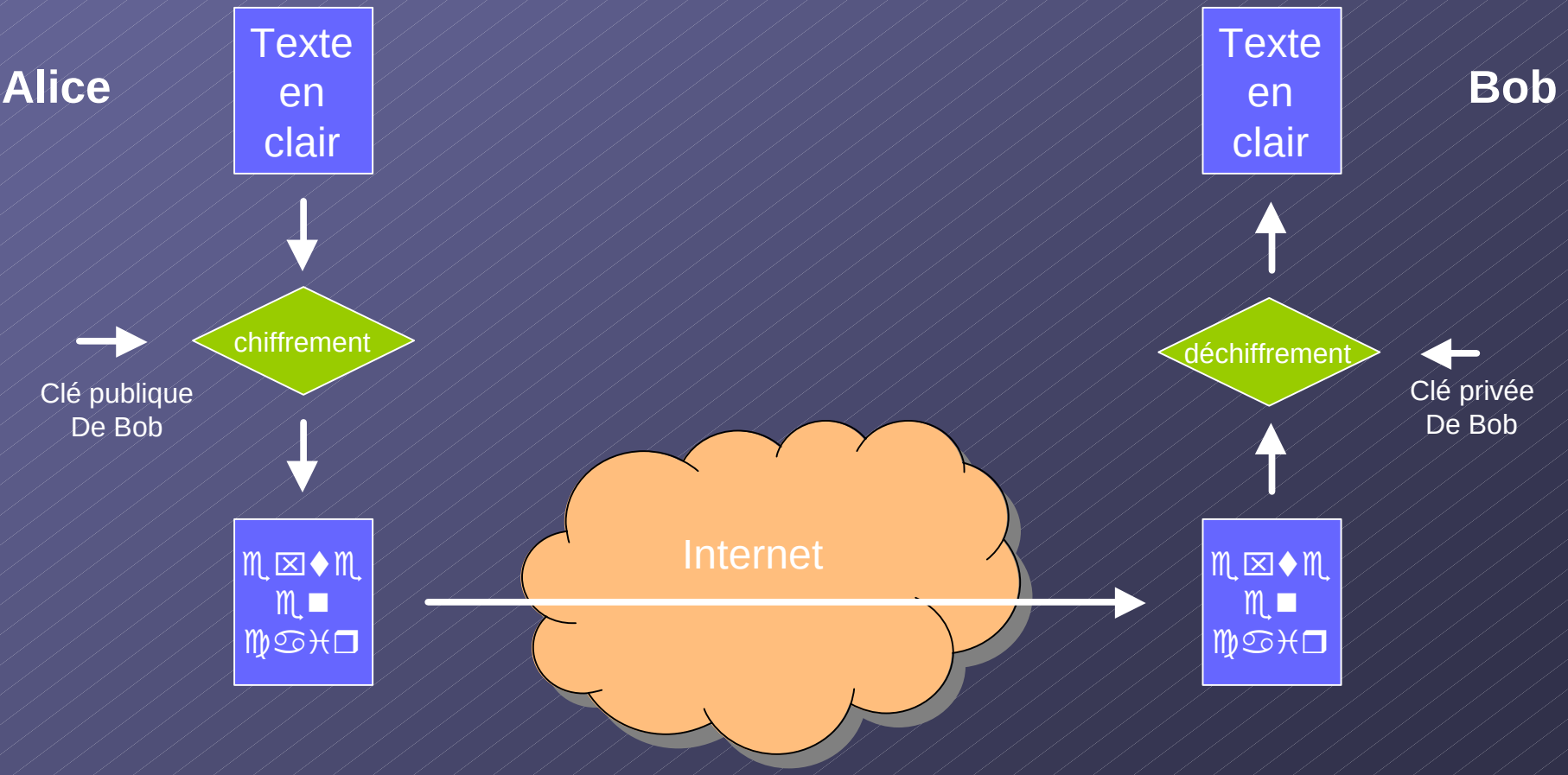
- Systèmes fermés
- Relations en étoile

Algorithmes asymétriques :

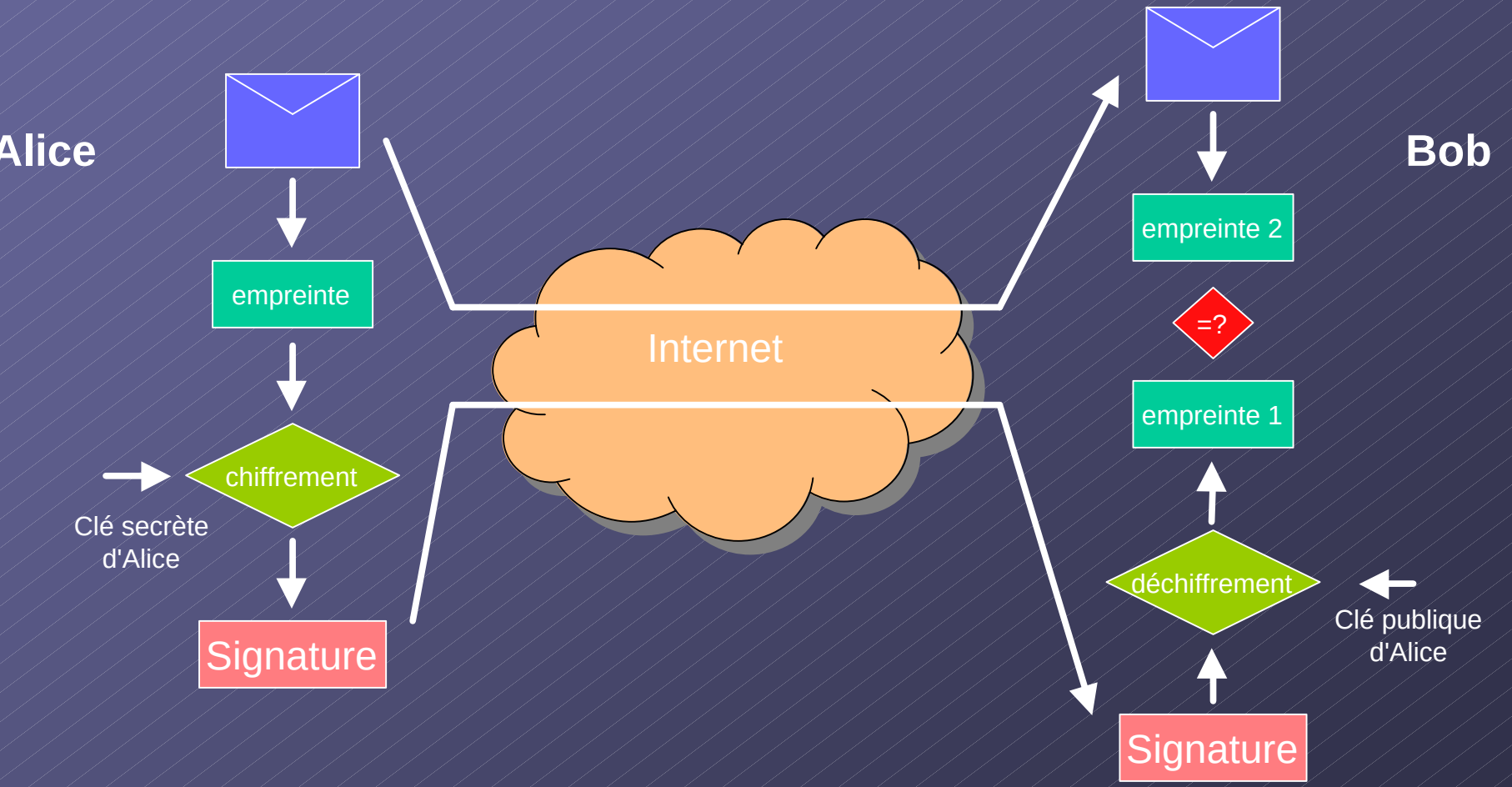
- Systèmes ouverts
- Relations "peer to peer"

La certification électronique utilise
des algorithmes asymétriques

Chiffrement à clefs asymétriques



Signature électronique



La certification, pourquoi?

- Comment être sûr qu'une clé publique correspond bien à la personne que l'on croit?
  - ➔Risque d'usurpation

- Certificat : preuve de la correspondance entre une clé publique et un ensemble d'informations (nom, prénom, email,…)

La certification, comment?

- Une *autorité de confiance* signe avec sa clé privée un document contenant :
  - L'identité d'une entité possédant un couple de clé
  - La clé publique
  - Des informations décrivant l'usage de cette clé
  - …
- Le résultat est un **certificat**
- L' autorité de confiance est appelée **Autorité de Certification**

Certificat X509

- Norme X509 (ITU-T X.509 international standard V3 - 1996
- *RFC2459* : instanciation particulière de la norme X.509 pour l'Internet

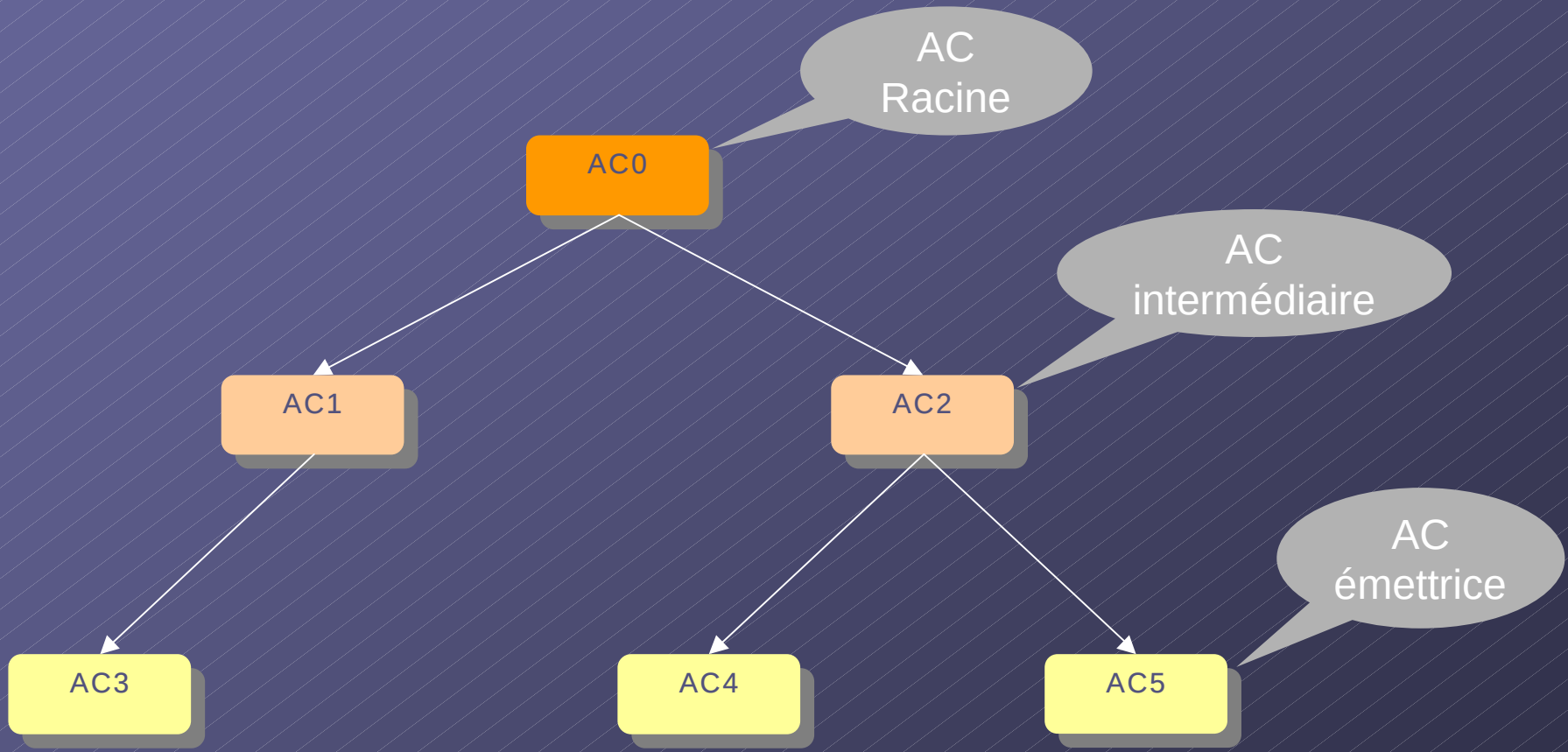
Certificat X509

- Un certificat X509 :
  - prouve l'identité d'une personne au même titre qu'une carte d'identité, dans le cadre fixé par l'autorité de certification qui l'a validé ;
  - pour une application, il assure que celle-ci n'a pas été détournée de ses fonctions ;
  - pour un site, il offre la garantie lors d'un accès vers celui-ci que l'on est bien sur le site auquel on veut accéder.

Certificats X509

Données	Version	Version de la norme X509
	Serial Number	No de série du certificat
	Issuer	DN de l'autorité de certification
	Validity	Dates de validité (création et péremption)
	Subject	DN de l'entité
	Subject Public Key Info	Clé publique de l'entité
	X509v3 extensions	Extensions X509
Signature	Signature Algorithm	Algorithme de signature
	Signature	Signature

Certification hiérarchique



AC0 + AC2 + AC5 + Cx = chaîne de certification

Infrastructure de Gestion de Clés

Ensemble des matériels, logiciels, personnes, règles et procédures nécessaire à une Autorité de Certification pour créer, gérer et distribuer des certificats X509.

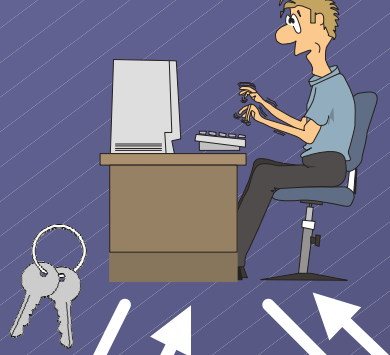
Infrastructure de Gestion de Clés

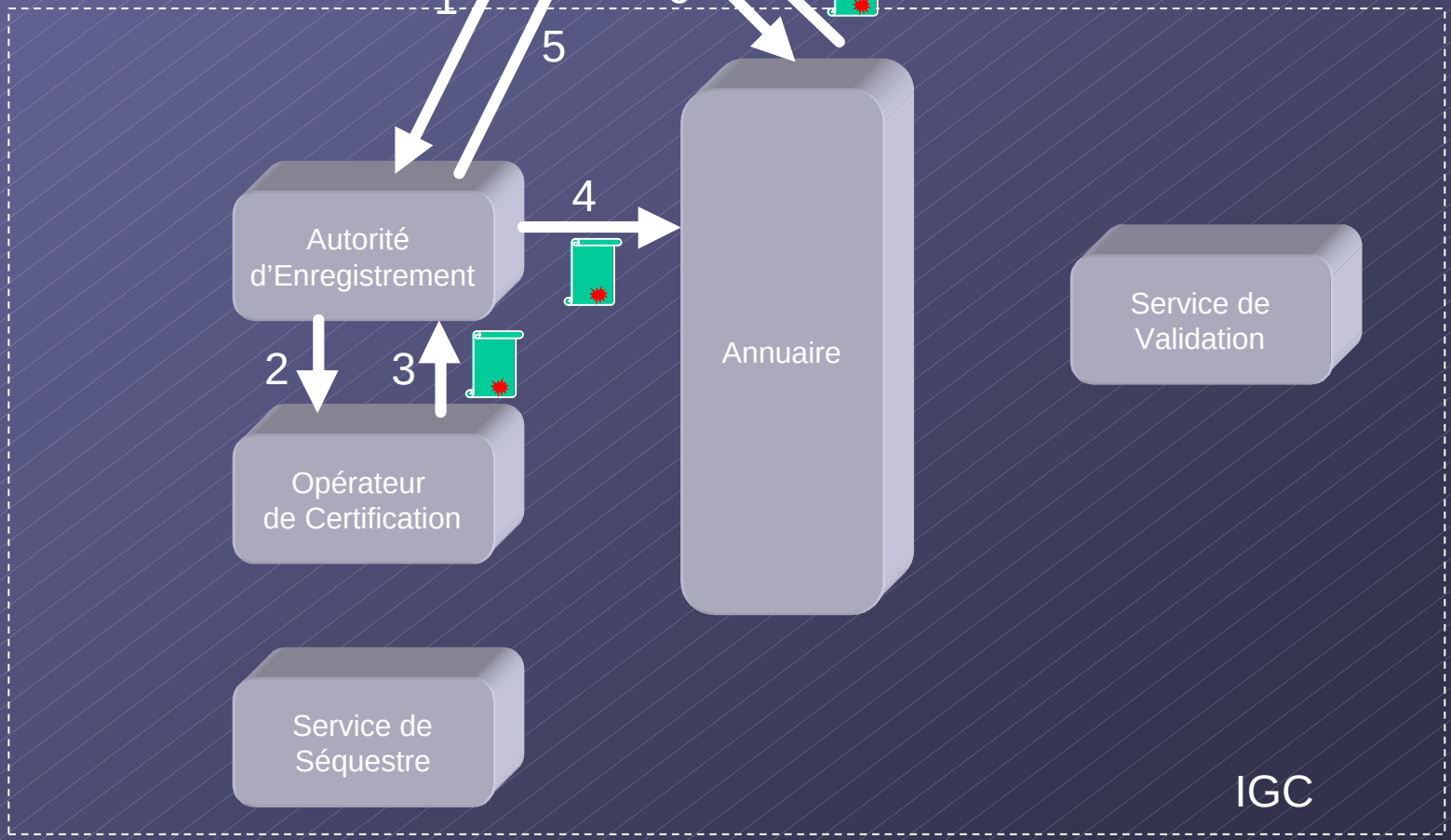
- Les fonctions principales d'une IGC sont :
  - Émettre et révoquer des certificats
  - Publier les certificats dans un annuaire
  - Éventuellement, fournir un service de séquestre et de recouvrement des clés privées

Infrastructure de Gestion de Clés

- Elle est constituée par :
  - Une autorité de certification (**AC**)
  - Une autorité d'enregistrement (**AE**)
  - Un opérateur de certification (**OC**)
  - Un annuaire de publication de certificats
  - Un service de validation
  - Éventuellement, un service de séquestre de clés

Scénario




1
5
6
7
4
2
3
Autorité d'Enregistrement
Annuaire
Service de Validation
Opérateur de Certification
Service de Séquestre
IGC

Applications

- Messagerie avec signature et/ou chiffrement
- Contrôle d'accès et confidentialité
  - Accès distants
  - VPNs
  - SSO et accès aux applications sécurisées
  - Sécurité poste de travail
- Nouvelles applications …

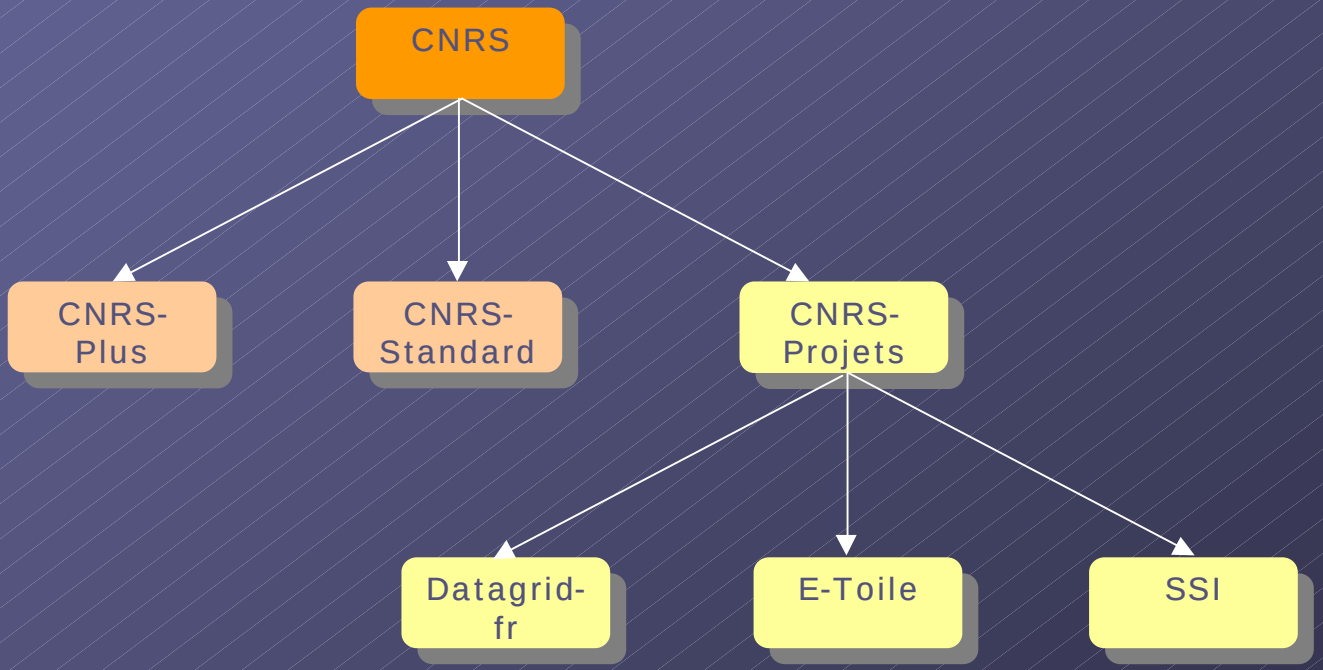
IGC CNRS

- Le CNRS
  - 1300 unités disséminées partout en France
  - 26000 personnes statutaires
  - 80000 personnes dans les unités
  - Pas de structure informatique centralisée (pour les labos)
  - 18 délégations régionales

IGC CNRS

- Juillet 2000 : décision officiel
- Maître d'œuvre : UREC
- Organisation
  - Comité de pilotage
  - Comité technique
  - Autres (DCSSI, …)
- Outil
  - Logiciel CNRS-IGC

IGC CNRS


CNRS
CNRS-Plus
CNRS-Standard
CNRS-Projets
Datagrid-fr
E-Toile
SSI

CNRS-Standard : Politique de Certification

- Pour qui?
  - Toute personne dans un laboratoire CNRS pourra disposer d'un certificat
  - Personnel CNRS ou non, permanent ou non
- Qui est l'autorité d'enregistrement ?
  - Directeur de l'unité
- Type de certificats
  - Pour les personnes
    - Pour authentification et signature : pas de séquestre de clés privées
    - Pour chiffrement : séquestre clés privées (non délivrés dans phase pilote)
  - Pour les services : Web, …
- Pour quoi faire? :
  - Toute application

CNRS-Standard : Politique de Certification

- Certificats de personne
  - Durée de validité : 1 an par défaut
  - DN

    `C=FR,O=CNRS,OU=`*`Code unité`*`,CN=`*`Prénom Nom`*`,Email=`*`email`*
  - Clés générées par l'utilisateur sur son poste

- Certificats de service
  - Durée de validité : 2 ans par défaut
  - DN

    `C=FR,O=CNRS,OU=`*`Code unité`*`,CN=`*`nom DNS`*`,Email=`*`email`*
  - Clés générées par l'AC

IGC CNRS : déploiement

- Environ 80 000 certificats à délivrer
  - Progressivement
- Comité de pilotage
  - Service du secrétariat général : BPC
- Pour le déploiement
  - Chef de projet et chargé de mission
- Exploitation des serveurs
  - Centre sécurisé « contrôlé par » la DSI
- Déploiement des AE
  - Délégués avec RSI
- Assistance aux utilisateurs
  - DSI avec les RSI
- UREC
  - Evolutions, veille, conception (développement)
  - Contrôles des procédures ?

IGC CNRS : études à mener

- Carte à puces, tokens, …
  - Où?
  - Comment?
- Certificat de chiffrement : séquestre
- Interconnexion avec d'autres IGC
  - Universités, …
- Applications
  - Dématérialisation procédures administratives
  - …
  - → C'est un autre projet
- Annuaires LDAP ou équivalent
  - → C'est un autre projet
- Horodatage

Conclusions

- Problèmes
  - Complexité des IGCs
  - Protection des clés privées
  - Pas complètement mûre (clients, …)
- Ce n’est pas la solution à tous les problèmes de sécurité
- Technologie séduisante
- Alternatives?

Références

- **IGC CNRS**
  - *http://www.urec.cnrs.fr/igc/Doc/IGC_docs.html*
- **IGC du CRU**
  - *http://pki.cru.fr/*
- **PKIX Working Group**
  - *http://www.imc.org/ietf-pkix/index.html*
- **PKI Forum**
  - *http://www.pkiforum.org/*
- **The Open–source PKI Book**
  - *http://ospkibook.sourceforge.net/docs/OSPKI-2.4.6/OSPKI/ospki-book.htm*
- **The PKI Page**
  - *http://www.pki-page.org/*
- **Serveur DCSSI**
  - *http://www.ssi.gouv.fr/*