ACI Sécurité Informatique

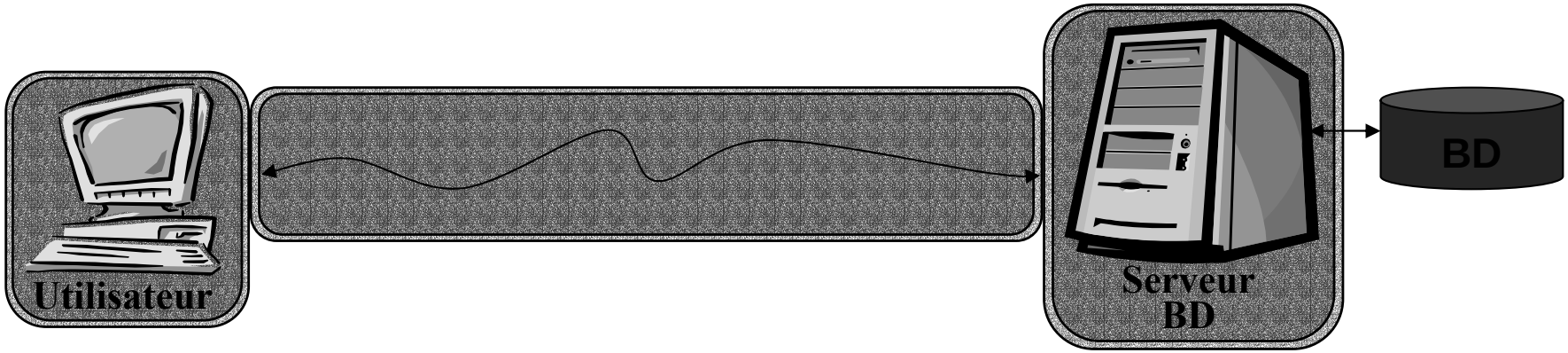
C.A.S.C

Contrôles d'Accès Sécurisés à des données Confidentielles

(2003-2006)

Participants : INRIA, ENS, ENST Bretagne, LRI, LIUPPA

Confidentialité dans les SGBD

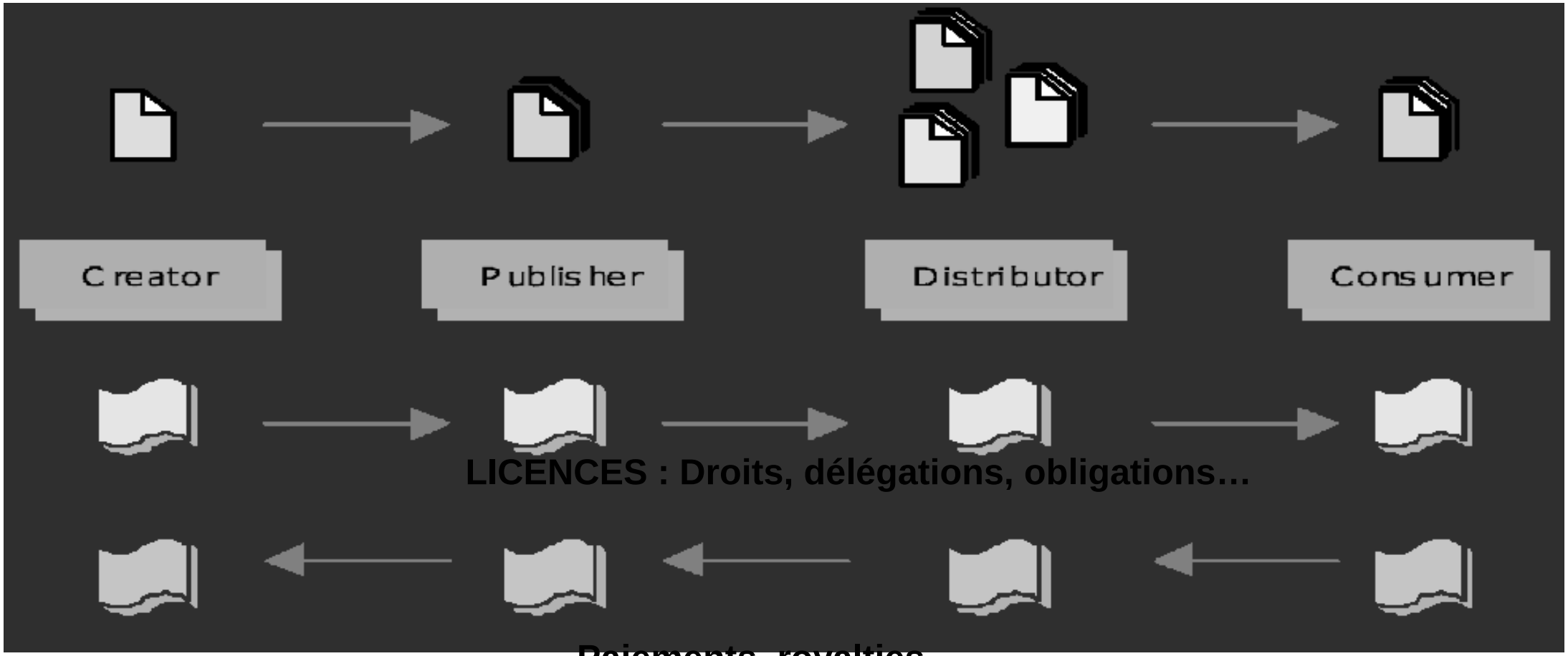


- **Identification / authentification**
- **Chiffrement des communications**
- **Contrôle d'accès sur le serveur**
  - Autorisations définies sur n'importe quel objet de la BD
    - N'importe quel granularité
    - Peuvent être définies sur des objets virtuels (i.e., données calculées)

Contexte : Evolution des systèmes d'information

- **Evolution des sources d'information**
  - BDs centralisées ➔ Sources de données largement distribuées, autonomes, hétérogènes
- **Evolution des modèles de données**
  - Tabulaires, structurées ➔ semi-structurées, arborescentes
- **Evolution des modes d'accès à l'information**
  - Client/serveur ➔ accès ubiquitaire, Push, P2P…
- **Apparition du contrôle d'*usage***
  - Contrôle d'accès ➔ Contrôle d'usage
    - Exemple : Digital Right Management (DRM)

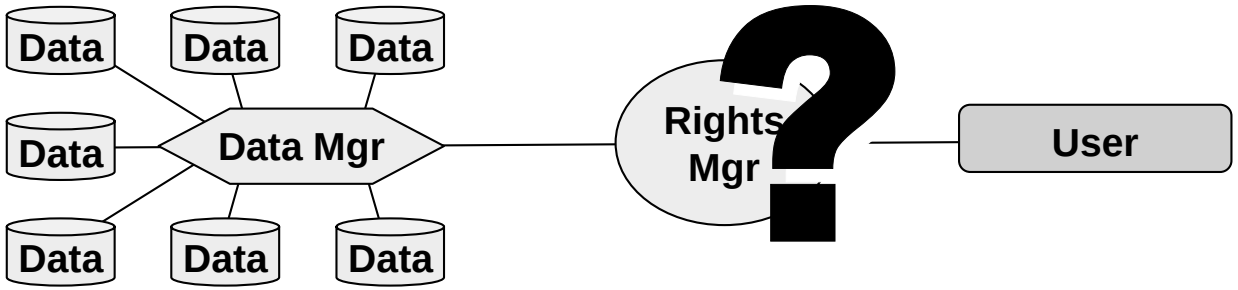
Exemple de contrôle d'usage : DRM et XrML



Modèle multi-tiers

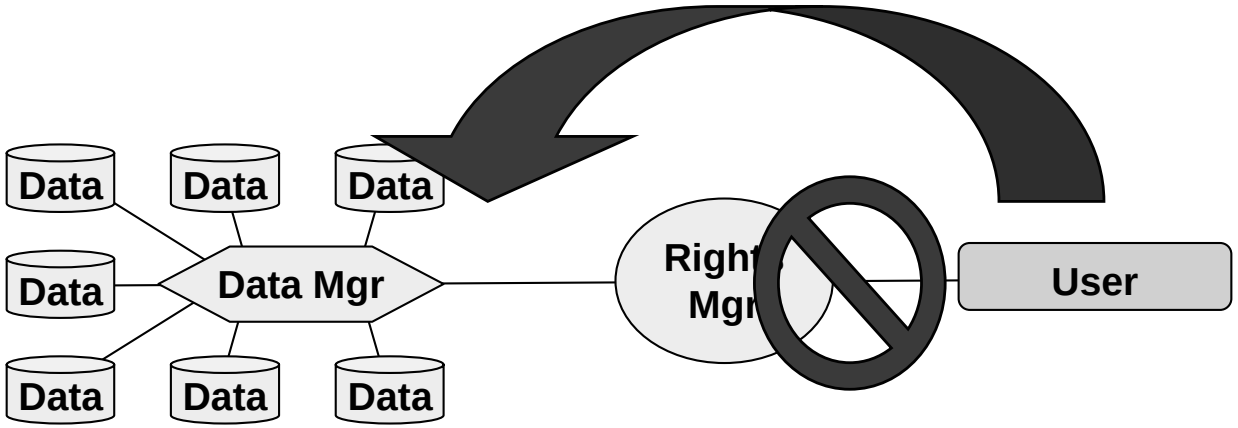
Exprimer les droits d'accès et d'usage ?

- **Les modèles existants sont inadaptés**
  - à la distribution, l'autonomie, l'hétérogénéité des sources de données
  - au nouveaux modèles de données (XML)
  - au différents modes d'accès
  - au contrôle d'usage



Comment garantir le respect des droits ?

- **Contournement de droits**
  - Attaques de l'empreinte disque
  - Attaques internes (e.g. rapport CSI/FBI)
- **Détournement de droits**
  - Violation de chartes de privacité (e.g., rapport IBM-Harris)



Objectifs de l'ACI CASC

1. **Abstraction des concepts à intégrer dans les modèles de droits d'accès et formalisation des procédures d'administration associées,**

2. **Définition d'un modèle de droits d'accès puissant et cohérent pour documents XML,**

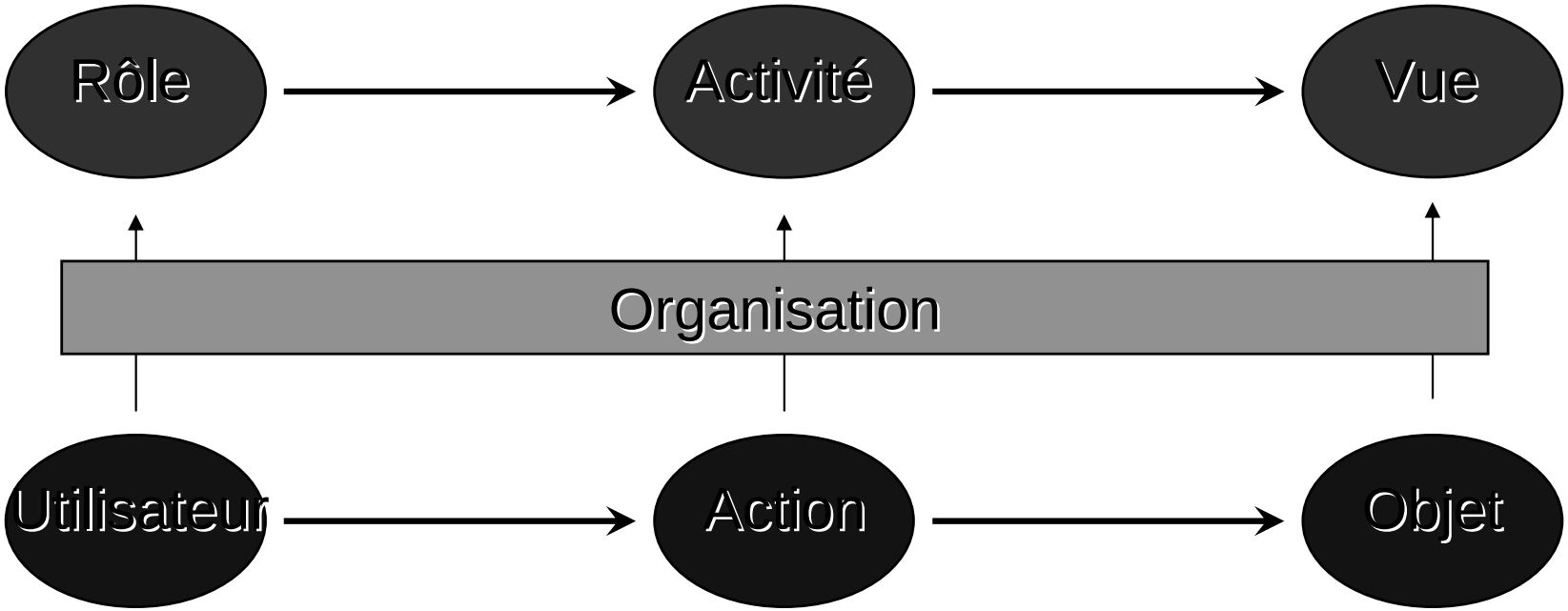
3. **Sécurisation matérielle des données, du contrôle des droits et de leur administration.**

➔ **l'ACI CASC est organisée en 3 tâches relatives à ces trois objectifs**

Participants

INRIA	**Luc Bouganim**	CR 1 - (Coordinateur)	**Sécurisation matérielle du contrôle de droits et interrogation de données chiffrées**
	Philippe Pucheral	PR-UVSQ (délég° INRIA)	
	François Dang Ngoc	2ème année de thèse	
ENST Bretagne	**Frédéric Cuppens**	PR (ENST Bretagne)	**formalisation de modèles de droits d'accès et d'usage intégrant organisation et contexte d'utilisation**
	Sylvain Gombault	MC (ENST Bretagne)	
	Alexandre Miège	2eme année de thèse (inscrit à l'ENST Paris)	
	Thierry Sans	1ère année de thèse	
LIUPPA	**AlbanGabillon**	PR (Univ. de Pau)	**modèles de droits d'accès pour documents XML**
	Manuel Munier	MC (Univ. de Pau)	
	Lilia Ighmouracene	1ère année de thèse	
Ens	**Giuseppe Castagna**	CR-CNRS (ENS Ulm)	**analyses de sécurité de transformations XML**
	Veronique Benzaken	PR (Univ. Paris XI)	
	Alain Frisch	3ème année de thèse	
	Marwan Burelle	2ème année de thèse	

T1 - Background : Or-BAC (ENST Bretagne)



- **Or-BAC (de l'ENST-B) est un modèle de droit permettant**
  - d'abstraire les notions d'utilisateur, d'action et d'objet
  - d'exprimer des droits contextuels,
  - d'exprimer des obligations ou recommandations
  - d'attacher les règles au concept d'organisation

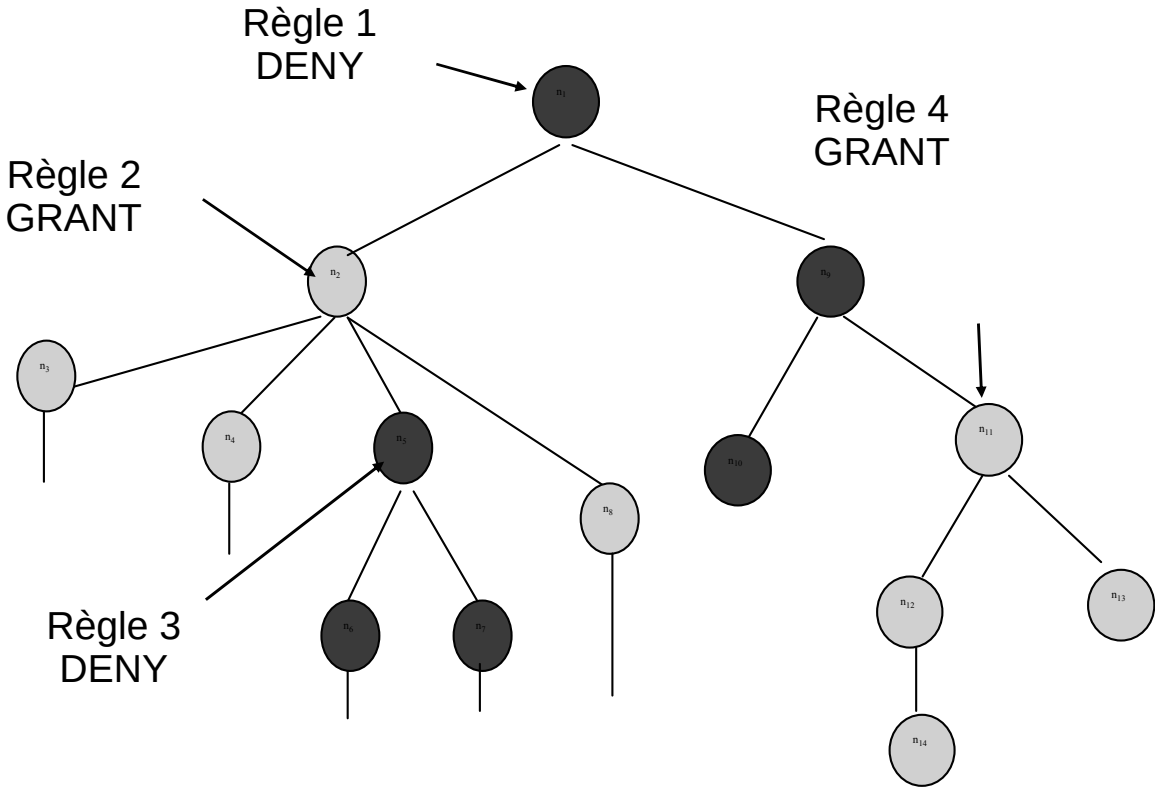
T1 : Mise en œuvre dans un environnement distribué

Abstraction des concepts à intégrer dans les modèles de droits d'accès et formalisation des procédures d'administration associées

- **Que doit on intégrer dans le modèle pour supporter de nouveaux modes d'accès ?**
  - Distribution du modèle et de son administration ?
- **Comment supporter différents contrôles d'usage ?**
  - Extension du modèle Or-BAC ?
  - Mise en œuvre dans le modèle multi-tiers ?

T2 - Background : Modèle de droits pour XML (LIUPPA)

- **Modèle de droit XML à base de règles**
  - Puissance des règles
  - grant / deny
  - Conflits et priorités



Document XML

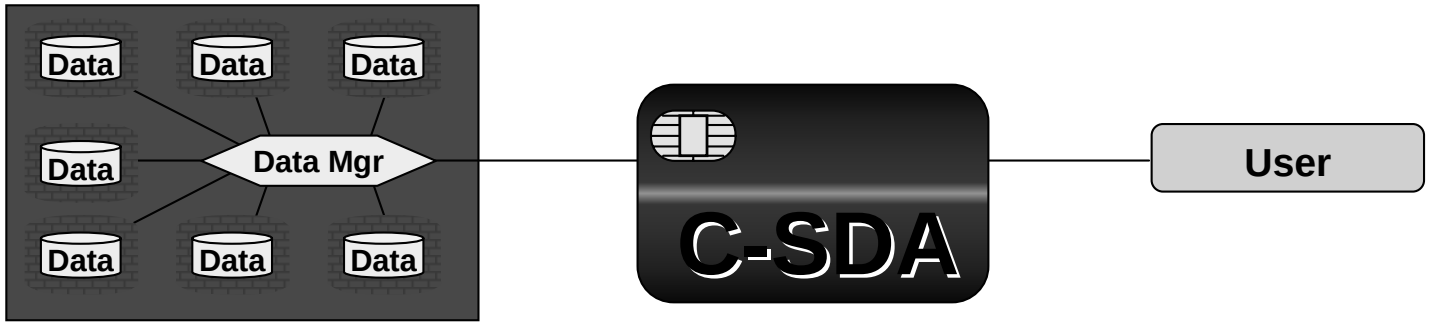
T2 : Extension du modèle de droit pour XML

Définition d'un modèle de droits d'accès puissant et cohérent pour documents XML

- **Prise en compte des mises à jour des documents XML ?**
- **Instanciation du modèle Or-BAC pour XML ?**
- **Analyse de la sécurité des transformations XML (LRI/ENS)?**

T3-Background : C-SDA (INRIA)

- **Sécurisation matérielle du contrôle des droits d'accès**
  - Les données sont chiffrées sur le serveur
  - Un logiciel embarqué dans un composant sécurisé (e.g., carte à puce) réalise l'ensemble des opérations liées à la confidentialité)
    - Chiffrement / déchiffrement,
    - contrôle d'accès,
    - Traitement



T3 : Sécurisation matérielle de XML-Or-BAC

Sécurisation matérielle des données, du contrôle des droits et de leur administration

- **Contrôle de droit XML Or-BAC dans une puce sécurisée**
  - Gestion des droits et conflits dans la puce ?
  - Prise en compte des obligations et recommandations ?
  - Prise en compte des ressources restreintes ?
  - Optimisation des traitements embarqués ?
  - Administration du modèle ORBAC ?

Merci !

Plus d’informations :

- **Luc.Bouganim@inria.fr**
- **http://www-smis.inria.fr/~bouganim/CASC**