

Grand Colloque STIC 2012

Projet FLUOR : convergence du contrôle de FLux et d'Usage dans les ORganisations

IT / Telecom Bretagne

CNRS - IODE

INRIA - LICIT

LIUPPA - CsySEC

SWID

UPF



<http://fluor.no-ip.fr/>



SeSur 2007

Consortium

- IT / Telecom Bretagne
- CNRS - IODE
- INRIA - LICIT
- LIUPPA - CsySEC
- SWID
- UPF - Terre Océan



- Travail collaboratif
 - Mutualisation des données
- Données distribuées
 - Contrôle de la distribution
- Gestion centralisée / distribuée
 - Modes connecté et déconnecté
- Dimension juridique
 - Gestion sécurisée des données personnelles

Objectifs

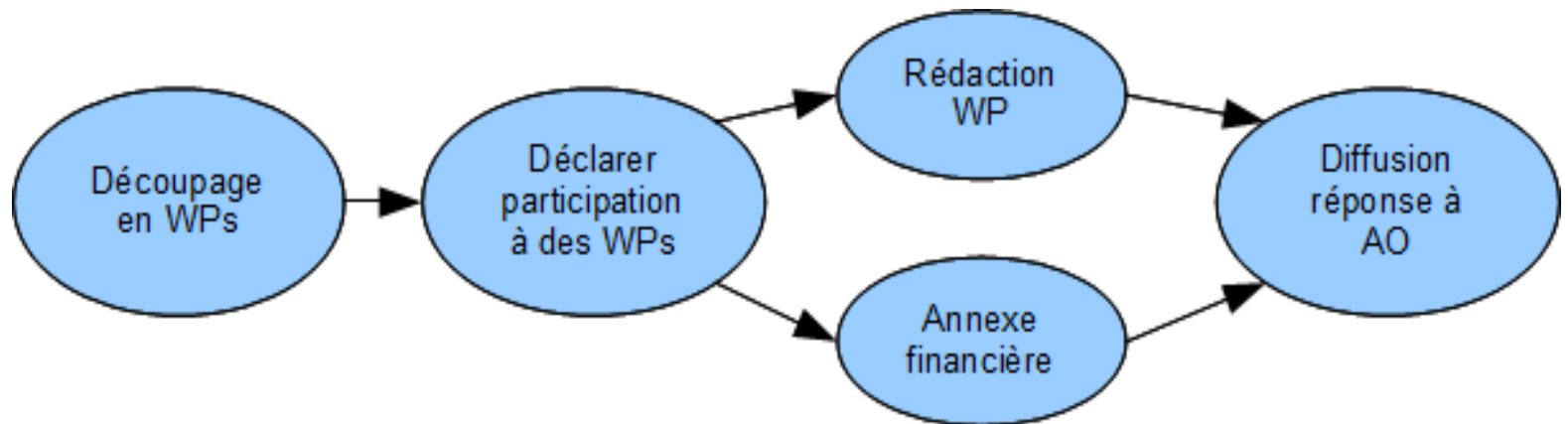
- Faire converger les modélisations de contrôle de flux et d'usage
 - Gestion sécurisée du cycle de vie des documents (métadonnées pour la traçabilité, contrôle d'accès/flux/usage au sein d'une chaîne de distribution, évaluation de la confiance, déclassification)
- S'appuyer sur les techniques de DRM pour déployer les exigences exprimées dans ce modèle de convergence
 - Architecture permettant une distribution sécurisée des documents (décentralisée, ne dépendant pas de composants propriétaires)
- Analyser les implications juridiques et légales des solutions techniques proposées
 - Solutions conformes au droit en vigueur, proposition d'évolution le cas échéant, ...

Problématique

- Contrôle d'accès évolutif et réactif
 - Confiance et contrôle d'accès
 - Pré-obligation
- Contrôle d'usage
 - Obligation avec délai, obligation de groupe
 - Violation, responsabilité et sanction
- Contrôle de flux
 - Distribution et déclassification
- Gestion de métadonnées
 - Données personnelles
 - Mesures de confiance
- Prise en compte de la dimension juridique
 - Régime juridique des métadonnées
 - Obligations de sécurité

Etude de cas

- Réponse à un appel d'offres
- Plusieurs partenaires se mettent d'accord pour répondre à un AO



- Structuration de la réponse
 - Annexe technique structurée en chapitres
 - Annexe financière structurée en pages Excel
 - Accord de consortium structurée en articles



Contrôle d'accès évolutif

Métadonnée relative à la confiance

- R1 : Permission de rédiger la synthèse si la confiance dans l'annexe technique dépasse un certain seuil

Permission(Rep_AO, Partenaire, Rediger, Synthese, Confiance_AT)

Hold(Rep_AO, S, A, O, Confiance_AT) :-

use(Rep_AO, Doc, annexe_technique),

has_trust(Doc, Level), Level > trust_threshold.

- Contrôle d'accès fondé sur la confiance
- Métadonnées : Indicateur de confiance
- Questions :
 - Comment définir et calculer la confiance (en un document, en un pair) ?
 - Quelle utilisation pendant le travail collaboratif, et pour quels résultats ?
 - Quelle utilisation pour la validation du niveau de confiance global ?

Utilisation de la notion de confiance

- 3 approches complémentaires
 - Calcul automatisé de valeurs de confiance « objectives », à partir de l'historique des modifications d'une version validée
 - Utilisation de valeurs de confiance « subjectives » pendant le processus de développement collaboratif du document => gain d'efficacité (temps, effort)
 - Phase de validation : à partir du réseau de confiance, minimisation du nombre d'évaluateurs pour atteindre un taux de satisfaction donné (problème NP difficile, heuristiques étudiées)



Contrôle d'accès évolutif

Métadonnée relative à la localisation

- R2 : Interdiction d'accéder à l'annexe financière en fonction de données de géo-localisation

Prohibition(Rep_AO, Partenaire, Acceder, AF, Risk_on_location)

- Modèle de sécurité pour des utilisateurs et/ou des données géo-localisées
 - Profil géo-temporel pour OrBAC
 - Prédicats spatiaux : touches, crosses, within,...
 - Fonctions spatiales : I(a), E(a), dim(a),...

$$\forall g_1 \in O, \forall g_2 \in O, \text{Within}(g_1, g_2) \leftrightarrow (g_1 \cap g_2 = g_1) \wedge (I(g_1) \cap E(g_2) \neq \emptyset)$$

- Cadre logique pour dériver automatiquement les mécanismes à appliquer pour protéger des données géographiques interdites
 - Floutage, masquage, suppression, leurre, pixellisation etc.

Le point de vue juridique :

Les métadonnées

- Nécessité de les qualifier
 - Cas des métadonnées personnelles
- Bien définir (et limiter) la finalité des traitements de métadonnées personnelles
 - Métadonnées pour gérer la confiance
 - Limiter la finalité du traitement à la gestion des modifications
 - Métadonnées pour localiser l'ordinateur du salarié
 - Limiter la finalité du traitement à la gestion des droits d'accès
- Déclaration du traitement auprès de la CNIL



Le point de vue juridique :

Métadonnées personnelles et gestion des risques

- Métadonnées – outil de surveillance du travail effectué
 - Quantitatif (ex : temps passé sur un dossier)
 - Qualitatif (ex : la manière de travailler, sur le lieu depuis lequel on travaille)
- S'agissant des métadonnées personnelles
 - Droit à l'information du salarié, du CE et du CTP sur l'usage
 - À des fins de surveillance individuelle par l'employeur
 - À des fins d'auto-surveillance ou de surveillance mutuelle dans le cadre du travail collaboratif
- Qui a accès aux métadonnées ?
 - Aux caractéristiques essentielles des métadonnées
 - À leur contenu



Le point de vue juridique :

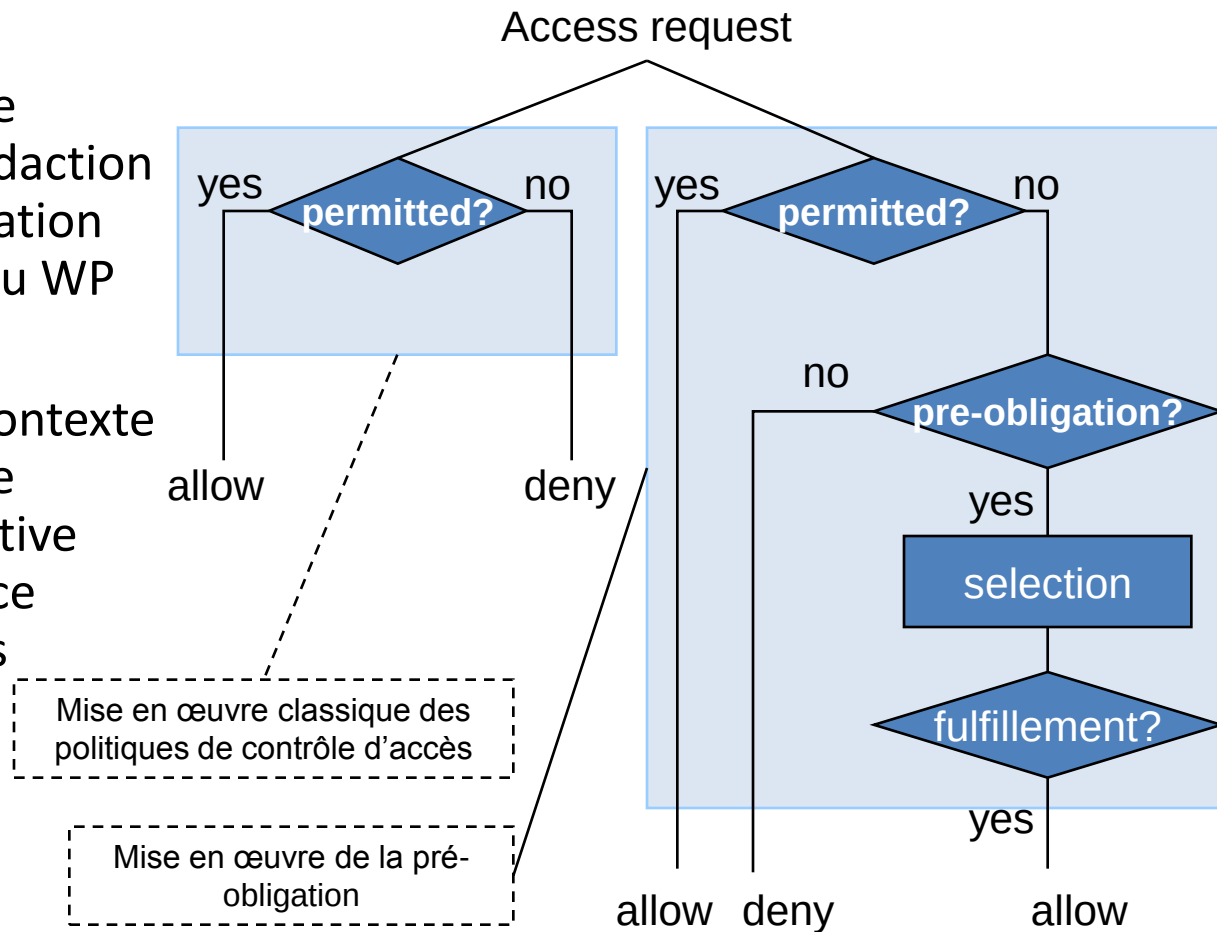
Quelle est la valeur probante des métadonnées ?

- Nécessité de distinguer la matière civile (preuve réglementée) et la matière commerciale (preuve libre)
- Les règles de preuve ne concernent pas les tiers
- Équivalence entre la preuve papier et la preuve électronique
- Préconstitution de la preuve
- Copie et transfert (ou migration) des métadonnées
 - risque d'altération ou de perte de la force probante
- Importance des conventions sur la preuve entre les parties à la réponse à l'appel d'Offre



Contrôle d'accès réactif

- R3 : Permission de contribuer à la rédaction d'un WP si déclaration de participation au WP
- Pré-obligation : Contexte actif associé à une permission qui active une obligation si ce contexte n'est pas satisfait

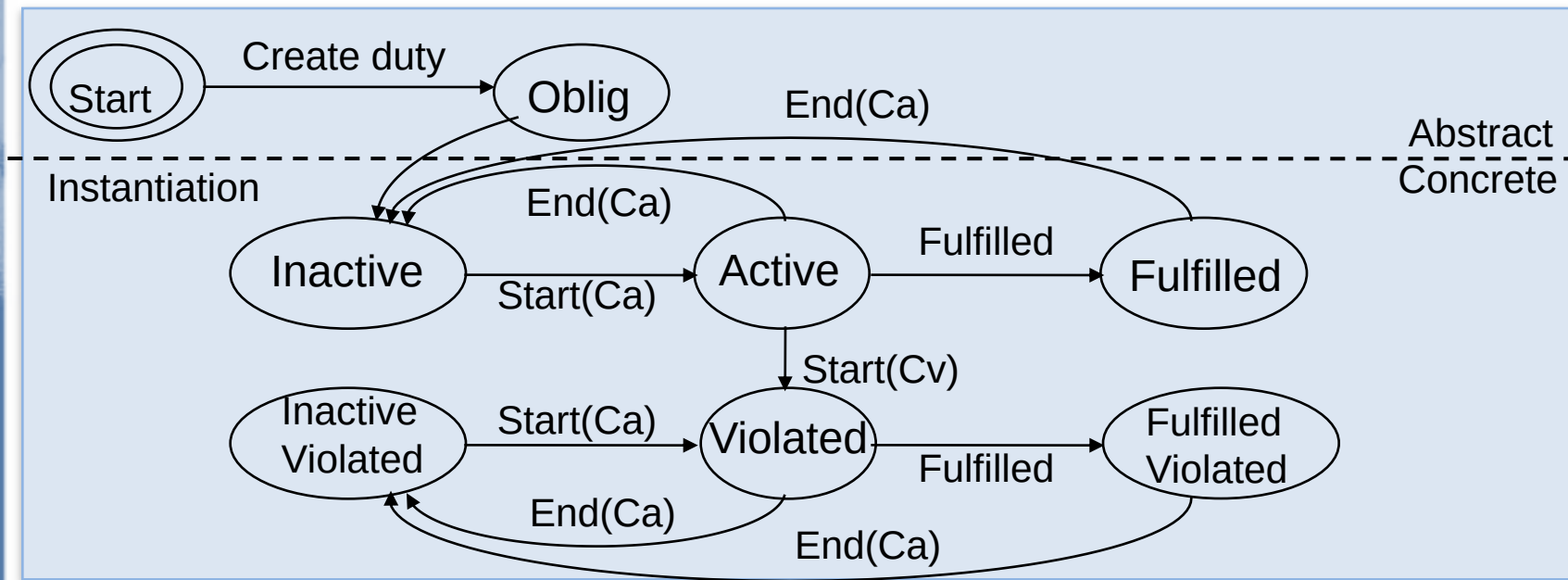


Permission(Rep_AO, Partenaire, Rediger, WP, Participation_WP)*



Contrôle d'usage

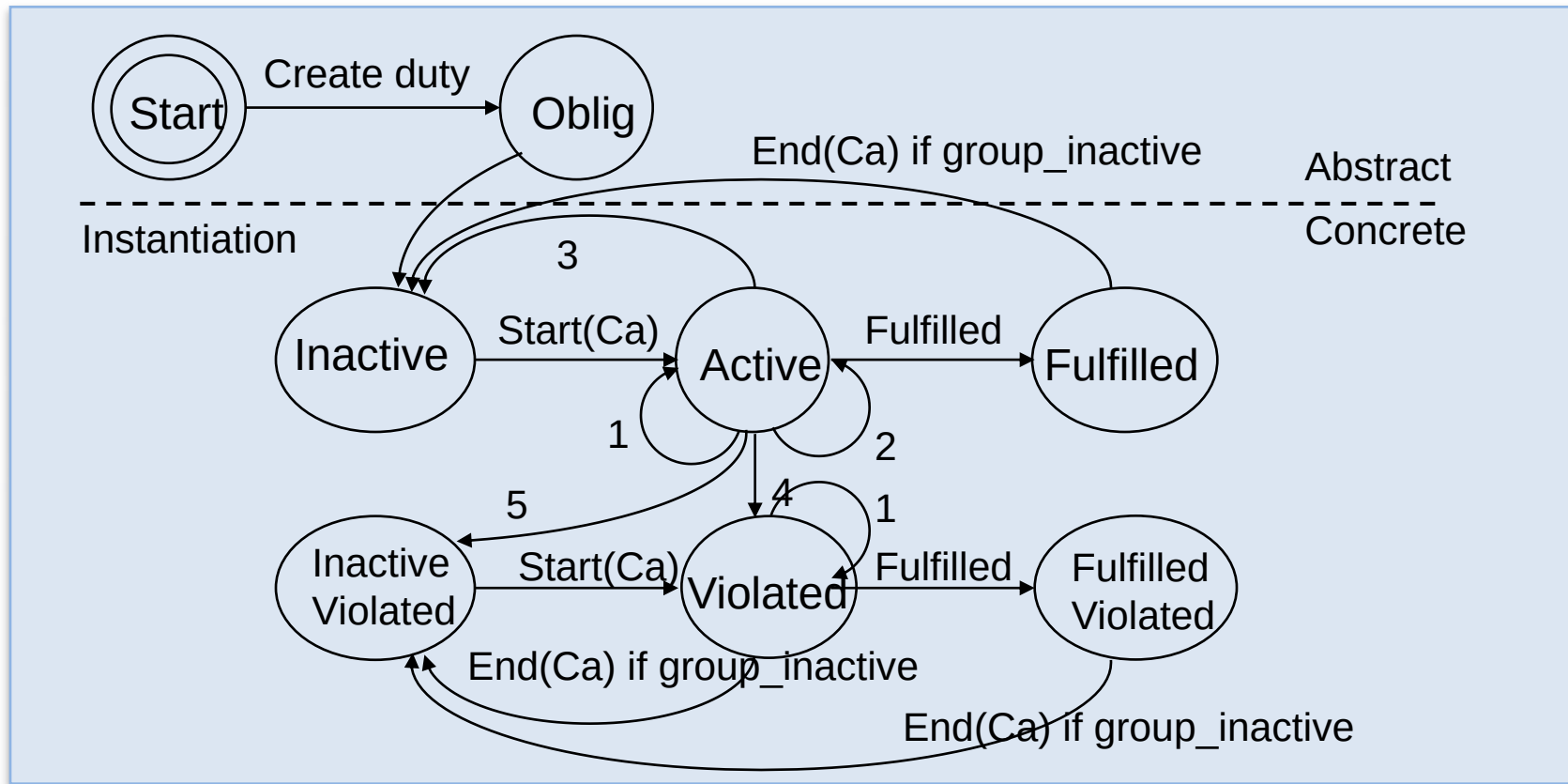
- R4 : Obligation d'élaborer l'annexe financière
Obligation(Rep-AO, Partenaire, Rediger, AF,
[accord_partenaire, deadline_AO], (deadline_AO – 1j))
 - Formalisation reposant sur les ECA rules
 - Composition de contextes
 - Preuve de déterminisme et de terminaison





Contrôle d'usage

- R5 : Obligation de relire chaque WP
 - Obligation collective : *Obligation(Rep-AO, Partenaire, Relire, WP, deadline_AO – 7j, diffusion_reponse, $\forall o \exists a \exists s$)*



Contrôle d'usage

- R6 : Obligation de contribuer à l'élaboration d'un WP proportionnellement à la demande financière
 - Utilisation des métadonnées pour détecter la violation
 - Sanction possible : réduction de la demande financière lorsque l'obligation est violée
- Modèle de responsabilité / Délégation
 - Formalisation des différentes dimensions de la responsabilité
 - responsabilité causale, fonctionnelle, liability
 - Gestion de la responsabilité en cas de délégation
 - Délégation de la responsabilité fonctionnelle
 - Délégation de la liability
 - Qui est responsable et doit être sanctionné en cas de violation

Le point de vue juridique :

Les obligations de sécurité

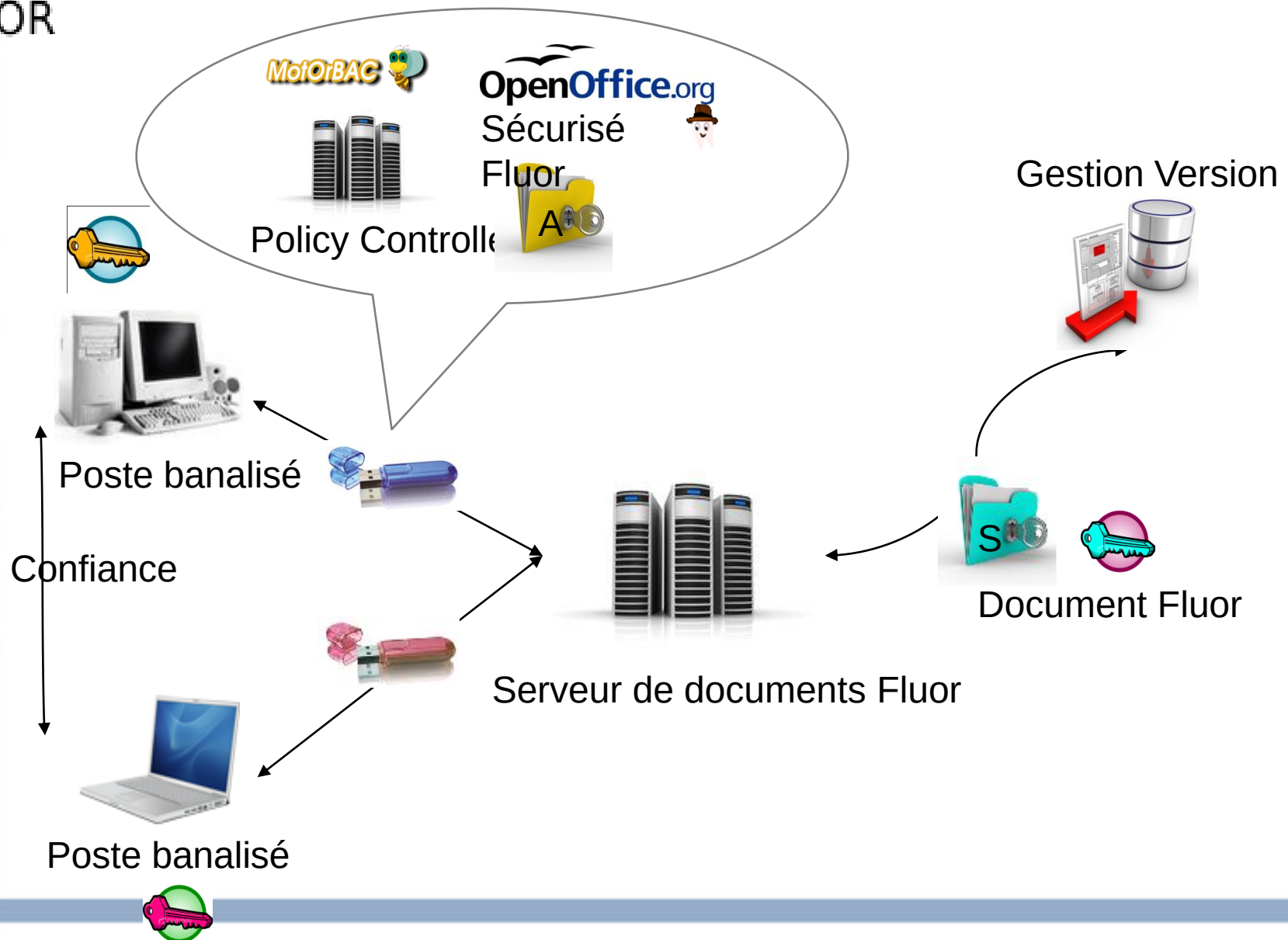
- Définition et objectif
 - Droit commun et obligation de sécurité
- Acteur majeur : le responsable de traitement
 - Mettre en place les moyens de protéger les données personnelles
- Le code pénal réprime les actions portant atteinte aux données personnelles
- Obligation de notifier en cas de violation
 - Absence d'éléments concrets pour la mise en œuvre

Contrôle de flux

- R7 : Déclassification sur ordre du coordonnateur d'une partie d'un WP car dépendance avec un autre WP
 - Politique de sécurité multi-niveaux avec déclassification
 - Contrôle de flux dans un système d'information actif
 - Spécification du système avec des ECA rules
 - Modèle de traces pour les propriétés de sécurité
 - Propriétés de confidentialité et d'intégrité
 - Propriétés de cohérence : détection des déclassifications implicites par déduction ou abduction

- R8 : Déclassification automatique de la synthèse si le projet est accepté
 - Déclassification sur événement
 - Langage d'expression de la politique de déclassification
 - Également basé sur les ECA rules
- declassify_event(content(Synth, Cont),public)*
After Do(insert(accept(Proj))
If has_synthesis(Proj,Synth), has_content(Synth,Cont) ;
- declassification_rule: declassify_event(P,L)*
initiates do(declassify(P,L)) ;
- Spécification des propriétés de sécurité sous forme d'invariants
 - Preuves des propriétés en B
 - Implémentation sous Oracle qui se fonde sur les VPD

Mise en œuvre : mode déconnecté



- Projet novateur
 - Cadre unique pour l'expression d'exigences de sécurité
 - Documents intelligents
 - Traçabilité et gestion de la confiance
- Actions de dissémination
 - Organisation de DPM (Data Privacy Management)
 - Organisation de SETOP (Spontaneous and Autonomous Security)
- Transfert industriel
 - Plugin de Open Office pour sécuriser des documents
 - Déploiement en environnement non contrôlé via l'approche non connectée
- Applications potentielles pour le cloud
 - Expression de politiques de haut niveau

Conclusion / Perspectives

- Gestion du mode déconnecté
 - Mécanismes de compensation a posteriori
 - Fluor 2 ?
- Travail via un navigateur
- Anonymisation → OpenStreetMap (?)
- Dématérialisation des actes notariés
 - Une confiance assurée par l'usage de la clé REAL personnelle à chaque notaire
 - Tele@ctable
 - Archivage sécurisé par le MICEN
 - Echanges cryptés entre les parties

- M. Munier, *A Secure Autonomous Document Architecture for Enterprise Digital Right Management*, 7th International Conference on Signal Image Technology & Internet Based Systems (SITIS'2011), Dijon, France, November 2011.
- Alban Gabillon. *Protection of Geographic Data*. Keynote Speaker. ACM/IEEE International Workshop on Security and Privacy Preserving in e-Societies (Seces'11). Lebanon. June 2011.
- X. Zheng, P. Maillé, S. Morucci, and C. T. Phan Le. Improving the Efficiency of Collaborative Work with Trust Management, in Proc. of 1st IFIP/IEEE Workshop on Managing Federations and Cooperative Management (ManFed.CoM), Dublin, Ireland, May 2011.
- A. Gabillon, P. Capolsini. *Rule-based Policy Enforcement Point for Map Service*. SPRINGL 2010. SIGSPATIAL ACM GIS 2010 International Workshop on Security and Privacy inGIS and LBS. November 2010. San Jose,CA, USA. ACM New York, NY, 2010. ISBN: 978-1-4503-0435-1.
- A. Gabillon and L. Letouzey. *A View-Based Access Control Model for SPARQL*. In Proc of the 2010 Network and System Security conference (NSS2010), Melbourne, Australia November 15th, 2010. ISBN: 978-1-4244-8484-3.
- Alban Gabillon, Patrick Capolsini: *Security mechanisms for geographic data*. p 297-302. MEDES '10: International ACM Conference on Management of Emergent Digital EcoSystems, Bangkok, Thailand, October 26-29, 2010. ACM 2010, ISBN 978-1-4503-0047-6.
- M. Munier, *A multi-view approach for embedded information system security*, 5th International Conference on Risks and Security of Internet and Systems (CRISIS'2010), Montréal, Québec, Canada, October 2010.
- Annie Blandin, La composition d'un espace européen autour du régime juridique des données personnelles, Journée d'études ETOS (Institut Télécom) et CERI (Sciences Po Paris), Technologies de la sécurité, mobilité et exceptionnalité, 5 mai 2011.

- X. Zheng, P. Maillé, S. Morucci, and C. T. Phan Le. Trust mechanisms for efficiency improvement in collaborative working environments, in Proc. of MASCOTS 2010 (short paper), Miami, FL, USA, Aug 2010.
- L. Letouzet, A. Gabillon. *Un modèle de contrôle d'accès pour les données RDF*. 5th Conference on Security in Network Architectures and Information Systems (SAR-SSI '10). Mai 2010. Nice.
- P. Capolsini, and A. Gabillon, Security policies for the Visualization of Geo Data, ACM SIGSPATIAL GIS 2009 International Workshop on Security and Privacy in GIS and LBS (SPRINGL'09). pp.02-11, November, 3rd 2009, Seattle, WA, USA, 2009.
- Gabillon, A. and P. Capolsini. Dynamic Security rules for Geo Data. in International workshop on Autonomous and Spontaneous Security (SETOP'09). 2009. St Malo, France: LNCS 5939 - Springer-Verlag. p. 136-152.
- A. Gabillon, and P. Capolsini, Modelling Security Policies for Geo Data,. 4th Conference on Security in Network Architectures and Information Systems (SAR-SSI '09). pp. 243-262, June, 22-26th 2009, Luchon, France, 2009
- C. T. Phan Le, F. Cuppens, N. Cuppens-Boulahia, and P. Maillé. Evaluating the trustworthiness of contributors in a collaborative environment, in Proc. of TrustCol (Orlando, FL, USA), Nov 2008.
- Romuald Thion, Daniel Le Métayer: FLAVOR: A Formal Language for a Posteriori Verification of Legal Rules. POLICY 2011: 1-8
- Daniel Le Métayer. Privacy by Design: A Matter of Choice. In Data Protection in a Profiled World, Springer 2010
- G. Piolle. *A dyadic operator for the gradation of desirability*, Proceedings of the 10th International Conference on Deontic Logic in Computer Science (DEON'10)", Springer Verlag, 2010, vol. 6181.

- Y. Elrakaiby, Frédéric Cuppens, N. Cuppens-Boulahia: Formal enforcement and management of obligation policies. *Data Knowl. Eng.* 71(1): 127-147 (2012)
- J. A. Thomas, N. Cuppens-Boulahia, F. Cuppens: Declassification Policy Management in Dynamic Information Systems. *ARES 2011*: 143-152
- Julien A. Thomas, Frédéric Cuppens, Nora Cuppens-Boulahia: Consistency Policies for Dynamic Information Systems with Declassification Flows. *ICISS 2011*: 87-101
- M. Ben Ghorbel-Talbi, F. Cuppens, N. Cuppens-Boulahia, D. Le Métayer, and G. Piolle Delegation of Obligations and Responsibility. *IFIP SEC 2011 - Future Challenges in Information Security and Privacy for Academia and Industry*. Lucerne, Switzerland, June 7-9, 2011.
- Frédéric Cuppens, Nora Cuppens-Boulahia: Multilevel Security Policies. *Encyclopedia of Cryptography and Security* (2nd Ed.) 2011: 811-812
- Yehia Elrakaiby, Frédéric Cuppens, Nora Cuppens-Boulahia: An Integrated Approach for the Enforcement of Contextual Permissions and Pre-Obligations. *IJMCMC* 3(2): 33-51 (2011)
- Catherine Barreau-Saliou personal data, privacy and competition law . Communication in sustainable development and global challenges, Chemnitz, Germany, July, 2011
- Yehia Elrakaiby, Frédéric Cuppens, Nora Cuppens-Boulahia: From Contextual Permission to Dynamic Pre-obligation: An Integrated Approach. *ARES 2010*: 70-78
- Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens, Nora Cuppens-Boulahia: Negotiating and delegating obligations. *MEDES 2010*: 281-288

- Julien A. Thomas, Nora Cuppens-Boulahia, Frédéric Cuppens: Expression and enforcement of confidentiality policy in active databases. MEDES 2010: 289-296
- Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens, Nora Cuppens-Boulahia, Adel Bouhoula: A delegation model for extended RBAC. Int. J. Inf. Sec. 9(3): 209-236 (2010)
- F. Cuppens, N. Cuppens-Boulahia. Specification et gestion des obligations pour le besoin de controle d'usage (un aperçu). Genie Logiciel, 94, May 2010.
- F. Cuppens, N. Cuppens-Boulahia. Specification and management of obligations for usage control. Invited speaker. CRISIS 2010, Montréal Canada, 2010.
- Yehia Elrakaiby, Frédéric Cuppens, Nora Cuppens-Boulahia: From state-based to event-based contextual security policies. ICDIM 2009: 241-247
- Yehia Elrakaiby, Frédéric Cuppens, Nora Cuppens-Boulahia: Formalization and Management of Group Obligations. POLICY 2009: 158-165
- Meriam Ben-Ghorbel-Talbi, Frédéric Cuppens, Nora Cuppens-Boulahia, Adel Bouhoula: An Extended Role-Based Access Control Model for Delegating Obligations. TrustBus 2009: 127-137
- Yehia Elrakaiby, Frédéric Cuppens, Nora Cuppens-Boulahia: Interactivity for Reactive Access Control. SECRIPT 2008: 57-64
- Julien A. Thomas, Nora Cuppens-Boulahia, Frédéric Cuppens. Environmental constraints management in digital right licences. SARSSI 2008 : 3ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information, Loctudy, France, 2008.

Thèses

- Y. Elrakaiby, Télécom Bretagne, soutenue décembre 2010
- L. Letouzey, UPF, soutenue en Juin 2011
- J.A. Thomas, Télécom-Bretagne, soutenue décembre 2011
- S. Moine, Télécom-Bretagne-IODE, prévue début 2012



FLUOR

Communications/Publications : Synthèse

Type	Revue	Conférence	Thèse	Conférence invité	Publications communes
Nombre	5	28	3 + 1	3	5