



HAL
open science

Assistance à l'ingénierie de logiciels pour mieux protéger la vie privée des utilisateurs

Selena Lamari, Nadja Benblidia, Chouki Tibermacine, Christelle Urtado, Sylvain Vauttier

► **To cite this version:**

Selena Lamari, Nadja Benblidia, Chouki Tibermacine, Christelle Urtado, Sylvain Vauttier. Assistance à l'ingénierie de logiciels pour mieux protéger la vie privée des utilisateurs. GdR GPL 2024 - Journées nationales du GdR Génie de la Programmation et du Logiciel, Jun 2024, Strasbourg, France. 2024. ⟨hal-04689927⟩

HAL Id: hal-04689927

<https://imt-mines-ales.hal.science/hal-04689927v1>

Submitted on 6 Sep 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

Assistance à l'ingénierie de logiciels pour mieux protéger la vie privée des utilisateurs

Selena Lamari^{1,2}, Benblidia Nadja², Chouki Tibermacine¹, Christelle Urtado³, Sylvain Vauttier³

¹ LIRMM, Univ. Montpellier, CNRS, Montpellier, France ² LRDSI, Univ. Blida 1, Blida, Algeria
³ EuroMov Digital Health in Motion, Univ. Montpellier & IMT Mines Ales, Ales, France

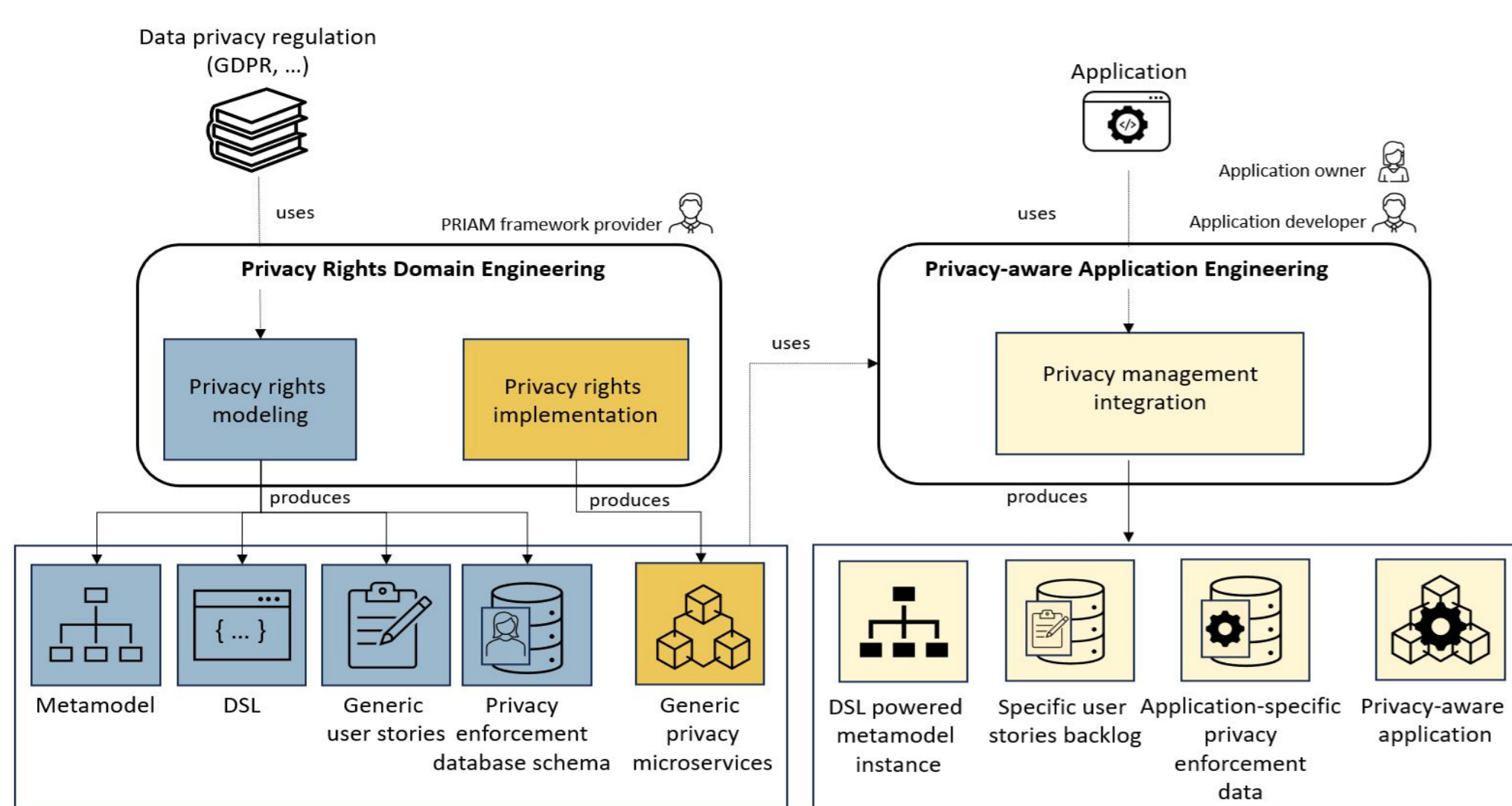
I. Contexte et motivation

- Depuis 2018 : **obligation d'implémenter le RGPD**, règlement européen de protection de la vie privée des utilisateurs par la protection des données personnelles.
- Mise en oeuvre **fastidieuse** pour les développeurs, en raison de la **longueur** et de la **complexité** du texte réglementaire.

Proposition d'une solution assistant les développeurs dans la mise en conformité au RGPD³ de leurs applications

II. PRIAM : Approche globale à 3 étapes

1. Formaliser les **concepts** d'un **règlement** à l'aide d'un **métamodèle** (Domain Engineering).
2. Fournir des **artéfacts génériques facilitant** l'implémentation des concepts du règlement dans des **applications en cours de développement** ou déjà **existantes** (évolution).
3. Proposer un **processus** et des **outils** permettant d'**adapter** les artéfacts génériques aux besoins spécifiques de chaque application (Application Engineering).

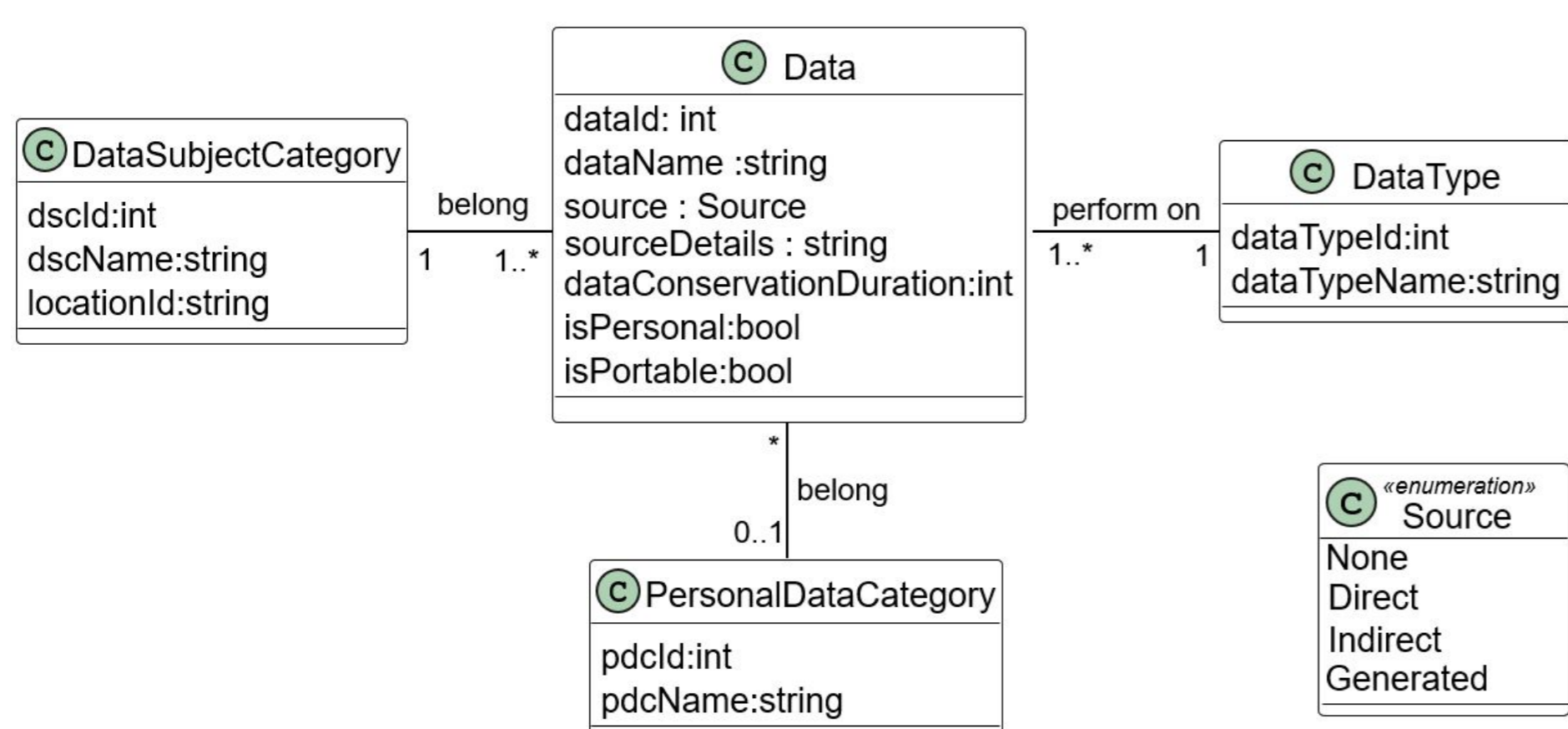


Approche proposée pour l'intégration de la protection de la vie privée

A. Modélisation du droit à la vie privée

1. Conception du métamodèle PRIAM

- Défini à partir du texte **réglementaire de la RGPD**.
- Comportant **50 classes** regroupées en **7 packages**.
- **Validation qualitative** par des **experts du domaine** (DSI, juristes) en utilisant un **questionnaire**⁴ évaluant la conformité au RGPD.



Extrait du métamodèle PRIAM (package "Data")

³ <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

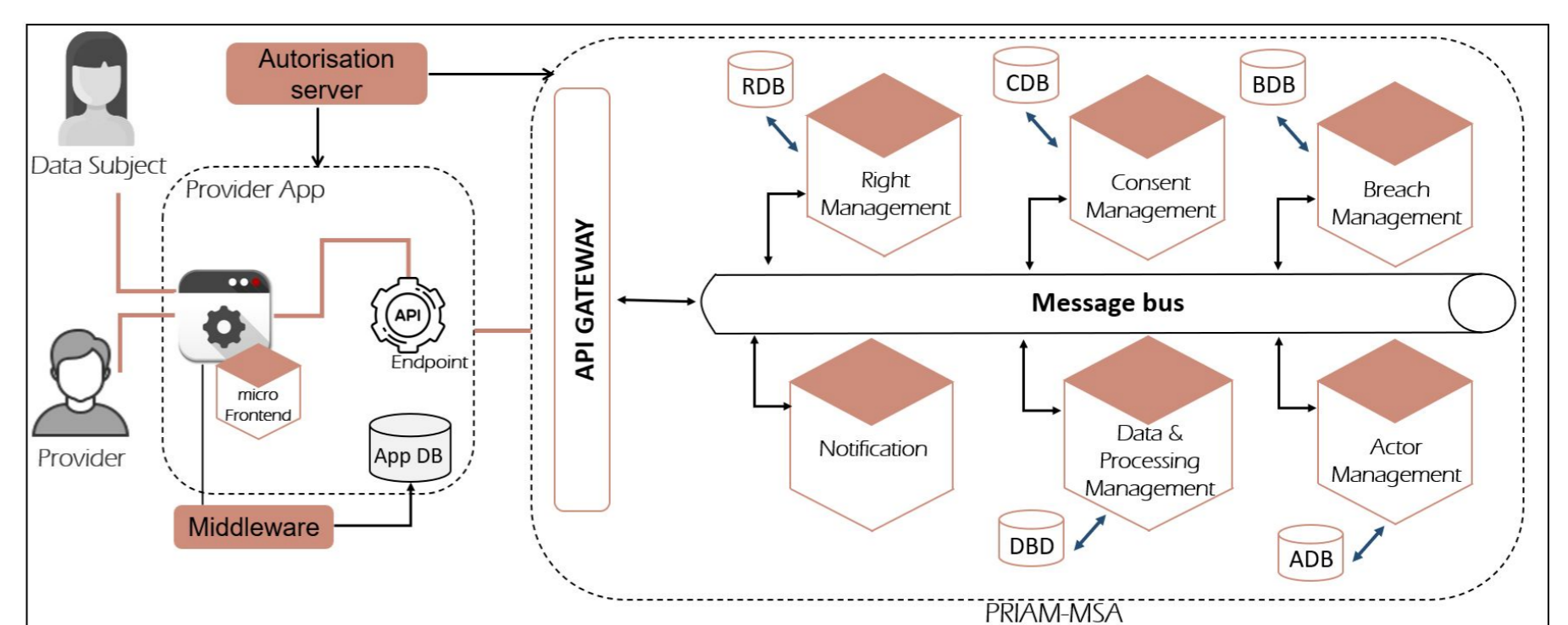
⁴ <https://www.dataprotection.ie/sites/default/files/uploads/2019-04/A-Guide-to-help-SMEs-Prepare-for-the-GDPR.pdf>

2. Conception d'un outillage d'IDM basé sur le métamodèle PRIAM

- **User stories génériques**.
- **Schéma de base de données générique** (BD PRIAM).
- **DSL** permettant d'**adapter** les artéfacts génériques aux **besoins spécifiques des applications**.

B. Implémentation des droits de la protection de la vie privée

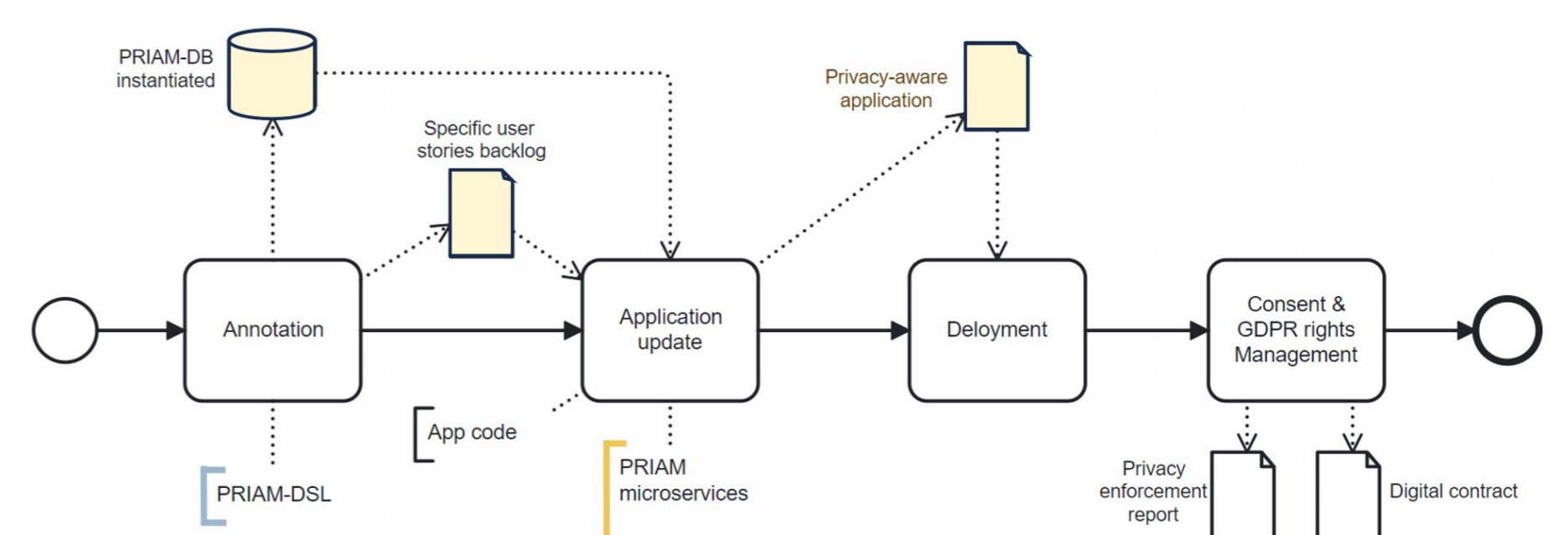
- Basée sur une **architecture à microservices** qui couvre les exigences du RGPD (implémentation des user stories génériques).
- Assure la **gestion d'accès aux données** en se basant sur le **consentement** des utilisateurs (interception des requêtes).
- Intègre un système de **sécurité OAuth2** (SSO) pour la **gestion de l'authentification**.



Architecture à microservices de PRIAM

C. Intégration de la gestion de la vie privée

1. **Annotation** manuelle des données personnelles et de leurs traitements à l'aide du **DSL**.
2. **Génération** automatique des **user stories** spécifiques.
3. **Génération** automatique du **script d'instanciation** spécifique de la **BD PRIAM**.
4. **Intégration** semi-automatique des **micro-services** à l'application en se basant sur les artéfacts spécifiques générés.
5. **Déploiement** de l'application **conforme au RGPD**.



Aperçu du processus de mise en vigueur de la Privacy

PoC sur un **cas d'étude** : application "Tea Store" utilisée comme démonstrateur dans le cadre de l'atelier Cisco Full Stack Observability⁵

III. Perspectives

- Réaliser des **expériences à grande échelle**, sur des applications plus vastes.
- **Généraliser l'approche** pour supporter tout autre règlement ayant un impact sur les exigences d'une application.

⁵ <https://github.com/DescartesResearch/TeaStore>