# Proposition de thèse en

# Cybersécurité et Utilisabilité

**Titre :** Approches basées modèles pour la conception et le développement de systèmes interactifs de gestion d'identité auto-souveraine utilisables et sûrs

**Mots clés :** Cybersécurité, Gestion des identités, Utilisabilité, Acceptabilité

**Title:** Model-based approaches to design and develop usable and dependable self-sovereign identity management interactive systems

**Keywords:** Cybersecurity, Identity Management, Usability, Acceptability

**Dates :** Octobre 2026 - Septembre 2029

**Unité de recherche :** Institut de Recherche en Informatique de Toulouse (IRIT)

**Directeurs de la thèse :** Romain Laborde (équipe SIERA), Célia Martinie (équipe ICS), Philippe Palanque (équipe ICS)

**Description du sujet**

L'identité auto-souveraine (Self-Sovereign Identity) [7] est un concept de gestion d'identité qui redonne aux utilisateurs le contrôle sur leurs données d'identité tout en diminuant celui des fournisseurs d'identités que l'on trouve dans les fédérations d'identités (e.g. Google Sign-In ou Facebook Connect). Cette nouvelle approche permet aussi aux utilisateurs de choisir et limiter les données personnelles qu'ils exposent aux services, contribuant ainsi à la confidentialité de leurs données (privacy).

Cependant, cette capacité à pouvoir contrôler son identité numérique a un impact sur la performance humaine car cela ajoute aux utilisateurs des activités articulatoires qui ne correspondent pas aux buts principaux de ces utilisateurs. Par exemple, lorsque le but principal d'un utilisateur est de consulter des documents dans le cloud, l'utilisateur ne consulte pas directement les documents après avoir entré l'adresse du cloud. Avant cela, elle/il s'identifie et effectue donc des actions supplémentaires avant d'accéder à ses documents. Ces activités articulatoires lui demandent d'engager des ressources supplémentaires (e.g. temporelles, cognitives, motrices…) et diminuent sa performance globale [3]. L'utilisateur du mécanisme d'identité auto-souveraine a notamment des actions de création, configuration et maintenance de portefeuilles d'identités numériques.

De manière générale, les politiques et mécanismes de sécurité ont un impact sur la performance humaine [1], et pas seulement pour les utilisateurs finaux. Les administrateurs des mécanismes de sécurité, chargés des politiques de sécurité et de leur mise en œuvre via différents mécanismes, ont des tâches différentes selon la politique de sécurité et les types de mécanisme. D'autre part, les entités qui effectuent des cyberattaques mènent des tâches plus ou moins complexes en fonction des politiques et mécanismes déployés. Les méthodes de conception et développement de mécanismes de sécurité utilisables et sûrs doivent donc permettre d'analyser dans quelle mesure les politiques de sécurité, mises en œuvre via ces mécanismes, fonctionnent comme spécifiées et dans quelle mesure elles impactent les tâches des utilisateurs finaux, des administrateurs et des entités attaquantes, sachant qu'un impact négatif peut

diminuer l'acceptabilité de ces mécanismes auprès des utilisateurs finaux (par exemple un temps d'attente jugé trop long pour des vérifications avant d'accéder à un service) [5] et des administrateurs.

Cette thèse traitera des méthodes pour concevoir des mécanismes de sécurité prenant en compte l'utilisabilité et de l'acceptabilité par les différents usagers. Ces méthodes seront appliquées aux mécanismes d'identité auto-souveraine, dont un premier prototype a été développé dans le cadre du projet TRUSTINClouds [8]. Elles pourront aussi être appliquées à d'autres types de mécanismes de sécurité.

Une première approche envisagée consiste à étudier les approches de vérification continue des politiques de sécurité basée modèles. Les méthodes et techniques basées modèles permettraient de décrire une politique de sécurité, les mécanismes de sécurité à mettre en œuvre dans le cadre de cette politique, ainsi que les systèmes interactifs nécessaires pour les utilisateurs et les tâches des utilisateurs. Les modèles produits seraient intégrés et mis en correspondance afin de vérifier que la politique de sécurité fonctionne comme spécifié de bout en bout, ainsi que son impact sur les tâches utilisateurs. Ces modèles ont vocation à évoluer rapidement en fonction de l'évolution des attaques et des politiques de sécurité. La maintenance et l'évolutivité des modèles est un élément clé de l'approche. De plus, nous proposerons des méthodes pour définir des IHM adaptées aux différentes catégories d'utilisateurs finaux, leur permettant d'exprimer les politiques d'usage (par exemple au moyen de langages visuels e.g. [2] selon leur niveau de compétence et selon l'utilisation qu'ils comptent faire de ces données. Dans le cas d'utilisateurs novices ou intermédiaires les interfaces devront être compatibles avec les principes « walk-up and use » [4] alors que pour les utilisateurs experts, comme les administrateurs, le matériel de formation sera construit en même temps que les interfaces et interactions [6]. Enfin, un effort tout particulier sera réalisé pour permettre aux différents utilisateurs de percevoir, comprendre et adapter les politiques d'usage définies. Ces solutions garantiront par construction l'acceptation des nouveaux mécanismes, de leurs interfaces utilisateurs afin de prévenir les rejets lors du déploiement tel que cela a été le cas de la solution d'identité numérique Alicem de ANTS abandonnée en 2022.

L'approche permettra d'aboutir à des solutions techniques qui seront par construction sécurisée, respectueuses des réglementations et acceptables par les usagers. Il sera nécessaire de caractériser les différents types d'usagers, leurs besoins et leurs compétences pour proposer des IHM adaptées.

**Contexte et environnement**

Cette offre de thèse s'inscrit dans le cadre du projet PEPR TRUSTINCloudS (https://trustinclouds.ovh/), qui vise à développer des solutions pour répondre aux principaux défis de cybersécurité propres aux environnements Cloud. Les travaux menés dans ce projet ont pour objectif d'adapter les mécanismes de sécurité traditionnels (notamment ceux développés dans le cadre de PEPR Cyber) aux spécificités des environnements Cloud, afin de faire face aux menaces propres aux différents modèles de Cloud (IaaS, PaaS, etc.).

L'objectif principal de TRUSTINCloudS est donc d'étudier et de développer de nouvelles méthodologies permettant de renforcer la sécurité du Cloud, puis de les mettre en œuvre au sein de plateformes expérimentales, dans la perspective de construire un Cloud souverain et digne de confiance.

Le projet est structuré autour de deux axes principaux : la sécurisation des infrastructures Cloud et la sécurisation des données hébergées sur ces infrastructures. Des travaux scientifiques seront menés sur ces deux thématiques afin de concevoir de nouvelles méthodes et de nouveaux outils pour améliorer la sécurité des infrastructures et des données.

Nous offrons un environnement de travail dynamique et respectueux dans le sud de la France, au sein d'une équipe très motivée réunissant des profils aux expertises et compétences variées. La personne recrutée bénéficiera d'un excellent environnement scientifique, de technologies récentes et d'un encadrement assuré par des chercheurs de renommée internationale dans ce domaine. Elle aura également l'opportunité d'intégrer dans ses travaux de recherche des dimensions multidisciplinaires, académiques et industrielles.

Le financement comprend le salaire ainsi que les frais associés au projet (ordinateur, participation aux réunions de projet et aux conférences scientifiques).

**Profil recherché**

Nous recherchons des candidats et candidates titulaires d'un diplôme d'ingénieur ou d'un Master en informatique, disposant de compétences dans un ou plusieurs des domaines suivants : génie logiciel, systèmes d'information, cloud computing, cybersécurité, IHM

La candidate ou le candidat devra également avoir démontré :

- de la créativité et une capacité d'analyse et de synthèse,
- de solides compétences techniques, ainsi que de bonnes aptitudes relationnelles et de communication,
- un fort engagement dans le travail et la capacité à proposer de nouvelles idées.

**Dates importantes**

L'examen des candidatures se poursuivra **jusqu'à ce que le poste soit pourvu**. Le **début du doctorat est prévu pour le 1er octobre 2026**.

**Candidature**

Les candidatures doivent être envoyées **par email** et comprendre les documents suivants :

- un curriculum vitae,
- les relevés de notes et diplômes (Master et Licence/Bachelor),
- une lettre de motivation incluant une déclaration d'intérêt pour la recherche,
- des lettres de recommandation.

Les dossiers doivent être envoyés aux adresses suivantes : romain.laborde@irit.fr et celia.martinie@irit.fr

**À propos des institutions d'accueil**

L'Université de Toulouse est l'une des principales universités françaises. Elle propose des formations dans les domaines des sciences, de la santé, du sport, de la technologie et de l'ingénierie. L'université compte plus de 31 000 étudiants, encadrés par plus de 2 500 enseignants-chercheurs et enseignants permanents. Chaque année, environ 400 doctorats sont délivrés par les 11 écoles doctorales de l'université. Le doctorant ou la doctorante suivra le programme doctoral intitulé « Mathématiques, Informatique et Télécommunications » (MITT). Des informations générales sur le doctorat sont disponibles sur le site de l'université (https://en.univ-toulouse.fr/research-dynamics-phd/doctoral-programmes).

L'Institut de Recherche en Informatique de Toulouse (IRIT) regroupe plus de 700 membres, dont environ 400 chercheurs et enseignants-chercheurs, ce qui en fait le plus grand laboratoire d'informatique

en France. Les chercheurs de l'IRIT sont rattachés à plusieurs institutions partenaires : le CNRS (Centre National de la Recherche Scientifique), l'INPT (Institut National Polytechnique de Toulouse), l'Université de Toulouse, l'Université Toulouse Capitole ou l'Université Toulouse Jean Jaurès. Les 21 équipes de recherche du laboratoire travaillent autour de sept grandes thématiques scientifiques, couvrant la majorité des domaines de l'informatique. Pour plus d'informations voir https://www.irit.fr

## À propos de Toulouse

Pour plus d'informations sur la ville de Toulouse, vous pouvez consulter le site officiel du tourisme de la ville (https://www.toulouse-tourisme.com/en/).

## Références


[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. Commun. ACM 42, 12 (Dec. 1999), 40–46. https://doi.org/10.1145/322796.322806

[2] Sven Coppers, Davy Vanacken, and Kris Luyten. 2020. FORTNIoT: Intelligible Predictions to Improve User Understanding of Smart Home Behavior. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 4, 4, Article 124 (December 2020), 24 pages. https://doi.org/10.1145/3432225

[3] Nicolas Broders, Célia Martinie, Philippe Palanque, Marco Winckler, Kimmo Halunen. (2020). A Generic Multimodels-Based Approach for the Analysis of Usability and Security of Authentication Mechanisms. Human-Centered Software Engineering. HCSE 2020. Lecture Notes in Computer Science, vol 12481. Springer, Cham. https://doi.org/10.1007/978-3-030-64266-2_4

[4] Clayton Lewis, Peter G. Polson, Cathleen Wharton, and John Rieman. 1990. Testing a walkthrough methodology for theory-based design of walk-up-and-use interfaces. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '90). Association for Computing Machinery, New York, NY, USA, 235–242. https://doi.org/10.1145/97243.97279

[5] Korir, Maina, Simon Parkin, and Paul Dunphy. 2022. An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control. Eighteenth symposium on usable privacy and security (SOUPS 2022), Usenix, https://www.usenix.org/system/files/soups2022-korir.pdf

[6] Célia Martinie, David Navarre, Philippe Palanque, Eric Barboni, and Sandra Steere. 2022. Engineering Operations-based Training. Proc. ACM Hum.-Comput. Interact. 6, EICS, Article 164 (June 2022), 25 pages. https://doi.org/10.1145/3534518

[7] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, Christoph Meinel, A survey on essential components of a self-sovereign identity, Computer Science Review, Volume 30, 2018, Pages 80-86, ISSN 1574-0137, https://doi.org/10.1016/j.cosrev.2018.10.002

[8] M. A. B. H. Salah, R. Laborde, D. Canavese, A. Benzekri, M. A. Kandi and A. Ferreira. XCId: An SSI-Based Cross-Cloud Identity Wallet, *2025 IEEE Conference on Communications and Network Security (CNS)*, 2025, pp. 1-9, https://ieeexplore.ieee.org/document/11195041


## Contacts


- Romain Laborde : romain.laborde@irit.fr
- Célia Martinie : celia.martinie@irit.fr
- Philippe Palanque : philippe.palanque@irit.fr