

DESIRE : une Troisième Voie pour un Système Européen de Notification d'Exposition¹

Tirer le meilleur des systèmes centralisés et décentralisés

Vincent Roca², Nataliia Bielova, Antoine Boutet, Claude Castelluccia,
Mathieu Cunche, Cédric Lauradoux, Daniel Le Métayer
Équipe PRIVATICS Inria, France
desire-contact@inria.fr

9 Mai 2020

Une finalité : construire une troisième voie qui prend le meilleur des approches centralisées et décentralisées

Le virus COVID-19 est difficile à détecter car de nombreuses personnes peuvent être porteuses, et donc contagieuses, sans le savoir et avant même d'en ressentir les symptômes. Lorsqu'une personne est testée positive au COVID-19, les professionnels de santé effectuent une « recherche des contacts » en demandant à la personne infectée de fournir des informations sur toutes les personnes qu'elle a côtoyées. Mais cette recherche manuelle est peu efficace si la personne infectée s'est rendue dans des lieux très fréquentés, comme des supermarchés et transports en commun, où elle a été en contact avec de nombreux inconnus.

L'objectif principal d'une application de notification d'exposition est de compléter la « recherche manuelle des contacts » et d'informer les personnes qui ont été à proximité de porteurs du virus COVID-19 même si ces porteurs n'ont même pas été testés au moment de l'interaction.

A ce jour, deux familles de protocoles existent en Europe : les protocoles dits « centralisés » (qui reposent sur la transmission des pseudonymes « exposés », d'une application d'une personne testée positive vers un serveur central) et les protocoles dits « décentralisés » (qui reposent sur la transmission par un serveur central des pseudonymes des personnes testées « positives » vers tous les smartphones). Ces protocoles ont, chacun, des avantages et des inconvénients, en matière de résistance à des attaques (effectuées par l'autorité centrale ou par des utilisateurs), en matière de contrôle par l'Autorité de Santé. Du fait de la nature différente des données, ils ne sont pas facilement interopérables.

Ce document présente une autre voie pour rassembler le meilleur des deux approches, dans l'objectif d'avoir un protocole interopérable à moyen terme au niveau européen : le protocole DESIRE – une évolution décentralisée de la proposition [ROBust and privacy-presERving proximity Tracing \(ROBERT\)](#). Deux améliorations majeures sont apportées par DESIRE :

1. Alors que le protocole ROBERT ne s'appuyait que sur des pseudonymes temporaires pour les applications, DESIRE s'appuie sur des « *Private Encounter Tokens* » (« *jetons privés de rencontre* ») ou PET, qui associent un pseudonyme unique et secret

¹ Ce document est conforme à la spécification technique du protocole DESIRE : <https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE>

² Vincent Roca est l'auteur pour tout contact. Les autres auteurs sont listés dans l'ordre alphabétique.

uniquement lors de la rencontre entre deux appareils mobiles à proximité l'un de l'autre. Ces jetons PET sont générés *conjointement et de manière confidentielle par les applications des deux utilisateurs*, ce qui apporte un meilleur niveau de protection de la vie privée. Cette génération locale dans les applications est une forme significative de décentralisation.

2. Toutes les données stockées par l'autorité centrale sont désormais chiffrées à l'aide de clés secrètes stockées sur les appareils mobiles des utilisateurs, ce qui fournit une protection efficace contre d'éventuelles fuites de données.

Ces nouvelles caractéristiques améliorent considérablement les garanties de confidentialité du protocole DESIRE vis-à-vis des autorités ou d'utilisateurs malveillants.

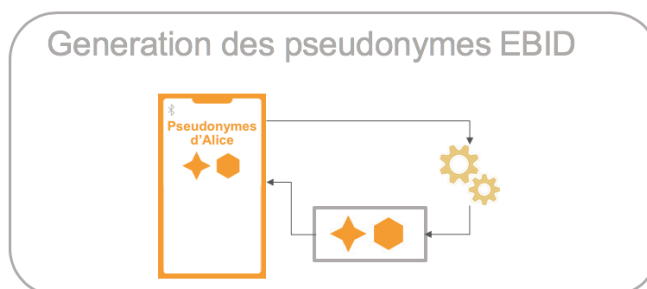
La génération locale des jetons PET de rencontre permet de bénéficier des garanties des approches décentralisées vis-à-vis d'une autorité centrale malveillante. De manière similaire à ROBERT, DESIRE donne la main aux autorités de santé (pour la régulation et l'apprentissage) en matière de gestion dans le cadre d'une stratégie sanitaire globale : il s'appuie sur une autorité centrale pour calculer le « score de risque » - un score qui détermine le niveau d'exposition de l'utilisateur au COVID-19. Avec l'aide d'épidémiologistes, la situation de l'épidémie peut être suivie en temps réel afin d'ajuster dynamiquement l'algorithme qui calcule le « score de risque ». En effet, un facteur clé de succès des applications de traçage de proximité est une intégration harmonisée au dispositif de santé, en particulier la possibilité [d'adapter ce « score de risque » à la situation épidémiologique locale et aux ressources disponibles](#).



Par ailleurs, une version complètement décentralisée du protocole est réalisable (elle n'est pas détaillée ici), modulo la perte d'une partie du contrôle par l'autorité de santé.

DESIRE : Aperçu du Protocole

Lors de son installation, l'application s'enregistre auprès de l'autorité centrale, qui crée un enregistrement dans sa base de données. Ce processus d'inscription utilise des jetons d'autorisation anonymes et est conçu de manière à préserver la vie privée de l'utilisateur. Il garantit également qu'une seule application est utilisée sur chaque appareil mobile, ce qui permet de prévenir certains types d'attaques.

Une fois enregistrée, l'application génère périodiquement de nouveaux pseudonymes temporaires, appelés « *Ephemeral Bluetooth Identifiers* » (*Identifiants Bluetooth éphémères*), ou EBID. On peut les voir comme des « surnoms » associés à l'application de l'utilisateur. En pratique, ils ressemblent à des nombres aléatoires ; dans ce document, par souci de simplicité, nous utiliserons des formes géométriques.



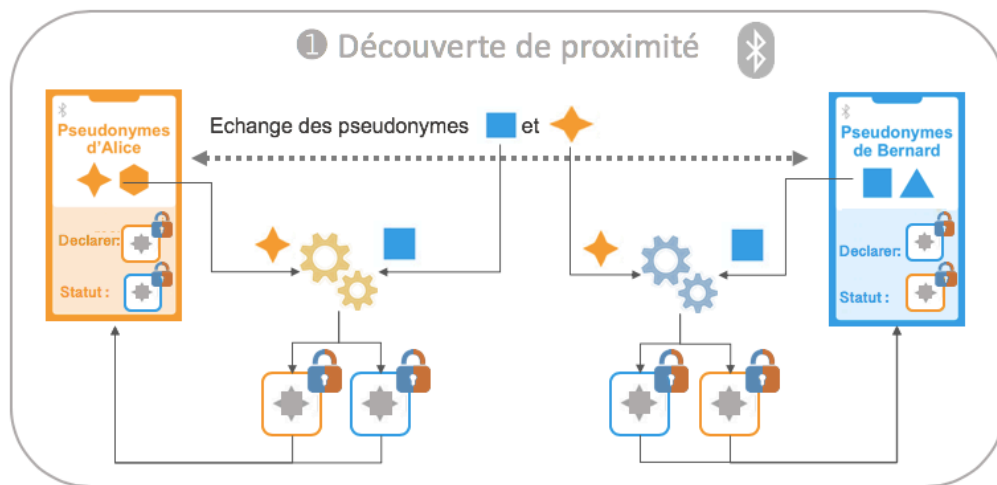
A titre d'illustration et de façon simplifiée, pour l'utilisatrice **Alice**, l'application génère périodiquement des pseudonymes EBID - ici  et  - qui seront utilisés l'un après l'autre. Ces pseudonymes sont destinés à être diffusés à tous les terminaux mobiles à proximité





d'**Alice**, mais ils ne seront jamais communiqués à l'autorité centrale : leur utilisation est locale et temporaire (durée d'utilisation limitée).



Le protocole comporte trois phases principales, décrites ci-dessous : la découverte de proximité, la déclaration suite à un diagnostic positif et la demande de statut d'exposition.

1 Découverte de proximité

L'application mobile d'**Alice** utilise des communications à courte distance en Bluetooth, pour « annoncer » le pseudonyme courant – soit  ou  dans notre exemple – aux utilisateurs qui se trouvent à proximité immédiate d'**Alice**. Dans notre exemple, l'application d'**Alice** annonce sa présence à l'application de **Bernard**.



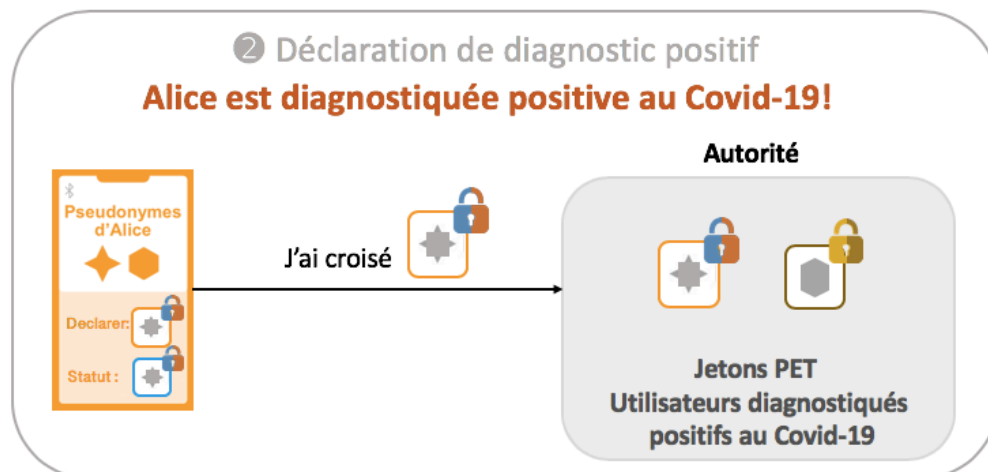
Chaque application mobile collecte tous les pseudonymes des utilisateurs qui sont à proximité. Pour s'assurer que seules les applications d'**Alice** et de **Bernard** enregistrent leur proximité réciproque, le protocole DESIRE s'appuie sur le [schéma d'échange de clés Diffie-Hellman](#) bien connu : avec ce schéma cryptographique, les applications d' **Alice** et de **Bernard** génèrent un secret partagé entre eux appelé « *jeton privé de rencontre* » (jeton PET, illustré par les symboles  et ) grâce à leurs EBID respectifs. L'application d'**Alice** utilisera le jeton orange  durant la phase 2 du protocole pour déclarer ses rencontres au cas où elle s'avérerait positive au test COVID-19 - ce jeton est stocké dans la liste « Déclarer » de l'appareil mobile d'**Alice**. Le jeton bleu  sera utilisé pour demander son statut d'exposition pendant la phase 3 du protocole - ce jeton est stocké dans la liste « Statut » de l'appareil mobile d'**Alice**.

L'application de **Bernard** générera les deux mêmes PET, mais les utilisera dans l'ordre inverse : le jeton bleu  pour déclarer ses rencontres et le jeton orange  pour demander son statut d'exposition.

Ces deux jetons PET ne sont connus que d'**Alice** et de **Bernard**, ils sont stockés localement sur leurs appareils mobiles et aucune autre personne ne peut les relier aux pseudonymes d'**Alice** ou de **Bernard**. De plus, personne ne peut établir de lien entre les jetons orange et bleu.

② Déclaration suite à un diagnostic positif

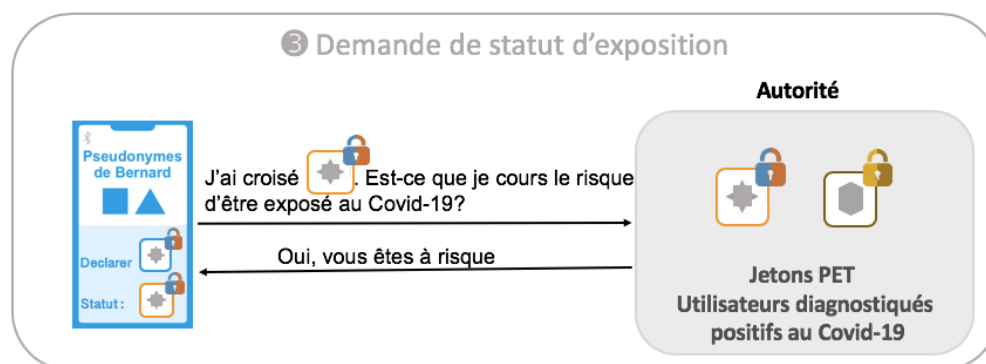
Alice est testée positive au COVID-19. Pour aider les personnes qui l'ont côtoyée pendant la période de contagion, elle accepte de communiquer anonymement à l'autorité centrale les jetons PET générés par son application.



Si **Alice** a un ou plusieurs jetons PET dans sa liste « Déclarer », l'autorité centrale reçoit ces jetons PET de manière indépendante, sans aucune information sur **Alice**. Par conséquent, l'autorité n'a aucune information sur les utilisateurs, en particulier aucun pseudonyme d'utilisateurs testés positifs au COVID-19, et n'est pas en mesure de relier ces jetons PET entre eux afin de construire leur « graphe de proximité ». Chaque fois que l'autorité reçoit un jeton PET, elle stocke ce jeton dans une liste de jetons.

③ Demande de statut d'exposition

Pour vérifier si **Bernard** a été à proximité d'utilisateurs diagnostiqués positifs au COVID-19 au cours des derniers jours (par exemple, deux semaines), l'application de **Bernard** fournit à l'autorité centrale tous les jetons PET de sa liste « Statut ». L'autorité centrale vérifie si les jetons PET de **Bernard** sont présents dans la liste globale des jetons qui indiquent la proximité des utilisateurs diagnostiqués positifs au COVID-19.



Si l'autorité constate que certains des jetons PET de **Bernard** sont présents dans cette liste, elle calcule un « score de risque », qui dépend notamment du nombre de jetons PET présents,

donc du nombre d'utilisateurs diagnostiqués COVID-19 avec lesquels **Bernard** a été en contact (et éventuellement d'autres informations, telles que la durée d'exposition et une estimation de la distance). L'autorité répond ensuite à la demande de **Bernard** en l'informant sur son risque d'exposition au COVID-19.

Avantages de DESIRE en matière de sécurité et de protection de la vie privée

Le principal avantage d'un jeton PET est de constituer un secret partagé uniquement par deux applications qui ont été à proximité. L'utilisation de deux listes de jetons PET différentes, « Déclarer » pour la déclaration de diagnostic positif et « Statut » pour la demande de statut d'exposition, permet d'assurer plusieurs propriétés en matière de sécurité et de confidentialité pour les utilisateurs du protocole DESIRE.

Tout d'abord, tant qu'**Alice** et **Bernard** sont en bonne santé, leurs applications fournissent des jetons différents depuis leurs listes « Statut » pour demander leur statut d'exposition (jeton bleu pour **Alice** et jeton orange pour **Bernard**). *L'autorité centrale n'est pas en mesure de déduire qu'**Alice** et **Bernard** ont été à proximité l'un avec l'autre, car ces jetons bleus et orange ne peuvent pas être reliés l'un à l'autre.*

Deuxièmement, considérons le cas où l'application d'**Alice** demande son statut d'exposition en utilisant un jeton bleu de sa liste de « statut » et qu'elle est ensuite diagnostiquée positive au COVID-19. Pour déclarer ses rencontres, l'application d'**Alice** communique son jeton orange de la liste « Déclarer ». *Là aussi l'autorité centrale n'est pas en mesure de déduire que les deux jetons, orange et bleu, appartiennent à la même utilisatrice, **Alice**.*

Pour conclure, l'utilisation de « *Private Encounter Tokens* » ou PET (« *jeton privé de rencontre* ») et l'utilisation de deux listes de jetons PET par application garantissent un niveau élevé de confidentialité au protocole DESIRE. De plus, avec le chiffrement systématique de chaque inscription dans la base de données du serveur, les clés de déchiffrement étant conservées par les clients, DESIRE se caractérise également par une forte résilience face aux risques de fuites de données du serveur.