

Caliopen, la messagerie libre sur la rampe de lancement

Le projet Caliopen, lancé il y a trois ans, est un projet ambitieux. Alors qu'il est déjà complexe de créer un nouveau logiciel de messagerie, il s'agit de proposer un agrégateur de correspondance qui permette à chacun d'ajuster son niveau de confidentialité.

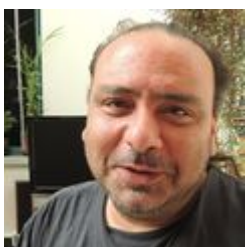
Ce logiciel libre mûrement réfléchi est tout à fait en phase avec ce que Framasoft s'efforce de promouvoir à chaque fois que des libristes donnent aux utilisateurs et utilisatrices plus d'autonomie et de maîtrise, plus de sécurité et de confidentialité.

*Après une nécessaire période d'élaboration, le projet Caliopen invite tout le monde à tester **la version alpha** et à faire remonter les observations et suggestions. La première version grand public ce sera pour dans un an environ.*

*Vous êtes curieux de savoir ce que ça donne ? Nous l'étions aussi, et nous avons demandé à **Laurent Chemla**, qui bidouillait déjà dans l'Internet alors que vous n'étiez même pas né·e, de nous expliquer tout ça, puisqu'il est le père tutélaire du projet Caliopen, un projet que nous devons tous soutenir et auquel nous pouvons contribuer.*



Bonjour, pourrais-tu te présenter brièvement ?



J'ai 53 ans, dont 35 passés dans les mondes de l'informatique et des réseaux. Presque une éternité dans ce milieu - en tous cas le temps d'y vivre plusieurs vies (« pirate », programmeur, hacktiviste, entrepreneur...). Mais ces temps-ci je suis surtout le porteur du projet Caliopen, même si je conserve une petite activité au sein du CA de la Quadrature du Net. Et je fais des macarons.

Le projet Caliopen arrive ce mois-ci au stade de la version alpha, mais comment ça a commencé ?

Jérémie Zimmermann est venu me sortir de ma retraite nîmoise en me poussant à relancer un très ancien projet de messagerie après les révélations de Snowden.

Ça faisait déjà un petit moment que je me demandais si je pouvais encore être utile à la communauté autrement qu'en publiant quelques billets de temps en temps, alors j'ai lancé l'idée en public, pour voir, et il y a eu un tel retour que je n'ai pas pu faire autrement que d'y aller, malgré ma flemme congénitale.

Quand tu as lancé le projet publiquement (sur une liste de diffusion il me semble) quelle était la feuille de route, ou plutôt la « bible » des spécifications que tu souhaitais voir apparaître dans Caliopen ?

Très vite on a vu deux orientations se dessiner : la première, très technique, allait vers une vision maximaliste de la sécurité (réinventer SMTP pour protéger les métadonnées, garantir l'anonymat, passer par du P2P, ce genre de choses), tandis que la seconde visait à améliorer la confidentialité des échanges sans tout réinventer. Ça me semblait plus réaliste - parce que compatible avec les besoins du grand public - et c'est la direction que j'ai choisi de suivre au risque de fâcher certains contributeurs.

J'ai alors essayé de lister toutes les fonctionnalités (aujourd'hui on dirait les « *User Stories* ») qui sont apparues dans les échanges sur cette liste, puis de les synthétiser, et c'est avec ça que je suis allé voir Stephan Ramoin, chez Gandi, pour lui demander une aide qu'il a aussitôt accepté de donner. Le projet a ensuite évolué au rythme des échanges que j'ai pu avoir avec les techos de Gandi, puis de façon plus approfondie avec Thomas Laurent pendant la longue étape durant laquelle nous avons imaginé le design de Caliopen. C'est seulement là, après avoir défini le « pourquoi » et le « quoi » qu'on a pu vraiment commencer à réfléchir au « comment » et à chercher du monde pour le réaliser.

La question qui fâche : quand on lit articles et interviews sur Caliopen, on a l'impression que le concept est encore super flou. C'est quoi l'elevator pitch pour vendre le MVP de la start-up aux business angels des internets digitaux ? (en français : tu dis quoi pour convaincre de nouveaux partenaires financiers ?)



Ça fait bien 3 ans que le concept de base n'a pas bougé : un agrégateur de correspondances qui réunit tous nos échanges privés (emails, message Twitter ou

Facebook, messageries instantanées...), sous forme de conversations, définies par ceux avec qui on discute plutôt que par le protocole utilisé pour le faire. Voilà pour ton *pitch*.

Ce qui est vrai c'est qu'en fonction du public auquel on s'adresse on ne présente pas forcément le même angle. Le document qui a été soumis à BPI France pour obtenir le financement actuel fait 23 pages, très denses. Il aborde les aspects techniques, financiers, l'état du marché, la raison d'être de Caliopen, ses objectifs sociétaux, ses innovations, son design, les différents modèles économiques qui peuvent lui être appliqués... ce n'est pas quelque chose qu'on peut développer en un article ou une interview unique.

Si j'aborde Caliopen sous l'angle de la vie privée, alors j'explique par exemple le rôle des indices de confidentialité, la façon dont le simple fait d'afficher le niveau de confidentialité d'un message va influencer l'utilisateur dans ses pratiques: on n'écrit pas la même chose sur une carte postale que dans une lettre sous enveloppe. Rien que sur ce sujet, on vient de faire une conférence entière (à Paris Web et à BlendWebMix) sans aborder aucun des autres aspects du projet.

Si je l'aborde sous l'angle technique, alors je vais peut-être parler d'intégration « verticale ». Du fait qu'on ne peut pas se contenter d'un nouveau Webmail, ou d'un nouveau protocole, si on veut tenir compte de tous les aspects qui font qu'un échange est plus ou moins secret. Ce qui fait de Caliopen un ensemble de différentes briques plutôt qu'une unique porte ou fenêtre. Ou alors je vais parler de la question du chiffrement, de la diffusion des clés publiques, de TOFU et du

RFC 7929...



Mais on peut aussi débattre du public visé, de design, d'économie du Web, de décentralisation... tous ces angles sont pertinents, et chacun peut permettre de présenter Caliopen avec plus ou moins de détails.

Caliopen est un projet complexe, fondé sur un objectif (la lutte contre la

surveillance de masse) et basé sur un moyen (proposer un service utile à tous), qui souhaite changer les habitudes des gens en les amenant à prendre réellement conscience du niveau d'exposition de leur vie privée. Il faut plus de talent que je n'en ai pour le décrire en quelques mots.

Il reste un intérêt pour les mails ? On a l'impression que tout passe par les webmails ou encore dans des applis de communication sur mobile, non ?

Même si je ne crois pas à la disparition de l'email, c'est justement parce qu'on a fait le constat qu'aujourd'hui la correspondance numérique passe par de très nombreux services qu'on a imaginé Caliopen comme un agrégateur de tous ces échanges.

C'est un outil qui te permet de lire et d'écrire à tes contacts sans avoir à te préoccuper du service, ou de l'application, où la conversation a commencé. Tu peux commencer un dialogue avec quelqu'un par message privé sur Twitter, la poursuivre par email, puis par messagerie instantanée... ça reste une conversation: un échange privé entre deux humains, qui peuvent aborder différents sujets, partager différents contenus. Et quand tu vas vouloir chercher l'information que l'autre t'a donné l'année passée, tu vas faire comment ?

C'est à ça que Caliopen veut répondre. Pour parler moderne, c'est l'*User Story* centrale du projet.

C'est quoi exactement cette histoire de niveaux de confidentialité ? Quel est son but ?

Il faut revenir à l'objectif principal du projet : lutter contre la surveillance de masse que les révélations d'Edward Snowden ont démontrée.

Pour participer à cette lutte, Caliopen vise à convaincre un maximum d'utilisateurs de la valeur de leur vie privée. Et pour ça, il faut d'abord leur montrer, de manière évidente, que leurs conversations sont très majoritairement *espionnables*, sinon espionnées. Notre pari, c'est que quand *on voit* le risque d'interception, on réagit autrement que lorsqu'on est seulement *informé* de son existence. C'est humain : regarde l'exemple de la carte postale que je te donne plus haut.

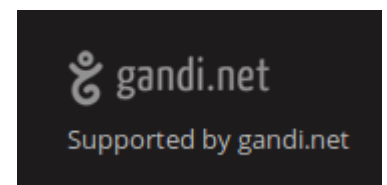
D'où l'idée d'associer aux messages (mais aussi aux contacts, aux terminaux, et même à l'utilisateur lui-même) un niveau de confidentialité. Représenté par une icône, des couleurs, des chiffres, c'est une question de design, mais ce qui est important c'est qu'en *voyant* le niveau de risque, l'utilisateur ne va plus pouvoir faire semblant de l'ignorer et qu'il va accepter de changer - au moins un peu - ses pratiques et ses habitudes pour voir ce niveau augmenter.

Bien sûr, il faudra l'accompagner. Lui proposer des solutions (techniques, comportementales, contextuelles) pour améliorer son « score ». Sans le culpabiliser (ce n'est pas la bonne manière de faire) mais en le récompensant - par une meilleure note, de nouvelles fonctionnalités, des options gratuites si le service est payant... bref par une *ludification* de l'expérience utilisateur. C'est notre piste en tous cas.

Et c'est en augmentant le niveau global de confidentialité des échanges qu'on veut rendre plus difficile (donc plus chère) la surveillance de tous, au point de pousser les états - et pourquoi pas les GAFAM - à changer de pratiques, eux aussi.

Financièrement, comment vit le projet Caliopen ? C'était une difficulté qui a retardé l'avancement ?

Sans doute un peu, mais je voudrais quand même dire que, même si je suis bien conscient de l'impression de lenteur que peut donner le projet, il faut se rendre compte qu'on parle d'un outil complexe, qui a démarré de zéro, avec aucun moyen, et qui s'attaque à un problème dont les racines datent de plusieurs dizaines d'années. Si c'était facile et rapide à résoudre, ça se saurait.



Dès l'instant où nous avons pris conscience qu'on n'allait pas pouvoir continuer sur le modèle du bénévolat, habituel au milieu du logiciel libre, nous avons réagi assez vite : Gandi a décidé d'embaucher à plein temps un développeur *front end*, sur ses fonds propres. Puis nous avons répondu à un appel à projet de BPI France qui tombait à pic et auquel Caliopen était bien adapté. Nous avons défendu notre dossier, devant un comité de sélection puis devant un panel d'experts, et nous

avons obtenu de quoi financer deux ans de développement, avec une équipe dédiée et des partenaires qui nous assurent de disposer de compétences techniques rares. Et tout ça est documenté sur notre blog, depuis le début (tout est public depuis le début, d'ailleurs, même si tous les documents ne sont pas toujours faciles à retrouver, même pour nous).

Et finalement c'est qui les partenaires ?

Gandi reste le partenaire principal, auquel se sont joints Qwant et l'UPMC (avec des rôles moins larges mais tout aussi fondamentaux).

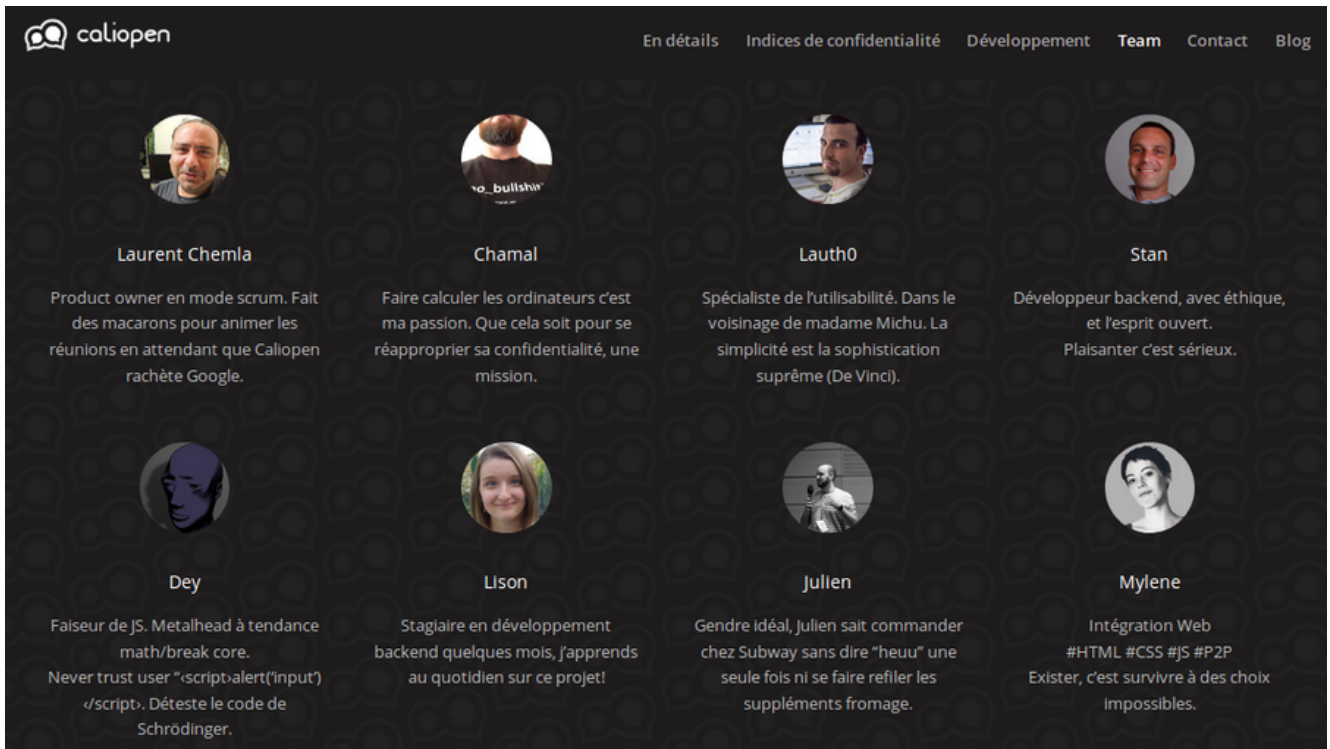
Quel est le modèle économique ? Les développeurs (ou développeuses, y'en a au fait dans l'équipe ?) sont rémunérés autrement qu'en macarons ? Combien faudra-t-il payer pour ouvrir un compte ?

Je ne suis pas sûr qu'on puisse parler de « modèle économique » pour un logiciel libre : après tout chacun pourra en faire ce qu'il voudra et lui imaginer tel ou tel modèle (économique ou non d'ailleurs).

Une fois qu'on a dit ça, on peut quand même dire qu'il ne serait pas cohérent de baser des services Caliopen sur l'exploitation des données personnelles des utilisateurs, et donc que le modèle « gratuité contre données » n'est pas adapté. Nous imaginons plutôt des services ouverts au public de type *freemium*, d'autres fournis par des entreprises pour leurs salariés, ou par des associations pour leurs membres. On peut aussi supposer que se créeront des services pour adapter Caliopen à des situations particulières, ou encore qu'il deviendra un outil fourni en Saas, ou vendu sous forme de *package* associé, par exemple, à la vente d'un nom de domaine.

Bref : les modèles économiques ce n'est pas ce qui manque le plus.

L'équipe actuelle est salariée, elle comporte des développeuses, et tu peux voir nos trombinettes sur <https://www.caliopen.org>



L'équipe de Caliopen

Trouver des développeurs ou développeuses n'est jamais une mince affaire dans le petit monde de l'open source, comment ça s'est passé pour Caliopen ?

Il faut bien comprendre que – pour le moment – Caliopen n'a pas d'existence juridique propre. Les gens qui bossent sur le projet sont des employés de Gandi (et bientôt de Qwant et de l'UPMC) qui ont soit choisi de consacrer une partie de leur temps de travail à Caliopen (ce que Gandi a rendu possible) soit été embauchés spécifiquement pour le projet. Et parfois nous avons des bénévoles qui nous rejoignent pour un bout de chemin ☐

Le projet est encore franco-français. Tu t'en félicites (cocorico) ou ça t'angoisse ?

J'ai bien des sujets d'angoisse, mais pas celui-là. C'est un problème, c'est vrai, et nous essayons de le résoudre en allant, par exemple, faire des conférences à l'étranger (l'an dernier au FOSDEM, et cette année au 34C3 si notre soumission est acceptée). Et le site est totalement trilingue (français, anglais et italien) grâce au travail (bénévole) de Daniele Pitrolo.

D'un autre côté il faut quand même reconnaître que bosser au quotidien dans sa langue maternelle est un vrai confort dont il n'est pas facile de se passer. Même si on est tous conscients, je crois, qu'il faudra bien passer à l'anglais quand l'audience du projet deviendra un peu plus internationale, et nous comptons un peu sur les premières versions publiques pour que ça se produise.

Et au fait, c'est codé en quoi, Caliopen ? Du JavaScript surtout, d'après ce qu'on voit sur GitHub, mais nous supposons qu'il y a pas mal de technos assez pointues pour un tel projet ?

Sur GitHub, le code de Caliopen est dans un *mono-repository*, il n'y a donc pas de paquet (ou dépôt) spécifique au front ou au back. Le client est développé en JavaScript avec la librairie ReactJS. Le backend (l'API ReST, les workers ...) sont développés en python et en Go. On n'a pas le détail mais ce doit être autour de 50% JS+css, 25% python, 25% Go. L'architecture est basée sur Cassandra et ElasticSearch.

Ce n'est pas que l'on utilise des technos pointues, mais plutôt qu'on évite autant que possible la dette technique en intégrant le plus rapidement possible les évolutions des langages et des librairies que l'on utilise.

Donc il faut vraiment un haut niveau de compétences pour contribuer ?

Difficile à dire. Si on s'arrête sur l'aspect développement pur, les technos employées sont assez grand public, et si on a suivi un cursus standard on va facilement retrouver ses habitudes (cf. <https://github.com/kamranahmedse/developer-roadmap>).

Effectivement quelqu'un qui n'a pas l'habitude de développer sur ces outils (docker, Go, webpack, ES6+ ...) risque d'être un peu perdu au début. Mais on est très souvent disponibles sur IRC pour répondre directement aux questions.

Néanmoins nous avons de « simples » contributions qui ne nécessitent pas de connaître les patrons de conception par cœur ou de devoir monter un cluster; par exemple proposer des corrections orthographiques, de nouvelles traductions, décrire des erreurs JavaScript dans des issues sur github, modifier un bout de css...

Ou même aider la communauté sur <https://feedback.caliopen.org/> ou sur les

réseaux sociaux, tout ça en fait partie.

Et bien sûr les alpha-testeurs sont bienvenus surtout s'ils font des retours d'expérience.



Qu'est-ce qui différencie le projet Caliopen d'un projet comme Protonmail ?

Protonmail est un Gmail-like orienté vers la sécurité. Caliopen est un agrégateur de correspondance privée (ce qui n'est rien-like) orienté vers l'amélioration des pratiques du grand public via l'expérience utilisateur. Protonmail est centralisé, Caliopen a prévu tout un (futur) écosystème exclusivement destiné à garantir la décentralisation des échanges. Et puis Caliopen est un logiciel libre, pas Protonmail.

Mais au-delà de ces différences techniques et philosophiques, ce sont surtout deux visions différentes, et peut-être complémentaires, de la lutte contre la surveillance de masse: Protonmail s'attaque à la protection de ceux qui sont prêts à changer leurs habitudes (et leur adresse email) parce qu'ils sont déjà convaincus qu'il faut faire certains efforts pour leur vie privée. Caliopen veut changer les habitudes de tous les autres, en leur proposant un service différent (mais utile) qui va les sensibiliser à la question. Parce qu'il faut bien se rendre compte que, malgré son succès formidable, aujourd'hui le nombre d'utilisateurs de Protonmail ne représente qu'à peine un millième du nombre d'utilisateurs de Gmail, et que quand les premiers échangent avec les seconds ils ne sont pas mieux protégés que M. Michu.

Maintenant, si tu veux bien imaginer que Caliopen est aussi un succès (on a le droit de rêver) et qu'il se crée un jour disons une dizaine de milliers de services

basés sur noooootre proooojet, chacun ne gérant qu'un petit dixième du nombre d'utilisateurs de Protonmail... Eh ben sauf erreur on équilibre le nombre d'utilisateurs de Gmail et - si on a raison de croire que l'affichage des indices de confidentialité va produire un effet - on a significativement augmenté le niveau global de confidentialité.

Et peut-être même assez pour que la surveillance de masse devienne hors de prix.



Est-ce que dans la future version de Caliopen les messages seront chiffrés de bout en bout ?

À chaque fois qu'un utilisateur de Caliopen va vouloir écrire à un de ses contacts, c'est le protocole le plus sécurisé qui sera choisi par défaut pour transporter son message. Prenons un exemple et imaginons que tu m'ajoutes à tes contacts dans Caliopen : tu vas renseigner mon adresse email, mon compte Twitter, mon compte Mastodon, mon Keybase... plus tu ajouteras de moyens de contact plus Caliopen aura de choix pour m'envoyer ton message. Et il choisira le plus sécurisé par défaut (mais tu pourras décider de ne pas suivre son choix).

Plus tes messages auront pu être sécurisés, plus hauts seront leurs indices de confidentialité affichés. Et plus les indices de confidentialité de tes échanges seront hauts, plus haut sera ton propre indice global (ce qui devrait te motiver à mieux renseigner ma fiche contact afin d'y ajouter l'adresse de mon email hébergé sur un service Caliopen, parce qu'alors le protocole choisi sera le protocole intra-caliopen qui aura un très fort indice de confidentialité).

Mais l'utilisateur moyen n'aura sans doute même pas conscience de tout ça. Simplement le système fera en sorte de ne pas envoyer un message en clair s'il dispose d'un moyen plus sûr de le faire pour tel ou tel contact.

Est-ce qu'on pourra (avec un minimum de compétences, par exemple pour des CHATONS) installer Caliopen sur un serveur et proposer à des utilisateurs et utilisatrices une messagerie à la fois sécurisée et respectueuse ?

C'est fondamental, et c'est un des enjeux de Caliopen. Souvent quand je parle devant un public technique je pose la question : « combien de temps mettez-vous à installer un site Web en partant de zéro, et combien de temps pour une messagerie complète ? ». Et les réponses aujourd'hui sont bien sûr diamétralement opposées à ce qu'elle auraient été 15 ans plus tôt, parce qu'on a énormément travaillé sur la facilité d'installation d'un site, depuis des années, alors qu'on a totalement négligé la messagerie.

Si on veut que Caliopen soit massivement adopté, et c'est notre objectif, alors il faudra qu'il soit - relativement - facile à installer. Au moins assez facile pour qu'une entreprise, une administration, une association... fasse le choix de l'installer plutôt que de déléguer à Google la gestion du courrier de ses membres. Il faudra aussi qu'il soit facilement administrable, et facile à mettre à jour. Et tout ceci a été anticipé, et analysé, durant tout ce temps où tu crois qu'on n'a pas été assez vite !

On te laisse le dernier mot comme il est de coutume dans nos interviews pour le blog...

À lire tes questions j'ai conscience qu'on a encore beaucoup d'efforts à faire en termes de communication. Heureusement pour nous, Julien Dubedout nous a rejoints récemment, et je suis sûr qu'il va beaucoup améliorer tout ça. ☐



- Devenir alpha-testeur
- Les fonctionnalités de Caliopen
- roadmap et bugreport
- GitHub de Caliopen