MINISTÈRES
ÉDUCATION
JEUNESSE
SPORTS
ENSEIGNEMENT
SUPÉRIEUR
RECHERCHE
Liberté
Égalité
Fraternité

LDE ISI 1

SESSION 2026

Δ

CAPET et CAFEP
(BAC +3)

Concours externe

Section

INFORMATIQUE, SECURITE ET MANAGEMENT DES SYSTEMES D'INFORMATION

Épreuve d'admissibilité 1

L'épreuve consiste à répondre à une série de questions en s'appuyant sur un dossier documentaire.
L'épreuve vise à vérifier les connaissances scientifiques et méthodologiques dans le domaine du management et de la sécurité des systèmes d'information, en intégrant les dimensions juridique et économique.

Durée : 4 heures

———

L'usage de la calculatrice est autorisé dans les conditions relevant de la nouvelle circulaire du 17 juin 2021 BOEN du 29 juillet 2021.

L'usage de tout ouvrage de référence, de tout dictionnaire et de tout autre matériel électronique est rigoureusement interdit.

Il appartient au candidat de vérifier qu'il a reçu un sujet complet et correspondant à l'épreuve à laquelle il se présente.

Si vous repérez ce qui vous semble être une erreur d'énoncé, vous devez le signaler très lisiblement sur votre copie, en proposer la correction et poursuivre l'épreuve en conséquence. De même, si cela vous conduit à formuler une ou plusieurs hypothèses, vous devez la (ou les) mentionner explicitement.

NB : Conformément au principe d'anonymat, votre copie ne doit comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé consiste notamment en la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de la signer ou de l'identifier.
Le fait de rendre une copie blanche est éliminatoire.

A

Tournez la page S.V.P.

INFORMATION AUX CANDIDATS

Vous trouverez ci-après les codes nécessaires vous permettant de compléter les rubriques figurant en entête de votre copie. Ces codes doivent être reportés sur chacune des copies que vous remettrez.

CAPET EXTERNE - INFORMATIQUE, SECURITE ET MANAGEMENT DES SYSTEMES D'INFORMATION

► Concours externe du CAPET de l'enseignement public :

Concours	Section/option	Epreuve	Matière
LDE	55106E	101	4061

► Concours externe du CAPET de l'enseignement privé :

Concours	Section/option	Epreuve	Matière
LDF	55106E	101	4061

IMPRIMERIE NATIONALE – 26 0456 – D'après documents fournis

Structure du sujet

Le sujet est structuré en trois dossiers qui peuvent être traités de façon indépendante puis d'une question qui met en perspective le traitement du sujet.

Sujet :

Dossier 1 - Enjeux du développement de Doctolib
Dossier 2 - Enjeux de l'intégration applicative chez Doctolib
Dossier 3 - Enjeux de la politique de sécurité chez Doctolib
Question de mise en perspective

Liste des documents à exploiter :

Document 1 - Les caractéristiques des plateformes
Document 2 - Le modèle économique des plateformes
Document 3 - Les effets de réseau dans les plateformes numériques
Document 4 - Sécurisation des données de santé : Doctolib face aux sénateurs
Document 5 - La plateforme monolithique de Doctolib
Document 6 - Les enjeux d'un monolithe
Document 7 - Doctolib a beaucoup évolué et s'interface de plus en plus avec d'autres outils
Document 8 - Siilo, une messagerie gratuite et sécurisée entre soignants
Document 9 - Les méthodes pour se connecter à la messagerie Siilo
Document 10 - Échanges sécurisés des données chez Doctolib
Document 11 - Programme de prime à la faille (*Bug Bounty*) chez Doctolib
Document 12 - Règles et récompenses du programme de prime à la faille (*Bug Bounty*)
Document 13 - Typologie des risques et grille de récompenses

DOCTOLIB

Doctolib est une entreprise française fondée en 2013 qui propose une plateforme numérique de gestion de téléconsultation et de rendez-vous médicaux. Aujourd'hui, c'est l'un des leaders européens de la e-santé, présent en France, en Allemagne et en Italie avec :

- plus de 80 millions d'utilisateurs (patients),
- plus de 400 000 professionnels de santé inscrits,
- des partenariats avec des hôpitaux, cliniques et cabinets libéraux.

Doctolib a joué un rôle clé pendant la pandémie de COVID-19 en permettant la prise de rendez-vous pour la vaccination et en développant massivement la téléconsultation. Le cœur de son modèle repose sur une plateforme de mise en relation, financée par les abonnements payés par les professionnels de santé.

Avec ses 2900 salariés et ses embauches continues, Doctolib a même rejoint en mars 2019 Deezer et Blablacar dans le cercle très fermé des licornes françaises, ces entreprises valorisées à plus d'un milliard d'euros. Depuis 2023, Doctolib est une *entreprise à mission* et a investi 92 millions d'euros dans des innovations qui permettront notamment de poursuivre son engagement au service des soignants et des patients, et de contribuer au développement de la prévention.

Doctolib lance aujourd'hui une nouvelle série d'innovations placées sous le signe de la collaboration entre soignants notamment grâce à Doctolib Siilo, première messagerie instantanée et gratuite, et ce suite au rachat de la société Siilo. Cette application permet aux professionnels de santé de se coordonner dans la prise en charge des patients et de communiquer via message, appel vocal ou vidéo pour améliorer la coordination des soins.

L'entreprise poursuit ainsi sa stratégie de croissance externe en intégrant de nouvelles entreprises, technologies ou services afin de poursuivre son engagement sociétal. Cette croissance nécessite une vigilance accrue en matière de sécurisation du système d'information. Pour répondre à cette exigence Doctolib lance son programme participatif de signalement de vulnérabilités (*Bug Bounty*).

En prenant appui sur vos connaissances, le contexte et le dossier documentaire, il vous est demandé de répondre aux questions relatives aux trois dossiers du sujet et à la question de sa mise en perspective.

Dossier 1 : Enjeux du développement de Doctolib

Depuis sa création, Doctolib s'est donné pour mission de contribuer à améliorer le quotidien des équipes soignantes et la santé des patients. Cette ambition d'être un service utile, fiable et accessible à tous s'est traduite par :

- la reconnaissance, pour la deuxième année consécutive, d'être le service qui améliore le plus le quotidien des Français, selon un sondage effectué par l'institut français d'opinion publique (IFOP) ;
- la réduction des délais d'accès aux soins pour les patients et l'amélioration des conditions de travail des soignants, notamment la diminution des rendez-vous non honorés ;
- l'utilisation de Doctolib par les patients dans tous les territoires (86 % des patients utilisateurs habitent en dehors des 5 plus grandes villes de France) et quel que soit leur âge (7,5 millions de patients de plus de 65 ans).

Travail à faire	
1.1	Exposer les avantages procurés par la plateforme développée par Doctolib pour chaque catégorie d'acteurs.
1.2	Montrer que l'existence d'externalités de réseau associées à la plateforme participe au développement de l'entreprise Doctolib.
1.3	Présenter le cadre réglementaire des données traitées par le biais de la plateforme Doctolib.

Avec le développement de la plateforme et l'augmentation du volume des informations à stocker et à sécuriser, Doctolib a décidé d'externaliser l'hébergement des données.

Doctolib a recours aux prestations de la société américaine Amazon Web Services (AWS), filiale du groupe Amazon spécialisée dans les services en nuage à la demande (*Cloud computing*) pour les entreprises et les particuliers.

Travail à faire	
1.4	Présenter les avantages et les limites d'externaliser l'hébergement des données auprès de ce prestataire.

Dossier 2 : Enjeux de l'intégration applicative chez Doctolib

La plateforme Doctolib se positionne comme « un compagnon de santé » pour les patients et une suite logicielle pour les soignants proposant des services adaptés aux spécialités de ces derniers.

Ces solutions sont construites historiquement sur une plateforme unique (architecture monolithique) qui prend en charge les interfaces *web* et les applications mobiles, en plusieurs langues, et qui est adaptée aux exigences des pays et aux spécialités des soignants.

Travail à faire	
2.1	Préciser les avantages et les limites du choix de l'architecture applicative en monolithe.

Avec la multiplication des outils et services numériques dédiés à la santé, les enjeux pour le service Doctolib consistent à correctement s'interfacer avec les logiciels métiers médicaux des praticiens, logiciels nombreux et pas toujours conformes aux standards internationaux d'interopérabilité (visant à faciliter l'échange de données entre systèmes d'information hospitaliers).

Interrogée lors des « *APIDays* », Marion Hozé, cheffe de produit (PM - *product manager*) chez Doctolib indique qu'il est souvent nécessaire d'adapter l'interopérabilité aux besoins, à l'environnement et au contexte. La mise à disposition récente par l'équipe technique de Doctolib d'une interface de programmation d'application (API - *application programmation interface*) facilite grandement les besoins d'intégration.

Travail à faire	
2.2	Analyser les bénéfices pour Doctolib liés à la mise à disposition d'une interface de programmation d'application (API).

Au-delà de cette innovation interne, l'entreprise a aussi recours à une politique de croissance externe, en procédant au rachat de sociétés spécialisées dans la « e-santé » afin d'élargir son offre et de renforcer sa position de leader en Europe. L'exemple du rachat de Siilo, une jeune pousse (*start-up)* néerlandaise qui a développé une messagerie sécurisée utilisée par de nombreux professionnels de santé pour leurs échanges cliniques, illustre bien cette stratégie.

Travail à faire	
2.3	Préciser les bénéfices attendus par Doctolib dans l'acquisition de cette société.

La circulation des données de santé entre professionnels via l'application de messagerie développée par Siilo oblige Doctolib à renforcer la sécurité de l'authentification des utilisateurs.

Travail à faire	
2.4	Identifier et qualifier les mécanismes techniques mis en place pour assurer une sécurisation de l'accès à la messagerie.

Dossier 3 : Enjeux de la politique de sécurité chez Doctolib

Le 23 juillet 2020, Doctolib a été victime d'une cyberattaque ciblant 6 128 rendez-vous médicaux. Les pirates ont accédé à des informations comme les noms, courriels et spécialités des médecins concernés.

En plus de l'identification et l'évaluation des menaces, la sécurité des données chez Doctolib s'appuie également sur la maîtrise des environnements techniques, en particulier ceux hébergés sur l'environnement Amazon Web Services (AWS). Bien que cette infrastructure en nuage (*cloud*) apporte de hauts standards de sécurité, elle implique aussi des responsabilités partagées et nécessite une vigilance constante face aux risques liés à la configuration et à l'exploitation.

Doctolib a adopté le chiffrement de bout en bout pour sécuriser la circulation des données de santé. Le protocole utilisé repose sur du chiffrement et du partage de clés. Il combine le chiffrement symétrique et asymétrique pour fournir un moyen rapide et efficace de chiffrer, et de partager des données entre les différents utilisateurs.

Travail à faire	
3.1	Expliquer en quoi le chiffrement symétrique combiné au chiffrement asymétrique constitue un moyen efficace de sécurisation des échanges.

Pour renforcer cette approche, Doctolib a mis en place un programme participatif de signalement de vulnérabilités (prime à la faille -*Bug Bounty*-), permettant à une communauté d'experts en cybersécurité (ou "hackers éthiques") d'identifier et de signaler les vulnérabilités potentielles. Cette démarche collaborative et proactive contribue à améliorer en continu la résilience du système d'information face aux menaces.

Doctolib s'engage à récompenser financièrement, jusqu'à hauteur de 20 000 euros, les experts qui détecteraient une faille dans la sécurité de l'entreprise.

Travail à faire	
3.2	Présenter les opportunités et les menaces de mise en place d'un programme de prime à la faille (*Bug Bounty*).
3.3	Caractériser la méthode de management des risques utilisée dans le programme de prime à la faille (*Bug Bounty*).
3.4	Expliquer comment le niveau de gravité d'une vulnérabilité est utilisé pour déterminer la récompense attribuée.

Question de mise en perspective

L'évolution du système d'information accompagne et permet la forte croissance de Doctolib. L'intégration et la sécurisation des données de santé sont un objectif stratégique.
En une page, à partir de vos connaissances et en vous appuyant sur l'analyse des trois dossiers précédents répondre de façon cohérente et argumentée à la question suivante :
Comment maîtriser les risques liés aux données dans un contexte d'évolution rapide et exponentielle du système d'information ?

Document 1 - Les caractéristiques des plateformes

Le cœur de la valeur d'une plateforme réside dans les données, qu'elle s'adresse à un marché entreprise à consommateur (*business to consumer)* ou entreprise à entreprise (*business to business)*. La plateforme organise et hiérarchise les contenus (proposition de services ou de produits) en vue de leur présentation aux utilisateurs finaux. Elle permet de générer la transaction d'échange entre la donnée proposée (offre) et la donnée recherchée (demande). Elle permet en sus de créer de la valeur via l'analyse d'un grand nombre de données et des transactions, en un temps record, soit pour affiner les propositions, soit pour en exploiter leur traduction vers d'autres services. [….]

Plus généralement, on peut définir une plateforme avec 3 critères :

- Intermédiaire : une plateforme est un intermédiaire entre 2 ou plusieurs pôles d'intérêts tout à fait différents mais interdépendants les uns des autres pour les produits ou services qui y sont échangés. Lorsque le succès est au rendez-vous, les utilisateurs retiennent la plateforme commerciale plus que les partenaires de l'écosystème.
- Sociale et mobile : une plateforme est à la fois sociale par la confrontation des avis des utilisateurs qui génère la confiance, et mobile puisque consultable en permanence où que l'on soit.
- Abaissement des barrières à l'entrée : une plateforme donne les moyens à de nouveaux acteurs de pénétrer un marché, elle met en concurrence tout le monde avec tout le monde ; en permettant à ces nouveaux acteurs de croître rapidement avec des effets de levier, elle abaisse considérablement les barrières à l'entrée. [...]

Source : Les nouvelles stratégies de plateforme - Cigref -décembre 2022

Document 2 - Le modèle économique de Doctolib

Doctolib fonctionne sur un modèle économique B2B (*business-to-business* - entreprise à entreprise), centré sur les professionnels de santé, et non sur les patients. Son modèle économique est basé sur un abonnement pour les professionnels de santé.

Les médecins, dentistes, kinés, psychologues, hôpitaux, cliniques, etc. paient un abonnement mensuel pour utiliser la plateforme. Le tarif varie selon le type de praticien et les options choisies, mais il se situe en moyenne autour de 100 à 150 € par mois et par professionnel.

Cet abonnement donne accès à différents services comme :

- un agenda en ligne synchronisé,
- la prise de rendez-vous en ligne par les patients,
- la téléconsultation (intégrée),
- des outils de gestion (dossiers patients, rappels automatiques par SMS, etc.),
- une meilleure visibilité sur Internet (profil Doctolib référencé par les moteurs de recherche).

Doctolib développe aussi des outils logiciels pour les établissements de santé (hôpitaux, cliniques), avec des offres sur mesure.

La gratuité pour les patients fait partie du modèle économique car les patients n'ont rien à payer : la recherche de praticiens, la prise de rendez-vous, les rappels automatiques, la téléconsultation (hors tarif de la consultation médicale elle-même) sont gratuits. Cela lui permet d'attirer une très large base d'utilisateurs, environ 80 millions en Europe. La société ne monnaie pas les données des patients à des fins publicitaires et elle insiste beaucoup sur ce point pour des raisons de confiance et de conformité au règlement général sur la protection des données (RGPD).

Source : d'après Doctolib.fr

Document 3 - Les effets de réseau dans les plateformes numériques

Gerhard Rohlfs, professeur d'université, est un des premiers à avoir parlé des effets de réseau (ou externalités de réseau) et à avoir étudié leur impact sur la demande de services de télécommunications. À la suite de son étude, de nombreux travaux théoriques se sont attachés à analyser les stratégies des entreprises produisant des biens ou des services à forts effets de réseau. Les études de J. Farrell et G. Saloner, E. Katz et C. Shapiro montrent, par exemple, comment les effets de réseau peuvent affecter les prix et les parts de marché et, sous certaines conditions, mener à une concentration du marché. Du point de vue empirique, de nombreux travaux ont cherché à quantifier les effets de réseau directs (liés au nombre d'utilisateurs) et indirects (liés à la quantité et la variété de biens ou services complémentaires), dans divers secteurs comme les télécommunications, l'informatique, les jeux vidéo, la presse ou le secteur bancaire.

L'attention s'est plus récemment portée sur les plateformes numériques, et sur les effets de réseau croisés entre les différentes faces. Rysman étudie les effets de réseau dans les services d'annuaire qui mettent en relation des consommateurs et des annonceurs (des entreprises). Il constate qu'une hausse du nombre d'annonceurs accroît l'audience du site et qu'en retour, une hausse du nombre de visiteurs sur le site attire un plus grand nombre d'annonceurs. Sur les plateformes, les effets de réseau ne sont pas seulement de nature quantitative (mesurée par le nombre d'utilisateurs sur chacune des faces), mais aussi de nature qualitative (mesurée par la qualité et la réputation des utilisateurs).

Source : d'après Cairn.info

Document 4 - Sécurisation des données de santé : Doctolib face aux sénateurs

Face à la commission des affaires sociales du Sénat, la licorne Doctolib a été interrogée sur ses pratiques en matière de sécurisation des données de santé. […]

Pour rappel, près de 15 millions de rendez-vous médicaux sont pris sur la plateforme chaque mois. Le sénateur de Paris Bernard Jomier, médecin de profession, interpelle Doctolib sur ses pratiques en matière de sécurisation. « Vous êtes un acteur majeur avec des responsabilités. La responsabilité de contrôler l'utilisation et la non fuite des données de santé avec risque de divulgation du secret médical. Alors comment faites-vous ? », a-t-il déclaré.

Le directeur général de Doctolib explique que les données transitant par Doctolib sont hébergées par Amazon web services (AWS) dans des centres de données situés en France et en Allemagne. Il rappelle que, comme la législation l'y oblige, AWS détient la certification « Hébergeur de données de santé » (HDS) et détient « les principales normes internationales ». Présentée par l'agence gouvernementale française pour la santé soit l'Agence du numérique en santé (ANS), la certification HDS (hébergeur de données de santé) a pour objectif de renforcer la sécurité et la protection des données personnelles de santé. L'obtention de cette certification prouve qu'AWS fournit un cadre en matière de mesures techniques et de gouvernance, visant à sécuriser et à protéger les données personnelles de santé, régi par la législation française. La certification HDS confirme qu'AWS garantit la confidentialité, l'intégrité et la disponibilité des données à ses clients et partenaires.

Aussi, complète-t-il, Doctolib possède lui-même « beaucoup de types de certifications », telle qu'ISO 27701 (norme qui décrit la gouvernance et les mesures de sécurité à mettre en place pour le traitement de données personnelles) et ISO 27001 (norme sur la sécurité des systèmes d'information). Le service AWS est « le seul aujourd'hui à avoir la capacité à héberger une aussi grosse quantité de données avec le niveau de service que l'on a aujourd'hui ».

Le choix d'un hébergeur américain avait été pointé du doigt pendant la pandémie de Covid-19, période durant laquelle Doctolib servait de plateforme centrale pour les prises de rendez-vous vaccinaux dans le cadre d'un contrat avec le ministère de la Santé. Des associations et des syndicats avaient ainsi déposé un recours en référé devant le Conseil d'État estimant qu'en ayant choisi le service AWS, la pépite française ne protégeait pas suffisamment les données personnelles des patients. L'entreprise AWS est en effet soumise aux lois américaines et notamment le *Cloud Act* qui permet aux autorités américaines, sous certaines conditions de pouvoir accéder aux données hébergées par des fournisseurs américains et ce, quelle que soit la localisation

des serveurs.

Suite à l'action des associations et syndicats, le Conseil d'État avait écarté la demande en relevant que les données recueillies dans le cadre des rendez-vous ne comprenaient pas de données de santé sur les motifs médicaux d'éligibilité à la vaccination et que des garanties avaient été mises en place pour faire face à une éventuelle demande d'accès par les autorités américaines. En effet le contrat conclu entre Doctolib et AWS prévoit une procédure spécifique en cas de demandes d'accès par une autorité étrangère prévoyant la contestation de toute demande ne respectant pas la réglementation européenne.

Sources : d'après usine-digitale.fr et aws.amazon.com, conseil-etat.fr

Document 5 – La plateforme monolithique de Doctolib

On désigne par monolithe, un logiciel informatique unique, qui est capable de proposer plusieurs services, dans plusieurs langues et pour différents utilisateurs finaux. Concernant Doctolib, il existe le site grand public (www.doctolib.fr), ainsi que le site pour les professionnels de la santé (pro.doctolib.fr), et d'autres sites secondaires, qui permettent par exemple l'interconnexion avec les systèmes d'information hospitaliers. À savoir que l'ensemble de ces sites est servi par un seul logiciel, installé sur des milliers de serveurs. Selon le trafic, il est ainsi possible d'équilibrer les requêtes *web* entrantes. C'est une seule unité à déployer, ce qui est un avantage et qui permet par exemple, chez Doctolib, de faire des mises en production trois fois par jour.

Lorsque qu'un service *web* dépend de plusieurs services, il est alors nécessaire d'assurer une coordination. A contrario ici, on déploie une seule grosse unité. Puis le système active telle ou telle partie du code, pour servir le site public ou le site professionnel.

Un monolithe fait appel à une seule technologie et un seul langage de programmation pour la partie côté serveur (ou « *backend* »). Chez Doctolib l'atelier de développement (*framework*) Ruby on Rails a été choisi. Le monolithe embarque plusieurs parties pour pouvoir interagir avec le navigateur *web*, mais aussi avec un téléphone mobile. Le même monolithe est capable de servir plusieurs types de périphérique, avec un seul « backend ».

Source : touilleur-express.fr

Document 6 – Les enjeux d'un monolithe

Les points forts

En premier lieu et c'est vraiment le point fort : c'est simple. Que ce soit lorsque vous développez, lorsque vous devez mettre à jour ou lorsque vous opérez un monolithe : c'est vraiment plus simple que de coordonner plusieurs serveurs.

Les outils de gestion des fonctionnalités permettent aux équipes de tester et de déployer des fonctionnalités selon des règles précises. La mise en production du code est dissociée de son activation pour les utilisateurs finaux. Vous pouvez aussi revenir en arrière lorsqu'une version ne fonctionne pas correctement.

Techniquement, il y a une seule pile (*stack*) technique à connaître. Vous pouvez ainsi utiliser la dernière version du langage, et les dernières librairies sans aucun problème.

Lors de la vague de vaccination liée à la COVID-19, cela a permis de gérer sans trop de problèmes la charge énorme de visiteurs.

Cela fonctionne avec une organisation en équipes agiles (*features teams*) multidisciplinaires collaborant autour d'une même fonctionnalité. C'est une excellente tactique pour développer rapidement, et ne pas payer de surcoût de synchronisation très élevée.

Le monolithe simplifie aussi l'intégration et l'assurance qualité. À chaque modification, nous passons une recette complète. Elle prend à peine 20 minutes et couvre l'ensemble du logiciel.

.../...

Aspects à surveiller avec la croissance

Lorsque le nombre d'équipes a commencé à fortement augmenter, si le système fonctionnait, il avait un coût d'évolutivité important. L'intégration continue et les tests deviennent coûteux et complexes.

Doctolib fait évoluer l'architecture de son monolithe vers une architecture plus modulaire notamment pour répondre à la problématique de montée en charge.

Source : d'après touilleur-express.fr

Document 7 - Doctolib a beaucoup évolué et s'interface de plus en plus avec d'autres outils

Créée comme plate-forme de prise de rendez-vous médicaux en 2013, Doctolib a beaucoup évolué et s'interface de plus en plus avec d'autres outils [...] Assez rapidement, la question de l'interopérabilité s'est posée : il était impossible que les médecins perdent du temps à jongler entre leurs propres logiciels de gestion de cabinet ou de dossier patient et une plate-forme en ligne. Mais la politique nécessaire de mise à disposition d'interface de programmation (API) a dû se mettre progressivement en place.

Doctolib traite des données sensibles [...]. C'est la raison pour laquelle ces données sont nécessairement hébergées chez un hébergeur certifié « hébergeur de données de santé ». De la même façon, la sécurisation des échanges est fondamentale et Doctolib met en place le chiffrement de bout en bout.

La plate-forme doit se connecter avec les logiciels métiers précisément pour échanger les informations de rendez-vous avec, le cas échéant, le motif de consultation [...]. Cette connexion sert à éviter toute ressaisie entre logiciels et ainsi faciliter l'adoption du service par les soignants.

Au départ, Doctolib n'avait pas créé sa propre interface de programmation (API) et n'était que consommateur des celles des différents éditeurs. « Mais cela nous amenait des problèmes de maintenabilité car chaque connexion est spécifique » relève Marion Hozé. [...]. Lorsque le développement commercial et la maturité de la plate-forme l'a permis, une interface de programmation (API) standard a finalement été créée afin que les acteurs tiers puissent s'y interfacer d'une manière unique, évitant ainsi à Doctolib de maintenir un trop grand nombre de connecteurs spécifiques. « Pour l'Allemagne, nous avons été obligés de nous adapter aux besoins locaux et nous avons donc modifié notre API en installant des 'interrupteurs de flux' permettant de ne synchroniser que ce qu'il faut dans chaque pays ... »

Lorsqu'un éditeur partenaire veut utiliser l'interface de programmation (API) Doctolib pour son produit, il est systématiquement accompagné par un chef de projet de la plate-forme [...]. Doctolib a développé depuis 2017 d'une part un greffon Chrome, d'autre part un petit client local [...]. « le but est toujours de faire gagner du temps médical aux praticiens ».

Enfin, l'interface de programmation (API) telle que développée au départ ne s'est pas révélée très adaptée pour les grosses structures.

Source : www.cio-online.com

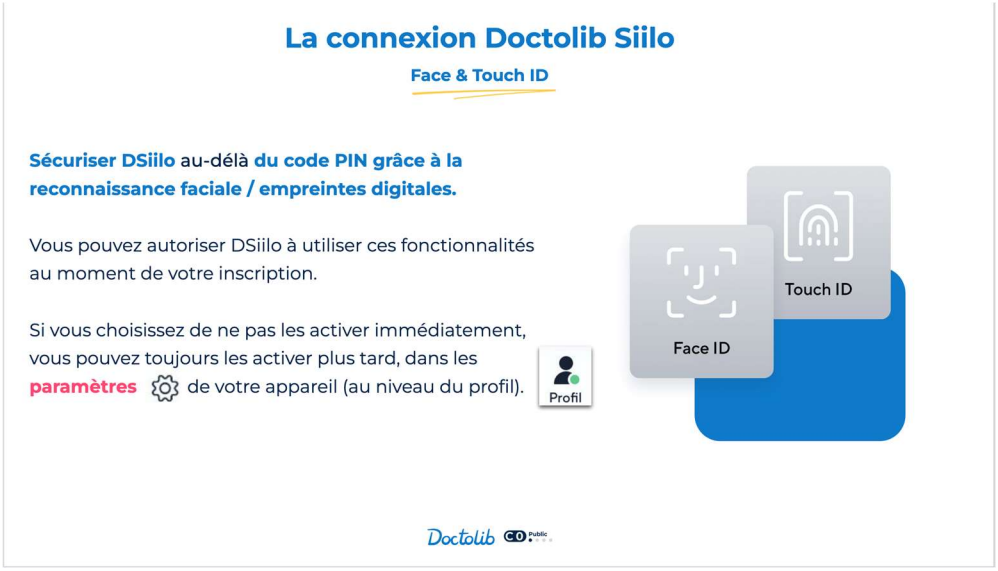
Document 8 – Siilo, une messagerie gratuite et sécurisée entre soignants

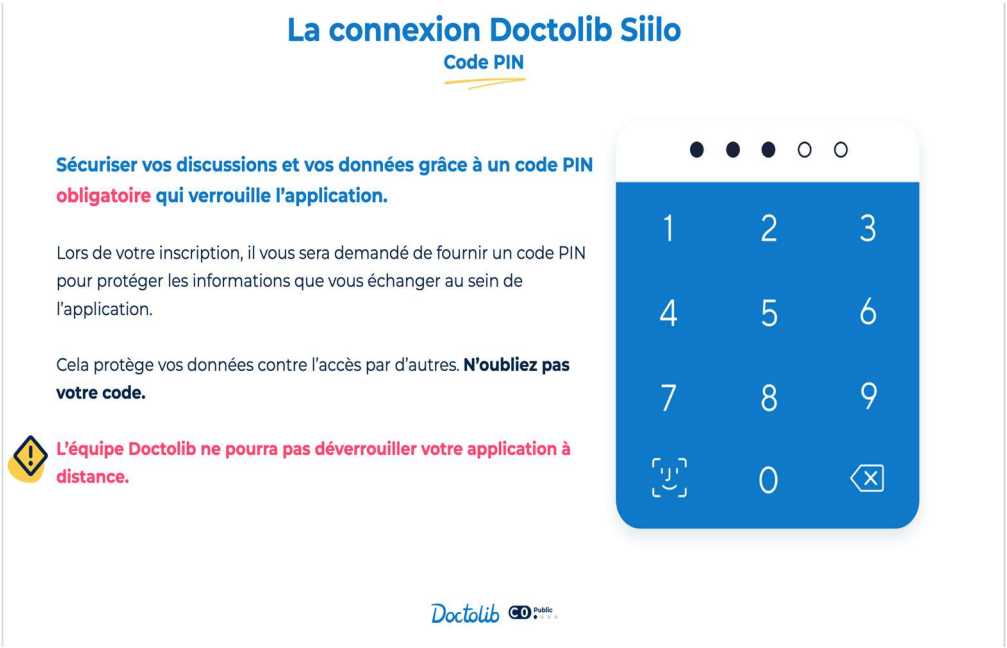
En mars 2022, Doctolib a levé un demi-milliard d'euros et avait déjà exprimé son ambition de développer une messagerie gratuite et sécurisée entre professionnels de santé. Quelques mois plus tard, cette ambition s'est concrétisée avec le lancement de Doctolib Team, un outil gratuit permettant aux soignants d'échanger en toute sécurité, de partager des documents et de collaborer autour de cas patients. La plateforme inclut également un annuaire de professionnels de santé. Le système de messagerie est en outre intégré aux logiciels sur abonnement de Doctolib, destinés aux professionnels de santé : Doctolib Patient et Doctolib Médecin.

Avec l'acquisition de Siilo, l'entreprise va pouvoir muscler sa plateforme de messagerie en s'appuyant sur une solide expertise dans le domaine. La jeune pousse (*start-up)* néerlandaise fondée en 2016 a développé une messagerie sécurisée pour soignants conçue pour être utilisée sur terminaux mobiles (*smartphones*). Ce sont ses choix technologiques qui ont attiré l'attention de Doctolib. Siilo revendique près de 500 000 utilisateurs qui échangent en moyenne 40 millions de messages par mois. La quarantaine de salariés de l'entreprise, basée au sein de son siège d'Amsterdam, devraient continuer d'y travailler.

Source : www.usine-digitale.fr

Document 9 – Les méthodes pour se connecter à la messagerie Siilo

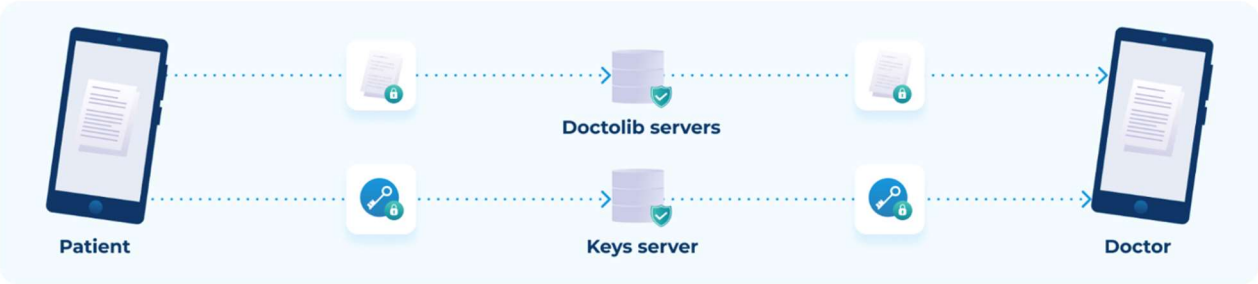




Document 10 – Échanges sécurisés des données chez Doctolib

Le chiffrement de bout en bout est idéal pour sécuriser l'échange de données sensibles où seuls les utilisateurs peuvent accéder aux données. Le protocole de bout en bout de Doctolib repose sur le chiffrement d'enveloppe (chiffrement et partage de clés). Il combine le chiffrement symétrique et asymétrique pour fournir un moyen rapide et efficace de chiffrer, et de partager des données entre les différents utilisateurs.

Dans un premier temps, le protocole chiffre la ressource (fichier, données, etc.) avec une clé de chiffrement symétrique générée aléatoirement. Cette clé de ressource est ensuite chiffrée de manière asymétrique à l'aide de la clé de chiffrement publique du destinataire de l'échange.



Les clés chiffrées peuvent ensuite être envoyées en toute sécurité vers l'espace en nuage (*cloud*) et stockées sur un serveur de clés distinct.

Lors de la consultation de la ressource le destinataire de l'échange pourra déchiffrer la clé de ressource à l'aide de sa clé privée asymétrique avant de déchiffrer la ressource à l'aide de la clé de ressource.

Source : media.doctolib.com

Document 11 – Programme de prime à la faille (*Bug Bounty*) chez Doctolib

Le programme de prime à la faille (*Bug Bounty*) de Doctolib est ouvert à tout expert en cybersécurité.

Dans un monde de plus en plus incertain, volatile et complexe, la cybersécurité est un enjeu majeur pour les entreprises. Depuis sa création en 2013, Doctolib a investi fortement dans ce domaine pour offrir les plus hauts niveaux de sécurité au personnel de santé et aux patients.

Doctolib participait déjà depuis plusieurs années à une version confidentielle de ce programme, et a décidé de l'ouvrir au public, en partenariat avec la plateforme YesWeHack, pour renforcer en continu la sécurité de ses systèmes.

Une étape importante pour Cédric Voisin, responsable sécurité des systèmes d'information de Doctolib : « Ce programme Bug Bounty étendu au public est un pas supplémentaire dans la prévention des failles de sécurité. Qui de mieux que les plus grands experts en cybersécurité pour les détecter ? En entretenant une relation de confiance avec eux, Doctolib conserve une longueur d'avance sur d'éventuels pirates mal intentionnés. »

Avec l'ouverture au public de son programme Bug Bounty, Doctolib propose désormais des récompenses financières pouvant s'élever jusqu'à 20 000 euros. Le montant de la prime est défini selon des critères précis, tenant compte du niveau d'importance de la faille et de la qualité du rapport de vulnérabilité soumis à l'équipe sécurité de Doctolib.

Pour participer, l'expert en cybersécurité s'inscrit au préalable sur la plateforme YesWeHack. Il compile ensuite un maximum d'informations techniques, qualifie le bogue (*bug*) et réalise des recommandations pour corriger la faille. Enfin, il soumet un rapport de vulnérabilité à l'équipe sécurité de Doctolib.

Source : about.doctolib.fr

Document 12 – Règles et récompenses du programme de prime à la faille (*Bug Bounty*)

Règles

Pour assurer la sûreté et la sécurité de toutes les parties concernées, nous avons établi les règles d'admissibilité cumulatives suivantes pour notre programme :

- être le premier à découvrir la vulnérabilité ;
- signaler la vulnérabilité exclusivement sur la plateforme yeswehack.com ;
- rédiger un rapport comportant une description claire de la vulnérabilité, écrire une procédure progressive pour reproduire le bogue et apporter des preuves par des captures d'écran ou de code ;
- fournir une explication claire de l'impact de l'exploitation de la vulnérabilité ;
- respecter les précautions d'essai (utilisation d'un faux compte patient et professionnel) dont en particulier l'interdiction d'hameçonnage sur les utilisateurs et les employés.

Le non-respect des règles précédentes entraînera le rejet de votre rapport.

Récompense

Il est considéré que le repérage de vulnérabilités importantes nécessite des récompenses plus élevées. Une structure de récompense spécifique et détaillée pour veiller à ce qu'il n'y ait ni confusion ni ambiguïté dans l'attribution des récompenses.

Source : d'après yeswehack.com

Document 13 – Typologie des risques et grille de récompenses (2 pages)

Typologie des données

Un système interne de catégorisation des données à caractère personnel (DCP) est mis en place en fonction de leur niveau de sensibilité et de risque de réidentification. Il permet d'évaluer avec précision la gravité de toute vulnérabilité identifiée, et de veiller à ce que les récompenses de notre programme soient adaptées au niveau de risque associé à la vulnérabilité.

Classification du RGPD	Typologie des données	Description et exemple
DCP	Type 1	Données présentant un faible risque de réidentification : - ID techniques - données pseudonymisées
DCP	Type 2	Données pour lesquelles l'identification des supports nécessite des données externes : - adresse IP - numéro de téléphone - adresse personnelle
DCP	Type 3	Données présentant un risque incontestable de réidentification - prénom et nom de famille - adresse électronique
Informations personnelles sur la santé	Type 4	Données susceptibles de fournir des informations sur l'état de santé d'une personne (par exemple : données sur les rendez-vous)
Informations personnelles sur la santé (et toute autre "catégorie spéciale de données" telle que définie à l'article 9 du RGPD)	Type 5	Toute information recueillie sur l'état de santé d'une personne, telle que ses signes vitaux, les résultats des tests et les diagnostics médicaux. Ces informations sont généralement collectées par les professionnels de santé et sont utilisées pour diagnostiquer et traiter les maladies, surveiller l'efficacité du traitement et suivre la progression de la maladie.

Grille de récompenses

Cette grille de récompenses a été conçue pour fournir des lignes directrices claires sur les types de vulnérabilité qui nous intéressent, ainsi que sur les récompenses correspondantes pour chacune d'elles. Si vous avez des questions sur notre grille de récompenses, nous vous encourageons à demander des éclaircissements par courriel.

Exploitation (catégorie)	Exploit (détail)	Impact sur les utilisateurs de Doctolib (professionnel et patient)
Accès aux DCP	Accès aux données du "type 1"	Faible
Accès aux DCP	Accès aux données "type 2"	Élevé
Accès aux DCP	Accès aux données du "type 3"	Élevé
Accès aux DCP	Accès aux données "type 4"	Critique
Accès aux DCP	Accès aux données du "type 5"	Critique
Manipuler notre application Patient pour envoyer des courriels à partir du serveur Doctolib	Attaque sophistiquée (ex : insérer des images dans les courriels Doctolib)	Moyen (peut-être élevé à notre discrétion)
Manipuler notre application Patient pour envoyer des courriels à partir du serveur Doctolib	Lien simple	Moyen
Manipuler notre application Patient pour envoyer des SMS à partir de "Doctolib"	Contrôle total du contenu	Élevé
Manipuler notre application Patient pour envoyer des courriels à partir du serveur Doctolib	Attaque de type injection Reliure injectable	Élevé
Scénarios intersites	Accès au DOM avec action de l'utilisateur requise (ex : xss)	Moyen

Source : d'après yeswehack.com