APPEL A CONTRIBUTION POUR LE FINANCEMENT D'UNE TECHNOLOGIE DE SECURISATION DES ECHANGES MULTISUPPORT

Ouvrir le chiffrement de haut niveau au grand public

NOVEMBER 14, 2018

SMES
6, rue Juge 75015 PARIS

Contents

PREAMBULE

Ce document a pour objectif de présenter SMes, son projet et son besoin en financement. Il est destiné aux sociétés de Capital Venture sollicitées

SMes est une entreprise de technologie fondée en 2017 par Sofiane. B, ingénieur docteur en Robotique et en Automatique.

SMes a pour mission de développer des applications destinées au grand public avec objectif de démocratiser la sécurité des échanges et permettre à tout utilisateur d'avoir le contrôle sur ses échanges.

1. LE PROJET

Aujourd'hui grâce à internet, aux réseaux de communications, aux smartphones, des milliards de personnes sont connectées échangent et envoient quotidiennement des milliards de messages, d'emails, de photos, etc.

Cependant, presque la totalité de ces échanges n'est pas ou est faiblement sécurisée, ce qui expose bien souvent la vie privée des milliards d'utilisateurs des réseaux sociaux et des messageries électroniques.

Chaque jour près de 270 milliards d'emails, 7000 milliards de SMS, 3 milliards de snaps sont envoyés. Beaucoup de ces échanges exposent la vie privée de leurs utilisateurs.

Beaucoup de projets ont été réalisé dans le but de permettre aux utilisateurs des réseaux de communication, de protéger leurs échanges à travers le chiffrement de messages, ainsi on compte de nombreuses messageries sécurisées tels que Telegram, Signal, Protonmail, d'autres opérateurs de messageries intègrent également le chiffrement de bout en bout en option, tel que Viber ou Whatsapp.

Cependant, le chiffrement proposé par les messageries actuelles et la sécurité revendiquée sont totalement dépendants de l'utilisation de la messagerie concernée. Il n'est donc permis aucune flexibilité à l'utilisateur.

De plus, le contenu chiffré par les messageries transite par les serveurs des mêmes messageries, bien que celles-ci affirment ne pas pouvoir accéder aux contenus une fois chiffres il serait plus **neutre de différencier les 2 services**.

SMes se propose de répondre à ces deux attentes :

1. Le chiffrement sécurisé avec RSA 4096 bits et AES 256 bits, le contenu chiffre ne transite pas par SMes

2. La sécurisation multi support, indépendamment de l'application ou du service utilisés

En donnant la possibilité à l'utilisateur de naviguer sur n'importe quelle messagerie, avec la garantie d'un très haut niveau de confidentialité, en offrant un canal de chiffrement indépendant du canal de messagerie.

La démarche de SMes a pour but de rendre possible le chiffrement de bout en bout pour tout partout et pour tous. L'application a été conçue pour offrir la sécurité, l'anonymat, la simplicité et la flexibilité.

En synthèse

Aujourd'hui il y a un intéressement et une sensibilisation ***grandissants*** *de la part du grand publique ainsi que des professionnels envers le sécurisations des échanges et la protection des données, sur le marché il* ***n'y a pas de réponse pertinente*** *à cette problématique (solutions pas flexibles, chers). C'est pour cela que nous nous proposons d'apporter une solution qui permette d'ouvrir le chiffrement de haut niveau au grand publique de façon flexible tout en garantissant l'anonymat et le respect de la vie privée.*

2. LA TECHNOLOGIE

SMes a pour objectif de répondre aux 2 problématiques citées précédemment :

- Permettre un chiffrement de bout en bout, robuste sur n'importe quelle messagerie et quel que soit le réseau utilisé.
- Offrir un canal de chiffrement totalement indépendant du canal de messagerie

Sans pour autant que l'utilisation de l'application ne nécessite une expertise particulière, en effet nous voulons démocratiser/étendre le chiffrement de bout en bout afin de permettre la confidentialité aux utilisateurs sur tous les réseaux.

SMes permet de chiffrer un contenu (pdf, doc, mp3, png, texto,...etc) et de l'envoyer à son ou ses destinataire(s) via n'importe quel messagerie (SMS, Messenger ™, Whatsapp ™, Viber ™, Facebook ™, Twitter ™,Yahoo ™, Gmail ™, Hotmail ™,...) et via n'importe quel réseau (internet, intranet, réseau téléphonique).

L'application exploite un protocole de chiffrement reposant sur deux algorithmes de chiffrements différents et fiables :

-Algorithme de chiffrement par clé asymétrique RSA-4096 bits

-Algorithme de chiffrement par clé symétrique AES-256 bits

3. EXPERIENCE UTILISATEUR

L'exploitation de l'application reste simple. L'utilisateur est invité à créer un compte sur SMes avec un minimum d'informations, sans besoin de fournir de donnée critique. La démarche consiste en 4 étapes :

1. **Création de compte** : à la création du compte une paire de clés RSA d'une longueur de 4096 bits est attribuée à l'utilisateur (opération à réaliser côte client, sur le terminal de l'utilisateur). L'utilisateur est ensuite invité à fournir un mot de passe de connexion dont la signature SHA-512 est envoyée sur le serveur :

    - Le mot de passe de connexion ne sert qu'à identifier la session de l'utilisateur et n'intervient en rien dans le chiffrement de ses messages.
    - La longueur du mot de passe de connexion doit être supérieure ou égale à 8 caractères, afin de protéger la session contre les attaques par dictionnaires, de plus des tentatives de connexion échouées résultent au blocage de l'adresse IP connecté pendant un laps de temps de sécurité.
    - Afin de faciliter l'expérience utilisateur, SMes permet l'authentification par empreinte digitale depuis la version 3.0, l'utilisateur peut s'affranchir de la saisie du mot de passe de connexion lorsqu'il le souhaite

2. **Création d'un mot de passe de déchiffrement :** L'utilisateur doit ensuite fournir un mot de passe (passe phrase) de déchiffrement, que seul lui connait. Ce mot de passe

n'est ni enregistré sur le terminal de l'utilisateur ni envoyé sur le serveur, ce mot de passe permet à l'algorithme AES-256 de chiffrer la clé privée créée précédemment (RSA-4096 bits). La clé RSA privé, chiffrée (et indéchiffrable, sauf par l'utilisateur) est envoyée sur le serveur.

Les mots de passe sont requis à la première connexion de l'utilisateur sur sa session, celui-ci n'a plus besoin ensuite de les réintroduire.

3. Ajout de destinataires : l'utilisateur rajoute des contacts via leur nom d'utilisateur, afin de chiffrer/déchiffrer des messages. SMes permet d'éditer un message texte, ou de sélectionner un fichier à chiffrer. Le contenu est chiffré selon le protocole suivant :

i. Une clé AES-256 bits est aléatoirement créée (différente pour chaque message), celle-ci chiffre le contenu à transmettre puis est ensuite elle-même chiffrée avec la clé publique du destinataire (disponible sur le serveur), le bloc obtenu est ensuite chiffré avec la clé privée de l'émetteur, le bloc obtenu est concaténé avec le message chiffre par AES-256 bits, le résultat est codé en base 64 et copier sur le clipboard, permettant à l'utilisateur de le coller dans la discussion de son choix. Le message ainsi envoyer est le code en base 64 d'une séquence binaire représentant un message chiffrer par les algorithmes les plus fiables qui existent aujourd'hui.

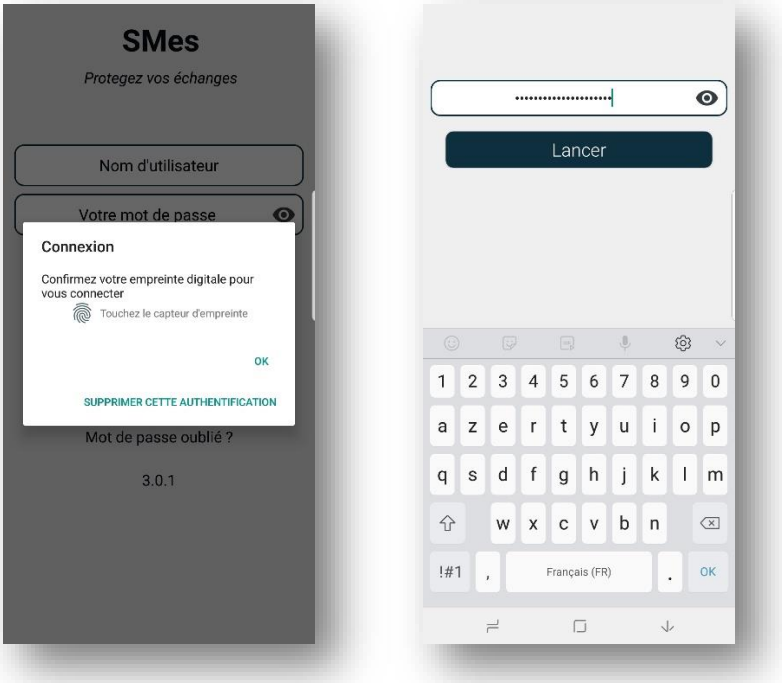
ii. Afin de déchiffrer un contenue reçu, l'utilisateur copie le message chiffrer vers le clipboard, puis sélectionne dans l'application le nom d'utilisateur de l'émetteur du message et choisit déchiffre, le contenu est directement importe puis déchiffrer grâce à la clé publique de l'émetteur (vérification de la signature, après deconcaténation) puis déchiffrer avec la clé prive du récepteur, le bloc obtenu représente la clé AES-256 bits qui permet de déchiffrer le message reçu, ce dernier est afficher en claire a l'utilisateur qui peut le sauvegardera à sa convenance dans le répertoire de l'application.

iii. Afin de faciliter l'expérience utilisateur, il est possible d'activer le mode automatique, cela permet d'importer et de déchiffrer automatiquement un message associer a un nom d'utilisateur, cela évite donc de réaliser la manipulation en ii

4. Partage d'information sur les réseaux sociaux : SMes offre un chiffrement de bout en bout entre 1 et plusieurs utilisateurs, en effet, si l'utilisateur le souhaite il peut chiffrer un contenu à destination de l'ensemble de ses contacts, cette fonctionnalité s'avère utile dans le cas du partage de contenu sur les réseaux sociaux, **lorsque l'utilisateur désire restreindre l'accès de ses publications au groupe de ses contacts**. Dans ce cas de figure le même protocole de chiffrement est réalisé mais la clé AES-256 bits est chiffrer pour chaque contact, séparément.

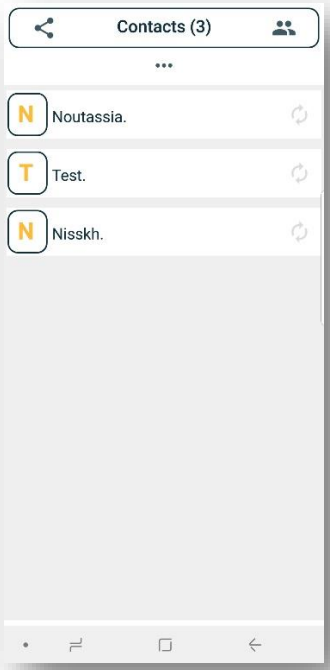
Le déchiffrement automatique : afin de faciliter l'utilisation de SMes notamment lors d'un ''tchat '', il suffit à l'utilisateur de copier le message reçu (appuie long sur le message puis copier) le message est automatiquement importé, déchiffré et affiché sur SMes, afin d'activer cette option l'utilisateur clique sur l'icône auto a cote du nom d'utilisateur de son contact.

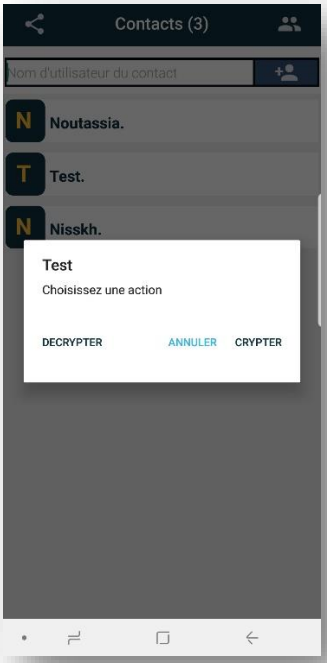
Les captures d'écrans suivantes illustrent l'expérience utilisateur sur SMes à la version 3.0.1



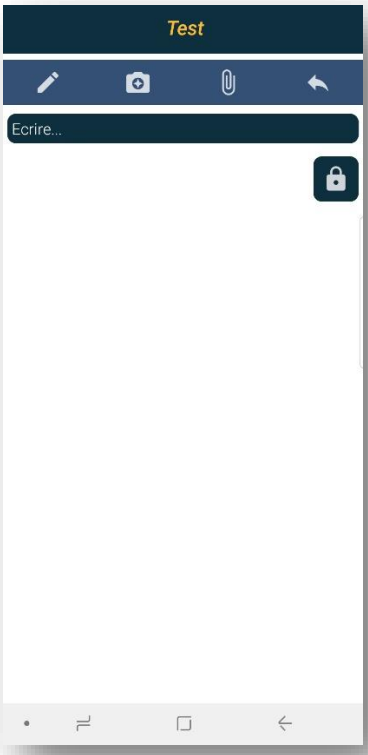
1. Connexion via nom d'utilisateur et mot de passe ou par empreinte digitale

2. Saisit du mot de passe de déchiffrement

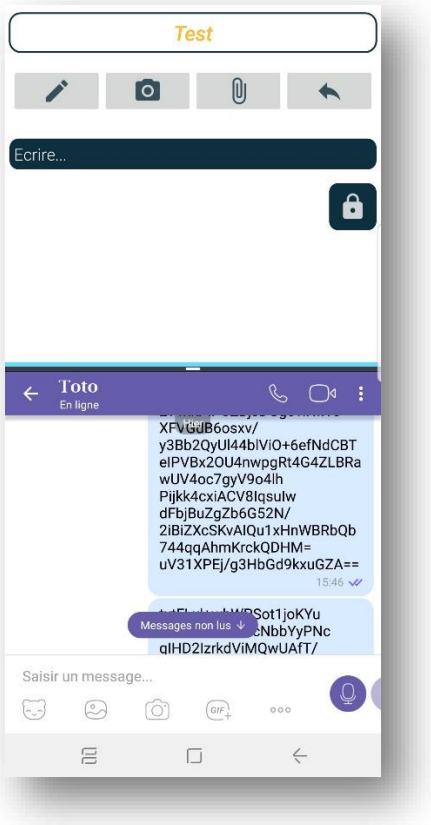




Rajout de contact par nom d'utilisateur Chiffrer ou déchiffrer en un clique



Editer un texte, importer un fichier ou une image, puis chiffrer automatiquement



Partage d'écran pour simplifier les choses

Figure 1 : différentes captures d'écrans illustrant l'application à la version 3.0.1.

4. LE MARCHE

L'application s'adresse en support à l'ensemble des réseaux sociaux. L'audience ciblée par l'application va des professionnels, journalistes, avocats, hommes d'affaires, chefs d'entreprises, homme politiques, diplomates mais également toute personne qui utilise les messageries et les réseaux sociaux désirant protéger sa vie privée et ses échanges, soit plus de 4 milliards de personnes. En effet, Facebook compte à lui tout seul 2.2 milliards d'utilisateurs, 1.2 milliard de personnes utilisent Messenger, 3 milliards utilisent Yahoo mail, 900 millions utilisent Gmail.

En effet, aujourd'hui le grand public est sensibilisé aux fuites de données, aux vols d'informations, aux écoutes et espionnages des communications, notamment grâce aux lanceurs d'alerte. On se rappelé tous des (SNOWDEN, Manings, Wikileaks, les récents scandales de Cambridge Analytica……). DuckDuckGo, un moteur de recherche dont la principale caractéristique est la confidentialité, vient d'atteindre le seuil de 30 millions de requêtes par jour, bien que cela ne représente qu'une toute petite portion du marché par rapport à Google ou Bing, cela marque l'intéressement de plus en plus croissant des personnes envers des services qui protègent leurs données.

De plus en plus de messageries proposent le chiffrement des messages, le marché des messageries sécurisées compte des projets ambitieux mais est loin d'être comblés, les principaux services de messageries sécurisées sont :

Protonmail spécialisé dans l'envoie des emails chiffres, Whatsapp, Telegram, Signal qui sont des messageries instantanées proposants un chiffrement de bout en bout.

5. TAILLE DU MARCHE

Aujourd'hui si on compte 4 Milliards d'utilisateurs dont 85% sous Android soit 3.4 milliards d'utilisateurs, si on ne considère que 10% de cette population est sensible à la sécurisation des messages, un potentiel de marché de **340 millions d'utilisateurs est largement atteignable uniquement pour Android et 400 millions toutes plateformes confondues.**

Aujourd'hui SMes est une application disponible pour les plateformes Android, néanmoins, nous avons comme ambition (d'améliorer l'appli en simplifiant le mode de sécurisation – copier / coller) de proposer ce service sur toutes les plateformes (IOS, Microsoft Phone, PC, MAC), afin de permettre à plus de personne d'utiliser SMes. En effet, le public vise par l'application comporte les professionnelles (journalistes, avocats, hommes d'affaires, politiques) mais également toute personne désirant protéger ses échanges sur les réseaux, potentiellement des milliards de personnes à travers le monde.

SMes est disponible en Français et en Anglais, mais d'autres traductions sont en cours d'ajout, tel que, l'Espagnole, l'Hindi, l'Arabe, le Chinois et bien d'autres encore.

6. LA CONCURRENCE

Protonmail : créé en 2013 la plateforme est passée de 2 millions d'inscrits en 2017 à 5 millions d'inscrits aujourd'hui. Le service offre 4 formules :

- Formule gratuite avec fonctionnalités limitées (espace de stockage de 500 Mo, et limitation à 150 messages par jours).
- Formule plus (1000 messages par jour et espace de stockage de 5 Go) 5 euros/mois et 48 euros/an.
- Formule professionnelle (Multi utilisateurs, 5 Go de stockage, messages illimites) 8 euro/mois et 75 euros/an par utilisateur.
- Formule visionnaire (Multi utilisateurs, 20 Go de stockage, messages illimites) 30 euros/mois, 288 euros/an.

Disponible sur IOS, Android, et navigateurs

Limites : ne permet pas de sécuriser des échanges au-delà de protomail, en effet, le service nécessite une adresse protonmail. En dehors de la version gratuite, limitée à 500 Mo, les services proposés vont de 5 euros/mois à 30 euros/mois avec une formule professionnelle à 8 euros/mois.

Telegram : créé en 2013, la plateforme compte aujourd'hui près de 200 millions d'utilisateurs. L'application est disponible pour IOS, Android, Windows et Linux. La création d'un compte nécessite une vérification du numéro de téléphone par l'utilisateur.

Limites : ne permet pas de sécuriser des échanges au-delà de Telegram

WhatsApp : créée en 2009, comptant aujourd'hui a près de 1.3 milliards d'utilisateur, cette messagerie n'est pas spécialisée dans le chiffrement de messages néanmoins elle offre un chiffrement de bout en bout à ses utilisateurs.

Limites : ne permet pas de sécuriser des échanges au-delà de Whatsapp

Signal : est une application pour Android et IOS, Signal permet aux utilisateurs d'envoyer des messages écrits, sonores et vidéo à d'autres utilisateurs Signal elle requiert un numéro de téléphone.

Les services cités ci-dessus n'offrent qu'une **sécurisation locale**, de plus le principe de **neutralité** n'est pas satisfait à partir du moment où les contenus chiffrés transitent par les serveurs du fournisseur du chiffrement.

7. LA VALEUR AJOUTEE DE SMes

SMes se distingue des applications citées précédemment par le fait que SMes n'est pas une messagerie chiffrée, mais un **service de chiffrement compatible avec toutes les plateformes de messageries de courriel et réseaux sociaux existants**.

Le niveau de **confidentialité délivré par le service repose sur des algorithmes puissants et fiables RSA 4096 bits et AES 256 bits**, l'utilisation de l'application est **simple, intuitive et surtout anonyme**, l'application ne collecte aucune donnée sur les utilisateurs, ne requiert aucune vérification à la création d'un compte. L'application permet de démocratiser le chiffrement de bout en bout et de sécuriser les échanges au grand public et permet son adaptation à l'ensemble des moyens de communications disponibles aujourd'hui.

Là où les autres applications **obligent la migration sur leurs plateformes**, en abandonnant l'utilisation des autres clients de messageries en échanges du chiffrement, **SMes permet de continuer à utiliser le réseau social préféré, la messagerie instantanée préférée ou la plateforme de courriel préférée en intégrant un niveau de sécurité extrêmement élevé.**

SMes offre 2 versions :

Version gratuite : sans limite de messages envoyés avec un nombre de contact maximal de 5, acceptable pour le grand publique.

Version Premium : sans limite de messages et de contact à 5,99 euros TTC, l'utilisateur peut chiffrer ce qu'il souhaite autant de fois qu'il le souhaite et a autant de personne qu'il souhaite

SMes offre la **sécurité**, la **neutralité**, la **flexibilité** et l'anonymat

8. LE MODELE ECONOMIQUE

Abonnement, l'objectif est de réaliser 200 000 abonnés la première année avec une progression de 15% chaque année pour atteindre plus de 1 millions d'abonnés sur un horizon de 5 années.

SMes a choisi la souscription à un abonnement pour tirer ses revenus. En effet, l'application propose dans sa version de base un rajout de contacts limité à 5 afin de chiffrer/déchiffrer des contenus et propose également un abonnement mensuel à 5,99 euros (TVA inclus), afin de rajouter autant de contacts que l'utilisateur souhaite. Mais pour financer son modèle économique SMes a besoin de fonds initiaux et d'investissements.

9. LES BESOINS DE SMes

Pour se développer SMes a besoin de faire appel à de nouvelles compétences :

A) Equipe Engineering & développement

Le rôle de cette équipe et l'administration des serveurs de SMes, la sécurisation du trafic, la maintenance, le déploiement, ainsi que le développement sur de nouvelles plateformes IOS, Microsoft Phone, BlackBerry, Navigateurs

B) Division marketing et développement commercial

A pour rôle de porter SMes au grand public par une présence sur les différents canaux de diffusion : réseaux sociaux, évènements…etc

Ci-dessous une synthèse des besoins pour lancer l'activité

Postes	Estimation budgétaire
Ressources cœurs **(administration de réseaux, développeurs)**	350 000 €
Développement commercial	150 000€
Infrastructures **(location de bureaux, équipements et serveurs en location)**	70 000€
Total	**570 000 €**

Tableau 1 : Synthèse des besoins pour le lancement de l'activité

10. REVENUS ESTIMES

L'objectif de SMes est de réaliser 1 millions d'abonnés dans un horizon de 5 années, soit 200.000 abonnés chaque année. Afin de se développer SMes a besoin de ressources financières, et publicitaires. Néanmoins, nous avons considéré une projection pessimiste permettant d'atteindre les 300.000 abonnés sur 5 ans, l'application permettrait de générer un résultat brut de 18M€ la cinquième année.

	2019	2020	2021	2022	2023
OPEX	- **530 000 €**	- **530 000 €**	- **635 000 €**	- **635 000 €**	- **635 000 €**
RESSOURCES	- 350 000 €	- 350 000 €	- 455 000 €	- 455 000 €	- 455 000 €
DEVELOPPEMENT COMMERCIAL	- 150 000 €	- 150 000 €	- 150 000 €	- 150 000 €	- 150 000 €
IMMOBILIER	- 30 000 €	- 30 000 €	- 30 000 €	- 30 000 €	- 30 000 €
CAPEX	- **70 000 €**				
INFRASTRUCTURE	- 70 000 €				
OPEX + CAPEX	- **600 000 €**	- **530 000 €**	- **635 000 €**	- **635 000 €**	- **635 000 €**
REVENUS	**1 200 000 €**	**4 800 000 €**	**9 000 000 €**	**12 600 000 €**	**18 900 000 €**
NB ABONNES	20 000	80 000	150 000	210 000	315 000
PRIX MOYEN UNITAIRE	5,0 €	5,0 €	5,0 €	5,0 €	5,0 €
RESULTAT BRUTS*	**600 000 €**	**4 270 000 €**	**8 365 000 €**	**11 965 000 €**	**18 265 000 €**
*** Hors taxes, impôts**					

Tableau 2 : tableau récapitulant les résultats attendus et OPEX CAPEX

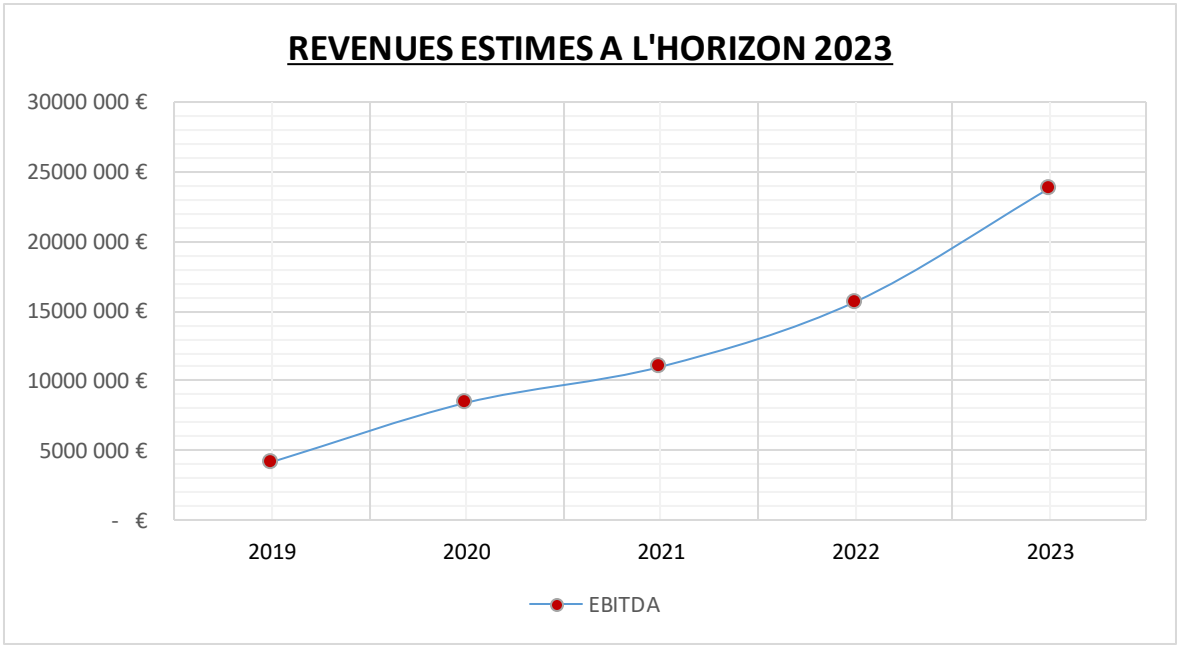


Figure 2 : Projection des revenus estimés sur un horizon de 5 années.

11. LES PRINCIPALES PHASES DU PROJET

2 grandes étapes permettront à SMes de s'ancrer sur le marché. La première année consistera à constituer les équipes, améliorer l'ergonomie de l'application et lancer SMes sur IOS et versions de bureau. La seconde année marquera l'extension de SMes à d'autres langues non couvertes actuellement et permettra également de stabiliser le fonctionnement de l'application.

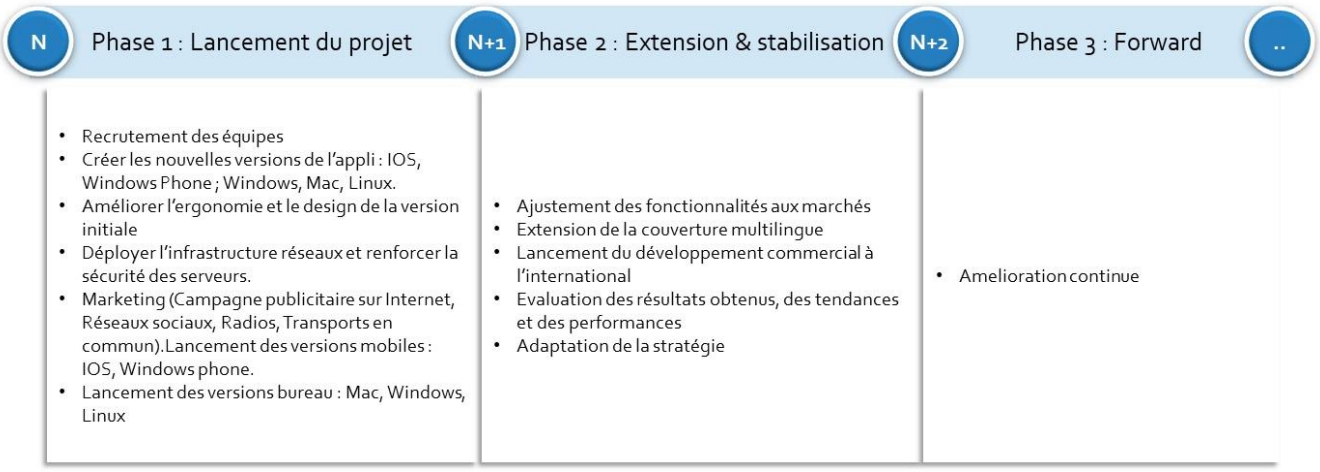


Figure 3 : résumé des grandes phases du projet

Au titre de ce projet, nous sollicitons un accompagnement correspondant **à une couverture budgétaire de 3 années** les principaux jalons visés la première année sont résumés dans la figure suivante : :

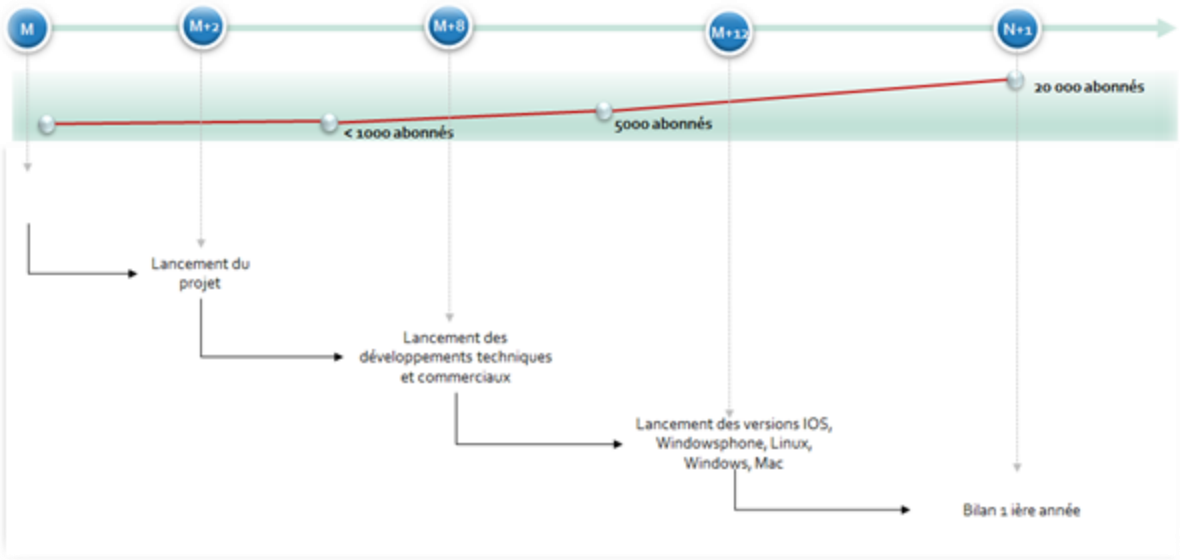


Figure 4 : résumé des différents jalons sur 1 année d'exercice

SMes travaillera continuellement dans la perspective d'améliorer constamment les 3 points clés suivants : **Fonctionnalités, Design, Fiabilité.**

1. Fonctionnalités : L'utilisation de SMes doit être la plus simple et efficace possible.

2. Design : Le design, l'ergonomie et le graphisme contextuel de l'application se doivent d'être aussi attractifs et fluides que possible.

3. Fiabilité : SMes doit tenir ces promesses en termes de sécurité et de confidentialité. SMes cible en premier lieu les utilisateurs déjà sensibilises à la protection de leurs données, puis dans un second temps, l'entreprise ciblera l'ensemble des utilisateurs des moyens de communications modernes, en sensibilisant d'avantage d'utilisateurs à la nécessiter de protéger leurs informations et donc à l'utilité du service proposé par SMes.

12. LE RISQUE ASSOCIE

Tout projet comporte bien évidement des risques, le risque majeur pour SMes est que l'application ne suscite aucun intérêt, toutefois l'investissement initial reste relativement limité, alors que le retour sur investissement quant à lui est potentiellement intéressant.

SMes ne compte pas sur les revenus publicitaires, SMes s'affranchit auprès de ses utilisateurs, des potentiels effets de conflit d'intérêts et indépendance vis-à-vis des annonceurs.

SMes, ne vends pas non plus de données, car au-delà de l'objectif de SMes de protéger les échanges des utilisateurs dans le monde, il n'est techniquement pas possible de vendre des données dont l'entreprise ne peut disposer, cela est une garantie d'autant plus forte pour les utilisateurs.

Le modèle de rémunération basé sur un abonnement est le plus approprié à la vocation de SMes car il permet :

- De s'affranchir des annonceurs, puisque ce sont les utilisateurs eux-mêmes qui font vivre l'entreprise et non pas les groupes publicitaires.
- Une plus grande efficacité, car les revenus suivent directement le nombre d'abonnés, il n'est donc pas nécessaire de disposer de plusieurs millions d'utilisateurs pour générer des revenus.

Tout en permettant à des milliards de personnes dans le monde, des professionnels, des artistes et des personnes lambda de pouvoir garantir la confidentialité et le respect de leur vie privée.

13. CONTACT

Brahim Sofiane BENCHABANE, Ingénieur en électronique spécialisé dans l'asservissement des systèmes. Sofiane est inscrit en Thèse de Doctorat dans la même filaire, avec une spécialisation en Robotique Biomédical et Intelligence Artificielle ;

Email : benchabane.ibrahim@gmail.com
Tél. 33.6.52.47.08.21