FPF Plénière mensuelle du 16 janvier 2025

Synthèse de l'intervention de Pierre Chassigneux

Pierre Chassigneux

Tout d'abord, quelques mots pour vous expliquer l'origine de la réflexion autour de b.connect. Il y a six ans je pilotais la direction du groupement CB en charge du projet *Faster by CB* et je me suis dit « cette énorme infrastructure d'authentification déployée dans le cadre de la DSP2, ne pourrait-elle pas être réutilisée en tout ou partie pour sécuriser non seulement le *check-out,* mais aussi le check-in (l'entrée en relation).

Avec 3D Secure, ce qui sert à aiguiller vers la banque, c'est le numéro, de la carte. Vous imaginez bien qu'on n'allait pas utiliser le numéro de la carte pour faire l'entrée en relation. Donc la deuxième idée, c'est la réutilisation des applications d'authentification bancaire que nous avons tous dans notre poche aujourd'hui, et des serveurs d'authentification des banques qu'on adresse au travers des API open-banking. Cela signifie que 50 millions de personnes vivant en France vont pouvoir bénéficier du service b.connect sans avoir à télécharger aucune application et sans avoir à réaliser aucun e-KYC.

Le problème de l'identité numérique, c'est la création d'un compte d'identité numérique, le processus d'enrôlement (e-KYC). La plupart du temps, malheureusement, les gens ne vont pas au bout du processus d'enrôlement car c'est compliqué : il faut fournir des documents, faire des selfies en photo et en vidéo, et il y a des taux d'erreur importants, de sorte que les gens sont obligés de s'y reprendre à plusieurs fois, et beaucoup abandonnent.

Avec b.connect on n'a pas ce problème. C'est la stratégie du « coucou », c'est-à-dire qu'on va se loger dans l'application bancaire, bénéficier du KYC que les banques ont réalisé sur leurs clients (depuis des dizaines d'années pour certains d'entre eux) et grâce au fait que les banques ont déployé des millions d'applications bancaires, on va pouvoir déployer très rapidement b.connect.

Avec b.connect, nous avons un double objectif : d'abord permettre aux consommateurs de ne plus avoir à gérer de mots de passe. Aujourd'hui, il y a à peu près 50 milliards de saisies de login/mot de passe par an en France, soit un peu plus de 2 fois le nombre de paiements par carte. Une très grande majorité est gérée par des mots de passe ; 10 à 20% sont gérés par ce qu'on appelle les « social login » (Google login, Facebook login…). Et il y a aussi des initiatives portées par un certain nombre d'acteurs très pointus en termes de sécurité, mais qui malheureusement pèsent très peu aujourd'hui sur ce marché.

Nos concurrents principaux sont les « social login » (Google et Facebook) qui, comme je l'indiquais plus haut, pèsent entre 10 et 20% sur ce marché en France (et beaucoup plus sur certains autres marchés). Mais ces solutions de « social login » ont une **double faiblesse**

- Ce sont principalement ce que j'appelle des SSO : vous utilisez le même login/mot de passe partout sur les sites, et si vous voulez passer en MFA, il faut faire un paramétrage. Or dans un marché de masse, si vous demandez aux gens d'aller dans la roue dentée du paramétrage, vous perdez 80% des utilisateurs. Donc les « social login » ne sont pas des solutions sécurisées. Ce sont des solutions faciles à utiliser puisqu'on a un mot de passe unique. Mais qui dit mot de passe dit phishing, on peut se faire voler son mot de passe, qui est un mot de passe rejouable. Donc les « social login » sont très problématiques au plan de la sécurité.
- Le modèle économique des GAFAM (apparente gratuité) repose sur la revente de nos données de connexion. Depuis quelques années, avec les efforts faits la Commission européenne et les régulateurs européens ou nationaux, il y a une prise de conscience de plus en plus forte de la nécessité de protéger ses données et de ne pas être le vecteur d'une monétisation de ses propres données.

Avec b.connect, nous traitons ces deux sujets.

- Ce n'est pas un SSO (ou alors un **SSO** MFA qui s'appuie sur un mécanisme d'authentification forte). Ça ne pourra pas être rejoué, car il n'y aura jamais de mot de passe dans l'environnement b.connect.
- Nous ne monétiserons jamais les données de connexion de nos utilisateurs.

Conséquence de cela : puisque nous avons prévu que le système soit gratuit pour les utilisateurs, il y aura un modèle économique pour les fournisseurs de services qui vont intégrer le bouton b.connect. Le sujet pour nous est donc d'inciter les fournisseurs de services à intégrer le bouton b.connect.

Aujourd'hui dans le e-commerce, il y a environ 25% d'abandons de panier car le client a oublié son mot de passe (ou son mot de passe ne fonctionne plus) et n'a pas envie de faire « mot de passe oublié » pour se recréer un nouveau mot de passe.

Ceux qui réussissent à passer cette première étape arrivent à la phase de paiement. Paiement par carte et, dans la plupart des cas, avec 3D Secure. Là, il y a encore 15% d'abandons de panier à cause de ce mécanisme d'authentification. Malgré les efforts qui ont été faits, les chiffres sont ceux-là : beaucoup de gens se sentent perdus avec cette solution d'authentification et abandonnent leur panier au moment du paiement.

Les Français ont une sensibilisation de plus en plus forte au risque d'usurpation d'identité en ligne.

88% de Français craignent une usurpation en ligne. 81% des fraudes sur Internet sont associées à des vols de données statiques (les « credentials » d'accès au compte). 71% des Français ne font pas confiance aux GAFAMs pour garantir la protection de leurs données personnelles. 58% des Français trouvent « agaçante » l'authentification par mot de passe.

Ce que j'ai appris de mes années chez CB et, auparavant, de mes années dans le domaine de la cybersécurité, c'est que quand on a à faire un choix entre sécurité et fluidité, c'est toujours au détriment de la sécurité : l'arbitrage se fait toujours en faveur de la fluidité du parcours.

Quand nous avons imaginé b.connect, nous nous sommes dit « il faut absolument que sécurité rime avec fluidité ». Mais c'est très difficile à faire. Comment avons-nous réussi à résoudre cette équation ? La décision d'authentifier activement n'est pas entre les mains de la banque, mais entre les mains du fournisseur de service, c'est-à-dire le e-commerçant. Ce n'est pas comme dans la DSP2, où le choix est entre les mains du banquier émetteur. Dans notre modèle, nous proposons un scoring hyper-perfectionné « sur deux cylindres » :

- Un cylindre que je qualifierai de de « *device fingerprint* » que vous connaissez, mais amélioré avec l'ajout d'une logique de cookie intelligent avec un *challenge response*, totalement transparent.
- Un cylindre qui est un scoring transactionnel. Chaque fois que vous cliquerez sur le bouton b.connect, un score sera calculé et selon le résultat de ce score, dans 80% des cas (selon nos estimations), vous aurez une authentification *frictionless,* c'est-à-dire sans action de l'utilisateur. Et dans les 20% restants, le système passera automatiquement la main à

l'application d'authentification bancaire, sans que vous ayez la moindre chose à faire si vous êtes dans une logique de smartphone : vous cliquez sur le bouton b.connect, le score est calculé, et s'il y a potentiellement un petit risque, on passe la main à la banque, mais de manière totalement transparent pour l'utilisateur l'application bancaire va s'ouvrir, contextualisée à b.connect (par exemple « BNPP pour b.connect »), vous faites un face-ID ou un touch-ID et c'est terminé

Le point fondamental pour nous, c'est cette fluidité, qui est liée à la puissance de ce moteur d'intelligence artificielle.

Le service sera gratuit pour l'ensemble des utilisateurs, mais les e-commerçants feront le choix de b.connect s'ils sont convaincus que ça leur apportera quelque chose à eux aussi. Il y a donc un véritable enjeu *business*, à deux niveaux :

- L'augmentation du nombre de paniers, en évitant les abandons lors de l'entrée en relation puis lors du paiement. Si je me suis battu pour arriver à lancer b.connect, c'est parce que nous sommes les seuls à faire le lien entre le *check-in* et le *check-out.* Je m'explique : lorsque vous cliquez par exemple sur le site de la Fnac, vous cliquez sur b.connect pour accéder à votre compte client. Vous achetez une tablette, et au moment de payer cette tablette avec votre carte CB, le score b.connect est transmis au *directory server* de CB (DSCB), qui va le transmettre au module de scoring RBA de CB, qui va le prendre en considération et envoyer un score enrichi (*Faster-by-CB* + b.connect) à l'ACS de la banque, qui va ensuite augmenter le taux *frictionless* des paiements par carte.

Du fait que vous utilisez b.connect en entrée et que le score b.connect va être transmis au *scheme* (qui peut être CB, Visa ou Mastercard : nous sommes totalement agnostique à l'égard des *schemes* de paiement) et va être pris en compte par le *scheme* pour ensuite augmenter le score final et le transmettre à l'émetteur. Bien évidemment, C'est toujours l'émetteur qui décide d'authentifier ou de ne pas authentifier activement son porteur, mais on va lui donner plus d'éléments de confiance, et donc augmenter le taux de *frictionless.* Et qui dit augmentation du taux de *frictionless* dit augmentation du taux de transformation.

Autre point important : b.connect est là non seulement pour authentifier, mais aussi pour donner des attributs d'identité. Exemple : je n'ai pas encore de compte sur le site de la Fnac et je veux me créer un compte. Je clique sur le bouton b.connect et je vais transmettre immédiatement à la Fnac toutes mes informations (nom, prénom, adresse mail, numéro de téléphone, adresse physique..) dès lors que j'ai donné mon consentement. La création de compte est donc largement facilitée (plus de mot de passe) ; il y a beaucoup moins d'abandons lors de la création du compte, et cela va aussi augmenter le chiffre d'affaires.

En outre, grâce aux éléments dits « non-rejouables » du MFA, on va réduire le risque de fraude qu'on appelle « *account takeover* » : aujourd'hui, les fraudeurs s'intéressent beaucoup plus au vol des *credentials* d'accès au compte qu'au numéro de carte, car la plupart des gens stockent leur numéro de carte sur leur compte client, et il suffit au fraudeur d'accéder au compte pour ensuite perpétrer une fraude. Les fraudes de type « *account takeover* » sont en augmentation de l'ordre de 50% ces deux dernières années. Le risque de vol de *credentials* est lié au fait que

les données sont statiques et peuvent être rejouées. Avec un système « non rejouable » comme b.connect, on lutte très efficacement contre ce type de fraude.

Dernier point : comme vous le savez, il y a aujourd'hui de plus en plus de faux sites. Quand nous mettrons le bouton b.connect sur un site, nous ferons un KYB et garantirons que ce site est bien celui qu'il prétend être. Il y aura donc un élément de confiance quant à l'identité et à l'authenticité du site sur lequel on va se connecter.

Le service b.connect sera lancé en juin prochain. Notre objectif est d'avoir au démarrage entre 10 et 20 très grandes enseignes du e-commerce pour attirer les utilisateurs et une fois que nous aurons créé des milliers de comptes clients, nous allons ouvrir l'*onboarding* à des milliers d'autres e-commerçants.

Merci de votre attention.

***

Hervé Sitruk

Merci Pierre.
J'ai une question : l'arrivée en 2026 du wallet d'identité numérique ne va-t-elle pas percuter b.connect ?

Pierre Chassigneux

Je te réponds à titre personnel :

- Avec b.connect, nous avons voulu définir un « couteau » et pas un « couteau suisse » Quand on a l'ambition de proposer un outil de connexion quotidienne pour un marché de masse, cet outil doit être hyper-simple et mono-fonction. Les logiques de wallet, qui sont par construction multifonctions, répondent à des usages qui ne sont pas ceux du quotidien. Les wallets d'identité ont un véritable intérêt dans une logique régalienne (pour prouver son identité partout en Europe devant les forces de l'ordre…).
- Nous ne sommes donc pas dans une logique de concurrence mais de complémentarité avec le wallet d'identité numérique.
- C'est un leurre d'imaginer que le wallet d'identité numérique sera disponible pour tous les français et tous les européens en 2026.

Hervé Sitruk

Je pense que nous avons besoin de solutions spécifiques au monde des paiements, mais nous allons être confrontés à une contrainte réglementaire et il faudra voir le moment venu

comment tout cela pourra s'articuler. Nous préparerons un position paper sur ces sujets et il serait bon que tu puisses participer à l'une de nos réunions pour challenger nos experts de l'identité numérique.

Pierre Chassigneux

Je voudrais faire une dernière remarque liée aux paiements : aujourd'hui, on observe une différenciation de plus en plus forte entre la *consumer authentication* et la *card holder authentication,* c'est-à-dire entre l'authentification d'un consommateur, quel que soit le moyen de paiement qu'il utilise, et l'authentification dans l'environnement du moyen de paiement. Click-to-Pay est typiquement basé sur cette distinction.

En termes de sécurité, il vaut toujours mieux sécuriser le plus en amont possible. Si je peux renforcer la sécurité au niveau du *check-in* (l'entrée en relation) je serai bien plus efficace que si je dois attendre le *check-out* pour le faire. Notre objectif est qu'une solution comme b.connect puisse être utilisée par n'importe quel moyen de paiement.

Vincent Duval

Peux-tu nous donner quelques indications chiffrées sur vos ambitions à l'horizon fin 2026 (nombre de clients, nombre de transactions…) ?

Pierre Chassigneux

Le lancement est pour juin 2025 et nous prévoyons d'avoir entre 5 et 10 millions de comptes b.connect créés d'ici juin 2026. Pour le lancement du service en juin/septembre prochains, nous visons entre 10 et 20 très grandes enseignes. Nous avons des discussions avancées avec une dizaine d'entre elles : des enseignes de e-commerce, mais aussi des mutualistes (qui sont soumis aux réglementations NIS2 et DORA et sont demandeurs de solutions d'authentification de type MFA).

Notre objectif est, dans un premier temps, « d'appairer » un maximum de comptes. Sachant que les Français ont en moyenne 8 fournisseurs de services (sites) avec lesquels ils sont en relation régulière, notre objectif pour la première année est que les gens qui auront créé leur compte b.connect aient « apparié » à b.connect la moitié de leurs comptes sur ces sites.

Notre *break-even* se situe aux alentours de 2 milliards de transactions.

Hervé Sitruk

Merci Pierre.