



**ENTRUST**

## Une grande banque britannique instaure confiance et sécurité dans chaque expérience de paiement grâce aux HSM nShield de Entrust

À mesure que la criminalité financière devient plus courante et plus complexe, les banques et les sociétés de services financiers travaillent constamment à l'amélioration des moyens de lutte contre la fraude, de l'installation des dernières technologies à la notification des clients lorsqu'un problème survient. Ce constat, ainsi que la garantie que l'argent de ses clients est en sécurité, est ce qui compose les activités d'une grande banque britannique.

La deuxième Directive européenne sur les Services de Paiement (DSP2) est destinée à améliorer la protection des consommateurs, à rendre les paiements plus sûrs et plus sécurisés et à faire baisser les coûts des services de paiement. La DSP2 régit tous les prestataires de services de paiement qui effectuent un paiement dans les États membres de l'UE et est applicable aux entreprises du monde entier.

Afin d'améliorer la sécurité et de réduire la fraude, la directive DSP2 impose une authentification forte des clients. En clair, cela signifie que davantage de contrôles seront mis en place pour les clients qui utilisent les services de banque en ligne, achètent en ligne ou effectuent des paiements sans contact.

« Nous sommes clients de Entrust depuis de nombreuses années maintenant, les HSM nShield de Entrust étant ceux de premier choix pour protéger les clés et les opérations de chiffrement de la banque. En déployant le pack d'options de services web, nous avons pu utiliser notre parc existant de HSM et fournir un moyen de chiffrer et de signer les données de transaction d'une manière conforme aux exigences de la directive DSP2. »

DÉCOUVREZ-EN PLUS SUR [ENTRUST.COM/FR/HSM](https://www.entrust.com/fr/hsm)

# » Grande banque britannique

## LE DÉFI COMMERCIAL

La banque devait mettre en place un mécanisme d'authentification forte des clients qui répondrait aux exigences de la directive DSP2 afin de réduire le risque de fraude en ligne. Elle devait mettre en œuvre un système d'authentification forte à deux facteurs (A2F) qui obligerait plus de 300 000 clients des services de banque en ligne à confirmer leur identité et les détails de leurs transactions, rapidement, simplement et à moindre coût.

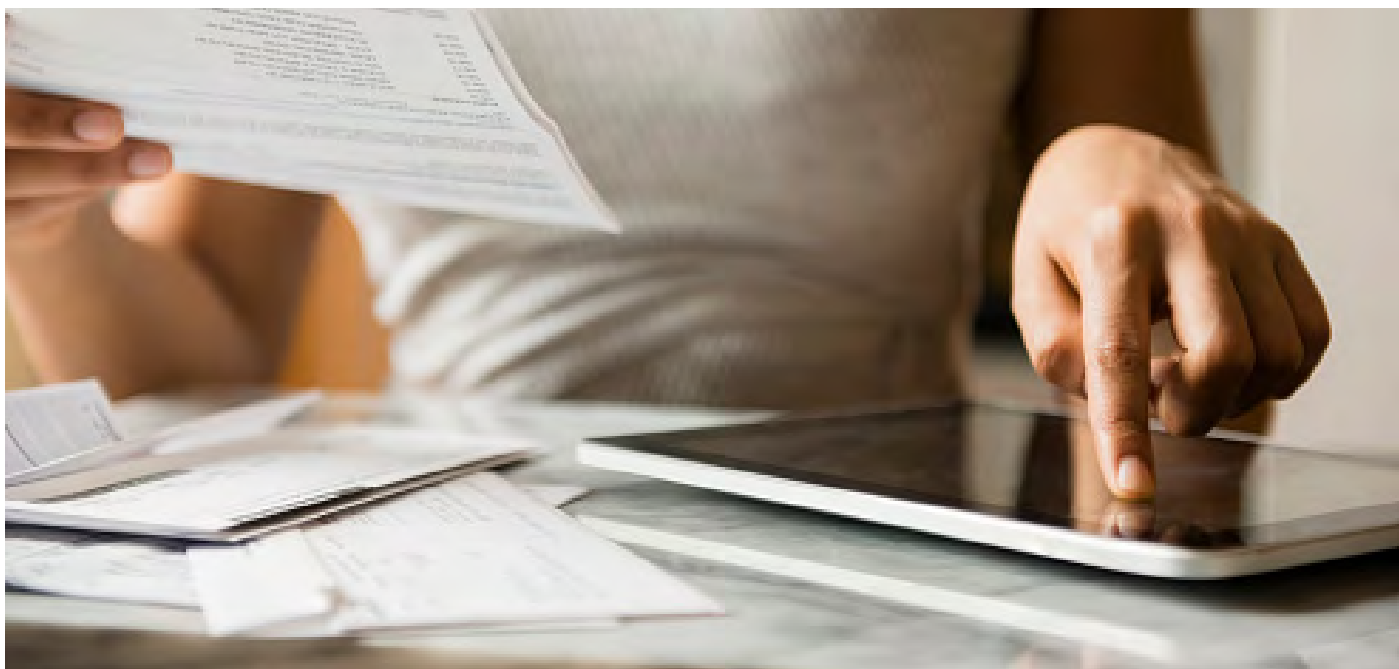
## DÉFI TECHNIQUE

L'un des changements apportés par la directive DSP2 est que l'authentification forte des clients exige d'inclure le montant de la transaction et le bénéficiaire dans le processus d'authentification. Le fait d'inclure des données de transaction dans le processus A2F signifie que les données doivent être chiffrées pour garantir leur sécurité et leur protection contre les pirates ou les individus malveillants. La solution a également besoin de fonctionner en temps réel, sans dégrader la vitesse du service visible par l'utilisateur final.

## SOLUTION

La banque a fourni à ses clients de banque en ligne un lecteur de carte à puce amélioré avec une fonctionnalité de QR code qu'ils peuvent utiliser pour se connecter, autoriser des paiements ou effectuer des changements administratifs. Les lecteurs de cartes ont une fonction d'affichage et de numérisation complète, plutôt que les traditionnels lecteurs de cartes avec une réponse de vérification.

L'application de banque en ligne affiche un QR code qui comprend les données de transaction chiffrées. Le client scanne le QR code avec le lecteur de carte à puce qui affiche ensuite les détails de la transaction. Si le client est satisfait, il saisit le code PIN de la carte à puce. Le lecteur affiche alors un code de réponse qui est réintroduit dans l'application de banque en ligne. Le code de réponse est ensuite vérifié et la transaction autorisée.





# Grande banque britannique



**Le soutien apporté par Entrust et son équipe de services professionnels a été sans faille. Ils nous ont aidé à développer une solution personnalisée et sur mesure qui a répondu à la fois aux besoins de la banque et aux exigences d'authentification forte de la DSP2. L'équipe de Entrust a été à la fois minutieuse et réactive, ce qui fait d'elle une solution AF2 robuste et rapide à déployer.**



Afin de protéger les données de la transaction tout au long de ce processus, le lecteur de carte doit être sécurisé et les données de la transaction doivent être chiffrées afin de garantir qu'elles ne peuvent être sabotées à aucune étape du processus.

Chacun des lecteurs de carte à puce est doté d'une clé publique et les données affichées dans le code QR sont chiffrées avec la clé privée associée. Cela signifie que le code QR ne peut pas être lu par un scanner de code QR standard, mais seulement par un lecteur de carte à puce émis par la banque avec la clé publique correspondante.

La banque possédait déjà un parc de modules matériels de sécurité (HSM) nShield® d'Entrust qu'elle utilise pour protéger les clés et les opérations de chiffrement de la banque. Elle utiliserait ces mêmes HSM certifiés FIPS 140-2 pour stocker et protéger les clés privées utilisées pour signer les données de transaction affichées dans le code QR avec le pack d'options de services web nShield.

Le pack d'options de services web nShield permet d'accéder aux HSM nShield d'Entrust, quel que soit leur lieu de résidence, en fournissant une API REST entre les applications nécessitant une clé de chiffrement et les services de protection des données. Il fournit une interface simple et fluide entre les lecteurs de cartes à puce et les HSM nShield de Entrust, sans qu'il soit nécessaire d'installer un client. Cela élimine les difficultés que peut présenter l'installation de logiciels sur des systèmes intégrés tels que les lecteurs de cartes.

Et sans qu'il soit nécessaire d'obtenir une licence pour des centaines de milliers de clients, cela représentait également une solution rentable. La mise en place et le déploiement ont été rapides et faciles avec l'aide de l'équipe de services professionnels Entrust. La banque avait besoin d'une option sur mesure du pack d'options de services web nShield standard, qui a été développé et construit par l'équipe de services professionnels, collaborant main dans la main avec les membres de l'équipe de la banque tout au long du projet.



# Grande banque britannique

## Défi commercial

Fournir une solution d'authentification forte à deux facteurs (A2F) du client pour répondre aux exigences de la DSP2

## Solution

- Les HSM nShield Connect de Entrust
- Pack d'options de services web nShield de Entrust
  - Connexion hautement accessible entre les applications cloud et les services HSM
  - Une interface simple, une intégration facile
  - Réduction des coûts et du temps de mise en place
- Équipe de services professionnels Entrust

## Résultat

Une solution d'authentification forte en temps réel, facile à déployer et sans heurts pour l'utilisateur final

## RÉSULTAT

La banque a pu offrir à ses plus de 300 000 clients de la banque en ligne une option d'authentification forte conforme à la directive DSP2, contribuant ainsi à protéger leurs entreprises contre les fraudes et les cyberattaques. Grâce au rendement élevé des HSM nShield de Entrust, le processus d'authentification des transactions s'est déroulé en temps réel, ce qui en fait un processus fluide et transparent pour l'utilisateur final. La solution générique personnalisée était beaucoup moins coûteuse et plus rapide à déployer que les autres options disponibles et envisagées par la banque.

## À PROPOS DE ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre portefeuille unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.



Découvrez-en plus sur

[entrust.com/fr/HSM](https://entrust.com/fr/HSM)



**ENTRUST**