DIRECTIVE DSP2 ET OPEN BANKING : DE LA CONFORMITÉ À L'AVANTAGE CONCURRENTIEL

Ping Identity

DSP2 & OPEN BANKING
NOTE D'INFORMATION SUR LA SOLUTION

FAVORISER L'INNOVATION GRÂCE AUX NORMES DE SÉCURITÉ

La directive DSP2, directive européenne révisée sur les services de paiement, bouscule le monde bancaire. Elle demande aux prestataires de services de paiement gestionnaires de comptes (ASPSP) d'exposer des API ouvertes afin de permettre à des prestataires tiers d'accéder à leurs informations de comptes clients, dès lors que le client a donné son consentement explicite.

Les ASPSP désignent tous les établissements financiers qui proposent des comptes de paiement avec accès en ligne. Visant à encourager la concurrence et à stimuler l'innovation dans le secteur financier, la directive DSP2 exige que tous les États membres la transpose en droit national d'ici le 13 janvier 2018. La France a publiée une ordonnance durant le mois d'août 2017, suivie de décrets d'applications publiés le 2 septembre 2017.

Étant donné la nature sensible des informations concernées, la directive DSP2 renforce également les règles applicables à la protection des données, à savoir vérification de l'identité des utilisateurs grâce à une authentification forte du client et possibilité pour les clients de donner leur consentement ainsi que de spécifier leurs préférences en matière d'utilisation des données.

ÉTABLIR UNE COHÉRENCE GRÂCE AUX NORMES

On pensait initialement que la directive DSP2 allait permettre de définir et de contrôler une norme stricte et interopérable pour des API ouvertes, afin d'offrir aux tiers un accès plus cohérent et plus facile à mettre en oeuvre. Un tel standard n'a pas été établi au travers de cette directive.

L'Autorité de la Concurrence et des Marchés britannique (CMA), chargée de renforcer la concurrence commerciale au Royaume-Uni, vient compléter la directive DSP2 avec sa norme en matière d'Open Banking. Elle définit des spécifications d'API ouvertes standardisées et détaille le type de données clients à partager ainsi que les conditions de leur disponibilité. La CMA tente de réduire le plus possible les obstacles à son usage afin d'opérer un véritable changement dans le secteur financier grâce à une concurrence et une innovation accrues.

Open Banking Ltd., l'entité de mise en oeuvre créée par la CMA pour fournir les spécifications d'API ouvertes standard, a adopté OAuth 2.0 et OpenID Connect (OIDC) comme protocoles standard d'authentification et d'autorisation pour les API ouvertes. Un partenariat avec le groupe de travail OpenID Financial API (FAPI) a permis de fournir des spécifications supplémentaires décrivant le protocole OAuth pour les applications financières.

D'autres pays étudient également l'idée d'une norme. L'Allemagne a mis en oeuvre l'Open Banking Project en 2010. De nombreuses start-ups américaines travaillent avec les banques pour développer des API mutuellement bénéfiques. Et Berlin Group, une initiative pan européenne pour les normes d'interopérabilité des paiements et leur harmonisation, définit des normes ouvertes et communes dans le domaine interbancaire.

IAM : CLÉ DE LA DIRECTIVE DSP2 ET DE L'OPEN BANKING

Ping Identity fournit la solution de gestion des accès et des identités (IAM) la plus complète pour répondre aux exigences de la directive DSP2 et de la norme sur l'Open Banking. S'appuyant sur les standards recommandés (auxquels nous avons participé), les fonctionnalités étendues de la plate-forme Ping Identity répondent parfaitement aux exigences de l'Open Banking. Elles sont spécifiquement conçues pour satisfaire aux strictes conditions de sécurité du secteur financier, tout en assurant une expérience utilisateur fluide et cohérente.

La plate-forme Ping Identity résout les défis de l'Open Banking de la manière suivante :

- Authentification : mise en place d'un flux d'authentification flexible prenant en charge une authentification forte client, et plus.
- Autorisation : émission et gestion de tous les jetons OAuth et OpenID Connect (OIDC), tout en respectant le juste champ d'application et authenticité.
- Gestion du consentement : stockage des données d'identité, des règles d'accès et de consentement requises pour le respect de la directive DSP2 et du Règlement général sur la protection des données (RGPD).
- Sécurisation des API : protection des API via une passerelle de contrôle des accès basée sur des règles (Security Gateway).

SECURITÉ DES ACCÈS

PingFederate (single sign-on fédéré) : procure aux ASPSP un hub pour les transactions OAuth d'Open Banking, tient lieu de serveur d'autorisation OAuth et émet des jetons à partir de plusieurs endpoints, et de multiples protocoles.

PingAccess (sécurité des accès) : réduit le code personnalisé et renforce la sécurité des API en jouant le rôle de serveur de ressources OAuth qui valide les jetons d'accès et applique les règles d'accès pour les API.

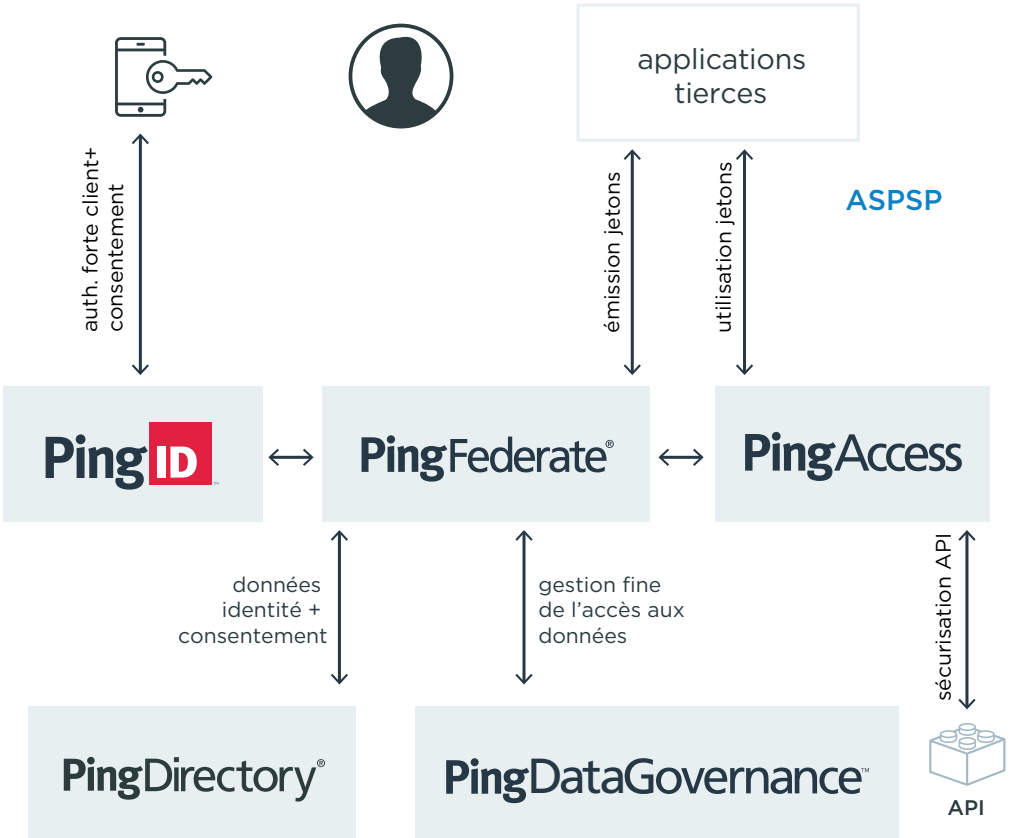
AUTHENTIFICATION CLIENT FORTE

PingID (authentification multi-facteurs) : un service simple et puissant qui assure une authentification forte client via notre service cloud d'authentification multi-facteurs et utilise des appareils mobiles réputés fiables pour une authentification et un consentement client fluides.

GESTION DU CONSENTEMENT

PingDirectory : référentiel de données hautement évolutif et flexible optimisé pour les identifiants clients ainsi que pour les données d'identité et de consentement.

PingDataGovernance : fournit des règles précises pour la gestion de l'accès aux données, le consentement et les données clients, ce qui donne aux entreprises le contrôle nécessaire pour un suivi des recommendations d'Open Banking et de l'application du RGPD.



DE LA CONFORMITÉ À L'AVANTAGE CONCURRENTIEL

Les solutions compatibles OAuth 2.0 et OIDC ouvrent la voie de la conformité. Mais au final, l'objectif visé étant l'avantage concurrentiel, c'est en offrant une meilleure expérience client qu'il pourra être réalisé. Si vos clients recherchent le confort, ils veulent aussi se savoir reconnus et en sécurité lors de chaque interaction. Les ASPSP qui ne se contentent pas des normes de conformité et qui proposent une expérience utilisateur sécurisée, unifiée et sans friction vont prendre l'ascendant.

La plate-forme Ping Identity offre le niveau de sécurité requis dans le secteur financier tout en fournissant à vos clients l'expérience qu'ils attendent. Réponse idéale aux défis que vous rencontrez, elle vous permet, au-delà des questions de conformité, de consolider un net avantage sur vos concurrents.

Pour découvrir comment Ping peut vous aider à transformer les défis de la directive DSP2 et de l'Open Banking en opportunités, consultez la page www.pingidentity.com/PSD2_FR.

#3264 | 7.17 | v02