Microsec aide les banques à tirer parti des possibilités offertes par la DSP2 grâce aux HSM nShield de Entrust

Les avantages d'un système bancaire ouvert, où les informations financières sont partagées de façon sécurisée avec l'accord du client, sont notamment une meilleure expérience client et de nouvelles opportunités génératrices de chiffre d'affaires. À l'aide des modules matériels de sécurité (HSM) nShield® de Entrust, Microsec a mis au point une solution inspirée de son secteur et de son expertise technique permettant aux banques et aux services financiers d'être à la fois conformes et compétitifs. Microsec est un des principaux acteurs du marché hongrois des technologies de l'information. Microsec assure le fonctionnement de l'autorité de certification e-Szignó, l'une des toutes premières autorités de certification (AC) en Europe à fournir des certificats qualifiés conformes à la nouvelle Directive sur les services de paiement (UE) 2015/2366 (DSP2).

Les principales activités de Microsec sont notamment :

- L'entretien et le développement du registre des sociétés et du système d'information des sociétés de Hongrie
- La fourniture d'une gamme complète de services de services d'infrastructure à clé publique (PKI) et de solutions commerciales, incluant entre autres des formations et du consulting, en Hongrie, en Europe Centrale et en Europe de l'Est
- La fourniture de services de confiance qualifiés conformes aux dispositions au règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS)

DÉFI COMMERCIAL

La deuxième Directive européenne sur les Services de Paiement (DSP2) vise à encadrer les services de paiement et les prestataires de services de paiement. Elle a pour objectif de donner une plus grande autonomie au consommateur dans l'accès et le contrôle de ses données financières et de renforcer la responsabilité des banques dans la protection de ces données.

La DSP2 permet également à des organismes tiers de concevoir de nouveaux services financiers innovants pour les comptes bancaires des consommateurs par le biais d'API ouvertes.

La DSP2 introduit deux changements majeurs dans le secteur des paiements. Elle instaure des exigences de sécurité plus strictes pour les transactions en ligne au moyen d'une authentification forte des clients et elle contraint les banques et autres institutions financières à autoriser les prestataires de services de paiement tiers à accéder aux comptes bancaires des consommateurs si les titulaires de ces comptes y consentent.

Microsec

Avant la DSP2, les prestataires de services financiers réalisaient des opérations au nom de leurs clients en utilisant les données d'identification de ces derniers. Cela exposait les données des clients à de sérieuses menaces de sécurité.

La directive DSP2 impose aux prestataires de services de paiement d'interagir avec les banques en utilisant leur propre identité plutôt que celle de leurs clients. Cela signifie que les banques devront publier des API ouvertes pour rendre les données des comptes clients accessibles aux prestataires de services financiers tiers. Pour ce faire, les banques devront déployer de nouvelles infrastructures qui intégreront l'utilisation de certificats numériques permettant d'identifier et d'authentifier à la fois le prestataire de services de paiement tiers et la banque.

CERTIFICATS NUMÉRIQUES QUALIFIÉS

Les normes techniques réglementaires de la DSP2 prévoient l'utilisation de certificats numériques qualifiés pour confirmer de manière sécurisée l'identité du prestataire de services de paiement (PSP) et sa clé publique. Les certificats qualifiés permettent aux PSP, dont les fournisseurs tiers (TPP) et les prestataires de services de paiement gestionnaire du compte (ASPSP) comme les banques, de se conformer à la DSP2. Ces certificats garantissent l'authenticité, la confidentialité et l'intégrité des communications, et constituent des preuves juridiquement contraignantes relatives aux opérations et à leur contenu.

Les certificats numériques qualifiés selon la DSP2 doivent être établis conformément à l'eIDAS qui exige que les prestataires de services de confiance (TSP) utilisent des systèmes fiables et des HSM certifiés pour protéger leur infrastructure d'émission de certificats. Les HSM nShield sont certifiés conformes aux Critères Communs EAL4 + AVA_VAN.5 et ALC_FLR.2 dans le cadre du profil de protection EN 419 221-5, conformément à la réglementation néerlandaise NSCIB. Grâce à la certification Critères Communs, les prestataires de services de confiance conformes à l'eIDAS qui fournissent des certificats numériques, des horodatages ou des signatures numériques peuvent bénéficier de solutions conformes à l'eIDAS.

Le prestataire de service de confiance qualifié (QTSP) qui émet le certificat doit vérifier toutes les données figurant sur le certificat qualifié et vérifier l'identité du prestataire de services de paiement. Les certificats qualifiés doivent être validés sur la base des listes de confiance de l'UE, qui contiennent la liste des prestataires de services de confiance qualifiés (QTSP) de chaque État membre de l'UE.

OPPORTUNITÉ OPÉRATIONNELLE

L'obligation d'utiliser des certificats numériques qualifiés a constitué pour Microsec une opportunité de développement et de générer plus de chiffre d'affaires. Microsec avait déjà permis à de nombreuses banques d'utiliser les outils d'authentification forte des clients prévus par la DSP2. L'obligation faite aux banques par la directive DSP2 de publier des API ouvertes pour rendre les comptes d'utilisateurs accessibles aux fournisseurs tiers impliquait en outre que Microsec pouvait également aider les banques et les fournisseurs tiers (TPP) à sécuriser leurs communications et à se conformer aux normes d'identification.

DÉFI TECHNIQUE

Pour pénétrer ce nouveau secteur d'activité, Microsec devait adapter et faire évoluer son infrastructure à clé publique (PKI) existante afin de pouvoir satisfaire la demande croissante et ainsi aider les banques et les fournisseurs tiers. Microsec avait besoin de définir de nouveaux profils de certificat pour les certificats spécifiques à la DSP2, de développer son logiciel d'AC pour les prendre en charge et de déterminer les procédures et modalités relatives à l'émission et à la gestion du nouveau type de certificat. Il lui fallait également procéder à l'évaluation de la conformité de son nouveau service de confiance : la fourniture de certificats qualifiés pour l'authentification des sites web.

INFRASTRUCTURE À CLÉ PUBLIQUE

Les applications commerciales de nouvelle génération ont de plus en plus recours à la technologie PKI afin de pouvoir assurer un haut niveau de sécurité à mesure que des modèles commerciaux en constante évolution deviennent de plus en plus dépendants du recours à des interactions électroniques qui nécessitent une authentification en ligne et le respect de réglementations toujours plus strictes en matière de sécurité des données.

Microsec

La directive DSP2 stipule que les prestataires de services de paiement doivent utiliser des certificats qualifiés, tels que définis dans le règlement eIDAS. Concrètement, il s'agit de certificats de clé publique basés sur des PKI qui sont conformes à la norme X.509. Bien que le règlement eIDAS soit neutre du point de vue technologique, la PKI est actuellement la seule technologie capable de garantir les niveaux d'ergonomie et de sécurité requis.

MODULES MATÉRIELS DE SÉCURITÉ (HSM)

Les HSM sont des appareils renforcés et inviolables qui permettent de garantir la sécurité des processus de chiffrement, de pouvoir générer, protéger et gérer les clés utilisées pour le chiffrement et le déchiffrement des données et d'établir des signatures et des certificats numériques. Les HSM sont testés, validés et certifiés conformes à des normes de sécurité parmi les plus rigoureuses telles que les FIPS 140-2 et les Critères Communs. Les HSM permettent aux organisations de :

- Respecter et même surpasser les normes réglementaires établies et émergentes en matière de cybersécurité, notamment l'eIDAS, la DSP2, le RGPD, la PCI DSS, l'HIPAA, etc.
- Bénéficier de meilleurs niveaux de fiabilité et de sécurité des données
- Conserver des niveaux élevés de service et de réactivité commerciale

Le règlement eIDAS stipule que les prestataires de services de confiance doivent utiliser des systèmes fiables et les normes techniques applicables requièrent explicitement l'utilisation de HSM certifiés pour protéger les clés privées utilisées pour émettre les certificats numériques.

SOLUTION

Microsec a consacré toute son énergie au développement du logiciel d'autorité de certification qui devait intégrer les nouveaux attributs nécessaires aux certificats numériques requis pour les opérations de TPP et d'ASPSP.

L'utilisation des HSM nShield de Entrust afin de protéger les clés privées utilisées pour l'émission des certificats numériques a permis à Microsec de répondre aux conditions de délivrance de certificats conformes à l'eIDAS et d'obtenir le statut conforme qui lui permet d'être reconnue comme un prestataire de services de confiance qualifié par tous les États membres de l'UE.

Microsec disposait déjà d'un important parc de HSM nShield de Entrust situé dans deux centres de données distincts : il disposait ainsi de la capacité et des moyens nécessaires pour répondre à l'augmentation prévue de la demande.

En outre, le cadre de gestion des clés Security World de nShield procure aux prestataires de services le contrôle total, une procédure de sauvegarde simplifiée, ainsi que l'évolutivité nécessaires au maintien d'une infrastructure de services qualifiée fiable.

Microsec a également mis en œuvre les procédures et protocoles nécessaires, notamment :

- La vérification de toutes les informations personnelles et organisationnelles requises lorsqu'une banque, un prestataire de services de paiement ou une société spécialisée dans la technologie financière sollicite un certificat
- La consultation du registre public de l'autorité nationale compétente pour vérifier que le prestataire de services de paiement dispose effectivement de l'autorisation de cette autorité compétente
- L'identification du numéro d'autorisation unique attribué au demandeur, qui fait office de numéro de référence ou d'identifiant unique au niveau mondial pour le certificat
- La vérification de la nature des fonctions que cette organisation pourrait être autorisée à remplir

RÉSULTATS

Microsec émet des certificats d'authentification web qualifiés (QWAC) conformes à l'eIDAS et des sceaux électroniques (QSealC) conformes à la norme ETSI TS 119 495, qui détermine la gestion et le format standard des données spécifiques à la DSP2. Le service est assuré dans tout l'Espace économique européen (EEE), et Microsec a déjà délivré des certificats spécifiques au DSP2 à des demandeurs de 10 États membres de l'UE.

Microsec

Besoin opérationnel

- Conception d'un service destiné à aider les banques et les fournisseurs tiers à respecter les règles de la directive DSP2

Besoin technologique

- Création d'une nouvelle solution à partir de l'infrastructure existante, à travers le développement des logiciels et des processus nécessaires pour l'émission des certificats spécifiques à la DSP2

Solution

- Les HSM nShield Solo de Entrust
- Des logiciels et processus d'AC personnalisés
- nShield Security World de Entrust

Résultats

- L'infrastructure en place a pu être rapidement et facilement complétée en vue du lancement d'un nouveau service permettant de bénéficier des nouvelles réglementations européennes et ainsi de générer plus de chiffre d'affaires.
- Une solution HSM éprouvée, fiable et performante
- Respect des normes réglementaires

Les services de confiance, le développement des logiciels associés et le consulting représentent actuellement les deux tiers du chiffre d'affaire de Microsec. Si l'on ajoute le nouveau service pour les prestataires de services de paiement, ses recettes internationales sont vouées à augmenter au cours des prochaines années.

Depuis 2007, Microsec est membre à part entière de l'Institut européen des normes de télécommunication (ETSI), un organisme de renommée mondiale. L'ETSI établit des normes applicables dans le monde entier pour les technologies informatiques pouvant servir de base aux futurs processus économiques. Microsec participe activement aux travaux du comité technique de l'ETSI pour les signatures électroniques et les infrastructures (TC ESI), et a contribué à l'élaboration de la norme de certification DSP2 TS 119 495.

Les produits et services de pointe de Microsec reposent sur son système d'assurance qualité inspiré de la norme ISO 9001:2008 et sur un système de gestion de la sécurité de l'information approuvé par la Lloyd's conformément à la norme ISO/IEC 27001:2013.

Pour en découvrir plus sur Microsec et ses solutions innovantes, rendez-vous sur : www.microsec.com

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

Nous contacter :
HSMinfo@entrust.com