Microsec aide les banques à tirer parti des possibilités offertes par la

(AC) en Europe à fournir des certiffcats qualiffés conformes à la nouvelle Directive sur les services de paiement (UE) 2□2□(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)

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 chi□rement, de pouvoir générer, protéger et gérer les clés utilisées pour le chi□rement et le déchi□rement 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 e□ectivement de l'autorisation de cette autorité compétente
- L'identification du numéro d'autorisation unique attribué au demandeur, qui fait o□ce 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.