DSP2 : tout ce qu'il faut savoir pour la conformité de vos certificats

La deuxième directive de l'Union européenne sur les services de paiement (DSP2) impose aux banques et autres prestataires d'appliquer des mesures de sécurité renforcées, à commencer par l'usage de certificats numériques qualifiés.

digicert® + QuoVadis

Qu'est-ce que la DSP2 ?

Depuis longtemps, la Commission européenne s'attache à renforcer la sécurité, la confidentialité et la fiabilité des paiements électroniques transfrontaliers au sein de l'Union. C'est ainsi qu'elle s'est attelée à la révision de la Directive sur les services de paiement (DSP), dont la nouvelle mouture a été baptisée DSP2 (Directive 2015/2366 de l'UE).

En vigueur depuis janvier 2018, la DSP2 vise à :

• Augmenter l'efficacité et renforcer l'intégration du marché européen des paiements

• Créer un espace de concurrence équitable pour les prestataires de services de paiement (PSP) dans l'UE

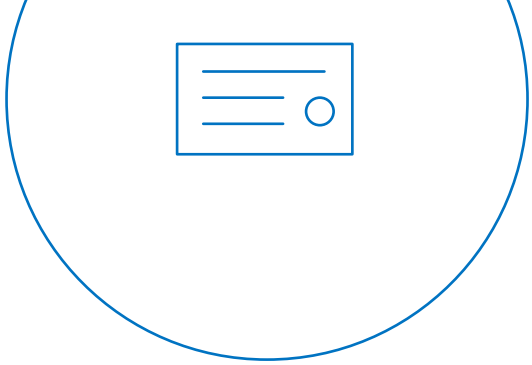
• Renforcer la sécurité des paiements électroniques

• Uniformiser les normes de protection des consommateurs

La DSP2 couvre de nombreux aspects du marché des paiements électroniques. On relèvera toutefois un durcissement des obligations de confidentialité et de sécurité des transactions en ligne auxquelles les banques et les prestataires de services de paiement seront soumis au sein de l'UE.

Qu'est-ce qu'un certificat eIDAS qualifié ?

Le règlement eIDAS (Règlement 910/2014 de l'UE) est un ensemble de normes établissant un cahier des charges pour les certificats numériques, l'authentification de leurs détenteurs, ainsi que les opérations des fournisseurs de services de confiance qualifiés (TSP, Trust Service Providers) qui les émettent.



Les certificats émis par des TSP qualifiés en accord avec les normes eIDAS sont appelés « certificats qualifiés ». Ils confèrent à leurs détenteurs un statut particulier dans certains cadres juridiques et règlementaires européens.

Pourquoi la DSP2 impose-t-elle des certificats qualifiés ?

Dans le cadre de la DSP2, les certificats numériques ont plusieurs vocations : valider l'identité des banques et prestataires de services de paiement, vérifier les rôles qu'ils sont autorisés à jouer, crypter les communications et, dans certains cas, poser un sceau infalsifiable sur des données ou des transactions.

En raison du caractère sensible des transactions financières, les normes techniques de réglementation (RTS) de la DSP2 spécifient que seuls les certificats eIDAS émis par des fournisseurs de services de confiance (TSP, Trust Service Providers) qualifiés peuvent servir à l'identification de prestataires de services de paiement.

DigiCert et QuoVadis sont-ils habilités à fournir des certificats qualifiés ?

QuoVadis, filiale de DigiCert, est un fournisseur de services de confiance (TSP, Trust Service Provider) qualifié de certificats eIDAS. Depuis ses implantations en Belgique, en Allemagne, aux Pays-Bas, en Suisse et au Royaume-Uni, QuoVadis émet des certificats conformes DSP2 pour ses clients à travers l'Europe.

Quels types de certificats qualifiés DigiCert et QuoVadis émettent-ils ?

DigiCert et QuoVadis émettent des certificats qualifiés pour signatures et sceaux électroniques, pour l'authentification des sites web (certificats TLS/SSL), pour l'horodatage et pour les exigences propres à la DSP2.

De quel type de certificat ai-je besoin pour me conformer à la DSP2 ?

Pour une communication sécurisée, la DSP2 préconise deux types de certificats numériques

- **Les certificats d'authentification web qualifiés (QWAC),** appliquant le protocole TLS tel que défini dans IETF RFC 5246 ou IETF RFC 8446, pour protéger les données lors de communications peer-to-peer et savoir qui contrôle les terminaux.
- **Les certificats de sceau électronique (eSeal) qualifiés** (QsealC), pour protéger des données ou des documents au moyen de normes comme ETSI, PAdES, CAdES ou XAdES, en plus de confirmer qu'ils proviennent bien d'une entité juridique.

De quel type de certificat ai-je besoin pour me conformer à la DSP2 ?

Chaque type de certificat DSP2 offre une protection spécifique aux différents domaines d'application.

	Certificats QWAC TLS/SSL	**Certificats eSeal / QsealC**
À quoi servent-ils ?	Identification des terminaux, protection des données durant les communications	Identification de l'origine des documents ou des données, et inviolabilisation lors du stockage et des communications
Quelles sont les fonctionnalités de sécurité ?	Confidentialité, authentification et intégrité	Authentification et intégrité
Ont-ils valeur juridique de preuve sur des transactions ?	Non	Sous eIDAS, oui
Lorsqu'elles passent par un intermédiaire, les données sont-elles protégées ?	Protection des communications peer-to-peer directes	Protection de bout en bout, même via un intermédiaire

Les normes techniques de règlementation (RTS) de l'Autorité bancaire européenne décrivent plusieurs scénarios dans lesquels les PSP peuvent utiliser des certificats pour sécuriser les communications. L'article 34, par exemple, propose un modèle de protection parallèle des données de transactions de paiement d'une part, et des canaux de communication par lesquelles celles-ci transitent d'autre part.

- Avec des certificats QWAC pour confirmer l'identité des PSP et leurs rôles respectifs, et pour sécuriser les communications au moyen du chiffrement TLS.

- Avec des certificats QsealC pour vérifier que les données applicatives soumises proviennent bien du PSP en question et n'ont pas été manipulées en cours de route.

Les banques recourant à des API pour l'accès en temps réel aux données client par des entités tierces agréées devront spécifier quel type de certificat DSP2 les PSP devront utiliser. Les PSP, eux, auront généralement besoin des deux.

Y a-t-il des exigences particulières concernant la gestion des clés privées ?

Si le règlement eIDAS impose souvent l'utilisation d'un dispositif de création de signature qualifiée (QSCD) pour protéger les clés privées, la DSP2 ne requiert aucun matériel de chiffrement spécifique pour les certificats QWAC ou QsealC.

Au lieu de cela, la directive autorise les sceaux électroniques avancés (Advanced eSeals) selon les définitions eIDAS, créés à l'aide de certificats QsealC.

Quels sont les jalons importants pour la mise en place des certificats DSP2 ?

Phase 1 : mars 2019

- Durant cette phase initiale, un environnement de test doit être mis en place dans lequel les prestataires tiers, même non agréés, pourront s'identifier au moyen de certificats tests et accéder à des comptes tests.

- DigiCert et QuoVadis proposent un processus simplifié d'émission de certificats DSP2 tests pour réaliser ces essais.

Phase 2 : juin 2019

- Durant cette phase, les banques doivent ouvrir leurs systèmes hébergeant des comptes client réels à des entités tierces agréées et déployer des certificats DSP2 de production.

- Les établissements financiers dans l'incapacité de respecter ce calendrier devront mettre en place une solution de repli, selon les termes de l'Article 33(6) du Règlement délégué (UE) 2018/389.

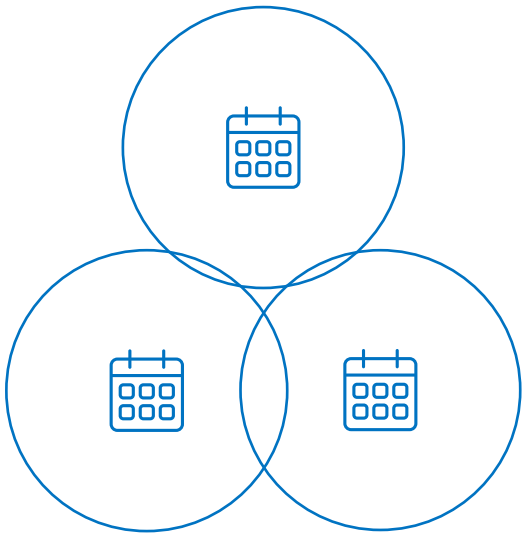
- DigiCert et QuoVadis sont d'ores et déjà prêts à émettre des certificats de production DSP2 qualifiés, lesquels sont délivrés à l'issue d'un contrôle plus poussé de l'identité des PSP et de leurs représentants agréés.

Phase 3 : septembre 2019

- Les établissements financiers s'engagent à opérer en totale conformité avec la DSP2.

Comment puis-je obtenir un certificat test DSP2 ?

Pour demander un certificat test, veuillez remplir le formulaire sur www.digicert.com/psd2-compliance-security-solutions. Ces certificats sont créés à partir d'une hiérarchie test, laquelle devra être ajoutée au magasin de certificats racine de confiance des systèmes de test.



Quelles sont les pièces à fournir pour obtenir un certificat DSP2 ?

Dans l'ensemble, les étapes de validation des certificats DSP2 sont semblables à celles des certificats TLS Extended Validation. Le règlement eIDAS met cependant davantage l'accent sur le contrôle d'identité. Généralement, cela implique la présentation des documents officiels du détenteur du certificat en personne au TSP qualifié.

Les certificats DPS2 étant délivrés à des entreprises, la personne se soumettant au contrôle d'identité devra être un fondé de pouvoir de l'entreprise (par exemple, un directeur dont le nom est inscrit au registre du commerce). Par la suite, ce fondé de pouvoir pourra autoriser d'autres collaborateurs (du département informatique, par exemple) à communiquer avec le TSP pour la gestion des certificats numériques.

NB : Pour faciliter le processus de validation en personne de son identité par le TSP, le fondé de pouvoir pourra recourir aux services d'un notaire accrédité par l'UE.

Le PSP demandeur devra également indiquer l'autorité nationale compétente ou l'autorité de règlementation financière à laquelle il est soumis. Le TSP qualifié devra s'assurer de la validité des agréments et rôles des demandeurs avant d'émettre les certificats.

Les rôles des PSP définis dans la norme ETSI TS 119 495 pour la DSP2 incluent :

- Fournisseur de services d'informations sur les comptes (PSP_AI)
- Fournisseur de services d'initiation de paiement (PSP_PI)
- Fournisseur de services associés aux comptes (PSP_AS)
- Fournisseur d'instruments de paiement par carte (PSP_IC)

Y a-t-il une norme spécifique aux certificats DSP2 ?

Une nouvelle norme ETSI (ETSI TS 119 495) vient compléter les autres normes eIDAS dans la définition des politiques applicables aux TSP, ainsi que des profils de certificats conformes aux RTS de la DSP2. Elle requiert les éléments d'identification suivants :

- L'autorité nationale compétente ou l'autorité de règlementation financière auprès de laquelle le PSP est inscrit
- Le numéro d'autorisation attribué au PSP par son autorité nationale compétente
- Les rôles DSP2 pour lesquels le PSP est agréé par son autorité nationale compétente

Lors du CA/Browser Forum, DigiCert a soumis la proposition de vote SC17 visant à inclure la DSP2 et d'autres formes d'identifiants organisationnels à la procédure d'émission de certificats TLS Extended Validation.

Pour en savoir plus, contactez DigiCert + QuoVadis
au +31 30 232 43 20 ou à psd2@quovadisglobal.com

© 2019 DigiCert, Inc. Tous droits réservés. DigiCert est une marque déposée de DigiCert, Inc. aux États-Unis et dans d'autres pays.
Les autres marques, déposées ou non, peuvent être des marques commerciales de leurs détenteurs respectifs.

digicert® + QuoVadis