DigiCert Group

Conformité au Règlement DORA

DigiCert ONE, des solutions garantes d'une fiabilité et d'une sécurité renforcées

digicert®

Janvier 2025

LIVRE BLANC

Conformité au Règlement DORA

DigiCert ONE, des solutions garantes d'une fiabilité et d'une sécurité renforcées

En bref

Le secteur des services financiers est sans doute le plus réglementé de tous. De la sécurité des systèmes de paiement aux obligations en matière de lutte contre le blanchiment d'argent, de nombreux facteurs nécessitent la mise en place de programmes matures pour la gestion des risques. C'est dans cet esprit que le Règlement DORA (Digital Operational Resilience Act) de l'Union européenne vise à rationaliser la gestion des risques liés aux technologies de l'information et de la communication (TIC) dans le domaine des services financiers. Il définit un cadre complet pour la gestion des risques, lequel prévoit un mécanisme de surveillance, l'obligation de signaler les incidents détectés, et le partage d'informations relatives aux menaces. Adopté par l'UE en décembre 2022, le règlement DORA entrera pleinement en application le 17 janvier 2025.

Champ d'application

Le règlement DORA s'applique à une grande partie du secteur financier. L'article 2, paragraphe 1 du document dresse la liste complète des différents types d'entreprises concernées. On note ainsi que le texte s'applique également aux nouveaux métiers des services financiers, tels que les acteurs du marché des cryptomonnaies, ainsi qu'aux prestataires de services TIC. Toutefois, de nombreuses exigences couvrent des pratiques déjà mises en œuvre dans de nombreuses sociétés du secteur, tant pour respecter la législation existante qu'à des fins de gouvernance interne.

L'article 1, chapitre 1 expose les grands principes du règlement DORA:

- Mettre en place un cadre interne de gouvernance et de contrôle pour la gestion des risques liés aux TIC
- Signaler les incidents majeurs liés aux TIC et notifier, à titre volontaire, les cybermenaces importantes aux autorités
- Déclarer aux autorités compétentes les incidents opérationnels ou de sécurité majeurs liés aux paiements, qu'ils soient ou non liés aux TIC
- Effectuer des tests de résistance des contrôles et pratiques de sécurité en place
- Partager des informations relatives aux cybermenaces et aux vulnérabilités
- Gérer le risque inhérent aux prestataires externes de services TIC

Impact

Les contrôles effectués dans le cadre du règlement DORA, ainsi que les amendes potentielles en cas de non-conformité, créent nécessairement des risques supplémentaires pour les entreprises du secteur. L'article 1, paragraphe 1 stipule notamment l'obligation de « notification aux autorités compétentes [...] des incidents opérationnels ou de sécurité majeurs liés aux paiements ». Les organisations ne peuvent donc plus passer sous silence les incidents dont elles ont été victimes, sous peine de sanctions financières. Quant aux risques auparavant jugés acceptables, ils devront pour certains d'entre eux être traités sans délai.

Leviers d'action

Si votre entreprise n'a pas encore adopté de dispositif de gestion des risques (ISO 27001 ou NIST 800-53, par exemple), l'heure est à l'action. En revanche, si un cadre de gouvernance est déjà en place, commencez par identifier les éventuels écarts entre vos pratiques actuelles et les obligations du règlement DORA. Élaborez et enclenchez un plan d'action pour combler ces lacunes, en documentant le processus pour en garder une trace et suivre votre progression.

Du fait des nouvelles obligations de déclaration des incidents, il est possible que certains risques autrefois tolérés soient désormais considérés comme inacceptables. Évaluez et modernisez en priorité vos systèmes d'ancienne génération et autres outils identifiés comme sources d'instabilité, de vulnérabilités et de surcharge de travail pour vos administrateurs IT.

Les solutions DigiCert

Partenaire de grands établissements financiers du monde entier, DigiCert aide ces derniers à renforcer la sécurité et la disponibilité de leurs systèmes critiques. Fruit de l'expertise de DigiCert en matière d'infrastructures à clés publiques (PKI) et de gestion du cycle de vie des certificats, la plateforme DigiCert ONE aide les entreprises du secteur à:

- Éliminer les pannes causées par des certificats expirés
- Résoudre plus efficacement les problèmes de sécurité liés aux certificats numériques
- Automatiser les identités sur l'ensemble des utilisateurs, des appareils et des machines afin de renforcer l'authentification et de sécuriser les communications
- Gérer les vulnérabilités dans les logiciels développés en interne
- Préserver l'authenticité et l'intégrité des logiciels et documents

Articles 1-3 – Pannes et autres incidents

Les articles 1 à 3 du règlement DORA portent sur l'obligation de notifier aux autorités les incidents de sécurité et les pannes touchant les systèmes TIC et de paiement. (Remarque : les défaillances touchant les systèmes de paiement n'affectent pas nécessairement les systèmes TIC.) L'article 3 contient la définition de ces deux types d'incidents:

- (8) « incident lié aux TIC » : un événement ou une série d'événements liés entre eux que l'entité financière n'a pas prévu, qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par l'entité financière
- (9) « incident opérationnel ou de sécurité lié au paiement » : un événement ou une série d'événements liés entre eux que les entités financières visées à l'article 2, paragraphe 1, points a) à d), n'ont pas prévu, lié ou non aux TIC, qui a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données liées au paiement ou sur les services liés au paiement fournis par l'entité financière

Avec DigiCert Trust Lifecycle Manager, les acteurs des services financiers peuvent dresser un inventaire complet de leurs certificats numériques, puis mettre en place des systèmes d'automatisation, d'alerte et de reporting pour anticiper et prévenir les pannes et les incidents de sécurité dus aux expirations ou révocations de certificats, ou autres changements effectués en urgence.

Article 9 – Protection et prévention

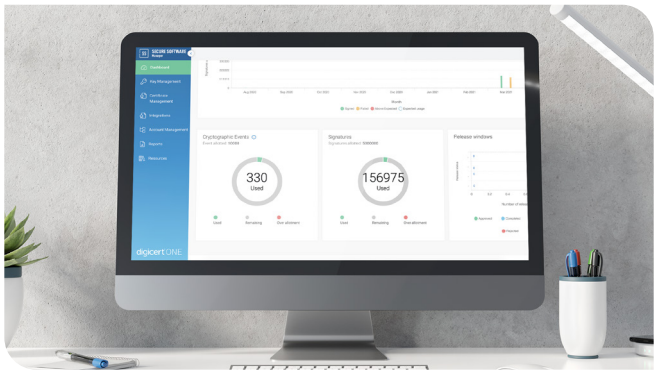
Axé sur la protection et la prévention, l'article 9 énonce des principes généraux concernant la confidentialité, l'intégrité, l'authenticité et la disponibilité des données – que celles-ci soient en cours d'utilisation, au repos ou en transit. Les établissements financiers de toutes tailles utilisent des infrastructures à clés publiques (PKI) pour renforcer l'authentification des utilisateurs et des machines, ainsi que pour faciliter le chiffrement des communications entre eux.

DigiCert Trust Lifecycle Manager combine PKI en tant que service, une gestion agnostique du cycle de vie des certificats et des intégrations robustes pour prendre en charge les identités et les charges de travail sécurisées sur les utilisateurs, les clouds et l'infrastructure sur site.

Article 11 – Réponse et reprise

Les prestataires de service financiers doivent agir rapidement en cas de compromission ou de révocation de certificats, ou – fait rare mais fortement perturbateur – en cas de déclassement (distrust) d'une autorité publique de certification.

Les capacités centralisées d'automatisation et d'inventaire de DigiCert Trust Lifecycle Manager permettent aux entreprises d'isoler, d'endiguer et de résoudre rapidement ces problèmes, tout en éliminant une grande partie des tâches manuelles généralement associées.



Article 25 – Gestion des vulnérabilités et tests de sécurité

L'une des sections les plus complètes du règlement DORA est l'article 25, paragraphe 1, qui détaille les catégories de test requises pour les outils et systèmes TIC.

> …l'exécution de tests appropriés, tels que des évaluations et des analyses de vulnérabilité, des analyses de sources ouvertes, des évaluations de la sécurité des réseaux, des analyses des écarts, des examens de la sécurité physique, des questionnaires et des solutions logicielles de balayage, des examens du code source lorsque cela est possible, des tests fondés sur des scénarios, des tests de compatibilité, des tests de performance, des tests de bout en bout et des tests de pénétration.

L'exécution de ces tests requiert un programme complet de sécurité faisant converger le physique et le numérique. Dans l'extrait ci-dessus, la mention des « solutions logicielles de balayage », autrement dit des logiciels de scanning, et des « examens du code source » nous intéresse particulièrement. En effet, les chaînes d'approvisionnement logicielles et le cycle de développement logiciels sont de plus en plus soumis aux exigences sectorielles et réglementaires, exigences pour lesquelles les outils traditionnels de test de sécurité des applications ne sont pas en mesure d'effectuer les contrôles requis.

DigiCert Software Trust Manager associe la signature de code d'entreprise à plusieurs techniques d'analyse de logiciels pour assurer une gouvernance rigoureuse des processus de signature de code, et ainsi détecter tout composant malveillant ou vulnérable au sein des logiciels. La solution combine gestion des clés et certificats de signature de code, l'analyse de la composition logicielle (SCA), la nomenclature logicielle (SBOM) et analyse des menaces ; le tout, unifié dans une approche basée sur des politiques. Software Trust Manager s'intègre facilement aux processus de développement logiciel et aux environnements CI/CD automatisés pour réduire en amont les risques d'incidents sur la chaîne d'approvisionnement logicielle.

Outils, méthodes, processus et politiques

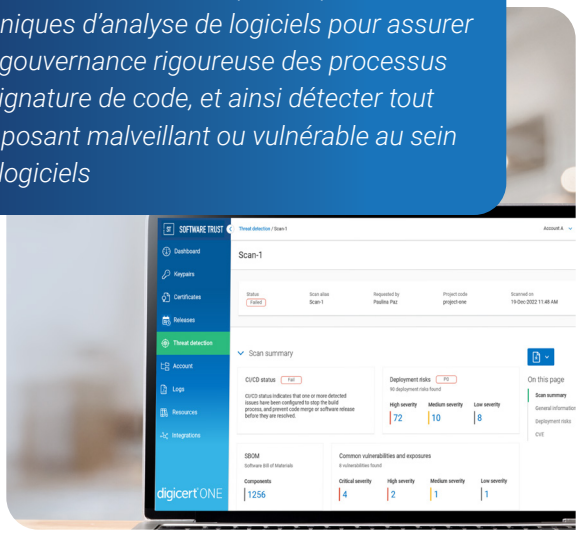
L'UE a publié des informations supplémentaires concernant les contrôles (techniques et autres) nécessaires pour se conformer au règlement DORA.

Chiffrement et cryptographie

Le recours au chiffrement pour sécuriser les données au repos, en transit et en cours d'utilisation est une pratique courante, pour ne pas dire requise, dans l'ensemble du secteur financier. Or, la robustesse d'un système de chiffrement est directement liée à la gestion des clés cryptographiques associées. Les articles 6 et 7 portant sur les exigences techniques stipulent les nouvelles obligations en matière de chiffrement, de gestion du cycle de vie des clés et d'application de toutes les politiques associées.

Trust Lifecycle Manager centralise l'application des politiques gouvernant l'émission, le renouvellement et la révocation des certificats numériques dans toute l'entreprise. Il est important de noter que cet outil n'entrave pas la propriété ni l'utilisation décentralisée des certificats par différentes unités opérationnelles. Par ailleurs, la solution Software Trust Manager, autre composante de la plateforme DigiCert ONE, enrichit Trust Lifecycle Manager de capacités de gestion des clés de signature de code et de contrôle d'accès spécialement conçues pour les environnements de développement logiciel.

DigiCert Software Trust Manager associe la signature de code d'entreprise à plusieurs techniques d'analyse de logiciels pour assurer une gouvernance rigoureuse des processus de signature de code, et ainsi détecter tout composant malveillant ou vulnérable au sein des logiciels



Gestion des vulnérabilités et des correctifs

Afin de satisfaire aux exigences réglementaires, les programmes de gestion des vulnérabilités étendent désormais leur champ d'action au cycle de développement logiciel. L'entrée en vigueur du règlement DORA en est l'exemple le plus récent. Comme le stipule l'article 10, paragraphe 2(d), les entreprises doivent:

- Tracer l'utilisation:
  - de bibliothèques tierces, y compris de bibliothèques à code source ouvert, utilisées par les services TIC qui soutiennent des fonctions critiques ou importantes;
  - de services TIC développés par l'entité financière elle-même, ou spécifiquement adaptés ou développés pour elle par un prestataire tiers de services TIC;

Pour suivre l'utilisation des composants logiciels tiers et répondre aux exigences de gestion des correctifs et de déclaration des vulnérabilités, les entreprises peuvent avoir recours aux nomenclatures logicielles (SBOM), à l'analyse de la composition logicielle (SCA) et à l'analyse des versions finales des logiciels pour y détecter d'éventuels malwares ou vulnérabilités, que ceux-ci aient été introduits par mégarde ou par malveillance.

Software Trust Manager combine signature de code, scans de sécurité logicielle et gestion des clés et certificats de signature pour vous fournir une approche basée sur des politiques qui sécurise le développement et la publication de logiciels. En intégrant Software Trust Manager à votre cycle de développement logiciel (SDLC) et à vos pipelines CI/CD, vous pourrez automatiser la gestion de la signature de code et la détection systématique des vulnérabilités dans vos versions logicielles.

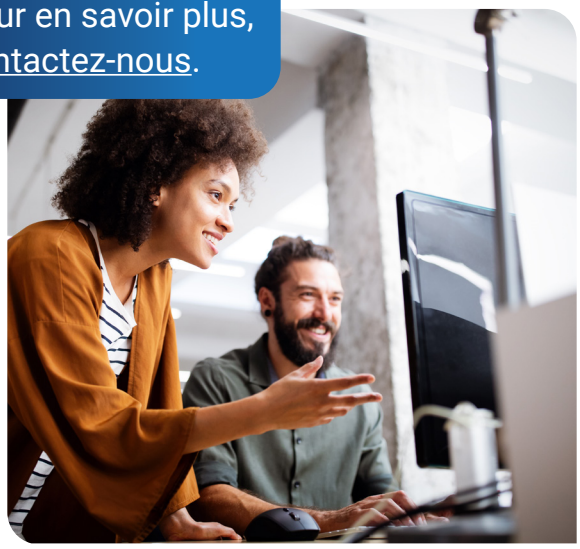
Conclusion

Le règlement DORA impose une approche complète de la cybersécurité et de la résilience opérationnelle dans l'ensemble des systèmes financiers. Il exige notamment la mise en place de dispositifs de gestion des risques, de contrôles de prévention et de détection, et de tests de sécurité réguliers, ainsi que la déclaration des incidents subis.

Les solutions DigiCert aident les établissements financiers à moderniser leurs PKI pour:

- Renforcer leur sécurité – Implémentez une authentification et un chiffrement robustes pour protéger vos données sensibles.
- Accroître leur résilience – Gérez et neutralisez rapidement les risques associés aux cyberattaques et autres perturbations opérationnelles.
- Simplifier leurs opérations – Automatisez la gestion de vos certificats et vos processus de sécurité des logiciels.
- Assurer leur conformité – Suivez votre niveau de conformité au règlement DORA à l'aide de journaux d'audit.

Pour en savoir plus, contactez-nous.



ANNEXE

Tableau des exigences techniques et des fonctionnalités DigiCert correspondantes

Exigence technique réglementaire	Fonctionnalité DigiCert
Article 6 – Chiffrement et contrôles cryptographiques	
1. Dans le cadre de leurs politiques, procédures, protocoles et outils de sécurité de TIC visés à l'article 9, paragraphe 2, du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre une politique en matière de chiffrement et de contrôles cryptographiques.	Trust Lifecycle Manager permet la surveillance et l'application centralisées des politiques de chiffrement liées aux certificats numériques utilisés pour identifier les utilisateurs et les machines, chiffrer les données en transit et générer des signatures numériques.
Article 7 – Gestion des clés cryptographiques	
2. Les entités financières définissent et mettent en œuvre des contrôles visant à protéger les clés cryptographiques tout au long de leur cycle de vie contre la perte, les accès non autorisés, la divulgation et la modification.	La plateforme DigiCert ONE utilise des modules de sécurité matériels (HSM) pour le stockage des clés privées et secrètes. Software Trust Manager inclut notamment un HSM basé dans le cloud pour stocker en toute sécurité les clés privées de signature de code.
3. Les entités financières élaborent et mettent en œuvre des méthodes pour remplacer les clés cryptographiques en cas de perte ou lorsque ces clés sont compromises ou endommagées.	Trust Lifecycle Manager et Software Trust Manager assurent le remplacement automatisé, groupé ou individuel, des certificats et des paires de clés associées, selon un intervalle de temps, une compromission ou un autre critère logique.
4. Les entités financières créent et tiennent un registre de tous les certificats et dispositifs de stockage de certificats pour au moins les actifs de TIC qui soutiennent des fonctions critiques ou importantes. Les entités financières tiennent ce registre à jour.	Trust Lifecycle Manager tient un inventaire continu de tous les certificats numériques au sein de votre entreprise, quelle que soit l'autorité de certification émettrice. La solution utilise pour cela différentes méthodes, dont l'intégration directe avec des plateformes de gestion des vulnérabilités et des autorités de certification tierces.
5. Les entités financières veillent au renouvellement en temps utile des certificats avant leur expiration.	DigiCert ONE automatise la gestion du cycle de vie des certificats pour un éventail de cas d'usage, parmi lesquels l'infrastructure d'entreprise, la signature de code logiciel, les appareils connectés, l'authentification des utilisateurs et la signature de documents.
Article 10 – Gestion des vulnérabilités et des correctifs	
1. Dans le cadre des politiques, procédures, protocoles et outils de sécurité des TIC visés à l'article 9, paragraphe 2 du règlement (UE) 2022/2554, les entités financières élaborent, documentent et mettent en œuvre des procédures de gestion des vulnérabilités.	Software Trust Manager fournit deux types d'analyses visant à détecter les problèmes potentiels dans vos logiciels développés en interne : l'analyse de la composition logicielle (SCA), pour identifier les logiciels open-source et tiers et détecter des vulnérabilités connues ; et l'analyse statique des binaires pour identifier les vulnérabilités, les malwares potentiels et les expositions de secrets. Ces processus génèrent chacun des nomenclatures logicielles (SBOM) dont la comparaison permettra de s'assurer qu'aucun composant supplémentaire n'a été inséré lors du cycle de développement.
2. a) determinar y actualizar los recursos de información que sean pertinentes y fiables para desarrollar y mantener la sensibilización sobre las vulnerabilidades,	DigiCert tiene socios que mantienen activamente bases de datos de vulnerabilidades y malware que utilizamos para realizar análisis de amenazas de software y notificar vulnerabilidades nuevas.

2(d) tracent l'utilisation : (i) de bibliothèques tierces, y compris de bibliothèques à code source ouvert, utilisées par les services TIC qui soutiennent des fonctions critiques ou importantes (ii) de services TIC développés par l'entité financière elle-même, ou spécifiquement adaptés ou développés pour elle par un prestataire tiers de services TIC	Software Trust Manager génère une nomenclature logicielle (SBOM) permettant d'identifier les composants contenus ou référencés dans vos logiciels. Ce même processus de scanning permet en outre de détecter des vulnérabilités connues et du code potentiellement malveillant, dans le cadre de votre programme de gestion des vulnérabilités au sein de vos logiciels développés en interne.
2(e) établissent des procédures pour une divulgation responsable des vulnérabilités aux clients, aux contreparties et au public	Software Trust Manager génère des nomenclatures logicielles que vous pouvez signer et publier lors de chaque nouvelle version pour améliorer la gestion des vulnérabilités et faciliter leur signalement.
Article 12 – Journalisation	
2(c) l'obligation de consigner dans les journaux les événements relatifs à l'ensemble des éléments suivants : iii) la gestion des modifications	Parties intégrantes de la plateforme DigiCert ONE, Trust Lifecycle Manager et Software Trust Manager assurent une journalisation détaillée et le signalement d'activités de sécurité ou d'administration de type renouvellement de certificats, rotation des clés ou signature de logiciels.
Article 13 – Gestion de la sécurité des réseaux	
(d) la définition et la mise en œuvre de contrôles d'accès au réseau afin de prévenir et de détecter les connexions au réseau de l'entité financière à partir de tout appareil ou système non autorisé, ou de tout point de terminaison ne répondant pas aux exigences de l'entité financière en matière de sécurité	Trust Lifecycle Manager s'intègre parfaitement aux technologies de gestion des terminaux comme Microsoft InTune, ainsi qu'aux solutions de gestion des infrastructures comme Terraform. Il permet ainsi d'automatiser la gestion des certificats utilisés pour authentifier les utilisateurs et les machines sur les réseaux d'entreprise.
(e) le chiffrement des connexions au réseau transitant par des réseaux d'entreprise, des réseaux publics, des réseaux nationaux, des réseaux tiers et des réseaux sans fil, pour les protocoles de communication utilisés, en tenant compte des résultats de la classification de données approuvée, des résultats de l'évaluation du risque lié aux TIC et du chiffrement des connexions au réseau prévu par l'article 6, paragraphe 2	Grâce aux capacités de découverte de Trust Lifecycle Manager, les terminaux de votre réseau disposent de certificats valides garants de communications chiffrées (TLS).