yubico

EBOOK - CONFORMITÉ DORA

Se préparer aux exigences du règlement DORA avec la YubiKey

Autorités européennes de surveillance (AES) / superviseurs principaux :

European Banking Authority

European Insurance and Occupational Pensions Authority

European Securities and Markets Authority

Entrée en vigueur : 16 janvier 2023 | Mise en application : 17 janvier 2025

Affecte approximativement :

- 22 000 établissements financiers[1]
- 15 000 fournisseurs de services TIC[2]

Des sanctions en cas de non-respect peuvent être infligées aux :

- établissements financiers
- individus tenus responsables
- membres du conseil d'administration
- fournisseurs de services tiers critiques

Près d'un cinquième de toutes les cyberattaques mondiales au cours des 20 dernières années ont ciblé le secteur financier[3]. Si le coût moyen d'une cyberattaque (0,45 million d'euros) ou d'une violation de données (5,53 millions d'euros) reste gérable pour une entreprise, le risque croissant de pertes extrêmes, pouvant atteindre 2,27 milliards d'euros, menace non seulement la solvabilité des entités compromises mais aussi la stabilité financière mondiale[4].

L'interdépendance technologique, telle que la dépendance partagée à l'égard des technologies de l'information et de la communication (TIC) tierces, accroît davantage le risque d'impact systémique entre les entités, les secteurs et les frontières. Par exemple, 8 % des cyberincidents mondiaux dans le secteur financier en 2023 pourraient être attribués à l'exploit MOVEit zero-day, illustrant l'impact significatif des violations de la chaîne d'approvisionnement par des tiers[5].

Qu'est-ce que le règlement DORA ?

Le règlement sur la résilience opérationnelle numérique (DORA)[6] vise à gérer les risques liés aux TIC dans le secteur financier européen et ses chaînes d'approvisionnement, afin de résister aux cyberincidents, d'y répondre et de s'en remettre, tout en assurant la stabilité financière même face à de graves perturbations.

DORA établit un cadre complet pour la gestion des risques internes et tiers. Le règlement vise à réduire la complexité réglementaire tout en harmonisant et en modernisant les règles de résilience opérationnelle et de gestion des risques issues de la législation antérieure dans l'ensemble de l'UE.

Qui doit se conformer au règlement DORA ?

Le règlement DORA est conçu pour s'appliquer à presque tous les établissements financiers ainsi qu'aux fournisseurs de services TIC tiers sur lesquels ils s'appuient, notamment les fournisseurs de services cloud, les processeurs de données et d'autres services TIC. Les fournisseurs de services TIC tiers concernés peuvent être basés n'importe où dans le monde, et pas uniquement dans des locaux situés au sein de l'Union européenne.

Au début de l'année 2025, certains fournisseurs de services TIC tiers seront classés comme « critiques » : des fournisseurs soutenant des fonctions essentielles ou importantes pour plusieurs établissements financiers, dont la défaillance pourrait avoir un impact systémique sur la stabilité, la continuité ou la qualité des services financiers[7]. Les AES exerceront une surveillance directe sur ces fournisseurs de services tiers critiques, en exigeant qu'ils établissent une filiale au sein de l'UE et qu'ils assument le coût de cette surveillance, proportionnel à leur chiffre d'affaires.

Établissements financiers[8]

Établissements de crédit	Établissements de paiement	Fournisseurs de services d'informations sur les comptes	Institutions de monnaie électronique	Sociétés d'investissement
Fournisseurs de services de crypto-actifs	Dépositaires centraux de titres	Contreparties centrales	Plateformes de négociation	Référentiels centraux
Gestionnaires de fonds d'investissement alternatifs	Sociétés de gestion	Fournisseurs de services de rapports de données	Sociétés d'assurance et de réassurance	Intermédiaires d'assurance, de réassurance et d'assurance à titre accessoire
Institutions de retraite professionnelle	Agence de notation financière	Administrateurs d'indices de référence critique	Prestataires de services de financement participatif	Référentiels des titrisations

Exemples de fournisseurs de services TIC tiers[9]

Directs ou indirects (sous-traitants)

Logiciels et services applicatifs (logiciels prêts à l'emploi ou développements personnalisés)	Services d'infrastructure réseau (à l'exclusion des télécommunications)
Centres de données	Services de conseil en TIC et services TIC gérés
Services de sécurité de l'information et de cybersécurité	Fournisseurs de cloud computing
Analyse de données et services de données (notamment la saisie de données, le stockage de données et le traitement de données)	Autre[10]

Quelle est la sanction en cas de non-conformité ?

Pour les fournisseurs de services tiers critiques informés de leur non-conformité, le règlement DORA accorde à l'organe de surveillance principal le pouvoir de contraindre le fournisseur à se conformer en imposant une sanction journalière (pouvant durer jusqu'à six mois) et pouvant atteindre 1 % du chiffre d'affaires moyen quotidien mondial de l'exercice précédent.

En ce qui concerne les établissements financiers reconnus en infraction, les autorités compétentes de chaque État membre définiront et appliqueront des sanctions administratives et/ou pénales « proportionnelles et dissuasives ». Ces sanctions peuvent être appliquées à un établissement financier, à une ou plusieurs personnes morales responsables de l'infraction et/ou à des membres de l'organe de direction.

Exigences du règlement DORA

DORA établit des exigences pour les établissements financiers afin de maintenir la sécurité des réseaux et des systèmes d'information et de soutenir la résilience. Pour ce faire, il établit des exigences pour les cinq piliers suivants :

Gestion des risques liés aux TIC	Signalement des incidents liés aux TIC	Tests de résilience opérationnelle numérique	Partage d'informations et de renseignements	Risque TIC tiers TPP | CTPP
Stratégies, politiques et outils pour protéger les données et les ressources TIC	Gestion et signalement des incidents liés aux TIC	Tests réguliers proportionnels à la taille et à l'importance de l'entité	Accords de partage formalisés	Atténuation du risque tiers par des dispositions contractuelles et un suivi

Alors que les établissements financiers exigeront, par le biais de dispositions contractuelles, des efforts similaires de gestion des risques de la part de leurs fournisseurs de services TIC pour se conformer au règlement DORA, les établissements financiers assument en fin de compte la responsabilité d'approuver, de gérer et de contrôler l'utilisation des services TIC, dans une démarche visant à « renforcer la responsabilisation » en matière de risques liés aux TIC des tiers[11].

Exigences du règlement DORA pour l'authentification

Dans le cadre du dispositif de gestion des risques requis, les entités concernées sont chargées d'établir des « politiques et des protocoles pour des mécanismes d'authentification solides » qui sont « fondés sur des normes pertinentes » et favorisent des « mesures de protection des clés cryptographiques »[12].

Les normes techniques réglementaires (NTR) conçues pour soutenir le règlement DORA ont été élaborées conformément aux normes internationales en matière de gestion des risques liés aux TIC, y compris la directive sur la sécurité des réseaux et des systèmes d'information (SRI, NIS en anglais), devenue SRI2, et le cadre de cybersécurité du NIST[13]. Ces normes précisent également que les méthodes d'authentification doivent être proportionnelles aux risques et conformes aux pratiques de pointe en matière d'accès à distance, d'accès privilégié et d'accès aux fonctions critiques ou importantes[14].

Comment identifier les risques d'authentification

Pour se conformer aux exigences d'authentification basée sur les risques de DORA, les entités concernées doivent choisir un mécanisme d'authentification en fonction de sa robustesse, en se référant à la norme mondiale NIST[15] ou eIDAS[16]. Ces lignes directrices reconnaissent **que toutes les solutions d'authentification multi-facteurs (MFA) ne se valent pas,** ce qui est reflété par les niveaux d'assurance d'authentification (AAL) ou niveaux d'assurance (LoA).

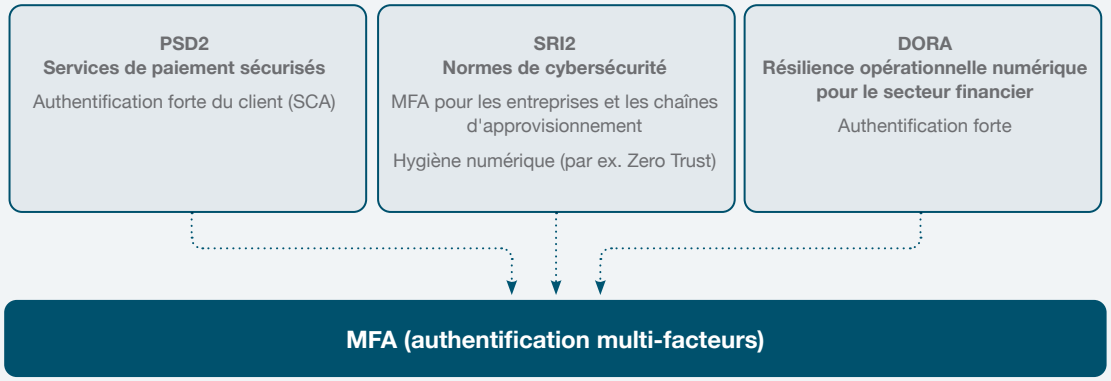
Bien que toute forme de MFA soit préférable à un simple mot de passe (AAL1/niveau de garantie faible), les formes classiques de MFA (AAL2/niveau de garantie substantiel), telles que les SMS, l'authentification mobile et les mots de passe à usage unique (OTP) présentent un taux de vulnérabilité aux attaques qui oscille entre 10 et 24 %[17]. Les systèmes d'authentification matériels résistants au phishing (AAL3/niveau de garantie élevé) offrent quant à eux les meilleures garanties, car ils limitent les risques de piratage des comptes[18].

AAL1	AAL2	AAL3
Authentification à facteur unique p. ex : nom d'utilisateur et mot de passe	**Authentification en deux étapes** p. ex : authentification à deux facteurs, passkeys synchronisées, passkeys matérielles sur des appareils à usage général	**Authentification multi-facteurs matérielle** p. ex : passkeys matérielles sur des clés de sécurité matérielles
		
• Garanties de sécurité faibles • Très vulnérable au phishing • Risquée pour les entreprises	• Authentification multi-facteurs/à deux facteurs résistante au phishing • Plus sécurisée qu'un mot de passe, mais vulnérable aux attaques • Plus adaptée aux entreprises, mais des lacunes en matière d'efficacité opérationnelle et d'exigences d'audit/de conformité	• MFA résistant au phishing • Sécurité et garanties maximales • Répond aux exigences de sécurité, d'efficacité opérationnelle et d'audit/de conformité des entreprises • Prend en charge FIDO et les cartes à puce/PIV • Conforme à la norme FIPS 140-2

En savoir plus dans notre guide sur la directive SRI2
Lire le guide

Quel est l'impact de la directive SRI2 sur le règlement DORA ?

DORA fait partie d'un trio de réglementations qui se concentrent sur le renforcement des protections numériques et la sécurisation des infrastructures numériques critiques, en commençant par le consommateur avec la directive sur les services de paiement (PSD), maintenant PSD2, puis en continuant vers les entreprises et leurs chaînes d'approvisionnement avec le règlement DORA et la directive SRI2. Ces trois règlementations gèrent les risques en exigeant une authentification forte. Étant donné que DORA a été conçu pour s'aligner sur la directive SRI2, les institutions financières, reconnues comme des entités critiques, devraient se conformer aux exigences renforcées de la SRI2, notamment la mise en œuvre de principes solides comme le MFA (AAL3/niveau de garantie élevé) et le Zero Trust.



Il est essentiel de noter que, bien que les exigences du règlement DORA prévalent sur celles de la SRI2 dans les domaines de chevauchement, les exigences de la SRI2 continuent de s'appliquer dans d'autres domaines[19]. Cela signifie que les exigences plus spécifiques de l'authentification multi-facteurs dans la SRI2, ainsi que les pratiques de cybersécurité telles que le Zero Trust, suggèrent que les entités concernées devraient évoluer vers l'utilisation exclusive d'une solution MFA résistante au phishing au niveau AAL2 ou supérieur.

Accélérer la conformité SRI2 avec la YubiKey

La YubiKey est une clé de sécurité matérielle conçue pour créer des entreprises où les utilisateurs résistent au phishing. Constituant une chaîne de confiance matérielle, la YubiKey offre une authentification hautement fiable et résistante au phishing. Fabriquée et programmée en Suède par Yubico, une société suédoise, la YubiKey est certifiée FIPS et FIDO.

Prenant en charge les protocoles à cartes à puce/PIV et FIDO2, ainsi que FIDO U2F, OTP/TOTP et OpenPGP, la YubiKey vous accompagne quelle que soit votre situation actuelle en matière de cybersécurité et s'adapte à de nombreux scénarios d'activité.

- Accès privilégié
- Environnements interdits aux mobiles
- Postes de travail partagés
- Personnel à distance
- Employés de bureau
- Accès des tiers
- Clients finaux

Avec la YubiKey, conformez-vous dès aujourd'hui aux exigences du règlement DORA. Pour des garanties élevées sur l'ensemble de votre chaîne d'approvisionnement TIC, exigez de tous vos fournisseurs de services qu'ils mettent en œuvre une solution MFA résistante au phishing pour leurs propres utilisateurs et systèmes.

Contactez-nous
yubi.co/contact-fr

En savoir plus
yubi.co/finance

Sources

[1] PwC, DORA et son impact sur les établissements financiers britanniques et les fournisseurs de services TIC, (consulté le 7 octobre 2024)

[2] Comité mixte des autorités européennes de surveillance, Rapport des AES sur le paysage des fournisseurs tiers de TIC dans l'UE, (18 septembre 2023)

[3] Le Fonds monétaire international, Rapport sur la stabilité financière dans le monde, (avril 2024)

[4] Ibid; Verizon, Rapport d'enquête sur les atteintes à la sécurité des données en 2024, 1er mai 2024

[5] Verizon, Rapport d'enquête sur les atteintes à la sécurité des données en 2024, (1er mai 2024)

[6] Journal officiel de l'Union européenne, RÈGLEMENT (UE) 2022/2554, (14 décembre 2022)

[7] Comité mixte des autorités européennes de surveillance, JS SC DOR-23-54, (26 mai 2023)

[8] Journal officiel de l'Union européenne, RÈGLEMENT (UE) 2022/2554, (14 décembre 2022)

[9] Comité mixte des autorités européennes de surveillance, Rapport des AES sur le paysage des fournisseurs tiers de TIC dans l'UE, (18 septembre 2023)

[10] DORA définit les autres services TIC comme suit : « Les services numériques et de données fournis par le biais des systèmes TIC à un ou plusieurs utilisateurs internes ou externes de manière continue, y compris le matériel en tant que service et les services matériels, qui incluent la fourniture d'une assistance technique par le fournisseur de matériel via des mises à jour de logiciels ou de micrologiciels, à l'exclusion du service téléphonique analogique traditionnel. » Journal officiel de l'Union européenne, RÈGLEMENT (UE) 2022/2554, (14 décembre 2022)

[11] Comité mixte des autorités européennes de surveillance, JC 2023 84, (17 janvier 2024)

[12] Journal officiel de l'Union européenne, RÈGLEMENT (UE) 2022/2554, (14 décembre 2022)

[13] Comité mixte des autorités européennes de surveillance, JC 2023 86, (17 janvier 2024)

[14] Ibid.

[15] NIST, Directives d'identité numérique NIST SP 800-63-4, (décembre 2022)

[16] Commission européenne, Niveaux d'assurances (LoA) eIDAS, (2014)

[17] Kurt Thomas et Angelika Moscicki, Nouvelle recherche : quelle est l'efficacité d'une hygiène de base sur un compte dans la prévention du piratage ?, (17 mai 2019)

[18] Office des publications de l'Union européenne,Règlement d'exécution (UE) 2015/1502 de la Commission, (septembre 2015)

[19] Journal officiel de l'Union européenne, Lignes directrices de la Commission sur l'application de l'article 4, paragraphes 1 et 2, du règlement (UE) 2022/2555 (directive SRI2), (18 septembre 2023)

yubico

À propos de Yubico

Yubico (Nasdaq Stockholm : YUBICO), l'inventeur de la YubiKey, fait figure de référence en matière d'authentification multi-facteurs (MFA) résistante au phishing, prévenant les piratages de compte et simplifiant la sécurisation des connexions pour tous. Depuis sa création en 2007, Yubico a joué un rôle de premier plan dans la mise en œuvre de standards mondiaux pour l'accès sécurisé aux ordinateurs, appareils mobiles, serveurs, navigateurs et comptes sur Internet. Yubico est l'un des créateurs et principaux contributeurs des standards d'authentification ouverts FIDO2, WebAuthn et FIDO Universal 2nd Factor (U2F), et un pionnier de l'authentification sans mot de passe à l'aide des passkeys les plus fiables, avec des clients dans plus de 160 pays.

Les solutions de Yubico permettent des connexions sans mot de passe utilisant la forme la plus sécurisée de la technologie passkey. Les YubiKeys sont prêtes à l'emploi dans des centaines d'applications et de services destinés aux particuliers et aux entreprises, faciles et rapides à utiliser, et offrent une sécurité rigoureuse.

Fidèle à sa mission de sécuriser Internet pour tous, Yubico fait don de YubiKeys à des organisations qui aident les personnes à risque par le biais de l'initiative philanthropique Secure it Forward. Ses sièges sociaux sont situés à Stockholm et à Santa Clara, en Californie. Pour plus d'informations sur Yubico, rendez-vous sur www.yubico.com.