EUROPEAN CENTRAL BANK

EUROSYSTEM

Direction générale Infrastructure de marché et paiements

DIVISION GESTION DE L'INFRASTRUCTURE DE MARCHÉ

BCE – Public

20 septembre 2024

Dispositif d'auto-certification TARGET pour les détenteurs de DCA RTGS et les systèmes exogènes [1]
– Obligations relatives à la sécurité et déclaration d'auto-certification

Introduction

Les principes du CPIM-OICV pour les infrastructures de marchés financiers [2] (IMF) définissent certaines responsabilités qui doivent être assumées par l'opérateur d'un système de paiement. Plus spécifiquement, le principe 17 concerne les questions de sécurité et de fiabilité opérationnelle des infrastructures de marchés financiers telles que les systèmes de paiement d'importance systémique.

Pour gérer les risques opérationnels associés à ses participants, le principe 17 dispose que « *une IMF devrait envisager de définir des obligations opérationnelles minimales pour ses participants. Par exemple, une IMF pourrait définir des obligations opérationnelles et de continuité d'activité pour ses participants en tenant compte du rôle et de l'importance de chaque participant pour le système* ». L'objectif de ces obligations est de remédier aux éventuelles vulnérabilités opérationnelles de l'IMF liées aux participants et, conformément à la stratégie correspondante du CPIM, de réduire le risque de fraude sur les paiements de gros lié à la sécurité des points d'accès [3].

Dans ce contexte, l'Eurosystème, en sa qualité d'opérateur du système TARGET, a défini un ensemble d'obligations visant à remédier aux risques en matière de sécurité de l'information et de cyber-résilience [4] auxquelles, actuellement, l'ensemble des détenteurs de DCA RTGS et des systèmes exogènes

---

1 Le « guide d'information des utilisateurs de TARGET » (ci-après Infoguide) considère comme utilisateurs de TARGET (y compris les utilisateurs de RTGS) les établissements de crédit, les systèmes exogènes et les autres entités effectuant des règlements dans TARGET. L'Infoguide contient également la notion de participants critiques et non critiques, qui peuvent être des établissements de crédit et des systèmes exogènes. Cela suggère que les termes de « participant » et « utilisateur » peuvent être utilisés de manière interchangeable pour les besoins de la présente note.

2 Pour une description complète des normes internationales relatives aux infrastructures des marchés financiers, cf. le site internet de la BRI : https://www.bis.org/cpmi/info_pfmi.htm.

3 Pour une description complète de la stratégie du CPIM en matière de réduction du risque de fraude sur les paiements de gros lié à la sécurité des points d'accès, cf. le site internet de la BRI : https://www.bis.org/cpmi/publ/d178.htm.

4 Selon les « recommandations en matière de cyber-résilience des infrastructures de marchés financiers » du CPIM-OICV, juin 2016, la cyber-résilience correspond à la capacité d'une IMF à anticiper, surmonter, maîtriser une cyber-attaque et à s'en remettre rapidement.

(participants critiques et non critiques) [5] doivent se conformer en tenant compte de leurs systèmes internes en matière de Chaîne des opérations de paiement telle que définie dans le présent document. De plus, les détenteurs de DCA RTGS qui autorisent l'accès à leur compte par des tiers [via l'accès multi-addressee] ou qui enregistrent des détenteurs de BIC adressables sont réputés avoir géré le risque lié à l'autorisation d'un tel accès par des tiers ou avoir enregistré les détenteurs de BIC adressables conformément aux exigences de sécurité qui leur sont imposées.

En outre, l'Eurosystème a défini un ensemble d'obligations visant à faire face au risque en matière de continuité d'activité et qui sont exclusivement applicables aux systèmes internes des participants considérés comme critiques au sens des règles figurant dans le guide d'information des utilisateurs de TARGET. Tous les détenteurs de RTGS DCA et les systèmes exogènes [6] doivent auto-certifier leur niveau de conformité aux obligations définies dans la section suivante.

Obligations relatives à la gestion de la sécurité de l'information et à la gestion de la continuité des activités

Gestion de la sécurité de l'information (applicable à tous les détenteurs de DCA RTGS et systèmes exogènes)

La configuration des systèmes internes (systèmes de back office, de front office, intergiciel (*middleware*), infrastructure permettant la connexion aux réseaux internes et au réseau externe) utilisés par les participants pour soumettre les transactions à TARGET peut varier de manière significative, en raison des différentes architectures qui peuvent être utilisées pour se connecter à TARGET.

Par conséquent, le périmètre des obligations de sécurité peut varier selon l'architecture spécifique mise en œuvre par le participant. En définissant le périmètre, le participant doit identifier les éléments qui font partie de la Chaîne des opérations de paiement. Plus précisément, la Chaîne des opérations de paiement démarre au Point d'entrée – un système utilisé pour la génération de transactions (postes de travail, applications de front office et de back office, intergiciel) – et s'arrête au système responsable de l'envoi du message au prestataire de service de réseau (*Network Service Provider*, NSP).

Il appartient à chaque entreprise d'évaluer si tout ou partie des obligations en matière de sécurité lui est applicable. Il convient également de noter que l'énoncé des obligations fait référence à la terminologie ISO 27000/2018(fr).

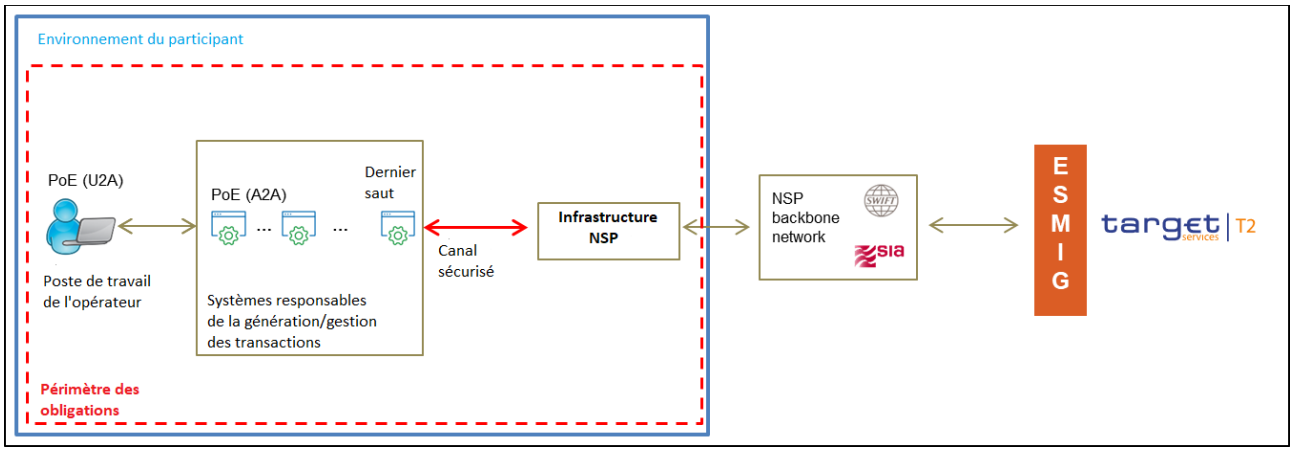
[5] Les banques centrales sont également couvertes par le dispositif d'auto-certification TARGET et doivent par conséquent se conformer aux obligations visant à remédier aux risques en matière de sécurité de l'information et de cyber-résilience définies dans le présent document.

[6] Tous les systèmes exogènes doivent auto-certifier leur niveau de conformité aux obligations définies dans le présent document quels que soient les comptes TARGET adoptés.

Une description des deux architectures possibles ainsi qu'un aperçu de la chaîne des opérations de paiement et des points d'entrée possibles sont fournis ci-après à titre d'illustration.

Participant disposant d'une infrastructure NSP dans son environnement

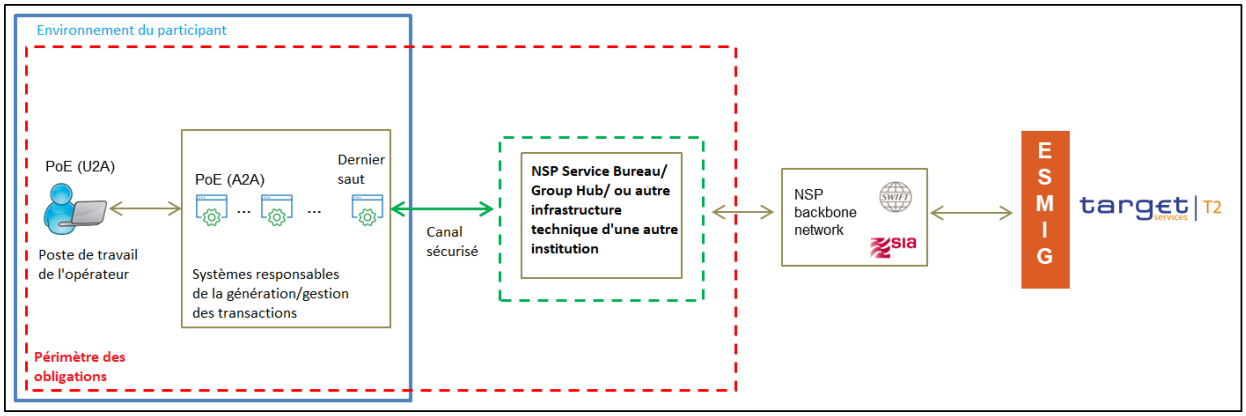
L'infrastructure NSP utilisée pour se connecter à TARGET fait partie de l'environnement du participant, tel qu'il est représenté dans la figure ci-après.



Le périmètre inclut a) le poste de travail utilisé par l'opérateur ; b) les systèmes responsables de la génération ou de la gestion des transactions (intergiciel, application de front office/back office) ; c) le canal sécurisé établi entre l'infrastructure NSP et le dernier saut ; d) l'infrastructure NSP ; e) l'environnement physique du participant.

Participant connecté via un prestataire de services (NSP Service Bureau), via une plateforme de groupe (Group Hub) ou une autre infrastructure technique d'une autre institution

Aucune composante de l'infrastructure NSP n'est hébergée dans l'environnement du participant ; les applications logicielles intermédiaires (*middleware*) et de back office communiquent donc directement avec le *NSP Service Bureau,* le *Group Hub* ou une *autre infrastructure technique d'une autre institution* grâce à un canal sécurisé fourni par eux (notamment application GUI, produit logiciel intermédiaire).



Le périmètre inclut i) le poste de travail utilisé par l'opérateur ; ii) les systèmes responsables de la génération ou de la gestion des transactions (intergiciel, application de front office/back office) ; iii) le canal sécurisé établi entre l'infrastructure NSP hébergée par Service Bureau/Group Hub/une autre infrastructure technique d'une autre institution et le dernier saut ; et iv) l'environnement physique du participant.

Une partie des obligations applicables en matière de sécurité peut être fournie par le NSP Service Bureau ou le Group Hub ou une autre infrastructure technique d'une autre institution, respectivement. À cet égard, les signataires de la déclaration d'auto-certification demeurent responsables du respect des obligations relatives à la sécurité, c'est-à-dire qu'ils doivent s'assurer que la conformité « réalisée pour leur compte » est atteinte. D'une manière générale, les détenteurs de DCA RTGS et les systèmes exogènes doivent veiller à ce que leur déclaration d'auto-certification signée reflète fidèlement la situation de leur entreprise en matière de sécurité, y compris les services qui peuvent être externalisés.

Dans le cas d'un établissement de crédit multi-pays, le Siège social peut héberger et opérer l'infrastructure technique utilisée pour se connecter à TARGET et la partager avec plusieurs succursales locales, au sein d'une plateforme spécifique au groupe.

Dans ce cas, le périmètre indiqué pour l'architecture « *Participant disposant d'une infrastructure NSP dans son environnement* » s'applique au Siège social, mais certaines obligations relatives à la sécurité demeurent applicables aussi aux succursales locales [7]. Par exemple, les contrôles relatifs à la sécurité physique doivent être réalisés par le participant à TARGET hébergeant l'infrastructure technique partagée et par la succursale. Le participant à TARGET hébergeant l'infrastructure technique partagée devra mettre en œuvre des contrôles protégeant le centre de données, tandis qu'une succursale devra s'assurer que les composantes utilisées pour la connexion à l'infrastructure technique partagée sont correctement protégées (poste de travail utilisé par l'opérateur).

S'agissant des détenteurs de DCA RTGS et des systèmes exogènes via *NSP Service Bureau*, les mêmes principes restent valables, ce qui signifie que le participant doit toujours avoir accès à l'information relative

[7] Les mêmes règles et périmètre s'appliquent si l'infrastructure technique utilisée pour se connecter à TARGET est gérée par un Siège social hors de l'Espace économique européen (EEE).

aux contrôles qui entrent et n'entrent pas dans son périmètre (s'assurer dans ce cas que le *NSP Service Bureau* correspondant respecte ces obligations).

Obligation 1.1 : Politique de sécurité de l'information

Les responsables doivent définir une orientation générale claire, conforme aux objectifs opérationnels, et faire la preuve de leur soutien et de leur engagement en faveur de la sécurité de l'information grâce à l'élaboration, à l'approbation et au maintien d'une politique de sécurité de l'information visant à gérer la sécurité de l'information et la cyber-résilience dans l'ensemble de l'entreprise, s'agissant de l'identification, de l'évaluation et du traitement de la sécurité de l'information et des risques liés à la cyber-résilience. Cette politique doit intégrer a minima les sections suivantes : objectifs, périmètre (y compris les domaines comme l'organisation, les ressources humaines, la gestion d'actifs, etc.), les principes régissant les responsabilités et leur partage.

Obligation 1.2 : Organisation interne

Un cadre de sécurité de l'information doit être établi pour assurer la mise en œuvre de la politique de sécurité de l'information au sein de l'entreprise. La direction doit coordonner et examiner l'élaboration du cadre de sécurité de l'information afin de s'assurer de la mise en œuvre de cette politique dans l'ensemble de l'entreprise, y compris l'allocation de ressources suffisantes et l'attribution des responsabilités en matière de sécurité pour remplir cet objectif.

Obligation 1.3 : Intervenants externes

L'introduction et/ou la dépendance à l'égard d'un intervenant externe ou d'intervenants externes ou des produits/services fournis par ces derniers ne doit pas réduire le niveau de sécurité de l'information de l'entreprise et de ses moyens de traitement de l'information. Tout accès par des intervenants externes aux moyens de traitement de l'information de l'entreprise doit être contrôlé. Lorsque l'accès par des intervenants externes ou par des produits/services d'intervenants externes est/sont nécessaire(s), une évaluation des risques doit être effectuée afin d'en déterminer les implications en termes de sécurité ainsi que les obligations en matière de contrôle. Les contrôles doivent être approuvés et définis dans un accord avec chacun des intervenants externes concernés.

Obligation 1.4 : Gestion des actifs

Toutes les ressources en matière d'informations, processus opérationnels et systèmes d'information qui les sous-tendent, comme les systèmes d'exploitation, infrastructures, applications métiers, produits et services standard et applications développées par les utilisateurs, dans le périmètre de la Chaîne des opérations de paiement doivent pouvoir être recensées et avoir un propriétaire désigné. La responsabilité du maintien et de la mise en œuvre des contrôles appropriés sur les procédures opérationnelles et les composants informatiques associés pour sauvegarder les ressources en matière d'informations doit être

dûment attribuée. **NOTE :** La mise en œuvre de contrôles spécifiques peut être déléguée, le cas échéant, par le propriétaire, mais celui-ci demeure responsable de la protection adéquate des actifs.

Obligation 1.5 : Classification des ressources d'informations

Les ressources en matière d'informations doivent être classées selon leur criticité pour la fluidité de réalisation de la prestation de service par le participant. La classification doit indiquer le besoin, les priorités et le degré de protection requis au moment du traitement selon les procédures opérationnelles correspondantes et grâce aux composants informatiques sous-jacents. Un dispositif de classification des ressources en matière d'informations approuvé par la direction doit être utilisé afin de définir un ensemble approprié de contrôles assurant la protection de cette ressource tout au long de sa durée de vie, y compris sa suppression et sa destruction, et de faire comprendre la nécessité de mettre en place des mesures de traitement spécifique.

Obligation 1.6 : Sécurité liée aux ressources humaines

Les responsabilités en matière de sécurité doivent être prises en compte préalablement à l'embauche via des descriptifs de poste et des conditions générales d'emploi appropriés. Tous les candidats à l'emploi, les prestataires et les tiers utilisateurs doivent être sélectionnés de façon appropriée, notamment pour les emplois sensibles. Les salariés, les prestataires et les tiers utilisateurs des moyens de traitement de l'information doivent signer un accord précisant leurs rôles et leurs responsabilités en matière de sécurité. Un niveau approprié de sensibilisation doit être garanti chez les salariés, les prestataires et les tiers utilisateurs, et ils doivent bénéficier d'une formation et d'entraînements aux procédures de sécurité et à une utilisation correcte des moyens de traitement de l'information, afin de réduire au minimum les risques éventuels en termes de sécurité. Une procédure disciplinaire formelle (pour les salariés) relative au traitement des infractions à la sécurité doit être mise en place. Des responsabilités doivent être définies afin de garantir la bonne gestion de la sortie ou du transfert au sein de l'entreprise d'un salarié, prestataire ou tiers utilisateur, ainsi que la restitution de l'ensemble des équipements et la suppression de tous les droits d'accès.

Obligation 1.7 : Sécurité physique et environnementale

Les moyens de traitement des informations critiques ou sensibles doivent être hébergés dans des zones sécurisées, protégés par des périmètres de sécurité bien définis, avec des barrières de sécurité et des contrôles à l'entrée appropriés. Ils doivent être protégés physiquement contre les accès non autorisés, les dommages et les intrusions. L'accès doit être autorisé seulement aux personnes qui entrent dans le champ de l'obligation 1.6. Des procédures et des normes doivent être établies pour protéger les supports physiques contenant des ressources en matière d'informations en cours de transfert.

Les équipements doivent être protégés des menaces physiques et environnementales. La protection des équipements (y compris ceux utilisés hors site) et la protection contre l'enlèvement de la propriété sont nécessaires afin de réduire le risque d'accès non autorisé à l'information et de prévenir toute perte ou

dommage. Des mesures spéciales peuvent être nécessaires afin de se prémunir de menaces physiques et de préserver les dispositifs de soutien tels que l'infrastructure d'alimentation et de câblage électriques.

Obligation 1.8 : Gestion de l'exploitation

Des responsabilités et des procédures doivent être établies pour la gestion et la mise en œuvre des moyens de traitement de l'information afin de couvrir de bout en bout tous les systèmes sous-jacents à la Chaîne des opérations de paiement.

En ce qui concerne les procédures opérationnelles, y compris l'administration technique des systèmes informatiques, une séparation des fonctions doit être mise en œuvre, le cas échéant, afin de réduire le risque de mauvaise utilisation du système par négligence ou de façon délibérée. Lorsque la séparation des fonctions ne peut pas être mise en œuvre pour des raisons objectives explicitées, des contrôles substitutifs doivent être mis en œuvre après une analyse formelle des risques. Des contrôles doivent être établis afin de prévenir et de détecter le chargement d'un code malveillant dans les systèmes de la Chaîne des opérations de paiement. Des contrôles doivent également être mis en place (y compris une sensibilisation des utilisateurs) afin de prévenir, détecter et supprimer tout code malveillant. Les codes mobiles ne doivent être utilisés que s'ils proviennent de sources sûres (signés via les composants COM de Microsoft et des applets Java). La configuration du navigateur (notamment l'utilisation d'extensions et de plug-in) doit faire l'objet d'un contrôle strict.

Des politiques de sauvegarde et de récupération des données doivent être mises en œuvre et elles doivent intégrer un plan permettant un processus de restauration qui est testé à intervalles réguliers au moins une fois par an.

Les systèmes critiques en matière de sécurité des paiements doivent faire l'objet d'un suivi et les événements de sécurité de l'information importants doivent être enregistrés. Les logs d'exploitation doivent être utilisés pour garantir que les problèmes du système d'information sont identifiés. Les logs d'exploitation doivent faire l'objet d'un examen régulier fondé sur la criticité des opérations, à partir d'un échantillon. La surveillance du système doit être mise à profit pour tester l'efficacité des contrôles identifiés comme critiques en matière de sécurité des paiements et pour vérifier la conformité à un modèle de politique d'accès.

L'échange d'informations entre entreprises doit être fondé sur une politique d'échange formalisée et réalisé conformément aux accords d'échange entre les parties concernées, et doit être conforme à tous les textes applicables. Les composantes de logiciels de tiers utilisées pour l'échange d'informations avec TARGET (par exemple, un logiciel mis à disposition par un *Service Bureau* dans le scénario 2 de la section relative au périmètre) doivent l'être dans le cadre d'un accord formel avec la tierce partie.

Obligation 1.9 : Contrôle d'accès

L'accès aux ressources en matière d'informations doit être justifié sur la base des exigences liées au métier (besoin d'en connaître [8]) et selon le cadre établi pour les politiques de l'entreprise (y compris la politique de sécurité de l'information). Des règles claires de contrôle des accès doivent être définies sur la base du principe du moindre privilège [9] pour refléter précisément les besoins des procédures opérationnelles et informatiques correspondantes. Le cas échéant (gestion des sauvegardes, par exemple), le contrôle des accès logiques doit être cohérent avec le contrôle des accès physiques à moins qu'il existe déjà des contrôles substitutifs appropriés (chiffrement, anonymisation des données à caractère personnel).

Des procédures formalisées et explicitées doivent être en place afin de contrôler l'attribution des droits d'accès aux systèmes d'information et aux services liés à l'information dans le périmètre de la Chaîne des opérations de paiement. Les procédures doivent couvrir tous les stades du cycle de vie de l'accès d'un utilisateur, depuis l'inscription initiale des nouveaux utilisateurs jusqu'à la radiation finale des utilisateurs qui n'ont plus besoin d'accès.

Une attention particulière doit être portée, le cas échéant, à l'attribution des droits d'accès d'une criticité telle que leur utilisation peut entraîner des effets négatifs graves sur les opérations du participant (administration système, dérogations aux contrôles du système, accès direct aux données de l'activité).

Des contrôles appropriés doivent être mis en place pour identifier, authentifier et autoriser les utilisateurs en des points spécifiques du réseau de l'entreprise, par exemple pour l'accès local et à distance aux systèmes de la Chaîne des opérations de paiement. Les comptes personnels ne doivent pas être partagés afin de garantir le respect de l'obligation de rendre compte.

S'agissant des mots de passe, des règles doivent être établies et leur application assurée par des contrôles spécifiques visant à garantir que les mots de passe ne sont pas faciles à trouver (règles de complexité et validité pour une durée limitée). Un protocole sûr de récupération et/ou de réinitialisation des mots de passe doit être établi.

Une politique doit être élaborée et mise en œuvre en ce qui concerne l'utilisation des contrôles cryptographiques afin de protéger la confidentialité, l'authenticité et l'intégrité de l'information. Une politique de gestion des clés doit être définie pour faciliter la mise en œuvre des contrôles cryptographiques.

Il doit exister une politique pour la diffusion d'informations confidentielles sur écran ou en version imprimée (politique de l'écran vide, du bureau vide) afin de réduire le risque d'accès non autorisé.

Lorsque le travail s'effectue à distance, les risques associés au travail dans un environnement non protégé doivent être étudiés et des contrôles techniques et organisationnels adaptés mis en œuvre.

---

8 Le principe du besoin d'en connaître se rapporte à l'identification de l'ensemble des informations auxquelles une personne doit avoir accès pour réaliser ses missions.

9 Le principe du moindre privilège consiste à adapter le profil d'accès d'un sujet à un système informatique afin qu'il soit en adéquation avec la fonction professionnelle correspondante.

Obligation 1.10 : Acquisition, développement et maintenance des systèmes d'information

Les obligations relatives à la sécurité doivent être identifiées et décidées avant le développement et/ou la mise en œuvre des systèmes d'information.

Des contrôles adaptés doivent être intégrés aux applications, y compris aux applications développées par les utilisateurs, afin de garantir un traitement correct. Ces contrôles doivent comporter la validation des données d'entrée, du traitement interne et des données de sortie. Des contrôles supplémentaires peuvent être nécessaires pour les systèmes qui traitent, ou ont un impact sur, des informations sensibles, importantes ou critiques. Ces contrôles doivent être déterminés sur la base des obligations relatives à la sécurité et de l'évaluation des risques en fonction des politiques établies (politique de sécurité de l'information, politique de contrôles cryptographiques).

Avant toute acceptation et mise en œuvre de nouveaux systèmes, leurs besoins opérationnels doivent être définis, explicités et testés. S'agissant de la sécurité des réseaux, des contrôles appropriés, incluant la segmentation et une gestion sécurisée, doivent être mis en œuvre en fonction de la criticité des flux de données et du niveau de risque des zones du réseau de l'entreprise. Des contrôles spécifiques doivent exister afin d'éviter que des informations sensibles ne se retrouvent sur les réseaux publics.

L'accès aux fichiers systèmes et au code source des programmes doit être contrôlé et les projets informatiques et les activités d'assistance conduits de manière sécurisée. Il convient de veiller à éviter l'exposition de données sensibles dans les environnements de test. Les environnements de projet et d'assistance doivent faire l'objet d'un contrôle strict. La mise en production des évolutions doit faire l'objet d'un contrôle strict. Il est nécessaire de procéder à une évaluation des risques pesant sur les principales évolutions qui vont être mises en production.

Des activités régulières de mise à l'épreuve de la sécurité des systèmes en production doivent également être menées selon un plan prédéfini s'appuyant sur les conclusions d'une évaluation des risques et ces tests de sécurité doivent intégrer, a minima, des évaluations de la vulnérabilité des systèmes. Toutes les lacunes mises en évidence lors des activités de mise à l'épreuve de la sécurité doivent être évaluées et des plans d'action pour combler les lacunes identifiées doivent être élaborés rapidement et faire l'objet d'un suivi.

Obligation 1.11 : Sécurité de l'information dans les relations avec les fournisseurs [10]

Afin d'assurer la protection des systèmes d'information internes du participant qui sont accessibles aux fournisseurs, les obligations relatives à la sécurité de l'information en vue de réduire les risques associés à l'accès du fournisseur doivent être explicitées et faire l'objet d'un accord formel avec le fournisseur.

[10] Dans le cadre de cet exercice, est considéré comme fournisseur tout tiers (et son personnel) tenu, en vertu d'un contrat (accord) avec l'établissement, de fournir un service et, en vertu du contrat de service, il est accordé à ce tiers (et à son personnel) un accès, à distance ou sur place, à des informations et/ou aux systèmes d'information et/ou aux moyens de traitement de l'information de l'établissement dans le périmètre ou associés au périmètre couvert par l'exercice d'auto-certification TARGET.

Obligation 1.12 : Gestion des incidents et améliorations en matière de sécurité de l'information

Afin de garantir une approche cohérente et efficace de la gestion des incidents relatifs à la sécurité de l'information, y compris la communication relative aux événements et aux faiblesses en matière de sécurité, les rôles, les responsabilités et les procédures, au niveau commercial et technique, doivent être définis et testés afin de garantir une reprise rapide, efficace, ordonnée et sûre après des incidents liés à la sécurité de l'information, notamment des scénarios s'appuyant sur une cause liée à la cyber-sécurité (fraude commise par des agresseurs extérieurs ou par une personne de l'intérieur). Le personnel intervenant dans ces procédures doit être correctement formé.

Obligation 1.13 : Examen de la conformité technique

Les systèmes d'information internes d'un participant (systèmes de back office, possibilités de connexion aux réseaux internes et au réseau externe) doivent être régulièrement évalués au regard de la conformité au cadre établi par l'entreprise pour ses politiques (politique de sécurité de l'information, politique de contrôles cryptographiques).

Obligation 1.14 : Virtualisation

Les machines virtuelles pour invités doivent respecter tous les contrôles de sécurité définis pour les matériels et systèmes physiques (durcissement, enregistrement). Les contrôles relatifs aux hyperviseurs doivent intégrer : durcissement de l'hyperviseur et du système d'exploitation d'hébergement, patches réguliers, séparation stricte des différents environnements (production et développement). La gestion centralisée, l'enregistrement et le suivi, comme la gestion des droits d'accès, en particulier pour les comptes disposant de privilèges élevés, doivent être mis en œuvre sur la base d'une évaluation des risques. Les machines virtuelles pour invités gérées par un même hyperviseur doivent avoir un profil de risque comparable.

Obligation 1.15 : Cloud computing

L'utilisation de solutions de cloud public et/ou hybride dans la Chaîne des opérations de paiement doit être fondée sur une évaluation formelle des risques prenant en compte les contrôles techniques et les clauses contractuelles associés à la solution de cloud retenue.

Si des solutions de cloud hybride sont mises en œuvre, il va de soi que le niveau de criticité du système global correspond au niveau le plus élevé des systèmes connectés. Toutes les composantes sur site des solutions hybrides doivent être séparées des autres systèmes sur site.

Gestion de la continuité des activités (applicable uniquement aux participants critiques)

Les obligations suivantes (2.1 à 2.6) se rapportent à la gestion de la continuité des activités. Chaque détenteur de DCA RTGS ou chaque système exogène classé par l'Eurosystème comme critique pour le

bon fonctionnement du service RTGS doit mettre en place une stratégie de continuité des activités comprenant les éléments suivants.

Obligation 2.1 : Des plans de continuité de l'activité ont été développés et des procédures visant à les maintenir à jour sont en place.

Obligation 2.2 : Un site opérationnel de remplacement doit être disponible.

Obligation 2.3 : Le profil de risque du site de remplacement doit être différent de celui du site principal, afin d'éviter que les deux sites soient affectés par le même événement au même moment. Par exemple, le site de remplacement devra dépendre d'un réseau électrique et d'un circuit informatique central différent de ceux du site principal.

Obligation 2.4 : En cas de perturbation opérationnelle majeure rendant le site principal inaccessible et/ou le personnel considéré comme critique indisponible, le participant critique doit être à même de reprendre le cours normal des opérations depuis le site de remplacement, où il doit être possible de clôturer correctement la journée opérationnelle et d'ouvrir la/les journée(s) opérationnelle(s) suivante(s).

Obligation 2.5 : Des procédures doivent être en place pour garantir que le traitement des transactions reprend depuis le site de remplacement dans un délai raisonnable après la perturbation initiale du service et proportionné à la criticité de l'activité qui avait été perturbée.

Obligation 2.6 : La capacité à gérer les perturbations opérationnelles doit être testée au moins une fois par an et le personnel critique doit être correctement formé. Le délai maximal entre deux tests ne devra pas dépasser un an.

Institution s'auto-certifiant

Les détenteurs de DCA RTGS et les systèmes exogènes peuvent techniquement se connecter à TARGET directement ou via une infrastructure technique partagée. Toutefois, dans ce dernier cas, il est au final de la responsabilité fondamentale des détenteurs de DCA RTGS ou des systèmes exogènes concernés d'évaluer attentivement quelles obligations de sécurité sont applicables à l'infrastructure technique unique et spécifique ainsi qu'à la configuration organisationnelle de son institution.

Chaque détenteur de DCA RTGS et chaque système exogène (c'est-à-dire les participants critiques et non critiques) doit soumettre une déclaration d'auto-certification à la banque centrale avec laquelle il entretient une relation de travail. Si certaines parties des opérations et/ou de l'infrastructure technique utilisée pour l'accès à TARGET sont partagées par différents détenteurs de DCA RTGS ou systèmes exogènes, chaque participant devra soumettre sa propre déclaration d'auto-certification à sa banque centrale.

Un tel concept technique partagé devra également comprendre des configurations où plusieurs participants utilisent, par exemple, la même technique ou application pour créer/traiter les ordres de transfert de liquidité

à envoyer à TARGET. Le recours à ces infrastructures techniques partagées doit également être indiqué dans la déclaration d'auto-certification.

Si un détenteur de DCA RTGS ou un système exogène a externalisé (une partie de) ses opérations auprès d'un tiers (par exemple, un NSP Service Bureau, une plateforme de groupe (Group Hub) ou une autre infrastructure technique d'une autre institution), il doit s'assurer que le tiers respecte les obligations de sécurité établies par l'Eurosystème pour les détenteurs de DCA RTGS et les systèmes exogènes [11].

Si une ou plusieurs obligations de sécurité ne sont pas applicables, les détenteurs de DCA RTGS ou les systèmes exogènes devront l'indiquer dans le tableau de vérification de la conformité ci-dessous. De plus, il conviendra d'expliquer dans la case pertinente incluse dans la déclaration d'auto-certification (intitulée « Vers la conformité ») pourquoi une obligation de sécurité en particulier n'est pas applicable.

En cas de doute, les détenteurs de DCA RTGS ou les systèmes exogènes sont invités à prendre contact avec la banque centrale avec laquelle ils entretiennent une relation contractuelle afin de clarifier le champ de leur déclaration d'auto-certification.

Signataire

La déclaration d'auto-certification devra être signée par un cadre exécutif de niveau C [12] responsable/chargé de la fonction de gestion des risques en matière de sécurité de l'information au sein de l'organisation du détenteur de DCA RTGS ou du système exogène.

Pour les participants critiques, la déclaration d'auto-certification devra également être signée par l'auditeur (externe ou interne) du détenteur critique de DCA RTGS ou du système exogène critique.

[11] Un *Service Bureau* est une organisation d'utilisateurs ou de non-utilisateurs de NSP qui connecte les utilisateurs non affiliés à NSP. Les services offerts par un service bureau comprennent le partage et l'exploitation de composantes de messagerie et/ou de connectivité NSP pour le compte des utilisateurs de NSP. Une *plateforme de groupe* (Group Hub) est une organisation d'utilisateurs ou de non-utilisateurs qui connecte les utilisateurs affiliés au sein du groupe. *Autre institution* fait référence à toute institution qui fournit une infrastructure technique au détenteur de DCA RTGS ou au système exogène.

[12] Un responsable de niveau C est un dirigeant de haut niveau d'une entreprise chargé de prendre des décisions à l'échelle de la société. Le « C » signifie « Chef ». Parmi les responsables de niveau C bien connus figurent notamment le PDG (*chief executive officer,* CEO), le directeur général (*chief operating officer*, COO) et le directeur des systèmes d'information (*chief information officer*, CIO). Si des compétences équivalentes lui ont été attribuées, le signataire pourrait également être un directeur de la gestion des risques (*chief risk officer*, CRO) ou un responsable de la sécurité des systèmes d'information (*chief information security officer*, CISO).

Vérification de la conformité

Pour chacune des obligations spécifiées par l'Eurosystème, les détenteurs de DCA RTGS et les systèmes exogènes doivent indiquer dans la déclaration d'auto-certification leur conformité ou non par rapport au contrôle ou si le contrôle n'est pas applicable.

En cas de non-conformité à une obligation spécifique, une description des risques majeurs [13] devra être incluse dans la case prévue à cet effet dans la déclaration d'auto-certification (intitulée « Vers la conformité »). De plus, un plan d'action visant à rectifier la situation et les dates prévues pour la mise en œuvre de chaque mesure individuelle devra être inclus. Ces informations doivent être évaluées et la mise en œuvre rapide de mesures de réduction des risques suivie par la banque centrale compétente. Enfin, il convient de noter que l'organe de gouvernance de l'Eurosystème en charge de la sécurité et de la fiabilité des opérations de TARGET est informé du résultat de l'exercice d'auto-certification et des progrès réalisés dans la mise en œuvre des mesures de réduction des risques, le cas échéant.

Niveau de conformité

Il est demandé aux détenteurs de DCA RTGS et aux systèmes exogènes d'indiquer s'ils respectent ou non les obligations relatives à la gestion de la sécurité de l'information fixées par l'Eurosystème agissant en sa qualité d'opérateur du système TARGET.

L'opérateur de TARGET applique une approche quantitative pour évaluer la conformité globale des détenteurs de DCA RTGS et des systèmes exogènes (la conformité aux obligations en matière de continuité des activités n'est évaluée que pour les participants critiques). Les critères suivants s'appliquent :

- **Conformité totale :** Les détenteurs de DCA RTGS et les systèmes exogènes qui satisfont à 100 % des obligations (l'ensemble des 15 obligations en matière de sécurité de l'information et l'ensemble des 6 obligations en matière de continuité des activités (uniquement pour les participants critiques)).
- **Non-conformité mineure :** Les détenteurs de DCA RTGS et les systèmes exogènes qui respectent moins de 100 %, mais au moins 66 % des obligations (à savoir 10 obligations en matière de sécurité de l'information et 4 obligations en matière de continuité des activités (uniquement pour les participants critiques)).
- **Non-conformité majeure :** Les détenteurs de DCA RTGS et les systèmes exogènes qui respectent moins de 66 % des obligations (à savoir moins de 10 obligations en matière de sécurité de l'information ou moins de 4 obligations en matière de continuité des activités (uniquement pour les participants critiques)).

[13] Un risque majeur serait, par exemple, l'insuffisance de mesures visant à lutter contre les attaques par déni de service, l'absence d'alimentation électrique sans coupure, etc.

Un détenteur de DCA RTGS ou un système exogène qui démontre qu'une obligation spécifique ne lui est pas applicable sera considéré comme étant en conformité avec l'obligation concernée en ce qui concerne l'évaluation décrite précédemment.

Déclaration pour le compte d'autres détenteurs de DCA RTGS/ systèmes exogènes

Un détenteur de DCA RTGS ou un système exogène peut soumettre une déclaration d'auto-certification à la banque centrale dont il dépend tout en déclarant également l'état de conformité pour le compte d'autres détenteurs de DCA RTGS/systèmes exogènes. Cette « déclaration pour le compte de » est possible si les deux conditions suivantes sont remplies :

(i) Tous les participants appartiennent au même « groupe bancaire » selon la définition de l'orientation TARGET et ils utilisent la même infrastructure technique pour la présentation des paiements

Que le détenteur de DCA RTGS ou le système exogène répertoriés par une déclaration d'auto-certification unique aient ou non noué une relation de travail avec la même banque centrale, les participants utilisent la même infrastructure pour la présentation des paiements dans TARGET.

Si un groupe bancaire a en son sein un participant critique, alors ce participant critique doit être celui qui soumet la déclaration d'auto-certification à la Banque centrale dont il dépend tout en faisant également les déclarations pour le compte des autres participants appartenant au même groupe.

(ii) Tous les participants répertoriés par la déclaration d'auto-certification unique sont en totale conformité avec les obligations applicables

Il se peut que certains détenteurs de DCA RTGS ou systèmes exogènes au sein d'un même groupe bancaire soient classés en tant que participant critique et d'autres en tant que participant non critique. Par conséquent, la déclaration d'auto-certification opère une distinction entre les participants qui doivent respecter les obligations en matière de sécurité de l'information et ceux qui doivent respecter à la fois les obligations relatives à la sécurité de l'information et les obligations relatives à la gestion de la continuité des activités (cases « déclaration pour le compte de » après chaque catégorie d'obligation dans la déclaration).

Si certains participants respectent un contrôle spécifique tandis que pour d'autres le même contrôle n'est pas applicable, les deux cases correspondant à cette obligation (« conforme à l'obligation » et « obligation non applicable ») doivent être cochées dans la déclaration

d'auto-certification. Des informations plus détaillées expliquant pourquoi une obligation particulière n'est pas applicable pour un participant donné doivent être présentées séparément dans la case correspondante de la déclaration.

Si un détenteur de DCA RTGS ou un système exogène n'est pas en conformité avec une obligation/l'une des obligations individuelles, ce participant précis doit soumettre sa propre déclaration d'auto-certification à la Banque centrale dont il dépend. Ce processus (tout participant non conforme au sein d'un « groupe » doit soumettre une déclaration d'auto-certification séparée) doit être respecté même si le contrôle manquant est le même pour tous les participants appartenant à ce « groupe ».

Déclaration d'auto-certification

Coordonnées

Le nom du détenteur de DCA RTGS ou du système exogène qui soumet la déclaration d'auto-certification et les coordonnées d'une personne à contacter pour de plus amples informations devront être indiqués ci-après.

Nom du détenteur de DCA RTGS ou du système exogène	
Adresse	
BIC	
Personne à contacter (nom) (en majuscules)	
Personne à contacter (numéro de téléphone)	
Personne à contacter (courriel)	

Utilisation du NSP Service Bureau ou du Group Hub ou d'une autre infrastructure technique d'une autre institution

Hormis l'établissement d'une connexion technique directe avec TARGET, les participants peuvent se connecter par l'intermédiaire d'un prestataire de service (NSP Service Bureau) ou d'une plateforme de groupe (Group Hub) ou d'une autre infrastructure technique d'une autre institution

Votre entreprise est-elle connectée à TARGET via un prestataire de service (NSP Service Bureau) ?	Oui ☐	Non ☐
Si oui, veuillez indiquer le nom et le BIC de ce prestataire.		

Votre entreprise est-elle connectée à TARGET via une plateforme de groupe (Group Hub) ?	Oui ☐	Non ☐
Si oui, veuillez indiquer le nom et le BIC de cette plateforme de groupe.		

Votre entreprise est-elle connectée à TARGET via une infrastructure technique d'une autre institution (non classée comme NSP Service Bureau/Group Hub) ?	Oui ☐	Non ☐
Si oui, veuillez indiquer le nom et le BIC de l'autre institution (des autres institutions)		

Obligations en matière de gestion de la sécurité de l'information (section applicable à tous les détenteurs de DCA RTGS et systèmes exogènes [14])

	Conforme à l'obligation	Non conforme à l'obligation	Obligation non applicable
Obligation 1.1	☐	☐	☐
Obligation 1.2	☐	☐	☐
Obligation 1.3	☐	☐	☐
Obligation 1.4	☐	☐	☐
Obligation 1.5	☐	☐	☐
Obligation 1.6	☐	☐	☐
Obligation 1.7	☐	☐	☐
Obligation 1.8	☐	☐	☐
Obligation 1.9	☐	☐	☐
Obligation 1.10	☐	☐	☐
Obligation 1.11	☐	☐	☐
Obligation 1.12	☐	☐	☐
Obligation 1.13	☐	☐	☐
Obligation 1.14	☐	☐	☐
Obligation 1.15	☐	☐	☐
Quelle norme est appliquée dans votre entreprise pour la gestion de la sécurité de l'information (ISO 27001, COSO, certification			

[14] C'est-à-dire que tous les **détenteurs de DCA RTGS et systèmes exogènes** doivent satisfaire aux exigences du présent tableau qui recense les différentes obligations en matière de gestion de la sécurité de l'information (cases à cocher) et répondre aux questions posées ci-dessous dans la présente section.

COBIT de l'ISACA, NIST) ?	
Votre entreprise a-t-elle recours pour les services essentiels à la Chaîne des opérations de paiement à un fournisseur de prestation de Cloud (clouds publics et hybrides ou solutions de stockage externe de documents) ?	

Déclaration au titre des obligations relatives à la gestion de la sécurité de l'information pour le compte d'autres détenteurs de DCA RTGS ou systèmes exogènes (le cas échéant)	
BIC du participant	Banque centrale du participant

Obligations relatives à la gestion de la continuité des activités (section applicable uniquement aux participants critiques)

	Conforme à l'obligation	**Non conforme à l'obligation**	**Obligation non applicable**
Obligation 2.1	☐	☐	☐
Obligation 2.2	☐	☐	☐
Obligation 2.3	☐	☐	☐
Obligation 2.4	☐	☐	☐
Obligation 2.5	☐	☐	☐
Obligation 2.6	☐	☐	☐

Déclaration au titre des obligations relatives à la gestion de la continuité des activités pour le compte d'autres détenteurs de DCA RTGS ou systèmes exogènes (le cas échéant)	
BIC du participant	Banque centrale du participant

Vers la conformité

La section suivante doit être complétée si un participant a) a identifié un cas de non-conformité à l'une des obligations en matière de sécurité ; ou b) a qualifié une obligation de « non applicable ».

Pour chaque obligation qualifiée de « non applicable » dans le tableau ci-après, veuillez expliquer brièvement pourquoi elle n'est pas applicable. Commentaires :
Quels sont les risques résultant de la non-conformité aux obligations 1.1 à 1.15 et 2.1 à 2.6 (veuillez répondre séparément pour chaque obligation pour laquelle il est indiqué « non conforme ») ? Commentaires :
Quelles mesures seront prises pour atteindre une pleine conformité avec toutes les obligations (veuillez répondre séparément pour chaque obligation pour laquelle il est indiqué « non conforme ») ? Commentaires :

Quand la pleine conformité sera-t-elle atteinte ?

Commentaires :

Certification

Les signataires confirment qu'ils ont lu et compris les obligations définies dans cette déclaration d'auto-certification. La déclaration sera renouvelée chaque année. Dans l'intervalle, toute non-conformité constatée doit être déclarée sans tarder à la banque centrale responsable.

Les signataires certifient que les informations contenues dans la déclaration donnent une idée précise et exacte de la situation actuelle. Ils certifient également que la déclaration a été préparée sous leur direction et supervision, et que les informations fournies ont été correctement rassemblées et évaluées par du personnel qualifié. Les informations soumises sont, à la connaissance des signataires, exactes, précises et complètes. Les signataires sont conscients que soumettre ces informations est une obligation matérielle et que soumettre des informations inexactes, imprécises ou fallacieuses constitue un manquement à l'article 25 (2) (c) de la Partie I, Annexe I de l'orientation relative à TARGET, qui est un motif de résiliation de la participation d'une institution à TARGET.

Enfin, les signataires confirment que leur entreprise dispose d'un mécanisme garantissant qu'ils continueront de se conformer aux obligations au cours de l'année à venir. Si la pleine conformité n'est pas encore atteinte, les signataires confirment que les mesures appropriées seront prises afin d'y parvenir au plus tard à la fin de l'année civile suivante.

Dans le cas où un participant soumet la déclaration et le rapport pour le compte d'autres détenteurs de DCA RTGS ou systèmes exogènes, les signataires confirment les aspects indiqués précédemment pour tous les participants mentionnés dans la déclaration. Les signataires sont conscients que soumettre ces informations est une obligation matérielle du participant pour le compte duquel ils signent et que soumettre des informations inexactes, imprécises ou fallacieuses constitue un manquement à l'article 25 (2) (c) de la Partie I, Annexe I de l'orientation relative à TARGET, qui est un motif de résiliation de la participation d'une institution à TARGET.

Signature

Nom du responsable (en majuscules)	
Titre/fonction (responsable de niveau C)	
Date	
Signature	

Signature de l'auditeur – à remplir uniquement par les participants critiques

Nom de l'auditeur (en majuscules)	
Titre (indiquer s'il s'agit d'un auditeur interne ou externe)	
Date	
Signature	

Cette déclaration d'auto-certification doit être renvoyée à :

Nom de la banque centrale	
Adresse	
Personne à contacter	