Conseil de
Union européenne

Bruxelles, le 6 mars 2015
(OR. en)

6488/15

CSCI 9
CSC 45

NOTE POINT "I/A"

Origine:	le Comité de sécurité du Conseil
Destinataire:	Coreper/Conseil
Objet:	Politique de sécurité en matière d'assurance de l'information concernant l'interconnexion

1. La décision du Conseil concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE[1] dispose ce qui suit: "Le cas échéant, le Conseil approuve, sur recommandation du Comité de sécurité, les politiques de sécurité énonçant les mesures destinées à mettre en œuvre la présente décision" (voir article 6, paragraphe 1).

2. Le Comité de sécurité du Conseil a décidé de recommander l'approbation d'une politique établissant des normes pour l'interconnexion de SIC traitant des informations classifiées de l'UE (ICUE), du point de vue de leur confidentialité, de leur intégrité, de leur disponibilité et, selon les cas, de leur authenticité et de leur non-répudiation.

3. Sous réserve de confirmation par le Coreper, le Conseil est invité à approuver la politique de sécurité ci-jointe.

[1] Décision 2013/488/UE du Conseil (JO L 274 du 15.10.2013, p. 1).

(Page laissée vide à dessein)

Politique de sécurité en matière d'assurance de l'information concernant l'interconnexion

IASP 3

SOMMAIRE

1. OBJET ET CHAMP D'APPLICATION

1. La présente politique, approuvée par le Conseil conformément à l'article 6, paragraphe 1, des règles de sécurité du Conseil (ci-après dénommées "RSC"), établit des normes applicables à la protection des informations classifiées de l'UE (ICUE). Elle constitue un engagement en vue de contribuer à atteindre un niveau équivalent de mise en œuvre des RSC.

2. La présente politique a pour objet d'établir les règles et restrictions applicables à l'interconnexion entre un SIC traitant des ICUE et un autre système d'information et de communication (SIC). Elle définit aussi un modèle (voir annexe I) utilisé comme langage commun pour décrire une interconnexion. Le présent document ne porte que sur les risques supplémentaires qu'une interconnexion fait peser sur un SIC.

3. Le Conseil et le Secrétariat général du Conseil (SGC) appliqueront la présente politique en matière de sécurité aux fins de la protection des ICUE, dans leurs bureaux et leurs systèmes d'information et de communication (SIC).

4. Les États membres agiront conformément à leurs dispositions législatives et réglementaires nationales pour faire en sorte que le traitement des ICUE par les structures nationales, et notamment les SIC nationaux, soit effectué dans le respect des normes établies dans les politiques de sécurité.

5. Les agences et les organes de l'Union créés en vertu du titre V, chapitre 2, du TUE, ainsi qu'Europol et Eurojust, devraient utiliser cette politique de sécurité comme référence pour la mise en œuvre des règles de sécurité au sein de leurs propres structures.

6. On entend par "interconnexion de systèmes" la connexion directe[2] d'au moins deux systèmes informatiques permettant à ceux-ci d'échanger des données[3] et d'autres ressources en matière d'information (communication, par exemple) de façon unidirectionnelle ou multi-directionnelle. La raison première de l'interconnexion de systèmes est la fourniture ou l'utilisation des types de services suivants:

   (a) un service d'échange d'informations,

   (b) un service de fourniture d'une infrastructure de communication technique (l'intention n'étant pas d'échanger de l'information).

7. La présente politique ne porte pas sur l'échange d'informations à l'aide de supports amovibles.

8. La présente politique s'applique à un SIC traitant des ICUE qui est interconnecté avec un autre système d'information (SI), lequel ne traite pas nécessairement des ICUE.

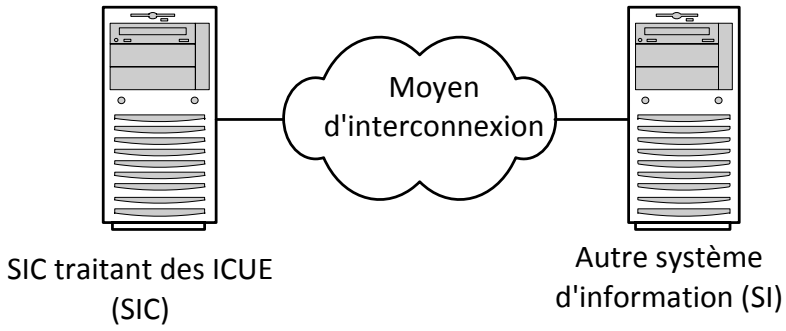

Figure 1Modèle d'interconnexion générique

[2] Par opposition à connexion en cascade.

[3] Aux fins du présent document, on entend par "données" la représentation spécifique d'informations (par exemple une série de bytes); ces données doivent avoir un format défini qui précise la manière dont l'information est encodée.

9. Une connexion entre deux systèmes informatiques doit être considérée comme une interconnexion lorsque ces systèmes présentent des différences en ce qui concerne au moins l'une des caractéristiques suivantes:

(a) le niveau maximal de classification des ICUE,

(b) les objectifs de sécurité[4],

(c) le mode d'exploitation de sécurité,

(d) l'autorité d'homologation de sécurité (AHS) compétente,

(e) les politiques applicables en matière de sécurité (par exemple un système de l'UE et un système d'un État membre),

(f) les autorités d'exploitation du système (AES) compétentes (par exemple le SGC, un organisme décentralisé de l'UE),

(g) les obligations légales,

(h) tout autre paramètre pertinent en matière de sécurité (besoin d'en connaître ou communauté d'intérêt, restrictions, protocoles spécifiques, équipements anciens, niveau de protection physique, type de réseau-support, propriété de l'information diffusée).

Toute modification du SIC introduisant de nouveaux composants[5] et ne répondant à aucun des critères définis ci-dessus n'est en principe pas considérée comme une interconnexion.

Dans n'importe quel autre cas, il appartient à la ou aux AHS responsables de décider si une connexion ou une liaison interne constitue une interconnexion.

---

[4] Tels qu'ils sont définis dans l'énoncé des impératifs de sécurité propres à un système.

[5] Par exemple un nouveau poste de travail, de nouveaux équipements de réseau, etc.

10. Indépendamment de la direction prévue du flux d'information, l'interconnexion peut ouvrir un canal de communication bidirectionnel[6] entre les deux SIC et pourrait permettre l'accès à de nombreux services et informations qui, sans qu'on le veuille, sortent du cadre des conditions d'activités.

11. L'interconnexion peut donc modifier l'évaluation des risques pesant sur le SIC de la manière suivante:

    (a) les sources de menace pour le SI peuvent être transférées vers le SIC,

    (b) les vulnérabilités du SI peuvent augmenter la probabilité de certains scénarios de risques et/ou leur impact sur le SIC,

    (c) les vulnérabilités du SI et l'interconnexion proprement dite peuvent créer un certain nombre de nouveaux scénarios de risques pour le SIC,

    (d) l'interconnexion établit une dépendance au niveau de l'activité et au niveau technique et peut donc faire courir des risques en termes de disponibilité,

    (e) l'exploitation des fonctionnalités et des vulnérabilités des deux systèmes interconnectés peut produire une synergie et de nouveaux vecteurs d'attaque,

    (f) les composants utilisés pour établir l'interconnexion et/ou atténuer les risques créés par l'interconnexion peuvent eux-mêmes être la cible d'une attaque et ils peuvent introduire de nouvelles vulnérabilités.

12. Le service de protection en bordure (BPS) est un service qui atténue les risques de sécurité introduits par l'interconnexion. Les contrôles qui assurent le service de protection en bordure sont qualifiés d'éléments de protection du réseau (par exemple procédure de sauvegarde, antivirus, contrôle d'accès physique). Les éléments spéciaux qui assurent la médiation entre les flux d'information et/ou fournissent les services de sécurité au point d'interconnexion sont qualifiés de dispositifs de protection du réseau (par exemple, pare-feu, régulateur de flux unidirectionnel).

---

[6] Par exemple lorsque l'interconnexion repose sur le protocole TCP.

2. POLITIQUE

13. Un SIC doit considérer tout système d'information interconnecté comme n'étant pas fiable et toutes les hypothèses relatives au SI devraient être soigneusement évaluées dans le cadre du processus de gestion des risques. Le SIC doit mettre en œuvre les contrôles appropriés (par exemple accords de niveau de service (ANS), services de protection en bordure) pour vérifier que les hypothèses relatives au SI sont correctes.

14. Une condition d'activité valide doit guider la décision d'interconnexion du SIC.

15. Le SIC doit empêcher les échanges d'informations et accès aux services qui ne sont pas expressément définis dans le cadre des conditions d'activité. Il convient d'empêcher que des informations ou services d'un certain niveau de classification passent sur un système ayant un niveau de classification moindre.

16. L'interconnexion entre un SIC et un SI ayant un niveau de classification moindre ou sans classification n'est pas autorisée sauf si des services de protection en bordure homologués sont installés entre le SIC et le SI, par exemple en utilisant un régulateur de flux unidirectionnel homologué. Le service de protection en bordure retenu doit atténuer les risques répertoriés pour les amener à un niveau acceptable.

17. L'interconnexion doit être soumise à un processus d'homologation et être approuvée par l'AHS compétente.

18. La procédure de gestion des risques pesant sur le SIC doit être répétée pour toute nouvelle interconnexion. Au minimum, le processus doit prendre en compte les aspects décrits à l'annexe II.

19. Lorsqu'une interconnexion crée des risques nouveaux de niveau élevé pour le SIC, il se peut que ce dernier doive faire l'objet d'une nouvelle homologation. Cette nouvelle homologation est nécessaire lorsque le SIC est interconnecté avec un SI non homologué.

20. Un SIC homologué pour traiter des informations TRÈS SECRET UE/EU TOP SECRET ne doit pas être interconnecté avec un réseau non protégé ou public (ni directement ni indirectement - via un autre SI).

21. Lorsque le SI n'offre qu'une infrastructure de communication aux fins du transport de données et que les données sont chiffrées au moyen d'un produit cryptographique agréé conformément à l'article 10 des règles de sécurité du Conseil, une telle connexion n'est pas considérée comme une interconnexion.

22. S'il est prévu de créer de nouvelles interconnexions avec un SI, lui-même déjà interconnecté à un SIC, l'autorité d'homologation de sécurité (AHS) compétente pour le SIC doit en être informée. Cette obligation d'information vaut aussi pour l'AHS compétente pour le SI si le SIC est à nouveau interconnecté.

23. Seuls les protocoles, le service de réseau et les flux d'informations ou de données nécessaires afin de mener à bien la mission opérationnelle peuvent être installés, configurés et utilisés pour l'interconnexion (principe du minimalisme).

24. Les utilisateurs et les processus utilisant l'interconnexion ou en faisant partie ne peuvent se voir accorder que les privilèges et les autorisations requis pour mener à bien leurs tâches et missions (principe du moindre privilège).

25. Un SIC interconnecté doit mettre en œuvre des mesures pour bloquer toute activité et tout flux d'informations qui ne constituent pas un élément légitime du fonctionnement de l'interconnexion (principe d'autoprotection).

26. Des mesures de protection doivent être appliquées sur divers composants de l'architecture d'interconnexion[7] afin d'éviter qu'il n'existe qu'une seule ligne de défense (principe de la défense en profondeur).

27. Une interconnexion doit être vérifiée[8] par l'AHS responsable au moment de la mise en œuvre initiale et à intervalles réguliers par la suite. Il convient que l'AHS puisse déjà intervenir durant les phases de planification et de conception et pendant l'évaluation de l'interconnexion au niveau des risques.

---

7 L'architecture, en dehors de l'interconnexion proprement dite, comprend aussi le SIC et le SI.

8 Il s'agit de vérifier si la mise en œuvre tient compte de la conception et des décisions concernant l'application de contrôles dans le processus de traitement du risque.

28. Le développement de l'interconnexion fait partie soit du projet de développement du SIC soit d'un projet séparé lorsqu'il s'ajoute à un SIC déjà déployé. La méthode de gestion du projet, la gestion des services et le cycle de vie de l'interconnexion ne relèvent pas du champ d'application du présent document. Cependant, le cycle de vie de l'interconnexion comprend les phases du cycle de vie de sécurité décrites dans le document IASP-L[9]:

(a) justification de sécurité de l'interconnexion - la justification de sécurité a pour objet de recenser toutes les exigences de sécurité nécessaires pour l'interconnexion ainsi que les exigences de sécurité nécessaires pour le SI,

(b) ingénierie de sécurité de l'interconnexion - les exigences de sécurité de l'activité sont traduites en principes de sécurité et en contrôles, choisis et mis en œuvre par la combinaison appropriée de personnes, de procédures et de technologies. À l'issue de cette phase, l'interconnexion devrait être opérationnelle dans l'environnement de production et homologuée au niveau requis,

(c) maintien de la sécurité de l'interconnexion - après qu'elle a été établie, l'interconnexion doit être activement entretenue et contrôlée pour s'assurer qu'elle fonctionne correctement et de manière sécurisée,

(d) suppression sécurisée de l'interconnexion - lorsque le besoin d'interconnexion n'existe plus ou si l'un des SIC interconnectés entre en phase de démantèlement, l'interconnexion est mise hors service, au moyen des procédures autorisées.

[9] IASP-L Politique de sécurité en matière d'assurance de l'information concernant la sécurité durant tout le cycle de vie d'un SIC (doc. 14968/12).

DÉFINITIONS

Homologation	Procédure conduisant à une déclaration formelle de l'autorité d'homologation de sécurité (AHS) indiquant qu'un système est agréé pour fonctionner à un niveau de classification déterminé, selon un mode d'exploitation de sécurité spécifique dans son environnement opérationnel et à un niveau de risque acceptable, pour autant qu'un ensemble approuvé de mesures de sécurité ait été mis en place sur le plan technique et physique, ainsi qu'au niveau de l'organisation et des procédures.
Authenticité	Garantie que l'information est véridique et émane de sources dignes de foi.
Disponibilité	Propriété consistant à être accessible et utilisable, à la demande d'une entité autorisée.
Système de communication et d'information	Système permettant le traitement d'informations sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information. Voir l'article 10, paragraphe 2, des RSC.
SIC	Système d'information et de communication traitant des ICUE.
Confidentialité	Propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées, ni accessibles à des processus non autorisés.
Information classifiée de l'UE (ICUE)	Information ou matériel identifié comme tel par une classification de sécurité de l'UE, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres. Voir l'article 2, paragraphe 1, des RSC.
Intégrité	Propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments.
Non-répudiation	Possibilité de prouver qu'une action ou un événement a eu lieu, de sorte que cette action ou cet évènement ne puisse être remis en cause par la suite.
Risque	Possibilité qu'une menace donnée se concrétise en tirant parti des vulnérabilités internes et externes d'une organisation ou d'un des systèmes qu'elle utilise, et cause ainsi un préjudice à l'organisation ou à ses ressources matérielles ou immatérielles. Le risque se mesure en tenant compte à la fois de la probabilité de voir se concrétiser des menaces et de l'impact de celles-ci.

MODÈLE D'INTERCONNEXION

1. La présente annexe définit un modèle possible pour la description d'une interconnexion. Le modèle a pour objectif de mettre au jour les risques que l'interconnexion fait peser sur un SIC.

2. Une interconnexion peut être décrite par deux paramètres, les "conditions de sécurité" et le "rôle" (voir figure 2), les "conditions de sécurité" représentant l'ensemble d'attributs tels que les différences de niveau d'homologation, la propriété, les modes de fonctionnement, etc., et le "rôle" décrivant le rôle du SIC dans l'interconnexion, défini par:

   (a) la "direction du flux" (la direction du flux d'information) du point du vue du SIC et

   (b) la "fourniture d'un service" - le rôle du SIC dans la fourniture ou l'utilisation du service offert par l'interconnexion.

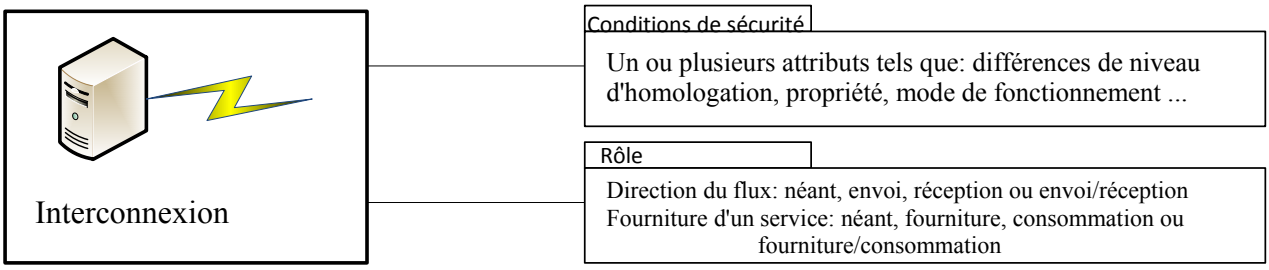

Figure 2 Les paramètres décrivant une interconnexion

3. Le modèle d'interconnexion requis au niveau (logique) de l'activité devrait être respecté lors de la mise en œuvre technique. En d'autres termes, la mise en œuvre technique ne devrait pas proposer plus de directions de flux ou de services que ce qui est nécessaire. Tout écart par rapport aux conditions d'activités au niveau technique devrait être traité comme un risque et atténué comme il convient par des services de protection en bordure.

4. Les valeurs de l'attribut "rôle" sont expliquées ci-dessous dans le tableau 1.

Attribut	**Valeur**	**Description**
Direction du flux	néant	L'activité ne nécessite aucun échange d'informations entre le SIC et le SI. Il pourrait cependant y avoir une interconnexion au niveau de l'infrastructure (susceptible de provoquer un flux d'informations non souhaité).
	réception	Le SIC reçoit certaines informations du SI.
	envoi	Le SIC envoie certaines informations au SI[10].
	envoi/réception	Le SIC envoie et reçoit les informations.
Fourniture de services	néant	Étant donné qu'il n'y a ni service utilisé ni service fourni, il n'y a pas de raison d'interconnecter deux systèmes du point de vue de l'activité. Cette situation n'est pas autorisée et l'interconnexion ne doit pas être établie.
	utilisation (utilisateur d'un service)	Le SIC utilise un service fourni par le SI. Dans la plupart des configurations de mise en œuvre, le SIC agira comme client du SI (mais différents modèles sont possibles).
	fourniture (prestataire de services)	Le SIC offre un service au SI. L'objectif du service peut être l'échange d'informations ou la fourniture d'une infrastructure (par exemple une infrastructure de communication). Dans le cas d'un échange d'informations, le SIC fait généralement office de serveur (mais différents modèles sont possibles).
	fourniture/consommation	Le SIC doit fournir des services et, dans le même temps, attend certains services de la part du SI.

Tableau 1 Les valeurs possibles de l'attribut "rôle" dans l'interconnexion

[10] Il convient de noter qu'une confirmation de réception (si demandée) est considérée comme un flux d'informations du récepteur à l'expéditeur.

5. Les contraintes et exigences en matière de mesures de sécurité supplémentaires pour les "rôles" et les "conditions de sécurité" seront décrites dans les lignes directrices en matière de sécurité dans le domaine de l'assurance de l'information.

6. Le fait que deux interconnexions différentes soient décrites par les mêmes "rôle" et "conditions de sécurité" les rend similaires du point de vue de la sécurité mais ne les rend pas pour autant identiques. En conséquence, en dehors du contrôle de la conformité avec les lignes directrices, il convient, dans chaque cas, de décider si une interconnexion est ou n'est pas "suffisamment sécurisée" en fonction du résultat d'un processus de gestion des risques.

Annexe II

ASPECTS À PRENDRE EN CONSIDÉRATION POUR LA GESTION DES RISQUES

1. L'impact de l'interconnexion sur la gestion du risque (pesant sur le SIC) dépend en très grande partie de la situation effective (conditions d'activités, mise en œuvre technique). La présente annexe définit une liste générique de questions devant être prises en compte selon les besoins. Les détails liés aux modèles et configurations de mise en œuvre spécifiques seront établis dans les lignes directrices.

2. La portée du processus de gestion des risques sera très probablement modifiée lorsqu'une interconnexion sera établie; plus particulièrement, les éléments ci-après doivent faire l'objet d'une analyse:

   (a) éléments d'information - de nouveaux éléments peuvent entrer dans le champ d'application du processus de gestion des risques,

   (b) processus opérationnels - un ou plusieurs processus opérationnels sont très probablement modifiés pour justifier l'interconnexion,

   (c) obligations contractuelles - l'interconnexion peut faire intervenir une obligation contractuelle incombant au propriétaire du SIC,

   (d) interfaces - l'interconnexion constitue une nouvelle interface.

3. Le processus d'identification de la menace devrait prendre en compte les événements non souhaités suivants:

   (a) des utilisateurs ou programmes non autorisés fonctionnant sur le SI tentent d'accéder à des services du SIC,

   (b) des utilisateurs ou programmes non autorisés fonctionnant sur le SIC tentent d'accéder à des services du SI,

   (c) des informations non communicables au SI sont transférées (par erreur ou délibérément) au SI,

(d) des informations non communicables au SIC sont transférées depuis le SI,

(e) le SI devient indisponible (y-a-t-il un impact sur le SIC?),

(f) le service offert par le SI demande beaucoup de temps ou de ressources ou n'est jamais fourni complètement,

(g) les informations reçues du SI sont altérées à des fins malveillantes (délibérément ou accidentellement) pour exploiter des vulnérabilités du SIC,

(h) les informations transmises du SIC au SI sont altérées à des fins malveillantes pour exploiter des vulnérabilités du SI,

(i) le fait qu'une transaction (par exemple un échange d'informations) a eu lieu a été porté à la connaissance des utilisateurs du SI,

(j) les transactions (par exemple l'envoi ou la réception) sont refusées par le SI,

(k) le SIC ne peut pas recevoir ou traiter des informations envoyées par le SI (par exemple un service n'est pas disponible),

(l) la quantité d'informations ou le nombre de requêtes adressés par le SI au SIC sont plus importants que prévu et provoquent une saturation,

(m) le service de protection en bordure et d'autres composants utilisés pour établir l'interconnexion présentent des vulnérabilités exploitables permettant une attaque contre le SIC,

(n) les informations relatives aux technologies, à l'infrastructure et aux vulnérabilités de l'architecture du SIC ont été portées à la connaissance des utilisateurs du SI,

(o) le SI est attaqué avec succès et devient une source d'attaque contre le SIC,

(p) les protocoles approuvés pour l'échange d'informations ne sont pas suivis.

4. Il est peu probable qu'un service de protection en bordure fournisse à lui seul une protection suffisante contre toutes les attaques possibles, ou permette de les détecter toutes, et il y a donc lieu de prendre en compte les contrôles suivants dans le traitement du risque:

   (a) il peut être nécessaire de revoir entièrement l'architecture du SIC (par exemple pour permettre une défense en profondeur adéquate),

   (b) il pourrait être nécessaire de sensibiliser et de former les utilisateurs et administrateurs du SIC pour les informer des nouveaux risques et leur expliquer les responsabilités qui leur incombent du fait de l'interconnexion.