Annexe 4

Catalogue de critères pour la reconnaissance de plateformes alternatives

Table des matières

1 Objectif et contenu

Le présent catalogue de critères énumère les exigences posées aux plateformes de procédures de transmission alternatives, dans la procédure de reconnaissance de celles-ci.

2 Notions

2.1 Fournisseur

Le fournisseur d'une plateforme est l'organisation qui met celle-ci à disposition de tiers (utilisateurs) en vue d'une utilisation professionnelle. Cette organisation peut être une entreprise privée ou une autorité.

2.2 Plateforme

Une plateforme est composée d'une application logicielle ainsi que d'autres composants de logiciel, de matériel et de réseau nécessaires à la bonne marche et à l'accessibilité de l'application logicielle.

3 Exigences relatives à la sécurité des informations

3.1 Exigences de base pour les entreprises privées

La sécurité des informations doit être garantie par l'une des méthodes suivantes:

a) Par l'établissement, l'implémentation, le fonctionnement, la surveillance, le réexamen, la mise à jour et l'amélioration d'un système de management de la sécurité de l'information (SMSI) conformément à la norme ISO/CEI 27001:2005 (Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences). Le champ d'application du SMSI doit comprendre toutes les unités d'organisation du fournisseur responsables de la procédure de transmission alternative sur le plan juridique, administratif et de l'exploitation. Une limitation du champ d'application à la seule exploitation technique de la plateforme par un fournisseur de services informatiques interne ou externe n'est pas admise.

L'efficacité et l'adéquation d'un SMSI doit être prouvée par la présentation d'un certificat émanant d'un organisme de certification qui atteste la certification du SMSI selon la norme ISO/CEI 27001:2005. L'organisme de certification doit être accrédité par le Service d'accréditation suisse (SAS) pour procéder à des audits selon la norme ISO/CEI 27001:2005.

Pour conserver cette reconnaissance, chaque rapport d'audit annuel de surveillance ou de renouvellement doit être remis spontanément à l'OFJ. En cas d'annulation de la certification selon la norme ISO/CEI 27001:2005 par l'organisme de certification, le DFJP retire la reconnaissance à l'entreprise privée pour autant que la preuve de la sécurité de l'information ne puisse pas être apportée par la méthode b).

b) Par la certification du SMSI sur la base d'un standard équivalent à la norme ISO/CEI 27001:2005. Dans un tel cas, les conditions suivantes doivent être remplies:

- **Les exigences mentionnées sous lettre a) relatives au champ d'application sont valables sans changement.**

- **L'efficacité et l'adéquation du SMSI conformément au standard équivalent doivent être prouvées par la présentation d'un certificat délivré par un organisme de certification. L'organisme de certification doit être accrédité par le SAS, l'autorité de surveillance des marchés financiers (FINMA) ou la Banque nationale suisse (BNS).**
- **L'équivalence de ce standard par rapport à la norme ISO/CEI 27001:2005 doit être attestée par un organisme de certification accrédité par le SAS pour procéder à des audits conformes à la norme ISO/CEI 27001:2005 et qui est simultanément accrédité par la FINMA et la BNS pour procéder à des audits selon un standard équivalent.**
- **L'organisme de certification qui vérifie l'équivalence est désigné par l'OFJ sur proposition du fournisseur. L'OFJ ne rejette la proposition que pour des raisons majeures.**
- **Les exigences mentionnées sous lettre a) relatives à la conservation de la reconnaissance sont valables sans changement; le standard ISO/CEI 27001:2005 doit cependant être remplacé par le standard équivalent.**

3.2 Exigences de base pour les autorités

Lorsque le fournisseur de la plateforme est une autorité, il peut être renoncé à une certification formelle, mais non à un SMSI conforme à la norme ISO/CEI 27001:2005. Dans un tel cas, l'efficacité et l'adéquation du SMSI doivent être prouvées par la production d'un rapport d'audit formel interne conformément à la clause 6 de la norme ISO/CEI 27001:2005. Le rapport d'audit ne doit contenir aucune constatation conduisant à une exclusion d'une certification. S'agissant des principes d'audit, de la réalisation de l'audit ainsi que des compétences et de l'expérience de l'auditeur, les lignes directrices ISO 19011:2011 (Lignes directrices pour l'audit des systèmes de management) et ISO 27007:2011 (Technologie de l'information – Techniques de sécurité – Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information) doivent être observées. L'audit doit être renouvelé au moins une fois par année. Chaque rapport d'audit doit être remis spontanément à l'OFJ. Si les rapports d'audit parviennent à la conclusion que le SMSI contient des divergences critiques conformément à la norme ISO/CEI 27001:2005 et si celles-ci ne sont pas corrigées dans le délai fixé par l'auditeur interne, le DFJP retire la reconnaissance de l'autorité.

Lorsque l'autorité utilise un standard équivalent à la norme ISO 27001:2005, les règles prévue au chiffre 3.1. b) sont applicables, à l'exception du fait que la certification formelle n'est pas prescrite pour les autorités. L'efficacité et l'adéquation du SMSI doit être prouvée, comme décrit ci-dessus, par la production d'un rapport d'audit formel interne du SMSI conformément au standard équivalent à la norme ISO/CEI 27001:2005.

3.3 Exigences supplémentaires pour les entreprises privées et les autorités

Les exigences décrites aux lettres a), b) et c) suivantes constituent des compléments aux critères d'audit selon la norme ISO/CEI 27001:2005 ou au standard équivalent conformément au chiffre 3.1.b). Il n'est pas autorisé d'exclure des mesures pour respecter ces critères d'audit lors de l'analyse de risque dans le cadre de l'établissement du SMSI. Cela doit être pris en compte de manière correspondante lors de la formulation des critères d'acceptation du risque.

a) Gestion de l'exploitation et de la communication

- **Les plateformes de développement, de test et de production doivent être séparées les unes des autres.**

- **Le réseau doit être segmenté. Les serveurs pour l'exploitation des plateformes doivent être répartis sur les segments de réseau conformément à leur besoin de protection.**
- **Les informations électroniques ne peuvent en principe être transmises et stockées que sous forme cryptée. Un chiffrement de bout en bout n'est pas nécessaire. Pour l'acheminement d'informations électroniques, il suffit que le canal de communication soit sécurisé. Si la sauvegarde d'informations électroniques sous forme cryptée n'est pas possible, le risque résultant de cette faiblesse technique pour la sécurité générale de l'information doit être réduite à un risque résiduel qui soit consistant avec les critères d'acceptation du risque du fournisseur, ceci au moyen de mesures d'organisation efficaces et adéquates (par ex. réglement des responsabilités, procédures et processus de travail, sensibilisation, formation et entraînement des collaborateurs concernés) sur la base de l'analyse de risque au centre du SMSI conformément aux chiffres 3.1 ou 3.2.**
- **En cas d'utilisation de mots de passe, le fournisseur n'est pas en droit de les stocker de manière durable ou de les consigner dans des fichiers journal. Si le stockage des mots de passe d'utilisateurs techniques est inévitable, ces mots de passe doivent être protégés d'une manière équivalente et l'efficacité de la méthode utilisée doit pouvoir être prouvée.**
- **Les procédures et systèmes cryptographiques engagés doivent correspondre à l'état de la technique et répondre aux menaces actuelles. Il convient de préférence d'utiliser des procédures et des systèmes standardisés, comme cela a été recommandé par l'Agence fédérale allemande du réseau d'électricité, du gaz, des télécommunications, de la poste et des chemins de fer dans son avis du 6 janvier 2010 relatif à la signature électronique conformément à la loi et à l'ordonnance sur la signature (Vue d'ensemble concernant les algorithmes adéquats).**
- **Afin d'empêcher la possibilité de deviner les mots de passe hors ligne (password guessing), il n'est pas autorisé de crypter les informations au moyen de clés dérivant de mots de passe lors d'un envoi.**
- **La solidité des procédures et des systèmes cryptographiques doit être décrite intégralement et de manière compréhensible dans le cadre d'une architecture de sécurité générale, être vérifiée périodiquement et, le cas échéant, être adaptée.**

b) Contrôle de l'accès

- **L'accès aux informations électroniques acheminées ne peut avoir lieu que par le biais d'une procédure d'authentification forte (par ex. des certificats numériques ou des jetons d'authentification personnels). Constituent des procédures d'authentification fortes celles définies dans les Directives concernant la sécurité informatique dans l'administration fédérale, annexe 2, chiffre 5.3. L'information d'authentification ne doit, en particulier, pas être envoyée en texte clair, ceci afin de ne pas être vulnérable aux attaques par écoute et par rejeu.**
- **Lorsque des mots de passe sont utilisés dans la procédure d'authentification, ceux-ci doivent toujours être envoyés au moyen de liaisons cryptées (par ex. dans le cadre d'une session SSL/TLS). Lorsque l'on utilise dans la procédure d'authentification uniquement des mots de passe, ceux-ci doivent, s'agissant de leur solidité, se conformer aux exigences formulées dans les Directives concernant la sécurité informatique dans l'administration fédérale, annexe 1, chiffre 2.4. Il peut être renoncé à une durée de validité limitée des mots de passe.**

c) Acquisition, développement et maintenance des composants des plateformes

- **Les serveurs qui sont accessibles par Internet doivent être renforcés de manière à répondre à leurs besoins. Dans ce cadre, il convient de se référer aux bonnes pratiques (Best Practices) telles qu'elles sont mises à disposition, par exemple, par le Center for Internet Security (CIS) avec les Benchmarks de configuration de sécurité.**
- **Les attaques connues contre des applications Web, telles qu'elles sont documentées par l'Open Web Application Security Projet (OWASP) doivent pouvoir être combattues efficacement.**

4 Exigences liées au système de management des services TI

4.1 Exigences de base

Pour une exploitation fiable des plateformes, il est nécessaire de prouver que les processus suivants d'exploitation sont documentés, introduits, exploitées, surveillés de manière permanente, vérifiés périodiquement, maintenus et améliorés:

- **Processus de fourniture des services**
  - **Gestion des niveaux de services**
  - **Etablissement de rapports de services**
  - **Gestion de la continuité et de la disponibilité des services**
  - **Budgétisation et comptabilisation des services**
  - **Gestion de la capacité**
- **Processus de gestion des relations**
  - **Gestion des relations commerciales**
  - **Gestion des fournisseurs**
- **Processus de résolution**
  - **Gestion des incidents et des demandes de services**
  - **Gestion des problèmes**
- **Processus de contrôle**
  - **Gestion des configurations**
  - **Gestion des changements**
  - **Gestion des mises en production et de leur déploiement**

Les processus d'exploitation doivent répondre aux standards internationaux ISO/CEI 20000-1:2011 (Technologies de l'information – Gestion des services – Partie 1: Exigences du système de management des services) et ISO/CEI 20000-2:2005 (Technologies de l'information – Gestion des services – Partie 2: Guide pour l'application de systèmes de management de services) ou à des standards comparables. Une certification correspondante est souhaitable mais pas obligatoire.

En outre, une fonction de centre de services (Service Desk) doit être créée, exploitée, surveillée en permanence, vérifiée périodiquement, maintenue et améliorée, dans le sens

prévu par ex. par la Bibliothèque pour l'infrastructure des technologies de l'information (Information Technology Infrastructure Library, ITIL).

4.2 Disponibilité

La disponibilité de la plateforme est calquée sur les heures d'ouverture des offices du registre foncier. En principe, une plateforme doit être disponible les jours ouvrables en permanence de 8h.00 à 18h.00. Une panne de la plateforme ne doit pas dépasser cinq minutes par événement. Cumulées, la durée totale des pannes ne doit pas excéder quinze minutes par jour ouvrable. Il est nécessaire de planifier une fenêtre de service éventuelle entre 18h.00 et 8h.00, heure suisse. La disponibilité de la plateforme doit être verbalisée et le procès-verbal doit être publié par le biais de la plateforme.

5 Sources

5.1 Normes ISO déterminantes

- ISO/CEI 20000-1:2011, Technologies de l'information – Gestion des services – Partie 1: Exigences du système de management des services
- ISO/CEI 20000-2:2005, Technologies de l'information – Gestion des services – Partie 2: Guide pour l'application des systèmes de management des services
- ISO/CEI 27000:2009, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire
- ISO/CEI 27001:2005, Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences
- ISO/CEI 27002:2005, Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la gestion de la sécurité de l'information
- ISO/CEI 27005:2011, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information
- ISO/CEI 27007:2011, Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
- ISO 19011:2011, Lignes directrices pour l'audit des systèmes de management

5.2 Références

- Agence fédérale allemande du réseau d'électricité, du gaz, des télécommunications, de la poste et des chemins de fer (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen), Avis relatif à la signature électronique conformément à la loi et à l'ordonnance sur la signature (Signaturgesetz und Signaturverordnung; vue d'ensemble des algorithmes appropriés), du 6 janvier 2010 (www.bundesnetzagentur.de > Sachgebiete > Qualifizierte elektronische Signatur > Veröffentlichungen > Geeignete Algorithmen)
- Directives concernant la sécurité informatique dans l'administration fédérale, Annexe 2: Définitions et directives concernant la sécurité des réseaux (www.isb.admin.ch)

- **Directives concernant la sécurité informatique dans l'administration fédérale, Annexe 1: Exigences de sécurité minimales et responsabilités relatives au besoin général de protection (www.isb.admin.ch)**
- **Open Web Application Security Project (OWASP) (http://www.owasp.org)**
- **Center for Internet Security (CIS) (http://www.cisecurity.org/)**
- **Office of Government Commerce (2001). Service Delivery. IT Infrastructure Library. The Stationery Office. ISBN 0-11-330017-4**