



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Département fédéral de la défense,  
de la protection de la population et des sports DDPS

**Office fédéral de la cybersécurité OFCS**

Version 5.1

---

# **Si001 – Protection informatique de base dans l'administration fédérale**

du 5 juillet 2024

---

## Table des matières

<b>1</b>	<b>Dispositions générales .....</b>	<b>3</b>
1.1	Objet.....	3
1.2	Champ d'application et cadre juridique.....	3
1.3	Dérogations .....	4
<b>2</b>	<b>Définitions .....</b>	<b>4</b>
<b>3</b>	<b>Principes .....</b>	<b>7</b>
<b>4</b>	<b>Exigences en matière de sécurité .....</b>	<b>8</b>
<b>5</b>	<b>Entrée en vigueur .....</b>	<b>19</b>
	<b>Abréviations.....</b>	<b>19</b>
	<b>Références .....</b>	<b>21</b>
	<b>Annexe A: Modèle de zones de la Confédération.....</b>	<b>22</b>
	<b>Annexe B: Niveaux de sécurité des moyens d'authentification et de vérification d'identité .....</b>	<b>24</b>
	<b>Annexe C: Réglementation de zone «Domaine de réseau bleu» .....</b>	<b>26</b>
C.1	Exigences et prescriptions relatives aux systèmes informatiques .....	26
C.2	Exigences et prescriptions relatives au domaine de réseau bleu .....	26
C.3	Exigences et prescriptions relatives à la communication autorisée.....	26
C3.1	Communication interne .....	26
C.3.2	Communication externe .....	26
	<b>Annexe D: Matrice d'accès du domaine de réseau bleu et de la SSZ.....</b>	<b>28</b>

# 1 Dispositions générales

## 1.1 Objet

<sup>1</sup> Se fondant sur l'art. 29, al. 1, de l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI<sup>1</sup>), la présente directive définit les exigences minimales liées à la catégorie de sécurité «protection de base» selon l'art. 17, al. 1, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI<sup>2</sup>) pour tous les moyens informatiques, dans la mesure où ces derniers ne doivent pas être soumis à une catégorie plus élevée. En vertu de l'art. 18, al. 2, LSI, tous les moyens informatiques doivent satisfaire à ces exigences.

<sup>2</sup> Chaque unité administrative (UA) est responsable de la sécurité de ses propres moyens informatiques. Elle doit mettre en œuvre et respecter la présente directive, et contrôler sa mise en œuvre et son respect.

<sup>3</sup> L'UA responsable doit documenter de manière compréhensible la mise en œuvre et le respect de la présente directive (par ex. sur la base de [Si001-Hi01]). Cette documentation doit être contrôlée et signée au moins par:

- a) le responsable de l'objet informatique à protéger (selon ch. 2, al. 1);
- b) le responsable de la sécurité de l'information de l'UA (au sens de l'art. 36 OSI);
- c) le mandant (d'un projet), et
- d) le responsable du processus d'affaires.

En outre, les signataires confirment que, selon leur évaluation, tous les fournisseurs de prestations (FP) participant à l'exploitation des moyens informatiques répondent aux exigences les concernant.

<sup>4</sup> L'UA responsable doit également documenter de manière compréhensible le contrôle de la mise en œuvre et du respect de la présente directive. La façon dont ce contrôle est exécuté dépend de l'objet informatique à protéger et de son besoin de protection. Elle doit être convenue et documentée avec le responsable de la sécurité de l'information. Si un objet à protéger est exploité par un ou plusieurs FP internes sur mandat de l'UA responsable, le contrôle est réputé réalisé lorsque les FP correspondants ont cosigné le document «Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale».

## 1.2 Champ d'application et cadre juridique

<sup>1</sup> Conformément à l'art. 29, al. 1, OSI, la présente directive s'applique à toutes les organisations visées à l'art. 2, al. 1 à 3, OSI.

<sup>2</sup> Le cadre juridique découle également de:

- a) l'ordonnance concernant la protection des informations (OPrI) et des directives concernant les prescriptions de traitement détaillées relatives à la protection des informations (directives de traitement);
- b) la loi fédérale sur la protection des données (LPD), pour ce qui est de la gestion des données personnelles;
- c) la loi fédérale sur l'archivage (LAR), pour ce qui est de l'archivage des données.

---

<sup>1</sup> SR 128.1

<sup>2</sup> SR 128

## 1.3 Dérogations

<sup>1</sup> Si une UA n'est pas en mesure d'observer une ou plusieurs exigences de la présente directive pour un objet informatique à protéger, elle doit, en vertu de l'art. 9, al. 1, OSI, demander une autorisation exceptionnelle selon l'une des trois méthodes exposées aux al. 2 à 4 ci-dessous.

<sup>2</sup> Les exigences signalées par un astérisque (\*) au ch. 4 comportent moins de risques du point de vue de la sécurité informatique de l'administration fédérale. Elles peuvent faire l'objet de dérogations si celles-ci sont justifiées et consignées dans le document «Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale» ou dans le concept de sécurité de l'information et de protection des données (SIPD). La dérogation est alors réputée approuvée par les responsables énoncés au ch. 1.1, al. 3.

<sup>3</sup> Le responsable de la sécurité de l'information de l'UA compétente peut approuver une demande formelle de dérogation lorsque les conditions ci-dessous sont réunies (cumulativement).

- a) Le responsable de la sécurité de l'information est tellement impliqué dans le processus d'octroi d'une autorisation exceptionnelle qu'il peut assumer cette responsabilité.
- b) La dérogation porte exclusivement sur l'utilisation d'informations de l'UA compétente ou sur d'autres objets informatiques à protéger qui n'ont aucun besoin de protection accru ou qui présentent un tel besoin en raison des seules exigences relatives à la protection des données.
- c) La dérogation ne concerne ni des services informatiques standard ni une autre UA.
- d) Toutes les personnes énoncées au ch. 1.1, al. 3, et le responsable de l'UA ou un membre de sa direction sont manifestement d'accord avec la dérogation.
- e) Le responsable de la sécurité de l'information tient à jour un registre des autorisations exceptionnelles accordées et, sur demande, le communique au service spécialisé de la Confédération pour la sécurité de l'information.

<sup>4</sup> Toutes les autres demandes de dérogation peuvent être soumises au NCSC conformément à la gestion des exigences et des directives concernant l'informatique de l'administration fédérale (P035). Elles doivent justifier les dérogations à la protection informatique de base et présenter de manière détaillée les mesures éventuelles et prévues pour réduire les risques.

<sup>5</sup> Les dérogations visées à l'al. 4 sont toujours limitées dans le temps (en général, deux ans).

## 2 Définitions

<sup>1</sup> Conformément à l'art. 17, al. 1, LSI, tous les moyens informatiques relèvent de la catégorie de sécurité «protection de base», à moins qu'ils relèvent d'une catégorie de sécurité supérieure. Les moyens informatiques visés par la loi comprennent tant des moyens informatiques individuels que plusieurs moyens informatiques de même nature ou liés entre eux, car la LSI et l'OSI ont pour objectif une couverture de sécurité complète. Puisque ces moyens sont souvent considérés comme des unités liées entre elles, notamment dans la pratique de l'administration fédérale, ils sont désignés ci-après sous le terme d'**objets informatiques à protéger**. Cette approche permet d'identifier et de gérer les unités à protéger avec plus de précision et améliore la clarté et l'efficacité dans le cadre de la mise en œuvre des mesures de sécurité subséquentes. Il faut définir un **responsable de l'objet informatique à protéger** pour chaque objet informatique à protéger.

<sup>2</sup> De plus, les définitions suivantes s'appliquent dans la présente directive:

- a) **Analyse des besoins de protection:** méthode structurée visant à déterminer le besoin de protection d'un objet informatique à protéger. Ce faisant, on opère une distinction entre une protection de base et un besoin de protection accru.
- b) **Concept de sécurité de l'information et de protection des données (SIPD):** description structurée des exigences de sécurité d'un objet informatique à protéger, des mesures de sécurité prévues et mises en œuvre ainsi que des risques résiduels.
- c) **Informations:** données enregistrées, traitées ou transmises par voie électronique<sup>3</sup>. Si les données se réfèrent à une personne identifiée ou identifiable, il s'agit alors de **données personnelles** au sens de la LPD.
- d) **Système informatique (système):** système technique d'information qui est exploité comme un logiciel (système) sur un matériel dédié ou virtualisé, ou une machine virtuelle<sup>4</sup>. Dans le deuxième cas, on parle de système informatique virtualisé.
- e) Un système informatique est<sup>5</sup>:
  - un **système serveur** lorsqu'il fournit avant tout des prestations informatiques;
  - un **système client** lorsqu'il bénéficie avant tout de prestations informatiques;
  - un **ordinateur client de l'administration fédérale** lorsqu'il est un système client géré au sein du service standard Bureautique. Il peut s'agir soit d'un système de poste de travail (SPT), soit d'un système client virtualisé qui fonctionne sur un appareil électronique (*smart device*), dans une *sandbox* comportant une gestion des appareils mobiles (*mobile device management*, MDM) selon [E021] (système MDM);
  - un **périphérique** lorsqu'il étend les fonctions d'autres systèmes informatiques et doit, pour ce faire, être intégré ou installé (pilote; par ex. imprimantes, appareils multifonctions ou systèmes de présentation dans les salles de conférence);
  - un **appareil de mesure** lorsque sa tâche principale consiste à transmettre à un autre système informatique les valeurs de mesure<sup>6</sup> d'un capteur situé sur le lieu de mesurage par l'intermédiaire d'une connexion dédiée qui n'est pas utilisable à d'autres fins. Le système informatique de destination peut soit se contenter de collecter les valeurs et de les compiler, soit les analyser et les traiter. La communication peut être bilatérale et aussi permettre, par exemple, de transmettre des commandes à l'appareil de mesure. Les appareils de mesure sont surtout utilisés dans les applications de l'Internet des objets (IdO);
  - un **élément du réseau** lorsqu'il sert principalement à transporter des données entre des systèmes informatiques tels que des commutateurs, des routeurs ou des filtres de paquets statiques simples (pare-feu IP). Dans le modèle de référence OSI (*open systems interconnection*), les éléments du réseau évoluent jusqu'à la couche 5 (couche session), y compris celle-ci;

---

<sup>3</sup> Dans la présente directive, le terme «informations» est employé de manière générique pour désigner les «informations et données». On parle de données uniquement lorsqu'il s'agit des données personnelles au sens de la protection des données.

<sup>4</sup> Le système informatique qui met à disposition le matériel virtualisé ou la machine virtuelle (hyperviseur) est lui aussi un logiciel et constitue donc un système informatique autonome.

<sup>5</sup> La distinction entre un système client et un système serveur est floue, car un système informatique peut être à la fois un système client et un système serveur.

<sup>6</sup> Ces valeurs de mesure peuvent également être des signaux acoustiques et/ou optiques.

- un **point d'application des règles ou *policy enforcement point* (PEP)** lorsqu'il sert principalement à mettre en œuvre des règles (provenant de politiques). Exemples: filtres de paquets dynamiques, gateway (passerelles) pour protocoles d'application, serveurs proxy et proxy inverse. Dans le modèle de référence OSI, les PEP évoluent jusqu'à la couche 7 (couche application), y compris celle-ci, et vérifient dès lors également le(s) protocole(s) de communication transmis.
- f) **Application:** logiciel d'application utilisé sur les systèmes informatiques d'une ou de plusieurs UA pour exécuter des processus d'affaires. Les applications de l'IdO se distinguent des autres applications principalement par le fait que les informations utilisées proviennent surtout d'appareils de mesure.
- g) **Réseau:** dispositif technique (composé principalement d'éléments du réseau et de connexions) servant à échanger des données entre des systèmes informatiques.
- h) **Segment de réseau (segment):** partie d'un réseau qui – pour des raisons d'équilibrage de charges et/ou de sécurité – est généralement séparée du reste du réseau au moyen d'éléments du réseau.
- i) **Zone:** regroupement logique de systèmes informatiques qui présentent des exigences de sécurité similaires et sont soumis à la même réglementation (*policy*) de zone. En particulier, une zone n'est pas limitée à un périmètre précis (par ex. un centre de calcul). Le raccordement au niveau réseau des éléments d'une zone est réalisé grâce aux éléments du réseau, tandis que l'application de la réglementation de zone relève des PEP.
- j) **Sous-zone:** une zone peut être subdivisée en sous-zones si la réglementation correspondante le prévoit. Chaque sous-zone constitue une zone. En particulier, toute sous-zone doit avoir une réglementation qui peut uniquement préciser celle de la zone supérieure; en d'autres termes, la réglementation de la sous-zone ne peut contenir que des exigences ou prescriptions supplémentaires (tout assouplissement est proscrit). Une sous-zone peut être subdivisée en sous-zones supplémentaires, mais uniquement en cas d'absolue nécessité.
- k) **Réglementation de zone:** elle décrit de manière structurée les exigences et les prescriptions relatives
- aux systèmes informatiques exploités dans la zone,
  - à la zone elle-même (par ex. peut-elle être segmentée sur le réseau et, si oui, comment?),
  - à l'authentification des personnes et des processus automatisés qui accèdent aux applications et aux systèmes informatiques exploités dans la zone, et
  - à la communication interne (pouvant dépasser le cadre du segment) et externe (pouvant dépasser le cadre de la zone d'application des règles [*policy enforcement zone*, PEZ]) autorisée pour la zone, c'est-à-dire les communications entrantes et sortantes admises<sup>7</sup>. Une communication entre deux ou plusieurs zones similaires<sup>8</sup> est considérée comme interne si les interfaces entre les zones sont conformes aux réglementations (*policy*) correspondantes et sont contrôlées par la PEZ commune.

<sup>7</sup> Une communication est sortante lorsque l'échange de données correspondant est initié par un système informatique de la zone en question. Dès lors, elle est entrante lorsque l'échange de données a certes été initié par un système informatique situé hors de la zone, mais s'adresse à un système informatique se trouvant dans cette dernière. Dans les deux cas, les données peuvent être échangées dans les deux directions.

<sup>8</sup> Ces zones peuvent également avoir des propriétaires différents.

- l) **Modèle de zones de la Confédération:** modèle générique pour la création de zones dans l'administration fédérale (cf. annexe A).

### 3 Principes

<sup>1</sup> **Forme de la fourniture de prestations:** la protection informatique de base s'applique à tous les objets informatiques à protéger, indépendamment de la forme de la fourniture de prestations. En d'autres termes, les exigences et mesures de sécurité relatives aux FP doivent être mises en œuvre par les FP tant internes qu'externes. En cas de FP externes, il faut en particulier veiller au respect des directives relatives à la sécurité informatique<sup>9</sup> et à l'obtention de l'autorisation correspondante de l'autorité supérieure, conformément aux processus spécifiques à un office ou à un département (cf. [Si001-Hi04]).

<sup>2</sup> **Virtualisation:** la protection informatique de base s'applique indépendamment du fait qu'un objet informatique à protéger soit exploité sur du matériel dédié ou de manière virtualisée sur du matériel utilisé conjointement. Concernant le besoin de protection accru, l'usage d'éventuelles technologies et solutions de virtualisation doit être justifié et documenté dans le concept SIPD.

<sup>3</sup> **Principe «Zero Trust»:** dans la mesure du possible, le dispositif de sécurité d'un objet informatique à protéger devrait être conçu de manière à ce que les exigences de sécurité énoncées au ch. 4 puissent être satisfaites en toute autonomie et à ce que l'objet soit cloisonné et isolé de son environnement, de sorte qu'il faille faire le moins d'hypothèses possibles sur la sécurité de l'environnement.

<sup>4</sup> **Principe «Defense in Depth»:** lorsque cela est possible et économiquement justifiable, un objet à protéger doit être sécurisé par plusieurs mesures de sécurité additionnelles qui se complètent mutuellement afin que le respect des exigences de sécurité soit redondant. Ces mesures de sécurité doivent avoir globalement un effet préventif, détecteur et réactif.

<sup>5</sup> **État de la technique:** toutes les mesures de sécurité (préventives, détectrices et/ou réactives) utilisées doivent correspondre à l'état de la technique<sup>10</sup>, être standardisées dans l'idéal et avoir fait leurs preuves sur le plan opérationnel. Les mesures obsolètes ou dont on connaît les vulnérabilités ou les faiblesses doivent être améliorées ou remplacées rapidement et indépendamment du cycle de vie.

<sup>6</sup> **Principe «Least Privilege» ou «Need to Know»:** l'octroi de droits d'accès et de privilèges doit se limiter au strict minimum. Cela s'applique par exemple aux utilisateurs des systèmes informatiques et des applications<sup>11</sup>, aux services et aux fonctionnalités complémentaires (*features*) qui sont activés dans ces systèmes et applications, ainsi qu'aux communications autorisées dans le cadre des réglementations (*policies*) de zone<sup>12</sup>.

<sup>8</sup> **Principe «Security by Design»:** la sécurité doit être prise en compte dès le début du développement des composants matériels et logiciels ou de leur utilisation dans des systèmes informatiques et des applications. Elle doit être mise à jour afin que ces systèmes

---

<sup>9</sup> Par exemple, le respect des directives relatives à la sécurité informatique peut être défini contractuellement et/ou garanti par des examens et certificats correspondants.

<sup>10</sup> Les recommandations de la Base d'aide au commandement (BAC) COE CRYPT du 24 janvier 2023 sur les procédés cryptographiques pour la protection de base (*Empfehlungen zu kryptografischen Verfahren für den Grundschutz*, en allemand) fournissent des renseignements sur l'état de la technique dans le domaine de la cryptographie.

<sup>11</sup> Dans l'idéal, un concept de rôles sera élaboré pour l'octroi des droits d'accès aux utilisateurs (dans le cadre d'un contrôle des accès fondés sur les rôles).

<sup>12</sup> Les protocoles de communication sont admis uniquement s'ils sont nécessaires à l'exploitation.

et applications ne présentent, dans la mesure du possible, aucune vulnérabilité ou faiblesse et que les possibilités d'attaque demeurent à un faible niveau.

<sup>9</sup> **Principe «Security by Default»:** les objets informatiques à protéger doivent être développés, configurés et exploités de telle sorte que toutes les mesures de sécurité judicieuses dans un environnement spécifique soient activées par défaut et puissent déployer leurs effets sans que les utilisateurs aient à s'en occuper.

<sup>10</sup> **Neutralité par rapport au produit:** les prescriptions et recommandations sont neutres en ce qui concerne le produit. Des déclarations favorables ou défavorables à l'usage de certains produits sont formulées uniquement lorsqu'elles concernent un service informatique standard<sup>13</sup> ou lorsqu'il existe d'autres motifs impérieux pour la sécurité informatique.

## 4 Exigences en matière de sécurité

<sup>1</sup> Les principes énoncés au ch. 3 doivent être pris en compte pour chaque objet informatique à protéger, et les exigences en matière de sécurité visées à l'al. 2, respectées. Ces exigences sont en partie reprises de la norme ISO/IEC 27002:2013 et structurées selon la norme ISO/IEC DIS 27002<sup>14</sup>.

<sup>2</sup> Les exigences en matière de sécurité qui concernent l'organisation (O), le personnel (P), la technique (T) et les informations (I) doivent toujours être respectées, tandis que les exigences relatives aux systèmes informatiques (S), aux applications (A) et aux zones (Z) doivent l'être uniquement lorsque des objets informatiques à protéger correspondants sont utilisés.

Organisation	
<b>O1</b>	<p>Responsabilité</p> <p>Une personne (au sein de l'UA compétente) doit être nommée responsable de l'objet informatique à protéger. Compétente pour mettre en œuvre la présente directive, elle doit avoir conscience de ses responsabilités et disposer de connaissances techniques suffisantes pour les assumer.</p>
<b>O2</b>	<p>Documentation</p> <p>O2.1 Une documentation à jour, harmonisée avec celle des FP impliqués, doit être disponible pour l'objet informatique à protéger. Elle doit couvrir toute la durée de vie (cycle de vie) de l'objet, et notamment:</p> <ul style="list-style-type: none"> <li>a) la chaîne d'approvisionnement (<i>supply chain</i>);</li> <li>b) les mesures de protection physiques, la nécessité de mesures techniques et architecturales pour protéger physiquement les systèmes informatiques devant être définie aux endroits requis avec l'Office fédéral des constructions et de la logistique (OFCL), armasuisse ou le Service fédéral de sécurité;</li> </ul>

<sup>13</sup> Par exemple, dans le domaine de la cryptographie asymétrique, on utilisera de préférence des certificats émis par la Swiss Government PKI (SG-PKI) et, pour le cryptage des fichiers classés CONFIDENTIEL sur les SPT, le logiciel de chiffrement de l'administration fédérale (couche 1).

<sup>14</sup> Contrairement à la norme ISO/IEC 27002:2013, le présent document opère une distinction entre les contrôles organisationnels (section 5), personnels (section 6), physiques (section 7) et techniques (section 8). La correspondance entre les contrôles issus de la norme ISO/IEC DIS 27002 et ceux provenant de la norme ISO/IEC 27002:2013 est récapitulée à l'annexe B de la norme ISO/IEC DIS 27002.



	<p>c) les éléments, les fonctions et les paramètres importants pour la sécurité;</p> <p>d) la gestion des clés lors de l'emploi de procédés cryptographiques;</p> <p>e) les modalités et les processus en cas de modification (dans le cadre de la gestion des changements), de réparation, d'élimination et de perte;</p> <p>f) les accords contractuels, et</p> <p>g) les processus et activités d'audit<sup>15</sup> destinés à contrôler la mise en œuvre et le respect de la présente directive.</p> <p>O2.2 Lorsque l'objet informatique à protéger (système informatique ou application) n'est pas exploité dans une zone de l'administration fédérale (par ex. nuage public), la documentation doit préciser:</p> <p>a) comment le besoin de protection de l'objet peut être satisfait dans cet environnement, et</p> <p>b) les mesures de sécurité complémentaires garantissant que cette situation n'engendre ni menace ni risque supplémentaires pour les autres objets informatiques à protéger de l'administration fédérale.</p>
<b>O3</b>	<p>Continuité de l'activité</p> <p>Concernant l'objet informatique à protéger, la continuité de l'activité doit être garantie et documentée dans le cadre d'un processus de gestion de la continuité des services informatiques (<i>IT Service Continuity Management, ITSCM</i>) ou de gestion de la continuité de l'activité (<i>Business Continuity Management, BCM</i>), conformément au besoin identifié lors de l'analyse des besoins de protection.</p>
<b>O4</b>	<p>Cyberincidents</p> <p>L'objet informatique à protéger doit être intégré au processus de gestion des cyberincidents.</p>
<b>Personnel</b>	
<b>P1</b>	<p>Sensibilisation et formation</p> <p>P1.1 Tous les utilisateurs de l'objet informatique à protéger doivent être formés et sensibilisés à la sécurité informatique selon leur niveau de responsabilité et leur fonction.</p> <p>P1.2 Tous les utilisateurs de l'objet informatique à protéger doivent connaître les directives d'application importantes pour celui-ci et s'engager à les respecter<sup>16</sup>.</p>
<b>P2</b>	<p>Obligation d'annonce</p> <p>Tous les utilisateurs de l'objet à protéger doivent signaler aussi rapidement que possible au service compétent (par ex. Service Desk du FP) les événements</p>

<sup>15</sup> Les processus et activités d'audit doivent être exécutés par un organe indépendant et conçus de telle sorte que la disponibilité des objets informatiques à protéger soit affectée le moins possible (en d'autres termes, les dysfonctionnements et les interruptions d'exploitation doivent être aussi limités que possible).

<sup>16</sup> Cela s'applique en particulier à l'utilisation de systèmes MDM et/ou de périphériques privés lors du travail mobile. Une liste des directives d'application est disponible à l'adresse:  
[https://intranet.dti.bk.admin.ch/isb\\_kp/fr/home/ikt-vorgaben/einsatzrichtlinien.html](https://intranet.dti.bk.admin.ch/isb_kp/fr/home/ikt-vorgaben/einsatzrichtlinien.html).

	critiques en matière de sécurité tels qu'un comportement anormal ou douteux du système ou une perte physique.
<b>Technique</b>	
<b>T1</b>	<p>Exploitation</p> <p>L'objet informatique à protéger doit être exploité conformément à l'état de la technique, en tenant compte des directives et recommandations de sécurité usuelles de la branche (meilleures pratiques).</p>
<b>T2</b>	<p>Configuration et paramétrage</p> <p>T2.1 Avant sa première mise en service, l'objet informatique à protéger doit être configuré et paramétré de façon à:</p> <ul style="list-style-type: none"> <li>a) être protégé contre un accès non autorisé;</li> <li>b) être renforcé, si cela est techniquement possible, et être exploité dans une configuration minimale nécessaire à l'accomplissement des tâches qui ne peut pas être modifiée par un utilisateur (en d'autres termes, les interfaces, modules et fonctions non utilisés doivent être désactivés), et</li> <li>c) permettre un enregistrement et une évaluation rapide des activités et événements importants pour la sécurité (avec horodatage).</li> </ul> <p>T2.2 L'activation, la modification, la désactivation et la désinstallation des configurations et des paramètres de sécurité requièrent une autorisation.</p>
<b>T3</b>	<p>Environnement de production</p> <p>L'environnement de production de l'objet informatique à protéger doit être séparé des environnements non productifs (par ex. environnements de développement ou de test). En cas de séparation logique, les dispositifs et mesures de sécurité correspondants doivent être justifiés et documentés.</p>
<b>T4</b>	<p>Faiblesses et vulnérabilités</p> <p>Il faut rechercher régulièrement et, de préférence, automatiquement (par ex. avec un scanner de sécurité) les faiblesses et les vulnérabilités de l'objet informatique à protéger avant sa mise en service et, en fonction de son besoin de protection et de son exposition à Internet, pendant l'exploitation.</p>
<b>T5</b>	<p>Authentification et autorisation</p> <p>T5.1 Tout accès à un objet informatique à protéger doit être authentifié<sup>17</sup> conformément au besoin de protection de ce dernier et autorisé selon le principe «Least Privilege» ou «Need to Know».</p> <p>T5.2 Tous les droits d'accès à l'objet informatique à protéger doivent être gérés dans le cadre d'un processus<sup>18</sup> défini et documenté et être tenus à jour en tout temps. En particulier, la nécessité et l'exactitude des droits</p>

<sup>17</sup> L'authentification peut être réalisée localement ou à l'aide d'une ou de plusieurs connexions réseau. Dans le second cas, elle est considérée dans son intégralité (c.-à-d. authentification locale sur un terminal et authentifications éventuelles sur des serveurs proxy).

<sup>18</sup> Dans le cadre de ce processus, la séparation des pouvoirs entre l'autorisation et l'attribution de droits d'accès doit être prise en compte lorsque cela est possible et judicieux, et documentée.

	<p>seront examinées au moins une fois par an, les droits (ou comptes) qui ne sont plus nécessaires étant supprimés.</p> <p>T5.3 Seuls des moyens d'authentification et de vérification d'identité gérés dans le cadre d'un processus défini et documenté peuvent être utilisés pour l'objet informatique à protéger. Ce processus doit couvrir l'ensemble du cycle de vie dudit moyen (y c. les possibilités d'accès en cas d'urgence, le blocage, la réinitialisation, la révocation et l'élimination).</p>
<b>T6</b>	<p>Authentification de l'utilisateur</p> <p>T6.1 L'utilisateur d'un SPT ou d'un système serveur doit être authentifié par un moyen d'authentification et de vérification d'identité présentant au moins le niveau de sécurité «moyen» selon l'annexe B ou grâce à une authentification à deux facteurs<sup>19</sup>.</p> <p>T6.2 L'utilisateur d'un système MDM doit être authentifié par une procédure compatible avec le système d'exploitation en question, telle qu'un numéro d'identification personnel (NIP)<sup>20</sup> ou une authentification biométrique (par ex. Touch ID ou Face ID pour les appareils iOS). Le NIP doit comporter au moins six caractères et ne pas être trop simple.</p> <p>T6.3 L'utilisateur d'un élément du réseau doit être authentifié par un moyen d'authentification et de vérification d'identité présentant au moins le niveau de sécurité «élevé» selon l'annexe B.</p>
<b>T7</b>	<p>Mots de passe</p> <p>Les exigences suivantes s'appliquent à l'authentification de l'utilisateur au moyen d'un mot de passe.</p> <p>T7.1* Le mot de passe</p> <ol style="list-style-type: none"> <li>a) doit être personnel<sup>21</sup>;</li> <li>b) doit être unique<sup>22</sup>;</li> <li>c) ne doit pas être communiqué à un tiers;</li> <li>d) ne doit pas être écrit ou doit être consigné de manière sécurisée ou être géré par un programme de chiffrement des mots de passe<sup>23</sup>;</li> <li>e) doit comporter au moins dix caractères (18 caractères pour les utilisateurs ayant des droits élevés), au moins trois des quatre catégories suivantes devant être présentes: majuscules, minuscules, chiffres et caractères spéciaux;</li> </ol>

<sup>19</sup> La nécessité d'une authentification à deux facteurs découle d'une décision prise par le Conseil fédéral le 4 juin 2010. Pour les collaborateurs de la Confédération, on utilise des certificats de classe B de la SG-PKI. En cas de système serveur, l'authentification de l'utilisateur se réfère au niveau du système d'exploitation.

<sup>20</sup> La différence conceptuelle entre un mot de passe et un NIP est expliquée dans la considération technologique «Passwörter vs. PINs» du 29 juin 2012. Par conséquent, les exigences minimales des NIP indiquées ici ne s'appliquent que de manière limitée.

<sup>21</sup> Les comptes impersonnels ne peuvent être octroyés que dans des cas particuliers dûment justifiés. Ils ne peuvent pas être utilisés pour accéder à des objets informatiques à protéger présentant un besoin de protection accru.

<sup>22</sup> Il est notamment interdit d'utiliser le même mot de passe pour s'authentifier dans plusieurs systèmes informatiques et applications.

<sup>23</sup> Sur le SPT, il faut utiliser l'outil de gestion personnelle des mots de passe (couche 1).

	<p>f) ne doit pas être ordinaire ni se référer à l'utilisateur (par ex. aucun attribut tel que l'identifiant de l'utilisateur, son nom, son prénom ou sa date de naissance).</p> <p>T7.2* Un mot de passe initial attribué de manière administrative doit être modifié dès sa première utilisation.</p> <p>T7.3* Lorsque le mot de passe est changé, il faut s'assurer que le nouveau ne correspond pas à l'un des dix mots de passe utilisés précédemment.</p> <p>T7.4* Après cinq tentatives erronées au plus, le mot de passe doit être bloqué. Il ne peut être débloqué que dans le cadre d'un processus défini.</p> <p>T7.5 Le mot de passe doit être changé sans délai si l'on soupçonne que des personnes non autorisées en ont connaissance ou qu'il y a un abus.</p> <p>T7.6* Au niveau du serveur, il faut veiller à ce que le mot de passe ne puisse pas être lu en texte clair ni être compromis facilement dans le cadre d'une autre attaque.</p>
<p><b>T8</b></p>	<p>Accès administratifs et accès à distance</p> <p>T8.1 Les accès administratifs à l'objet informatique à protéger doivent être exécutés de manière documentée et contrôlée. En particulier, ils doivent bénéficier d'une sécurisation cryptographique tout en étant enregistrés et évalués de façon compréhensible.</p> <p>T8.2 Les systèmes informatiques utilisés pour les accès administratifs doivent être dédiés à cette tâche et, de préférence, exploités dans une zone de gestion. L'utilisation des comptes (privilegiés) correspondants doit pouvoir être attribuée à une personne. De plus, les comptes ne peuvent disposer que des droits d'accès minimaux requis, dont la durée de vie sera aussi courte que possible<sup>24</sup>. Ils doivent être affectés à l'une des couches d'un modèle de couches<sup>25</sup> et ne peuvent servir qu'à l'administration au sein de cette couche (pour éviter une escalade des privilèges). En particulier, les comptes ne peuvent pas être employés pour des accès non administratifs à Internet.</p> <p>T8.3 Un accès direct à distance est autorisé pour un prestataire externe si:</p> <ol style="list-style-type: none"> <li>a) le propriétaire de l'objet est d'accord et consent à d'éventuelles violations du secret de fonction conformément aux procédures spécifiques à l'office ou au département (cf. [Si001-Hi03], [Si001-Hi04]);</li> <li>b) l'accès est réalisé via un compte dédié et l'utilisateur est authentifié par un moyen d'authentification et de vérification d'identité présentant au moins le niveau «moyen» selon l'annexe B;</li> <li>c) l'utilisation de ce compte est limitée dans le temps et surveillée;</li> <li>d) lorsque cela est techniquement possible, l'accès est exécuté via un <i>jump host</i>;</li> <li>e) le raccordement technique du compte au réseau bénéficie d'une sécurisation cryptographique (par ex. avec SSH), et</li> <li>f) la possibilité d'auditer les processus externalisés est garantie en tout temps.</li> </ol>

<sup>24</sup> Idéalement, les comptes sont gérés dans le cadre d'une solution Privileged Access Management (PAM) et ne sont valables que pour la durée d'une activité administrative précise.

<sup>25</sup> Ce modèle de couches est défini, par exemple, dans le cadre de la directive AR012 sur l'architecture.

<b>Informations (données)</b>	
<b>I1*</b>	<p><b>Admissibilité des systèmes informatiques</b></p> <p>Les informations importantes pour les affaires peuvent être enregistrées et traitées sur des systèmes informatiques uniquement lorsqu'ils appartiennent à une UA de l'administration fédérale ou lorsque le respect des exigences techniques de sécurité énoncées dans le présent document est défini contractuellement pour ces systèmes (par ex. dans le cadre d'une solution en nuage).</p>
<b>I2</b>	<p><b>Confidentialité et intégrité</b></p> <p>12.1 La confidentialité et l'intégrité des informations importantes pour les affaires doivent être protégées à tout moment par des procédés cryptographiques, conformément à leur besoin de protection et en tenant compte des particularités physiques<sup>26</sup> (cela vaut également pour les données de test et les données de production utilisées à des fins de test). Lorsque les informations sont cryptées, les clés utilisées à cet effet doivent être gérées de telle sorte qu'une récupération et, partant, un décryptage des informations soient possibles à tout moment. En général, cela requiert une administration complexe des clés (avec un mécanisme de récupération des clés) et un test régulier de la récupération.</p> <p>12.2 Les systèmes informatiques utilisés doivent être appropriés pour garantir la protection de la confidentialité et de l'intégrité des informations<sup>27</sup>.</p>
<b>I3</b>	<p><b>Disponibilité</b></p> <p>13.1 La disponibilité des informations importantes pour les affaires doit être garantie à tout moment, conformément au besoin de protection.</p> <p>13.2 Les UA responsables des informations doivent disposer d'une stratégie de sauvegarde<sup>28</sup> et la mettre en œuvre. Cette stratégie doit prévoir un principe multigénérationnel et un stockage hors ligne des principaux jeux de données afin que celles-ci puissent être récupérées même en cas de malicieux chiffrant les informations (rançongiciel).</p>
<b>I4</b>	<p><b>Supports de données</b></p> <p>Les supports de données sur lesquels sont enregistrées les informations importantes pour les affaires doivent à tout moment être protégés conformément au besoin de protection de ces informations. Des processus appropriés doivent être définis et mis en œuvre pour la réparation et l'élimination de ces supports<sup>29</sup>.</p>

<sup>26</sup> En particulier, les informations ayant un besoin de protection accru qui sont enregistrées sur les disques durs de systèmes serveurs physiques sans protection particulière doivent être sécurisées grâce à un chiffrement du disque dur.

<sup>27</sup> Par exemple l'enregistrement et le traitement d'informations classées CONFIDENTIEL, de données sensibles ou de profils de la personnalité sur des systèmes MDM ne sont pas autorisés ou ne le sont que dans le cadre d'une communication vocale chiffrée [E027].

<sup>28</sup> Lorsque l'UA responsable est un bénéficiaire de prestations (BP), la stratégie de sauvegarde peut également provenir du FP. Elle doit cependant être vérifiée et considérée comme appropriée par le BP. Des exercices réguliers concernant cette stratégie revêtent alors une importance primordiale: la possibilité de récupérer les données après une perte doit être contrôlée régulièrement et confirmée par le BP.

<sup>29</sup> Lors de l'élimination des supports de données, il faut en particulier veiller à ce que leur contenu ou les données enregistrées ne puissent pas être reconstitués.

<b>Systemes informatiques</b>	
<b>S1</b>	<p>Affectation à une zone</p> <p>Le système informatique doit être affecté à une zone et exploité conformément à la réglementation de cette zone<sup>30</sup>.</p>
<b>S2</b>	<p>Mises à jour et correctifs</p> <p>Il faut s'assurer soit que le ou les fabricants du système informatique proposent pendant toute sa durée de vie des mises à jour et des correctifs (patches) qui peuvent être vérifiés et installés rapidement<sup>31</sup>, soit que le système informatique est exploité dans une zone dédiée et aussi hermétique que possible (par ex. zone technique), des mesures de sécurité complémentaires garantissant que cette situation n'engendre ni menace ni risque supplémentaires pour les autres objets informatiques à protéger de l'administration fédérale. Si un remplacement est prévu, le système informatique peut encore être exploité pendant deux ans au plus, à condition que la poursuite de l'exploitation soit exposée dans un concept SIPD.</p>
<b>S3</b>	<p>Comptes de service</p> <p>S3.1 Les comptes utilisés par les services système (comptes de service) doivent être spécifiques<sup>32</sup> et posséder uniquement les droits minimums requis pour fournir les services.</p> <p>S3.2* Les comptes de service doivent être gérés automatiquement et requérir une authentification cryptographique forte. Idéalement, celle-ci s'appuiera sur une cryptographie asymétrique, les clés privées utilisées à cet effet devant être consignées de manière sûre. Si l'authentification repose sur des mots de passe, ils doivent être sensiblement plus forts (et plus longs) que pour l'authentification de l'utilisateur.</p>
<b>S4</b>	<p>Protection de l'intégrité et protection contre les maliciels</p> <p>S4.1 L'intégrité des composantes logicielles utilisées sur le système informatique doit être garantie (par ex. à l'aide de signatures numériques). En particulier, l'intégrité de chaque système serveur ayant un besoin de protection accru doit être contrôlée régulièrement<sup>33</sup>.</p> <p>S4.2 Lorsqu'une perte d'intégrité est détectée, le système informatique doit être immédiatement coupé du réseau, sécurisé et examiné. Si sa compromission est confirmée, il doit être intégralement supprimé et reconfiguré.</p> <p>S4.3 Le système informatique doit être intégré dans un concept de protection contre les maliciels basé sur [SB003], qui définit en particulier la marche à suivre lorsqu'un maliciel est identifié, les services à informer et la manière de le faire.</p>

<sup>30</sup> Un système informatique qui ne peut être affecté à aucune autre zone fait partie d'Internet. Il n'existe alors aucune réglementation de zone. De plus, il se peut que des éléments du réseau ne soient attribués ni à une zone ni à Internet. Ils doivent être documentés.

<sup>31</sup> Pour les APS qui ne sont pas connectés en permanence au réseau, il faut s'assurer qu'ils sont mis à jour au moins une fois par mois avec des mises à jour et des correctifs.

<sup>32</sup> Un compte de service est réputé spécifique lorsqu'il n'est utilisé que pour un service.

<sup>33</sup> Conformément à la décision du Conseil fédéral du 16 décembre 2009.

<b>S5</b>	<p>Ordinateurs clients de l'administration fédérale</p> <p>S5.1 Les supports de données internes non volatils (par ex. disques durs) doivent être visiblement cryptés sur un ordinateur client de l'administration fédérale. En cas de système MDM, il faut prévoir en plus une possibilité de réinitialiser à distance ses paramètres de base et de supprimer toutes les informations enregistrées localement.</p> <p>S5.2 En l'absence d'activité de l'utilisateur, l'accès à l'ordinateur client de l'administration fédérale doit être bloqué automatiquement (au bout de 15 min. au plus pour les SPT et de 3 min. au plus pour les systèmes MDM). Une activation manuelle des blocages d'accès au système doit aussi être possible. Si un tel blocage n'est pas possible pour des raisons techniques, l'accès aux ordinateurs clients de l'administration fédérale non surveillés doit être protégé physiquement (par ex. par verrouillage de la pièce).</p> <p>S5.3 La fonction de démarrage automatique en cas de raccordement de supports de données externes (par ex. clés USB) doit être désactivée sur un ordinateur client de l'administration fédérale.</p> <p>S5.4 Les utilisateurs d'un SPT ne peuvent avoir aucun droit d'administrateur local.</p> <p>S5.5 Un accès administratif au SPT à des fins d'assistance n'est autorisé qu'avec l'autorisation explicite préalable de l'utilisateur.</p>
<b>S6</b>	<p>Périphériques</p> <p>S6.1 Un périphérique peut être utilisé lorsque</p> <ol style="list-style-type: none"> <li>il a été acquis auprès d'un service d'achat de la Confédération, et</li> <li>son intégrabilité<sup>34</sup> et sa sécurité élémentaire sont dûment confirmées par le FP.</li> </ol> <p>S6.2 Le périphérique doit être configuré de manière minimale par le FP et protégé contre les modifications non autorisées (de la configuration).</p> <p>S6.3 Lorsque l'appareil est utilisé pour imprimer des documents classifiés:</p> <ol style="list-style-type: none"> <li>il doit être exploité localement ou doit permettre d'authentifier l'utilisateur, et</li> <li>les supports de données internes non volatils (par ex. disques durs) doivent pouvoir être écrasés conformément aux recommandations en vigueur<sup>35</sup>, cet écrasement pouvant être déclenché manuellement par l'utilisateur ou automatiquement.</li> </ol> <p>S6.4 L'utilisation de périphériques privés lors du travail mobile doit respecter la directive d'application [E026].</p>
<b>Applications</b>	
<b>A1</b>	<p>Achat / développement</p> <p>A1.1 L'application doit être achetée ou développée dans le cadre d'un processus méthodique (de préférence HERMES<sup>36</sup>), en tenant compte</p>

<sup>34</sup> L'intégrabilité signifie, par exemple, que l'appareil peut être relié aux registres des collaborateurs de l'administration fédérale pour des fonctions comme ScanToMail.

<sup>35</sup> Par ex. DoD 5220.22-M ou NIST SP 800-88

<sup>36</sup> <https://www.hermes.admin.ch>

	<p>précocement des directives et recommandations en vigueur en matière de sécurité<sup>37</sup> (meilleures pratiques).</p> <p>A1.2 Lors du développement de logiciels d'application, il faut notamment veiller à</p> <ul style="list-style-type: none"> <li>a) conserver le code source de manière sûre;</li> <li>b) réglementer clairement et contrôler de manière compréhensible l'accès aux référentiels correspondants;</li> <li>c) surveiller les processus Build et n'exécuter les modifications dans la Build Pipeline que sous supervision;</li> <li>d) tester régulièrement les logiciels, et</li> <li>e) garantir à tout moment leur intégrité (par ex. à l'aide de signatures numériques).</li> </ul>
<b>A2</b>	<p>Entretien et maintenance</p> <p>Un entretien et une maintenance professionnels doivent être garantis pour l'application et ses composantes (par ex. bibliothèques logicielles) pendant toute la durée de vie. Cela englobe en particulier l'installation de mises à jour et de correctifs (patches) réguliers qui sont techniquement nécessaires à l'exploitation ou à la sécurité.</p>
<b>Zones</b>	
<b>Z1</b>	<p>Conformité</p> <p>Z1.1 La zone doit être conforme au modèle de zones de la Confédération et avoir un propriétaire, un nom unique<sup>38</sup>, une réglementation (<i>policy</i>) de zone et un exploitant<sup>39</sup> (cela ne s'applique ni à Internet ni à la zone Internet). Si elle comprend des systèmes informatiques et des applications qui sont exploités en dehors de l'administration fédérale (par ex. sur un nuage public), le raccordement au réseau doit être défini dans la réglementation de zone.</p> <p>Z1.2 L'exploitant doit veiller à ce que seules les communications admises par la réglementation de zone soient exécutées depuis et vers la zone et, grâce à des mesures de sécurité complémentaires appropriées (par ex. isolement et segmentation), à ce qu'elles n'engendrent ni menace ni risque supplémentaires pour les autres systèmes informatiques et applications au sein et hors de la zone.</p> <p>Z1.3 La zone doit être intégrée à un registre géré par le responsable de la sécurité de l'information compétent ou sur mandat de ce dernier. Un responsable de la sécurité de l'information est compétent si l'UA dont il a la charge agit en tant que propriétaire ou exploitant de la zone.</p>

<sup>37</sup> Pour le développement d'applications Web, il faut, par exemple, prendre en considération les directives et les recommandations de l'Open Web Application Security Project (OWASP), qui couvrent également la gestion sûre du code du programme.

<sup>38</sup> L'unicité peut découler, par exemple, de l'indication du propriétaire comme suffixe dans le nom de la zone (par ex. SZ-BAC pour une zone de serveurs exploitée par la BAC). Si un propriétaire met plusieurs fois en œuvre une zone, les noms correspondants doivent être clairement différenciés.

<sup>39</sup> L'exploitant est un FP qui gère la zone au niveau de la technique du réseau sur mandat du propriétaire. Si le propriétaire de la zone est un FP, le propriétaire et l'exploitant peuvent être identiques. Lorsque le propriétaire modifie la réglementation d'une (sous-)zone, un délai raisonnable de mise en œuvre doit être accordé à l'exploitant.



<b>Z2</b>	<p>Accès</p> <p>Z2.1 Un accès restreint<sup>40</sup> à une zone est autorisé uniquement pour les personnes et les processus automatisés qui ont été authentifiés par un moyen d'authentification et de vérification d'identité présentant au moins le niveau «moyen» (le niveau «faible» suffit pour les appareils de mesure). Les dérogations suivantes sont admises:</p> <ul style="list-style-type: none"> <li>a) accès anonymes et personnalisés créés dans le cadre des applications de cyberadministration utilisables par une large partie de la population dans une zone de serveurs. Les pages Web correspondantes doivent être sécurisées avec TLS (HTTPS) et protégées contre les attaques automatisées grâce à des formulaires (par ex. Captcha);</li> <li>b) accès temporaires pour charger des données sur un système serveur<sup>41</sup>;</li> <li>c) accès automatisés effectués avec le consentement d'un propriétaire de zone dans le cadre des contrôles de sécurité des sites Internet (<i>scans</i>).</li> </ul> <p>En cas d'accès à une zone présentant un besoin de protection accru (par ex. SZ+), le moyen d'authentification et de vérification d'identité doit avoir au moins le niveau «élevé» selon l'annexe B. Les dérogations a) et b) susmentionnées ne sont alors pas autorisées.</p> <p>Z2.2 Un accès illimité à une zone n'est admis que pour les personnes qui se connectent via un ordinateur client de l'administration fédérale, sont authentifiées par un moyen d'authentification et de vérification d'identité présentant au moins le niveau «élevé» selon l'annexe B et utilisent une connexion cryptographique sécurisée (par ex. avec SSH).</p>
<b>Z3</b>	<p>Communication interzone</p> <p>Toute communication interzone doit passer par une PEZ<sup>42</sup>. Celle-ci doit s'assurer que la communication est conforme à la réglementation des zones concernées. Pour ce faire, les modèles et relations de communication autorisés doivent être définis aussi précisément que possible dans les réglementations des zones (dans l'idéal sur la couche applicative et sous la forme d'une <i>allow list</i>). Si un test de conformité dans une PEZ n'est pas possible (par ex. dans le cas d'une communication cryptée de bout en bout), il peut également être effectué par les systèmes informatiques dans les zones elles-mêmes (au sens d'un PEP). Toutefois, des mesures complémentaires d'atténuation des risques doivent alors être prévues et documentées.</p>
<b>Z4</b>	PEZ

<sup>40</sup> Un accès est dit restreint lorsque des mesures techniques (par ex. filtrage de paquets IP) sont mises en place pour le limiter à un seul ou à quelques systèmes informatiques ou applications définis et aux protocoles indispensables pour l'accès. Dans tous les autres cas, l'accès est réputé illimité.

<sup>41</sup> Dans ce cas, la délimitation des systèmes serveurs correspondants par rapport aux autres systèmes informatiques de la même zone doit être documentée soit dans la réglementation de zone, soit – conjointement avec toutes les mesures de sécurité complémentaires visant à minimiser les risques – dans la documentation de sécurité de l'application. Bien entendu, le propriétaire de la zone doit également donner son accord à l'exploitation des systèmes serveurs.

<sup>42</sup> Bien que cela s'applique en principe également à la communication d'une sous-zone vers sa zone supérieure, il est possible d'y renoncer dans des cas justifiés documentés dans les réglementations des sous-zones correspondantes.

	<p>Z4.1 Les PEP exploités dans une PEZ ne peuvent être gérés de manière virtualisée qu'au sein de la zone. En d'autres termes, aucun système informatique des autres zones ne peut être exploité sur le matériel utilisé en commun.</p> <p>Z4.2 Le propriétaire d'une PEZ ou d'une infrastructure proxy Web doit définir la manière dont l'accès aux ressources sur Internet est réalisé et quels accès sont autorisés. Il peut le faire dans la réglementation de zone de la PEZ ou dans une directive distincte. Dans le champ d'application du service informatique standard Communication de données, la réglementation est édictée dans le cadre de [Si004].</p> <p>Z4.3 La connexion d'une PEZ à Internet doit être hautement disponible, voire redondante. En outre, l'exploitant doit s'assurer grâce à des mesures appropriées que les systèmes informatiques séparés d'Internet par la PEZ sont dûment protégés contre des attaques de déni de service (<i>denial of service</i>, DoS) ou de déni de service distribué (<i>distributed DoS</i>, DDoS).</p>
<p><b>Z5</b></p>	<p>Surveillance</p> <p>Z5.1 La communication au sein d'une zone doit être surveillée de telle sorte que les attaques puissent être identifiées de manière aussi fiable que possible (par ex. grâce à des systèmes de détection ou de prévention d'intrusion [<i>intrusion detection system</i>, IDS; <i>intrusion prevention system</i>, IPS]) et que l'exploitant puisse réagir rapidement et adéquatement en cas de besoin.</p> <p>Z5.2 Les informations collectées lors de la surveillance doivent être conservées et protégées contre des manipulations ultérieures, conformément aux dispositions légales (en particulier la législation sur la protection des données et l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération).</p>

## 5 Entrée en vigueur

<sup>1</sup> La présente directive entre en vigueur le 5 juillet 2024.

<sup>2</sup> Les objets informatiques à protéger mis en service avant l'entrée en vigueur de la présente directive sont soumis aux dispositions qui s'appliquaient au moment de leur mise en service.

## Abréviations

BA	Bureautique
BAC	Base d'aide au commandement
BCM	Gestion de la continuité de l'activité ( <i>Business Continuity Management</i> )
BP	Bénéficiaire de prestations
CA	Autorité de certification ( <i>Certification Authority</i> )
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CDF	Contrôle fédéral des finances
CF	Ordinateur client de l'administration fédérale (client fédéral)
ChF	Chancellerie fédérale
CVC	Communication vocale chiffrée
CZ	Client Zone
DAKO	Transmission de données ( <i>Datenkommunikation</i> )
DDoS	Déni de service distribué ( <i>Distributed DoS</i> )
DIS	Draft International Standard, projet de norme internationale
DNS	Système de noms de domaine ( <i>Domain Name System</i> )
DoS	Déni de service ( <i>Denial of Service</i> )
DSID	Délégué à la sécurité informatique du département
DSIO	Délégué à la sécurité informatique de l'unité administrative
EAL	Niveau d'évaluation ( <i>Evaluation Assurance Level</i> )
FIDO	Fast ID Online
FP	Fournisseur de prestations
IAM	Gestion des identités et des accès ( <i>Identity and Access Management</i> )
ID	Identifiant
IdO	Internet des objets
IDS	Système de détection d'intrusion ( <i>intrusion detection system</i> )
IEC	Commission électrotechnique internationale (International Electrotechnical Commission)
IKE	Internet Key Exchange
IP	Protocole Internet ( <i>Internet Protocol</i> )
IPS	système de prévention d'intrusion ( <i>intrusion prevention system</i> )
IPsec	IP security, sécurité du protocole Internet
ISO	Organisation internationale de normalisation
IT	Technologies de l'information
ITSCM	Gestion de la continuité des services informatiques ( <i>IT Service Continuity Management</i> )
JSON	JavaScript Object Notation
JWT	JSON Web Token
LoA	Niveau d'assurance ( <i>Level of Assurance</i> )
LSI	Loi sur la sécurité de l'information
MDM	Gestion des appareils mobiles ( <i>Mobile Device Management</i> )
NIP	Numéro d'identification personnel ( <i>Personal Identification Number, PIN</i> )
NW	Accès illimité au réseau ( <i>Network Full Access</i> )
OFCL	Office fédéral des constructions et de la logistique

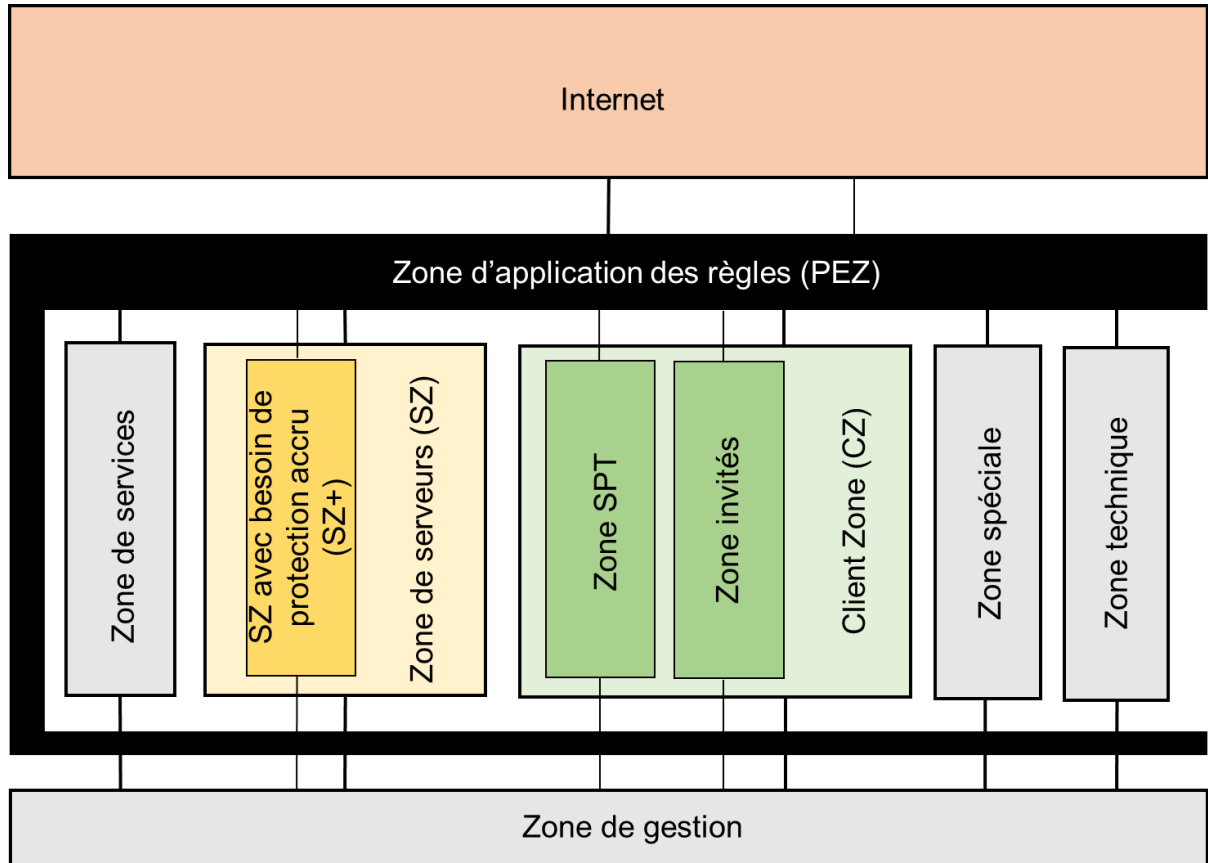
OFCS	Office fédéral de la cybersécurité
OPCy	Ordonnance sur les cyberrisques
OPrl	Ordonnance concernant la protection des informations
OSI	Open Systems Interconnection
OTP	Mot de passe à usage unique ( <i>one-time password</i> )
OWASP	Open Web Application Security Project
PAM	Gestion des accès privilégiés ( <i>Privileged Access Management</i> )
PEP	Point d'application des règles ( <i>policy enforcement point</i> )
PEZ	Zone d'application des règles ( <i>policy enforcement zone</i> )
PKI	Infrastructure à clés publiques ( <i>Public Key Infrastructure</i> )
RA	Accès restreint au réseau ( <i>Restricted Access</i> )
SAML	Security Assertion Markup Language
SG-PKI	Swiss Government PKI
SIPD	Sécurité de l'information et protection des données
SMS	Short Message Service
SPT	Système de poste de travail
SS	Service standard
SSH	Secure Shell
SSO	Single Sign-On
SSZ	Zone de services partagés ( <i>shared service zone</i> )
SZ	Zone de serveurs ( <i>Server Zone</i> )
SZ+	Zone de serveurs avec besoin de protection accru
TCP	Transmission Control Protocol
TIC	Technologies de l'information et de la communication
TLS	Transport Layer Security
TNI	Transformation numérique et gouvernance de l'informatique (secteur de la ChF)
TPM	Trusted Platform Module
TT	Terminal de tiers
UA	Unité administrative

## Références

- [E021] TNI, E021 - Directive d'application pour la synchronisation des smartphones et tablettes, version 2.1 du 9 juin 2020
- [E026] TNI, E026 - Directive d'application sur le système de poste de travail, version 1.0 du 11 juin 2019 (sera remaniée et adaptée au travail mobile)
- [E027] TNI, E027 - Directive d'application Communication vocale chiffrée (CVC), version 1.1 du 1<sup>er</sup> octobre 2021
- [LSI] Loi du 18 décembre 2020 sur la sécurité de l'information
- [OSI] Ordonnance du 8 novembre 2023 sur la sécurité de l'information
- [SB003] NCSC, Malwareschutz Strategie in der Bundesverwaltung, 2021
- [Si001-Hi01] Mise en œuvre des mesures de protection informatique de base dans l'administration fédérale, version 4.6 du 31 mars 2021
- [Si001-Hi03] Exigences liées aux risques de violation du secret de fonction dans l'administration fédérale 2021, version 1.4 du 31 mars 2021
- [Si001-Hi04] Recommandation concernant la mise en œuvre opérationnelle de la procédure de consentement, 15 décembre 2020
- [Si002-Hi01] Demande pour l'obtention de comptes impersonnels (comptes E et F), 15 décembre 2020
- [Si004] Réglementation de l'accès aux ressources sur Internet. Directive de l'administration fédérale relative aux proxys web, version 1.3 du 4 octobre 2016 (état: 1<sup>er</sup> avril 2019)

## Annexe A: Modèle de zones de la Confédération

Le modèle de zones de la Confédération (cf. illustration A.1) est un modèle générique destiné à la création de zones dans l'administration fédérale. Il définit comment les systèmes informatiques et les réseaux de cette dernière doivent être organisés et gérés en zones et en sous-zones.



**Illustration A.1:** Modèle de zones de la Confédération

Dans le modèle de zones de la Confédération, on distingue les zones et sous-zones suivantes:

- a) **Internet:** zone qui ne correspond à aucun critère des autres zones et pour laquelle aucune exigence (de sécurité) ne peut être définie.
- b) **Zone d'application des règles (Policy Enforcement Zone, PEZ):** zone pour les PEP nécessaires à l'application des règles de communication externe avec d'autres zones.
- c) **Zone de services (Service Zone):** zone destinée aux systèmes serveurs nécessaires à la fourniture de services d'infrastructure (par ex. serveurs DNS et serveur de temps).
- d) **Zone de serveurs (Server Zone, SZ):** zone destinée aux systèmes serveurs.
- e) **Zone de serveurs avec besoin de protection accru (SZ+):** sous-zone de la SZ destinée aux systèmes serveurs sur lesquels sont notamment gérées des applications ayant un besoin de protection accru selon l'analyse des besoins de protection.

- f) **Client Zone (CZ):** zone destinée aux systèmes clients. L'exploitation de systèmes serveurs dans la CZ ou une sous-zone est autorisée si la réglementation (*policy*) correspondante le prévoit et si ces systèmes serveurs sont utilisés principalement par les systèmes clients de la même (sous-)zone (par ex. serveur local de bureautique ou d'impression).
- g) **Zone SPT:** sous-zone de la CZ destinée aux systèmes clients qui fonctionnent comme des systèmes de poste de travail (SPT) et sont utilisés exclusivement pour le service standard Bureautique / UCC.
- h) **Zone invités:** sous-zone de la CZ destinée aux systèmes clients qui ne sont pas gérés par une unité administrative de la Confédération, tels que les appareils utilisés par des collaborateurs externes ou des employés de l'administration fédérale dans le cadre de la politique «Bring Your Own Device».
- i) **Zone spéciale:** zone destinée aux systèmes informatiques de l'administration fédérale qui présentent des caractéristiques particulières et des exigences correspondantes (par ex. exploitation autosuffisante ou connexion réseau à faible bande) et qui peuvent être administrés depuis la zone de gestion (par ex. réseau de transport assorti d'exigences spécifiques).
- j) **Zone technique:** zone particulière destinée aux systèmes informatiques et aux systèmes de l'IdO, tels que les systèmes de domotique ou de *facility management*, les systèmes d'enregistrement du temps de travail, les systèmes de mesure et les systèmes de télédiagnostic.
- k) **Zone de gestion:** zone particulière destinée aux systèmes informatiques qui sont utilisés exclusivement pour administrer les systèmes informatiques des autres zones.

Toute (sous-)zone du modèle de zones de la Confédération peut être mise en œuvre plusieurs fois.

## Annexe B: Niveaux de sécurité des moyens d'authentification et de vérification d'identité

Les moyens d'authentification et de vérification d'identité actuellement disponibles ou utilisés avec les protocoles de fédération correspondants sont répartis selon les quatre niveaux de sécurité suivants (faible, moyen, élevé et élevé+)<sup>43</sup>:

- a) **Faible:** les informations d'authentification transmises par le réseau étant statiques et identiques pour chaque authentification, elles peuvent être exploitées par un intrus et utilisées à mauvais escient, par exemple pour une attaque par rejeu suivie d'une usurpation d'identité. Le nom d'utilisateur et le mot de passe sont des exemples typiques de ce type d'informations d'authentification. Si celles-ci sont utilisées en tant que jeton de fédération au sens de la norme I050, il suffit de les protéger à un niveau faible contre les attaques visant leur intégrité et de les relier au contexte de l'utilisateur. À titre d'exemple, on peut citer divers «jetons au porteur» tels que les cookies.
- b) **Moyen:** les informations d'authentification sont systématiquement modifiées à chaque connexion et ne peuvent donc pas être utilisées à mauvais escient pour une attaque de rejeu suivie d'une usurpation d'identité. Font partie de cette catégorie, par exemple, les noms d'utilisateur et les mots de passe avec code de vérification envoyé par SMS ou la restriction à un appareil, les solutions logicielles utilisant des mots de passe à usage unique (one-time password [OTP], par ex. Google Authenticator), des implémentations de FIDO2 (par ex. Passkeys) offrant des possibilités de synchronisation et d'exportation des clés, ainsi que les certificats logiciels délivrés par la SG-PKI (classe C, D ou E). Si les informations d'authentification sont utilisées comme jeton de fédération, elles doivent être, d'une part, protégées contre les attaques visant leur intégrité et, d'autre part, liées au contexte de l'utilisateur (par ex. session) d'une manière correspondant à l'état de la technique. On peut citer comme exemples les tickets Kerberos des forêts de ressources de la norme standard Bureautique et les jetons au porteur tels que JWT transmis via SAML ou OIDC/OAuth.
- c) **Élevé:** les informations d'authentification sont dynamiques et dépendent d'une clé cryptographique qui est stockée dans un module matériel dédié et qui ne peut pas, en déployant un effort raisonnable, être déchiffrée à l'aide de ce module. Si le moyen d'authentification et de vérification d'identité est personnel, l'enregistrement de la personne ou la remise du moyen de vérification à celle-ci doivent être basés sur un document d'identité officiel (passeport ou carte d'identité, par ex.). Si la vérification de l'identité de la personne et l'enregistrement ont lieu conjointement, les moyens d'identification doivent être remis par courrier recommandé. La remise peut également être protégée par un code secret (mot de passe ou NIP, par ex.) ou par des caractéristiques biométriques (Touch ID ou Face ID avec Apple, Hello avec Windows, par ex.). Cette catégorie comprend notamment les jetons OTP, les solutions OTP basées sur un TPM, les implémentations de FIDO2 (par ex. Passkeys) dépourvues de possibilités de synchronisation et d'exportation des clés, ainsi que Swisscom Mobile ID. Si les informations d'authentification sont utilisées comme jeton de fédération, elles doivent être, d'une part, protégées contre les attaques visant leur

<sup>43</sup> La norme informatique I050 définit quatre niveaux de confiance (*Level of Assurance*, LoA), qui peuvent servir à fixer les exigences minimales de sécurité à imposer aux moyens d'authentification et de preuve d'identité qui seront utilisés. Cependant, comme il n'existe pas de classification selon les LoA des moyens d'authentification et de preuve d'identité actuellement disponibles et en usage, on utilisera ici, à titre transitoire, une classification simple qui met l'accent sur quelques aspects de sécurité techniques.



intégrité et, d'autre part, liées au contexte de l'utilisateur (par ex. session) d'une manière correspondant à l'état de la technique. Il s'agit par exemple de l'identité SSO/la fédération SSO du portail SSO et des tickets Kerberos des forêts utilisateurs, si ceux-ci ont été émis sur la base d'une authentification de l'utilisateur avec un certificat de classe B délivré par la SG-PKI.

- d) **Élevé+**: les moyens d'authentification et de vérification d'identité répondent aux exigences du niveau «élevé» (y c. les exigences applicables au protocole de fédération). En outre, tant le module matériel que le processus d'enregistrement sous-jacent doivent être reconnus pour être utilisés par l'administration fédérale. Cette catégorie ne comprend que les certificats de classe B délivrés par la SG-PKI sur des cartes à puce.

Les exemples cités dans le texte et figurant sous forme de résumé dans le tableau B.1 ne constituent pas une liste exhaustive.

Niveau de sécurité	Exemples de moyens d'authentification et de vérification d'identité
<b>Faible</b>	<ul style="list-style-type: none"> <li>• Nom d'utilisateur et mot de passe</li> <li>• «jeton au porteur» (par ex. cookies)</li> </ul>
<b>Moyen</b>	<ul style="list-style-type: none"> <li>• Nom d'utilisateur et mot de passe avec code de vérification envoyé par SMS<sup>44</sup></li> <li>• Nom d'utilisateur et mot de passe liés à un appareil</li> <li>• Solution logicielle OTP (par ex. Google Authenticator)</li> <li>• Implémentations de FIDO2 (par ex. Passkeys) offrant des possibilités de synchronisation et d'exportation des clés</li> <li>• Certificat logiciel délivré par la SG-PKI (classe C, D ou E)</li> <li>• Tickets Kerberos de la forêt de ressources du service informatique standard Bureautique</li> <li>• «Jeton au porteur» tel que JWT transmis par SAML ou OIDC/OAuth</li> </ul>
<b>Élevé</b>	<ul style="list-style-type: none"> <li>• Jeton (token) OTP (par ex. RSA, Vasco, etc.)</li> <li>• Solution OTP basée sur un TPM</li> <li>• Implémentations de FIDO2 (par ex. Passkeys) dépourvues de possibilités de synchronisation et d'exportation des clés</li> <li>• Swisscom Mobile ID</li> <li>• Identité SSO/fédération SSO du portail SSO</li> <li>• Tickets Kerberos des forêts utilisateurs (SG-PKI<sup>45</sup>)</li> <li>• Jeton SAML émis dans le cadre de l'eIAM <sup>45</sup></li> </ul>
<b>Très élevé</b>	<ul style="list-style-type: none"> <li>• Certificat sur carte à puce délivré par la SG-PKI (classe B)</li> </ul>

**Tableau B.1:** Niveaux de sécurité de quelques moyens d'authentification et de preuve d'identité

<sup>44</sup> En principe, les procédures d'authentification basées sur l'envoi d'un SMS ne devraient être utilisées qu'en l'absence d'une meilleure solution.

<sup>45</sup> Le texte indique que tant les tickets Kerberos que les jetons SAML doivent avoir été émis sur la base d'une authentification de l'utilisateur avec un certificat de classe B établi par la SG-PKI.

Fondamentalement, un niveau de sécurité ne peut pas être amélioré en cumulant plusieurs moyens d'authentification et de vérification d'identité de même niveau. Ainsi, un certificat logiciel délivré par la SG-PKI reste, par exemple, au niveau de sécurité «moyen» même s'il est combiné avec un nom d'utilisateur et un mot de passe avec code de vérification envoyé par SMS.

## **Annexe C: Réglementation de zone «Domaine de réseau bleu»**

### **C.1 Exigences et prescriptions relatives aux systèmes informatiques**

<sup>1</sup> Le domaine de réseau bleu et la zone de services partagés (*shared service zone*, SSZ) sont encore disponibles pour des raisons de rétrocompatibilité. La SSZ est soumise à une réglementation de zone.

<sup>2</sup> Tant la réglementation de zone de l'annexe avec toutes les dérogations (autorisations exceptionnelles) et les accords<sup>46</sup> que la matrice d'accès de l'annexe D s'appliquent jusqu'à ce que les aspects de propriété du domaine de réseau soient clarifiés et que les directives correspondantes soient édictées.

<sup>3</sup> Un système informatique peut être géré dans le domaine de réseau bleu s'il remplit les exigences de sécurité visées à l'art. 16 LSI et à l'art. 27 OSI.

### **C.2 Exigences et prescriptions relatives au domaine de réseau bleu**

<sup>1</sup> Le domaine de réseau bleu peut être segmenté.

<sup>2</sup> Une subdivision en sous-zone au sens du ch. 2, al. 2, let. j, est possible.

### **C.3 Exigences et prescriptions relatives à la communication autorisée**

#### **C3.1 Communication interne**

<sup>1</sup> La communication interne peut être réalisée directement. Elle n'est soumise à aucune restriction allant au-delà d'une segmentation réseau.

#### **C.3.2 Communication externe**

<sup>1</sup> La communication externe ne doit pas être réalisée directement, mais doit passer par un ou plusieurs PEP (par ex. dans une PEZ).

<sup>2</sup> Il faut s'assurer qu'un système informatique du domaine de réseau bleu ne peut pas entretenir simultanément plusieurs communications externes avec des systèmes informatiques d'autres zones.

<sup>3</sup> Les exigences et prescriptions suivantes s'appliquent aux communications entrantes:

- a) Seuls des protocoles qui sont publiés et standardisés ou pour lesquels il existe un serveur reverse proxy digne de confiance peuvent être utilisés en tant que tels. Les

---

<sup>46</sup> Il est question ici d'un accord avec les Services du Parlement.

protocoles et formats de données SOAP/XML, REST/XML et/ou REST/JSON doivent être employés pour les services web.

- b) La communication est réalisée grâce à un serveur reverse proxy qui (i) authentifie la personne initiant la communication, (ii) protège le trafic des données et (iii) enregistre et évalue rapidement les données secondaires correspondantes. Dans le cas des services web, une authentification des processus (consommateurs et fournisseur de ces services) sur la base de certificats SSL/TLS reconnus suffit, et la protection du trafic des données doit être exécutée grâce à une vérification du contenu des messages<sup>47</sup> ainsi qu'à une authentification et un cryptage transparents des données reposant sur HTTPS.
- c) Un accès illimité au réseau est uniquement possible à partir d'un système informatique exploité par une unité organisationnelle de l'administration fédérale.

<sup>4</sup> La directive de l'administration fédérale relative aux proxys web [Si004] s'applique aux communications sortantes.

---

<sup>47</sup> Si un cryptage de bout en bout entre le consommateur et le fournisseur du service web est nécessaire et si le pare-feu de ce service ne peut dès lors pas vérifier directement le contenu des messages, des mesures complémentaires devront être mises en œuvre pour garantir cette vérification au moins indirectement.

## Annexe D: Matrice d'accès du domaine de réseau bleu et de la SSZ

Les tableaux suivants sont repris de la version 4.0 de la matrice d'accès (anciennement [Si002]) et s'appliquent respectivement à l'authentification des personnes se connectant au domaine de réseau bleu et à la zone de services partagés (Shared Service Zone, SSZ) (tableau D.1) et à l'authentification des systèmes partenaires et des processus (tableau D.2). Les dérogations relatives aux applications de cyberadministration (exigence Z2.1 a) continuent de s'appliquer.

	Niveau de protection	Base (NP0)				1 (NP1)				2 (NP2)			
	Terminal d'utilisateur	CF	CF	TT	TT	CF	CF	TT	TT	CF	CF	TT	TT
	Méthode d'accès	NW	RA	NW	RA	NW	RA	NW	RA	NW	RA	NW	RA
Domaine de réseau bleu	Hard crypto token	o	o	n	o	o	o	n	o	o	o	n	o
	OTP	o	o	n	o	o	o	n	o	o	o	n	o
	OTP sans appareil	n	o	n	o	n	o	n	o	n	n	n	n
	Soft crypto token	n	n	n	n	n	n	n	n	n	n	n	n
	Mot de passe ou NIP	n	n	n	n	n	n	n	n	n	n	n	n
SSZ	Hard crypto token	o <sup>48)</sup>	o	n	o	o <sup>50)</sup>	o	n	o	o <sup>50)</sup>	o	n	o
	OTP	o <sup>50)</sup>	o	n	o	o <sup>50)</sup>	o	n	o	o <sup>50)</sup>	o <sup>50)</sup>	n	o
	OTP sans appareil	n	o	n	o	n	o	n	o	n	n	n	n
	Soft crypto token	n	o	n	o	n	o	n	o	n	n	n	n
	Mot de passe ou NIP	n	o	n	o	n	o	n	o	n	n	n	n

Tableau D.1: Authentification de personnes se connectant au domaine de réseau bleu ou la SSZ

	Niveau de protection	Base (NP0)		1 (NP1)		2 (NP2)	
	Méthode d'accès	NW	RA	NW	RA	NW	RA
Domaine de réseau bleu / SSZ	Hard crypto token	n	o	n	o	n	o
	OTP / OTP sans appareil	Aucune application pratique					
	Soft crypto token	n	o	n	o	n	o <sup>49)</sup>
	Mot de passe ou NIP	n	o <sup>50)</sup>	n	n	n	n

Tableau D.2: Authentification de systèmes partenaires et des processus correspondants

<sup>48</sup> Seul cas d'application: administration de systèmes via Admin-LAN (zone de gestion FP).

<sup>49</sup> Autorisé uniquement pour l'accès à Sedex et à d'autres applications par l'intermédiaire desquelles seuls des messages standardisés peuvent être échangés et/ou des processus définis peuvent être suivis.

<sup>50</sup> Admis uniquement pour les données télémétriques (instruments de mesure).