Kanton Bern
Canton de Berne

Instruction

sur la

protection de base en matière de sécurité de l’information et de cybersécurité (IPSIC)

Date	16.12.2024
Version	2.0
Statut	réceptionné
Classification	Non classifié
Auteurs	Sascha Tarli / Daniel Lörtscher
Nom du fichier	ICSGW-fr.docx
N° de document	416978
N° d’affaire	2018.KAIO.621

Éditeur : Office d’informatique et d’organisation (OIO) du canton de Berne

L'Office d'informatique et d'organisation (OIO),

vu l'article 12, alinéa 1, lettre c de l'ordonnance de Direction du 3 janvier 2011 concernant la sûreté de l'information et la protection des données (OD SIPD)[1] en corrélation avec l'article 11d, alinéa 3 de l'ordonnance du 18 octobre 1995 sur l'organisation et les tâches de la Direction des finances (Ordonnance d'organisation FIN ; OO FIN)[2],

édicte l'instruction suivante :

Art. 1 Objet et but

[1] La présente instruction fixe les exigences en matière de protection de base au sens de l'article 5, alinéa 4 OD SIPD pour les ressources TIC, les informations et les données personnelles des autorités cantonales en vue de garantir la sécurité de l'information et des données.

[2] Si les exigences SIPD sont poussées, il convient de mettre en œuvre, outre la protection de base, les mesures de protection décrites dans le concept SIPD.

Art. 2 Champ d'application et utilisation

[1] La présente instruction s'applique aux autorités cantonales visées à l'article 4, alinéa 2 de la loi du 7 mars 2022 sur l'administration numérique (LAN)[3].

[2] Elle s'applique également aux autres organes cantonaux chargés de tâches publiques dès lors qu'ils utilisent des ressources TIC des autorités cantonales au sens de l'article 32, alinéa 1 LAN.

[3] Si les autorités acquièrent des ressources TIC auprès de tiers mandatés (ci-après « fournisseurs de prestations »), ceux-ci doivent en principe être tenus, dans le cadre d'un contrat et sur la base des dispositions des annexes 2 à 6 pertinentes dans le cas concret, en particulier des conditions générales du canton de Berne relatives à la sécurité de l'information et à la protection des données (CG SIPD), de garantir la protection de base.

[4] Si l'alinéa 3 n'est que partiellement applicable en raison de la position du prestataire sur le marché ou si celui-ci entend garantir la protection de base par d'autres mesures que celles requises dans les annexes 2 à 6, les risques correspondants doivent être indiqués dans l'analyse SIPD ainsi que dans le concept SIPD. Il faut se fonder pour ce faire sur la preuve, fournie par le soumissionnaire au moment de son offre, dans laquelle il doit documenter la garantie de la protection de base (art. 5, al. 4) malgré les dérogations à l'IPSIC. Des mesures adaptées doivent être mises en œuvre pour ramener les risques à un niveau supportable ; conformément à l'article 5, alinéa 5 OD SIPD, le concept SIPD doit fournir la preuve que les responsables des autorités compétentes acceptent les risques résiduels.

Art. 3 Annexes

[1] La présente instruction comprend les annexes suivantes, qui décrivent les exigences en matière de protection de base du canton de Berne :

Annexe 1 : Objets à protéger, classification et niveaux de protection ;

[1] OD SIPD ; RSB 152.040.2
[2] OO FIN ; RSB 152.221.171
[3] LAN ; RSB 109.1

Annexe 2 : Exigences en matière de protection de base des ressources TIC, des informations et des données personnelles (protection de base) ;
Annexe 3 : Protection de base pour le traitement de données sur mandat ;
Annexe 4 : Conditions générales du canton de Berne relatives à la sécurité de l’information et à la protection des données (CG SIPD).
Annexe 5 : Utilisation des facteurs d’authentification
Annexe 6 : Procédures cryptographiques

Art. 4 Définitions

a) **Ressources TIC :** les biens et services des technologies de l’information et de la communication (TIC), y compris le matériel et les logiciels (art. 4, al. 3, lit. a LAN).

b) **Informations :** données, sous quelque forme que ce soit, relatives à des faits et non à des personnes.

c) **Données personnelles :** données, sous quelque forme que ce soit, relatives à une personne physique ou morale, identifiée ou identifiable (art. 2, al. 1 LCPD).

d) **Sécurité de l’information et des données :** état de garantie de la confidentialité, de la disponibilité, de l’intégrité et de la traçabilité des ressources TIC, des informations et des données personnelles.

e) **Moyen d’authentification :** objet matériel ou numérique contrôlé par une personne physique et utilisé pour prouver l’identité (authentification) de celle-ci ; p. ex. une clé cryptographique, un secret ou une caractéristique biométrique.

f) **Incident de sécurité :** événement qui compromet la confidentialité, la disponibilité, l’intégrité ou la traçabilité des ressources TIC, des informations ou des données personnelles.

g) **Vulnérabilité :** faiblesse ou erreur dans une ressource TIC pouvant potentiellement conduire à un incident de sécurité.

Art. 5 Définition et respect des exigences en matière de protection de base

[1] Pour chaque ressource TIC, les autorités définissent les exigences requises en matière de protection de base à partir d’une analyse SIPD conformément à l’article 5, alinéa 2 OD SIPD.

[2] Si l’analyse SIPD révèle qu’une ressource TIC doit satisfaire à des exigences plus élevées que la protection de base, ces exigences SIPD poussées sont décrites dans un concept SIPD.

[3] Les exigences en matière de protection de base qui ne sont pas ou que partiellement remplies doivent également être mentionnées en tant que risques dans le concept SIPD, qui doit aussi décrire la manière de les éviter, de les réduire ou de les accepter.

[4] Les autorités ainsi que les fournisseurs de prestations doivent pouvoir prouver que les exigences en matière de protection de base sont satisfaites.

[5] Pour l’analyse SIPD et le concept SIPD, les autorités utilisent les modèles arrêtés et publiés par l’OIO.

Art. 6 Niveau de protection

[1] Les ressources TIC, les informations et les données personnelles sont des valeurs dont la protection doit être suffisamment élevée par rapport à leur importance et à la menace qu’elles représentent (niveau de protection).

[2] Les ressources TIC, les données personnelles et les informations doivent être classifiées par les autorités en fonction de leur importance et de la menace qu’elles représentent. Selon la classification, un niveau de protection compris entre 0 et 3 est nécessaire. La protection de base garantit les niveaux de protection 0 et 1 (cf. annexe 1).

[3] Le respect d’un certain niveau de protection suppose la mise en place des mesures correspondantes de protection technique, organisationnelle, physique et personnelle.

Art. 7 Classification des informations

[1] La classification des informations protège les intérêts publics et privés suivants :

a) la capacité de décision et d’action des autorités,
b) l’ordre public et la sécurité.

[2] Les autorités classifient les informations dont la prise de connaissance par une personne non autorisée peut nuire aux intérêts publics visés à l’alinéa 1. La classification comporte les échelons suivants :

a) « INTERNE », si l’information dont une personne non autorisée prend connaissance peut nuire aux intérêts publics,
b) « CONFIDENTIEL », si l’information dont une personne non autorisée prend connaissance peut nuire considérablement aux intérêts publics,
c) « SECRET », si l’information dont une personne non autorisée prend connaissance peut nuire gravement aux intérêts publics.

[3] La classification doit se limiter au strict nécessaire et être si possible temporaire.

[4] Les niveaux de protection nécessaires pour chaque degré de classification sont définis à l’annexe 1.

Art. 8 Disposition transitoire pour les ressources TIC et contrats existants

[1] Les autorités adaptent les ressources TIC et les contrats existants aux exigences en matière de protection de base lors de la prochaine acquisition ou modification, mais au plus tard quatre ans après l’entrée en vigueur de la présente instruction.

Art. 9 Abrogation d’instructions

[1] L’instruction d’exécution de l’OIO relative à l’ordonnance de Direction concernant la sûreté de l’information et la protection des données (IE-SIPD) du 18 mars 2024 est abrogée au 31 décembre 2024.

[2] Les instructions suivantes de l’OIO sont abrogées au 31 décembre 2024 :

a) Instruction du 25 août 2021 régissant l’utilisation des facteurs d’authentification (RII 1.3.004)
b) Instruction sur les procédures cryptographiques du 28 juin 2022.

Art. 10 Entrée en vigueur

[1] La présente instruction entre en vigueur le 1er janvier 2025.

Berne, le 16 décembre 2024

Office d’informatique et d’organisation

Beat Jakob
01.02.2025 14:39
Geregeltes elektronisches Siegel · www.be.ch/signatur
Cachet électronique réglementé · www.be.ch/signature

chef de l’office

Historique du document

Contrôle de validation

Version	Nom	Date	Remarques
0.5	SG FIN	20.03.2024	Approbation du projet à l’intention de Consultation
0.44	CD OIO	26.08.2024	Arrêté, sous réserve du contrôle par le BPD
0.44	Ueli Buri	04.09.2024	Contrôle BPD
1.0	Beat Jakob	05.09.2024	Signature
2.0	CD OIO	16.12.2024	Arrêté avec annexes 5 et 6

Kanton Bern
Canton de Berne

Annexe 1 à l'IPSIC

Objets à protéger, classification et niveaux de protection

Date	16.12.2024
Version	2.0
Statut du document	réceptionné
Classification	Non classifié
Auteur	Sascha Tarli
Nom du fichier	ICSGW Anhang 1 Schutzniveaus-fr
N° de document	422479410927
N° d'affaire	2024.KAIO.76

Éditeur : Office d'informatique et d'organisation (OIO)

Les autorités doivent garantir la sécurité de l'information et des données en prenant les mesures nécessaires de protection organisationnelle, technique, personnelle et physique. Chaque objet à protéger, qu'il s'agisse d'une ressource TIC, d'une information ou de données personnelles, doit être soumis à une évaluation de son besoin de protection. Il faut ensuite mettre en place le niveau de protection correspondant en adoptant des mesures de protection adéquates.

Les niveaux de protection sont les mêmes pour la sécurité de l'information et la sécurité des données. Ils vont de 0 à 3 (y compris après l'entrée en vigueur de la loi sur la sécurité de l'information et la cybersécurité [LSIC][1] et de l'ordonnance sur la sécurité de l'information et des données [OSID][2]).

Loi sur la sécurité de l'information et la cybersécurité (LSIC) (projet)		**Ordonnance sur la sécurité de l'information et des données OSID (projet)**	**Loi sur la protection des données LCPD**
Protection des intérêts de l'État		**Mesures dédiées à la sécurité de l'information et des données**	**Protection des intérêts des personnes physiques**
Ressources TIC	Informations	Mesures de protection selon l'état de la technique	Données personnelles
Très haute protection	SECRET	Niveau de protection 3	Données personnelles représentant une menace grave pour la sécurité des individus (intégrité corporelle, vie, liberté)
Haute protection	CONFIDENTIEL	Niveau de protection 2	Données personnelles sensibles et données personnelles confidentielles (secret professionnel, secret fiscal, etc.)
Protection de base	INTERNE	Niveau de protection 1	Données personnelles générales
	Non classifié	Niveau de protection 0	Données non personnelles (hors champ de protection de la LCPD)
Contrôle de sécurité relatif aux personnes (CSP) selon la LSIC par l'autorité d'engagement		Dispositions d'exécution pour la LSIC et la LCPD	Examen de la fiabilité conformément à la loi sur le personnel par l'autorité d'engagement

Les objectifs de protection de la LSIC sont à distinguer de ceux de la loi sur la protection des données (LCPD) :

a) La LSIC protège l'État contre les troubles illégaux de sa liberté de décision et de son action.
b) La LCPD protège les personnes contre les atteintes illégales à leur personnalité.

Ces deux objectifs sont atteints en déterminant le besoin de protection de chaque objet à protéger, en attribuant la désignation ou la classification correspondante au sens de l'article 7 IPSIC et en mettant en œuvre le niveau de protection adéquat[3].

[1] LSIC, après 1re lecture au Grand Conseil le 5 décembre 2024
[2] Projet en cours de consultation au Grand Conseil, à titre illustratif, avec la LSIC (version de juillet 2024) ; version française encore indisponible
[3] Cas particulier : le niveau de protection des informations et des données personnelles est fixé à 0 si celles-ci ont été publiées par une autorité ou sont destinées à l'être. Exemple : données sur l'appartenance d'un membre du Grand Conseil à un parti dans une intervention ou un procès-verbal du Grand Conseil.

Historique du document

Contrôle de validation

Version	Nom	Date	Remarques
0.5	SG FIN	20.03.2024	Approbation du projet à l'intention de consultation
0.17	CD OIO	26.8.24	Arrêté, sous réserve du contrôle par le BPD
0.17	Ueli Buri	4.5.24	Contrôle BPD
1.0	Beat Jakob	5.9.24	Signature OIO
2.0	CD OAIO	16.12.2024	Arrêté avec annexe 5 et 6

Kanton Bern
Canton de Berne

Annexe 2 à l'IPSIC

Exigences en matière de protection de base des ressources TIC, des informations et des données personnelles (protection de base)

Date	16.12.2024
Version	2.0
Statut du document	réceptionné
Classification	Non classifié
Auteur	OIO
Nom du fichier	ICSGW Anhang 2 Anforderungen an den Grundschutz von ICT-Mittel, Informationen und Personendaten-fr.docx
N° de document	422028410927
N° d'affaire	2024.KAIO.76

Éditeur : Office d'informatique et d'organisation (OIO)

1. Exigences générales en matière de protection de base

Les autorités doivent mettre en œuvre ces exigences ou, si elles recourent à des prestations TIC de tiers mandatés (ci-après fournisseurs de prestations), veiller par voie contractuelle à leur mise en œuvre (art. 2, al. 1 et 2 IPSIC).

ID	Exigence	Description
1	Sécurité organisationnelle	
1.1	Organisation	
1.1.1	Lignes directrices en matière de sécurité de l'information	Les comités directeurs des autorités ainsi que leurs fournisseurs de prestations doivent avoir adopté des lignes directrices en matière de sécurité de l'information (analogues à la norme ISO 27001) et défini les responsabilités en lien avec la sécurité de l'information et des données. Les collaboratrices et collaborateurs des deux parties ainsi que les éventuels sous-traitants doivent être informés à ce sujet. Les lignes directrices doivent être révisées chaque année.
1.1.2	Séparation des tâches incompatibles (Segregation of Duties)	Les tâches, les compétences et les responsabilités (TCR) doivent être structurées de telle sorte que les tâches incompatibles en raison de conflits d'intérêts, par exemple les tâches opérationnelles ainsi que le contrôle de celles-ci, soient réparties entre différentes personnes. En cas de tâches incompatibles, il convient d'établir et de documenter la séparation des tâches.
1.1.3	Gestion des incidents de sécurité	Des procédures efficaces et un triangle TCR clair sont établis et documentés afin de garantir une réaction rapide et efficace aux incidents de sécurité. Les autorités et les fournisseurs de prestations désignent un interlocuteur en cas d'incident de sécurité et définissent les modalités de sa disponibilité.
1.1.4	Obligation de signaler les incidents de sécurité et les vulnérabilités	Un signalement est obligatoire en cas d'incident de sécurité au sens de l'article 4, lettre f IPSIC (par analogie avec l'art. 74d LSI[1], en lien avec l'art. 18 P-OCyS[2]), en particulier dans les cas suivants : 1. l'incident a provoqué des interruptions dans les ressources TIC qui touchent des collaboratrices et collaborateurs ou des tiers ; 2. l'autorité concernée ou le fournisseur de prestations ne peut maintenir son activité qu'en fonctionnement de secours ; 3. des informations importantes pour l'activité sont modifiées ou publiées par des personnes non autorisées ;

[1] Loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI, FF 2023 2296) ; cette partie n'est pas encore en vigueur.
[2] Projet du 22 mai 2024 en vue de la consultation sur l'ordonnance fédérale sur la cybersécurité (OCyS)

		4. l’incident a entraîné une manipulation ou une fuite d’informations ; 5. il n’a pas été détecté pendant plus de 90 jours, en particulier si des indices laissent penser qu’il a été exécuté en vue de préparer une cyberattaque ; 6. l’incident est lié à des actes de chantage, de menace ou de contrainte et donc dirigé contre l’autorité ou le fournisseur de prestations, y compris leur personnel. Les incidents de sécurité doivent être signalés au plus tard dans les 24 heures et les vulnérabilités au sens de l’article 4, lettre g IPSIC dans les 48 heures suivant leur découverte. Le contenu du signalement doit satisfaire aux exigences du P-OCyS.
1.1.5	Transfert du stockage et/ou du traitement des données	Le stockage et/ou le traitement des données peut être transféré uniquement vers un pays offrant un niveau de protection adéquat des données conformément à l’annexe 1 de l’ordonnance fédérale du 31 août 2022 sur la protection des données (ordonnance sur la protection des données, OPDo)[3]. Sinon, le fournisseur de prestations doit signaler le transfert à l’autorité au moins 60 jours avant le délai de résiliation contractuel.
1.2	**Gestion des informations**	
1.2.1	Classification des informations	Les informations et les données personnelles doivent être classifiées par les autorités conformément à l’article 7 IPSIC et protégées conformément à l’annexe 1 à l’IPSIC au moyen de mesures de protection organisationnelle, technique, physique et personnelle selon le niveau de protection nécessaire.
1.2.2	Élimination sécurisée des supports de données	Avant l’élimination de supports de données, il convient de s’assurer de façon vérifiable que l’ensemble des informations et des données personnelles ont été effacées de manière irrécupérable. L’élimination doit être conforme au besoin de protection des informations (classe de protection 2 au minimum selon la norme DIN 66399) ou à une norme équivalente.
1.2.3	Changement sécurisé des supports de stockage	En cas de changement des supports de stockage à des fins de maintenance, sur demande de l’autorité mandante ou à l’échéance du contrat, une élimination sécurisée au sens du chiffre 1.2.3 ci-avant des données de

[3] Annexe 1 à l’OPDo ; RS 235.11

		contenu et des données secondaires de l'autorité mandante, y compris des sauvegardes éventuelles, doit être effectuée. Cet effacement des données doit être attesté au moyen d'un rapport.
1.2.4	Archivage et effacement	L'archivage et l'effacement d'informations et de données personnelles sont effectués conformément aux règles fixées contractuellement. En l'absence de règles contractuelles, le fournisseur de prestations doit s'informer auprès de l'autorité mandante, avant l'effacement de données, au sujet de la stratégie d'archivage et d'effacement et des éventuelles conditions légales. Les données qui ne sont plus nécessaires ou qui ont été détournées de leur but doivent être effacées de manière démontrable et irrécupérable.
1.3	**Contrats**	
1.3.1	Sécurité de l'information et des données dans les contrats conclus avec les fournisseurs de prestations	Les fournisseurs de prestations doivent s'engager contractuellement à respecter les exigences en matière de sécurité de l'information et des données et être tenus de soumettre également leurs sous-traitants à ces exigences.
1.4	**Gestion de la continuité des services informatiques**	
1.4.1	Garantie de la continuité des activités	Les autorités ainsi que leurs fournisseurs de prestations doivent veiller à l'existence d'une stratégie de gestion de la continuité des services informatiques pour les ressources TIC dont ils sont responsables. Une telle stratégie garantit que les ressources TIC restent en service aussi longtemps que nécessaire même en cas de situation extraordinaire. En cas d'interruption, la stratégie garantit que la remise en service s'effectue aussi rapidement que nécessaire.
2	**Sécurité des personnes**	
2.1	**Sécurité du personnel**	
2.1.1	Aptitude et fiabilité du personnel et des fournisseurs de prestations	Les autorités et leurs fournisseurs de prestations font appel uniquement à des spécialistes appropriés et dignes de confiance. En cas d'engagement ou d'affectation de personnes, les autorités et les fournisseurs de prestations procèdent au préalable à des vérifications à leur sujet conformément à un processus de recrutement fixé par écrit et sur la base du CV et des certificats de qualification.

		La fiabilité du personnel est contrôlée avant l'engagement ou l'affectation puis à intervalles réguliers. L'étendue et la périodicité du contrôle est fonction du risque associé à la mise à contribution du personnel.
2.1.2	Déclarations de confidentialité	Avant de leur donner l'accès à des ressources TIC, des informations ou des données personnelles dont le niveau de protection est fixé à 2 selon l'annexe 1 relative à l'article 6 IPSIC, l'autorité doit enjoindre les collaboratrices et collaborateurs des fournisseurs de prestations (y c. de leurs sous-traitants) au respect de la confidentialité au moyen d'une déclaration ou d'une convention de confidentialité et les informer des conséquences en cas de violation de celle-ci. Les collaboratrices et collaborateurs des autorités doivent être rendus attentifs par leur supérieur hiérarchique, sous une forme compréhensible, au secret de fonction imposé par la loi (art. 58 de la loi du canton de Berne sur le personnel[4], art. 320 du code pénal[5]).
2.2	**Formation**	
2.2.1	Habilitation du personnel à la sécurité de l'information et à la protection des données	Les autorités et les fournisseurs de prestations doivent veiller à ce que leurs collaboratrices et collaborateurs soient régulièrement formés, de manière adaptée à leurs tâches et à leur niveau hiérarchique, à la garantie de la sécurité de l'information et de la protection des données.
3	**Sécurité physique**	
3.1	Protection des ressources TIC, des informations et des données personnelles	Les ressources TIC, les informations et les données personnelles utilisées par le fournisseur de prestations pour l'autorité doivent être protégées selon l'état de la technique (ISO 27'002:2022, réf. 7.1 à 7.9, cf. chap. 3 de la présente annexe). Si cela n'est pas possible, la sécurité doit être garantie par d'autres mesures et l'autorité responsable doit en être notifiée.
4	**Sécurité technique**	
4.1	**Contrôle des accès**	
4.1.1	Limitation de l'accès et procédures de connexion sécurisées	L'accès aux ressources TIC se fait par une procédure de connexion (authentification) adaptée au niveau de protection (cf. chap. 2 Niveaux de sécurité pour les moyens d'authentification). L'accès est possible uniquement sur la base d'un concept des droits d'utilisateur fondé sur des rôles d'utilisateurs. Sur le plan technique, les ressources TIC doivent être conçues de manière à imposer les directives en

[4] LPers, RSB 153.01
[5] CP, RS 311.0

		matière de mots de passe conformément à l'annexe 5 « Utilisation des facteurs d'authentification ». Pour les authentifications de machine à machine, il convient de recourir à des procédures d'authentification basées sur des certificats.
4.1.2	Vérification des droits d'accès	Les droits d'accès aux ressources TIC, en particulier les droits privilégiés des fournisseurs de prestations, doivent être administrés dans le cadre d'un processus documenté et ils doivent être tenus à jour. Il convient de n'accorder aux utilisateurs et aux personnes disposant des droits d'administrateur que les droits nécessaires à l'accomplissement de leurs tâches (principe Least Privilege). L'utilité, la nécessité et l'adéquation des droits d'accès doivent être contrôlés chaque année. Les droits qui ne sont plus nécessaires doivent être supprimés. Les fournisseurs de prestations définissent par écrit et, sur demande de l'autorité, publient la liste des personnes pouvant accéder aux ressources TIC avec les droits d'administrateur (concept des droits d'utilisateur).
4.1.3	Gestion des facteurs d'authentification	L'annexe 5 « Utilisation des facteurs d'authentification » s'applique.
4.1.4	Authentification des utilisateurs via Internet	Dans le cas d'une authentification par Internet (p. ex. via une solution de type Software as a Service), l'utilisateur doit recourir à une authentification à plusieurs facteurs (au moins deux facteurs).
4.1.5	Accès à distance des fournisseurs de prestations	Les fournisseurs de prestation peuvent accéder à distance aux ressources TIC si les conditions suivantes sont réunies : a) L'accès se fait par un compte utilisateur personnel ; b) Le moyen d'authentification utilisé garantit au minimum le niveau de protection 1 conformément au chapitre 2 de la présente annexe « Niveaux de sécurité pour les moyens d'authentification » ; c) Le compte d'utilisateur d'un fournisseur de prestations mandaté est limité dans le temps et/ou son utilisation est enregistrée et la journalisation est vérifiée périodiquement ; d) L'accès s'effectue via un Jump Host (serveur intermédiaire utilisé pour l'authentification) ; e) La connexion réseau utilisée pour l'accès est cryptée selon l'état actuel de la technique. Toute dérogation doit être notifiée à l'autorité.
4.1.6	Compte d'administrateur	Les comptes d'administrateurs

		a) doivent être configurés avec les droits minimaux requis ; b) ne peuvent être utilisés que pour les activités d'administration (dans un but précis) ; pour les autres activités, un compte standard doit être utilisé ; c) doivent être contrôlés chaque année quant à leur utilité, leur nécessité et leur adéquation ; d) doivent pouvoir être associés à une personne physique unique, identifiée et vérifiée ; e) doivent être enregistrés, surveillés et évalués ; f) ont un mot de passe enregistré sous forme cryptée qui doit rester confidentiel.
4.1.7	Compte d'utilisateur de service	Les comptes d'utilisateurs de service impersonnels pour des processus automatisés a) doivent être configurés avec les droits minimaux requis ; b) ne peuvent être utilisés que pour les activités du service défini ; c) doivent être contrôlés chaque année quant à leur utilité, leur nécessité et leur adéquation ; d) doivent être documentés de manière compréhensible au moyen des indications suivantes : • but du compte de service, • personne responsable du compte, • responsable suppléant·e du compte, • personnes bénéficiant des droits d'accès. e) Les exigences en matière de mots de passe sont les mêmes que pour les comptes administrateur. Si le mot de passe ne peut pas être modifié chaque année pour des raisons techniques, il doit comporter au minimum 32 caractères.
4.1.8	Compte d'utilisateur test	Les comptes d'utilisateurs test a) doivent être identifiables en tant que tels et porter le nom de la personne responsable ; b) ne doivent à aucun moment permettre l'accès à des données de production de l'administration cantonale ; c) ne doivent pas inclure de droits privilégiés.
4.2	**Cryptographie**	
4.2.1	Utilisation de procédures cryptographiques	Les exigences fixées dans l'instruction sur les procédures cryptographiques[6] doivent être remplies. Le degré

[6] Instruction du CST du 28 juin 2022 sur les procédures cryptographiques (interne à l'OIO sur Confluence)

		de confidentialité et d'intégrité doit correspondre au besoin de protection des ressources TIC, informations et données personnelles. Elles doivent être sécurisées au moyen de procédures cryptographiques adéquates tenant compte du lieu d'utilisation.
4.3	**Sécurité de l'activité**	
4.3.1	Documentation	Pour les ressources TIC, une documentation à jour dans la langue requise et sous une forme facile à lire doit être présentée aux autorités. Si les ressources TIC sont fournies ou exploitées par des fournisseurs de prestations, la documentation, y compris relative aux prestations des sous-traitants, doit être garantie contractuellement. La documentation doit couvrir la durée de vie entière des ressources TIC et contenir les données suivantes : a) l'architecture du réseau et du système ; b) les composants, fonctions et paramètres importants pour la sécurité ; c) la gestion des clés lors de l'utilisation de procédures cryptographiques ; d) les processus lors des modifications, de la maintenance, des réparations, des éliminations et des pertes ; e) les prestations des sous-traitants et l'importance de celles-ci pour la sécurité. f) L'accès à la documentation doit être garanti aux autorités même en cas de panne des ressources TIC.
4.3.2	Gestion des changements	En cas de changement planifié, l'impact du changement sur la sécurité de l'information et des données doit être évalué par l'autorité mandante. Il doit être validé dans le cadre d'une procédure d'autorisation et sa mise en œuvre doit être enregistrée de manière compréhensible. Les changements qui sont mis en œuvre sans avoir été planifiés doivent être contrôlés sans délai et documentés.
4.3.3	Gestion des capacités	Les capacités nécessaires des ressources TIC doivent faire l'objet d'une estimation et d'une surveillance. Elles doivent être coordonnées avec les autorités mandantes et mises à disposition à temps.
4.3.4	Séparation des environnements de développement, de test et d'intégration des environnements de production	L'environnement de production des ressources TIC doit être séparé des autres environnements. Les mesures de séparation correspondantes sont documentées de manière compréhensible.
4.3.5	Protection contre les programmes malveillants	Les ressources TIC doivent être protégées contre les programmes malveillants (maliciels). La solution utilisée

		à cet effet doit être tenue à jour en permanence vis-à-vis des attaques à contrer. Les exploitants de ressources TIC (autorités ou fournisseurs de prestations) doivent disposer d'un concept de protection contre les maliciels, qui règle : a) les processus et les responsabilités ; b) la mise à jour des logiciels de protection contre les maliciels ; c) la définition des priorités et de la périodicité de la numérisation (p. ex. clients, serveurs, stockage des données) ; d) la mise en œuvre technique ; e) la procédure d'élimination des maliciels et l'évaluation de l'ampleur des dommages.
4.3.6	Journalisation des activités et événements importants pour la sécurité	Les événements importants pour la sécurité doivent être enregistrés de manière compréhensible et protégés contre tout traitement non autorisé. Les enregistrements doivent être conservés de manière à pouvoir être évalués.
4.3.7	Procédures documentées de sauvegarde et de restauration des données	Les autorités responsables des ressources TIC veillent à la mise en œuvre des procédures définies et testées en vue de la sauvegarde et de la restauration des données individuelles, de la ressource TIC et des configurations correspondantes. La mise en œuvre de ces procédures doit être vérifiable. La stratégie de sauvegarde doit prévoir un principe multigénérationnel (sauvegarde quotidienne, hebdomadaire ou mensuelle). La capacité de restauration et la cohérence des sauvegardes doivent être testées de manière régulière et vérifiable. Toute perte de données à la suite d'une restauration de données doit être signalée dans un rapport, qui sera mis à la disposition de l'autorité mandante.
4.3.8	Sauvegarde des données critiques	Lorsqu'une perte de données peut entraîner des répercussions graves sur les autorités et sur l'accomplissement de leurs tâches, il convient de procéder à la sauvegarde des données selon le principe multigénérationnel et à une sauvegarde hors ligne selon la technique « Write once read many » (WORM) ou à l'aide d'un découplage physique du réseau. Les données sauvegardées doivent être disponibles même en cas d'attaque par rançongiciel et leur intégrité doit être garantie.

4.3.9	Heure du système	L’heure du système doit être synchronisée de manière centralisée et ne peut être modifiée que par la personne compétente en la matière.
4.3.10	Protection de l’intégrité	L’intégrité des composants logiciels utilisés sur les ressources TIC doit être garantie, p. ex. à l’aide de signatures numériques ou de sommes de contrôle.
4.3.11	Pas d’installation ni d’exécution non autorisée de logiciels sur les terminaux TIC	Seuls des logiciels vérifiés et autorisés peuvent être installés et exécutés sur les terminaux TIC (ordinateurs portables, PC, serveurs, etc.). Il convient de faire cesser l’exécution de logiciels non vérifiés sur les terminaux TIC.
4.3.12	Mise en œuvre rapide des correctifs et mises à jour de sécurité	Pendant toute leur durée d’utilisation, les ressources TIC ainsi que leurs composants (p. ex. bibliothèques logicielles, firmware, pilotes, middleware et systèmes d’exploitation) doivent faire l’objet d’une maintenance et d’un entretien dont la mise en œuvre est rapide et la régularité vérifiable. Cela comprend notamment l’installation régulière de mises à jour opérationnelles ou de sécurité et de correctifs (patchs). Il convient de mettre en place des processus permettant de garantir un testing et une correction rapide des erreurs. L’installation de patchs de sécurité dans les services/systèmes existants tient compte des risques et des fenêtres de maintenance convenues contractuellement. Si les patchs correspondants ne sont pas disponibles, d’autres mesures de protection appropriées doivent être prises en fonction de la vulnérabilité ou de la menace.
4.3.13	Examen des vulnérabilités et des faiblesses	Avant et pendant leur utilisation, les ressources TIC doivent être régulièrement contrôlées en fonction de leur besoin de protection et de leur degré d’exposition à Internet afin d’identifier les éventuelles vulnérabilités. Si cela s’avère nécessaire, elles devront être renforcées.
4.3.14	Utilisation de terminaux mobiles	L’accès aux ressources TIC et le traitement des données par les fournisseurs de prestations sont autorisés uniquement sur les appareils gérés et sûrs (p. ex. End Point Security ou sécurité des points d’accès, cryptage du disque, Remote Wipe, protection contre les maliciels, mises à jour de sécurité). En cas de perte d’appareils mobiles, un processus de sécurité réglementé doit être mis en œuvre.
4.3.15	Interruptions de service	En cas de panne de service, l’événement doit être signalé immédiatement aux autorités mandantes et celles-ci doivent être informées régulièrement de l’évolution de la situation. Après la reprise du service, un rapport doit

		être rendu dans un délai raisonnable afin d'informer au sujet de l'événement.
4.4	**Sécurité du réseau**	
4.4.1	Trafic réseau	Si le protocole utilisé le permet (p. ex. https, ldaps, sftp, ssh), le trafic réseau doit toujours avoir lieu de manière cryptée. Il doit être conforme à la Network Security Policy du canton de Berne.
4.4.2	Réseaux pour l'administration	Les accès administratifs aux systèmes TIC de l'autorité mandante doivent s'effectuer à partir d'un réseau dédié et être sécurisés par des Jump Hosts ou au moyen d'une authentification à facteurs multiples. Les accès administratifs doivent être documentés et présentés à l'autorité mandante sur demande de celle-ci. La durée de conservation est régie par l'article 4 ODSC[7] relatif aux données administrées.
4.5	**Développement et maintenance**	
4.5.1	Développement	Lors du développement d'applications, il faut veiller à a) conserver le code source de manière sûre en réglementant clairement et en contrôlant de manière compréhensible l'accès aux référentiels correspondants ; b) surveiller les processus Build et n'exécuter les modifications dans la Build Pipeline que sous supervision ; c) tester régulièrement les logiciels quant aux vulnérabilités et aux fonctionnalités ; d) garantir à tout moment l'intégrité des logiciels (p. ex. à l'aide de signatures numériques). e) L'adaptabilité ou l'interchangeabilité des procédures cryptographiques utilisées doit être garantie. f) Pour les macros Office, les lettres c) et d) s'appliquent.
4.5.2	Configuration et paramétrage	Avant leur première mise en service, les ressources TIC doivent être configurées et paramétrées de façon à a) être protégées contre tout accès non autorisé ; b) être renforcées sur le plan technique ; c) être exploitées 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).

[7] Ordonnance du canton de Berne sur les données secondaires de communication (ODSC, RSB 153.011.5)

4.5.3	Utilisation de données de production dans les systèmes de test, de formation et de développement	Aucune copie d'informations et de données personnelles issues des systèmes de production ne doit en principe être utilisée dans les systèmes de test, de formation et de développement. Les exceptions doivent être décrites dans le concept SIPD et accompagnées de mesures de traitement des risques et elles doivent être soumises à un contrôle préalable. Les fournisseurs de prestations veillent à l'effacement, selon un processus standardisé, des fichiers de données après leur transfert (copies) et des données des systèmes de test peu après la fin des tests.
4.5.4	Logiciels vérifiés	Les logiciels ne peuvent être enregistrés que sur des terminaux TIC (ordinateurs portables, PC, serveurs, etc.) qui proviennent de sources fiables et dont l'absence de failles de sécurité et de maliciels a été contrôlée.
4.5.5	Maintenance planifiée	Les fenêtres de maintenance prévues doivent être communiquées aux autorités mandantes au moins 30 jours ouvrables à l'avance.

2. Niveaux de sécurité pour les moyens d'authentification

Il convient en principe de respecter les normes TIC[8] du canton de Berne relatives à l'infrastructure « Single Sign-On », aux méthodes d'authentification et au « raccordement à un fournisseur d'identité (IdP) ». Les exemples cités ne sont pas exhaustifs et sont résumés dans le tableau.

Niveau de protection selon l'IPSIC	Méthodes d'authentification possibles
0	• Nom d'utilisateur et mot de passe • Jetons au porteur (p. ex. cookies)
1	• Nom d'utilisateur et mot de passe avec code de vérification envoyé par SMS[9] • Nom d'utilisateur et mot de passe liés à un appareil (TPM ou jeton cryptographique) • Solution logicielle OTP (One-Time Password) (p. ex. application Microsoft Authenticator) • Certificat logiciel • Tickets Kerberos des forêts de ressources • Jetons au porteur transmis via SAML (Security Assertion Markup Language) ou OIDC (OpenID Connect) / OAuth (Open Authorization) tels que JSON Web Token (JWT)
2	• Jeton OTP (p. ex. RSA, Vasco) • Solution OTP basée sur un TPM (p. ex. Single-Sign-On du BE-PTC) • Jeton FIDO2 • Swisscom Mobile ID • SwissID
3	• Solution PKI propre ou solution PKI de la Confédération

3. Sécurité physique

Les exigences décrites en détails dans la norme ISO 27002:2022: réf. 7.1 à 7.9, comprennent les thèmes suivants (les chapitres de l'ancienne version sont également mentionnés à titre indicatif) :

Version 2022	Ancienne version de 2013	Thème
7.1	11.1.1	Périmètre de sécurité physique
7.2	11.1.2, 11.1.6	Contrôle d'accès physique
7.3	11.1.3	Sécurisation des bureaux, locaux et installations
7.4	Pas de référence	Surveillance de la sécurité physique
7.5	11.1.4	Protection contre les menaces physiques et environnementales
7.6	11.1.5	Travaux dans les domaines de la sécurité
7.7	11.2.9	Environnement de travail épuré et verrouillage de l'écran
7.8	11.2.1	Placement et protection des appareils et des équipements
7.9	11.2.6	Sécurité des appareils, des équipements et des valeurs à l'extérieur des locaux

[8] Normes TIC du canton de Berne
[9] En principe, les procédures d'authentification basées sur les SMS ne doivent être utilisées que s'il n'existe pas de meilleure solution.

Historique du document

Contrôle de validation

Version	Nom	Date	Remarques
0.2	SG FIN	20.03.2024	Approbation du projet à l’intention de Consultation
0.41	CD OIO	26.08.2024	Arrêté, sous réserve du contrôle par le BPD
0.41	Ueli Buri	04.09.2024	Contrôle BPD
1.0	Beat Jakob	05.09.2024	Signature OIO version d
1.0	Beat Jakob	16.10.2024	Signature OIO version f
2.0	CD OIO	16.12.2024	Arrêté avec annexes 5 et 6

Kanton Bern
Canton de Berne

Annexe 3 IPSIC

Protection de base pour le traitement de données sur mandat

Date	26.08.2024
Version	2.0
Statut du document	réceptionné
Classification	Non classifié
Auteurs	Daniel Lörtscher / Sascha Tarli
Nom de fichier	ICSGW Anhang 3 Grundschutz Auftragsdatenbearbeitung-fr
N° de document	422029410927
N° d'affaire	2024.KAIO.76

Éditeur : Office d'informatique et d'organisation (OIO)

1. Objet

La présente annexe 3 à l'IPSIC définit les exigences relatives au traitement d'informations et de données personnelles par des tiers mandatés par les autorités (ci-après fournisseurs de prestations). Les ressources TIC utilisées par les fournisseurs de prestations doivent satisfaire aux exigences de l'IPSIC, annexes comprises.

La société Bedag Informatique SA est la propriété du canton de Berne. Ses obligations, notamment en matière de sécurité de l'information et des données, sont décrites au préalable séparément dans la Stratégie de propriétaire 2024 Bedag Informatique SA et dans les dispositions d'exécution (en allemand) correspondantes. Ces deux documents contraignants datés du 13 décembre 2023 font partie du cadre réglementaire des TIC de l'administration cantonale. Ils priment les dispositions contractuelles.

2. Exigences de sécurité

Les exigences de sécurité pour chaque niveau de protection sont décrites à l'annexe 1 à l'IPSIC.

Les mesures décrites pour les niveaux de protection 0 et 1 correspondent aux exigences de la protection de base pour le traitement de données sur mandat. Il a été renoncé à une description générale et abstraite des exigences du niveau de protection 3. Ces exigences doivent être définies en fonction des risques dans le concept SIPD de façon à compléter le niveau de protection 2.

ID	Exigences de sécurité	Niveau de protection 0	Niveau de protection 1	Niveau de protection 2
1	Lieu du traitement et du stockage des données (y c. en cas de redondance et de sauvegarde)	Monde entier	Les États, les territoires, les secteurs spécifiques d'un État et les organisations internationales offrant un niveau de protection adéquat sont mentionnés à l'annexe 1 à l'ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo)[1]	
2	For et droit applicable	Aucune exigence	Suisse	
3	Informations sur les demandes d'enquête des autorités publiques	Aucune exigence	Les fournisseurs de prestations ainsi que leurs sous-traitants doivent publier leurs obligations légales de communiquer les données à des autorités extracantonales ou étrangères.	
4	Informations sur les certifications et rapports d'audit existants	Aucune exigence	Mise à disposition des certifications et rapports d'audit existants. A minima : Preuve du respect de la protection de base conformément à l'IPSIC ou norme ISO/IEC 27001 La certification ISO27001 n'est pas équivalente à notre protection de base. Sans preuve du respect de cette dernière, une analyse des risques est donc requise.	Mise à disposition des certifications et rapports d'audit existants. A minima : Preuve du respect de la protection de base conformément à l'IPSIC ou norme ISO/IEC 27001 norme ISO 27017 norme ISO 27018 Les certifications ISO ne sont pas équivalentes à notre protection de base. Sans preuve du respect de cette dernière, une analyse des risques est donc requise.
5	Informations sur les conditions de service (Terms of Service)	Consultable en ligne en tant que Terms of Service pour tous les utilisateurs finaux.		

[1] OPDo ; RS 235.11

6	Gestion des données secondaires	Aucune exigence	Informations transparentes sur l'ensemble des données de journalisation et de télémétrie générées par le service et par les utilisateurs, sur la finalité de leur utilisation, sur les groupes autorisés à y accéder et sur le lieu et la durée de leur conservation.	
7	Données dédiées à l'assistance et aux tests	Aucune exigence	Les données dédiées à l'assistance et aux tests doivent toujours, même dans le cas des organisations d'assistance qui appliquent le modèle Follow the Sun, rester dans des pays offrant un niveau de protection adéquat des données au sens de l'annexe 1 à l'OPDo. Les données de test et d'assistance doivent être effacées de manière irrécupérable immédiatement après utilisation.	
8	Séparation des données des autres clients et conception technique des services en nuage	Les fournisseurs de prestations peuvent démontrer, sur la base de l'architecture choisie et de la documentation mise à disposition, que le service proposé assure une séparation adéquate par rapport aux autres clients. Sur demande, les fournisseurs de prestations mettent à disposition gratuitement les concepts, architectures et documentations.		
9	Emplacement Identity Store	Dans des pays offrant un niveau de protection adéquat des données au sens de l'annexe 1 à l'OPDo.		
10	Droits d'accès	En cas d'accès temporairement nécessaire par les fournisseurs de prestations, les droits d'accès correspondants sont modifiés ou retirés rapidement et au plus tard après 14 jours.		
11	Cryptage des données de contenu (Data at Rest)	Aucune exigence	Toutes les données de contenu doivent être stockées sous forme cryptée.	Toutes les données de contenu sont enregistrées sous forme cryptée. Si les clés privées utilisées pour le cryptage ne sont pas connues exclusivement de l'autorité, les fournisseurs de prestations doivent s'engager contractuellement à les utiliser uniquement avec l'accord exprès de l'autorité.
12	Sécurité du réseau	Utilisation de pare-feu et de systèmes IDS/IPS (Intrusion Detection System / Intrusion Prevention System). En cas d'exigence de disponibilité accrue, il convient de prévoir en complément une protection DDoS (Distributed Denial of Service).	Utilisation de pare-feu et de systèmes IDS/IPS ainsi que d'un pare-feu d'application (XML/WAF) ou d'un modèle Zero Trust. En cas d'exigence de disponibilité accrue, il convient de prévoir en complément une protection DDoS.	

13	Communication cryptée	La transmission des données ainsi que toute autre communication entre les fournisseurs de prestations et les autorités, entre les emplacements en nuage et au sein de ceux-ci, ainsi qu'avec les éventuels sous-traitants des fournisseurs de prestations doivent être effectuées conformément aux prescriptions de l'annexe 6 relative aux procédures cryptographiques.
14	Portabilité – mise à disposition des données	La possibilité doit être donnée, à intervalles réguliers et à l'échéance du contrat, d'exporter les données dans un format standard applicable en conservant toutes les relations logiques. Les éventuels frais supplémentaires doivent être publiés. Le service dispose d'une fonctionnalité permettant d'effectuer des snapshots de systèmes/containers ou d'exporter des données sans l'implication des fournisseurs de prestations par l'intermédiaire d'interfaces standardisées ou publiées (API [Application Programming Interface] et procès-verbaux).
15	Sauvegarde en dehors des services en nuage	Mise à disposition d'une interface permettant la sauvegarde des données ou des snapshots de systèmes/containers sur un autre emplacement sur site ou en nuage.

Historique du document

Contrôle de validation

Version	Nom	Date	Remarques
0.2	SG FIN	20 mars 2024	Approbation du projet à l’intention de Consultation
0.24	CD OIO	26 août 2024	Approbation sous réserve du contrôle par le BPD
0.24	Ueli Buri	4 septembre 2024	Contrôle BPD
1.0	Beat Jakob	5 septembre 2024	Signature OIO version d
1.0	Beat Jakob	16 octobre 2024	Signature OIO version f
2.0	CD OIO	16 décembre 2024	Arrêté avec annexes 5 et 6

Conditions générales du canton de Berne

relatives à la

sécurité de l'information et à la protection des données

CG SIPD BE

du 26 août 2024
révisées le 16 décembre 2024
Version 2.0

Table des matières

1. But

1.1 Les présentes conditions générales relatives à la sécurité de l'information et à la protection des données (CG SIPD) ont pour but de garantir la sûreté de l'information et des données et, partant, la protection des données lors de l'acquisition et de l'utilisation de ressources TIC par les autorités du canton de Berne.

1.2 La mise en œuvre des CG SIPD et le respect des exigences posées dans le cadre de l'instruction sur la protection de base en matière de sécurité de l'information et de cybersécurité (IPSIC) permet d'assurer la protection de base pour les ressources TIC, les informations et les données personnelles, y compris par les fournisseurs de prestations.

2. Définitions

Au sens des présentes CG, on entend par :

2.1 **Autorités :** les autorités cantonales mandantes, les autorités communales ainsi que les organes chargés de tâches publiques du canton et des communes, quelle que soit leur forme juridique (art. 4, al. 1 et 2 de la loi du 7 mars 2022 sur l'administration numérique [LAN][1]).

2.2 **Fournisseur de prestations :** une personne physique ou morale qui fournit des ressources TIC à une autorité sur mandat de celle-ci.

2.3 **Ressources TIC :** les biens et services des technologies de l'information et de la communication (TIC), y compris le matériel et les logiciels (art. 4, al. 3, lit. a LAN).

2.4 **Informations :** données, sous quelque forme que ce soit, relatives à des faits et non à des personnes (art. 4, lit. b IPSIC).

2.5 **Données personnelles :** données, sous quelque forme que ce soit, relatives à une personne physique ou morale, identifiée ou identifiable (art. 2, al. 1 de la loi du 19 février 1986 sur la protection des données [LCPD][2]).

2.6 **Sécurité de l'information et des données :** état de garantie de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des ressources TIC, des informations et des données personnelles (art. 4, lit. d IPSIC).

2.7 **Traitement :** toute activité ayant directement trait à des informations ou des données personnelles, notamment le fait de recueillir, de conserver, de modifier, de combiner, de communiquer ou de détruire des données personnelles (art. 2, al. 4 LCPD).

2.8 **Communication :** le fait de rendre des informations ou des données personnelles accessibles, notamment de les transmettre, de les publier, d'autoriser leur consultation ou de fournir des renseignements (art. 2, al. 5 LCPD).

2.9 **Incident de sécurité :** événement qui compromet la confidentialité, la disponibilité, l'intégrité ou la traçabilité des ressources TIC, des informations ou des données personnelles (art. 4, lit. f IPSIC).

[1] LAN ; RSB 109.1
[2] LCPD ; RSB 152.04

3. Assujettissement à la loi cantonale sur la protection des données

3.1 Le fournisseur de prestations prend acte que, par son activité de traitement de données sur mandat d'une autorité au sens de l'article 16 LCPD, il est soumis à la LCPD dans la même mesure que l'autorité mandante. En particulier, la communication des données personnelles à des tiers requiert l'accord exprès de l'autorité.

4. Rapport avec le contrat et avec les CG CSI

4.1 Les CG SIPD font partie intégrante du contrat conclu entre le fournisseur de prestations et l'autorité. Les accords dérogatoires sont réservés.

4.2 Les conditions générales TIC-Services de la Conférence suisse sur l'informatique (CG ANS)[3] en vigueur au moment de la conclusion du contrat font également partie du contrat. Néanmoins, les dispositions contractuelles et les CG SIPD priment.

5. Sécurité de l'information et des données

5.1 Responsabilité

5.1.1 L'autorité conserve le pouvoir décisionnel en lien avec les informations et les données personnelles traitées dans le cadre de son mandat ; cela vaut aussi bien pour les données de contenu que pour les données secondaires de communication au sens de l'article 1, alinéa 1, lettres a et b de l'ordonnance du 20 novembre 2019 sur les données secondaires de communication (ODSC)[4]. Elle conserve également la responsabilité de la protection des données et est habilitée à donner des instructions en la matière (responsabilité en matière de garantie, art. 8, al. 1 LCPD).

5.1.2 Le fournisseur de prestations veille, dans le cadre de son domaine de compétence, à la sécurité des ressources TIC, informations et données personnelles qui lui sont confiées.

5.1.3 Le fournisseur de prestations n'acquiert aucun droit sur les informations et les données personnelles traitées. Il doit mettre en œuvre efficacement les mesures SIPD et suivre les instructions de l'autorité mandante (responsabilité en matière de mise en œuvre).

5.2 Mise en œuvre de la protection de base

5.2.1 Le fournisseur de prestations met en œuvre les mesures de protection de base selon l'IPSIC en vigueur lors de la conclusion du contrat et contrôle leur efficacité de manière vérifiable. Les précisions spécifiques aux prestations sont réglées dans le contrat.

5.3 Mise en œuvre de la protection élevée conformément à l'analyse SIPD et au concept SIPD

5.3.1 S'il ressort de l'analyse SIPD de l'autorité que les informations et les données personnelles à traiter présentent un besoin de protection accru, le fournisseur de prestations doit mettre en œuvre les mesures nécessaires convenues contractuellement conformément au concept SIPD et contrôler leur efficacité de manière vérifiable (art. 5 OD SIPD[5] : analyse SIPD et concept SIPD).

[3] CG ANS, version de 2025
[4] ODSC, RSB 153.011.5
[5] OD SIPD, RSB 152.040.2

6. Traitement des données

6.1 Finalité

6.1.1 Les informations et les données personnelles ne peuvent être traitées que par les collaboratrices et collaborateurs du fournisseur de prestations qui en ont besoin pour l'exécution du contrat. Le traitement des informations et des données personnelles ne peut être effectué que dans le but défini par le contrat.

6.2 Traitement et communication d'informations ou de données personnelles

6.2.1 Sauf autorisation contraire, le fournisseur de prestations ne peut traiter ou communiquer des informations ou des données personnelles de l'autorité que pour le compte de celle-ci. Les requêtes de divulgation de données présentées par des personnes privées ou par d'autres autorités doivent être transmises sans délai à l'autorité.

6.2.2 Les mesures de contrainte prévues par les codes de procédure et ordonnées par d'autres autorités compétentes sont réservées. Dans ces cas également, dans la mesure où la loi le permet, le fournisseur de prestations doit adresser le requérant ou la requérante à l'autorité ou informer immédiatement cette dernière.

6.3 Lieu de traitement des informations et des données personnelles

6.3.1 Sauf disposition contraire du contrat, le traitement des informations et des données personnelles peut avoir lieu uniquement en Suisse ou dans un État offrant un niveau de protection adéquat des données conformément à l'annexe 1 de l'ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo)[6].

7. Sous-traitance

7.1 Le contrat détermine si, et dans quelle mesure, le fournisseur de prestations peut avoir recours à des sous-traitants qui, en exerçant directement les prestations essentielles confiées par le fournisseur de prestations, entreraient eux-mêmes dans le champ d'application des CG SIPD. S'ils sont connus au moment de la conclusion du contrat, ces sous-traitants sont mentionnés dans le contrat et leur intervention est autorisée par l'autorité.

7.2 Le fournisseur de prestations impose contractuellement à ses sous-traitants, selon le chiffre 7, la mise en œuvre des mesures de sécurité conformément au contrat principal, au concept SIPD, ainsi qu'aux CG SIPD et aux CG CSI.

8. Audits

8.1 Contrôle de la légalité

8.1.1 Pour permettre le contrôle du caractère légal de la fourniture des prestations, le fournisseur de prestations accorde un droit d'audit et de contrôle aux organes de surveillance étatique indépendants suivants, dans le cadre de leurs tâches légales :

a) autorité de surveillance compétente en matière de protection des données ;
b) organe de surveillance financière compétent.

[6] OPDo ; RS 235.11

Le fournisseur de prestations est tenu, dans le cadre des bases légales en vigueur, de collaborer avec les organes de surveillance et, en particulier, de fournir les informations et documents requis.

8.2 Contrôle des prestations

8.2.1 L'autorité peut réaliser des audits dans le domaine de la sécurité de l'information, de la protection des données, des processus et de la facturation en lien avec les prestations convenues contractuellement.

8.3 Réalisation des audits

8.3.1 La direction des audits incombe à l'autorité. Après consultation du fournisseur de prestations, elle définit

a) les objets à auditer tels que les processus, les services de base, les logiciels, les fichiers de données, les documentations et codes source, les factures de prestations ;
b) l'organisation chargée de l'audit, qui ne peut pas être un concurrent direct du fournisseur de prestations, et
c) la procédure et les modalités de l'audit.

8.3.2 L'autorité annonce en principe au moins un mois à l'avance l'exercice des droits d'audit, en précisant le thème et le calendrier de l'audit. Ce délai peut être raccourci en cas d'incident de sécurité.

8.3.3 Le fournisseur de prestations participe à l'audit à ses propres frais conformément aux instructions de l'autorité ou de l'organisation chargée de l'audit. Elle octroie à ses collaboratrices et collaborateurs ou à ses mandataires les droits d'accès et de consultation nécessaires et répond à leurs questions.

8.3.4 L'autorité soumet au secret l'organisation chargée de l'audit ainsi que ses collaboratrices et collaborateurs ou ses mandataires.

8.4 Coûts

8.4.1 Les coûts d'un audit réalisé par un tiers mandaté à cet effet sont en principe pris en charge par l'autorité. Par ailleurs, les parties assument en principe elles-mêmes les coûts générés par l'audit.

8.4.2 Si l'audit révèle que des prescriptions légales ou contractuelles ont été violées et que l'autorité chargée de l'audit a fait des constatations d'importance moyenne ou élevée, le fournisseur de prestations est néanmoins tenu de payer au canton, dans les 30 jours suivant la présentation du rapport final approuvé par l'autorité chargée de l'audit,

a) les indemnités indûment perçues (trop-perçu) à la suite de la fourniture insatisfaisante des prestations contractuelles, majorés d'un intérêt de 5 %, ainsi que
b) tous les frais internes et externes supportés par l'autorité dans le cadre de l'audit.

8.4.3 Les frais engagés pour remédier aux manquements constatés dans le cadre de l'audit sont à la charge du fournisseur de prestations.

9. Obligation de signaler et mesures immédiates en cas d'incident de sécurité ou de vulnérabilité

9.1 En cas d'incident de sécurité ou de vulnérabilité au sens de l'article 4, alinéas f et g IPSIC, le fournisseur de prestations est tenu d'informer l'autorité et de collaborer avec elle, en particulier

a) en cas d'incident de sécurité ou de vulnérabilité au sens de l'annexe 2, chiffre 1.1.4 IPSIC ou
b) si une autre autorité extracantonale ou étrangère met en œuvre des actes de contrôle ou des mesures auprès du fournisseur de prestations, dans la mesure où ceux-ci concernent des informations, des données personnelles ou des ressources TIC conformément au contrat conclu ou
c) si des ressources TIC sont retirées au fournisseur de prestations par saisie, faillite ou autre mesure d'exécution forcée ou par d'autres événements ou mesures de tiers. Le fournisseur de prestations informera immédiatement toutes les personnes responsables que le pouvoir décisionnel en lien avec les informations et les données personnelles revient exclusivement à l'autorité conformément au contrat.

Les incidents de sécurité susmentionnés doivent être signalés au plus tard dans les 24 heures et les vulnérabilités dans les 48 heures suivant leur découverte. Le contenu du signalement doit satisfaire aux exigences de l'ordonnance fédérale sur la cybersécurité.

9.2 Dans les cas susmentionnés, le fournisseur de prestations prend sans délai les mesures immédiates requises par la loi conformément à l'état actuel de la technique afin de sécuriser les informations et les données personnelles ainsi que les ressources TIC utilisées pour le traitement de celles-ci et d'éviter ou de réduire au minimum les répercussions négatives.

9.3 Le fournisseur de prestations documente à l'intention de l'autorité les incidents et les éventuelles violations de la sécurité de l'information et des données. En outre, il met en œuvre et documente les mesures qui sont nécessaires, selon l'état actuel de la technique, pour éviter que de telles atteintes ne se reproduisent.

10. Confidentialité et engagement de personnel

10.1 Les chiffres 13 et 14 des CG CSI de janvier 2020 s'appliquent, notamment les sanctions pénales et de droit privé qui y sont décrites.

11. Restitution et effacement à l'échéance du contrat

11.1 À l'échéance du contrat, le fournisseur de prestations doit restituer gratuitement à l'autorité, au format convenu ou dans un format pouvant être traité ultérieurement selon l'état actuel de la technique, l'ensemble des informations et des données personnelles en sa possession.

11.2 Les informations ou les données personnelles traitées par le fournisseur de prestations doivent être effacées gratuitement et de manière irrécupérable par ce dernier conformément aux instructions des autorités et selon les exigences du chiffre 1.2.3 de l'annexe 2 à l'IPSIC. Cette obligation s'applique également au matériel de test et au matériel mis au rebut. Le procès-verbal de l'effacement doit être présenté à la première demande de l'autorité.

* * *

Historique du document

Contrôle de validation

Version	Nom	Date	Remarques
0.5	SG FIN	20 mars 2024	Approbation du projet à l'intention de Consultation
0.31	CD OIO	26 août 2024	Arrêté CD OIO, sous réserve du contrôle par le BPD
0.31	Ueli Buri	4 août 2024	Contrôle BPD
1.0	Beat Jakob	5 septembre 2024	Signature OIO version d
1.0	Beat Jakob	16 octobre 2024	Signature OIO version f
2.0	CD OIO	16 décembre 2024	Arrêté avec annexes 5 et 6

Kanton Bern
Canton de Berne

Annexe 5 à l'IPSIC

Utilisation des facteurs d'authentification

Date	16.12.2024
Version	1.0
Statut du document	réceptionné
Classification	non classifié
Auteur	OIO
Nom du fichier	Umgang mit Authentisierungsmerkmalen-fr.docx
N° de document	432568
Numéro d'affaire	2024.KAIO.76

Éditeur : Office d'informatique et d'organisation du canton de Berne (OIO)

1. Objet, but et définitions

Objet et but

Art. 1 La présente annexe régit l'utilisation des facteurs d'authentification aux ressources TIC afin qu'elle soit uniforme.

Définitions

Art. 2 Dans cette annexe, ces termes sont définis comme suit :

a *Identification :* méthode par laquelle une personne ou un utilisateur technique prouve son identité pour accéder à une ressource TIC, en indiquant son identité numérique, par exemple son nom d'utilisateur ou d'utilisatrice et le mot de passe qui lui est associé ;

b *Authentification :* contrôle, par la ressource TIC, que les données indiquées par la personne ou l'utilisateur technique correspondent à celles qui figurent dans le fichier de données correspondant. L'accès est autorisé si les données correspondent.

c *Facteur d'authentification :* attribut permettant d'apporter la preuve de l'identité à une ressource TIC.

d *Mot de passe :* facteur d'authentification composé d'une suite de caractères.

e *Numéro d'identification personnel (code PIN) :* facteur d'authentification composé d'une suite de caractères, qui est lié à un appareil ou à un dispositif de sécurité précis et qui n'est jamais transmis sur des réseaux.

f *Facteur biométrique :* facteur d'authentification correspondant à une caractéristique individuelle et inaltérable du corps humain.

g *Dispositif de sécurité :* ressource TIC générant un mot de passe à usage unique ou contenant un facteur d'authentification complexe utilisé à des fins d'identification.

h *Compte d'administrateur :* accès à une ressource TIC qui permet d'y effectuer des modifications s'appliquant à tous les utilisateurs et utilisatrices de la ressources et qui confère des droits plus étendus que ceux des autres utilisateurs et utilisatrices.

i *Compte d'utilisateur de service :* accès à une ressource TIC qui est utilisée par une autre.

j *Compte d'administrateur intégré :* compte d'administrateur indissociable d'une ressource TIC.

2. Consignes pour les utilisateurs et utilisatrices

Principe

Art. 3 [1] Les mots de passe, les codes PIN et les dispositifs de sécurité sont personnels et confidentiels. Il est interdit de les communiquer ou de les confier à d'autres personnes.

[2] Il incombe à la personne qui les détient de conserver et d'utiliser ses mots de passe, codes PIN et dispositifs de sécurité de manière responsable.

[3] Le mot de passe ou le code PIN doit être immédiatement modifié si une autre personne en a connaissance ou au moindre soupçon que cela puisse être le cas.

[4] Toute perte de dispositif de sécurité ou d'appareil sécurisé par un code PIN ou un mot de passe doit être immédiatement signalée au Centre de services de l'OIO comme incident de sécurité.

Utilisation illégitime par des tiers

Art. 4 [1] Quiconque soupçonne que des personnes non autorisées tentent de travailler en utilisant le mot de passe d'une tierce personne doit immédiatement en informer sa hiérarchie ou la personne responsable de la ressource TIC.

[2] Si une personne saisit son mot de passe ou son code PIN en présence d'un tiers, elle doit en changer dès que possible à l'abri des regards.

Utilisation des facteurs d'authentification

Art. 5 [1] Les mots de passe et codes PIN doivent être enregistrés sous forme cryptée (p. ex. avec le gestionnaire de mots de passe « KeePass » disponible sur le poste de travail cantonal).

[2] Il convient de protéger du vol par des moyens conformes à l'état actuel de la technique :

a les mots de passe,

b les codes PIN,

c les dispositifs de sécurité,

d les appareils mobiles utilisés pour l'authentification.

Choix du mot de passe

Art. 6 Le mot de passe et le code PIN

a doivent en principe être générés automatiquement et enregistrés dans un gestionnaire de mots de passe conformément à l'article 5 ;

b doivent être différents pour chaque ressource TIC ;

c doivent être choisis de manière à n'avoir ni analogie ni relation connue avec la personne qui les utilise, afin de ne pas être faciles à deviner.

3. Conditions requises pour les systèmes et applications

Principe

Art. 7 [1] L'accès via un compte d'administrateur est contrôlé au minimum par deux facteurs d'authentification indépendants l'un de l'autre.

[2] Ces facteurs d'authentification sont choisis dans au moins deux de ces catégories :

a savoir : par exemple mot de passe ou code PIN,

b possession : par exemple ordinateur portable, dispositif de sécurité ou téléphone portable,

c corps : un facteur biométrique (p. ex. empreinte digitale).

Dispositions générales

Art. 8 Toute application doit satisfaire aux conditions suivantes :

a Elle permet à toute personne de changer ou réinitialiser son mot de passe son mot de passe à tout moment.

b Elle masque la saisie du mot de passe.

c Elle interdit la réutilisation des derniers mots de passe utilisés.

d Elle enregistre les mots de passe sous forme cryptée.

e Elle peut exiger un changement de mot de passe.

f Elle documente la procédure d'authentification conformément à une norme industrielle actuelle.

PIN

Art. 9 [1] L'utilisation d'un code PIN est autorisée dans l'un ou l'autre des deux cas suivants :

a l'authentification requiert en plus un dispositif de sécurité ou un facteur biométrique,

b l'authentification à l'aide du code PIN ne peut s'effectuer que sur un appareil déterminé, qui dans ce cas est considéré comme un dispositif de sécurité.

[2] Dans les cas décrits à l'alinéa 1, lettre b, il faut prévoir un facteur d'authentification supplémentaire au sens de l'article 7 pour l'accès via l'appareil mobile à

a des informations classées au minimum CONFIDENTIELLES,

b des données personnelles particulièrement dignes de protection,

c des données personnelles soumises à une obligation de secret particulière.

[3] Si un code PIN est utilisé, .il est possible de le remplacer par un facteur biométrique évitant de le saisir à chaque fois.

Complexité du mot de passe

Art. 10

[1] Le mot de passe

a est composé d'au moins dix caractères,

b distingue majuscules et minuscules,

c comporte au minimum un caractère appartenant à au moins trois de ces groupes :

1. lettres majuscules,
2. lettres minuscules,
3. chiffres,
4. autres caractères.

[2] Le mot de passe des comptes avec droits d'accès étendus ou des comptes d'administrateur doit comprendre au minimum quinze caractères.

[3] Le mot de passe des comptes d'utilisateur de service ou des comptes d'administrateur intégrés doit comprendre au minimum 26 caractères.

[4] Les codes PIN doivent être formés d'au moins huit caractères.

Changement de mot de passe

Art. 11

[1] Les mots de passe et les codes PIN ont en principe une durée de validité illimitée.

[2] Les mots de passe des comptes avec droits d'accès étendus et des comptes d'administrateur doivent être changés au moins une fois tous les six mois.

[3] Les mots de passe des comptes d'utilisateur de service et des comptes d'administrateur intégrés doivent être changés au moins une fois par an. S'il n'est pas possible, pour des raisons techniques, de changer une fois par an de mot de passe, alors celui-ci doit comporter au minimum 32 caractères.

[4] Le nouveau mot de passe ne doit pas pouvoir être déduit facilement de l'ancien.

[5] Si des éléments indiquent que des mots de passe ou des codes PIN ont été rendus accessibles à des personnes non autorisées, les responsables du système et des applications réinitialisent immédiatement les mots de passe ou les codes PIN des utilisateurs et utilisatrices potentiellement concernés.

Première connexion

Art. 12 Pour leur première connexion à un système, les nouveaux utilisateurs et utilisatrices reçoivent un mot de passe à usage unique.

Transmission sous forme cryptée des facteurs d'authentification

Art. 13 Les facteurs d'authentification (p. ex. nom d'utilisateur et mot de passe) ne peuvent être communiqués que séparément et doivent être cryptés lors de leur transmission sur des réseaux. Font exception les mots de passe à usage unique.

Blocage du mot de passe

Art. 14 [1] Le mot de passe ou le code PIN est bloqué après cinq saisies incorrectes.

[2] Seules les personnes responsables du système et des applications peuvent en principe débloquer le mot de passe. La personne titulaire du compte peut aussi le débloquer elle-même après s'être identifiée au moyen d'un autre mot de passe ou après avoir répondu à plusieurs questions de sécurité.

[3] Un déblocage automatique n'est possible qu'à l'issue d'un délai de 30 minutes au minimum.

[4] Après dix saisies incorrectes, les données professionnelles sont supprimées dans l'outil de gestion de la mobilité en entreprise (Enterprise Mobility Management, EMM). Les données privées sont conservées lorsque c'est techniquement possible.

4. Utilisation abusive et exceptions

Utilisation abusive

Art. 15 Si une utilisation illégitime est signalée, les personnes responsables du système et des applications déterminent s'il y a effectivement eu utilisation abusive et, le cas échéant, qui est en l'auteur. Elles engagent les mesures appropriées.

Exceptions

Art. 16 [1] Des dérogations à la présente annexe sont admises dans l'un ou l'autre des cas suivants, pour autant que le risque qui en découle reste raisonnable :

a l'instruction n'est applicable dans des applications existantes qu'au prix de charges disproportionnées ;

b le système utilisé ne permet pas la mise en œuvre intégrale de la présente instruction ;

c la réglementation des suppléances ne peut être appliquée autrement que par une identification commune.

[2] Une dérogation est valable un an au maximum. Elle peut être renouvelée.

[3] L’autorité responsable de la protection des données (art. 8, al. 1 LCPD) est compétente pour autoriser des dérogations. S’il existe plusieurs autorités responsables, cette compétence revient à celle qui veille à la protection globale des données (art. 8, al. 2 LCPD).

[4] Les responsables du système et des applications consignent les informations suivantes :

a qui a autorisé la dérogation ;

b sur quelles dispositions de la présente annexe porte la dérogation, pour quel motif et dans quelle mesure ;

c quelles ressources TIC, quelles personnes ou quels groupes de personnes sont concernés par la dérogation ;

d combien de temps dure la dérogation.

[5] Les responsables du système et des applications communiquent la dérogation avec les informations qui précèdent à la personne responsable de la sécurité informatique (RSI BE), qui en informe à son tour le délégué cantonal ou la déléguée cantonale à la sécurité informatique du canton (DSI BE).

Historique du document

Contrôle de validation

Version	Nom	Date	Remarques
1.0	CD OIO	16.12.2024	Arrêté avec l’IPSIC version 2.0

Kanton Bern
Canton de Berne

Annexe 6 à l'IPSIC

Procédures cryptographiques

Date	16 décembre 2024
Version	1.0
Statut du document	réceptionné
Classification	Non classifié
Auteur	Anton Jurt
Nom du fichier	ICSGW Anhang 6 Kryptographischen Verfahren-fr.docx
N° de document	432567
N° d'affaire	2024.KAIO.76

Éditeur : Office d'informatique et d'organisation du canton de Berne (OIO)

Sommaire

1. Dispositions générales

Art. 1 Objet

[1] La présente annexe régit l'utilisation uniforme et sûre de procédures cryptographiques lors de la mise en œuvre de ressources TIC.

[2] Elle a été élaborée sur la base des documents référencés ([1], [2], [3], [4]) dans l'optique d'être consolidée et d'offrir la possibilité d'une adaptation rapide, mais aussi d'illustrer les spécificités cantonales.

Art. 2 Définitions

1. Suites cryptographiques	Combinaisons définies permettant une communication sécurisée. Elles sont utilisées pour déterminer quels algorithmes de chiffrement sont acceptés par un serveur Web pour la transmission des données.
2. Authentification des données	Procédure cryptographique garantissant que les données envoyées ou enregistrées n'ont pas été modifiées et qu'elles proviennent effectivement de leur auteur·e.
3. Clés éphémères	Paires de clés générées et utilisées à chaque nouvelle connexion.
4. Perfect Forward Secrecy (PFS)	Méthode cryptographique de mise en accord de clés qui empêche le déchiffrement des données même après la divulgation de la clé principale.
5. Fonction de hachage	Conversion d'une chaîne de caractères en valeur ou clé numérique généralement plus courte et de longueur fixe. La valeur numérique correspond à la valeur de hachage et à un autre affichage de la chaîne de caractères d'origine. Cette valeur ne peut pas être reconstituée en sens inverse.
6. Cryptographie hybride	Combinaison d'une procédure cryptographique post-quantique et d'une procédure de chiffrement classique.
7. Secure Shell (SSH)	Protocole réseau cryptographique dédié à l'exploitation sécurisée de services réseau sur des réseaux non sécurisés.
8. Hardware Securtity Module (HSM)	Appareil périphérique interne ou externe permettant l'exécution sûre d'opérations ou d'applications cryptographiques.

2. Gestion des clés

Art. 3 Sauvegarde et archivage

[1] La gestion des clés cryptographiques doit être sécurisée. Il est essentiel d'empêcher en particulier la copie, l'utilisation frauduleuse et la manipulation de clés cryptographiques.
[2] Le matériel utilisé (carte à puce, HSM) doit être certifié afin de garantir une sauvegarde sécurisée des clés.
[3] Avant toute modification, les clés publiques doivent être sauvegardées de manière sécurisée.

Art. 4 Clés de session (clés éphémères)

[1] Toutes les clés éphémères doivent être supprimées définitivement après utilisation.
[2] Il convient de s'assurer qu'aucune copie de ces clés n'est générée.
[3] Les clés éphémères ne peuvent être utilisées que pour une seule connexion et ne doivent pas être enregistrées durablement.

Art. 5 Durée d'utilisation

[1] Le tableau ci-dessous définit la durée d'utilisation de différents types de clés.
[2] Cette durée ne doit pas être dépassée.

Durée d'utilisation des clés

Type de clé (description au chap. 7)	Durée d'utilisation	
	Durée d'utilisation initiateur Originator-Usage Period (OUP)	Durée d'utilisation récepteur Recipient-Usage Period (RUP)
1. Clé privée de signature	1 à 3 ans	
2. Clé publique de vérification de signature	Plusieurs années (selon la taille de la clé)	
3. Clé symétrique d'authentification	≤ 2 ans	≤ OUP + 3 ans
4. Clé privée d'authentification	1 à 2 ans	
5. Clé publique d'authentification	1 à 2 ans	
6. Clé symétrique de chiffrement de données	≤ 2 ans	≤ OUP + 3 ans
7. Clé symétrique d'enveloppement de clés	≤ 2 ans	≤ OUP + 3 ans
8. Clé initiale[1] symétrique	1 an	-
9. Clé privée de transport de clés	+ 2 ans[2]	
10. Clé publique de transport de clés	1 à 2 ans	
11. Clé symétrique d'accord de clés	1 à 2 ans[3]	
12. Clé statique privée d'accord de clés	1 à 2 ans[4]	
13. Clé statique publique d'accord de clés	1 à 2 ans	
14. Clé éphémère privée d'accord de clés	une transaction d'accord de clés	
15. Clé éphémère publique d'accord de clés	une transaction d'accord de clés	
16. Clé symétrique d'autorisation	≤ 2 ans	
17. Clé privée d'autorisation	≤ 2 ans	
18. Clé publique d'autorisation	≤ 2 ans	

Art. 6 Nombres aléatoires

[1] Pour générer des nombres aléatoires en vue de créer des clés cryptographiques ou des signatures, il est nécessaire d'utiliser un générateur aléatoire basé sur un matériel vérifié, à savoir un True Random Number Generator (TRNG).
[2] De surcroît, les générateurs de nombres aléatoires de l'une des classes suivantes sont autorisés : DRG.3, DRG.4, PTG.3 ou NTG.1 [9].

[1] Également appelée « clé principale » (en anglais « master key » ou « key derivation key »).
[2] Dans les applications de messagerie dans lesquelles les messages reçus sont enregistrés et décryptés ultérieurement, la durée d'utilisation de la clé privée de transport peut dépasser celle de la clé publique de transport.
[3] Dans les applications de messagerie dans lesquelles les messages reçus sont enregistrés et décryptés ultérieurement, la durée d'utilisation par le récepteur (« Recipient-Usage Period ») de la clé peut dépasser la durée d'utilisation par l'initiateur (« Originator-Usage Period »).
[4] Dans les applications de messagerie dans lesquelles les messages reçus sont enregistrés et décryptés ultérieurement, la durée d'utilisation de la clé statique privée d'échange de clés peut dépasser celle de la clé statique publique d'échange de clés.

3. Algorithmes cryptographiques et longueurs de clés

Art. 7 Procédures symétriques

[1] Pour le chiffrement symétrique, l'Advanced Encryption Standard (AES) est obligatoire.
[2] Le chiffrement par bloc doit satisfaire aux exigences suivantes :

a *Longueur de clés*
La longueur de clé doit être si possible de 256 bits, et au minimum de 128 bits. Les chiffrements par bloc autorisés sont indiqués au point 1 du tableau ci-après.

b *Modes d'exploitation*
Les modes d'exploitation autorisés sont listés au point 2 du tableau ci-après.

c *Conditions d'exploitation*
Pour les modes d'exploitation mentionnés dans le tableau, les conditions d'exploitation indiquées dans la colonne du milieu s'appliquent de façon contraignante.

d *Procédure de remplissage*
Le mode Cipher Block Chaining (CBC) nécessite une étape supplémentaire de remplissage. Les procédures de remplissage mentionnées au point 3 sont autorisées pour remplir le dernier bloc de texte en clair de façon à atteindre la taille du chiffrement utilisé.

[3] Les chiffrements de flux ou « chiffrements par flot » dédiés ne sont pas autorisés, à l'exception de l'AES en mode compteur.

1. Chiffrements par bloc autorisés

a)	**AES-128**
b)	**AES-192**
c)	**AES-256**

2. Modes d'exploitation autorisés

Il faut en principe utiliser des modes d'exploitation proposant la variante Authenticated Encryption with Associated Data (AEAD). Les exceptions sont à justifier.

Mode d'exploitation	Conditions	AEAD
a) Counter with Cipher Block Chaining Message Authentication (CCM)	Les vecteurs d'initialisation ne doivent pas se répéter durant une période de changement de clé.	oui
b) **Galois/Counter-Mode (GCM)**		oui
c) **Counter Mode (CTR)**		non
d) Counter with Cipher Block Chaining Message Authentication (CCM)	La longueur des tags d'authentification doit être au moins égale à 64 bits.	oui
e) Cipher-Block Chaining (CBC)	Les vecteurs d'initialisation doivent être imprévisibles. Cela signifie qu'un potentiel attaquant ne doit pas être en mesure de découvrir quels vecteurs d'initialisation seront utilisés ou d'influencer le choix du vecteur d'initialisation. Pour la génération de vecteurs d'initialisation imprévisibles, il faut utiliser les procédures suivantes : – **Vecteurs d'initialisation cryptés :** utilisation d'une procédure déterministe pour créer des vecteurs de pré-initialisation (p. ex. un compteur). Chiffrement du vecteur de pré-initialisation qui utilise le chiffrement par bloc et la clé adéquats ainsi que le texte de chiffrement en tant que vecteur d'initialisation. – **Vecteurs d'initialisation aléatoires :** création d'une chaîne de bits aléatoire de longueur n et utilisation de celle-ci en tant que vecteur d'initialisation. L'entropie de la chaîne de bits aléatoire doit être au moins égale à 95 bits.	non

3. Procédures de remplissage autorisées

a)	**Remplissage ISO selon la norme ISO/IEC 9797-1:2011**
b)	**Remplissage selon la RFC 5652**
c)	**Remplissage ESP selon la RFC 4303**

Art. 8 Procédures asymétriques classiques

[1] Pour un chiffrement asymétrique, seules les procédures listées dans le tableau ci-dessous sont autorisées.
[2] Pour l'algorithme de chiffrement RSA, la procédure de formatage « EME-OAEP » est obligatoire.

Procédures asymétriques autorisées

Procédure	Longueur minimale de clé [bits]	Utilisation
a) RSA	3000	Chiffrement, échange de clés, signature numérique
b) Diffie-Hellman (DH)	3000	Accord de clés
c) EC Diffie-Hellman (ECDH)	250	Accord de clés
d) ElGamal	3000	Chiffrement, accord de clés
e) DSA	3000[5]	Signature numérique
f) ECDSA	250	Signature numérique
g) DLIES	3000	Procédure de chiffrement hybride
h) ECIES	250	Procédure de chiffrement hybride

Art. 9 Procédures asymétriques post-quantiques

Pour un chiffrement post-quantique asymétrique, seules les procédures listées dans le tableau ci-dessous sont autorisées.

Procédures post-quantiques autorisées

a)	FrodoKEM-976, FrodoKEM-1344
b)	mceliece460896, mceliece6688128, mceliece8192128
c)	mceliece460896f, mceliece6688128f, mceliece8192128f

Les procédures post-quantiques mentionnées ici ne bénéficient généralement pas du même niveau de confiance que les procédures classiques bien établies, car elles n'ont pas fait l'objet de recherches aussi poussées en ce qui concerne, par exemple, la résistance des canaux auxiliaires ou la sécurité d'implémentation. En conséquence, une telle procédure ne doit être utilisée que combinée à une procédure classique. Les procédures hybrides autorisées sont les suivantes :

CatKDF, CasKDF

[5] Recommandé jusqu'en 2029 seulement, étant peu répandu et bientôt obsolète.

Art. 10 Fonctions de hachage

[1] Seules les fonctions de hachage listées au point 1, puissantes d'un point de vue cryptographique, sont autorisées.
[2] Pour générer une clé cryptographique de chiffrement à partir d'un mot de passe ou pour enregistrer un mot de passe, seules les fonctions de hachage de mot de passe listées au point 2 sont autorisées.
[3] L'utilisation de SHA1 est exclue.

1. Fonctions de hachage autorisées

Dans les premières lignes du tableau, il s'agit de SHA2 (le numéro n'est pas publié dans la version 2).

a)	SHA-256, SHA-512/256, SHA-384 et SHA-512
b)	SHA3-256, SHA3-384, SHA3-512

2. Fonctions de hachage de mot de passe autorisées

a)	Argon2
b)	bcrypt
c)	scrypt
d)	PBKDF2

Art. 11 Authentification des données

[1] Exigences concernant les procédures MAC :
a Les procédures MAC mentionnées au point 1 peuvent être utilisées en tenant compte des longueurs minimales de clés ou de tags.
b La clé utilisée pour le MAC ne doit pas être la même que pour le chiffrement.
[2] Exigences concernant les signatures numériques :
Les procédures de signature listées au point 2 et les longueurs de clés associées sont autorisées.

1. Procédures MAC autorisées

Procédure		Longueur minimale de clé [bits]	Longueur minimale de tag [bits]
a)	CMAC	256	96
b)	HMAC	256	128
c)	KMAC256	256	96
d)	GMAC	256	96

2. Procédures de signature autorisées

Procédure		Longueur minimale de clé [bits]
a)	RSA	3000
b)	DSA	3000[6]
c)	ECDSA	250

[6] Recommandé jusqu'en 2029 seulement, car peu répandu et bientôt obsolète.

Art. 12 Procédures de signature post-quantiques

[1] Pour utiliser des procédures post-quantiques, il faut en principe les combiner avec des procédures de signature classiques. Cette hybridation vise à pallier le stade de recherche moins avancé en ce qui concerne la sécurité de l'implémentation.

Art. 13 Transport et mise en accord des clés

[1] Perfect Forward Secrecy (PFS) :
Seules les procédures asymétriques d'accord de clés permettent d'atteindre la caractéristique de sécurité Perfect Forward Secrecy. Pour éviter les attaques de type « man-in-the-middle » (attaques de l'homme du milieu), l'échange de clés doit se faire de manière authentifiée, par exemple au moyen d'une signature (art. 11, ch. 2).

[2] Procédures symétriques :
Pour le transport de clés de session, toutes les procédures de chiffrement symétriques listées à l'article 7 sont autorisées. L'utilisation combinée de l'une des procédures MAC mentionnées à l'article 12, point 1 du tableau, est absolument impérative Les procédures asymétriques d'accord de clés au sens du point 1 sont autorisées.

[3] Procédures asymétriques :
Pour le transport de nouvelles clés de session, seules les procédures de chiffrement asymétriques classiques indiquées à l'article 8 sont autorisées. Pour l'accord de clés, les procédures mentionnées au point 2 doivent être utilisées.

1. Procédures d'accord de clés autorisées (procédures symétriques)
Key Establishment Mechanism 5 selon la norme ISO/IEC 11770-2:2018

2. Procédures d'accord de clés autorisées (procédures asymétriques)
a) Elliptic Curve Key Agreement of ElGamal Type (ECKA-EG)
b) Authentification d'instance avec RSA et accord de clés avec RSA
c) MTI/A0 (Two-pass Diffie-Hellman)

4. Protocoles cryptographiques

Art. 14 Transport Layer Security (TLS)

[1] Les versions TLS listées au point 1 doivent être utilisées en tant que normes minimales. Il faut privilégier les versions plus puissantes du protocole. Les versions moins puissantes du protocole TLS et les versions du protocole SSL sont interdites, y compris en tant que solutions de repli.

[2] Utilisation de suites cryptographiques :

a *TLS 1.2 :* Les suites cryptographiques listées au point 2 pour la version 1.2 du protocole sont autorisées. Si possible, il convient d'utiliser les suites cryptographiques avec Perfect Forward Secrecy.

b *TLS 1.3 :* Les suites cryptographiques listées au point 3 pour la version 1.3 du protocole sont autorisées.

[3] Les longueurs de clés minimales pour TLS doivent satisfaire aux prescriptions du chapitre 3 « Algorithmes cryptographiques et longueurs de clés ».

1. Versions TLS autorisées

a) TLS 1.2

b) TLS 1.3

2. Suites cryptographiques TLS 1.2 autorisées

Propriétés	Suites cryptographiques TLS 1.2 autorisées
a) Suites cryptographiques avec Perfect Forward Secrecy	– TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_ECDSA_WITH_AES_128_CCM – TLS_ECDHE_ECDSA_WITH_AES_256_CCM – TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 – TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 – TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 – TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 – TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 – TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 – TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
b) Suites cryptographiques sans Perfect Forward Secrecy (utilisation jusqu'en 2026)	– TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 – TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 – TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 – TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 – TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 – TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 – TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 – TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 – TLS_DH_DSS_WITH_AES_128_CBC_SHA256 – TLS_DH_DSS_WITH_AES_256_CBC_SHA256 – TLS_DH_DSS_WITH_AES_128_GCM_SHA256 – TLS_DH_DSS_WITH_AES_256_GCM_SHA384 – TLS_DH_RSA_WITH_AES_128_CBC_SHA256 – TLS_DH_RSA_WITH_AES_256_CBC_SHA256 – TLS_DH_RSA_WITH_AES_128_GCM_SHA256 – TLS_DH_RSA_WITH_AES_256_GCM_SHA384
c) Suites cryptographiques pour l'accord de clés avec des données échangées au préalable (Pre-Shared Key)	– TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 – TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384 – TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256 – TLS_DHE_PSK_WITH_AES_128_CBC_SHA256 – TLS_DHE_PSK_WITH_AES_256_CBC_SHA384 – TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 – TLS_DHE_PSK_WITH_AES_256_GCM_SHA384 – TLS_DHE_PSK_WITH_AES_128_CCM – TLS_DHE_PSK_WITH_AES_256_CCM

3. Suites cryptographiques TLS 1.3 autorisées

a) TLS_AES_128_GCM_SHA256

b) TLS_AES_256_GCM_SHA384

c) TLS_AES_128_CCM_SHA256

Art. 15 Datagram Transport Layer Security (DTLS)

[1] DTLS étant basé sur TLS, les prescriptions de l'article 14 s'appliquent. En cas d'utilisation de DTLS, il y a lieu de clarifier au préalable quelles suites cryptographiques, parmi les suites prescrites, sont compatibles avec DTLS. Les versions DTLS listées dans le tableau ci-après sont autorisées.

1. Version DTLS autorisée
TLS 1.2

Art. 16 Secure Shell (SSH)

[1] Seule la version SSH mentionnée au point 1 est autorisée.

[2] Seules les méthodes d'échange de clés (key exchange) mentionnées au point 2 sont autorisées.

[3] Seuls les algorithmes de chiffrement listés au point 3 sont autorisés.

[4] Si un chiffrement n'est pas exploité selon le mode GCM, la mise en œuvre d'une procédure MAC est obligatoire pour assurer l'intégrité. Seules les procédures listées au point 4 sont autorisées.

[5] Authentifications autorisées :

a *Authentification du serveur*
Seules les procédures mentionnées au point 5 sont autorisées pour authentifier le serveur.

b *Authentification du client*
Si le client utilise des clés d'authentification (public key authentication), celles-ci doivent correspondre à l'un des types de clés listés au point 6. La longueur minimale de clé pour l'algorithme de chiffrement RSA est définie au point 6.

1. Version SSH autorisée
SSH-2

2. Méthodes d'échange de clés autorisées
a) diffie-hellman-group-exchange-sha256
b) diffie-hellman-group15-sha512
c) diffie-hellman-group16-sha512
d) ecdh-sha2-nistp256
e) ecdh-sha2-nistp384
f) ecdh-sha2-nistp521

3. Chiffrements SSH autorisés

a) AEAD_AES_128_GCM

b) AEAD_AES_256_GCM

c) aes128-ctr

d) aes192-ctr

e) aes256-ctr

4. Procédures autorisées pour la protection MAC

a) hmac-sha2-256

b) hmac-sha2-512

5. Procédures autorisées pour l'authentification de serveur

Procédure	Longueur minimale de clé [bits]
a) ecdsa-sha2-nistp384	250
b) ecdsa-sha2-nistp521	250
c) x509v3-ecdsa-sha2-nistp256	250
d) x509v3-ecdsa-sha2-nistp384	250
e) x509v3-ecdsa-sha2-nistp521	250

6. Types de clés prescrits

a) RSA

b) Ed25519

Art. 17 Internet Key Exchange (IKE) et Internet Protocol Security (IPsec)

[1] Exigences concernant IKE

a *Versions*
Seules les versions IKE mentionnées au point 1 sont autorisées Il est obligatoire d'utiliser des certificats pour l'authentification mutuelle. Si des clés prépartagées (pre-shared keys, PSK) sont utilisées, elles doivent comprendre des lettres, des chiffres et des caractères spéciaux, et contenir au moins 20 caractères.

b *Procédures de chiffrement*
Le chiffrement des messages échangés via IKE_AUTH, CREATE_CHILD_SA ou INFORMATIONAL-Exchange doit respecter l'une des procédures mentionnées au point 2.

c *Procédures de protection de l'intégrité*
Pour protéger l'intégrité des messages échangés via IKE_AUTH, CREATE_CHILD_SA ou INFORMATIONAL-Exchange, seules les procédures mentionnées au point 3 sont autorisées.

d *Génération de clés*
La génération de clés doit être conforme à l'une des procédures listées au point 4.

e *Échange de clés*
Seuls les groupes Diffie-Hellman listés au point 5 sont autorisés pour l'échange de clés.

f *Procédure d'authentification (peer authentication)*
Pour l'authentification, l'une des procédures listées au point 6 doit être utilisée.

[2] Exigences concernant IPsec

a *Protocoles*
L'utilisation du protocole AH est interdite. Si aucun chiffrement n'est souhaité, il est obligatoire d'utiliser le chiffrement « null » avec le protocole ESP conformément au point 7, au lieu du protocole AH.

b *Chiffrement de paquet ESP*
Pour le chiffrement des paquets EPS, seules les procédures listées au point 8 sont autorisées.

c *Protection de l'intégrité ESP*
L'intégrité des paquets ESP doit être assurée au moyen de l'une des procédures listées au point 9.

[3] Security Association Lifetime et Re-Keying
La durée d'utilisation d'une Security Association (SA)[7] doit être fixée en fonction des exigences de sécurité propres à l'application. Dans les scénarios d'utilisation habituels, la IKE-SA-Lifetime doit correspondre à 24 heures maximum et la IPsec-SA-Lifetime à 4 heures maximum.

1. Version IKE autorisée pour l'échange de clés

IKEv2

2. Procédures de chiffrement IKEv2 autorisées

Les procédures ENCR_AES_CBC et ENCR_AES_CTR ne garantissent pas la protection de l'intégrité. Par conséquent, elles doivent impérativement être combinées avec une procédure de protection de l'intégrité (conformément au point 3).

Procédure	Longueur minimale de clé AES [bits]
a) ENCR_AES_CBC	256
b) ENCR_AES_CTR	256
c) ENCR_AES_GCM_16	256
d) ENCR_AES_GCM_12	256
e) ENCR_AES_CCM_16	256
f) ENCR_AES_CCM_12	256

[7] Connexion sécurisée par IPsec entre deux partenaires de communication, y compris les paramètres cryptographiques, algorithmes, clés et modes d'exploitation pour cette connexion.

3. Procédures de protection de l'intégrité autorisées

a) AUTH_AES_XCBC_96

b) AUTH_HMAC_SHA2_256_128

c) AUTH_HMAC_SHA2_384_192

d) AUTH_HMAC_SHA2_512_256

4. Procédures prescrites pour la génération de clés

a) PRF_AES128_XCBC

b) PRF_AES128_CMAC

c) PRF_HMAC_SHA2_256

d) PRF_HMAC_SHA2_384

e) PRF_HMAC_SHA2_512

5. Groupes Diffie-Hellman autorisés pour l'échange de clés

Dans la mesure du possible, il convient de toujours appliquer Perfect Forward Secrecy. Pour ce faire, un nouvel échange de clés Diffie-Hellman via CREATE_CHILD_SA est requis en tenant compte des groupes Diffie-Hellman autorisés.

ID	Groupes
15	3072-bit MODP group
16	4096-bit MODP group
19	256-bit random ECP group
20	384-bit random ECP group
21	521-bit random ECP group
28	brainpoolP256r1
29	brainpoolP384r1
30	brainpoolP512r1

6. Procédures d'authentification autorisées

Procédure	Longueur [bits]	Fonction de hachage
a) ECDSA-256 avec Kurve secp256r1	256	SHA-256
b) ECDSA-384 avec Kurve secp384r1	384	SHA-384
c) ECDSA-512 avec Kurve secp521r1	512	SHA-512
d) ECDSA-256 avec Kurve brainpoolP256r1	256	SHA-256
e) ECDSA-384 avec Kurve brainpoolP384r1	384	SHA-384
f) ECDSA-512 avec Kurve brainpoolP512r1	512	SHA-512
g) RSASSA-PSS	4096	SHA-384

h)	ECGDSA-256 avec Kurve brainpoolP256r1	256	SHA-256
i)	ECGDSA-384 avec Kurve brainpoolP384r1	384	SHA-384
j)	ECGDSA-512 avec Kurve brainpoolP512r1	512	SHA-512

7. Protocole IPsec autorisé

Encapsulated Security Payload (ESP)

8. Chiffrements de paquet ESP autorisés

Lors de l'utilisation d'ESP, le mode tunnel doit être préféré au mode transport.

Procédure	Longueur minimale de clé AES [bits]
a) ENCR_AES_CBC	256
b) ENCR_AES_CTR	256
c) ENCR_AES_GCM_16	256
d) ENCR_AES_GCM_12	256
e) ENCR_AES_CCM_16	256
f) ENCR_AES_CCM_12	256

9. Procédures de protection de l'intégrité ESP autorisées

a) AUTH_AES_XCBC_96

b) AUTH_AES_CMAC_96

c) AUTH_HMAC_SHA2_256_128

d) AUTH_HMAC_SHA2_384_192

e) AUTH_HMAC_SHA2_512_256

Art. 18 Messaging Layer Security (MLS)

MLS 1.0 est autorisé.

Suites cryptographique MLS autorisées

a) MLS_128_DHKEMP256_AES128GCM_SHA256_P256

b) MLS_256_DHKEMP384_AES256GCM_SHA384_P384

c) MLS_256_DHKEMP521_AES256GCM_SHA512_P521

5. Autres mesures de sécurité

Art. 19 Chiffrement des disques durs

S'il est impossible, pour des raisons d'efficience et/ou d'espace, d'utiliser un chiffrement avec authentification (cf. art. 7, al.2), l'utilisation du mode XTS-AES est obligatoire.

Art. 20 Bluetooth

[1] Lors de l'utilisation du bluetooth, il convient d'utiliser au minimum la version 4.2 avec un correctif actuel.

[2] Pour le bluetooth BR/EDR/HS, il faut utiliser au minimum le mode de sécurité 4, niveau 3 (Secure Simple Pairing) et, pour le bluetooth LE, le mode de sécurité 1, niveau 4.

[3] Dans la mesure du possible, la méthode « Just Works » doit être évitée pour l'appairage.

Art. 21 WLAN

Les procédures cryptographiques autorisées en lien avec le WLAN sont décrites dans le tableau ci-dessous.

Procédures cryptographiques WLAN

Mode WLAN	Domaine	Procédures autorisées
a) WPA3-Enterprise	Authentication	Plusieurs EAP
	Encryption	AES-CCMP 128
	Key derivation & confirmation	HMAC-SHA256
	Frame protection	BIP-CMAC-128
b) Mode WPA3-Enterprise à 192 bits (pour la protection de données sensibles)	Authentication	EAP TLS_ECDHE_EC-DSA_WITH_AES_256_GCM_SHA384
	Encryption	GCMP-256
	Key derivation & confirmation	HMAC-SHA384
	Frame protection	BIP-GMAC-256
c) WPA2-Enterprise	Si le mode WPA3 n'est pas pris en charge par un appareil ou un composant, il est possible de recourir au Mixed Mode avec WPA2-Enterprise.	

Art. 22 Certificats PKI

[1] Les normes de cyberadministration suivantes doivent être respectées :
a) eCH-0170 Modèle de qualité pour l'authentification des sujets [5]
b) eCH-0048 Classes de certificats PKI [6]

[2] CP/CPS en vigueur de l'autorité de certification (CA) du canton de Berne :
a) CPCPS Root-CA_BECH [7]
b) Normes CP CPS de sécurité et de certification CERT-001-BE-CH [8]

6. Liste des abréviations

Abréviation	Signification
AEAD	Authenticated encryption with associated data
AH	Authentication Header
CCM	Counter with Cipher Block Chaining Message Authentication
CBC	Cipher-Block Chaining
CTR	Counter Mode
DH	Diffie-Hellman
DLIES	Discrete Logarithm Integrated Encryption Scheme
DRG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ESP	Encapsulated Security Payload
GCM	Galois/Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware Security Module
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
MAC	Message Authentication Code
NTG	Non-physical Random Number Generator
LSIC	Loi sur la sécurité de l'information et la cybersécurité
PFS	Perfect Forward Secrecy
PTG	Physical Random Number Generator
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SA	Security Association
SSL	Secure Socket Layer
SSH	Secure Shell Protocol
SHA	Secure Hash Algorithms
TLS	Transport Layer Security
TRNG	True Random Number Generator

7. Types de clés (tableau art. 5)

Type de clés	Description
a) Clé privée de signature	Une clé privée de signature est la clé privée d'une paire de clés asymétriques utilisée par des algorithmes pour des clés publiques afin de générer des signatures numériques destinées à un usage de longue durée. Dans le cadre d'une utilisation

		conforme, les clés privées de signature peuvent être utilisées pour garantir l'authenticité et l'intégrité ainsi que la non-répudiation de messages, documents ou données enregistrées.
b)	Clé publique de vérification de signature	Une clé publique de vérification de signature est la clé publique d'une paire de clés asymétriques utilisée par un algorithme pour des clés publiques afin de vérifier les signatures numériques. L'objectif est de contrôler l'identité d'un·e utilisateur·trice et/ou l'intégrité des données, mais aussi de garantir la non-répudiation de messages, documents ou données enregistrées.
c)	Clé symétrique d'authentification	Les clés symétriques d'authentification sont utilisées avec des algorithmes de clés symétriques pour vérifier l'identité et l'intégrité de sessions de communication, de messages, de documents ou de données enregistrées. Il faut noter que, dans les modes de chiffrement et d'authentification pour un algorithme de clés symétriques, une seule et unique clé est utilisée pour l'authentification et le chiffrement.
d)	Clé privée d'authentification	Une clé privée d'authentification est la clé privée d'une paire de clés asymétriques utilisée avec un algorithme pour des clés publiques afin de garantir l'identité d'une entité en créant une session de communication authentifiée ou une autorisation de réaliser une action.
e)	Clé publique d'authentification	Une clé publique d'authentification est la clé publique d'une paire de clés asymétriques utilisée avec un algorithme pour des clés publiques afin de garantir l'identité d'une entité lorsqu'une session de communication ou une autorisation de réaliser une action est créée.
f)	Clé symétrique de chiffrement de données	Ce type de clé est utilisé avec des algorithmes de clés symétriques afin de protéger la confidentialité de données (c.-à-d. de chiffrer des données de texte en clair). La même clé est utilisée également pour annuler la protection de la confidentialité(c.-à-d. pour déchiffrer les données). Il faut noter que, dans les modes de chiffrement authentifiés pour un algorithme de clés symétriques, une seule et unique clé est utilisée pour l'authentification de la source et pour le chiffrement.
g)	Clé symétrique d'enveloppement de clés	Les clés symétriques d'enveloppement de clés (key wrapping keys) sont utilisées avec des algorithmes de clés symétriques afin de chiffrer d'autres clés. La clé d'enveloppement utilisée pour chiffrer une clé permet aussi l'inversement de la procédure de chiffrement (c.-à-d. le déchiffrement de la clé chiffrée).
h)	Clé initiale symétrique	Une clé initiale ou clé principale symétrique est utilisée pour dériver d'autres clés symétriques (p. ex. clés de chiffrement de données ou clés d'enveloppement de clés) dans le cadre d'une procédure cryptographique symétrique.
i)	Clé privée de transport de clés	Une clé privée de transport de clés est la clé privée d'une paire de clés asymétriques utilisée pour déchiffrer les clés qui ont été chiffrées à l'aide de la clé publique correspondante. Ce type de clé est généralement utilisé pour générer des clés symétriques (p. ex. clés d'enveloppement, clés de chiffrement de données ou clés MAC) et, le cas échéant, d'autres instruments de chiffrement (p. ex. vecteurs d'initialisation).
j)	Clé publique de transport de clés	Une clé publique de transport de clés est la clé publique d'une paire de clés asymétriques utilisée pour le chiffrement de clés. Ce type de clé est utilisé pour générer des clés symétriques (p. ex. clés d'enveloppement de clés, clés de chiffrement de données ou clés MAC) et, le cas échéant, d'autres instruments de chiffrement (p. ex. vecteurs d'initialisation).
k)	Clé symétrique d'accord de clés	Ce type de clé symétrique est utilisé pour générer des clés symétriques (p. ex. clés d'enveloppement de clés, clés de chiffrement de données ou clés MAC) et éventuellement d'autres instruments de chiffrement (p. ex. vecteurs d'initialisation) dans le cadre d'un algorithme symétrique de mise en accord de clés.
l)	Clé statique privée d'accord de clés	Une clé statique privée d'accord de clés est la clé privée de longue durée d'une paire de clés asymétriques utilisée pour générer des clés symétriques (p. ex. clés d'enveloppement de clés, clés de chiffrement de données ou clés MAC) et, le cas échéant, d'autres instruments de chiffrement (p. ex. vecteurs d'initialisation).

m)	Clé statique publique d'accord de clés	Une clé statique publique d'accord de clés est la clé publique de longue durée d'une paire de clés asymétriques utilisée pour générer des clés symétriques (p. ex. clés d'enveloppement de clés, clés de chiffrement de données ou clés MAC) et, le cas échéant, d'autres instruments de chiffrement (p. ex. vecteurs d'initialisation).
n)	Clé éphémère privée d'accord de clés	Une clé éphémère (clés de session) privée est la clé privée de courte durée d'une paire de clés asymétriques utilisée une seule fois pour générer une ou plusieurs clés symétriques (p. ex. clés d'enveloppement de clés, clés de chiffrement de données ou clés MAC) et, le cas échéant, d'autres instruments de chiffrement (p. ex. vecteurs d'initialisation).
o)	Clé éphémère publique d'accord de clés	Une clé éphémère (clés de session) publique est la clé publique de courte durée d'une paire de clés asymétriques utilisée au cours d'une seule et unique transaction de clés pour générer une ou plusieurs clés symétriques (p. ex. clés d'enveloppement de clés, clés de chiffrement de données ou clés MAC) et, le cas échéant, d'autres instruments de chiffrement (p. ex. vecteurs d'initialisation).
p)	Clé symétrique d'autorisation	Une clé symétrique d'autorisation est utilisée pour octroyer des droits à une entité dans le cadre d'une méthode cryptographique symétrique. La clé d'autorisation est connue de l'entité responsable de la surveillance et de l'octroi de droits d'accès pour les entités autorisées, ainsi que de l'entité qui souhaite l'accès à certaines ressources.
q)	Clé privée d'autorisation	Une clé privée d'autorisation est la clé privée d'une paire de clés asymétriques qui sert à prouver le droit du propriétaire à des autorisations.
r)	Clé publique d'autorisation	Une clé publique d'autorisation est la clé publique d'une paire de clés asymétriques utilisée pour contrôler les autorisations pour une entité qui connaît la clé privée d'autorisation associée.

8. Documents de référence

Référence	Documents	N° archive
[1]	BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen" Version: 2024-01 (en allemand)	
[2]	BSI TR-02102-2 "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)" Version: 2024-1 (en allemand)	
[3]	BSI TR-02102-3 "Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)" Version: 2024-01 (en allemand)	
[4]	BSI TR-02102-4 "Kryptographische Verfahren: Teil 4 – Verwendung von Secure Shell (SSH)" Version: 2024-01 (en allemand)	
[5]	eCH-0170 « Modèle de qualité pour l'authentification des sujets » version 2.0	
[6]	eCH-0048 « Classes de certificats PKI » version 2.0	
[7]	CPCPS_Root-CA_BECH	(OIO) n° 166147
[8]	Normes CP CPS de sécurité et de certification CERT-001-BE-CH	(OIO) n° 188753
[9]	BSI : Functionality classes for random number generators	

Historique du document

Contrôle de validation

Version	Nom	Date	Remarques
1.0	CD OIO	16.12.2024	Arrêté avec IPSIC version 2.0