POLITIQUE DE SECURITE
DES SYSTEMES D'INFORMATION

HISTORIQUE DES MODIFICATIONS

Version	**Objet de la modification**	**Statut**
08/03/2022	Publication de la politique de sécurité des systèmes d'information de K-ElectroniK	
13/03/2022	Ajout de l'outil de cryptographie	

TABLE DES MATIERES

Partie I - Éléments stratégiques

I. Chapitre 1 - Périmètre de la PSSI

La Politique de Sécurité des Systèmes d'Information (PSSI) reflète la vision stratégique de la direction de l'entreprise K-ElectroniK en matière de sécurité des systèmes d'information et de gestion des risques SSI.

Dans le cadre du rachat de la société madrilène OBSOL, la société K-ElectroniK souhaite établir un référentiel pour urbaniser son système d'information et le maintenir à jour de manière à garantir la norme ISO 9001 et poursuivre son activité de manière pérenne.

Dans un contexte où les menaces cyber sont plus que fréquentes, il convient de disposer d'un socle fondateur de la sécurité des systèmes d'information pour garantir le fonctionnement de l'activité de K-Electronik, contrôler les cybermenaces et améliorer les pratiques informatiques au sein de la compagnie qui se développe à l'international.

Pour information, les dernières données de l'ANSSI révèle une tendance en forte hausse, avec 786 intrusions en 2020 et 1082 en 2021. Soit une progression de 37% en parallèle de la constante amélioration des acteurs malveillants.

Le rachat de l'entité OBSO doit donc amener K-ElectroniK à augmenter fortement son seuil de vigilance en terme de sécurité du système d'information.

La PSSI servira les intérêts de la compagnie K-ElectroniK, de toutes les boutiques propres de K-ElectroniK, de ses entrepôts, de son lieu de production et par conséquent de ses fournisseurs.

II. Chapitre 2 - Enjeux et orientations stratégiques

Le système d'information de K-ElectroniK doit intégrer un système déjà existant, considéré comme obsolète.

La démarche d'urbanisation doit se faire sans venir perturber l'activité, et permettre de satisfaire les clients et la Direction Générale de la compagnie.

Plus précisément, les différents services composant la compagnie doivent être en mesure de continuer leur activité :

- Le service commercial doit pouvoir répondre aux demandes des clients, chiffrer les devis, prendre leur rendez-vous et reporter de leur activité.

- Le service production doit continuer d'avoir accès aux prix des fournisseurs, gérer les plannings de production, gérer le flux opérationnel de la production, planifier les livraisons, répondre aux commandes clients dans les meilleurs délais. Les logiciels fait maison et GESTCOMS doivent pouvoir continuer de fonctionner, y compris pendant l'intégration de Madrid au SI.

- Le service RH doit continuer d'avoir accès à l'ERP RH (SMART RH), même pendant le déploiement de CEGID à Madrid.

- Le service Finance doit pouvoir continuer d'utiliser CEGID, même pendant le déploiement de CEGID à Madrid.

III. Chapitre 3 - Aspects légaux et réglementaires

Ce chapitre identifie le référentiel légal et réglementaire lié au périmètre de l'étude.

Cette PSSI se doit de respecter plusieurs textes légaux et réglementaires. Pour cela, un seul acteur en France est considéré comme LA référence de la sécurité des SI : l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Afin d'anticiper toutes les questions relatives à la certification ISO 9001, dont une partie a déjà été mise en place au sein de la société K-ElectroniK, nous prendrons comme référence toutes les pratiques et conseils d'urbanisation du SI recommandées par l'ANSSI applicables à la stratégie de développement de la société dans le cadre actuel.

Plus précisément, promulguée le 19 décembre 2013, la loi n°2013-1168 de programmation militaire (LPM) suit les orientations fixées par le Livre blanc sur la défense et la sécurité nationale 2013. Elle constitue l'outil législatif qui va permettre aux opérateurs publics et privés critiques pour la nation de mieux se protéger et à l'ANSSI et à d'autres services de l'État de mieux les soutenir en cas d'attaque informatique. Son article 22 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale et confère au Premier ministre de nouvelles prérogatives.

Textes et réglementations :

- Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

RÈGLEMENTATION APPLICABLE AUX OPÉRATIONS RELATIVES AUX MOYENS DE CRYPTOLOGIE

- Loi n° 2004-575 du 21 juin 2004 pour la confiance en l'économie numérique – Titre III De la Sécurité dans l'économie numérique – Chapitre Ier Moyens et prestations de cryptologie.

Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004 575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et prestations de cryptologie.

- Décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage.
- Arrêté du 29 janvier 2015 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie.

RÈGLEMENTATION RELATIVE AU CONTRÔLE DES EXPORTATIONS DE BIENS ET TECHNOLOGIES DOUBLE USAGE

- Règlement (CE) n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.

- Règlement délégué (UE) no 1382/2014 de la Commission du 22 octobre 2014 modifiant le règlement (CE) no 428/2009 du Conseil instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage ».

- Décret n°2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage.

- Arrêté du 13 décembre 2001 relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les États membres de la Communauté européenne de biens et technologies à double usage

IV. Chapitre 4 - Échelle de besoins

Afin d'assurer le respect des engagements pris dans cette PSSI, nous demanderons un avis externe en matière d'évaluation de la sécurité du SI.

Pour respecter la recommandation de l'ANSSI, nous ferons appel à un organisme travaillant avec la méthode EBIOS Risk Manager.

Cette méthode a été récemment validée et se distingue par une approche qui réalise une synthèse entre conformité et scénarios. Elle adopte une approche de management du risque qui part du plus haut niveau pour s'intéresser progressivement aux éléments métiers et techniques, en étudiant les chemins d'attaques possibles.

La méthode d'analyse de risque EBIOS Risk Manager est un outil pratique, pédagogique et collaboratif pour intégrer le numérique dans le management des risques.

En un mot, elle doit continuer de vivre et évoluer au contact d'une communauté d'utilisateurs déjà engagée dans cette démarche. K-ElectroniK fournira des utilisateurs internes déjà engagés dans la démarche de certification ISO 9001.

La première version de la méthode EBIOS remonte à 1995, soit à peine cinq ans après l'annonce publique de création du World Wide Web. Une première actualisation d'EBIOS a été réalisée en 2004, puis une évolution significative en 2010.

L'ANSSI a élaboré la version 2010 de la méthode EBIOS, avec le soutien du Club EBIOS, pour prendre en compte les retours d'expérience et les évolutions normatives et réglementaires. Elle introduisait aussi les concepts de biens essentiels et d'événements redoutés pour apprécier les risques de sécurité de l'information au niveau des activités de l'organisation et non plus seulement au niveau technique.

EBIOS Risk Manager est issue de cet héritage. Fruit d'une collaboration étroite, elle positionne pleinement la sécurité numérique au niveau des enjeux stratégiques et opérationnels des organisations. Elle offre ainsi un véritable cadre en matière de management du risque numérique.

En annexes, vous pourrez trouver le guide de la méthode EBIOS Risk Manager ainsi que des fiches méthodes. Le tout étant téléchargeables sur le site de l'ANSSI.

Annexes N°XX

V. Chapitre 5 - Besoins de sécurité

Afin d'anticiper les recommandations issues du résultat de la méthode EBIOS Risk Manager, nous mettons en place des outils permettant une urbanisation déjà sécurisée avec des produits et des services qualifiés par l'ANSSI.

Tous ces outils et services ont été sélectionnés dans le catalogue « liste-produits-et-services-qualifies » téléchargeable en .pdf sur le site de l'ANSSI. Vous pourrez retrouver en annexes la liste des produits ainsi que les certificats de chaque produit et service.

Ces outils et services apparaissent comme qualifié et recommandé pour de nouveaux déploiements ou de nouvelles prestations par l'ANSSI. En page 1 de ce catalogue, il est précisé comment le niveau de recommandation est calculé.

Pour être précis, K-ElectroniK instaure un niveau de sécurité du SI plus élevé en passant par les outils et services listés dans le tableau suivant :

OBJECTIF	OUTILS / SERVICES	EDITEUR
Protection du poste de travail Utilisateur	Windows 11	MICROSOFT
Protection du poste de travail Boutique et Utilisateur et Production	ZoneCentral	PRIM'X TECHNOLOGIES
Firewall	Stormshield Network Security	STORMSHIELD
Sonde de détection d'intrusion	Jizo	SESAME IT
Switchs unilatéraux sécurisés	Tap Cuivre et TAP Optique	ALLENTIS
Sauvegarde et Restauration de données	VEEAM AVAIBILITY ORCHESTRATOR	VEEAM
Cloud	Hosted Private Cloud (IaaS)	OVH SAS
Backup	Managed Veeam Backup	OVH SAS
CRM	CRM for Jira	ATLASSIAN
Gestion de projets	Jira Project Management	ATLASSIAN
Réunion de travail	Teams	MICROSOFT
Cryptographie	Hsm TrustWay Proteccio	ATOS / BULL

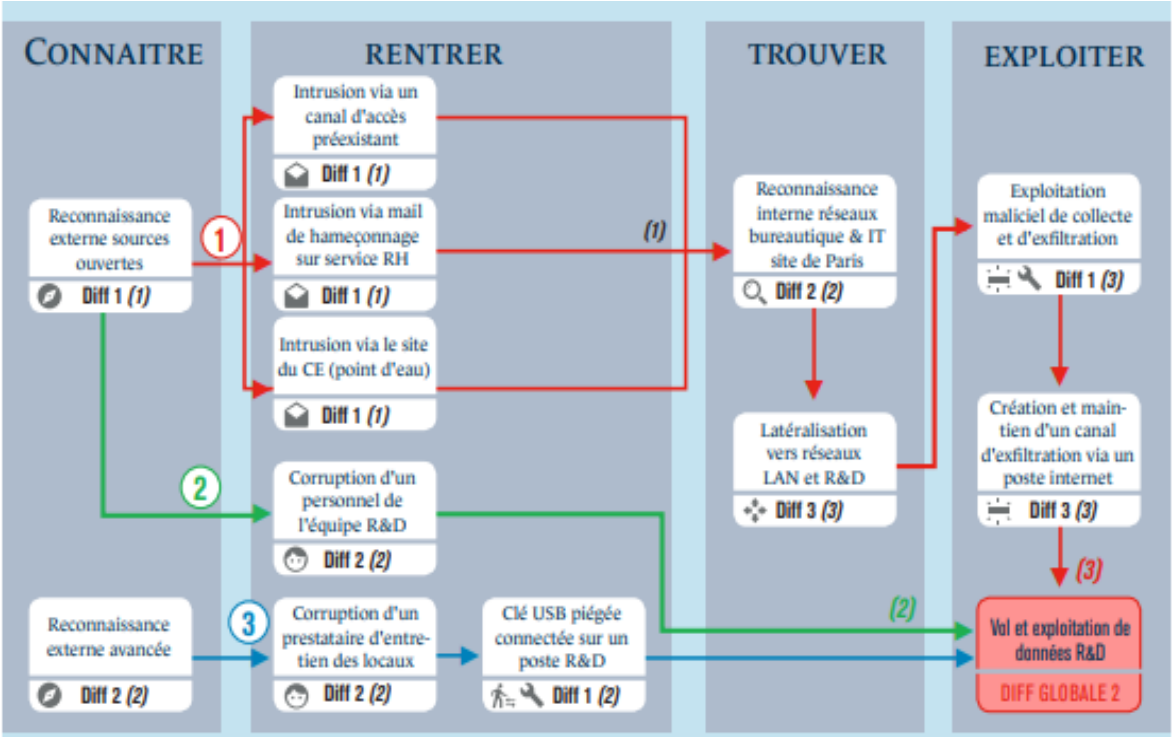
VI. Chapitre 6 – Origines des menaces

Dans le tableau suivant, nous trouverons la grille d'évaluation des menaces envisagées et possibles. L'évaluation du mode opérationnel se fait en fonction de la difficulté ainsi que par sa probabilité d'occurrence.

PROBABILITÉ DE SUCCÈS DU MODE OPÉRATIONNEL	DIFFICULTÉ TECHNIQUE DU MODE OPÉRATIONNEL				
	0 – NÉGLIGEABLE	1 – FAIBLE	2 – MODÉRÉE	3 – ÉLEVÉE	4 – TRÈS ÉLEVÉE
4 – QUASI-CERTAINE	4	4	3	2	1
3 – TRÈS ÉLEVÉE	4	3	3	2	1
2 – SIGNIFICATIVE	3	3	2	2	1
1 – FAIBLE	2	2	2	1	0
0 – TRÈS FAIBLE	1	1	1	0	0

Source : Méthode EBIOS Risk Manager - Fichier en .pdf « fiches-methodes-ebios_projet » du site de l'ANSSI – page 57.

Partie 2 – Menaces et règles de sécurité



La difficulté technique du scénario est estimée globalement à « 2 – Modéré », les modes opératoires les moins difficiles techniquement étant ceux numérotés ② et ③. Compte-tenu des probabilités de succès évaluées précédemment, il est possible d'établir la synthèse suivante :

	Probabilité succès	Difficulté technique	Vraisemblance
Chemin ①	3 – Très élevée	3 – Élevée	V2 – Vraisemblable
Chemin ②	1 – Faible	2 – Modérée	V2 – Vraisemblable
Chemin ③	2 – Significative	2 – Modérée	V2 – Vraisemblable
		Scénario global	V2 – Vraisemblable

Les trois modes opératoires envisagés dans le graphe d'attaque ont le même niveau de vraisemblance. On aboutit à une vraisemblance **« V2 – Vraisemblable »** pour le scénario. Par rapport à l'évaluation réalisée avec la méthode standard (V3), la vraisemblance estimée est moindre. La prise en compte du critère de difficulté technique apporte une pondération sur l'estimation du niveau de vraisemblance. En effet, si le mode opératoire ① apparaît comme ayant la probabilité de succès la plus élevée, il présente également une difficulté technique relativement élevée.

Source : Méthode EBIOS Risk Manager - Fichier en .pdf « fiches-methodes-ebios_projet » du site de l'ANSSI – page 58.

Exemples de types de menaces

Exemple 1 :

- Personnels, prestataires, fournisseurs susceptibles d'être animés par un esprit de vengeance

EXEMPLE : salarié mécontent licencié récemment.

- Personnels ayant fait l'objet d'un processus d'habilitation de sécurité et/ou d'une enquête, qui apporte un certain niveau d'assurance sur leur intégrité.
- Satisfaction des cibles à l'égard de leur salaire ou de leur considération au sein de l'organisation.

Source : Méthode EBIOS Risk Manager - Fichier en .pdf« fiches-methodes-ebios_projet » du site de l'ANSSI.

Exemple 2 :

- Informations sur l'entité et son écosystème facilement accessibles sur Internet (sites web, forums de discussions en ligne, réseaux socio-professionnels, etc.).
- Participation régulière de l'entité, de ses partenaires (fournisseurs, sous-traitants, clients) ou d'anciens salariés à des salons professionnels ou forums en ligne **(Note 3)**.
- Usage du chiffrement dans les relations de l'entité avec l'extérieur, dans les services offerts par l'entité à l'extérieur **(Note 4)**.
- Compétences particulières nécessaires pour la recherche des informations, compte tenu du domaine d'activité de l'entité **(Note 5)**.

Note 3 : beaucoup d'informations sont aisément obtenues au travers d'approches informelles dans les milieux professionnels. Lors de démarches commerciales notamment, de nombreuses informations sensibles sont souvent échangées
EXEMPLE : faux client, réponse à un appel d'offres.
Note 4 : les protocoles de chiffrement permettent de limiter l'impact des fuites de données, en particulier vis-à-vis des interceptions ou détournements de trafic.
Note 5 : des attaques nécessitant de fortes compétences dans un ou plusieurs domaines d'expertise en lien avec l'activité de la cible

Source : Méthode EBIOS Risk Manager - Fichier en .pdf« fiches-methodes-ebios_projet » du site de l'ANSSI.

Exemple 3 :

Les critères diffèrent selon la technique d'intrusion utilisée par l'attaquant.

ATTAQUE FRONTALE DE SERVICES

- Nombre de services et/ou d'applicatifs exposés sur Internet.
- Services exposés ayant fait l'objet d'une homologation ou d'un processus de développement intégrant la sécurité.
- Technologie de filtrage mise en place

EXEMPLE : **REVERSE PROXY, WAF, etc. (Note 6).**

- Utilisation de biens supports « de frontière » certifiés ou qualifiés **(Note 7)**.

Note 6 : ces outils fonctionnent sur la base de signatures et sont assez efficaces pour détecter les attaques les plus grossières.

Note 7 : une technologie qualifiée ou certifiée est plus robuste vis-à-vis des exploits, car elle a fait l'objet d'une qualité de développement accrue, avec une attention importante donnée à la sécurité, et a fait l'objet de tests d'intrusion

EXEMPLE : certification de sécurité de premier niveau, critères communs, agrément, référentiel général de sécurité.

Source : Méthode EBIOS Risk Manager - Fichier en .pdf« fiches-methodes-ebios_projet » du site de l'ANSSI.

Exemple 4 :

- Maîtrise des interventions des prestataires : gestion des accès aux locaux, supervision, journalisation, etc.**(Note 13)**.
- Processus d'habilitation de sécurité ou enquête préliminaire réalisés pour les prestataires qui interviennent sur site.
- Utilisation de matériels informatiques gérés par l'organisation pour que les prestataires effectuent les interventions sur les biens supports de l'entité

EXEMPLE : valise de maintenance, clé USB de *firmware* **(Note 14).**

- Nombre et facilité d'accès des points de connexion physique et logique aux réseaux informatiques de l'entité.
- Existence de liens de télémaintenance ou de connexions avec des réseaux tiers sécurisés.
- Existence d'une politique de sécurité pour la chaîne d'approvisionnement industrielle.

EXEMPLE : exigences contractuelles, audits de sécurité des fournisseurs, etc.

- Existence de mesures de sécurité pour la maintenance des biens supports **(Note 15)**.
- Existence de mesures de sécurité physique et type de technologie utilisée : contrôle d'accès

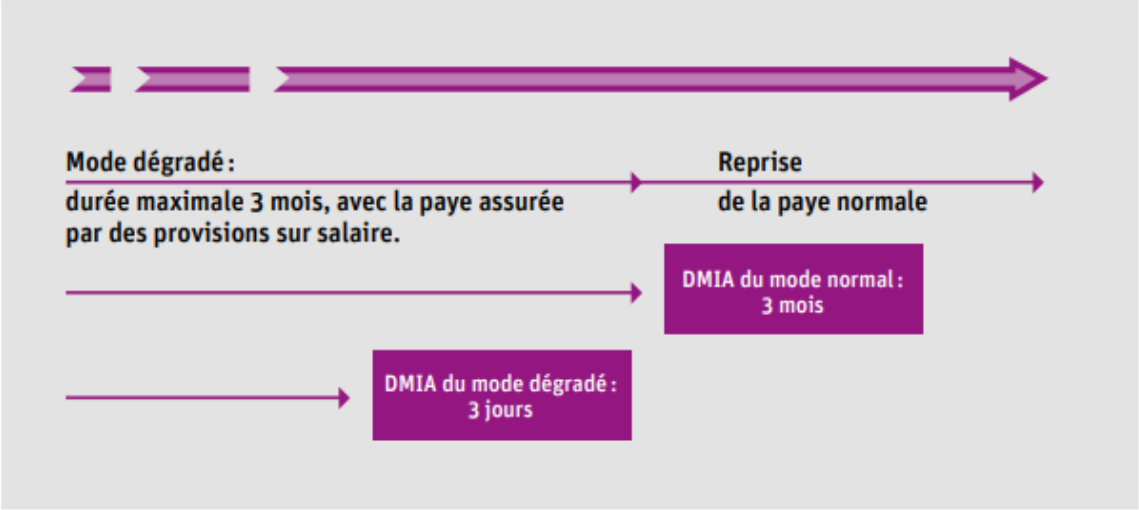
EXEMPLE : portique, badge, digicode, biométrie, vidéo protection, etc.

- Supervision de la sécurité physique et réactivité des équipes d'intervention en cas de détection d'intrusion (sur place, à distance, 24/7, seulement heures ouvrées).
- Nombre de barrières à franchir pour accéder physiquement aux biens supports critiques **(Note 16)**.

Source : Méthode EBIOS Risk Manager - Fichier en .pdf« fiches-methodes-ebios_projet » du site de l'ANSSI.

Partie 3 : Plan de continuité d'activité

Nous prévoyons de fonctionner avec un mode dégradé dans le cas où le SI serait défaillant. Afin d'anticiper tout dysfonctionnement, un mode dégradé validé par la gouvernance de la société sera activé. Garantir le fonctionnement des services vitaux de la société est primordial. Il comprend également la paie des salariés pour trois mois grâce à une provision financière prévue spécialement pour le mode dégradé.



Source : [hfds-guide-pca-plan-continuite-activite- sgdsn.pdf (economie.gouv.fr)]

EXEMPLE DE MESURE DES CONSÉQUENCES DE L'INTERRUPTION DE SERVICE ET DONC DE LA CRITICITÉ DE CHAQUE PROCESSUS

Activité	Processus	Humain	Financier	Contractuel	Environnement	Juridique et réglementaire	Opérationnel	Social	Perte d'image
Commercial	Prise de commande	1	4	2	1	1	3	1	3
Commercial	Relation client	1	3	3	1	1	3	2	3
Commercial	Niveau de service	2	3	4	2	3	2	2	3
Commercial	Livraison	2	2	4	1	1	4	2	3
Achat	Approvisionnement	1	3	2	2	3	3	2	3
Production	Fabrication	4	3	4	3	2	3	3	2
Logistique	Stockage	1	4	2	2	1	3	2	1
Ressources humaines	Paye	1	3	é	1	3	1	4	2
Finances	Facturation	1	4	2	1	1	1	1	2

1 = très faible - **2** = faible - **3** = fort - **4** = très fort

EXEMPLE DE TABLEAU DE SCÉNARIO DE RISQUES
(AVEC UNE QUANTIFICATION DES EFFETS SUR LES RESSOURCES CRITIQUES)

	local	route	moyen de transport	système d'information	ressource humaine	ressource intellectuelle	fournisseur et sous-traitance	produit critique
Catastrophe naturelle : inondation	4	4	4	3	3	2	1	2
Catastrophe naturelle : tempête	2	4	4	3	2	2	1	2
Grave accident	4	1	1	4	4	2	3	1
Crise sanitaire	1	1	3	2	4	2	3	1
Attentat terroriste	4	1	1	1	4	3	2	2
Crise sociale	1	1	4	1	4	2	3	3
Arrêt électricité	3	3	3	4	2	1	3	3
Arrêt Telecom ou Internet	3	2	2	4	2	3	3	2

1 = très faible - **2** = faible - **3** = fort - **4** = très fort

Source : [hfds-guide-pca-plan-continuite-activite- sgdsn.pdf (economie.gouv.fr)]

Partie 4 : Architecture réseau

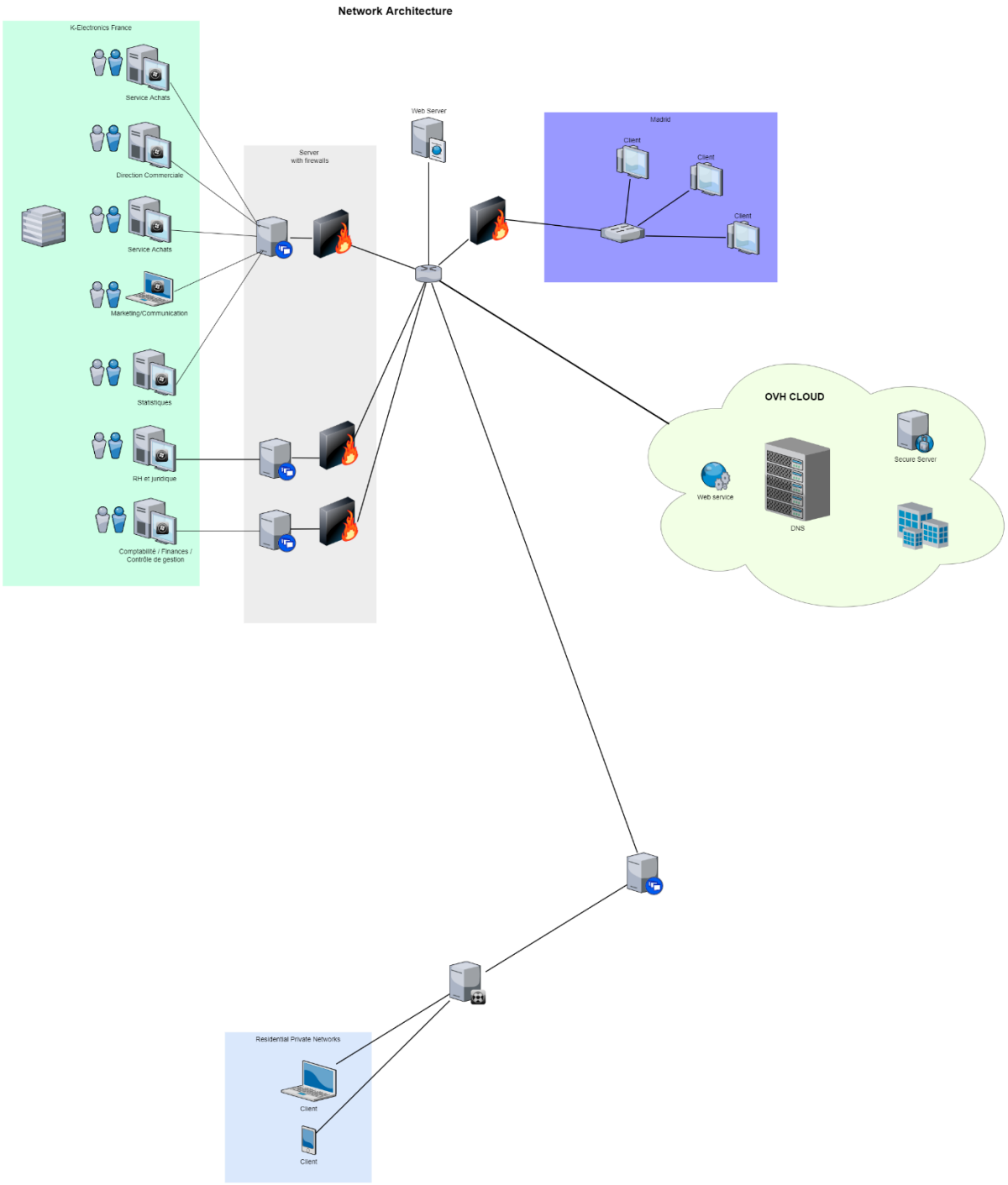
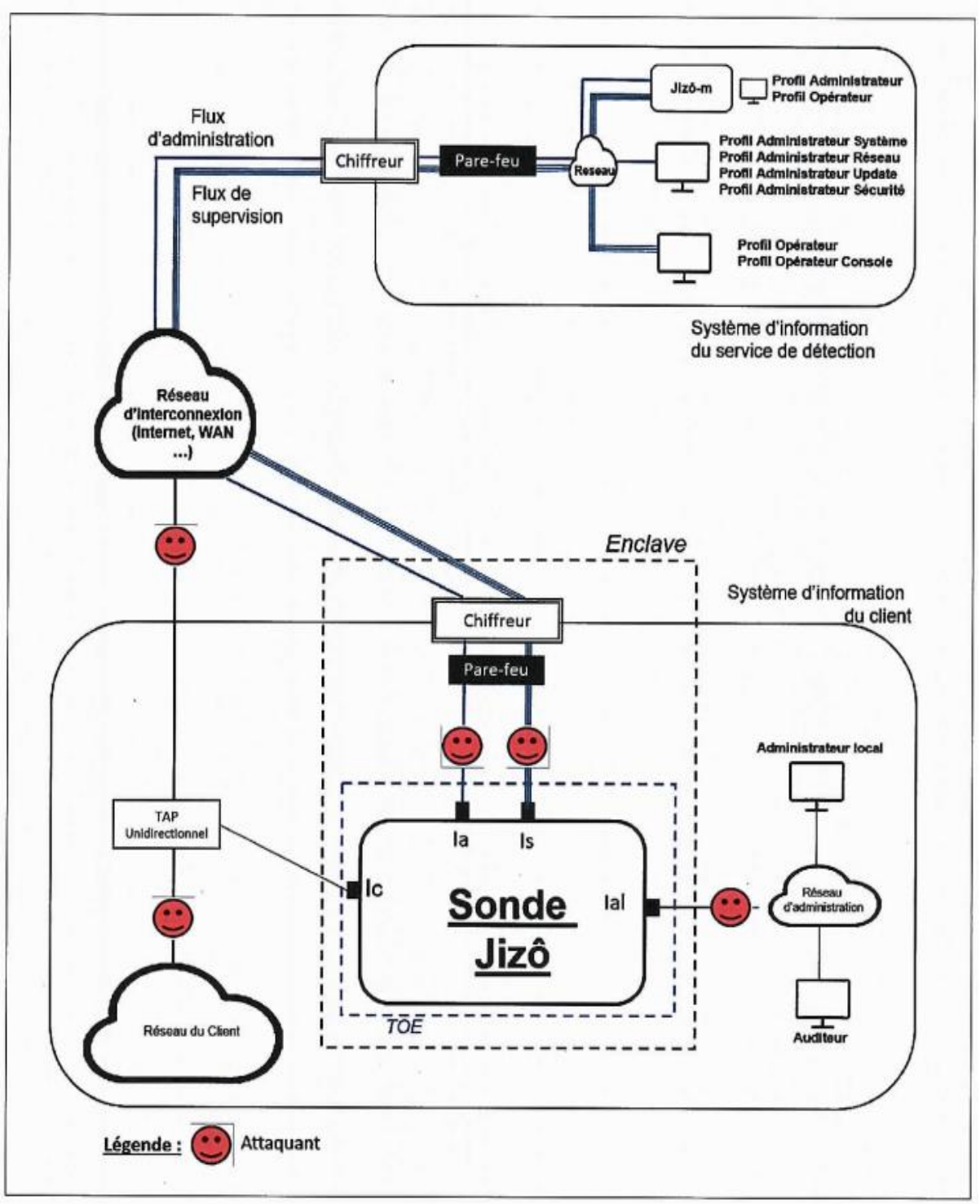


Schéma de la sonde de détection JIZO :



Partie 5 : Annexes

Cf. Dossier Annexes.