



**PRÉFET
DE LA RÉGION
D'ÎLE-DE-FRANCE**

*Liberté
Égalité
Fraternité*

**Direction régionale et interdépartementale
de l'environnement, de l'aménagement
et des transports d'Île-de-France**

CYBERSÉCURITÉ

Guide d'intégration de la cybersécurité dans les projets de la DiRIF

DiRIF
Direction des routes
Île-de-France



Le service public des autoroutes et routes nationales en Île-de-France

V1.4
29/11/2021

Historique des versions du document

Version	Date	Commentaire
1.0	24/05/2017	Version initiale pour commentaires et compléments
1.1	24/08/2017	Identification des données sensibles et de précisions sur les procédures d'installation, de sauvegarde et de restauration
1.2	26/09/2017	Prise en compte des remarques suite à soumission du document aux services d'ingénierie (DIMET) et de modernisation (SMR)
1.3	01/02/2019	Prise en compte des remarques suite à relecture DETT
1.4	29/11/2021	Actualisation suite aux remarques du projet Sirius 3.0 RAD et des commentaires du RSSI délégué DiRIF

Affaire suivie par

Abel BENOIT ROSARIO - Chargé de mission politique de sécurité des SI de la DiRIF

Tél. : 06 65 12 65 40

Courriel : abel.benoit-rosario@developpement-durable.gouv.fr

Rédaction

Abel BENOIT ROSARIO – DiRIF/STT/DETT

Mohammed ABOULATHAR – DiRIF/STT/DETT/UIRC



Relecture

Michèle MARLIERE - DiRIF/STT/DETT

Caroline LORENZ – DiRIF/STT/DETT/UIRC



Validation

Jérôme ROQUES – RSSI délégué DiRIF

Diffusion

A tous les porteurs de projets s'intégrant dans le SI de la DiRIF, ou en interface avec celui-ci

I. Préambule.....	5
A. Procédure de contact de l'équipe cybersécurité de la DiRIF...	6
B. Engagement du prestataire.....	7
II. Exigences de cybersécurité.....	8
A. Connaître le Système d'Information.....	8
1. Identifier les composants applicatifs des systèmes déployés.....	8
2. Inventorier les comptes utilisateurs et leur niveau de privilège.....	8
B. Authentifier et contrôler les accès.....	9
1. Changer les éléments d'authentification par défaut sur les équipements et services.....	9
2. Stocker les mots de passe dans des conteneurs sécurisés.....	9
C. Sécuriser les postes, les serveurs et les équipements.....	10
1. Limiter au strict besoin opérationnel les droits d'administration.....	10
2. Mettre en place une solution antivirus.....	10
3. Gérer les authentifications.....	10
4. Mettre en place une matrice des flux applicatifs et un pare-feu applicatif.....	10
5. Durcir les configurations.....	12
6. Restreindre l'utilisation des supports amovibles.....	14
7. Restreindre les collectes de données.....	14
8. Limiter les accès à internet au strict nécessaire.....	15
9. Protéger les expositions directes sur Internet.....	15
10. Gérer le nomadisme en chiffrant les postes nomades.....	15
D. Sécuriser les applications web.....	16
E. Sécuriser l'infrastructure réseau.....	16
F. Sécuriser l'administration.....	17
1. Utiliser des protocoles d'administration sécurisés.....	17
2. Désactiver les services inutilisés.....	18
G. Permettre la continuité d'activité et la maintenance.....	18
1. Respecter le socle technique de la DiRIF.....	18
2. Déployer des systèmes à jour.....	18
3. Fournir les procédures détaillées d'exploitation.....	19
4. Privilégier l'usage de produits qualifiés ou labellisés par l'ANSSI.....	20
H. Superviser et auditer.....	21
1. Mettre en place la politique de journalisation.....	21

2. Contrôler les accès physiques et mettre en place une vidéo-protection.....	22
3. Contrôler la prise en compte des mesures avant tout déploiement en production.....	22

III. Glossaire.....23

IV. Annexes.....24

<i>Annexe 1 - La liste des documents de référence.....</i>	<i>24</i>
<i>Annexe 2 - La fiche d'engagement du prestataire ou du porteur de projet.....</i>	<i>25</i>
<i>Annexe 3 - La Politique de gestion des mots de passe de la DiRIF.....</i>	<i>26</i>
<i>Annexe 4 - Les outils approuvés pour le stockage des mots de passe.....</i>	<i>26</i>
<i>Annexe 5 - Les mesures de cybersécurité s'appliquant aux réseaux Wi-Fi.....</i>	<i>29</i>
<i>Annexe 6 - Le formulaire de demande de mise en place de règles de filtrage de flux.....</i>	<i>30</i>

I. Préambule

Le présent document définit, sous la forme d'un guide, les exigences de sécurité à respecter par l'ensemble des projets (intégrant des matériels, des logiciels ou des équipements) s'intégrant dans le Système d'Information de la DiRIF.

Ce guide s'inscrit dans le cadre :

- des **projets d'installation ou de modification de postes clients, de serveurs ou d'équipements terrains ou réseaux et sécurité, au sein du parc de la DiRIF**,
 - Par exemple,
 - Dans le cadre d'installation d'équipements terrains ou de systèmes industriels de type Panneaux à Messages Variables, caméras, unités de mesures et de traitement, automates, détecteurs, ...
 - Dans le cadre de déploiement de postes clients, de serveurs, de logiciels, d'applications ou de scripts, de commutateurs réseaux, de routeurs, de modems, ...
- des **projets d'interfaçage du SI de la DiRIF avec l'extérieur**,
 - Par exemple,
 - Dans le cadre d'une interconnexion avec un partenaire ou un prestataire de la DiRIF,
 - Dans le cadre de l'hébergement externalisé d'un composant du SI.

En fin de document figurent plusieurs annexes :

1. La liste des documents de référence, notés [DR...] ci-après,
2. La fiche d'engagement du prestataire ou du porteur de projet,
3. La Politique de gestion des mots de passe,
4. Les outils approuvés par la DiRIF pour le stockage des mots de passe,
5. Les mesures de cybersécurité s'appliquant aux réseaux Wi-Fi,
6. Le formulaire de demande de mise en place de règles de filtrage de flux.

Parmi les mesures techniques que les organisations doivent prendre pour garantir la cybersécurité de leurs systèmes d'information, on qualifie les plus simples et élémentaires d'entre elles d'hygiène informatique, car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.

Les exigences de cybersécurité présentées dans ce document sont toutes inspirées du Guide d'hygiène informatique [DR01] de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), et permettent de fixer les règles de protection minimales applicables à tout SI et donc également aux SI de l'État, par application de la Politique de Sécurité des SI de l'État [DR02].

Les données soumises au Règlement Général à la Protection des Données (RGPD) doivent respecter les préconisations du document de référence [DR15].

A. Procédure de contact de l'équipe cybersécurité de la DiRIF

Dans le cadre des marchés de maintenance ou d'achat de la DiRIF, les demandes de dérogations sur l'application des exigences de cybersécurité **seront soumises à validation** de l'équipe cybersécurité de la DiRIF.

Il sera alors demandé un plan d'actions, mentionnant le délai de réalisation, pour la mise en conformité par rapport à la cible de cybersécurité présentée dans ce document.

L'équipe cybersécurité de la DiRIF peut être contactée via la boîte mail fonctionnelle suivante:

contact-cybersecurite-dirif.dett@developpement-durable.gouv.fr

Pour faciliter la gestion de cette boîte fonctionnelle, **les mails devront mentionner, dans l'objet du mail, la mention « Guide cybersécurité » et préciser le projet associé** à la demande.

Une fiche d'engagement du prestataire ou du porteur d'un projet est mise en place afin que le soumissionnaire d'un projet puisse s'engager sur l'application des mesures de cybersécurité mentionnées dans ce document.

B. Engagement du prestataire

Il fait l'objet d'une fiche d'engagement du prestataire porteur du projet, qui sera obligatoirement jointe à l'offre datée et signée.

Cette fiche d'engagement est fournie en Erreur : source de la référence non trouvée. Pour chacune des mesures de cybersécurité, le porteur du projet doit :

- soit cocher la case « NC », s'il est Non Concerné par la mesure de cybersécurité,
- soit cocher la case « OK », si la mesure de cybersécurité est prise en compte.

Nom/Prénom :	Entreprise/Organisation :	Intitulé du Projet :

Mesure de cybersécurité	NC	OK	Commentaires
A - Connaître le SI	<input type="checkbox"/>	<input type="checkbox"/>	
B - Authentifier et contrôler les accès	<input type="checkbox"/>	<input type="checkbox"/>	
C - Sécuriser les postes, les serveurs et les équipements	<input type="checkbox"/>	<input type="checkbox"/>	
D - Sécuriser les applications web	<input type="checkbox"/>	<input type="checkbox"/>	
E - Sécuriser l'infrastructure réseau	<input type="checkbox"/>	<input type="checkbox"/>	
F - Sécuriser l'administration	<input type="checkbox"/>	<input type="checkbox"/>	
G - Permettre la continuité d'activité et la maintenance	<input type="checkbox"/>	<input type="checkbox"/>	
H - Superviser et auditer	<input type="checkbox"/>	<input type="checkbox"/>	

Pour chacune des mesures de cybersécurité, le porteur du projet doit :

- soit cocher la case « NC », s'il est Non Concerné par la mesure,
- soit cocher la case « OK », si la mesure est prise en compte.

Commentaires :
.....
.....
.....

La fiche d'engagement doit obligatoirement être datée et signée.

Date :	Signature :

II. Exigences de cybersécurité

Les exigences de cybersécurité se basent sur les **8 thématiques** suivantes :

- A - Connaître le Système d'Information,
- B - Authentifier et contrôler les accès,
- C - Sécuriser les postes, les serveurs et les équipements,
- D- Sécuriser les applications web,
- E - Sécuriser l'infrastructure réseau,
- F - Sécuriser l'administration,
- G - Permettre la continuité d'activité et la maintenance,
- H - Superviser et auditer.

A. Connaître le Système d'Information

1. Identifier les composants applicatifs des systèmes déployés

Afin d'anticiper les obsolescences logicielles, il est demandé d'**établir un inventaire des systèmes et applications** qui seront déployés au sein du système d'information de la DiRIF.

Pour chacun des composants du système qui seront déployés, il est demandé :

- d'identifier la localisation¹ dans le SI,
- de fournir la version applicative déployée, et celle préconisée par l'éditeur,
- de fournir la date de fin de support des logiciels si annoncée par l'éditeur,
- d'indiquer la date d'application des derniers correctifs de sécurité,
- de lister les dépendances avec d'autres composants du SI.

2. Inventorier les comptes utilisateurs et leur niveau de privilège

Des **comptes nominatifs** doivent être mis en place.

Il est demandé de lister les utilisateurs et leur rôle au sein du système qui sera déployé.

En complément, il est demandé de fournir la liste :

- des comptes de services (hiérarchisés),
- des comptes d'administration.

¹ Tatouage, adresse IP, localisation d'installation physique

B. Authentifier et contrôler les accès

1. Changer les éléments d'authentification par défaut sur les équipements et services

Il est impératif de partir du principe que les configurations par défaut des systèmes d'information sont systématiquement connues des potentiels attaquants.

Les éléments d'authentification par défaut des composants du système installé doivent donc être modifiés dès leur installation et, **s'agissant des mots de passe, ils devront être conformes à la politique de gestion des mots de passe décrite en Annexe 3 - La Politique de gestion des mots de passe de la DiRIF.**

Les certificats par défaut doivent tous être remplacés.

Il est imposé que les **certificats soient paramétrables pour prendre en compte les certificats générés par l'infrastructure de gestion de clés de la DiRIF (certificats issues de la PKI DiRIF).**

2. Stocker les mots de passe dans des conteneurs sécurisés

Le stockage des mots de passe doit se faire dans un outil de coffre-fort numérique chiffré. La solution logicielle imposée sur le parc de la DiRIF pour le stockage sécurisé des mots de passe est la solution **KeePass2² disponible sur Windows** (ou son alternative qui est la solution **KeePassXC³ pour les environnements sous Linux**).

Le paramétrage de ces outils est présenté en Annexe 4 – Les outils approuvés pour le stockage des mots de passe.

Un même mot de passe ne pourra être partagé qu'au sein d'un parc homogène de composant (ces composants ayant la même fonction et fonctionnant tous avec la même version de logiciel).

Il est également demandé de vérifier que le stockage des mots de passe dans les configurations soit réalisé à l'aide d'un chiffrement conforme au Référentiel Général de Sécurité, annexe B1 du document de référence [DR09].

2 <https://keepass.info/>

3 <https://keepassxc.org/>

C. Sécuriser les postes, les serveurs et les équipements

1. Limiter au strict besoin opérationnel les droits d'administration

Le **principe du moindre privilège doit être appliqué.**

Le principe du moindre privilège est le principe selon lequel **chaque intervenant doit disposer d'un compte ayant exactement les droits nécessaires à l'accomplissement de ses tâches.**

Il est recommandé qu'un utilisateur du système d'information ne dispose pas de privilèges d'administration sur son poste de travail.

Cette mesure vise à limiter les conséquences de l'exécution malencontreuse d'un code malveillant.

2. Mettre en place une solution antivirus

La **solution antivirus imposée par la DiRIF sur le réseau technique de la DiRIF est soit Windows Defender, soit la solution ESET Nod32.**

Il est imposé de **configurer l'antivirus pour une inspection automatique du contenu des supports amovibles dès leur branchement.**

3. Gérer les authentifications

Afin de rendre plus difficiles les attaques sur les authentifications (attaque par brute force ou par dictionnaire), il est **imposé une augmentation du délai entre deux tentatives de connexions.**

4. Mettre en place une matrice des flux applicatifs et un pare-feu applicatif

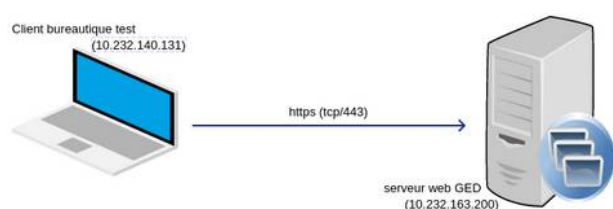
Après avoir réussi à prendre le contrôle d'un poste de travail (par exploitation d'une vulnérabilité par exemple), un attaquant cherchera souvent à étendre son intrusion aux autres postes de travail pour accéder aux documents des utilisateurs. Afin de rendre plus difficile ce déplacement latéral de l'attaquant, **il est imposé d'activer le pare-feu local des postes de travail et des serveurs au moyen de logiciels intégrés (pare-feu local Windows) ou spécialisés.**

Le filtrage le plus simple consiste à bloquer l'accès aux ports d'administration par défaut des postes de travail (ports TCP 135, 445 et 3389 sous Windows, port TCP 22 sous Unix), excepté depuis les ressources explicitement identifiées (postes d'administration et d'as-

sistance utilisateur, éventuels serveurs de gestion requérant l'accès à des partages réseau sur les postes, etc.).

Une **analyse des flux entrants utiles (administration, logiciels d'infrastructure, applications particulières, etc.) doit être menée pour définir la liste des autorisations à configurer**. Il est demandé de bloquer l'ensemble des flux par défaut et de **n'autoriser que les services nécessaires** depuis les composants correspondants (liste blanche).

Il est demandé de réaliser cette analyse sur les flux sortants pour la détermination complète de la matrice des flux.



Par exemple, dans le cas d'un poste client se connectant sur un serveur au travers du protocole HTTPS, la matrice des flux est la suivante :

Mise en Place de règles de filtrage de flux – Marché MIRT Lot 1			
Demandeur :		Nom/Prénom :	<A compléter>
		Entreprise/Organisation :	<A compléter>
		Intitulé du projet :	<A compléter>
Date de la demande :		<A compléter>	
IP Source / VPN	IP Destination	Service / Protocole	Description
Client bureautique test 10.232.140.131	Serveur web GED 10.232.163.200	HTTPS (TCP/443)	Accès web pour consultation de la Gestion Électronique de Document

Le document pour compléter la matrice de flux est présenté en Annexe 6 – Le formulaire de demande de mise en place de règles de filtrage de flux.

La **déclinaison de cette matrice des flux est à réaliser localement au sein des pare-feux applicatifs** des composants déployés dans le système d'information.

5. Durcir les configurations

a. Cas des postes opérateurs et des serveurs Windows

Le durcissement des configurations des postes opérateurs Windows repose sur les mécanismes AppLocker (cf document de référence [DR05]) décrits au paragraphe ci-après.

i) Mise en place de restrictions logicielles avec AppLocker

L'intérêt principal des mécanismes de restrictions logicielles réside dans la possibilité de limiter l'exécution des programmes à une liste de programmes dûment autorisés (principe de liste blanche).

Le principe d'une liste blanche procure plusieurs avantages :

- une meilleure protection contre les programmes malveillants : en empêchant systématiquement l'exécution des programmes non répertoriés dans la liste, et susceptibles de contenir un code malveillant sont bloqués, que ce dernier soit connu ou non des bases de signature de l'antivirus ;
- un blocage de l'installation ou de l'utilisation de logiciels indésirables, en particulier ceux qui sont susceptibles de porter atteinte aux performances ou de rendre instables les systèmes et qui, dans tous les cas, augmentent la surface d'attaque de celles-ci ;
- un blocage de l'installation ou de l'utilisation de logiciels sans licence certifiée.

Sur un système à jour de ses correctifs de sécurité et respectant le principe de séparation des privilèges, l'activation des mécanismes de restrictions logicielles augmente la maîtrise du système.

Enfin, en règle générale, l'activation des mécanismes de restrictions logicielles n'engendre pas d'altération des performances du système, cette mesure est totalement transparente pour l'utilisateur.

Bien que les mécanismes de restriction logicielle puissent s'appliquer sur des systèmes serveurs, c'est essentiellement sur les postes de travail utilisateurs qu'ils présentent un intérêt.

Il est demandé, sur l'ensemble des postes opérateurs et serveurs déployés, de n'autoriser par AppLocker l'exécution que des applicatifs maîtrisés et de veiller à protéger également les emplacements systèmes accessibles en écriture depuis un compte non-administrateur et de traiter par exception à AppLocker les cas de vigilance

connus (regsvr32.exe, InstallUtil.exe et le lancement d'application 16 bits via NTVDM.exe).

b. Cas des serveurs Linux

Le durcissement des configurations des serveurs Linux repose sur les mécanismes décrits ci-après. **Les mesures de l'ANSSI sur la sécurisation d'un système GNU/Linux** indiquées dans le document de référence [DR08] **sont imposées sur le réseau technique de la DiRIF.**

i) Sécuriser le service d'administration OpenSSH

Il est demandé de réaliser la séparation des privilèges, ce qui permet de limiter les impacts d'une faille en cherchant à respecter le principe de moindre privilège, c'est-à-dire limiter les services à réduire les droits au strict nécessaire.

Il est demandé d'utiliser une arborescence indépendante (chroot) à chaque fois qu'est mis en place le service SFTP :

- les utilisateurs du service SFTP seront ainsi isolés dans une arborescence fichiers et n'auront pas de visibilité ou d'accès sur le reste du système,
- la volumétrie ne sera pas partagée avec d'autres partitions et évitera ainsi les risques de saturation.

La possibilité de se connecter en SSH avec **le compte root** (compte générique que l'on retrouve sur tous les systèmes Unix/Linux et utilisé comme compte d'administration) **doit être désactivée.**

Chaque utilisateur doit disposer de son propre compte, unique. La possession d'un compte dédié pour chaque utilisateur permet une gestion plus fine des accès et une meilleure traçabilité. Un utilisateur ayant connaissance que son compte lui est dédié peut être plus vigilant sur son usage.

Les directives AllowUsers (ou AllowGroups dans le cas d'un groupe d'utilisateurs) permet de spécifier la liste des utilisateurs autorisés à se connecter au service SSH en restreignant les accès utilisateurs suivant leur adresse IP.

L'altération de l'environnement par un utilisateur doit être bloquée par défaut.

Toute fonctionnalité de redirections de flux (AllowTcpForwarding) doit être désactivée au niveau de la configuration du serveur SSH.

La redirection X11 doit être désactivée sur le serveur.

6. Restreindre l'utilisation des supports amovibles

Il est demandé de **désactiver les exécutions automatiques** (autorun).

Il est demandé de **déclencher automatiquement un scan antivirus lors de l'insertion d'un média amovible**.

Sur les systèmes Linux, il est demandé de mettre en place la directive noexec sur les supports amovibles.

7. Restreindre les collectes de données

Il s'agit de **configurer les systèmes pour limiter les données recueillies par l'éditeur d'une solution dans le but de maîtriser la confidentialité de ses données**.

a. Application aux systèmes d'exploitation Windows

Il est demandé d'appliquer les mesures suivantes sur les systèmes d'exploitation Windows afin de restreindre les collectes de données et leur diffusion :

- Désactivation du service de télémétrie,
- Désactivation de l'agent personnel Cortana,
- Restriction de l'utilisation de Windows Desktop Search à des recherches locales,
- Désactivation de l'envoi de rapports d'erreurs et de diagnostic,
- Désactivation de la personnalisation des saisies clavier, vocales et manuscrites,
- Désactivation du programme d'amélioration de l'expérience utilisateur,
- Désactivation de la géolocalisation,
- Désactivation de l'identifiant unique de publicité utilisé pour partager les informations collectées,
- Désinstallation des applications universelles non utilisées,
- Pas d'utilisation d'un compte Microsoft pour l'ouverture de session utilisateur,
- Désactivation du stockage dans le cloud One Drive.

8. Limiter les accès à internet au strict nécessaire

Si un accès internet est nécessaire au fonctionnement d'un système, il est nécessaire de compléter chacun des flux sortants dans la matrice de flux applicative mentionné au paragraphe 4 - Mettre en place une matrice des flux applicatifs et un pare-feu applicatif.

9. Protéger les expositions directes sur Internet

Dans le cas particulier d'exposition d'un composant du SI sur Internet, il est nécessaire de compléter chacun des flux entrants et sortants dans la matrice de flux applicative mentionné au paragraphe 4 - Mettre en place une matrice des flux applicatifs et un pare-feu applicatif.

10. Gérer le nomadisme en chiffrant les postes nomades

Les terminaux nomades (ordinateurs portables, tablettes, ordiphones) sont par nature exposés à la perte et au vol. Ils peuvent contenir localement des informations sensibles et constituer un point d'entrée vers de plus amples ressources du système d'information. Des mesures spécifiques de sécurisation de ces équipements sont donc à prévoir.

Le Ministère s'est doté d'une solution pour sécuriser les postes nomades par le **chiffrement complet des disques et des partitions locales** : il s'agit de la solution Cryhod⁴.

Des préconisations quant à son utilisation sécurisée sont disponibles sur la fiche logicielle [DR17].

4 www.ssi.gouv.fr/entreprise/qualification/cryhod/

D. Sécuriser les applications web

Les mesures suivantes sont imposées pour **renforcer les protections des sites web** [DR11] contre les attaques :

- Les architectures web de type « n-tiers » se prêtent bien à une approche de type défense en profondeur [DR18]. Il convient de ne pas concentrer toutes les mesures de sécurité sur le « tiers » présentation, mais au contraire de développer chaque composant afin qu'il assure sa propre protection.
 - Les droits sur les bases de données utilisées par les applications web doivent être gérés finement pour mettre en œuvre également le principe de moindre privilège.
 - La transformation des mots de passe doit faire intervenir un sel⁵ aléatoire.
- Les traitements doivent tous être faits du côté du serveur. Les entrées en provenance des clients ne doivent pas être considérées comme fiables et par conséquent, aucune vérification ne doit être déléguée aux clients.
 - Par exemple, si le code JavaScript exécuté côté client peut faire certains contrôles à des fins d'ergonomie (pour signaler une probable faute de frappe dans un champ par exemple), il ne faut en aucun cas se contenter de ce contrôle. Il faut au contraire partir du postulat que le code client a pu ne pas s'exécuter (JavaScript désactivé ou requêtes malveillantes).

E. Sécuriser l'infrastructure réseau

Il est demandé de **privilégier les installations filaires** pour l'ensemble du parc technique de la DiRIF.

Une dérogation est accordée pour la maintenance des équipements sous circulation : un point d'accès Wi-Fi temporaire peut être activé pour une durée de 3 heures maximum sur ces équipements. Des mesures spécifiques de cybersécurité s'appliquent alors et elles sont présentées en Annexe 5 – Les mesures de cybersécurité s'appliquant aux réseaux Wi-Fi.

En cas d'ajout ou de modification d'équipements réseaux, il est nécessaire de soumettre pour validation l'architecture proposée à l'équipe cybersécurité, selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF, en précisant les références des matériels envisagés et fournir le sy-

5 L'ajout d'un sel sur un mot de passe est une méthode pour rendre l'empreinte des mots de passe plus sûre en ajoutant aux mots de passe une chaîne de caractères aléatoires avant de calculer leur empreinte, ce qui rend l'opération pour retrouver le mot de passe à partir de son empreinte plus difficile.

noptique de raccordement et de chaînage, ainsi que les détails d'implémentation de l'architecture réseau proposée.

La configuration des équipements réseaux et sécurité déployés au sein du parc de la DiRIF sera réalisée au travers du Marché d'Infogérance des Réseaux Techniques (MIRT Lot 1 – Réseaux IP).

F. Sécuriser l'administration

1. Utiliser des protocoles d'administration sécurisés

Si aujourd'hui la sécurité des systèmes d'information est mise en avant, cela n'a pas toujours été le cas. C'est pourquoi de nombreux protocoles réseaux ont dû évoluer pour intégrer cette composante et répondre aux besoins de confidentialité et d'intégrité qu'impose l'échange de données (cf document de référence [DR04]).

Les **protocoles réseaux suivants sont considérés comme non sécurisés et sont proscrits du réseau technique** de la DiRIF : telnet, HTTP, IMAP, SMTP, POP3, FTP, rlogin, rcp, rsh, LDAP, VNC.

Bien qu'il soit difficile d'en dresser une liste exhaustive, les protocoles les plus courants reposent sur l'utilisation de TLS [DR14] et sont souvent identifiables par l'ajout de la lettre « S » (pour Secure en anglais) à l'acronyme du protocole.

Citons par exemple :

- HTTPS pour la navigation Web,
- IMAPS, SMTPS ou POP3S pour les services réseaux de messagerie,
- LDAPS pour l'accès aux services d'annuaire.

Il est imposé d'**utiliser uniquement des protocoles d'administration sécurisés** sur le parc technique de la DiRIF.

La version minimale de TLS qui est imposée sur le réseau technique de la DiRIF est **TLS1.3**. Il est donc demandé d'abandonner HTTP au profit de HTTPS, avec TLS1.3 ou ultérieur.

La version minimale de SSH qui est imposée sur le réseau technique de la DiRIF est **SSHv2** [DR10]. Il est donc demandé d'abandonner Telnet au profit de SSHv2 ou ultérieur.

La version minimale de SNMP qui est imposée sur le réseau technique de la DiRIF est **SNMPv3** ou ultérieur.

2. Désactiver les services inutilisés

Afin de réduire les surfaces d'attaque sur les composants du SI, **seuls les services utilisés doivent être activés**.⁶

Pour ce faire, il est demandé de désactiver l'ensemble des services pour ensuite n'activer que les services nécessaires au fonctionnement du système.

G. Permettre la continuité d'activité et la maintenance

1. Respecter le socle technique de la DiRIF

Dès la conception de l'architecture physique à mettre en place dans le cadre d'un projet, il est demandé de se rapprocher des équipes informatiques, réseau et cybersécurité de la DiRIF afin de **se conformer au socle technique en place** au moment du projet.

Ainsi, pour des raisons de maintenabilité et d'homogénéité du parc de serveurs Linux, il peut être imposé d'installer une version spécifique de Debian.

2. Déployer des systèmes à jour

Il est demandé de déployer des systèmes les plus à jour lors de leur installation. Il s'agit donc de vérifier auprès des éditeurs et des constructeurs les versions préconisées avant d'envisager leur installation sur le Système d'Information de la DiRIF.

a. Utilisation de la dernière version recommandée / supportée par les constructeurs sans failles connues mis en évidence par le CERT-FR⁷

Il s'agit de vérifier que **les versions déployées sont les dernières versions** préconisées par les constructeurs ou éditeurs des :

- Firmware / Système d'exploitation / logiciels,
- mises à jour de sécurité.

6 Par exemple, si le service web « httpd » correspondant à un frontal web a été installé par défaut mais qu'il n'est pas utilisé, il convient de le désactiver.

7 www.cert.ssi.gouv.fr/

b. Cas particulier d'utilisation de systèmes obsolètes

Si des **systèmes obsolètes** (qui ne sont plus supportés par leurs fabricants) devaient être déployés provisoirement, il conviendra d'**envoyer la liste** à l'équipe cybersécurité de la DiRIF, selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF, **afin de les isoler** au maximum du reste du SI de la DiRIF.

Cette mesure s'applique aussi au niveau du réseau par un **filtrage strict des flux**, tout comme elle s'applique au niveau des **secrets d'authentification qui doivent être dédiés à ces systèmes obsolètes**.

c. Mise à jour des bases antivirales

Comme indiqué au paragraphe Mettre en place une solution antivirus, il est demandé à ce que **l'antivirus récupère les mises à jour des bases de signatures**.

3. Fournir les procédures détaillées d'exploitation

a. Procédure d'installation et de configuration des systèmes et des services

Selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF, il est demandé de **fournir les procédures détaillées d'installation et de configuration (dont le paramétrage) de chaque composant** du système afin de permettre à la DiRIF leur remise en service, après un incident de sécurité.

b. Procédures de sauvegarde et de restauration de chacun des composants

Selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF, il est demandé de **fournir les procédures détaillées de sauvegarde et de restauration de chaque composant** du système afin de permettre à la DiRIF la restauration de tout le système dans son dernier état consistant.

c. Procédures de purges de données

Selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF, il est demandé de **fournir les procédures détaillées des purges de données** à opérer afin d'éviter les saturations d'espace disque par les composants du système, en précisant les durées de conservation des données.

4. Privilégier l'usage de produits qualifiés ou labellisés par l'ANSSI

La qualification est prononcée par l'ANSSI et permet d'attester d'un niveau de sécurité et de confiance dans les produits et les prestataires de service listés dans les catalogues que publie l'agence.

La qualification offre donc des garanties de sécurité et de confiance sur les produits ou les prestations de service.

Cette qualification fait suite à une étude approfondie du fonctionnement technique de la solution et de son écosystème. **Il est demandé de privilégier l'usage de produits qualifiés par l'ANSSI lorsqu'ils sont définis.**

A titre d'exemple, la solution de « coffre-fort » de mots de passe KeePass2 a obtenu, pour sa version 2.10 portable, une Certification de Sécurité de Premier Niveau⁸ (CSPN) par l'ANSSI.

En particulier, lorsque le projet prévoit d'entreposer tout ou partie des données dans un cloud, il est **imposé d'utiliser un fournisseur qui soit labellisé par la certification SecNumCloud⁹**. Ce point sera nécessairement soumis à validation de l'équipe cybersécurité de la DiRIF, selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF.

8 https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/

9 <https://www.ssi.gouv.fr/actualite/secnumcloud-la-nouvelle-reference-pour-les-prestataires-dinformatique-en-nuage-de-confiance/>

H. Superviser et auditer

1. Mettre en place la politique de journalisation

Il est **imposé la journalisation** [DR13] **des accès aux données et des opérations effectuées** suivants (horodatés et conservés pendant au moins un an) :

- pare-feu :
 - paquets bloqués,
- systèmes et applications :
 - authentification :
 - réussites et échecs d'authentifications,
 - gestion des comptes et des droits :
 - modification des données d'authentification (ajout ou suppression de compte / rôle et affectation de droits)
 - Modification des stratégies de sécurité :
 - édition / application / réinitialisation de configuration,
 - activité des systèmes et des processus :
 - démarrages / arrêts,
 - dysfonctionnements / surcharges du système,
 - chargements / déchargements de modules,
 - activité matérielle (défaillances, connexions / déconnexions physiques)
 - services :
 - erreurs de protocoles (par exemples les erreurs 403, 404 et 500 pour les services HTTP),
 - traçabilité des flux applicatifs aux interconnexions (URL sur un relai HTTP, en-têtes des messages sur un relai SMTP, etc.).
- antivirus :
 - détections d'éléments suspects par l'antivirus.

Afin de pouvoir corréler ces événements entre différents composants, leur source de synchronisation de temps (grâce au protocole NTP) doit être identique.

2. Contrôler les accès physiques et mettre en place une vidéoprotection

Il est demandé de **suivre les recommandations** [DR16] de l'ANSSI **qui s'appliquent aux systèmes de contrôle d'accès physique et de vidéoprotection**.

3. Contrôler la prise en compte des mesures avant tout déploiement en production

Il s'agit de **passer en revue la prise en compte par les projets de l'ensemble des mesures de cybersécurité listées** dans le présent document (cf document de référence [DR12]).

A cette fin et selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF, il est demandé d'envoyer à l'équipe cybersécurité de la DiRIF tous les éléments lui permettant d'apprécier la prise en compte des différentes mesures.

Si l'équipe cybersécurité de la DiRIF le juge nécessaire, des tests plus approfondis pourront être exigés avant la mise en production, par exemple via la mise à disposition d'une plateforme de tests ou de préproduction. À défaut, la vérification de l'application des mesures de sécurité pourra être vérifiée une fois le déploiement en production réalisé.

III. Glossaire

- **Cybersécurité** : La cybersécurité englobe tous les moyens qui permettent d'assurer la protection et l'intégrité des données au sein d'une infrastructure.
- **ANSSI** : Agence Nationale de Sécurité des Systèmes d'Information
- **PSSIE** : Politique de Sécurité des SI de l'État
- **telnet** (terminal network) : protocole datant de 1969 permettant de communiquer avec un serveur distant par échange de lignes de texte, en clair,
- **SSH** (Secure SHell) : protocole de communication sécurisé permettant d'administrer un serveur,
- **HTTP** (HyperText Transfert Protocol): protocole datant de 1990 permettant la communication entre un navigateur Web et un serveur exposant des pages Web,
- **HTTPS**: variante sécurisée de HTTP, par l'usage des protocoles TLS,
- **TLS** (Transport Layer Security) : Le protocole Transport Layer Security est une des solutions les plus répandues pour la protection des flux réseaux. C'est le successeur du protocole SSL.
- **IMAP** (Internet Message Access Protocol) : protocole permettant d'accéder à des courriers électroniques directement sur les serveurs de messagerie,
- **IMAPS** : variante sécurisée de IMAP, par l'usage des protocoles TLS,
- **SMTP** (Simple Mail Transfer Protocol) : protocole utilisé pour transférer les courriers électroniques vers des serveurs de messagerie,
- **SMTPS** : variante sécurisée de SMTP, par l'usage des protocoles TLS,
- **POP3** (Post Office Protocol, v3) : protocole qui permet de récupérer les courriers électronique situés sur un serveur de messagerie,
- **POP3S** ou **POPS** : variante sécurisée de POP3, par l'usage des protocoles TLS,
- **FTP** (File Transfer Protocol): protocole destiné au transfert de fichiers,
- **SFTP**: variante sécurisée de FTP, par l'usage de SSH,
- **rlogin** : protocole obsolète qui permet d'ouvrir une session à distance sur une autre machine,
- **rcp** (remote copy) : protocole obsolète pour copier des fichiers sur ou à partir d'une autre machine,
- **rsh** (remote shell): protocole obsolète pour se connecter sur une autre machine pour exécuter une unique commande,
- **LDAP** (Lightweight Directory Access Protocol): protocole d'accès aux services d'annuaire via l'envoi de requêtes d'opération à un serveur,
- **LDAPS** : variante sécurisée de LDAP, par l'usage des protocoles TLS,
- **VNC** (Virtual Network Computing) : système de visualisation et de contrôle d'un environnement de bureau d'un ordinateur distant.

IV. Annexes

Annexe 1 - La liste des documents de référence

L'ensemble des documents de référence mentionnés dans le document ont été établis par l'ANSSI :

Réf.	Intitulé
DR01	Guide d'hygiène informatique ➔ www.ssi.gouv.fr/hygiene-informatique/
DR02	Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) ➔ www.ssi.gouv.fr/pssie/
DR03	Recommandations de sécurité relatives aux mots de passe ➔ www.ssi.gouv.fr/guide/mot-de-passe/
DR04	Recommandations relatives à l'administration sécurisée des systèmes d'information ➔ www.ssi.gouv.fr/securisation-admin-si/
DR05	Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows ➔ www.ssi.gouv.fr/windows-restrictions-logicielles/
DR06	Recommandations de sécurité relatives aux réseaux WiFi ➔ www.ssi.gouv.fr/nt-wifi/
DR07	Cybersécurité des systèmes industriels ➔ www.ssi.gouv.fr/entreprise/guide/la-cybersecurite-des-systemes-industriels/
DR08	Recommandations de sécurité relatives à un système GNU/Linux ➔ www.ssi.gouv.fr/reco-securite-systeme-linux/
DR09	Règlement Général de Sécurité (RGS) ➔ www.ssi.gouv.fr/rgs/
DR10	Usage sécurisé d'(Open)SSH ➔ www.ssi.gouv.fr/nt-ssh/
DR11	Sécuriser un site Web ➔ www.ssi.gouv.fr/securisation-sites-web/
DR12	Guide d'intégration de la sécurité des systèmes d'information dans les projets ➔ www.ssi.gouv.fr/gissip/
DR13	Mise en œuvre d'un système de journalisation ➔ www.ssi.gouv.fr/journalisation/
DR14	Transport Layer Security (TLS) ➔ www.ssi.gouv.fr/nt-tls/
DR15	Règlement Général à la Protection des Données (RGPD) ➔ www.ssi.gouv.fr/rgpd/
DR16	Sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection ➔ www.ssi.gouv.fr/nt-videoprotection/
DR17	Utilisation de Cryhod ➔ www.ssi.gouv.fr/recos-cryhod/
DR18	Défense en profondeur ➔ www.ssi.gouv.fr/defense-profondeur/

Annexe 2 - La fiche d'engagement du prestataire ou du porteur de projet

Nom/Prénom :	Entreprise/Organisation :	Intitulé du Projet :

Mesure de cybersécurité	NC	OK	Commentaires
A - Connaître le SI	<input type="checkbox"/>	<input type="checkbox"/>	
B - Authentifier et contrôler les accès	<input type="checkbox"/>	<input type="checkbox"/>	
C - Sécuriser les postes, les serveurs et les équipements	<input type="checkbox"/>	<input type="checkbox"/>	
D - Sécuriser les applications web	<input type="checkbox"/>	<input type="checkbox"/>	
E - Sécuriser l'infrastructure réseau	<input type="checkbox"/>	<input type="checkbox"/>	
F - Sécuriser l'administration	<input type="checkbox"/>	<input type="checkbox"/>	
G - Permettre la continuité d'activité et la maintenance	<input type="checkbox"/>	<input type="checkbox"/>	
H - Superviser et auditer	<input type="checkbox"/>	<input type="checkbox"/>	

Pour chacune des mesures de cybersécurité, le porteur du projet doit :

- soit cocher la case « NC », s'il est Non Concerné par la mesure,
- soit cocher la case « OK », si la mesure est prise en compte.

Commentaires :

.....

.....

La fiche d'engagement doit obligatoirement être datée et signée.

Date :	Signature :

Annexe 3 - La Politique de gestion des mots de passe de la DiRIF

Les mots de passe doivent contenir 12 caractères ou plus, et être composés d'au moins un caractère de chacun des types suivants:

- majuscules,
- minuscules,
- chiffres,
- caractères spéciaux.

Les mots de passe ne doivent pas dériver d'un mot du dictionnaire et être différents des mots de passe par défaut (cf document de référence [DR03]).

Annexe 4 - Les outils approuvés pour le stockage des mots de passe

Pour assurer le stockage sécurisé des mots de passe, la DiRIF a approuvé l'utilisation d'outils de type coffre-forts de mots de passe : KeePass2 et KeePassXC.

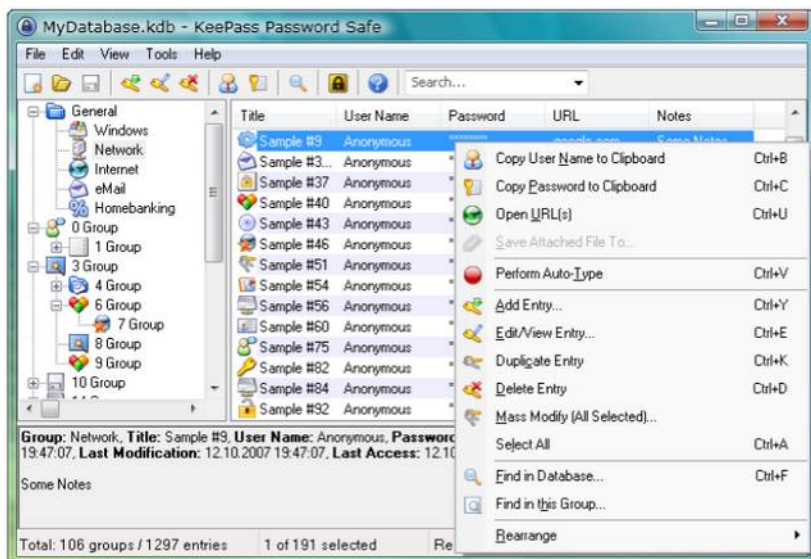
Les logiciels KeePass2 et KeePassXC sont tous les deux des logiciels open source qui permettent de gérer différents mots de passe de manière sécurisée et chiffrée. Tous les mots de passe sont stockés dans une base de données, verrouillée avec une clé maître (Master Password) ou un fichier clé (Key File). Il suffit de se rappeler du mot de passe maître et/ou de sélectionner le fichier clé pour accéder à la base de données. Les solutions KeePass2 et KeePassXC permettent de gérer tous les deux des bases de données de mots de passe sous format « .kdbx ».



Selon les modalités de prise de contact mentionnées au paragraphe Procédure de contact de l'équipe cybersécurité de la DiRIF, le mot de passe d'accès à ce coffre-fort doit être communiqué à l'équipe cybersécurité de la DiRIF via un canal de confiance ou à défaut, un canal distinct du canal de transmission des données. Ainsi, si les données chiffrées sont transmises par courriel, une remise du mot de passe en main propre ou par téléphone doit être privilégiée.

Le Master Password de KeePass2 (ou KeePassXC) devra être transmis à la DiRIF et devra lui-même respecter la politique de gestion des mots de passe décrite plus haut.

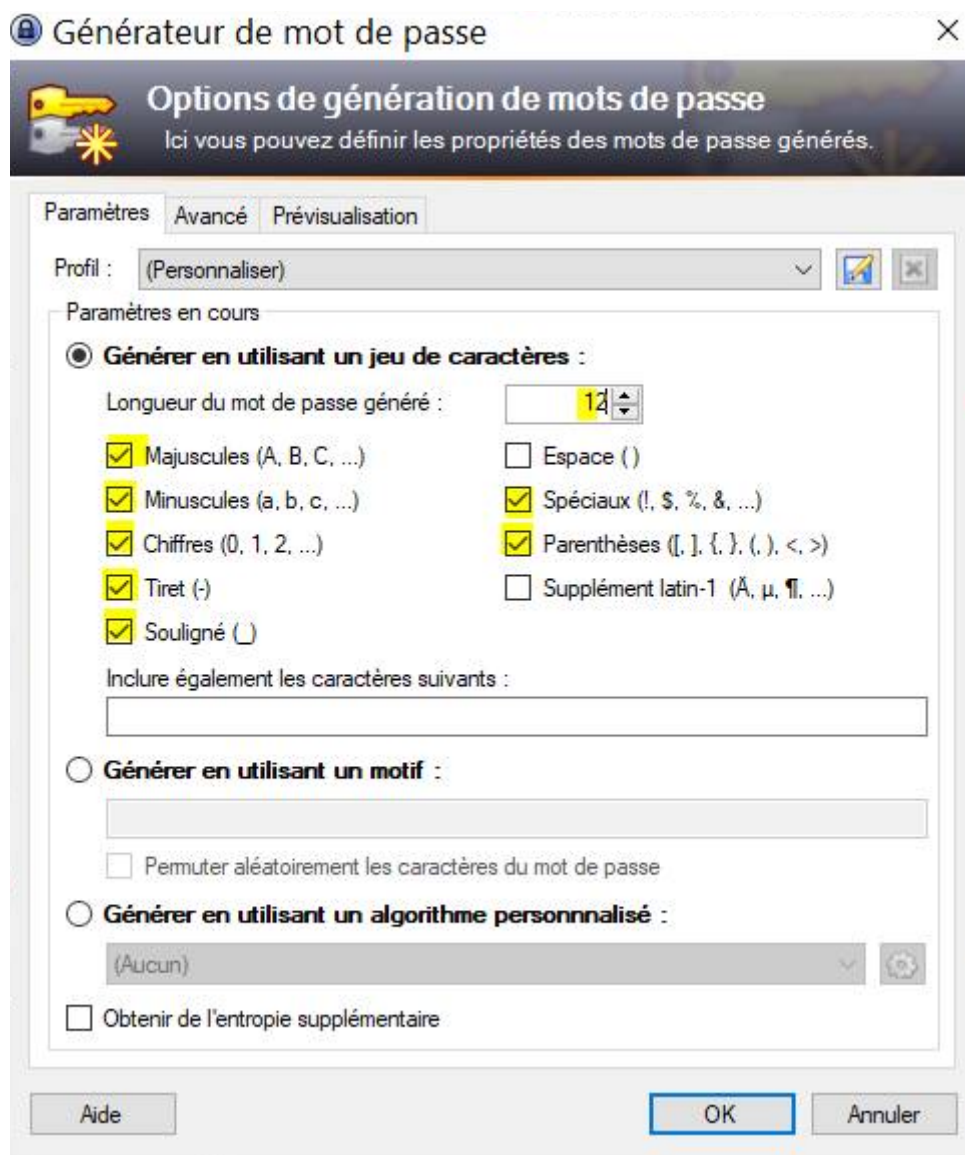
Les outils KeePass2 et KeePassXC supportent la définition de groupes de mot de passes et chaque mot de passe peut être copié / collé, par exemple dans une fenêtre d'authentification.



KeePass2 et KeePassXC fournissent également un générateur de mot de passe qui est paramétrable suivant divers critères, les paramétrages imposés par la DiRIF sont:

- Longueur du mot de passe → 12 caractères ou plus,
- Types de caractère à utiliser par la fonctionnalité de génération de mots de passe,
 - Majuscules → Oui,
 - Minuscules → Oui,
 - Chiffres → Oui,
 - Tirets → Oui,
 - Underscore → Oui,
 - Espace → Non,
 - Caractères spéciaux: !, \$, % , &, ... → Oui
 - Parenthèses: [,], {, }, (,), <, > → Oui
 - Supplément Latin-1 (Codage de caractères ASCII étendu) → Non

Le paramétrage imposé pour les mots de passe des systèmes à déployer au sein du SI de la DiRIF se résume donc à :



Un guide d'utilisation du gestionnaire de mot de passe Keeppass2 est proposé par les services du Secrétariat Général de Bercy¹¹.

¹¹ https://www.economie.gouv.fr/files/bro-guide-secu-info-print_0.pdf

Annexe 5 – Les mesures de cybersécurité s’appliquant aux réseaux Wi-Fi

Il est demandé de suivre les recommandations [DR06] de l’ANSSI qui s’appliquent aux réseaux Wifi sur des périmètres industriels [DR07] et de respecter à minima l’ensemble des mesures suivantes :

- Lorsqu’il s’agit de configurer un point d’accès Wifi, il est demandé de configurer le point d’accès pour utiliser un chiffrement robuste. Le mode WPA2 avec l’algorithme de chiffrement AES-CCMP est fortement recommandé,
- Il est demandé de s’interfacer avec une infrastructure d’authentification centralisée en s’appuyant sur WPA-Entreprise (standard 802.1x et protocole EAP), et d’utiliser une des méthodes d’authentification suivantes :
 - EAP-TLS, qui exige toutefois une Infrastructure de Gestion de Clés (IGC), avec clé privée et certificat à déployer auprès de chaque utilisateur. Lorsqu’EAP est utilisé, il convient par ailleurs que les clients vérifient l’authenticité du serveur d’authentification ;
 - EAP-TTLS, qui ne nécessite que le déploiement de certificats X509 serveurs et peut donc s’avérer plus pratique lorsqu’il est difficile de déployer des certificats clients. Ceux-ci s’authentifient alors généralement par couple utilisateur/mot de passe. Le support EAP-TTLS n’étant pas natif sous Windows, il convient de s’assurer qu’il est pris en charge par les clients Wi-Fi potentiels ;
 - PEAP, similaire à EAP-TTLS mais nativement pris en charge par Windows.
- Lorsque que le point d’accès Wi-Fi prend en charge la fonctionnalité de private Vlan invité et afin d’améliorer la protection en confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi, il est demandé de le configurer en mode isolated.
- Il est demandé de désactiver systématiquement la fonction WPS (Wi-Fi Protected Setup) des points d’accès.
- Sécuriser l’administration du point d’accès Wi-Fi, en:
 - utilisant des protocoles d’administration sécurisés (par exemple, HTTPS),
 - connectant l’interface d’administration à un réseau filaire d’administration sécurisé, a minima en y empêchant l’accès aux utilisateurs Wi-Fi,
 - utilisant des mots de passe d’administration robustes (respectant la politique de gestion des mots de passe présentée au chapitre Changer les éléments d’authentification par défaut sur les équipements et services), d’une longueur supérieure à 20 caractères.
- Il est demandé de rediriger l’ensemble des événements générés par les points d’accès vers l’infrastructure centrale de supervision de la DiRIF (solution Splunk),
- Il est demandé de remonter les événements de sécurité vers l’infrastructure centrale de supervision de la DiRIF (solution Splunk de la DiRIF),

- ## Annexe 6 – Le formulaire de demande de mise en place de règles de filtrage de flux

Guide d'intégration de la cybersécurité dans les projets de la DiRIF – V1.4 – 29/11/2021