



**Cadre de cohérence technique  
Normes et Contraintes**

# **Cadre de cohérence technique Normes et Contraintes**

<b>Date</b>	<b>Version</b>	<b>Auteur</b>
03/06/13	0.1	MCC
17/01/14	0.4	MCC
23/02/16	1.0	Pierre Le Clainche (SDSI/BEP)
29/06/16	1.1	Pierre Le Clainche (SDSI/BEP)
03/2017	2017.01	MCC
07/2017	2017.02	Pierre Le Clainche (SDSI/BEP)
11/2017	2018.01	Pierre Le Clainche (SDSI/BEP)
04/2018	2018.05	MC
01/2019	2019.00	MC
03/2019	2019.03	MC
05/2019	2019.04	MC
08/2020	2020.01	



## **Cadre de cohérence technique Normes et Contraintes**

### **SOMMAIRE**

<b>1 PRÉSENTATION GÉNÉRALE.....</b>	<b>3</b>
1.1 OBJECTIF DU DOCUMENT.....	3
1.2 DOCUMENTS DE RÉFÉRENCES.....	4
<b>2 EXPLOITATION.....</b>	<b>5</b>
2.1 RÉPARTITION DE LA CHARGE / PROXY.....	5
2.2 SAUVEGARDES.....	5
2.3 INDUSTRIALISATION.....	6
2.4 SUPERVISION.....	7
2.5 JOURNALISATION.....	8
2.6 CONFIGURATION.....	9
2.7 VIRTUALISATION.....	9
2.8 STOCKAGE.....	9
<b>3 ARCHITECTURE TECHNIQUE.....</b>	<b>11</b>
3.1 MODÈLE ET SERVICES.....	11
3.2 API.....	11
3.3 CONCEPTION.....	12
3.4 DOCUMENTATION.....	12
3.5 LOGICIELS ET SYSTÈME.....	13
3.6 DÉCOUPAGE EN ZONE.....	13
<b>4 DÉVELOPPEMENT.....</b>	<b>14</b>
4.1 GÉNÉRAL.....	14
4.2 JAVA ET PHP.....	15
4.2.1 Tiers application.....	16
4.2.2 Tiers données.....	16
4.2.3 Tiers présentation.....	17
<b>5 POSTE DE TRAVAIL.....</b>	<b>18</b>
<b>6 RÉSEAU.....</b>	<b>18</b>
7 SÉCURITÉ.....	21
7.1 POSTE DE TRAVAIL.....	21
7.2 CHIFFREMENT.....	21
7.3 APPLICATIONS.....	21
<b>9 FORMAT D'ÉCHANGE.....</b>	<b>25</b>
9.1 GÉNÉRAL.....	25
9.2 SIG.....	25
9.3 MULTIMÉDIA.....	26
<b>10 RÈGLES SUPPRIMÉES.....</b>	<b>27</b>

**Cadre de cohérence technique  
Normes et Contraintes**

# 1 PRÉSENTATION GÉNÉRALE

## 1.1 OBJECTIF DU DOCUMENT

Ce document fait partie du cadre de cohérence technique (CCT) du Ministère de la Culture (MC).

Le CTT est composé de plusieurs documents :

- Socle technique : (MC\_CCT\_STE\_vAAAA.X.odt) document regroupant les différents composants techniques et les versions associées. Ce document offre une vision de ce que doit être le système d'information du MC pour ce qui est des composants techniques mis en place sur les différents projets du MC. Sont traités dans ce document les aspects :
  - Infrastructure : OS, composants système, base de données, bases NoSQL ;
  - Développement : langages, API et framework ;
  - Bureautique : antivirus, suite logicielles, messagerie, etc.
  - Solution logicielle (CMS, GED etc.)
- Normes et contraintes (présent document) : (MC\_CCT\_NOC\_vAAAA.X.odt) Ce document regroupe l'ensemble des règles à suivre impactant la « façon de faire » les projets, notamment sur les sujets suivants :
  - Architecture et conception
  - Développement
  - Exploitabilité
  - Réseau
  - Sécurité
  - Documentation
- Normes de développement API REST : (MC\_CCT\_API\_REST\_vAAAA.X.odt) Ce document regroupe l'ensemble des règles à suivre lors du développement d'une API REST pour le compte du ministère de la Culture ;
- Application en mode logiciel à la demande (SaaS) : (MC\_CCT\_Mode\_SaaS\_vAAAA.X.odt) Ce document regroupe l'ensemble des règles à suivre lors de la mise en œuvre d'une application en SaaS. Ce document sera communiqué en phase de réalisation de projet.

Le CCT est versionné comme suit « vAAAA.X » où :

- AAAA correspond à l'année de rédaction du document
- x correspond à la version de l'année de référence.

Le CCT s'applique à partir de l'année AAAA jusqu'à ce qu'une version plus récente s'applique et remplace de fait la version précédente.

Dans ce document, la colonne « Statut », indique l'état d'une règle par rapport à la version précédente (nouveau, modifié, identique). Tout écart d'usage avec ce document doit faire l'objet d'une explication argumentée de la part des prestataires de réalisation et d'une validation explicite de la part du Ministère.

En cas de mise en place d'un produit et non d'un développement spécifique, certaines règles ou contraintes peuvent ne pas être compatibles avec le produit en question. Dans ce cas, il est demandé au prestataire de lister ces différences et de proposer une solution alternative.



## **Cadre de cohérence technique Normes et Contraintes**

### **1.2 DOCUMENTS DE RÉFÉRENCES**

<b>Document</b>	<b>Description</b>
MC_CCT_STE	Socle technique de référence
MC_CCT_Mode_SaaS	Contraintes liées à l'utilisation des applications en mode SaaS
MC_CCT_API_REST	Contraintes liées à la mise en place d'une API Rest
RGAA	Référentiel Général d'Accessibilité pour les Administrations
RGI	Référentiel Général d'Interopérabilité
Cadre Commun d'Urbanisation SI Etat	Description des 5 couches de l'urbanisation (stratégie, métier, fonctionnelle, applicative et infrastructure) avec des règles de dérivation
Cadre Commun d'Architecture des Référentiels de données	Règles communes d'architecture et de gestion des référentiels de données métier.
RGS	Référentiel général de sécurité
PSSIE	Politique de Sécurité des Systèmes d'Informations de l'État
ANSSI	Agence nationale de sécurité des systèmes d'information
SI	Système d'information
SSI	Sécurité des systèmes d'information

**Cadre de cohérence technique  
Normes et Contraintes**

## 2 EXPLOITATION

### 2.1 RÉPARTITION DE LA CHARGE / PROXY

N°	Titre	Statut
E1-01	La solution privilégiée pour la répartition de charge est la solution logicielle HAProxy	Identique
E1-02	Les mécanismes de haute disponibilité et de répartition de charge entre les serveurs de présentation et les serveurs d'application sont ceux présents nativement dans les technologies utilisées.	Identique
E1-03	La charge nominale doit pouvoir être absorbée lors d'un incident sur au moins un élément redondé. Par exemple s'il y a 3 instances applicatives prévues chaque instance doit pouvoir absorber 50 % de la charge nominale, afin d'absorber la charge nominale en cas de défaillance d'une instance.	Identique
E1-04	A l'exception des applications très sensibles, l'hébergement des « tiers » d'une application s'effectue sur des environnements mutualisés.	Identique
E1-05	Une application utilisant un socle technique donné doit être développée dans un souci de compatibilité avec les autres applications utilisant ce même socle.	Identique
E1-06	Toutes les applications Web sont situées derrière au moins un reverse proxy (type apache httpd) et potentiellement un répartiteur de charge (de type HAProxy). La mise en place de ces éléments techniques doit être transparent pour l'application.	Identique
E1-07	Toute application doit prendre en compte l'utilisation de proxy sortant pour accéder des services externes.	Identique
E1-08	Toutes les applications doivent pouvoir être exposées sur plusieurs noms de domaines (par exemple un domaine interne, un domaine Internet, un domaine RIE/ADER) sans impacts sur l'application. Ceci sous entend que tous les liens http dans une application doivent être relatifs.	Identique
E1-09	Les règles de reverse proxy sont à la charge du prestataire de réalisation.	Identique
E1-10	Les reverse proxies sont généralement mutualisés et fournis par la SDSI	Identique

### 2.2 SAUVEGARDES

N°	Titre	Statut
E2-01	Chaque application doit prévoir un plan de sauvegarde incluant une procédure de sauvegarde et de restauration. La procédure de sauvegarde doit distinguer les données métier (fichier, base de données) des données techniques (fichiers de paramétrage).	Identique
E2-02	Le plan de sauvegarde doit inclure la durée de rétention, la fréquence des sauvegardes, et le type (incrémentale, totale, etc.), l'heure de passage des sauvegardes en fonction des contraintes projet	Identique
E2-03	La sauvegarde des données applicatives s'appuie sur des solutions mutualisées mises en œuvre par le ministère.	Identique



## Cadre de cohérence technique Normes et Contraintes

### 2.3 INDUSTRIALISATION

N°	Titre	Statut
E03-01	Toute application (ou sous-application) doit être identifiée par un trigramme	Identique
E03-02	Chaque version applicative doit être clairement identifiable et numéroté x.y.z où : <ul style="list-style-type: none"><li>x : numéro de version majeure</li><li>y : numéro de version mineure</li><li>z : bugfix</li></ul> Il est <b>interdit</b> de livrer un composant en version SNAPSHOT.	Identique
E03-03	Le nom des binaires applicatifs (issus d'un développement spécifique) doit porter les informations : <ul style="list-style-type: none"><li>Le nom ou le trigramme de l'application</li><li>Le numéro de version</li></ul> Par exemple : <b>&lt;TRIGRAMME_APP&gt;_x.y.z.war</b>  Afin de conserver un nom stable lors des déploiements de war l'utilisation de liens symboliques est recommandée.	Identique
E03-04	Le nom du livrable doit être normé, par défaut : [TRIGRAMME_APPLICATION]_[SOUS_APPLICATION].X.Y.Z où : <ul style="list-style-type: none"><li>TRIGRAMME_APPLICATION correspond au trigramme de l'application</li><li>SOUS_APPLICATION correspond éventuellement à l'identification d'un sous module de l'application</li><li>X.Y.Z correspond au numéro de version</li></ul>	Identique
E03-05	Les livrables doivent être compressés au format zip contenant un répertoire racine nommé à l'identique du nom du fichier livré contenant l'arborescence suivante : <ul style="list-style-type: none"><li>src : fichiers source de l'application</li><li>bin : fichiers binaires</li><li>etc : fichiers de configuration</li><li>scripts : scripts d'exploitation (sh)</li><li>doc : documents d'installation et procédure spécifique à cette livraison.</li><li>git : zip contenant le ou les repos git de développement au format bare</li><li>A la racine un fichier release note détaillant les modifications macroscopiques par rapport à la version précédente.</li></ul>	Modifiée
E03-06	Chaque livraison doit être complète avec les éléments ci-dessus. Dans le cas contraire, le ministère se réserve le droit de refuser la livraison.	Identique
E03-07	Sauf mention contraire, les scripts système doivent être au format linux et de type <b>bash</b>	Identique
E03-08	Tout traitement automatique de type batch doit renvoyer un code retour suivant les différents cas possibles de réussite et d'échec. La documentation associée doit faire apparaître la description des codes retour.	Identique
E03-09	Tout composant applicatif doit générer des fichiers de logs configurable (emplacement et verbosité).	Identique
E03-10	Une procédure de compilation doit systématiquement être prévue et doit permettre de générer les binaires livrés à partir des sources livrées	Identique
E03-11	L'utilisation de MAVEN pour la gestion du cycle de développement des projets JAVA est obligatoire	Identique



## Cadre de cohérence technique Normes et Contraintes

E03-12	Le projet doit fournir les url de l'ensemble des repository MAVEN utilisés (hors maven central). En cas d'utilisation de librairies non disponible sur les repository publiques, ces librairies doivent être inclus dans le livrable et un script sh/bat permettant de l'ajouter au repository local doit être livré.	Modifiée
E03-13	En cas de présence de plusieurs batchs sur un projet un plan de programmation doit être fourni présentant la séquence de passage, la plage horaire prévue et l'ordonnancement éventuel.	Identique
E03-14	L'organisation des répertoires sur les serveurs doit respecter les standard linux à savoir : <ul style="list-style-type: none"> <li>• fichiers de logs dans /var/log/app</li> <li>• application binaire dans /var/opt/app</li> <li>• fichiers de configuration dans /etc/app où app correspond au nom ou trigramme de l'application.</li> </ul>	Identique
E03-15	Il est demandé de fournir des scripts au format systemd permettant de réaliser les opérations de base d'exploitation pour <b>chaque</b> composant applicatif : <ul style="list-style-type: none"> <li>• Démarrer un service/une application/un batch</li> <li>• Arrêter un service/une application/un batch</li> <li>• Vérifier le status (démarré/arrêté et idéalement la version installée)</li> </ul>	Identique
E03-16	Le plan de la documentation technique (GEX, DAT) est fourni par la SDSI et doit être respecté. Il peut cependant être adapté pour les besoins particuliers des projets.	Identique
E03-17	La procédure d'installation doit prévoir un mécanisme de retour-arrière, par exemple avec l'utilisation de liens symboliques vers les livrables.	Identique
E03-18	La procédure d'installation doit autant que possible être automatisée par scripts ou package rpm. En cas de livraison au format rpm, le source rpm doit être livré.	Identique
E03-19	Pour chaque livraison une estimation de la durée d'installation nécessaire doit être fournie permettant de planifier la durée d'interruption de service.	Identique
E03-20	Il est demandé de prévoir l'automatisation du démarrage des services lors de la procédure d'installation.	Identique
E03-21	La rotation de log doit utiliser logrotate	Identique

### 2.4 SUPERVISION

N°	Titre	Statut
E04-01	En cas d'erreur sur un traitement batch celui-ci doit notifier l'erreur, par l'envoi d'e-mail en précisant à minima le fichier de logs à consulter.	Identique
E04-02	Chaque application – hors contrainte de produit – doit inclure une page de monitoring présentant son état avec les informations suivantes : <ul style="list-style-type: none"> <li>• Numéro de version de l'application</li> <li>• Vérification d'accès vers l'ensemble des composants tiers qu'elle appelle (base de données, annuaire LDAP, autre application, librairie système nécessaire, etc.).</li> </ul> <p>Cette page doit être facilement interprétable par une sonde de supervision de type nagios, par exemple check_http avec une regex (pas de page html décorée, avec javascript etc.)</p>	Identique



## Cadre de cohérence technique Normes et Contraintes

E04-04	L'URL de la page de supervision doit être facilement identifiable afin d'en interdire l'accès par des règles de reverse proxy simple (par exemple via l'utilisation d'un sous-contexte particuliers /exploitation/ ou /monitoring/).	Identique
E04-05	Un batch traitant de gros volumes de données doit indiquer son état d'avancement dans les logs	Identique
E04-06	Une durée estimative de temps d'exécution doit être précisée dans la documentation technique pour chaque traitement batch.	Identique

### 2.5 JOURNALISATION

N°	Titre	Statut
E05-01	La génération des logs applicatives doit se baser sur une solution permettant de paramétrer l'emplacement et la verbosité des logs.	Identique
E05-02	La politique de logs définissant le niveau de logs et la politique de rotation doit être externalisée des binaires applicatifs.	Identique
E05-03	Les logs applicatifs doivent à minima contenir les éléments suivants : <ul style="list-style-type: none"> <li>• Horodatage</li> <li>• Niveau de log</li> <li>• Classe ou objet générant la trace</li> <li>• Message explicite et permettant une première analyse</li> </ul>	Identique
E05-04	Afin d'éviter une saturation des fichiers de logs, une politique de rotation de logs doit être définie précisant si la rotation est effectuée sur n fichiers d'une taille fixe ou sur une date.	Identique
E05-05	L'application doit disposer d'un mode debug, qui permet, en cas de défaillance, de comportement suspect, ou de test intensif, de suivre pas à pas son déroulement (horodatage du début et de la fin de chaque module applicatif au minimum). Le mode debug correspond à minima à la bascule des logs à un niveau DEBUG. Ce mode trace doit ainsi permettre : <ul style="list-style-type: none"> <li>- de suivre pas à pas le déroulement des opérations, à un niveau très fin (opération unitaire de donnée stockée, de transfert de message, de traitement)</li> <li>- de fournir le contenu des données liées aux opérations précédentes</li> <li>- d'indiquer précisément la position de l'opération dans le programme - de détailler précisément toutes les erreurs, ou problèmes, même internes</li> </ul> La possibilité de passer en mode debug à chaud serait appréciée.	Identique
E05-06	Tout processus d'une application doit «journaliser» le moment où il est lancé et le moment où il s'arrête. En cas de fin anormale, un message d'erreur doit être journalisé. La description de ce message doit être contenue dans la documentation de mise en exploitation.	Identique
E05-07	La documentation technique de l'application doit préciser la taille disque nécessaire aux logs afin d'éviter toute saturation.	Identique
E05-08	Tout composant applicatif de type application web doit fournir 2 types de logs distincts : <ul style="list-style-type: none"> <li>• Logs d'accès</li> <li>• Logs applicatifs</li> </ul>	Identique
E05-09	Le format des logs d'accès doit respecter le format du fichier accesslog d'apache httpd. Si ce n'est pas le cas, le prestataire doit fournir le pattern grok correspondant	Identique





## **Cadre de cohérence technique Normes et Contraintes**

E05-10	<p>Le format des logs applicatifs doit respecter le pattern log4j suivant (<a href="https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html">https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html</a>):</p> <pre>%d %p [%t] %C{1} - %m\n</pre> <p>où :</p> <ul style="list-style-type: none"><li>%d correspond à la date du log (au format yyyy-MM-dd HH:mm:ss,SSS)</li><li>%p correspond au niveau de log (INFO, DEBUG, ERROR, etc.)</li><li>%t correspond au nom du thread courant</li><li>%C correspond au nom de la classe générant le log</li><li>%m correspond au message</li></ul> <p>remarque : En cas de problème de performance, il est possible de ne pas utiliser le %C Le chiffre suivant le %C et entre {} correspond à une limitation dans le nom complet de la classe + package. Il est laissé libre.</p>	Identique
--------	--	-----------

## **2.6 CONFIGURATION**

N°	Titre	Statut
E06-01	Le format de fichier de configuration à privilégier est le fichier de propriétés clé/valeur	Identique
E06-02	Le(s) fichier(s) de configuration de l'application doi(ven)t être externalisé(s) des binaires applicatifs et de l'arborescence du serveur applicatif. Un nouveau déploiement du binaire ne doit pas remplacer le(s) fichier(s) de configuration.	Identique
E06-03	Le(s) fichier(s) de configuration doi(ven)t regrouper l'ensemble du paramétrage propre à l'environnement où il est exécuté.	Identique
E06-04	Il est demandé que le nombre de fichiers de configuration pour un module applicatif soit limité, idéalement à un seul fichier.	Identique
E06-05	Dans le cas où plusieurs fichiers de configuration sont présents pour un même composant applicatif, il n'est pas admissible de devoir renseigner la même propriété dans plusieurs fichiers. Dans ce cas un script sh doit permettre d'automatiser cette action.	Identique

## **2.7 VIRTUALISATION**

N°	Titre	Statut
E07-01	Le socle de virtualisation est basé sur des produits référencés au CCT.	Identique
E07-02	Les applications et sites Web sont – sauf mention contraire – déployées sur le socle de virtualisation du MC.	Identique

## **2.8 STOCKAGE**

N°	Titre	Statut
----	-------	--------



**Cadre de cohérence technique  
Normes et Contraintes**

E08-01	La documentation technique doit décrire la volumétrie nécessaire pour le projet : <ul style="list-style-type: none"><li>• Exploitation : (logs, livrables, sauvegardes, etc.)</li><li>• Base de données (données, indexes, etc.)</li><li>• Espace disque (index type lucene)</li><li>• Espace disque partagé ; • etc.</li></ul>	Identique
E08-02	La documentation technique doit préciser les partitions partagées.	Identique



## **Cadre de cohérence technique Normes et Contraintes**

### **3 ARCHITECTURE TECHNIQUE**

#### **3.1 MODÈLE ET SERVICES**

N°	Titre	Statut
AT01-01	Toutes les informations saisies ou envoyées en entrée du serveur doivent être contrôlées au niveau du serveur, y compris celles déjà validées au niveau du client.	Identique
AT01-02	Une application WEB doit être du type N-Tiers.	Identique
AT01-03	Le ministère s'appuie sur le standard Java (Spring) ou sur des architectures à base de PHP pour le développement des applications développées et/ou hébergées par le ministère.	Identique
AT01-04	Toutes les couches d'une application doivent être indépendantes. Les interfaces entre les couches doivent s'appuyer sur des normes et standards.	Identique
AT01-05	Une application ne doit comporter aucune adhérence vis-à-vis du matériel d'un constructeur particulier sur les équipements serveurs, stockage, sauvegardes et réseau.	Identique
AT01-06	Chaque tiers d'une application multi-tiers doit être indépendant des autres niveaux. Il faut définir avec précision les interfaces pour permettre l'indépendance entre ces niveaux et la modification de l'un d'entre eux (déplacement, multiplication des instances, multiplication des serveurs, ...) sans impact sur les autres.	Identique
AT01-12	L'usage du protocole HTTPS est obligatoire dès lors qu'une authentification est requise. De façon générale l'utilisation du protocole HTTPS est recommandé	Identique

#### **3.2 API**

N°	Titre	Statut
AT-API-01	Lors de la création de services Web, l'approche top/bottom est à privilégier en commençant par la définition des API avant leur implémentation.	Identique
AT-API-02	En cas de mise en place de services REST, il est demandé de traiter les erreurs avec un code http correspondant à l'erreur et de renvoyer un contenu de type JSON avec à minima : <ul style="list-style-type: none"><li>• Un code</li><li>• Une description</li></ul> Il est interdit de renvoyer une pile d'exécution ou des informations permettant de comprendre l'architecture sous-jacente mise en place.	Identique
AT-API-03	Le format d'API REST/JSON est à privilégier au format SOAP/XML	Identique
AT-API-04	En cas de mise en place d'API sur un projet (y compris pour des besoins internes au projet), il est demandé de façon obligatoire, de réaliser la documentation de l'API au format openAPI (v2 minimum v3 recommandée) <a href="https://www.openapis.org/">https://www.openapis.org/</a> . Cette définition devra être réalisé avec l'outil swagger ( <a href="https://swagger.io/">https://swagger.io/</a> ). Les fichiers de définition yaml et json sont des livrables attendus du projet.	Modifiée



## **Cadre de cohérence technique Normes et Contraintes**

AT-API-05	Une API Rest doit être compatible avec le modèle de maturité de Richardson au moins au niveau 2 (utilisation correcte des verbes et des codes retour du protocole http) Voir le document MC_CCT_API_REST_AAAA.xx	Identique
AT-API-06	Dans le cadre de la mise en œuvre d'une architecture orientée service, il est recommandé de s'appuyer sur les Web Services SOAP ou REST.	Renommée (AT01-07)
AT-API-07	L'utilisation des Web Services REST est à privilégier. Toute autre utilisation est soumise à l'approbation du ministère.	Renommée (AT01-08)
AT-API-08	En cas de mise en place de services REST, il est demandé de documenter l'ensemble des services incluant les différentes URI définies, les verbes http autorisés, les codes retour possibles. Cette documentation devra utiliser le standard OpenAPI (v2 minimum v3 recommandée).	Renommée (AT01-09)

### **3.3 CONCEPTION**

N°	Titre	Statut
AT02-01	L'utilisation de diagrammes et de conventions de représentations graphiques ne suffit pas. Il est nécessaire d'associer les graphiques d'une description textuelle en français.	Identique
AT02-02	Il est demandé d'utiliser le langage de modélisation UML et/ou BPMn pour la modélisation de processus. Il est demandé les diagrammes UML suivants : <ul style="list-style-type: none"><li>• Cas d'utilisation</li><li>• Classe</li><li>• État-transition</li><li>• Séquence (lors de traitement faisant interagir plusieurs composants techniques)</li></ul>	Identique
AT02-03	Le MCD et le MPD doivent être maintenus à jour et livré à chaque livraison	Identique

### **3.4 DOCUMENTATION**

N°	Titre	Statut
AT03-04	En phase de travail nécessitant les relectures et l'édition, la documentation du projet doit être livrée au format open document : <ul style="list-style-type: none"><li>• ODT pour le texte,</li><li>• ODS tableur</li></ul>	Identique
AT03-05	La version finale d'un document peut être livrée au format PDF	Identique
AT03-06	Afin d'harmoniser les livrables des plans type des documents techniques suivants sont fournis : <ul style="list-style-type: none"><li>• Dossier d'Architecture Technique (DAT)</li><li>• Guide d'Exploitation (GEX)</li></ul> Ces plans peuvent être enrichis par le prestataire en fonction des besoins de son projet. Ils seront présentés au prestataire en début de projet.	Identique
AT03-07	Concernant la partie technique des projets, il est attendu, sauf mention contraire, les documents suivants : <ul style="list-style-type: none"><li>• Dossier d'Architecture Technique (DAT)</li><li>• Guide d'exploitation (GEX)Un document de Spécifications techniques détaillées (STD) peut être demandé).</li></ul>	Identique



## **Cadre de cohérence technique Normes et Contraintes**

### **3.5 LOGICIELS ET SYSTÈME**

N°	Titre	Statut
AT04-01	Toute application métier doit fonctionner sur un système d'exploitation conforme aux standards POSIX et/ou LSB (Linux Standard Base) et référencés dans le CCT.	Identique
AT04-02	Pour les serveurs, l'installation d'un noyau 64 bits du système d'exploitation est fortement recommandé.	Identique

### **3.6 DÉCOUPAGE EN ZONE**

N°	Titre	Statut
AT05-01	Les applications doivent respecter une étanchéité entre les zones applicatives Internet et zone applicative Intranet	Identique
AT05-02	Les applications doivent respecter un découpage au sein d'une zone (Internet ou Intranet) : <ul style="list-style-type: none"><li>• DMZ (reverses proxies, cache applicatif, etc.)</li><li>• Application (serveur Web, serveur applicatif, batch, etc.)</li><li>• Données (SGBR, base NoSQL, etc.)</li></ul>	Identique
AT05-03	Les communications inter zones Intranet / Internet sont interdites par défaut, en cas de besoins de ce type, les modalités de communication (port, protocole, sens des échanges, etc.) seront à discuter en atelier technique.	Identique
AT05-04	Seules les communications de la zone Intranet vers la zone Internet sont autorisées. Des mécanismes de publication de données peuvent prévoir des copies de données entre ces 2 zones.	Identique



## Cadre de cohérence technique Normes et Contraintes

### 4 DÉVELOPPEMENT

#### 4.1 GÉNÉRAL

N°	Titre	Statut
D01-01	Les applications doivent se conformer au RGAA (Référentiel Général d'Accessibilité pour les Administrations).	Identique
D01-02	Le niveau d'accessibilité souhaité et les tests associés sont précisés au cas par cas par chaque projet. La cible étant un niveau AA sur les projets ouverts sur Internet.	Identique
D01-03	Les applications doivent se conformer au RGI (Référentiel Général d'Interopérabilité).	Identique
D01-04	Les applications doivent se conformer au RGS (Référentiel Général de Sécurité). Tout écart doit être signalé et justifié et accepté par le ministère. L'ensemble du corpus RGS est accessible sur le site de l'ANSSI ( <a href="http://www.ssi.gouv.fr/">http://www.ssi.gouv.fr/</a> ).	Identique
D01-05	Pour les échanges applicatifs, le ministère impose l'utilisation du protocole http(s) et échanges via Web Services. L'utilisation des EJB n'est pas autorisée.	Identique
D01-06	Les fonctions de recherche – sauf mention contraire – ne doivent pas être sensibles à la casse.	Identique
D01-07	Les temps de réponse moyens des pages Web ne doivent pas dépasser – sauf mention contraire – les temps suivants : <ul style="list-style-type: none"> <li>• Page ou recherche simple : 2s</li> <li>• Page ou recherche complexe : 5s</li> </ul>	Identique
D01-08	Les applications doivent se conformer au document inter ministériel « Cadre Commun d'Urbanisation SI Etat »	Identique
D01-09	Les applications doivent se conformer au document inter ministériel « Cadre Commun d'Architecture des Référentiels de données »	Identique
D01-10	Lors de l'utilisation de composants open source, en cas d'anomalie constatée sur le composant si un correctif ou une évolution est nécessaire : <ul style="list-style-type: none"> <li>• L'administration doit en être informée</li> <li>• Le correctif ou l'évolutif doit être soumis à la communauté gérant le composant.</li> </ul>	Identique
D01-11	Il est demandé d'utiliser le gestionnaire de versions GIT.	Identique
D01-12	L'administration demande à chaque livraison un clone complet du repository git du projet (git clone –mirror) en plus des sources de l'application (sauf si le projet est accessible sur un repository public : github / gitlab). Si l'export est anonymisé (nom des développeurs : dev1 à devN) cela doit être prévu dès le départ du projet afin de conserver un historique propre du projet.	Modifiée
D01-13	L'export des repos git doit respecter les contraintes suivantes : export avec la commande --mirror <ul style="list-style-type: none"> <li>• Tous les répertoires contenant un repos git doivent être suffixés par '.git'</li> <li>• Une archive zip doit être créée contenant le ou les repos git et doit être nommée : &lt;NOM_PROJET&gt;-git-repos-&lt;VERSION&gt;.zip où <ul style="list-style-type: none"> <li>◦ NOM_PROJET correspond au nom du projet</li> <li>◦ VERSION correspond à la version au format x.y.z</li> </ul> </li> </ul>	Identique



## Cadre de cohérence technique Normes et Contraintes

D01-14	<p>Il est demandé la gestion des branches de développement au sens git comme suit :</p> <ul style="list-style-type: none"> <li>• Une branche, par défaut <b>master</b>, doit correspondre à une branche de livraison contenant les versions (tags) livrées à l'administration. Cette branche doit <b>toujours</b> être compilable et ne doit <b>jamaïs</b> contenir de version SNAPSHOT</li> <li>• Une branche, par défaut develop, doit contenir les versions « propres » internes au prestataire. Cette branche correspond à la branche de recette interne du prestataire. Cette branche se <b>merge</b> dans la branche master</li> <li>• Les branches sous la branche develop sont laissées à la libre utilisation du prestataire et correspondent au développement des fonctionnalités.</li> </ul> <p>Théoriquement, en développement, les opérations de push sont réalisées sur les branches sous la branche develop. Les branches develop et master ne reçoivent que des merges.</p> <p>Si la branche de livraison est différente de master, il convient de préciser à l'administration le nom de cette branche et de l'indiquer dans la documentation technique (GEX).</p>	Modifiée
--------	--	----------

### 4.2 JAVA ET PHP

N°	Titre	Statut
D02-01	Le PHP est utilisé pour les applications de type CMS ou petites applications.	Identique
D02-02	Les applications métier sont développées en Java.	Identique
D02-03	Lors des développements spécifiques il est demandé d'utiliser Maven pour gérer le cycle de développement.	Identique
D02-04	Lors de l'utilisation de MAVEN, Il doit être possible de générer les binaires à partir des sources à partir de des commandes Maven standard : « mvn package ». Toute action complémentaire (par exemple l'installation de librairies tierces et non présentes sur les repos Maven) doit être documentée.	Identique
D02-05	La liste des repository MAVEN nécessaires (hors maven central) à la compilation et au packaging d'une application doit être fournie	Modifiée
D02-06	La présence de commentaires dans le code est fortement recommandée, surtout sur les parties de codes complexes.	Identique
D02-07	La javadoc doit être à présente avec à minima les informations suivantes : Description des méthodes, des paramètres d'entrée/sortie et des exceptions	Identique
D02-08	<p>La politique de qualité du code du prestataire doit être précisée : par exemple checkstyle, PMD, cobertura, sonar, findbugs, formatter Eclipse etc. et la politique / fichiers de configuration associés doivent être livrés au MC.</p> <p>Le MC analyse le code source via Sonar et utilise les plugins suivants :</p> <ul style="list-style-type: none"> <li>• checkstyle-sonar-plugin</li> <li>• qualinsight-sonarqube-smell-plugin</li> <li>• sonar-findbugs-plugin</li> <li>• sonar-groovy-plugin</li> <li>• sonar-java-plugin</li> <li>• sonar-l10n-fr-plugin</li> <li>• sonar-pmd-plugin</li> </ul>	Identique
	<ul style="list-style-type: none"> <li>• sonar-typescript-plugin</li> </ul>	



## Cadre de cohérence technique Normes et Contraintes

D02-09	L'utilisation de framework permettant de gérer la structure des projets (l'injection de dépendances, configuration) comme Spring est fortement recommandée.	Identique
D02-10	Le développement par couche est demandé avec à minima les couches : <ul style="list-style-type: none"><li>• Présentation ou Controller,</li><li>• Métier ou service</li><li>• DAO</li></ul>	Modifiée
D02-11	L'ensemble des paramètres de l'application doit être externalisé en fichier de configuration (pas de paramétrage « en dur »).	Identique
D02-12	Des tests unitaires sont demandés par l'administration, leur exécution doit être possible via les mécanismes standard de Maven.	Identique
D02-13	Sur les projets Maven, le groupId à utiliser est « fr.gouv.culture.[nomProjet] », l'artifactId correspond au nom du module applicatif.	Identique
D02-14	Sur les projets Maven, aucune référence à l'environnement d'intégration du prestataire ne doit être présente dans le fichier pom.xml afin de garantir la portabilité du build sur les environnements du ministère.	Identique
D02-15	Il est demandé de placer un fichier README.md au format markdown à la racine de chaque module applicatif	Identique
D02-16	Le fichier README.md doit contenir à minima : <ul style="list-style-type: none"><li>• Le nom du projet – nom du module en titre niveau 1</li><li>• Un chapitre description de niveau 2 présentant le projet et le module applicatif</li><li>• Un chapitre compilation de niveau 2 présentant la procédure de compilation à partir des sources</li></ul> le reste est laissé libre au prestataire	Identique
D02-17	La SDSI est en cours de déploiement d'une solution d'intégration continue (jenkins). La procédure de compilation et de packaging de l'application doit donc respecter les standard, notamment maven.  <b>Une erreur de compilation entraîne un rejet de livraison.</b>	Identique

### 4.2.1 Tiers application

N°	Titre	Statut
D03-01	Les applications JAVA doivent fonctionner avec le(s) conteneur(s) de servlet référencé(s) dans le CCT ou être exécutée en mode fatjar	Modifiée
D03-02	Dans une application web, un client ne peut communiquer avec son serveur d'application qu'en http ou https.	Identique
D03-03	Le framework Angular est à privilégier lors de la création d'ihm Web moyenne à complexe. Pour des applications plus simple, possibilité d'utiliser le framework vue.js	Modifiée

### 4.2.2 Tiers données

D04-01	L'accès aux bases de données n'est possible que depuis le tiers application.	Identique
D04-02	L'utilisation des triggers dans une base de données est déconseillé et doit être systématiquement justifiée.	Identique





## **Cadre de cohérence technique Normes et Contraintes**

D04-03	L'utilisation des procédures stockées n'est permise que dans les cas où les performances attendues ne peuvent être atteintes sans elles.	Identique
D04-04	Le tiers données et application ne sont pas sur le même serveur.	Identique

### **4.2.3 Tiers présentation**

<b>N°</b>	<b>Titre</b>	<b>Statut</b>
D05-01	Les applications doivent pouvoir être placées derrière un reverse proxy de type apache httpd et un répartiteur de charge de type HAProxy sans impact sur l'applicatif.	Identique



## **Cadre de cohérence technique Normes et Contraintes**

### **5**POSTE DE TRAVAIL

N°	Titre	Statut
PT01-01	Les applications doivent être indépendantes du système d'exploitation du poste client.	Identique
PT01-02	Les systèmes d'exploitation des postes utilisateurs doivent supporter et pouvoir mettre en œuvre les deux piles Ipv4 et Ipv6.	Identique
PT01-03	Lorsqu'un client de messagerie est utilisé, celui-ci doit être conforme aux directives du ministère et être compatible avec les composants recommandés dans le CCT.	Identique
PT01-04	Il est recommandé de ne pas utiliser les macros des suites bureautiques.	Identique
PT01-05	Les logiciels utilisés sur les postes de travail doivent être validés par le ministère. Cette validation cherche à favoriser les logiciels libres, indépendants du système d'exploitation.	Identique
PT01-06	Les versions des logiciels mentionnés dans le CCT sont les versions strictement imposées. Le déploiement de toute nouvelle version d'un logiciel sur le poste de travail doit être validée par comité CCT.	Identique
PT01-08	Les impressions doivent s'appuyer sur la gestion des imprimantes du poste de travail.	Identique
PT01-09	Les appliquestes (applets) Java sont proscrites. En cas de besoin, l'application pourra avoir recours à HTML5 et/ou Getdown / Update4j sous réserve de validation par le MC.	Modifiée

### **6**RÉSEAU

N°	Titre	Statut
R01-01	Tout port non nécessaire au fonctionnement normal d'une application doit être fermé.	Identique
R01-02	Il est obligatoire d'utiliser des ports TCP / UDP fixes.	Identique
R01-03	Tout composant raccordé au réseau doit se conformer au plan d'adressage IP du ministère de la Culture.	Identique
R01-04	Les ports spécifiques utilisés doivent être paramétrables pour permettre leur affectation lors des installations, évitant ainsi les doublons éventuels entre applications et facilitant les contrôles de flux réseau.	Identique
R01-05	L'utilisation des ports doit obligatoirement être conforme aux recommandations de l'IANA (ports standards compris entre 0 et 1023 et ports spécifiques à partir de 1024).	Identique



**Cadre de cohérence technique  
Normes et Contraintes**

R01-06	L'application utilisera des protocoles routables au-dessus de TCP avec des ports prédéfinis fixes. Pour les ports supérieurs à 1024, ils seront choisis dans la plage 8000 à 8999.	Identique
R01-07	Les flux applicatifs doivent s'appuyer sur des protocoles de transport standardisés : - TCP pour le mode connecté, - UDP pour l'échange de messages asynchrones.	Identique
R01-08	La topologie des infrastructures mutualisées (réseaux d'accès, réseaux de stockage...) ne peut évoluer dans le seul but de satisfaire les besoins d'une application spécifique.	Identique
R01-09	Les équipements réseaux doivent supporter et pouvoir mettre en œuvre les deux piles Ipv4 et Ipv6.	Identique
R01-10	Tout flux non explicitement autorisé est interdit.	Identique
R01-11	Le point de terminaison SSL côté ministère doit aboutir sur un reverse proxy.	Identique
R01-12	La connexion d'un serveur vers l'extérieur passe obligatoirement par un proxy sortant.	Modifiée
R01-13	L'accès à Internet à partir de l'application se fait via utilisation de proxy.  L'accès à l'application doit être transparent à l'utilisation de serveurs mandataires inverse « reverse-proxies » (apache).	Modifiée
R01-14	Pour l'utilisation de listes de diffusion, l'application s'appuiera sur le produit SYMPA en exploitation au ministère. L'ajout et la suppression d'abonnés dans des listes existantes se fera via l'interface SYMPA en mode messagerie. L'application planifiera la nuit l'envoi de messages à des listes de diffusion.	Identique
R01-15	Il est demandé de renseigner dans le document d'architecture de l'application (DAT) une matrice des flux présentant pour chacun le port, le protocole, la source et la destination tant pour les services internes qu'externe à l'application et au MC. Les ports non présents dans cette matrice seront considérés fermés.	Modifiée
R01-16	Le ministère de la Culture est organisé en multi-sites entre l'administration centrale et les services déconcentrés avec des débits variants entre ces sites et compris entre 4Mbs et 100Mbs.	Nouveau
R01-17	Chaque site du ministère de la Culture est protégé par un équipement de sécurité type firewall.	Nouveau
R01-18	Les différents sites du ministère de la Culture sont organisés autour d'un datacenter principal en région parisienne et d'un site de PRA en région.	Nouveau
R01-19	Une matrice des flux à jour tout au long du projet est demandée sur chaque projet explicitant les protocoles utilisés afin de gérer les ouvertures éventuelles de flux sur les équipements de sécurité.	Nouveau
R01-20	Tous les sites du ministère de la Culture ont un point d'accès au RIE (Réseau interministériel de l'État) permettant des communications avec des applications inter ministérielles.	Nouveau



**MINISTÈRE  
DE LA CULTURE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat  
Général**

Libellé : [MC\\_CCT\\_NOC\\_v2020.01.odt](#)

Auteur : [SNUM](#)

## **Cadre de cohérence technique Normes et Contraintes**

R01-21	L'accès Internet des différents sites se fait par la PFAI (plateforme d'accès à Internet) du RIE.	Nouveau
--------	---	---------



## **Cadre de cohérence technique Normes et Contraintes**

# **7SÉCURITÉ**

## **7.1 POSTE DE TRAVAIL**

N°	Titre	Statut
S01-01	Tout poste de travail ou serveur (Windows ou LSB) doit être équipé des antivirus qualifiés par le ministère, à jour de sa base antivirale. Complément : Les applications ne doivent ni nécessiter leur désactivation ni empêcher leur mise à jour (moteur ou base de signature) automatique telle que prévue par le ministère. L'analyse temps réel est activée. La mise à jour de la base de signatures est effectuée automatiquement et quotidiennement, sauf alerte urgente, auquel cas la diffusion peut être immédiate. Un « scan » hebdomadaire est effectué sur tous les médias locaux.	Identique
S01-02	L'environnement de travail doit être protégé contre les virus, les logiciels malveillants et les intrusions.	Identique
S01-03	Ni l'utilisation d'une application ni son installation ne doit nécessiter la désactivation ou gêner la mise à jour de l'antivirus et/ou de l'anti-logiciels malveillants et/ou du pare-feu.	Identique
S01-04	Sauf instruction contraire par les responsables sécurité, les systèmes d'exploitation et les logiciels installés sur les stations de travail doivent être à jour des correctifs validés par les structures en charge de la sécurité du SI.	Identique

## **7.2 CHIFFREMENT**

N°	Titre	Statut
S02-01	La confidentialité d'informations ou de documents entraîne de facto l'utilisation d'un outil de chiffrement adéquat conformément aux règles fixées par le référentiel général de sécurité (RGS)	Identique

## **7.3 APPLICATIONS**

N°	Titre	Statut
S03-01	Le protocole WS-Security doit être utilisé pour sécuriser les Web Services SOAP entre une application du ministère et celle d'un partenaire hors zone de confiance réseau.	Identique
S03-02	Les serveurs d'application, batch, script doivent être exécutés avec un utilisateur système dédié autre que root. Il appartient au prestataire de développement de définir cet utilisateur dans la documentation d'exploitation.	Identique



## Cadre de cohérence technique Normes et Contraintes

S03-03	Les applications doivent se conformer à la PSSIE (Politique de sécurité des systèmes d'information de l'Etat), voir <a href="http://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf">http://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf</a>	Identique
S03-04	La solution technique doit s'intégrer à l'infrastructure actuelle du ministère et	Identique
	être conforme aux règles de sécurité applicables. D'une manière générale, elle doit être à l'état de l'art sur les aspects sécurité. Elle doit prendre en compte l'ensemble des recommandations de l'ANSSI.	
S03-05	<p>Toute fonction d'authentification s'appuyant sur un couple « identifiant/mot de passe » mise en place dans le cadre d'un projet doit respecter les règles de base suivantes. Le système doit :</p> <ul style="list-style-type: none"><li>• contraindre une complexité minimale obligatoire paramétrable (nombre de caractères en général, types de caractères);</li><li>• forcer le changement de mot de passe au-delà d'une durée paramétrable;</li><li>• empêcher la réutilisation des X (paramétrable) derniers mots de passe;</li><li>• bloquer temporairement (durée paramétrable) le compte au-delà de X (paramétrable) tentatives infructueuses;</li><li>• invalider une session au-delà d'un délai qui doit être paramétrable</li><li>• en cas d'erreur sur le mot de passe ou l'identifiant, le message renvoyé par le système ne doit pas indiquer si le compte existe ou non.</li><li>• stocker une empreinte des mots de passe, générée selon un algorithme conforme au RGS. Une fonction de hachage doit être utilisée, avec une graine (« salt ») différente pour chaque utilisateur. En aucun cas le mot de passe ne doit être enregistré en clair dans la base.</li></ul> <p>De façon générale et sauf avis contraire de l'administration, l'authentification est réalisée sur l'annuaire LDAP du MC.</p>	Identique
S03-06	Le protocole https est obligatoire lors de l'échange des identifiants de connexion de l'utilisateur et lors d'ouverture de session applicative. Plus généralement, un mot de passe ne doit jamais circuler en clair sur le réseau et ne jamais être écrit dans les fichiers de logs.	Modifiée
S03-07	Un mot de passe ne doit <b>jamais</b> être stocké en clair dans une base de données ou annuaire LDAP.	Identique
S03-08	Lors d'échange de fichier le protocole <b>(S)</b> FTP est privilégié. Pour de la synchronisation de fichier, l'utilisation de rsync est autorisée.	Identique
S03-09	Les applications doivent être conformes aux recommandations de l'OWASP afin de se protéger contre les 10 principaux risques identifiés : <a href="http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a>	Identique
S03-10	Lors de l'accès aux données, il est interdit de construire une requête SQL par concaténation directe des paramètres. L'utilisation de preparedStatement ou namedQuery est obligatoire.	Identique



## **Cadre de cohérence technique Normes et Contraintes**

S03-11	Les stacktraces ne doivent pas être montrées à l'utilisateur. Plus généralement, les pages web (ou retour de service Web) d'une application ne doivent pas faire apparaître d'information sur l'architecture mise en place (serveur web, conteneur de servlet, OS, service applicatif, port, adresse IP, etc..). Ces informations ne doivent jamais être transmises, y compris en cas d'erreur..	Modifiée
S03-12	Les messages d'erreur doivent être anonymisés, par exemple en cas d'erreur d'authentification, le message ne doit pas distinguer les cas de mauvais login des cas de mauvais mot de passe.	Identique
S03-13	Les données dynamiques affichées en page HTML doivent être échappées et contrôlées afin d'éviter les failles XSS.	Identique
S03-14	Pendant la phase de réalisation et de garantie de l'application, le fournisseur	Identique
	s'engage à maintenir les différentes couches applicatives à jour des correctifs de sécurité.	
S03-15	Les événements pertinents en matière de sécurité, par exemple une connexion en tant qu'administrateur global de l'application, une suppression de données non réversible, doivent être inscrits dans un fichier journal, celui du système ou un journal propre à l'application, dans un format standard.	Identique
S03-16	La télémaintenance est proscrite à tout moment de la vie du projet puis de l'application.	Identique
S03-17	L'accès aux statistiques sera restreint aux agents du ministère de la Culture en charge du suivi applicatif et aux administrateurs systèmes. L'accès aux connexions système sera restreint aux administrateurs systèmes.	Identique
S03-18	Afin de garantir une bonne sécurité de l'application, il doit être possible d'identifier de manière fiable par leur URL les pages destinées au grand public (front-office), de celles destinées aux utilisateurs internes et aux administrateurs (back-office).	Identique
S03-19	Le nom des utilisateurs (et mot de passe) des bases de données n'est pas défini par le maître d'œuvre. Il doit être possible de les changer à tout moment sans impacts pour l'applicatif en dehors de la modification de fichiers de configuration.	Identique
S03-20	Toutes les applications livrées au MC font l'objet d'un audit de sécurité en interne MC. Le prestataire s'engage à apporter les modifications suite aux éventuelles vulnérabilités détectées.	Identique
S03-21	Les données en entrées d'un système (IHM et Web Services et paramètres de batchs) doivent être contrôlées (format, taille, etc.) côté serveur.	Identique
S03-22	Pendant la phase de réalisation et de garantie de l'application, les développements doivent rester compatibles avec les mises à jour de sécurité des logiciels utilisés (système d'exploitation, serveur web, moteur de servlets, bases de données...).	Identique



**Cadre de cohérence technique  
Normes et Contraintes**

S03-24	Les flux réseau pour lesquels la confidentialité et/ou l'intégrité doivent être garanties, qu'ils soient entre l'utilisateur et l'application ou entre deux systèmes, doivent être sécurisés par le biais de protocoles conformes au RGS (le plus souvent TLS). En aucun cas un mot de passe ne doit circuler en clair sur le réseau.	Identique
S03-25	Afin d'éviter l'afflux de messages indésirables (spam), il est recommandé de ne pas mentionner d'adresses de messagerie sous forme textuelles sur les sites publics, y compris dans les données non visibles (méta données, "Dublin core", références de liens, champs mailto:). Un système de « question/reponse » de type « captcha » permettant de bloquer l'usage par des robots doit être mis en place.  Lorsque l'envoi de messages est nécessaire, un formulaire de saisie devra être proposé permettant au public de contacter l'administration.	Identique
S03-26	Les applications utilisent des ressources mutualisées. Elles ne sont pas autorisées à modifier le paramétrage d'exploitation et de sécurité des environnements dans lesquels elles s'exécutent.	Identique
S03-27	Les produits proposés assurant une ou des fonctions de sécurité telles que des fonctions d'identification, de signature électronique, de confidentialité ou d'horodatage, doivent être si possible validés par l'ANSSI	Identique
S03-28	La durée de session d'une application Web est par défaut de 30 minutes	Identique





## **Cadre de cohérence technique Normes et Contraintes**

# **8 FORMAT D'ÉCHANGE**

## **9.1 GÉNÉRAL**

N°	Titre	Statut
FE01-01	Tout fichier XML doit être accompagné de son schéma.	Identique
FE01-02	En complément du RGI, tout fichier XML doit être encodé en Unicode. Plus généralement afin d'éviter tout problème d'encodage l'UTF-8 est demandé sur toute la chaîne applicative.	Identique
FE01-05	En complément du RGI, pour tous les échanges de documents bureautiques internes et externes, seuls les formats OpenDocument ISO 26300 et PDF sont autorisés.	Identique
FE01-06	Pour les échanges de données, l'utilisation du format XML ou JSON est recommandée.	Identique

## **9.2 SIG**

N°	Titre	Statut
FE02-01	Le format d'échange des fichiers géographiques retenu est le format ShapeFile et/ou GeoJSON	Identique
FE02-02	Lorsqu'une application doit exporter ou importer des flux d'informations géographiques avec d'autres système, l'utilisation des standards définis par l'OGC (Open Geospatial Consortium <a href="http://www.opengeospatial.org/">http://www.opengeospatial.org/</a> ) et normalisés par l'ISO est demandé, en particulier, utiliser les protocoles : <ul style="list-style-type: none"><li>• WMS : Web Map Service, norme ISO 19128, permet d'échanger des cartes</li><li>• WFS : Web Feature Service, permet d'échanger des données géographiques en XML (GML).</li></ul>	Identique
FE02-03	Le ministère impose l'utilisation des API et fonds de plan de l'IGN. Une clé d'utilisation sera fournie au prestataire lors du démarrage des prestations nécessitant cette technologie.	Identique
FE02-04	Les ShapeFiles doivent être accompagnés de méta données selon la norme internationale 19115	Identique
FE02-05	Le ministère utilise le système de projection Lambert 93 pour la métropole et UTM pour les DOM/TOM	Identique



## **Cadre de cohérence technique Normes et Contraintes**

### **9.3 MULTIMÉDIA**

<b>N°</b>	<b>Titre</b>	<b>Statut</b>
FE03-01	Les formats PNG et JPEG doivent être utilisés pour échanger les informations graphiques et les images fixes.	Renommée (FE01-03)
FE03-02	Les flux audiovisuels, s'ils sont autorisés par le ministère, doivent respecter les formats MPEG-2 ou MPEG-4.	Renommée (FE01-04)
FE03-03	<p>Les contenus de type vidéo du MC sont généralement mis en ligne sur la chaîne youtube du ministère : <a href="https://www.youtube.com/c/Minist%C3%A8redelaCultureFrance">https://www.youtube.com/c/Minist%C3%A8redelaCultureFrance</a> .</p> <p>Les contenus de type audio du MC sont généralement mis en ligne sur soundcloud : <a href="https://soundcloud.com/culture-gouv">https://soundcloud.com/culture-gouv</a></p> <p>Les applications manipulant ces types de contenu doivent prévoir un connecteur/lecteur vers ces diffuseurs de contenu multi-média.</p> <p>A noter que certains contenus sont également stockés sur la chaîne dailymotion dédiée au ministère de la culture.</p>	Renommée et (FE01-07) Modifiée



## Cadre de cohérence technique Normes et Contraintes

### 10 RÈGLES SUPPRIMÉES

Ce paragraphe regroupe les règles qui ont été supprimées ainsi qu'une explication associée.

N°	Titre	Statut
S03-22	Les événements pertinents en termes de sécurité, par exemple une connexion en tant qu'administrateur global de l'application, une suppression de données non réversible, doivent être inscrits dans un fichier journal, celui du système ou un journal propre à l'application, dans un format standard.	Doublon par rapport à la règle S03-15
E04-03	La page de monitoring décrite ci-dessus doit être sur un sous contexte applicatif facilement identifiable permettant d'en interdire l'accès par des règles simples de reverse-proxy, par exemple <b>/application/monitoring/</b>	Doublon par rapport à la règle E04-04
PT01-07	Les applications JAVA doivent fonctionner avec la version de JRE définie dans le CCT	Supprimé et remplacé par la règle PT01-09
AT01-13	Ces normes sur les API ont été déplacées vers le chapitre dédié aux API	Déplacées vers AT-API-01
AT01-14		Déplacées vers AT-API-02
E03-22	Script systemd	Doublon règle E03-15
AT01-11	Un document de standardisation de l'usage des services REST est en cours de rédaction à la SDSI, ce document sera fourni au prestataire en début de réalisation.	Le document fait désormais partie du CCT
AT01-09	En cas de mise en place de services REST, il est demandé de respecter le modèle de maturité de Richardson au moins jusqu'au niveau 2 inclus (utilisation de ressources, conformité des verbes et codes retour HTTP).	Doublon AT-API05