Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE
L'INTÉRIEUR

Cadre de cohérence technique
du ministère de l'intérieur

Guide d'architecture

cctmi

Table des matières

Versions du document 1.1

Introduction 1.2

Sécurité & Interopérabilité 1.3

Composants et services génériques 1.4

Réseau de transport 1.5

Méthodologie 1.6

Développement 1.7

Architecture technique 1.8

Versions du document

Version du CCT	Date de modification du document	Auteurs
3.0	Mars 2019	JC Bastoul

Guide d'architecture

Introduction

Cette version du guide d'architecture est temporaire. Elle rassemble les règles de l'ancien référentiel de règle qui relève de l'architecture et des réseaux.

Sécurité & Interopérabilité

Ref	Statut	Intitulé
1329	RG	Afin de faciliter l'interopérabilité technique entre différents composant du SI, l'utilisation de protocoles ouverts et par ordre de préférence normés ou standards et ouvert est fortement recommandée.

Composants et services génériques

Ref	Statut	Intitulé
1164	RG	Les accès externes aux applications doivent se faire impérativement via les passerelles d'accès sécurisés du ministère.
1170	RG	L'accès aux applications sensibles doit être réalisé via un proxy/reverse proxy et/ou un élément de filtrage de contenu (de type Web Application Filtering).
1182	RG	Les PBX doivent permettre de générer des tickets de taxation au fil de l'eau, ainsi que les éléments permettant de réaliser une analyse du trafic (à postériori).
1184	RG	Les locaux techniques doivent répondre aux spécifications des documents suivants : Hôtels de polices et commissariats de circonscription : - Spécifications générales d'environnement technique des hôtels de police - Locaux techniques et salles SIC (MCIC, CORCICA, CRISTAL, Vidéo), version 0.4 du 5 février 2009 - Annexe technique - Locaux techniques et salles SIC (MCIC, CORCICA, CRISTAL, Vidéo), version 8.0 du 06 février 2009 Autres sites : se référer au CSTG en vigueur
1185	RG	Dans tous les bâtiments où il existe un local technique « courant fort », celui-ci doit être distinct du répartiteur général.
1187	RG	Le détail des spécifications relatives à la téléphonie se trouve dans le document [TEL0].
1199	RG	La résolution DNS doit être utilisée systématiquement pour éviter toute adhérence avec les couches réseaux. Le recours au nommage symbolique facilite la mutualisation dans le cas des sites Web et les opérations de migration.
1200	RG	Les serveurs doivent gérer un cache pour la résolution DNS afin de ne pas surcharger inutilement les DNS.
1201	RG	Les domaines accessibles aux utilisateurs internes s'inscrivent dans les schémas de nommage DNS du ministère. L'annexe 3D8 fixe les domaines de noms sur les intranet du ministère et les règles d'administration des serveurs DNS.
1202	RG	Les pièces jointes (au format MIME conformément au RGI) sont limitée à une taille de 5 Mo après encodage.
1205	RG	La consultation des courriels doit mettre en oeuvre l'un des deux standards POP3 (RFC 1939) ou IMAP4 (RFC 3501).
1206	RG	Les connexions POP3 ou IMAP4 sécurisées doivent mettre en oeuvre TLS (anciennement SSL), il est en de même pour SMTP.
1207	RG	L'émission d'un message depuis l'extérieur ne peut avoir en adresse source une adresse de messagerie interne au ministère.
1211	RG	Le service de messagerie doit s'interfacer avec les logiciels anti-pourriel et anti-espiogiciel validés par le ministère.
1212	RG	Pour des questions de sécurité, le serveur applicatif utilisant des fonctions de messagerie ne doit pas être configuré en relais ouvert.
1328	RG	Les composants métiers référencés dans la partie PRODUITS du CCT (Partie 8, chapitre 11) doivent être utilisés en lieu et place de développements spécifiques.
1178	rc	Afin d'améliorer l'accueil téléphonique et de limiter le taux d'appels non aboutis, il est recommandé que le PBX dispose des fonctionnalités suivantes : - Messagerie vocale, - Musique d'attente, - Guide vocal. On peut y adjoindre un Serveur Vocal Interactif (SVI) dans certains cas.
1210	rc	Chaque application si nécessaire utilisera une adresse de messagerie dédiée selon un formalisme prédéfini permettant de l'identifier facilement.

Réseau de transport

Ref	Statut	Intitulé

1131	RG	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).
1132	RG	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.
1133	RG	Tout composant raccordé au réseau doit se conformer au plan d'adressage IP du ministère de l'intérieur.
1134	RG	Le NAT (translation d'adresse) est interdit sur les réseaux du ministère hors zones d'hébergement.
1135	RG	Il est obligatoire d'utiliser des ports TCP / UDP fixes.
1136	RG	Tout port non nécessaire au fonctionnement normal d'une application doit être fermé.
1137	RG	Les applications de données ne doivent pas marquer le champs DSCP. Le DSCP doit être à sa valeur par défaut : 0.
1138	RG	Le champs DSCP des applications vidéos et VOIP/TOIP doit être paramétrable.
1139	RG	Pour qu'un site soit éligible pour recevoir des flux vidéo il faut que le débit de l'interface d'accès soit supérieur ou égal à 1,2 Mbps. Pour les flux de VOIP/TOIP le débit de l'interface d'accès doit être supérieur ou égal à 1,2Mbps.
1140	RG	Le détail des spécifications relatives à la QoS se trouve dans le document [QOS].
1141	RG	Les applications doivent tenir compte du temps de latence et de la bande passante disponible et être développées en optimisant les échanges client / serveur afin d'offrir des temps de réponse répondant aux exigences de l'application. Le temps de latence moyen constaté en métropole est d'environ 20 ms (site central à site départemental), mais peut atteindre 500 ms dans les DOM/COM, voire 2000 ms en cas de congestion réseau.
1142	RG	Les applications s'appuyant sur les messageries tactiques et les réseaux TETRAPOL doivent : - prendre en compte dès la conception les caractéristiques de débit de ces réseaux (flux et taille de trame) - mettre en œuvre le protocole normalisé d'échange de données des réseaux TETRAPOL - être validées par les directions de programme des réseaux TETRAPOL - faire l'objet de tests en plate-forme
1143	RG	Le protocole réseau utilisé est TCP/IP V4.
1144	RG	Les flux applicatifs doivent s'appuyer sur des protocoles de transport standardisés : - TCP pour le mode connecté, - UDP pour l'échange de messages asynchrones.
1145	RG	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.
1146	RG	Pour la collecte de flux externes et quand IPSEC est utilisé, le tunnel sécurisé s'arrête aux concentrateurs VPN en entrée de passerelle de sécurité du ministère.
1148	RG	Lorsqu'une application utilise un composant faisant l'objet de mise à jour de sécurité de façon fréquente et automatisée, cette mise à jour doit se faire par connexion à un serveur intermédiaire installé localement sur le réseau du Ministère de l'Intérieur. La mise à jour par connexion à des serveurs sur Internet n'est pas autorisée.
1149	RG	Tout flux non explicitement autorisé est interdit.
1150	RG	Le point de terminaison TLS (anciennement SSL) côté ministère doit aboutir sur un reverse proxy.
1153	RG	Les configurations réseaux et système doivent être sauvegardées tout en gérant le versionning des modifications.
1154	RG	Les spécifications d'ingénierie relatives aux réseaux locaux sont rassemblées dans le document [LAN].
1156	RG	Pour qu'un LAN soit compatible avec la ToIP, le câblage du site doit respecter les règles minimales suivantes : - Câblage capillaire supportant au minimum le Fast Ethernet (catégorie 5E) ou catégorie supérieure normalisée (6,6A et plus) - Rocade supportant le Gigabit Ethernet, le cuivre dans une catégorie adaptée pourra être utilisé sur de courtes distances inférieures à 100 m, la fibre sera la règle.
1157	RG	Les flux multimédias ne doivent pas utiliser plus de bande passante que celle qui leur est réservée sur les réseaux WAN du ministère .
		Les équipements terminaux de vidéo dédiées (visioconférence) et de VOIP/TOIP doivent être placés dans

1158	RG	des VLANs dédiés.
1151	rc	Pour les flux de VOIP/TOIP, les flux de signalisation et de voix doivent être chiffrés en TLS (anciennement SSL)
1155	rc	Pour les sites devant accueillir la ToIP, l'installation des switchs PoE est recommandée en respectant les contraintes de l'infrastructure.
1159	rc	Dans le cadre de l'utilisation de VLAN dédiés pour les équipements terminaux de vidéo et de VOIP/TOIP, la technologie 802.1x en EAP – TLS sera privilégiée.
1355	rc	Les équipements réseaux doivent supporter et pouvoir mettre en oeuvre les deux piles Ipv4 et Ipv6.
1378	rc	Toute application accessible depuis Internet doit faire l'objet d'un audit SSI statique et dynamique avant sa mise en production.

Méthodologie

Ref	Statut	Intitulé
1331	RG	Si une application Web offre la fonctionnalité de déposer des fichiers en vue d'un stockage sur le serveur, il est impératif de respecter les points suivants: - limiter les types de fichiers à déposer et s'assurer de cette limitation en s'appuyant sur les fonctions de vérification du type mime du langage de programmation utilisé sans se limiter à la simple vérification de l'extension; - Privilégier le stokage sur un système de fichiers dans une arborescence dédiée, extérieur à celle servie par le serveur HTTP.
1346	RG	Pour la construction d'identifiants de session, il est obligatoire d'utiliser les mécanismes génériques de gestion de session proposés par les langages de développement (Java, PHP).

Développements

Ref	Statut	Intitulé
1421	RG	Il est OBLIGATOIRE d'utiliser des API et des bibliothèques pour interagir avec les autres systèmes (système de gestion de base de données, système d'exploitation, etc.).
1427	RG	Il est OBLIGATOIRE d'intercepter et de traiter de manière adéquate et au juste niveau les exceptions interrompant le fonctionnement normal de l'application. Toute exception interrompant l'exécution d'une portion de code doit être interceptée, analysée et traitée par l'application. Ainsi, il est nécessaire d'utiliser des blocs de traitement et les gestionnaires d'exception éventuellement fournis par le langage utilisé (blocs d'instructions try / catch / finally, handler-bind, try / except, etc.).
1227	RG	L'application ne doit pas modifier les classes ou les bibliothèques fournies par les logiciels du socle technique.
1252	RG	Les transactions doivent respecter les règles ACID et laisser les bases de données dans un état cohérent et disponible en cas d'anomalie.
1281	RG	L'utilisation des fonctions spécifiques des systèmes de gestion des bases de données (triggers, procédures stockées) doit être limitée et justifiée afin de limiter au strict nécessaire la dépendance des applications avec les bases de données.
1293	RG	L'application ne doit utiliser aucune technologie nécessitant une utilisation exclusive d'un serveur. Elle devra pouvoir cohabiter avec toute autre application hébergée sur les mêmes serveurs dès lors que le socle technique est identique, quel que soit l'état technique des composants utilisés.
1294	RG	L'application ne doit adhérer ni au système d'exploitation ni au matériel.
1295	RG	Si leur niveau de sensibilité le permet, tous les composants de l'application doivent pouvoir coexister sur des serveurs mutualisés sans compromettre le niveau de sécurité et d'exploitabilité des autres applications.
1307	RG	Tout traitement doit positionner un état (STATUS) de fin normale ou anormale, permettant ainsi un enchaînement automatique approprié vers les traitements suivants.
1308	RG	En cas de bases de données dupliquées, une procédure de contrôle de cohérence des données entre la base principale et la base dupliquée doit être prévue.
1309	RG	En cas de dégradation d'une base dupliquée, une procédure détaillée de remise à niveau de la base dégradée doit être livrée.
1310	RG	Dans les environnements d'exécution ne disposant pas de mécanisme automatique de gestion des ressources, l'application doit réserver au plus tard et libérer au plus tôt les ressources qu'elle s'est assignées (mémoire, fichier, verrou, session ...).
1311	RG	Les opérations lourdes d'une application (chargement de base de données, réorganisation de fichier, etc.) doivent comporter des points de reprise.
1358	RG	Tout logiciel applicatif développé au profit du ministère de l'intérieur doit fonctionner sur les deux piles Ipv4 et Ipv6.
1395	rc	Il est RECOMMANDÉ de séparer et de cloisonner physiquement les couches de présentation (interface homme-machine, etc.), application, et de traitement et d'accès aux données (bases de données, fichiers, etc.) constituant les applications.
1259	rc	L'application doit vérifier la configuration de la plate-forme de l'utilisateur (navigateur, version, gestion des cookies...) lors de sa connexion et l'informer des éventuelles mises à jour à opérer pour pouvoir utiliser toutes les fonctionnalités ou lui indiquer les fonctionnalités qui ne seront pas utilisables.
1362	rc	Il est recommandé que le référentiel permette aux applications clientes de faire des mises à jour totales ou incrémentales

Architecture technique

Ref	Statut	Intitulé	
1038	RG	L'utilisation d'un serveur de servlets et d'un développement spécifique http sur un même serveur n'est pas autorisée.	
1042	RG	La communication entre serveurs d'application utilisera les protocoles prévus par le standard JEE. Tout autre mode spécifique ou propriétaire de communication sera rejeté.	
1043	RG	Il est interdit de faire communiquer un client directement avec un serveur d'EJB sans passer par un serveur http.	
1058	RG	Toutes les couches d'une application doivent être indépendantes. Les interfaces entre les couches doivent s'appuyer sur des normes et standards.	AT
1059	RG	Une application ne doit comporter aucune adhérence vis à vis du matériel d'un constructeur particulier sur les équipements serveurs, stockage, sauvegardes et réseau.	
1061	RG	Chaque niveau 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.	
1128	RG	L'utilisation des procédures stockées n'est pas recommandée. n'est permise que dans les cas où les performances attendues ne peuvent être atteintes sans elles.	
1130	RG	Les applications doivent s'appuyer sur un serveur base de données « open source » si les contraintes du projet en terme de performance et/ou sécurité, et/ou continuité ne justifient pas l'utilisation d'un logiciel éditeur.	
1064	rc	L'utilisation des Web Services SOAP sur HTTP est à privilégier. Toute autre utilisation est soumise à l'approbation du ministère.	
1127	rc	L'utilisation des triggers dans une base de données doit être systématiquement justifiée. Toutefois, on peut les utiliser : - pour remplir les journaux applicatifs, - pour exécuter des fonctions simples, - pour réaliser des cumuls, - pour la propagation d'une modification d'une table «mère» vers les tables «filles», - pour la « dénormalisation ». On ne doit pas les utiliser dans les cas suivants : - triggers « en cascade », - triggers entre serveurs distants, - pour effectuer de la « réplication programmée » (pour effectuer de la réplication, il convient de s'appuyer sur les outils natifs ad hoc fournis en général avec la base de données).	
1356	rc	Les systèmes d'exploitation des serveurs doivent supporter et pouvoir mettre en oeuvre les deux piles Ipv4 et Ipv6.	