Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE
L'INTÉRIEUR

Cadre de cohérence technique
du ministère de l'intérieur

Guide d'intégration

cctmi

Table des matières

Versions du document

Version du CCT	Date de modification du document	Auteurs
3.0	Mars 2019	JC Bastoul
3.0.2	Juin 2019	JC Bastoul
3.0.3	Décembre 2019	JC Bastoul
3.0.3a	Décembre 2019	JC Bastoul
3.0.4	Juillet 2020	JC Bastoul
3.0.5	Octobre 2020	JC Bastoul
3.0.6	Décembre 2020	JC Bastoul

Guide d'intégration d'une application dans l'écosystème ministériel

Introduction

Une application n'est pas un objet indépendant de tout contexte. Au delà du processus métier qu'elle est appelée à outiller et pour lequel elle est conçue, elle doit s'intégrer dans un **contexte existant** : le système d'information du ministère, et celui de l'État. Plus précisément

- l'application aura tout bénéfice à utiliser des **communs**, composants et services existants qu'il convient de ne pas réécrire, avec pour ne citer que celles-ci, les fonctions d'identification et d'authentification des utilisateurs, les services de confiance (signature électronique, horodatage...), les services d'archivage ..etc.
- l'application pourra, plutôt que de les recréer, réutiliser les **données** existantes, voire des traitements de ces données ; à l'inverse, elle peut être amenée à rendre disponible les données ou traitements qu'elle va créer,
- l'application doit être sécurisée
- et bien sûr, l'application doit pouvoir être exploitée, hébergée, soutenue à moindre coût pour les professionnels qui assurent ces services

Le présent guide traite donc d'intégration. Son objet est de faciliter une intégration harmonieuse de l'application dans le système d'information du ministère et de l'Etat et de l'inscrire dans ses processus métier. Ce guide considère l'application comme une boite noire : il ne traite que des échanges de l'application avec son environnement. En d'autres termes, il ne s'occupe que de ses interfaces et n'aborde pas d'autres sujets -- importants -- comme l'architecture interne, ou les bonnes pratiques de codage.

Structure du document

Le guide liste les 6 piliers d'une intégration réussie : les utilisateurs (usagers comme agents), les données et les API, la sécurité, la fabrique de code et l'hébergement, les services transverses. Chacun de ces piliers sera décliné en domaines et chaque domaine fait l'objet d'une fiche.

Dans une phase de dégrossissage, ce tableau peut serveur de check list pour le chef de projet et lui permettre d'éviter des surprises au moment de l'intégration ou de la mise en production.

Chaque fiche, relevant d'un pilier et d'un domaine, est structurée de la façon suivante :

- le **contexte**
- les **impacts sur l'application**
- les **règles et recommandations** : nous conservons ici la même signification que dans le CCT historique (pré V3). Les règles s'imposent, les recommandations sont à comprendre comme des bonnes pratiques.
- **informations utiles** : le guide se veut avant tout une aide à l'acteur ministériel. Celui-ci trouvera dans ce pavé d'information tous les liens vers des éléments pouvant lui faciliter la tâche : contacts, offres de service, ressources utiles, zones d'échange et de collaboration ...

Les piliers de l'intégration

Le tableau qui suit liste les 5 piliers d'une intégration réussie, mentionnés plus haut, et les décline de façon plus précise en domaines à couvrir. Dans une phase de dégrossissage, ce tableau peut serveur de check list pour le chef de projet et lui permettre d'éviter des surprises au moment de l'intégration ou de la mise en production.

Piliers	Fiches de domaine	Check
1 - Utilisateur (personne physique ou morale, usager ou agent) - PU	1 - Gestion de l'identité des usagers	
	2 - Gestion de l'identité des agents	
	3 - Gestion de l'identité des personnes morales	
	4 - L'environnement de travail numérique de l'utilisateur (ETNA pour l'agent)	
	5 - Chaîne de soutien utilisateur	
	6 - Qualité du parcours utilisateur	
2 - Données & API - PD	1 - Données et services	
	2 - Gestion des échanges	
	3 - Analyser et valoriser les données	
	4 - Données personnelles	
	5 - Cycle de vie de la donnée / Archivage	
3 - Sécurité - PS	1 - La sécurité (SSI, DISSIP, PSSI...) et l'homologation	
4 - Fabrique de code - PF	1 - Forges d'intégration et de déploiement continus	
5 - Hébergement - PH	1 - Mise en place d'un hébergement	
	2 - Pilier hébergement service supervision	
6 - (Autres) Service transverse -PA	Synthèse des services transverses	

Pilier utilisateur - Introduction

L'utilisateur, qu'il soit un usager / citoyen, un agent, une entreprise ou une association (dans les deux cas une personne morale) doit être le premier souci du concepteur d'une nouvelle application.

Le service à offrir à l'utilisateur amène à se poser quelques questions fondamentales :

- **Quelle identification / authentification de l'utilisateur ?** Cette question est importante car les fonctions d'identification authentification ne doivent pas être embarquées par l'application elle-même, mais consommées comme un service extérieur.
- **Quel environnement numérique de travail (ETNA) ?**
- **Quel soutien à l'utilisateur ?**
- **Prise en compte de l'expérience utilisateur, de l'accessibilité du service**

En lien avec ces 4 questions, 6 domaines ont été définis :

1. **Identification de l'usager / citoyen**
2. **Identification de l'agent**
3. **Identification d'une personne morale (association ou entreprise)**
4. **L'environnement de travail numérique de l'agent (ETNA)**
5. **Mise en place d'une chaîne de soutien à l'utilisateur**
6. **Prise en compte de l'expérience usager, tout au long du cycle de vie du service**

Usager : gestion des identifications / authentifications

Contexte

Les applications ouvertes au public nécessitent, dans leur majorité, une **identification** de l'usager, ainsi que son **authentification**. Dans une classique approche en silo, l'application gère elle-même cette fonction d'identification et authentification, mais les usages sur Internet font appel de façon croissante à des fournisseurs d'identités mutualisés. Un nombre de plus en plus important de services acceptent des connexions utilisant une identité « GAFA » de l'usager avec un bouton Facebook, Google, LinkedIn, Twitter... Ces systèmes, tous basés sur le protocole OpenID Connect, font office de **système d'authentification unique, ou SSO (Single Sign On)**. L'usager, une fois identifié et authentifié par un fournisseur d'identité, par exemple Facebook, obtient un jeton qui va lui permettre d'accéder, avec la même identification, et de façon simplifiée à tous les services qui acceptent cette identité.

La DINSIC, en s'inspirant de cet usage répandu sur Internet, et en utilisant le protocole sous-jacent OpenID Connect a conçu un SSO nommé **FranceConnect**.

Il a été décliné en trois variantes :

- **FranceConnect particulier** (objet de la suite de la fiche)
- ProConnect (entreprise, association)
- AgentConnect, variante réservée aux agents publics.

Choix de l'identité. L'usager, sur tous les services mettant en œuvre le « bouton » FranceConnect, peut s'identifier auprès du fournisseur d'identité de son choix (FI) dans une liste de fournisseurs agrée : service des impots, Ameli, IDN de la poste, MobileConnect des opérateurs de téléphonie..
Plusieurs niveaux d'authentification sont possibles. Conformément au règlement européen eIDAS, l'usager peut choisir trois niveaux d'authentification, sous réserve que ceux-ci soient offerts par ses fournisseurs d'identité :

- niveau **faible**, suffisant pour la majorité des services, dans lequel l'authentification de l'utilisateur s'appuie sur un seul secret, généralement son mot de passe ;
- niveau **substantiel**, dans lequel l'authentification de l'usager est renforcée par un second facteur : SMS, mot de passe à usage unique (OTP One time password) ..etc ;
- niveau **élevé**, dans lequel l'authentification de l'usager est renforcée par un second facteur mettant en œuvre des moyens de sécurité forts (carte à puce, token, biométrie).

Qualité de l'identité. Quel que soit le fournisseur d'identité et le niveau d'authentification, la qualité de l'identité de l'usager est garantie grâce à son croisement avec celle présente dans le RNIPP(Répertoire National d'Identification des Personnes) tenu par l'INSEE.

Gestion de l'identité dans l'application

Avec FranceConnect, l'application reçoit l'identité pivot définie dans le RGI (nom, prénom, genre, date de naissance, lieu de naissance), accompagnés d'autres attributs selon les possibilités du fournisseur d'identité (adresse, adresse de messagerie, téléphone...), du niveau d'authentification utilisé et d'un identifiant unique et opaque de la personne propre à l'application (FranceConnect génère, pour une même personne, des identifiants applicatifs différents pour empêcher le
croisement des fichiers).

Impact pour les applications

l'identification et l'authentification des usagers ne doivent plus être prises en charge « en silo » au sein de l'application. Ces fonctions peuvent maintenant être mutualisées, à moindres frais, dans l'offre étatique FranceConnect. Le chef de projet pourra trouver des informations pratiques sur la mise en œuvre des SSO (y compris FranceConnect) dans la fiche dédiée.

Dans le cadre d'un raccordement à FranceConnect, l'application doit être capable d'assurer les fonctions suivantes

- Stockage de l'identifiant opaque FranceConnect
- Procédure de réconciliation à la première connexion, c'est à dire d'appairage de l'identité pivot de FranceConnect avec celle connue

de l'application

- Vérification du niveau d'authentification, qui doit être supérieur ou égal au niveau requis par l'application. Par exemple, une application exigeant un niveau d'authentification substantiel acceptera un usager authentifié au niveau élevé, mais refusera un usager authentifié au niveau faible.
- Secrets FranceConnect sur les serveurs (authentification mutuelle application/FranceConnect)
- Gestion des cas d'erreur (voir codes retours FranceConnect : personne décédée, homonymes)

Règles et recommandations

Ref	Statut	Intitulé
1166	RG	Les accès du grand public aux téléservices se font obligatoirement en TLS dès que des données à caractères personnelles sont échangées.
1344	RG	Pour réaliser le maintien d'une session authentifiée, seuls les mécanismes de cookie de session gérés par le langage (HTTPSession en Java par ex.) sont acceptés.
1435	rc	L'appairage de l'identité pivot de FranceConnect avec une identité connue de l'application, également appelé processus de réconciliation, peut intégrer la fourniture par l'usager d'une information complémentaire, vérifiable par l'application, et permettant de lever de potentielles ambiguïtés. Exemple : fourniture du numéro de permis dans le cadre de la démarche télépoint.

Informations utiles

Contacts utiles

- FranceConnect Particulier a été conçu et est opéré par la DINSIC. Tous les contacts utiles sont indiqués sur les pages ressources données ci-dessous.
- Contacts ministère à fournir

Offres de service

- Site dédié aux partenaires (publics ou privés), c'est à dire tout organisme désirant utiliser FranceConnect comme fournisseur de service ou de données, ou se positionner en fournisseur d'identité : https://partenaires.franceconnect.gouv.fr

Ressources

- « Comment ca marche ? » : https://franceconnect.gouv.fr

Zone d'entraide

- Forum, git, wiki, ... tous outils de collaboration susceptible de faciliter les échanges et l'entraide entre les consommateurs et avec les producteurs

Agent : gestion des identifications / authentifications / autorisations

Contexte

Les applications nécessitent généralement une quadruple fonction **d'identification**, **d'authentification, d'autorisation** et **d'habilitation** de leurs utilisateurs (on se restreint dans cette fiche au cas des utilisateurs / agents). Dans une classique approche en silo, l'application gère elle-même ces fonctions ; mais la volonté (cf règle 1114) est aujourd'hui de mutualiser ces fonctions et de les déléguer à un **système d'authentification unique, ou SSO (Single Sign On)**. L'utilisateur / agent, une fois identifié et authentifié par ce SSO, obtient un jeton qui va lui permettre d'accéder, avec les droits qui lui ont été reconnus, à toutes les applications prises en charge par ce SSO.

Remarque: la gestion des droits d'accès à l'application peut se décomposer en deux volets : la fonction d'attribution de droits (ou habilitation) et la fonction de contrôle d'accès (ou autorisation)*

Dans un monde idéal, le SSO est unique. Dans la réalité du ministère, ce n'est pas le cas. Les principaux SSO disponibles sont les suivants :

- 4 SSO web ministériels, affectés grosso modo à des populations identifiées : gendarmes, policiers, personnels de la préfecture de police, et tous les autres.
- Le projet DINUM AgentConnect, fédérateur des SSO web des agents publics, dans ses deux instances (AgentConnect internet et AgentConnect RIE).
- Toutes les applications n'étant pas de type web (c'est à dire basées sur un client léger - le navigateur), il existe également plusieurs SSO "lourd", généralement basé sur Kerberos : les AD (Active Directory) pour les parcs d'ordinateurs Windows, ainsi que l'instance de kerberos mise en oeuvre pour le parc de postes Linux de la gendarmerie.

Pour être complet, certaines applications ne peuvent s'intégrer dans un SSO. Une alternative consiste alors à les coupler à un annuaire LDAP existant (par exemple annuaire messagerie) pour que l'utilisateur puisse bénéficier au moins d'un mot de passe unique, à défaut d'un login unique.

La suite de cette fiche se focalise sur les SSO web et ne traitera plus des SSO "lourds" (pour ces derniers, quelques éléments sont disponibles dans l'annexe SSO.

Dans une vision orientée application, une application ministérielle, si elle est susceptible d'être utilisée par des agents externes au ministère, devra prendre en charge au moins deux SSO (web), voire plus :

- l'un des 4 SSO ministériels, pour les agents du ministère
- AgentConnect, pour des agents publics n'appartenant pas au ministère.
- Pour complexifier la donne, chacun de ces SSO peut offrir **plusieurs instances** distinctes, par exemple l'instance internet de AgentConnect pour les accès Internet, et l'instance RIE d'AgentConnect pour les accès en inter-ministériel (RIE peut être vu comme l'intranet interministériel)

Dans une vision orientée utilisateur, un agent du ministère est susceptible de s'authentifier auprès de deux SSO :

- « son » SSO ministériel pour les applications ministérielles
- AgentConnect s'il veut accéder à une application inter-ministérielle.

Enfin, il existe des agents qui ne disposent d'aucune solution d'identification, notamment durant la phase de déploiement de AgentConnect. On peut en effet raisonnablement penser que la diffusion de AgentConnect à l'ensemble des collectivités territoriales va prendre du temps. L'idée d'un SSO « balai » est donc en réflexion au moment où cette fiche est écrite.

Le tableau suivant fait une synthèse des SSO à prendre en compte par les applications du ministère selon deux critères :le type de population, et réseau d'accès.

Accès	Agents MI (4 catégories)	Agents État non MI	Agents autres fonctions publiques	Agents non identifiés par leur organisme de rattachement
Accès intranet	L'un des 4 SSO du ministère sur un critère population : - PROXIMA pour les gendarmes - CHEOPS NG pour les policiers - [PASSAGE PP pour certains agents PP] - PASSAGE2 pour tous les agents restants	Pas de cas d'usage identifié -En cible AgentConnect-RIE	Pas de cas d'usage identifié -En cible AgentConnect-RIE	Réflexion en cours
Accès RIE (inter-ministériel)	En cible AgentConnect-RIE A négocier avec MoE	En cible AgentConnect-RIE	Sauf exception, ces agents arrivent par Internet. Exception connue : les agents des SDIS pour NexSIS En cible AgentConnect-RIE	Réflexion en cours
Accès Internet	Privilégier les accès extranet (Hesperis, Neo, Span, Nomade) - Accès à une application métier : AgentConnect-Internet - Accès à un service RH : FranceConnect - Cf section dédiée dans la présente fiche	En cible AgentConnect-Internet	En cible AgentConnect-Internet	Réflexion en cours

Remarques : les cas d'usages répertoriés dans le tableau ne sont pas tous stabilisés. Quand une solution cible est indiquée, cela signifie qu'une solution d'attente doit être négociée avec la MoE.[2]

Les SSO du ministère -- Cas simple des applications et des agents du MI

L'approche de développement traditionnelle en silo consiste à établir une base des utilisateurs au sein de l'application et de gérer localement les authentifications et les autorisations, voire les habilitations. **Cette approche doit être proscrite** pour de multiples raisons :

En matière d'**identité**,

- pour les agents, le ministère s'est doté d'un "Référentiel des Identités et des Organisations" (RIO) qui est le référentiel à privilégier ;
- dans ses travaux sur l'état plate-forme, FranceConnect et le RGI, l'état (la DINSIC) a défini des identités pivot, pour l'usager, pour l'agent et pour l'entreprise ou l'association.

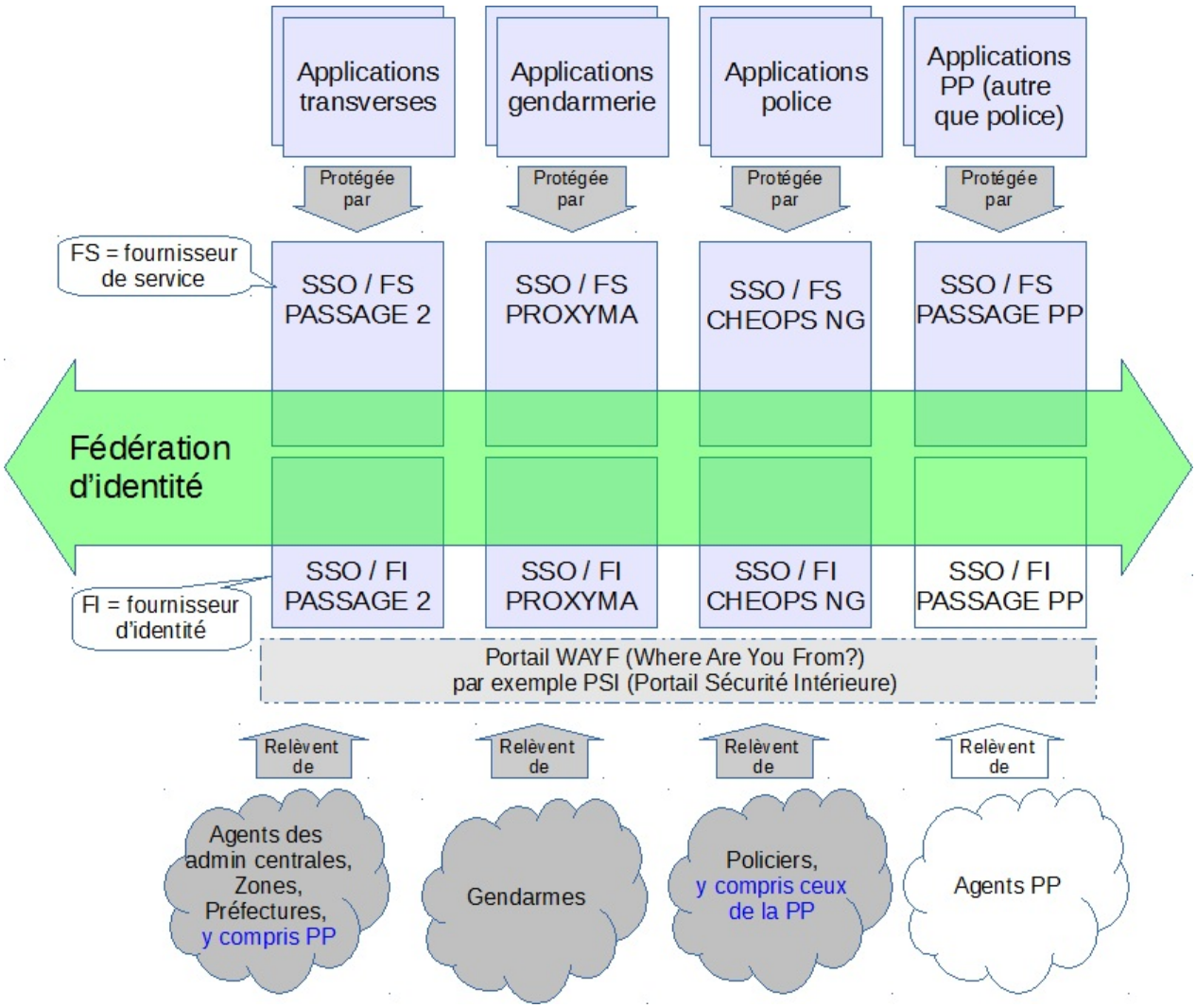
En matière d'**authentification**, le ministère a mis en place 4 SSO web qui couvrent l'ensemble de la population du ministère : CHEOPS-NG pour les policiers, WEBSSO PROXYMA pour les gendarmes, PASSAGE-PP pour la PP, PASSAGE2 pour les autres. Ces SSO sont reliés entre eux dans une fédération d'identité, ce qui permet par exemple à un agent authentifié par CHEOPS-NG d'accéder à une application protégée par PASSAGE2.

En matière d'**autorisation**, les Web SSO du ministère s'appuient tous sur un annuaire qui leur est accolé, et qui est alimenté par un **outil d'habilitation** qui prend en compte les attributs de l'agent. Cette habilitation reste à grosse maille (des profils), l'application garde en général la main sur les droits fins qui restent très spécifiques à chaque application.

Très schématiquement, un SSO peut se décomposer en deux parties :

- le « Fournisseur de service » (FS) qui protège les applications.
- l' « Fournisseur d'identité » (FI) qui identifie, authentifie et contrôle les droits aux usagers pour l'accès à ces applications protégées.

Ce découpage du SSO en FS / FI apparaît sur le schéma qui suit.



Le schéma ci-dessus fait apparaître les 4 SSO internes du ministère dont il a déjà été fait mention. :

- le SSO de la gendarmerie PROXYMA
  qui protège les applications de la gendarmerie (fonction FS)
  et prend en charge la population des gendarmes (fonction FI)
- le SSO de la police CHEOPS NG
  qui protège les applications de la police et prend en charge la population des policiers
- le SSO de la préfecture de police PASSAGE PP
  qui protège les applications de la PP et prend en charge les agents de la PP. Il est à noter que dans la cible stratégique validée en COREP de juillet 2016, PASSAGE PP **garderait sa fonction de fournisseur de service mais perdrait sa fonction de fournisseur d'identité :** en effet, pour que chaque population ne dépende que d'un unique SSO interne, les policiers de la PP relèveraient plutôt du SSO de la police CHEOPS NG, et les autres agents de la PP, par exemple des agents de la mairie de Paris, seraient appelés à être pris en charge par PASSAGE 2.
- et le SSO des services transversaux PASSAGE 2 qui protège les applications transverses pour le compte des agents « administratifs » des services centraux, des zones de défense, des préfectures.

Ces 4 principaux SSO sont en « **fédération d'identité** ». Concrètement, cela signifie qu'un usager identifié et authentifié par son SSO de rattachement (normalement unique) peut accéder à une application contrôlée par un autre SSO du ministère pourvu qu'il en ait les droits[1]. Par exemple un policier peut accéder à une application transverse relevant du SSO PASSAGE2, en se faisant authentifier par le SSO dont il relève, en l'occurrence, CHEOPS NG.

Le schéma fait également apparaître une fonction dite WAYF (Where Are You From?). Cette fonction est rendue nécessaire par la multiplicité des SSO, et permet, dans certains cas marginaux de donner le choix du SSO à l'utilisateur.

La copie d'écran qui suit montre la page d'accueil de l'un de ces portails, avec les boutons des 4 SSO du ministère.

AgentConnect

La section qui précède a documenté le cas d'usage le plus simple : un agent du MI accédant à une application du MI sur son Intranet. Le tableau des cas d'usage de l'introduction liste plusieurs autres cas. Le SSO qui y apparaît, en cible est le plus souvent FranceConnect Agent dans ses deux instances, FranceConnect Agent internet et FranceConnect Agent RIE.

Le SSO FranceConnect, conçu par la DINSIC, s'appuie sur le protocole standard **OpenID Connect**. Ce protocole est aussi celui utilisé par un grand nombre de sociétés de l'Internet, Facebook, Google, LinkedIn ...etc.

Il a été décliné en trois variantes :

- FranceConnect
- ProConnect (pour les personnes morales : entreprise, association)
- **AgentConnect** et ses deux instances, RIE et Internet, qui nous occupe ici.

Remarque importante : la mise en œuvre de AgentConnect s'appuie sur des composants existants et maitrisés au sein du ministère :

- AgentConnect s'appuie sur les FI (Fournisseurs d'Identité) existants dans les SSO ministériels
- Le protocole standard d'AgentConnect, OpenID Connect, est déjà supporté par les fournisseurs de services de nos SSO ministériels, tous basés sur la même brique opensource LemonLDAP::NG

Cas des connexions des agents via internet

Les agents peuvent être autorisés à se connecter à une application du MI via Internet. Le risque de ce type de connexion est l'exposition d'une donnée très sensible : la liste des agents du ministère. Deux cas de figure existent selon que l'on accède à une application métier ou à un service à l'agent.

Connexion à une application métier

Ce cas devrait être peu usité car les applications métier sont généralement confinées à l'intranet ou au RIE. Néanmoins la solution cible est l'utilisation de **FranceConnect Agent**.

Connexion à une application offrant un service à l'agent (RH, formation, ...)

Dans ce cas d'usage, l'agent accède à un service qui relève plus des ressources humaine que du métier. L'authentification de l'agent, considéré comme un citoyen, peut alors être déléguée à **FranceConnect**. FranceConnect fournit (entre autres) l'adresse mail personnelle de l'agent, et c'est celle-ci qui sera utilisée pour vérifier la qualité d'agent du ministère et la fourniture du n° RIO utilisé pour la connexion. Cette solution nécessite que l'adresse mail personnelle de l'agent, identique à celle du fournisseur d'indentité FranceConnect que celui-ci va choisir, soit enregistrée dans le SI RH du ministère.

Impacts sur les applications

Selon le périmètre d'usage de l'application, les actions suivantes sont requises :

1. inscrire l'application dans le SSO ministériel dont elle relève (PROXIMA, CHEOPS NG, PASSAGE PP ou PASSAGE 2)
2. S'assurer de la fédération des identités pour que l'application ne soit pas restreinte à la population « naturelle » du SSO dans lequel elle est inscrite. Exemple : on peut souhaiter qu'une application inscrite dans PASSAGE 2 puisse être accessible par des gendarmes et des policiers, ce qui nécessite une action de fédération inter-SSO
3. Inscrire l'application dans AgentConnect si elle doit être utilisée par des agents externes au ministère de l'intérieur.

Règles et recommandations

Ref	Statut	Intitulé
1436	RG	L'identification de l'agent doit être conforme aux identités pivot telles qu'elles sont décrites dans les documentations en ligne d'AgentConnect. Cette conformité sémantique est très importante pour faciliter l'insertion de l'application dans l'approche état plateforme : c'est-à-dire lui permettre de s'intégrer à AgentConnect et d'exposer si besoin des API de données.
1071	RG	Pour les cartes à puce à usage interne, il est obligatoire de s'appuyer sur le standard IAS-ECC, format retenu dans le cadre de l'IGC ministérielle.
1169	RG	Si une application du ministère est accessible à des utilisateurs d'une autre administration à partir de leur infrastructure (via RIE par exemple), l'authentification et la gestion des droits de ces utilisateurs ne peuvent être déléguées qu'à condition d'apporter des garanties de sécurité. Cette disposition est garantie intrinsèquement par AgentConnect
1167	RG	Les habilitations (par exemple les droits fins d'une application) associées aux utilisateurs doivent être contenues dans une base protégée.
1382	RG	Le RIO (Référentiel d'Identité et d'Organisation) est le référentiel socle des identités pour l'ensemble du ministère. Tout annuaire ou application utilisant l'identité d'un agent du ministère doit s'appuyer sur le RIO et au minimum intégrer le champ identifiant RIO.
1114	RG	Une application ne doit plus prendre en charge la fonction d'authentification de ses utilisateurs : elle doit déléguer cette fonction au SSO du ministère dont elle relève, ou à AgentConnect quand le périmètre d'usage dépasse celui des agents du ministère.

Informations utiles

Informations utiles pour les SSO ministériels :

Contacts utiles

Les contacts sont renseignés dans les offres de service.

Pour mettre en place une fédération : personnes à contacter

Offres de service

- Offre de service pour les SSO de la sécurité intérieure (ST(SI)² / PROXIMA, CHEOPS NG et PSI) : offre ST(SI)².
- Le ST(SI)² donne également la possibilité de mettre en place un portail d'authentification pour les applications locales :http://auth.local.gendarmerie.fr/info.html.
- Offre de service pour le SSO de la PP (PASSAGE PP) : http://wiki.sdsic.ppol.mi/lib/exe/fetch.php?media=referentiel:offre_de_service_passage_pp.pdf
- Offre de service pour le SSO transversal (DSIC / PASSAGE 2) : à fournir

Ressources

- Portail Sécurité Intérieure :https://auth.sso.psi.minint.fr/.
- SSO PROXIMA : https://auth.sso.gendarmerie.fr/saml/singleSignOn
- Guide de raccordement des applications derrière les SSO du ST(SI)²
- SSO CHEOPS NG: https://auth.sso.police.fr/
- SSO PASSAGE PP: https://auth.sso.ppol.minint.fr/
- SSO PASSAGE2: https://auth.sso.minint.fr/

Zone d'entraide

- *Forum, git, wiki,... tous outils de collaboration susceptible de faciliter les échanges et l'entraide entre les consommateurs et avec les producteurs*. Le ST(SI)² fournit pour le portail d'authentification pour les applications locales un forum ouvert aux gendarmes : forum dédié |

Informations utiles pour AgentConnect :

Contacts utiles

- AgentConnect est conçu et opéré par la DINUM.

Offres de service

Ressources

- http://etatplateforme.modernisation.gouv.fr/actualite/franceconnect-se-decline-egalement-pour-les-agents-de-la-fonction-publique

Personne morale : gestion des identifications / authentifications / autorisations

Contexte

Certaines applications ou traitement de données ne s'adressent pas à une personne physique, citoyen ou agent, mais à une **personne morale : une entreprise ou une association**. Dans ce cas de figure deux questions se posent immédiatement

- comment identifier de façon unique la personne morale
- quelle lien établit-on avec la personne physique mandatée pour réaliser l'opération au nom de la personne morale

Identité d'une entreprise

La base Sirene, opérée par l'Insee, est le fournisseur des données d'identité des entreprises et de leurs établissements. Celle-ci fait partie des données de référence du Service public de la donnée mis en place par la loi pour une République numérique. Cette identité a deux composantes :

- le SIREN : identifiant unique de l'unité légale (entreprise)
- le SIRET : identifiant unique d'un établissement - le SIRET est constitué du SIREN auquel on ajoute l'identifiant de l'établissement

Les entreprises peuvent être également référencées ou immatriculées dans d'autres registres :

- RCS (Registre du commerce et des sociétés), qui concerne les sociétés commerciales, opéré par Infogreffe pour le compte de l'ensemble des greffes des Tribunaux de commerce français.
- RM (Répertoire des métiers), qui concerne les entreprises artisanales, opérés par les chambres de métiers et de l'artisanat

Il faut noter que ces immmatriculations contiennent toutes le n° SIREN de l'entreprise qui reste donc l'identifiant principal. Synthèse utile sur Service-public.fr

Remarque : l'identité dont il a été question jusqu'ici est exclusivement française. Une entreprise étrangère, ou travaillant à l'international doit être identifiée à un niveau plus global (européen, international). Il existe un European Unique identifier (EUID) au niveau de la communauté européenne, ainsi que de multiples "Unique business identifier" à un niveau plus global. Ces identités ne sont pas dans le périmètre de la présente fiche.

Identité d'une association

Lors de sa déclaration en préfecture, l'association reçoit automatiquement un numéro d'inscription au répertoire national des associations (RNA). Elle doit en outre demander son immatriculation au répertoire Sirene lorsqu'elle souhaite demander des subventions auprès de l'État ou des collectivités territoriales, lorsqu'elle emploie des salariés ou lorsqu'elle exerce des activités qui conduisent au paiement de la TVA ou de l'impôt sur les sociétés. Extrait service-public.fr

Fonctions d'identification, d'authentification et d'autorisation

Comme dans le cas de l'identification / authentification d'une personne physique, ces fonctions d'identification et d'authorisation sont appelées à être prises en charge par une instance du fédérateur d'identité FranceConnect, ici dans sa déclinaison personne morale (ProConnect). Il ne s'agit pour le moment que d'une cible : ProConnect est encore en phase de développement. Dans l'attente de la disponibilité de ce service, et afin de faciliter une convergence future, il convient de respecter quelques bonnes pratiques qui sont listées dans la section "Impacts".

S'adresser à une personne morale implique aussi de se poser la question du mandat : c'est bien une personne physique qui est mandatée pour réaliser l'opération au nom de la personne morale. Le mandataire doit être identifié et authentifié en temps que personne physique.

Au delà se pose la question de la réalité du mandat. A qui incombe cette vérification, à la personne publique qui met en oeuvre un service ou à l'entreprise qui le consomme ? Cette question n'est pas tranchée et sera résolue avec ProConnect.

"Dites le nous une fois!" (Programme DLNUF)

Le programme de simplification "Dites le nous une fois" (DLNUF), consiste à éviter de réclamer à une personne physique ou morale des informations ou des justificatifs qu'elle a déjà fournis. Il est fondé notamment par la loi pour un Etat au service d'une société de confiance (dite loi ESSOC). Dans le cas de l'entreprise, l'API entreprise est un levier pertinent permettant d'appliquer ce programme et donc de simplifier les démarches et d'en améliorer la qualité. L'API entreprise permet de récupérer tout un ensemble d'informations sur l'entreprise - sous réserve de son assentiment - en interrogeant plusieurs fournisseurs de données tels qu'Infogreffe (Registre du Commerce et des Sociétés), le RNA, l'Insee, les finances publiques, et plusieurs autres. cf site API Entreprise.

Impacts sur les applications

En l'absence du fédérateur ProConnect, et afin de s'y préparer, il convient de mettre en oeuvre quelques bonnes pratiques :

- identifier l'entreprise par son SIREN (ou SIRET s'il s'agit des établissements)
- identifier l'association par son SIREN / SIRET si elle en possède un, sur son numéro RNA sinon.
- planifier la mise en oeuvre de OpenID connect, protocole d'identification / authentification mis en oeuvre par les trois déclinaisons de FranceConnect

Règles et recommandations

Ref	Statut	Intitulé
1437	REG	L'identification d'une entreprise doit s'appuyer sur son SIREN (ou SIRET s'il s'agit des établissements). L'identification d'une association doit s'appuyer sur son SIREN (ou SIRET s'il s'agit des établissements) si elle un possède un. Elle s'appuiera sur son numéro RNA dans le cas contraire.
1438	rc	Dans le but de faciliter le raccordement futur d'un service en ligne au fédérateur d'identité ProConnect, il est fortement conseillé de mettre en oeuvre le protocole d'identification / authentification OpenID Connect ou de prévoir sa mise en oeuvre future dans l'architecture de l'application.

Informations utiles :

Contacts utiles

Offres de service

Site API Entreprise

Ressources

Définition du SIREN : Définition INSEE

Définition du SIRET : Définition INSEE

Zone d'entraide

Agent : l'environnement numérique de travail (ENT)

Contexte

L'utilisateur, qu'il soit un agent, un citoyen, un partenaire, utilise de façon croissante plusieurs terminaux. Ce qu'on appelle traditionnellement le poste de travail devient multiple et ne se réduit plus au seul ordinateur de bureau. Pour ne prendre que le cas de l'agent du ministère de l'intérieur :

- l'ordinateur, fixe ou portable, avec de nombreuses variantes
  - des OS différents. Au ministère ils se limitent à Windows 7 ou 10 et Linux, plus marginalement CLIP OS (un OS multiniveau sécurisé, basé sur un noyau Linux et maintenu par l'ANSSI)
  - les terminaux légers et les terminaux "SPAN" qui s'appuient sur une fonction de déport d'écran
  - le nouveau poste nomade NOEMI
  - les terminaux virtuels, envisagés mais encore à l'état de prototype, mais le VDI devient envisageable avec les infrastructure de cloud qui sont en cours de déploiement
- les terminaux mobiles, smartphone ou tablettes, avec plusieurs offres adressant pour le moment des publics différents
  - Offre Néo pour les agents de la sécurité intérieure, qui s'appuie sur une déclinaison durcie d'Android (SECdroid)
  - Offre Hesperis pour les autorités, qui s'appuie sur l'OS Android
  - Offre sécurisée CALL MI (basée sur ERCOM)
  - Offre FileMI qui permet d'accéder à un stockage partagé (NextCloud) et ses services associés
  - il faut ajouter un contexte à venir, avec le réseau radio du futur, qui utilisera lui aussi des terminaux dans un contexte encore à définir

La diversité des terminaux est déjà grande avec les agents, il est clair qu'elle l'est encore plus dès qu'on adresse l'usager, qui n'est pas soumis au cadrage d'un contexte professionnel.

La terminologie de "poste de travail" est à entendre ici en prenant encompte à la fois la mobilité et la diversité des terminaux.

Principe cible : l'utilisateur doit pouvoir accéder aux services applicatifs pour lesquels il est habilité, en toute sécurité, à tout moment, quel que soit le type de terminal, en tous lieux. Cf ATAWAD (Any Time, AnyWhere, Any Device).

Ce principe cible devra être nécessairement contextualisé : par exemple, dans le cas des agents du ministère, le principe du "Any Device" se limite aux terminaux fournis par le ministère et il faut rappeler que celui-ci ne reconnait pas aujourd'hui les terminaux personnels (dits BYOD). Néanmoins nous pouvons décliner quelques règles et recommandations très structurantes pour nos applications.

De la diversité croissante et difficile à endiguer des terminaux découle une première règle, essentielle, celle de l'adhérence minimale de l'application au poste de travail.
Une application doit être accessible indifféremment sur un terminal Windows, Linux, Android, IOS, sur le grand écran d'un poste de bureau comme sur celui d'un smartphone.

Impacts pour l'application

Règles et recommandations

Recommandation (proposition)

Ref	Statut	Intitulé
1439	RG	Toute application doit viser le minimum d'adhérence au poste de travail. Elle doit être indépendante du système d'exploitation (OS) de ce poste de travail. En conséquence : il s'agit d'une application WEB - c'est à dire une application qui s'appuie sur les protocoles et langages du web notamment HTTP, html / css / javascript et qui est compatible avec l'un des navigateurs préconisé par le cadre de cohérence technique

1440	rc	Dans le cas des terminaux mobile (Android, SECdroid, IOS..) la règle 1439 d'adhérence minimale de l'application au terminal s'applique toujours. Néanmoins, les terminaux mobiles ont de fortes spécificités : d'une part une grande richesse de fonctionnalités dont l'application peut avoir besoin (captation d'image, de mouvement, de position...) et d'autre part la perte possible du réseau nécessitant un mode déconnecté. Le développement de clients applicatifs (ou application mobile, ou web app, ou appliquettes), mis à disposition dans les magasins Android, apple, ou dans nos magasins privés, outre une meilleure ergonomie, permet d'exploiter pleinement les fonctions spécifiques du terminal mobile. Mais le développement, la sécurisation et le maintien de ces applications mobiles sont coûteux. La technologie récente des **Progressive Web Applications (PWA)** qui exploite les fonctions et les API du navigateur peut permettre de faire l'économie d'une application mobile. Elle permet d'installer et utiliser l'application web comme une application native capable de gérer le mode hors ligne et d'avoir accès aux fonctions du terminal mobile. Il n'y a donc qu'une application à maintenir, sa mise à jour est automatique et elle fonctionne sur toutes les plateformes. Dans ce contexte, les solutions préconisées sont par ordre de priorité : 1- **de préférence** une application web (html 5/ css 3/ javascript) sans application mobile. Si nécessaire, la version 5 de HTML permet d'offrir un mode sans connexion et la solution PWA permet d'améliorer l'ergonomie de l'application avec une expérience usager similaire à celle d'une application mobile. 2- **en dernier ressort** et si la solution PWA n'apporte pas les fonctionnalités attendues, une application développée nativement pour l'OS considéré (android).
1441	rc	Toute application devrait pouvoir s'adapter à tous les terminaux validés au sein du ministère, ordinateurs, tablettes et smartphone. Trois approches sont possibles par ordre de préférence : 1. **De préférence** le « Responsive web design » qui produit, sur une seule URL, un code html unique, auto-adaptatif, qui s'adapte aux caractéristiques du terminal. 2. **à défaut**, la diffusion dynamique (« Dynamic serving » qui produit, sur une seule URL, un code html spécifique à chaque type de terminal. 3.**à proscrire**, des URLs et du code spécifiques à chaque type de terminal.
1442	rc	Une application mobile (quand une application web ne peut faire l'affaire - cf règle 1440) devrait être configurable de telle sorte qu'elle soit hébergeable indifféremment dans un magasin Hesperis, CALL MI ou Neo. En effet chacun de ces environnements impose ses propres contraintes.
1228	RG	Les applications et les sites de communication web doivent respecter les standards proposés par les organismes reconnus tels que le W3C, l'ECMA ou l'IETF et être validés avec l'ensemble des navigateurs mentionnés dans le référentiel technique des produits.
1086	rc	Il est recommandé de ne pas utiliser les macros des suites bureautiques.
1096	RG	Tout logiciel ou nouvelle version de logiciel devant être installé sur les terminaux de communication RUBIS (TIE et TDG fixe) doit au préalable être validé par le ministère. Toute demande d'ajout de logiciel doit être faite au ministère ou à la SDRTA pour le ST(SI)². Aucun autre logiciel que ceux autorisés dans le CCT ne peut être installé sur un TDG fixe.
1097	RG	Les versions des logiciels mentionnés dans le référentiel technique des produits (Terminal de communication RUBIS) sont les versions strictement imposées. Le déploiement toute nouvelle version d'un logiciel sur les terminaux de communication RUBIS (TIE et TDG fixe) est effectué conformément aux directives émises par le ministère ou le ST(SI)².
1160	RG	Tout poste de travail ou serveur (Windows ou Linux) doit être équipé des antivirus qualifiés par le ministère à jour de sa base antivirale.
1162	RG	Ni l'utilisation d'une application ni son installation ne doit nécessiter la désactivation ou gêner la mise à jour de l'anti-virus et/ou de l'anti-espiogiciels et/ou du pare-feu.
1176	RG	Les offres de téléphonie au travers de liens ADSL mono poste, prévus pour le grand public, sont interdites pour le ministère.
1260	rc	Les applications internes doivent être testées dans tous les environnements compatibles avec la cible de déploiement.
1316	rc	Le client lourd installé sur le poste client doit pouvoir être installé par une procédure automatique en mode silencieux et manuel.
1318	RG	Les applications doivent disposer d'une fonction de désinstallation qui effectue un retour arrière sur toute modification effectuée par l'application sur le poste de travail. La fonction de désinstallation doit supprimer du poste de travail tout composant logiciel spécifique à l'application.
1354	RG	Pour les produits libres destinés à la bureautique, ce sont exclusivement les versions disponibles sur le site intranet officiel du ministère qui doivent être téléchargées par les administrateurs des parcs informatiques et utilisées.
1380	RG	Toute application devant être déployée sur un poste de travail Windows doit s'enregistrer dans la base de registre.

1093	RG	Les données applicatives doivent être stockées dans des ressources réseau partagées, sauvegardées et sécurisées en terme d'accès.
1147	RG	L'accès au système d'information du ministère par des technologies sans-fil est interdit en dehors des offres de services de nomadisme ministérielles approuvées par le ministère.

Informations utiles

Contacts utiles

- Contact gendarmerie : sdac.stsisi@gendarmerie.interieur.gouv.fr
- Contact DSIC : à fournir

Offres de service

Offres dans le domaine de la mobilité

- Offre Hesperis
- Offre Call MI
- Offre SPAN
- Offre NOEMI - Nouveau poste nomade - En cours de construction
- Offre File MI - Offre basée sur NextCloud permettant des partages de fichiers entre équipements nomade et poste de travail - En cours de construction.
- Offre Neo - Offre de service mobilité du ST(SI)²
- Offre de sécurisation des web apps par le Centre de Cyberdefense du Ministère de l'Intérieur (CNGESSI): lien à fournir

Poste fixe

- Offre poste de travail DSIC – lien à fournir
- Gendarmerie : offre « Poste de travail » destinée aux chefs de projets, prestataires informatiques ou développeurs locaux qui mettent en œuvre des applications destinées à être utilisées sur les postes de travail banalisés des agents de la Gendarmerie Nationale.
- **PIST (plate-forme d'intégration des stations de travail)** : plateforme de poste de travail virtualisée, mise à disposition des chefs de projet pour tester le bon fonctionnement de leur application dans le cadre des procédures de montées de version logicielle. cf NE 30319 /GEND/ST(SI)²/SDAC/BCCP du 15/04/2013.

Ressources

- ADSL (Application de Demande et de Suivi Logiciel) gendarmerie
- Zone de téléchargement de la DSIC
- CLIP OS est un système d'exploitation multiniveau sécurisé, basé sur un noyau Linux. Capable de gérer des informations de plusieurs niveaux de sensibilité, il a été élaboré par L'ANSSI pour répondre aux besoins de l'administration. Page ANSSI sur CLIP OS

Zone d'entraide

- Wiki SIC gendarmerie
- Forum SIC gendarmerie
- Forum, git, wiki, ... tous outils de collaboration susceptible de faciliter les échanges et l'entraide entre les consommateurs et avec les producteurs

Agent : mise en place d'une chaîne de soutien utilisateur

Contexte

Fiche en cours d'écriture.

Règles et recommandations

Règle

Ref	Statut	Intitulé
1306	RG	L'application doit contenir une fonction permettant l'affichage d'une page d'information avec texte paramétrable à destination des utilisateurs.

Informations utiles

Contacts utiles

Offres de service

Zone d'entraide

- *Forum, git, wiki, ... tous outils de collaboration susceptible de faciliter les échanges et l'entraide entre les consommateurs et avec les producteurs*

Utilisateur : qualité du parcours utilisateur

Contexte

Un sujet essentiel

La qualité du parcours usager d'une application, d'un service, d'une démarche en ligne, est un sujet essentiel, souvent sous évalué dans la conduite du projet, souvent traité en mode réactif après la mise en production. Or il s'agit sujet essentiel car il touche à la finalité même du service: le service sera-t-il facile à trouver, suffisamment simple à comprendre et à utiliser pour toucher le public visé, en y incluant notamment les personnes en situation de handicap (accessibilité numérique). Les risques d'une non qualité d'un parcours usager sont nombreux :

- coût financier des correctifs après coup – toujours significativement plus important que le coût d'une prise en compte en amont
- risque de non adoption ou de rejet de la démarche en ligne
- risque d'exclusion des publics fragiles
- risque de dégradation d'image (campagne de presse, réseaux sociaux)
- risque de recours (par exemple des associations de personnes handicapées)

Cette qualité est aujourd'hui mesurée, par l'État lui-même (cf section suivante) comme par la société civile (par exemple les associations de défense des personnes en situation de handicap, des étrangers ...etc).

Prise en compte précoce

La qualité du parcours usager est un sujet qui doit être pris en compte en amont du projet, dès la phase de conception et tout au long de son cycle de vie. Cette prise en compte possède ses méthodes souvent associées à la méthode agile. On parle généralement d'ergonomie (ancien monde), ou plus souvent aujourd'hui d'expérience utilisateur (User Experience, ou UX).

Vérifier et mesurer

La qualité du parcours usager doit être ensuite vérifiée et mesurée dans une démarche d'amélioration continue. Cette mesure passe par différents outils de suivi d'audience, des enquêtes de satisfaction.

Au delà des dispostifs de mesure conçus avec la démarche et au sein du ministère, La satisfaction de l'usager est également mesurée sous l'impulsion des services du premier ministre, DINUM et DITP. Deux dispositifs sont mis en place :

- Mesure à chaud : le bouton "Mon Avis" qui **doit obligatoirement** être intégré à la fin de chaque démarche en ligne. Les résultats statistique de cette mesure sont publiés dans l'observatoire de la qualité des démarches en ligne (cf section suivante)
- Mesure à froid avec le dispositif VoxUsagers : site de VoxUsagers

L'observatoire de la qualité des démarches en ligne

La DINUM a mis en place un observatoire de la qualité des démarches en ligne. Cet observatoire est public. Il évalue finement, chaque trimestre, les 250 démarches en ligne les plus utilisées. Les critères d'évaluation de chaque démarche intègrent

- la satisfaction des usagers, collectée à chaud grâce au bouton "Mon Avis" obligatoirement intégré sur chaque démarche.
- l'accessibilité numérique (RGAA),
- la prise en compte du handicap,
- le critère "dites le nous une fois" (DLNUF)
- compatibilité avec les équipements mobiles
- disponibilité et rapidité
- l'intégration à FranceConnect
- ..etc.

Ces critères d'évaluation sont détaillés sur le site de l'observatoire : critères d'évaluation,

Accessibilité numérique

L'accessibilité numérique (RGAA) est une composante importante (et légalement obligatoire) de la qualité d'une démarche en ligne. L'accessibilité est évaluée par l'observatoire public cité supra.

Un grand nombre de ressources sont disponible pour réaliser des démarches conformes au RGAA. Pour en citer quelques unes :

- la DAE (Direction des Achats de l'État) a mis en place un ensemble complet de prestations d'accompagnement, d'audit et formation
- la DILA fournit des ressources aux développeurs sur son site PIDILA
- ressources financières avec le fond pour l'insertion des personnes handicapées dans la fonction publique (FIPHFP)

Pour plus d'information, voir la section ressources en fin de fiche.

Règles et recommandations

Ref	Statut	Intitulé
1219	rc	La charte graphique de la DICOM s'applique aux applications WEB accessibles au public.
1230	RG	Conformément à l'arrêté du 21 octobre 2009 relatif au référentiel général d'accessibilité pour les administrations, les applications du ministère concernées par le décret n° 2009-546 du 14 mai 2009 doivent respecter le Référentiel Général d'Accessibilité pour les Administrations (RGAA) disponible sur le site : https://www.numerique.gouv.fr/publications/rgaa-accessibilite/
1443	RG	L'accessibilité numérique (conformité au RGAA – Référentiel Général d'Accessibilité pour les Administrations) est une obligation légale. Elle doit être pris en compte dès la conception de l'application afin d'en minimiser le coût.

Informations utiles

- Observatoire de la qualité des démarches en ligne
- Sondage usager à froid - "Partagez votre expérience pour aider le service public à s'améliorer"
- Les 10 principes d'une démarche en ligne exemplaire

Contacts utiles

Offres de service

- Offres de service pour réaliser une enquête de satisfaction. A fournir.
- Offre de service Matomo de la DICOM. Informations à fournir. Contact DICOM, dépôt forge DNUM.
- Suivi statistique des sites internet, sur le site de la DICOM : DICOM - Suivi statistique des sites internet

Ressources

- Accessibilité numérique (RGAA)
  - RGAA version 4
  - Site accessibilité numérique de la DINUM. Ce site concentre l'essentiel des ressources mises en ligne par la DINUM au sujet de l'accessibilité numérique.
  - DINUM : panorama des solutions
  - Site accessibilité DILA.
  - DAE - Accord-cadre à bons de commande " Prestations d'accompagnement, d'audit et formation en matière RGAA et accessibilité numérique". Noter que ce document liste des contacts pour chaque ministère, dont le ministère de l'intérieur (DEPAFI).
    - Offres des attributaires
  - DAE - Page descriptive de la DINUM
  - Possibilités de financement : le Fonds pour l'insertion des personnes handicapées dans la fonction publique FIHFP.

L'activation de ce fond passe par la DRH / SDASAP.

Zone d’entraide

- Il existe une **communauté Accessibilité numérique**, interministérielle et animée par la DINSIC. Informations sur le wiki DINUM (Ce wiki nécessite la création d'un compte personnel)

Pilier données et API - Introduction

Toute application offre des services et manipule des données, des concepts métier, qui jouent souvent un rôle plus large et plus durable que l'application elle-même. Il est important de se poser, au sujet de ces données, un certain nombre de question :

1. **Concevoir une application orientée service et données** - Cette question en recouvre plusieurs :
2. **Réutilisation** Les données que doit manipuler mon application existent elles déjà ailleurs et ai je envisagé une réutilisation ?
3. **Exposition des données** - L'application est elle pensée pour faciliter la réutilisation des données qu'elle crée ou transforme ?
4. **Exposition des traitements** - Au delà d'une exposition brute de données, mes traitements sur les données eux mêmes peuvent être exposés. Sont ils exposés en vue d'une réutilisation possible ?
5. **Gestion des échanges** - Les échanges, internes comme externes, sont pris en charge par des dispositifs ministériels ou interministériels dédiés. Ont ils été pris en compte ?
6. **Analyser et valoriser les données** - Les données sont un patrimoine indépendamment des traitements qui leur sont appliqués. Elle doivent pouvoir être croisées, analysées, anonymisées, parfois recyclées en données ouvertes ...etc. Toutes les mesures ont elle été prises pour faciliter cette valorisation ultérieure?
7. **Données personnelles** - Les données à caractère personnel sont soumises à de fortes obligations réglementaires : RGPD, chapitre XII de la loi pour l'informatique et les libertés ... Ces obligations ont elles été prises en compte ?
8. **Archivage** - Le cycle de vie complet des données manipulées par l'application a-t-il été pensé ?

Dans ces 5 questions élémentaires à se poser au sujet des données manipulées par l'application, au moins les deux premières font la part belle aux API : API de consommation de données externes, API d'exposition de données internes, API d'exposition ou de consommation de traitement, API management. C'est la raison pour laquelle ce pilier traite à la fois des données et des API.

Les API sont un dispositif généralement approprié dès qu'il s'agit de gérer des échanges au fil de l'eau, des échanges inter-applicatif, ou des échanges avec l'usager. Ce n'est plus nécessairement vrai en matière d'analyse, de données ouvertes, les dispositifs concernés fonctionnant généralement en temps différés, et avec des masses de données qui peuvent être considérables.

Les fiches de domaine qui suivent approfondissent les 5 questions fondamentales mentionnées dans cette introduction.

Données et API -- Concevoir une application orientée données et services

Contexte

Les données sont un patrimoine de l'État. Leur portée et leur importance peut déborder du traitement, de l'application qui va les exploiter. Il est donc important, dès la conception d'un nouveau traitement ou d'une nouvelle application, de scruter celle-ci selon le prisme des données et de se poser quelques questions simples qui sont exposées dans le tableau qui suit.

Sujet	Quelle question doit on se poser ?
Réutilisation (consommation de données déjà existantes)	les données que doit manipuler mon application existent-elles déjà ailleurs et ai je envisagé une réutilisation ?
Exposition	l'application est elle pensée pour faciliter la réutilisation des données qu'elle crée ou transforme ?
Exposition de traitements	Au-delà d'une exposition brute de données, les **traitements** sur les données peuvent être exposés. Sont-ils exposés en vue d'une réutilisation possible ?

Les services. Réutiliser des données, exposer des données, exposer des traitements : ces actions sont des services et « exposés » aux travers d'interfaces, ou API (Application Programming Interface). La notion dAPI est aussi ancienne que l'informatique et recouvre des réalités très diverses. Dans sa signification contemporaine, beaucoup plus précise, et massivement utilisée dans le monde de l'Internet, l'API est un service WEB qui utilise le protocole http(s) et un style d'architecture REST ou REST full.

Le type d'interface dont il sera question dans la suite de la fiche sera ce type d'API HTTP/REST.

Le document « Démarche d'APIsation » du ministère de l'Agriculture décrit la démarche dans toute sa dimension : architecture, design, sécurité et gouvernance.

Réutilisation

Rappel de la question initiale : les données que doit manipuler mon application existent-elles déjà ailleurs et ai je envisagé une réutilisation ?

La réponse à cette question nécessite de croiser les données métier manipulées par l'application avec les données réutilisables, au niveau ministériel comme interministériel.

Il peut s'agir

- de données de référence, souvent qualifiés de "communs", exposés sur des dispositifs de type MDM (Master Data Management) - Il peut s'agir du GDR (Gestion de Données de Référence) de la DSIC, ou les données de référence exposées par le SIR du ST(SI)² pour la sécurité intérieure ;
- de données exposées dans le SI de l'État, dans le cadre État Plateforme et de FranceConnect Plateforme. Exemple : l'API Entreprise ;
- de données exposées par d'autres applications ;
- de données ouvertes.

La question initiale peut être affinée en plusieurs sous questions :

1. La donnée existe-t-elle ?
2. La donnée est elle réutilisable dans le contexte de mon application?

La donnée existe-t-elle ?

Les outils de recherche :

- les données ouvertes dans data.gouv.fr
- le référentiel CANEL

- datalab.minint.fr
- les catalogues d'API (la majorité des API exposent des données plus que des traitements) : api.minint.fr pour le ministère et api.gouv.fr pour l'Etat.

La donnée est elle réutilisable ?

Il n'est pas suffisant que la donnée existe, encore faut-il que sa sémantique soit compatible, que sa qualité soit satisfaisante, que la qualité de service de l'exposition soit compatible avec les exigences de mon application, que les performances soient suffisantes, qu'une solution de repli ait été prévue en cas d'interruption de service, le cas échéant qu'un contrat de service ait été établi avec le fournisseur.

Exposition

Rappel de la question initiale : l'application est elle pensée pour faciliter la réutilisation des données qu'elle crée ou transforme ?

Une application peut produire des données métier qui peuvent s'avérer intéressantes au-delà du contexte de l'application. Il est alors obligatoire de prévoir une exposition de ces données pour une ré-utilisation éventuelle. Ce type d'exposition est la base de l'approche État Plate-forme avec ses API données. Autres sujets à aborder : mise à disposition sous forme de données ouvertes, catalogage obligatoire, facilitation des traitements par des outils d'analyse, anonymisation ....

Modalités d'exposition : une exposition par API, quand elle ne participe pas à un inter-ou intra-applicatif planifié, a tout bénéfice à utiliser les services d'une plateforme d'échange et de sa brique de gestion d'API (API Management). En effet une brique de gestion d'API offre un certain nombre de services tels que

- la gestion de la performance (il est possible de limiter les appels par acteurs - throttling)
- le contrôle d'accès s'il est nécessaire
- la contractualisation - Cf offre de service datapass.api.gouv.fr de la DINUM pointée en fin de fiche.
- la traçabilité et l'accounting
- de la conversion (API SOAP en API REST par exemple)
- à compléter ....

Questions ouvertes : le chef de projet n'a pas vraiment intérêt à exposer « ses » données ? Cela représente pour lui un risque et un surcoût. Pour aller au-delà du vœu pieux, il semble nécessaire qu'il existe une entité tierce pour (1) identifier les données intéressantes et (2) payer le surcoût.

Question subsidiaire : mon application produit elle des données de référence ? Dans la définition qui en est donnée dans le Cadre Commun d'Architecture des Référentiel de données une donnée de référence se définit par les propriétés suivantes :

1. elles sont utilisées fréquemment par un grand nombre d'utilisateurs, internes et externes
2. leur qualité est critique pour un grand nombre de processus
3. leur sémantique est partagée et relativement stable dans le temps
4. elles ont une durée de vie qui va au-delà des processus opérationnels qui les utilisent
5. la facilité d'accès à ces données est critique

Si ma donnée entre dans cette catégorie des données de référence, il faudra envisager de la traiter comme telle, et probablement d'utiliser un système d'exposition dédié : GDR ou SIR.

Exposition de traitements

Rappel de la question initiale : Au-delà d'une exposition brute de données, les **traitements** sur les données peuvent être exposés.

Sont-ils exposés en vue d'une réutilisation possible ?

Règles et recommandations

Pour information, il existe des règles pertinentes dans le périmètre des référentiels de données dans le Cadre Commun d'Architecture des Référentiel de données

Le référentiel "stratégie d'API" est lui même un recueil de règles et de recommandations (ou bonnes pratiques) : Stratégie d'API - Règles et recommandations

Ref	Statut	Intitulé
1445	RG	Pour toute donnée, les conditions d'une possible réutilisation doivent être envisagées. Réutilisation en mode différé sous forme de publication de jeu de données ouvertes, et exposition au fil de l'eau sous forme d'API.
1446	RG	Toute nouvelle API susceptible d'être réutilisée, doit être cataloguée et documentée sur le catalogue api du ministère (api.minint.fr) si son usage est strictement restreint au ministère, sinon sur celui de l'état (data.gouv.fr).
1447	rc	Toute nouvelle API susceptible d'être réutilisée devrait être exposée via l'une des plateformes d'API Management du ministère.
1448	RG	En cas de consommation d'API externe, l'intermédiation d'une plateforme d'échange doit être privilégiée.
1360	RG	Il est obligatoire de réutiliser les données existantes
1100	RG	Les composants fonctionnels manifestement communs à plusieurs applications doivent être développés sous forme de services réutilisables.

Informations utiles

Contacts utiles

- Administrateur ministériel des données
- Administrateurs de données métier

Offres de service

Systèmes référentiels du ministère (MDM) :

- Offre de service GDR (Gestionnaire de Données de Référence) - Lien vers l'offre à venir - Contact GDR
- Offre de service du SIR

Contractualisation pour les API de l'État :

- La DINUM a mis en place un outil de contractualisation pour des API cataloguées sur api.gouv.fr. Cette outil de gestion des habilitations juridiques pour les données à accès restreint, nommé Data Pass est accessible sur https://datapass.api.gouv.fr. La mise en oeuvre d'une contractualisation (délivrance d'un "passe") pour votre API est réalisée en collaboration avec la DINUM.

Ressources

- Exploration du patrimoine de données en vue d'une réutilisation:
  - Données ouvertes de l'Etat
  - Datalab ministériel
  - Catalogue d'API ministériel
  - Catalogue d'API gouvernemental
- Possibilités de réutilisation : les catalogues d'API cités au dessus documentent généralement les conditions d'une réutilisation.
- Stratégie API du MI
- Etude API du MAA (sous réserve autorisation)

Zone d'entraide

- A renseigner

Données et API -- Gestion des échanges

Contexte

Les applications sont rarement autarciques : elles s'intègrent dans un écosystème ministériel, voire interministériel (SI de l'État), voire au-delà (SI collectivités, partenaires, usagers ..) avec lesquels elles échangent des données. Celles-ci peuvent être des données externes qu'elles consomment, ou des données internes qu'elles exposent (à la consommation des autres applications).

Interfaces d'échange -- ou API

Dans la stratégie de l'État plateforme, qui s'aligne en cela sur des pratiques généralisée dans l'Internet, les données sont échangées selon le profil recommandé P1 « Fondations État Plateforme » défini dans le Réglement Général d'Interopérabilité (RGI) qui préconise des interfaces API basées sur le protocole https, le style d'architecture REST, le format de données JSON, et le protocole d'authentification OpenID Connect. Un certain nombre de bonnes pratiques ont été définies pour ces échanges, notamment au niveau ministériel avec la stratégie API qui définit le niveau sémantique des API REST.

Pour des raison de compatibilité avec les systèmes historiques (legacy in english), les interfaces peuvent être encore des webservices SOAP, mais leur usage est déconseillé pour les nouvelles applications.

Beaucoup d'autres modes d'échange ont existé et existent encore :

- échanges par fichier -- Encore très répandus, notamment pour les données ouvertes.
- CFT, RMI/JRMP, PeSIT ...

Les plateformes d'échange

Le ministère structure ses échanges autour de deux plate-formes d'échange, [toutes deux associées à un gestionnaire de données de références] :

- INES, opérée par la DSIC
- SIR (Système d'Interface et de Référence), opérée par le ST(SI)²

Il font tous les deux l'objet d'une offre de service que vous retrouverez dans la section informations utiles.

Les autres DSI (PP, ANTS, ANTAI ...) ne se sont pas dotées de plateforme d'échange, quoiqu'il puisse en exister dans des silos applicatifs.

Au delà du ministère, pour faciliter la gestion des flux interministériels, la DINSIC est en train de se doter d'une plateforme d'API Gateway / Management et d'un composant de contractualisation, FranceConnect Plateforme.

Le composant majeur des plateformes d'échange est l'**API Gateway / API Management**. Celui offre un certain nombre de fonctions essentielles telles que :

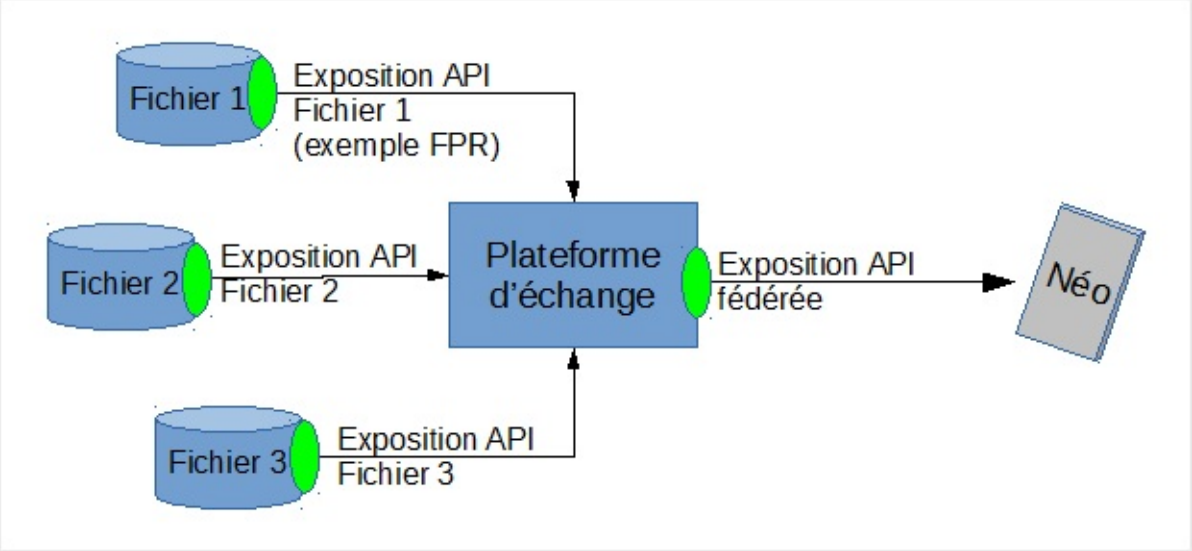
- **Passerelle d'API** avec des fonctions d'exposition des services et des ressources, de sécurisation des flux, de régulation du trafic (seuils, quotas), de contrôle des identités et des droits (par jetons)
- **Magasin d'API** avec des fonctions de publication, des API, de souscription aux API, de tableau de bord pour les développeurs -- Cette fonction est portée au ministère par un autre composant : https://api.minint.fr
- **Editeur d'API** avec des fonctions de gouvernance (cycles de vie, versioning) , facturation, monitoring, autorisation

Les plateformes d'échanges peuvent également fournir, pour des raisons de compatibilité avec les applications historiques, des fonctions permettant de gérer et de transformer les flux :

- ESB (Enterprise Service Bus). Ces bus de services sont capables de prendre en charge des transformations ainsi que des agrégations de flux dans des contextes d'échanges inter-applicatifs.
- SAS fichier

Fonctions d'intermédiation des plateformes d'échange.

La plateforme d'échange peut également offrir un service à valeur ajoutée sous forme d'une intermédiation entre un consommateur et plusieurs fournisseurs.

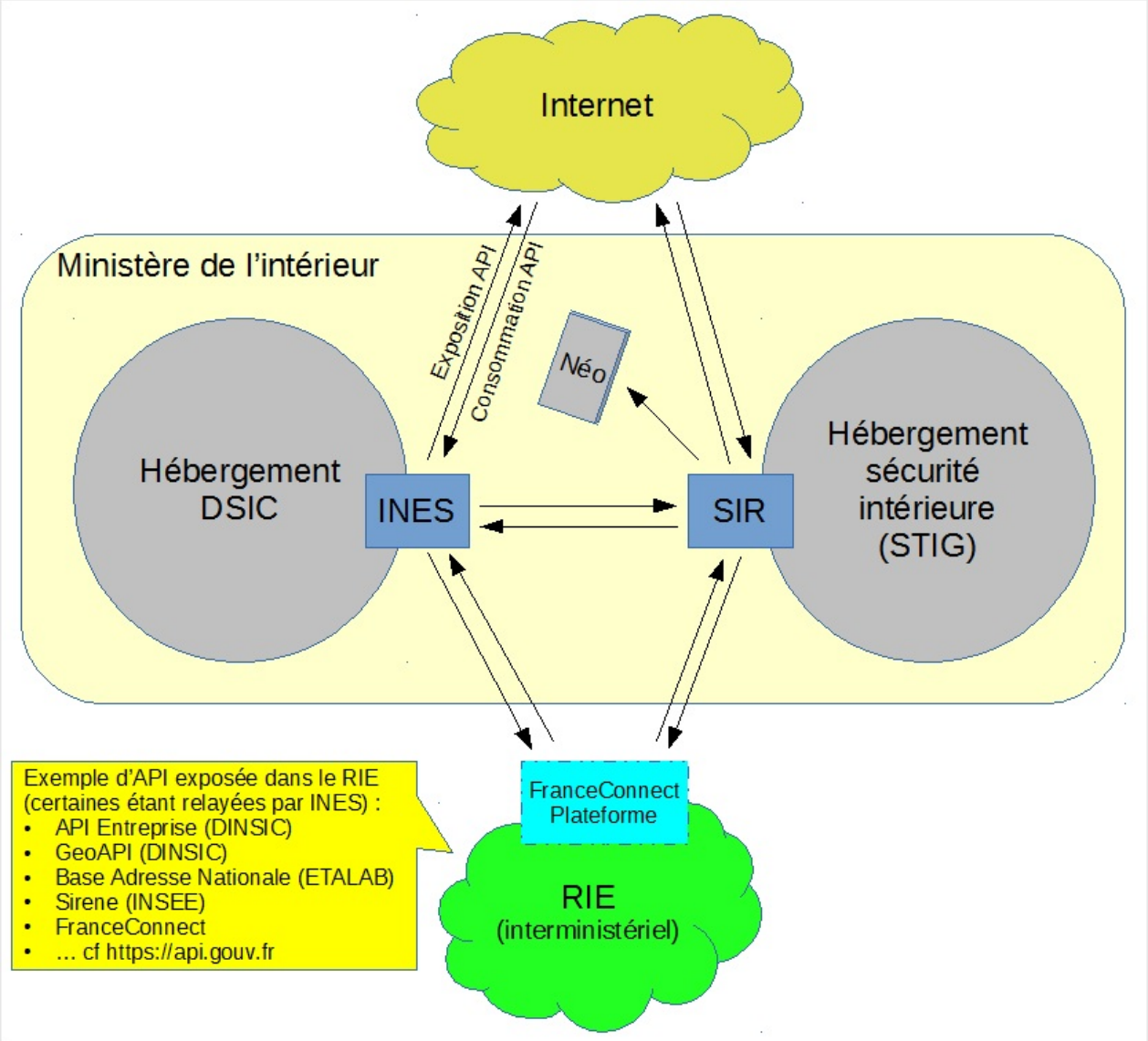


L'exemple ci-dessus montre un cas d'intermédiation avec la possibilité pour une application mobile du smartphone Néo qui équipe les forces de l'ordre d'interroger plusieurs fichiers de police en une seule demande sur une API fédérée.

API Entreprise de la DINSIC est un autre exemple d'intermédiation et de service à valeur ajoutée en ce qu'elle agrège des informations de l'INSEE (Sirene) et d'Infogreffe.

INES - DSIC	SIR - ST(ST)²
La plateforme INES met en œuvre 3 composants : • API management (tel que décrit ci-dessus) • ESB (Bus de service) qui permet de transformer ou d'agréger des flux. • SAS fichier La plateforme INES est appelée à prendre en charge tous les flux d'API internes au applications hébergées par la DSIC. La plateforme INES mutualise le raccordement au RIE et à Internet. C'est elle qui permet de « consommer » des API externes, comme par exemple l'API entreprise, la BAN, l'API INSEE …etc. INES est raccordé au SIR et route les flux destinés aux applications de sécurité interieure hébergées au STIG	La plateforme SIR est basée sur un ESB (Bus de service) qui permet notamment d'assurer le routage, la sécurisation, et des agrégations de flux d'API. La plateforme SIR prend en charge les flux d'API sortant du périmètre du centre d'hébergement de la sécurité intérieure (STIG). Le SIR ne prend pas en charge les flux internes au STIG. SIR est raccordé à INES et route les flux destinés aux applications de hébergées dans le centre d'hébergement de la DSIC. Le SIR route et aggrège tous les flux API avec les équipements mobiles des forces de l'ordre, notamment les applications des smartphones Neo (interrogation de fichier ..etc). Cf schéma ci-dessus.

Urbanisation des flux



Les deux plateformes d'échanges sont dédiées aux deux principaux hébergements nationaux, INES pour l'hébergement DSIC et SIR pour l'hébergement de la sécurité intérieure. Les flux inter-applicatifs transitant entre les deux hébergements sont relayés (contrôlés, sécurisés ...) via INES et SIR.

Impacts sur les applications

Impact positif : les applications n'ont pas à contractualiser avec chacun de leur partenaire d'échange, ce rôle est délégué avec la plateforme d'échange qui centralise cette fonction.

A compléter.

Règles et recommandations

Ref	Statut	Intitulé
1449	rc	La consommation d'API interne devrait passer par une fonction d'API gateway pour avoir une bonne visibilité sur l'ensemble des flux de consommation.
1450	RG	Les flux inter-applicatifs inter-centres d'hébergement transitent par INES et SIR.
1451	RG	La plateforme INES est le point d'entrée pour les API interministérielles (API entreprise, API INSEE, BAN ...etc). Grâce à son API management, elle est garante du respect du contrat de service établi avec les fournisseurs extérieurs.
1363	RG	Le format de présentation et d'échange d'une adresse postale doit respecter la norme AFNOR XPZ 10-011.
1047	rc	Si l'échange entre deux applications nécessite une transformation des données, il est recommandé de s'appuyer sur les plateformes d'échange du ministère.
1048	RG	Les échanges asynchrones entre deux applications du ministère ou avec un partenaire en zone de confiance réseau doivent être réalisés via les plate formes d'échange du ministère.
1065	RG	Les échanges par Web Service ou par API doivent permettre à chaque système impliqué dans l'échange de s'assurer de l'identité du partenaire
1072	RG	Tout fichier XML doit être accompagné de son schéma.
1074	RG	Les formats PNG et JPEG doivent être utilisés pour échanger les informations graphiques et les images fixes.
1075	RG	Les flux audiovisuels, doivent respecter les formats MPEG-2 ou MPEG-4.
1076	RG	En complément du RGI, pour tous les échanges de documents bureautiques internes et externes, seuls les formats OpenDocument et PDF sont autorisés.
1078	RG	Le format d'échange des fichiers géographiques retenu est le format ShapeFile.
1120	RG	Tout échange d'informations avec un SI externe au ministère doit faire l'objet d'un traitement particulier par des serveurs proxy déployés au sein d'une DMZ (conformément aux recommandations de l'ANSSI) afin de vérifier l'innocuité et l'intégrité des flux ou des fichiers. Les infrastructures nationales existantes (ex : SIR, INES) doivent être systématiquement privilégiées.
1165	RG	Les interconnexions avec des partenaires externes doivent être réalisées en priorité à l'aide de VPN IPSEC, selon les recommandations de configuration ANSSI. A défaut, l'usage du protocole TLS, basé sur l'authentification mutuelle par certificat, sera utilisé.

Informations utiles

Contacts utiles

- Contact INES à fournir
- Contact SIR à fournir

Offres de service

Les plateformes d'échange / API management :

- Offre INES
- Offre SIR (version CCT 2.8)

Ressources

- Stratégie API du MI

Zone d'entraide

- A renseigner

Données et API - Analyser et valoriser les données

Contexte

Plusieurs constats ont amené le Ministère de l'Intérieur à s'intéresser aux sciences de la donnée :

- La maîtrise de la donnée, de la science de la donnée et de l'intelligence artificielle est identifiée par le Gouvernement comme un enjeu stratégique.
- Dans le domaine informationnel, les directions métiers du Ministère de l'intérieur ont des pratiques, des processus et outillages très hétérogènes.
- Le Ministère de L'Intérieur héberge des infocentres mais possède peu de compétences BI (Business Intelligence). La diversité des outils et des pratiques rend difficile toute tentative de maîtrise des données produites et hébergées par la DSIC
- La complexité technique et le manque de compétences en matière d'information décisionnelle constituent des barrières à l'accès aux données métier et à leur compréhension.

Fort de ces constats, plusieurs initiatives sur la valorisation des données métiers à destination des directions métiers du Ministère sont en cours de développement. En particulier, plusieurs axes sont adressés :

- Le développement d'un savoir faire "DATA" au sein du Ministère ;
- La Mutualisation des ressources techniques et des compétences SIC nécessaires aux usages actuels (BI - Business Intelligence) et aux usages à développer (DATA Science et IA)

En vue de :

- accompagner les directions métier dans l'identification des usages potentiels de la Data science et de l'IA et dans la mise en œuvre de ces projets d'application ;
- Faciliter la mise en place d'expérimentation sur les données et optimiser le passage à l'échelle des projets de data science et d'IA ;
- Fiabiliser les statistiques et produire des indicateurs clé de performance (KPI).

Impact sur l'application

Toute application qui sera amenée à alimenter une plateforme technique de valorisation de données, devra intégrer

- **des extracteurs de données** - permettant de sortir les données opérationnelles de l'application pour les intégrer au sein de la plateforme technique.
- si besoin des mécanismes d'**anonymisation des données**, avant d'alimenter la plateforme technique de valorisation des données.

Règles et recommandations

Informations utiles

Contacts utiles

- **Administrateur ministériel des données** : Les besoins remontés par les directions seront traitées par **Daniel Ansellem** (daniel.ansellem@interieur.gouv.fr), administrateur de données au sein de la MGMSIC.
- **Chef de produit de l'offre de service "ENTREPOT"** : Les besoins remontés par les projets doivent être remontés à **Christophe Marquaille** (christophe.marquaille@interieur.gouv.Fr), Product Owner de l'offre Entrepôt. qui se charge d'identifier et/ou de cadrer le besoin

Offres de service

Offre de service "ENTREPOT" DSIC :

- Entrepôt - Mise à disposition du service sur le cloud PI - v1.1
- Entrepôt - Présentation détaillée v1.1

Ressources

Zone d'entraide

Gestion des données personnelles

Contexte

Tout d'abord qu'entend-on par données personnelles ? *On considère comme donnée personnelle toute information relative à une personne physique vivante identifiée ou identifiable, directement ou indirectement.*

Au vu de cette définition, rares sont les applications du ministère qui ne traitent pas de données personnelles.

La protection des données personnelles relève de plusieurs cadres juridiques :

- Le règlement européen RGPD (Règlement Général pour la Protection des Données)
- la loi 78-17 informatique et libertés
- La directive européenne 2016-680, transposée dans le chapitre XIII de la loi pour l'informatique et les libertés qui s'applique au périmètre de la sécurité publique et des infractions pénales
- La sûreté de l'État et le renseignement

Le RGPD

Le règlement européen renforce de façon significative les droits de l'usager sur ses données personnelles, notamment :

- Droit d'accès aux données, de rectification
- Selon les circonstances : droit à l'effacement, opposition
- Pour certains traitements (et très rare au MI) : portabilité des données

Politique de conformité des données personnelles du ministère de l'intérieur (PCDP-MI)

Le RGPD ne parle pas d'application mais de **traitement de données** définition très large qui désigne ainsi toute action sur ces données. Un traitement peut être automatisé (une ou plusieurs applications) ou non (par exemple l'utilisation de la messagerie électronique pour envoyer un mail). Le RGPD ne s'applique qu'aux traitements automatisés (donc pas à un mail pris isolément), ainsi qu'à tous les fichiers même papier (dont un simple tableau excel).

Selon le RGPD, tout traitement doit avoir un **responsable de traitement** : dans la pratique celui qui détermine la finalité et les moyens du traitement. Ce responsable sera typiquement le préfet d'un département, ou le directeur d'une administration centrale.

Chaque responsable de traitement a l'obligation de maintenir un *registre* des traitements dont il a l'initiative (ce qui exclut les traitements nationaux dont il n'est qu'utilisateur). Ce registre peut être audité par la CNIL, et également, en tant que document administratif, communiqué sur demande citoyenne après occultation des mentions relatives à la sécurité (Cf annexe 2 de la note du DPD).

Lorsqu'un traitement est susceptible "d'engendrer un risque élevé pour les droits et les libertés des personnes physiques" (art 35 du RGPD), **le responsable du traitement doit faire mener une analyse d'impact du traitement sur la protection des données à caractère personnel**.

Remarque : l'analyse d'impact est souvent nommée PIA, Privacy Impact Assesment ou encore Etude d'Impacts sur la Vie Privée. (Cf annexe 3 de la note du DPD). Elle doit comporter l'avis du délégué ministériel avant sa validation par le responsable du traitement. L'analyse permet de vérifier la conformité juridique du traitement, d'évaluer les risques, et de mettre en place les mesures de sécurité appropriées. Si une homologation SSI est menée, il est recommandé de la coupler à l'analyse d'impact RGPD : les deux vont recenser les mêmes risques (notamment SSI), et elles différeront sur le périmètre des enjeux : impact sur les droits et libertés pour la PIA, impact sur le ministère pour l'homologation SSI.

Le RGPD crée également la fonction nouvelle du DPD, Délégué à la Protection des Données. Au ministère, le délégué ministériel à la protection des données est rattaché directement au Secrétariat Général. Il est compétent pour tous les services centraux et déconcentrés du ministère, ainsi que pour ses opérateurs. Il est désigné formellement auprès de la CNIL dont il est le principal interlocuteur. Le DPD s'appuie sur un réseau de "correspondants à la protection des données" qui relaient son action au sein des directions centrales et des services déconcentrés (préfectures) et assistent les responsables de traitement dans leurs responsabilités (Cf annexe 1 de la note du DPD).

La loi 78-17 Informatique et libertés

La loi fixe les principes généraux, précise les marges de manœuvres nationales du RGPD, transpose les directives 2016/680 et 2002/58/CE, et contient le droit strictement national.

Chapitre XIII de la loi informatique et libertés

La directive européenne 2016-680, transposée dans le chapitre XIII de la loi pour l'informatique et les libertés, s'applique à la place du RGPD le périmètre du RGPD dans le périmètre de la sécurité publique et des infractions pénales. Elle reprend les compétences du délégué, ainsi que les obligations de registre et d'analyse d'impact.

Impacts pour l'application

La protection des données à caractère personnel, que celle-ci relève du RGPD ou du chapitre XIII de la loi pour informatiques et libertés (périmètre sécurité publique et infractions pénales) a un **impact important pour l'application** dans l'ensemble de son cycle de vie (conception, exploitation, décommissionnement). Ainsi que le spécifie le RGPD dans l'article 25, la protection des données doit être prise en compte **dès la conception, et par défaut** (en angais, privacy by design, privacy by default).

Le guide méthodologique de la CNIL « Analyse d'impact relative à la protection des données / La méthode», la démarche de mise en conformité s'appuie sur deux piliers :

- les **principes et droits fondamentaux**, qui sont non négociables parce que réglementaires. On peut citer parmi les droits fondamentaux, l'information des personnes concernées, l'exercice des droits selon les situations (d'accès, de rectification, d'effacement, de limitation du traitement ....)
- la **gestion des risques sur les droits et libertés des personnes**, qui permet de déterminer les mesures techniques appropriées.

La mise en conformité nécessite la mise en place d'un ensemble de mesures, dont beaucoup sont d'ordre fonctionnel, organisationnel, ou de mise en place de processus. Un certain nombre de ces mesures sont techniques et relève donc du présent cadre de cohérence technique.

Les relations avec les sous-traitants qui traitent des données personnelles pour le compte du ministère sont également impactées (nouveaux devoirs du sous-traitant). Le nouveau cadre juridique a les conséquences suivantes, y compris sur l'existant :

- nécessité de modifier tous les contrats de sous-traitance pour les mettre en conformité avec l'article 28 du RGPD ;
- pour les traitements relevant du chapitre XIII de la loi, mise en place obligatoire d'une journalisation (logs) selon des critères impératifs (article 70-15 de la loi).
- pour tous les traitements : mise en place du concept de limitation du traitement des données (marquage de certaines données pour empêcher leur utilisation, sans toutefois les effacer).

La CNIL a édité un catalogue des mesures de mise en conformité (Analyse d'impact relative à la protection des données / Les bases de connaissance). Le tableau ci-dessous synthétise dans ce catalogue les mesures techniques relevant d'un CCT.

Mesures de protection des données (extrait guide CNIL cité ci dessus)	Mesures techniques
2 - Anonymisation	La DSIC offre un service de traitement de la donnée qui inclue une prestation d'anonymisation </br>Anonymisation de données
3 - Archivage	La protection des données à caractère personnelle a des impacts sur la politique d'archivage. Cf fiche cycle de vie de la donnée. (offre de service Maarch RM, VITAM, chiffrement des données)
4 - Chiffrement	Le référentiel de composant du CCT préconise des composants de chiffrement, comme les composants PRIM'S
5 - Cloisonnement des données	NA
7 - Contrôle d'intégrité	NA
8 - Contrôle des accès logiques	Cf Fiches identification et authentification de l'agent et de l'usager
11 - Exercice des droits de l'usager	Ces nouveaux droits de l'usager induisent principalement des mesures organisationnelles.Du point de vue technique, la mise en œuvre des droits de l'usager nécessite un bon niveau d'authentification de celui-ci. _Cette fonction pourrait être utilement mutualisée par un téléservice au niveau ministériel (ou au-delà).
19 - Gestion des postes de travail	La protection des données à caractère personnelles implique le poste de travail. Cf fiche ETNA
35 - Surveillance	NA
37 - Sécurité des canaux informatiques (réseaux)	NA

Remarque : les mesures proposées par la CNIL a) ne sont pas obligatoires b) ne sont pas nécessairement adaptées à notre situation c) ne sont pas nécessairement suffisantes par rapport à nos problématiques. On peut s'en servir comme guide, mais toujours avec du recul.

Le guide CNIL « Analyse d'impact relative à la protection des données » dans son volet base de connaissance est un catalogue des mesures destinées respecter les exigences légales du RGPD et à traiter les risques. Un certains nombre de ces mesures relèvent du CCT.

A compléter : inventaires des mesures techniques pertinentes.

Règles et recommandations

Règles à identifier

Informations utiles

Contacts utiles

- Le DPD - Délégué ministériel à la Protection des Données : delegue-protection-donnees@interieur.gouv.fr
- Les correspondants du DPD : l'information peut être obtenue sur l'intranet du DPD Page des correspondant sur l'intranet du DPD. Pour information les adresses fonctionnelles des correspondants des départements ont la forme pref-donnees-personnelles@nomdudepartement.gouv.fr. Pour les services centraux, donnees-personnelles-nomduservice@interieur.gouv.fr

Offres de service

La DSIC offre un service de traitement de la donnée qui inclue une prestation d'anonymisation : Anonymisation de données

Ressources

- Site Intranet du DPD
- Politique de conformité des données personnelles du ministère de l'intérieur (PCDP-MI)
- La CNIL publie son registre https://www.cnil.fr/fr/la-cnil-publie-son-registre-rgpd
- Analyse d'impact relative à la protection des données la méthode : CNIL - Méthode
- Périmètres à prendre en compte avant de réaliser ou non une analyse d'impact : CNIL - Base de connaissance
- Modèles de PIA : se renseigner auprès du correspondant de votre service
- Guide pratique de la publication en ligne et de la réutilisation des données publiques - Ce guide, rédigé conjointement par la CADA (Commission d'Accès aux Documents Administratifs) et la CNIL fait l'objet d'une consultation publique jusqu'au 4 avril 2019. Consultation publique

Formations et ateliers organisées par le DPD : se renseigner auprès de son équipe (cf contacts utiles)

Zone d'entraide

- Les correspondants DPD ont un espace collaboratif qui leur est dédié : OCMI DPD
- A titre d'expérimentation, le réseau DPD utilise également un espace collaboratif interministériel : OSMOSE

Cycle de vie de la donnée et archivage

Contexte

La donnée au sens large (document, donnée structurée ou non) a un cycle de vie, que l'on peut figurer par sa température.

- elle est "chaude" lorsqu'elle est utilisée quasi-quotidiennement par son service producteur et ses consommateurs. Durant cette phase, elle doit être pleinement disponible, dans la limite bien sûr de la sécurité Si et de la protection des données personnelles.
- elle devient "tiède" à la fin de son usage public mais qu'elle reste à disposition du service producteur
- puis "froide" lorsque la donnée n'est plus utilisée qu'à des fins historiques scientifiques ou statistiques.

Ou intervient l'archivage dans ce cycle de vie de la donnée ? La définition de l'archivage, selon le code du patrimoine article L 211-1 est très large et recouvre l'ensemble du cycle décrit ci-dessus. 'Les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité' Au sens du code du patrimoine, les données sont considérées comme des archives dès leur création. les données "chaudes" sont des archives courantes, les données "tièdes" sont des archives intermédiaires, et les données "froides" sont des archives définitive.

Impact sur les applications

L'aplication doit prendre en compte dans sa conception le cycle de vie de la donnée. C'est à dire les trois phases de l'archivage : courant, intermédiaire et définitif.

1. L'application détient exploite utilise des données chaudes, ou archives courantes dans la langue des archivistes.
2. Lorsque ces données "tiédissent", c'est à dire qu'elles ne sont plus consommées, elles doivent être versées à un système prenant en charge les archives intermédiaires. Le ministère est doté d'un système d'archivage intermédiaire et il convient de s'assurer que le versement pourra être mis en place avec un minimum d'effort (respect des interfaces).
3. La dernière phase concerne l'archivage définitif - ou la destruction, choix qui dépend du responsable des archives ministérielles - Les archives définitives sont externalisées ...

Règles et recommandations

Règle (proposition)

Toute application doit prévoir dans sa conception le versement des données aux archives intermédiaires du ministère, dans le respect de l'interface SEDA.

Ref	Statut	Intitulé
1129	RG	Lorsqu'une application comporte des données actives et des données historiques, elles doivent être stockées dans des bases ou des fichiers différents.
1444	RG	Toute application nécessitant un archivage des données doit prévoir dans sa conception le versement des données aux archives intermédiaires du ministère, dans le respect de l'interface SEDA.

Informations utiles

Contacts utiles

La MAN, Mission des Archives Nationales est une délégation au ministère de l'intérieur du service des archives nationales : Mission des Archives Nationale

Offres de service

Le service d'archivage intermédiaire du ministère s'appuie sur le progiciel Maarch-RM. Le service est réalisé par le SGAMI Sud-Ouest, sous pilotage DSIC. Offre de service : lien à fournir

Offre de service VITAM.

Ressources

Lien sur les spécifications de l'interface SEDA (standard d'échange de données pour l'archivage) : Lien sur le standard SEDA

VITAM : programme interministériel archivage numérique

VITAM : page de ressources

Le référentiel général de gestion des archives (R2GA) : R2GA

Zone d'entraide

Pilier sécurité

SSI et homologation

Contexte

La **sécurité (SSI)** d'une application, n'est pas une option, elle est l'une des conditions qui lui permettront d'offrir le service attendu en garantissant la disponibilité, la confidentialité et l'intégrité de l'information.

Le souci de la SSI concerne toutes les applications, elle ne se limite pas aux **SI « vitaux » ou « essentiels »** tels que les définit le SHFD.

La SSI doit être prise en compte dès la conception de l'application et jusqu'à son dé-commissionnement. Sa prise en compte est inscrite dans le projet par une **démarche d'intégration de la sécurité des systèmes d'information dans les projet, ou DISSIP**.

Dans le prolongement de la DISSIP, la sécurité de l'application est attestée, avant sa mise en production, par son **homologation de sécurité**. L'homologation permet à un responsable, s'appuyant sur l'avis des experts, de s'informer et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. La décision d'homologation constitue donc un acte formel par lequel l'Autorité :

- atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- en accepte les risques résiduels

Le responsable de la DISSIP et de l'homologation de sécurité, sont principalement la direction / chefferie de projet MoA (métier), assistée du RSSI métier. Le chef de projet MoE et le RSSI MoE ont un rôle de support.

Les principaux acteurs de la SSI sont :

- Le Service du Haut Fonctionnaire à la Défense (SHFD)
- La chaîne SSI (RSSI…) qui irrigue l'ensemble du ministère, préfectures comme directions centrales, maîtrises d'œuvre (les DSI / acteurs SIC) comme maîtrises d'ouvrages (directions métier).

Remarque : la sécurité des données à caractère personnel est une composante importante de la SSI, mais elle est traitée dans une autre fiche, régie par un règlement spécifique (le RGPD) et ses acteurs sont distincts du réseau SSI : le Délégué à la protection des données et son réseau de correspondants. Par contre, il faut attirer l'attention sur le fait que l'application, selon sa sensibilité, peut nécessiter une analyse de risque au sens SSI / DISSIP, ainsi qu'une analyse d'impact au sens protection des données à caractère personnel / RGPD. Ces deux analyses de risque ont un coût et il y a un bénéfice à les mutualiser, malgré le fait qu'elles dépendent de réseaux différents (chaîne SSI et réseau DPD)

La SSI comporte également un aspect technique sous la forme de composants de sécurités préconisés dans le référentiel de composant du CCT. Pour exemple, les composants de chiffrement PRIM'X, les composants de signature électronique et d'horodatage ...etc.

Impacts sur les applications

La présente fiche CCT adresse les applications sur plusieurs plans distincts :

- rappel de la méthode : la démarche projet (DISSIP), l'homologation de sécurité
- les impacts budgétaires qui doivent être prévus, notamment
  - l'éventuelle sous-traitance de l'analyse de risque EBIOS ou FEROS
  - l'audit PASSI (Prestation d'Audit SSI) par un partenaire agréé ANSSI
- les règles et recommandations insufflées par les acteurs en charge de la SSI (pôle SSI des acteurs SIC et SHFD), qui sont des éléments à prendre en compte pour obtenir l'homologation de sécurité de l'application
- les composants de sécurité spécifiés dans le référentiel de produits du CCT, ainsi que les offres de services existantes, que celles-ci soient ministérielles ou interministérielles.

Règles et recommandations

Deux règles essentielles :

Règle (proposition à valider)

Rappel de la règle INT-HOMOLOG-SSI de la PSSI MI (Homologation de sécurité des systèmes d'information). Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies.

Règle (proposition à valider)

La sécurité de l'information (ou SSI) est prise en compte dès la conception de l'application. Cette prise en compte est structurée par la DISSIP, démarche d'intégration de la sécurité des systèmes d'information.

Les règles qui suivent sont extraite du référentiel de règles 2.8, dans un ordre se rapprochant de la chronologie du projet :

1. les règles de méthodologie et de gouvernance
2. les recommandations de méthodologie et de gouvernance
3. les règles puis les recommandations relevant du développement

Ref	Statut	Intitulé
1385	RG	Il est OBLIGATOIRE d'identifier et de hiérarchiser les exigences de sécurité applicables au développement de l'application. Les arbitrages et les évolutions seront formalisés et tracés dans la documentation technique de réalisation ou le dossier de sécurité et d'homologation. Les exigences de sécurité applicables au développement sont constituées des éléments suivants : - La politique de sécurité des systèmes d'information applicable. - La sensibilité (confidentialité, intégrité, disponibilité) des données traitées et traitantes (code source, paramétrages, etc.). - L'analyse de risques exprimant les besoins et identifiant les objectifs de sécurité. - Les exigences de sécurité issues de la fiche d'expression rationnelle des objectifs de sécurité (FEROS). - Les éventuelles menaces prises en compte au cours de l'analyse de risque. - Les éventuelles réglementations applicables (protection du secret, données personnelles, etc.). Ces exigences de sécurité sont exprimées par les directions métier aux équipes de projet (ou aux prestataires) concernées en amont du développement. Elles sont accompagnées d'une métrique convenue permettant de les hiérarchiser, et d'effectuer des arbitrages le cas échéant, en termes d'impacts métier.
1386	RG	Il est OBLIGATOIRE d'identifier et de définir l'ensemble des rôles (métier et technique) et des privilèges strictement nécessaires et suffisants, pour le développement et la mise en oeuvre de l'application. Les rôles et privilèges associés aux acteurs du développement, aux utilisateurs et aux exploitants de l'application tant sur le plan fonctionnel (métier), que sur le plan technique (MOE, équipe projet, administrateur, opérateur sauvegarde, etc.) doivent être formalisés au sein de la documentation technique du projet (cahier des charges fonctionnel, doctrine d'emploi, etc.) ou du dossier de sécurité et d'homologation (matrice de couverture des risques, dossier d'administration et d'utilisation, etc.).
1387	RG	Il est OBLIGATOIRE d'identifier et de définir les responsabilités (métier, technique, sécurité) des différents acteurs impliqués dans le développement. Les responsabilités des différents acteurs doivent être formalisées au sein du plan de management (ou équivalent) de projet de développement : - dans le domaine fonctionnel pour la partie métier ; - dans le domaine technique pour la partie architecture, programmation, intégration, etc. ; - dans le domaine de la vérification (revue de code, tests, etc.).
1388	RG	Il est OBLIGATOIRE d'identifier au sein de l'équipe de projet un correspondant sécurité garant de la prise en compte de l'ensemble des questions de sécurité pour le projet de développement.
1398	RG	Il est INTERDIT d'utiliser des protocoles, services ou algorithmes obsolètes pour la conception de nouvelles applications Exemples de services, protocoles ou algorithmes obsolètes et vulnérables : - rlogin, rsh, telnet, SNMP v1, SSH v1. - SSL, TLS v1.0, TLS v1.1. - RC4, MD5, SHA1, DES, 3DES. - LM, NTLM v1.
1420	RG	Il est OBLIGATOIRE de contrôler les données, à traiter et traitées, en entrée et en sortie des modules et des fonctionnalités développés et codés. Afin de prévenir les risques de types injection, les données doivent être : - filtrées en rejetant les caractères non autorisés et non pris en compte ; - normalisées en les réduisant à leur représentation la plus simple ; - validées en vérifiant le format, le type, l'origine ou encore la longueur des données attendues ;

		- encodées selon le contexte de traitement.
1433	RG	Il est INTERDIT de livrer une application informatique ou un logiciel incluant des paramètres d'authentification par défaut dans les codes sources ou les fichiers de configuration. Aucun paramètre d'authentification par défaut, ne doit être stocké dans les codes sources ou les fichiers de configuration inclus dans les livraisons au risque d'être utilisés pour les déploiements ultérieurs.
1110	RG	L'application doit être conçue et développée dans le strict respect des règles de sécurité en vigueur au Ministère en particulier, pour les applications Web, veiller à ne pas être sensible aux 10 principales menaces identifiées par l'OWASP (Open Web Application Security Project)
1334	RG	De manière à mettre en place le principe de moindre privilège, il est nécessaire de définir, au niveau du SGBD, des comptes de connexion correspondants aux différents rôles définis (type administrateur, relecteur, contributeur, …).
1336	RG	De manière à se prémunir des attaques dites XSS, et en sus du filtrage des données non sûres, l'encodage des mots clé de la grammaire HTML (HTML entity encoding) doit être effectué avant stockage ou affichage de données.
1342	RG	L'ensemble des informations relatives aux sessions (variables de l'utilisateur, droits d'accès, etc.) doivent être stockées côté serveur en les associant à un identifiant de session, qui doit être la seule information envoyée au client. En particulier, il est proscrit de transmettre ces données, par sérialisation par exemple, vers le client dans l'objectif d'assurer une persistance de ces données.
1337	RG	De manière à se prémunir du vol de cookie de session ou contenant des informations sensibles (authentification ou données) par attaque de type XSS, le mécanisme HTTPOnly doit être utilisé pour sécuriser l'emploi de ces cookies.
1348	RG	Des mécanismes de nettoyage des bases de données doivent être prévus afin de supprimer tout contenu illégitime (ex : existence de scripts en lieu et place d'une chaîne de caractère)
1434	rc	En cas de DISSIP renforcée il est RECOMMANDE d'armer la comitologie projet d'un COSEC (Comité Sécurité) dont le but serait de conduire la DISSIP, de préparer l'homologation et qui serait animé par le correspondant sécurité du projet.
1194	RG	La traçabilité des actions de gestion des utilisateurs et de leurs droits doit être assurée.

Informations utiles :

Contacts utiles

- Liste des RSSI du ministère (page à fournir sur http://ssi.minint.fr)
- Rechercher "son" RSSI avec son identifiant orion : mon RSSI
- Contact formation (SHFD - Section Communication Accompagnement Formation) : SHFD-SCAF
- Contact SHFD : à fournir

Offres de service

- SHFD : moyens sécurisés à disposition de l'utilisateur pour l'exercice de sa fonction
- SHFD : infrastructure de gestion de clé
- SHFD : catalogue de services
- DSIC : Catalogue de service (signature électronique, horodatage)
- DSIC : marché de prestations de conseil d'expertise et d'audit dans le domaine de la sécurité des systèmes d'information : *La DNUM concentrera à terme les services achats et les marchés associés*
  - Lot 1
  - Lot 2 (audit)

Ressources

L'essentiel des ressources sont exposées sur le site SHFD

- Page maitrise d'ouvrage (homologation, DISSIP, clauses de sécurité dans les marchés, achat de produits de sécurité) : MoA
- Page référentiels Référentiels

Zone d'entraide

Pas de collaboratif identifié.

Pilier fabrique de code

Forges d'intégration et de déploiement continu

Contexte

Dans l'esprit du guide d'intégration, il est convenu d'ignorer le contenu de l'application (une boite noire) et de n'adresser que ses interfaces avec l'écosystème ministériel et interministériel. Le pilier fabrique de code peut paraitre déroger avec cette approche. En réalité, les nouvelles pratiques de fabrique de code et de produits, sous l'impulsion des méthodes agiles et du devops, obligent à considérer ce domaine comme une interface obligatoire et structurante avec l'écosystème.

La construction d'une nouvelle application, d'un nouveau produit, s'appuie aujourd'hui dans une chaîne d'**intégration continue** puis de **déploiement continu**. Les hébergements cloud, du ministère (PI), ou de l'État (offre FranceCloud) , renforcent cette tendance.

La **chaîne d'intégration continue** vise à la production, d'un paquetage déployable de l'application ou d'un produit. Elle met à disposition un dépôt des codes source, permet d'**automatiser** les phases de compilation, de jeu des tests unitaires, de vérification de qualité du code...

La **chaîne de déploiement continu** vise à automatiser les opérations de déploiement auparavant réalisées manuellement par une équipe d'exploitation. Cette automatisation permet de fiabiliser le déploiement et d'augmenter la fréquence des livraisons, et des mises en production. Avec les environnement de cloud et la conteneurisation, le déploiement continu consiste permet aussi de scripter les infrastructures (infra "as code") qui hébergeront l'application ou le produit.

La pratique du **"DevOps"** consiste à rapprocher ces deux chaînes, l'intégration qui est classiquement du ressort du développeur (dev) et le déploiement qui est de la responsabilité de l'exploitant (ops).

Les chaînes d'intégration et de déploiement s'appuient sur une usine de développement, ou forge, constituée d'un bouquet d'outils assez standards dans lesquels ont trouve généralement

- Dépôt GIT - pour référencer les différentes versions des codes source et des scripts de déploiement associés
- Ordonnanceur de tâches (intégration et déploiement) : jenkins ou hitlab runner
- Dépôt d'artefacts (images docker, OS, paquetages d'application ...) : NEXUS
- outils pour automatiser les tests unitaire
- outils d'analyse de code

Les services du numérique du ministère de l'intérieur (DNUM, ST(SI)², DSIC de la PP et des SGAMI, ...) ont mis en place ces forges d'intégration et ou de déploiement. Cette fiche présente ici le cas de la **forge DNUM [/ DC]**, dont les fonctions recouvrent à la fois intégration et déploiement. Ce n'est pas la seule forge utilisée au ministère mais elle est appelée à jouer un rôle croissant pour les applications et produits dans le périmètre de responsabilité de la DNUM.

[Remarque : la forge DNUM est à l'origine une forge de déploiement continu, connue sous le nom de forge DC de la DSIC. Elle récupère les fonctions d'une forge d'intégration continue, dite forge BCA, qui est en phase de décommissionnement]

La forge DNUM

La forge DNUM est l'offre de service de la DNUM qui propose tout l'outillage nécessaire à l'intégration continue, au déploiement continu, et au suivi des projets sur le cloud :

- gitlab dépôt de code git des scripts de déploiement et autres configurations
- openstack, son API, et des fichiers d'architecture YAML permettant de piloter le cloud PI.
- ansible et python les langages de scripts
- CLI forge DC l'outil en ligne de commande qui assiste l'intégrateur et l'exploitant dans l'automatisation des commandes
- gitlab runner l'ordonnanceur utilisé pour automatiser les actions, à prendre en charge par le projet
- nexus le dépôt de binaires et proxy cache des dépôts applicatifs de l'internet (maven, npm, composer, ...)

Les fonctions d'intégration continue de la forge DNUM

La forge DNUM est ainsi l'outil des développeurs, product owner et chefs de projet. Elle permet de créer des paquetages déployables. Le paquetage déployable à privilégier au sein de la forge DNUM est l'image Docker stockée sur le dépôt Nexus. La reconstruction de cette image Docker et sa validation est effectuée par un pipeline gitlab runner et des scripts Ansible. Cet agencement d'outils est une façon simple de fournir l'ensemble de l'applicatif et de ses dépendances, tout en réduisant l'écart entre développement et production. Outre ce paquetage déployable, les livrables suivant sont aussi obligatoirement présent sur le dépôt Gitlab :

- le code source de l'application
- une version incluse dans l'application (par exemple sur une page)
- une requête runtime de test
- les scripts de build (utilisés pour construire le paquetage)
- les scripts de test introduisant des conditions d'acceptabilité des User Story et qui incluent nécessairement des conditions d'exploitabilité du déploiement

Il est possible de synchroniser la forge DNUM avec des dépôts externes au ministère de l'intérieur de manière autonome au sein de son projet, par exemple dans un pipeline d'intégration continue. Il s'agit d'opération de type "pull" et à sens unique (l'intérieur va chercher ce qu'il y a à l'extérieur). A cet effet, il est **OBLIGATOIRE** de reconstruire les binaires en interne au ministère de l'intérieur à partir des sources, des scripts, et des dépendances. Dans ces configurations hybrides (interne/externe), l'homogénéité des configurations influe beaucoup sur la compatibilité développement/production. La chaîne d'intégration et notamment ses tests automatisés sont les garants de la livraison d'un paquetage déployable opérationnel en production.

Les fonctions de déploiement continu de la forge DNUM

La forge DNUM est aussi l'outil privilégié des "devops", et des exploitants. Son mode de déploiement s'appuie actuellement sur les images gérées par le service Glance d'OpenStack. Toutefois, la forge DC s'ouvre aussi à d'autres méthodes de déploiement, et prend le chemin de la conteneurisation. Outre le déploiement, le CAEX (cahier d'exploitation) est aussi l'un des objectif de livrable de la forge DNUM. La forge DC ne livre pas à proprement parler le CAEX qui référence les commandes permettant de démarrer, arrêter, sauvegarder, restaurer, superviser, déclencher un PRA, ... Mais la forge DC normalise et accompagne l'exploitant en simplifiant progressivement toutes ces procédures.

D'autres outils sont enfin actuellement utilisés au delà du déploiement pour gérer l'exploitation au titre de la sauvegarde et archivage, supervision. Il est obligatoire d'en tenir compte dans les scripts de déploiement pour entrer dans le cadre de l'offre d'exploitation du ministère :

- fournir une sauvegarde régulière en précisant son emplacement, sa fréquence, sa taille et son augmentation, ses règles d'archivage, et le processus de restauration
- fournir une ou plusieurs transaction de test sous la forme d'une URL retournant l'état de fonctionnement de l'application et un message éventuel ciblant le problème relevé

Forge DNUM et équipe produit

La forge DNUM est aussi l'outil des équipes produit, et les prochaines étapes consisteront à outiller les équipes pour les rendre autonomes jusque l'exploitation ! Rien n'empêche ainsi un projet d'expérimenter le commit-2-run via un pipeline gitlab runner de bout en bout !

Impacts sur l'application

Le ministère doit pouvoir conserver la maitrise de ses applications et ses produits, que ceux-ci soient développés en interne ou en participation avec de prestataires externes. Cette maitrise passe par la détention du code source, des licences appropriées, des scripts de compilation et de paquetage, des scripts de construction des infrastructures et de déploiement. En définitive la capacité à reconstruire complètement l'application en cas de perte.

Les forges d'intégration et de déploiement du ministère sont un moyen d'atteindre cet objectif. Celles-ci permettent par ailleurs de mettre à disposition des concepteurs des composants réutilisables.

Règles et recommandations

Propositions de règles et recommandation non encore validées :

- Le ministère doit pouvoir conserver la maitrise de ses applications et ses produits. En conséquence il doit en détenir les codes sources ainsi que tous les scripts permettant leur reconstruction. Cette règle s'applique également à des produits non hébergés sur un site du ministère.

Les règles et recommandations qui suivent émanent du CCT V2.8 et sont insuffisantes dans le nouveau contexte décrit dans la présente fiche.

Ref	Startup	Intitulé
1389	RG	Il est OBLIGATOIRE de définir et de formaliser un suivi rigoureux des dérogations, des bogues, des anomalies et des vulnérabilités tout au long du développement. Ce suivi, adossé à la matrice de couverture des risques, permettra d'évaluer le niveau de sécurité de l'application à la livraison, et de hiérarchiser les corrections à apporter. Les outils de suivi de développement utilisés doivent intégrer les aspects bogues, anomalies et vulnérabilités afin de suivre l'état de sécurité de l'application tout au long de son cycle de vie, de la conception au retrait de service. Ils doivent intégrer les critères de causes et de conséquences des bogues de sécurité. Les critères de causes et de conséquences des bogues de sécurité doivent s'inspirer des sources ouvertes (OWASP, CWE, etc.). Ces éléments d'information viendront enrichir le dossier de vulnérabilités résiduelles du dossier de sécurité et d'homologation.
1399	RG	Il est OBLIGATOIRE de réaliser et maintenir à jour un inventaire des codes externes (bibliothèques, framework, API, etc.) utilisés par l'application.
1418	RG	Il est OBLIGATOIRE de disposer de conventions et de règles de codage adaptées au langage utilisé et de les appliquer dans le cadre du développement. Ces règles et conventions contribuent à la lisibilité et à la qualité du développement de l'application. Elles doivent être jointes à la documentation technique du projet de développement et constituent un référentiel de vérification lors des revues de code. Elles sont idéalement vérifiables à l'aide d'un outil adapté.
1423	RG	Il est OBLIGATOIRE de mettre en oeuvre les fonctions de gestion (création, allocation, libération, etc.) et de manipulation (lecture, écriture, etc.) des ressources informatiques (mémoire, fichier, etc.) au plus près de leur utilisation effective.
1429	RG	Il est OBLIGATOIRE de réaliser des revues des codes sources pendant la phase d'implémentation et de programmation.
1430	RG	Il est OBLIGATOIRE de décrire et de formaliser les tests unitaires pour chaque unité de code lors de la phase d'implémentation et de programmation.
1431	RG	Il est OBLIGATOIRE de mettre en oeuvre un processus d'intégration des modules unitaires de l'application. Le processus d'intégration permet de vérifier, lors de l'assemblage des modules unitaires de l'application : - l'absence de dysfonctionnements des fonctionnalités et fonctions métier ; - l'absence de dysfonctionnements lors des interactions avec les services externes ; - l'absence de dysfonctionnements avec l'environnement d'accueil.
1432	RG	Il est OBLIGATOIRE de gérer les anomalies détectées lors du processus d'intégration via les outils de suivi des bogues et des vulnérabilités utilisés pour l'application.
1104	RG	La gestion des anomalies (bug tracking) doit s'appuyer sur les outils recommandés par le CCT.
1106	RG	La documentation propre à chaque base de données centrale doit être constituée au minimum d'un dictionnaire de données, d'un ensemble de règles de gestion, et d'un modèle conceptuel de données (ou d'un diagramme de classe). Cette documentation, actualisée en fonction d'éventuelles mises à jour, doit être consultable.
1229	RG	Toute application développée à l'initiative et sous la responsabilité des échelons décentralisés doit: - ne répondre qu'à un besoin local dans le domaine applicatif ; - être réalisée avec les logiciels mentionnés dans le CCT ; - être maintenue localement ; - être en conformité avec la loi informatique et libertés et notamment faire l'objet des déclarations CNIL adaptées en fonction des traitements automatiques effectués ; - faire l'objet d'une utilisation limitée à un réseau local ; - faire l'objet d'une étude de sécurité pour elle-même et vis à vis du système d'information et de

		communication du ministère.
1428	rc	Il est RECOMMANDÉ d'effectuer des analyses statiques des codes sources pendant la phase d'implémentation et de programmation.
1107	rc	Le cadre de cohérence technique RECOMMANDE de respecter : - la démarche générale pour le développement des logiciels, - les règles de nommage et de codage, - les règles pour les journaux et les traces applicatives, - les règles pour la gestion des exceptions, - les règles pour la documentation du code source.
1108	rc	Le langage UML doit être privilégié pour la modélisation.
1391	RG	Il est OBLIGATOIRE d'utiliser un outil de gestion de version pour gérer et stocker les fichiers (codes sources, scripts, etc.) des applications.
1246	RG	Le code source d'une application ne doit pas être adhérent à un EDI.
1250	RG	L'usage de fichiers dits plats est déconseillé au profit de données structurées (JSON, XML...). L'utilisation de format autre que le XML doit être explicitement justifiée.
1265	RG	Les codes sources et la documentation des applications doivent être versionnés et centralisés à l'aide d'un outil de gestion de configuration référencé au CCT.
1279	RG	Les applications PHP ou JAVA doivent utiliser un framework de développement respectant au possible le modèle MVC et référencé au CCT.
1345	RG	Les jeux de tests permettant d'effectuer les vérifications de bon fonctionnement et de non régression de l'application doivent être fournis conformément à la procédure projet en vigueur en vue d'assurer la qualification des piles logicielles.

Informations utiles

Contacts

- Contact pour ouverture de compte sur la forge DNUM : forge-dsic@interieur.gouv.fr
- Autre possibilité de contact : Rocket.chat

Offres de service

- Ateliers pratiques sur les outils utilisés par les forges
- Forge DNUM - http://gitlab.forge-dc.cloudmi.minint.fr/

Ressources

- Forge BCA (bientôt décommissionnée) https://forge.dsic.minint.fr
- Forge DNUM http://gitlab.forge-dc.cloudmi.minint.fr

Zone d'entraide

- Rocket.chat : https://forge.dsic.minint.fr/chat/
- TCHAP - https://www.tchap.gouv.fr/ - Salon Forge-DC

Pilier hébergement et exploitation

Mise en place d'un hébergement

Contexte

Grandes tendances

Le métier de l'hébergement est en pleine mutation sous l'effet de plusieurs tendances :

- Des **tendances technologiques**
  - de la virtualisation au cloud,
  - de la machine virtuelle au conteneur
  - avec comme dénominateur commun le franchissement d'un pas supplémentaire dans l'automatisation : intégration continue, déploiement continu des applications comme des infrastructures.
- Des **tendances métier**
  - interpénétration du métier des "dev" (développeurs) et de celui des "ops" (exploitants hébergeurs) - le DevOps,
  - interpénétration des métiers et des développeurs avec l'expansion des méthodes agiles.
- Des **tendances organisationnelles au niveau de l'état**,
  - qui structure de façon croissante la production informatique sur un petit nombre de sites,
  - et qui travaille activement à l'intégration et à l'ouverture de tous les SI jusqu'ici gérés en silos.

Doctrine de l'Etat

Ces tendances se sont matérialisées par une **"doctrine d'utilisation de l'informatique en nuage par l'état"** publiée sur LEGIFRANCE. Le tableau qui suit synthétise les trois cercles de solution d'hébergement étatique, cloud interne pour le 1er cercle, cloud dédié pour le 2nd cercle et cloud externe pour le 3ème cercle, avec leur conditions d'usage.

Cercle de solution	Condition d'usage	Nature du service	Disponibilité de offre	Catalogue
1er cercle Cloud interne	Données et traitement sensibles Besoins régaliens	Service de type IaaS et PaaS, sur une base OpenStack, infrastructure interne (CloudMI et MINEFI/DGFIP). Conformité au référentiel SecNumCloud Essentiel de l'ANSSI	CloudMI redondé sur deux sites</br>depuis 1er semestre 2020	Catalogue de service ministériel et interministériel Portail PI Portail PIMS à venir
2nd cercle Cloud dédié	Données et traitement de sensibilité moindre mais nécessitant un certain niveau de pérennité	Cloud industriel, infrastructures dédiées, migration simple avec le cercle 1. Conformité au référentiel SecNumCloud Essentiel de l'ANSSI	Non planifié (non prioritaire)	
3ème cercle Cloud externe	Données et traitement peu sensibles	Service de type SaaS, sur cloud public	Marché Cloud Cercle 3 notifié depuis la fin du 1er semestre 2020.	**Catalogue UGAP** Une convention entre l'UGAP et la DNUM est signé depuis début novembre 2020 pour le périmètre du ministère de l'Intérieur.

Les technologies employées sur le premier et le deuxième cercle devront être les mêmes afin de permettre des portages entre les plateformes. Le troisième cercle se différentie des deux premiers d'un point de vue technologique, rendant les portages plus complexes. Ceci ne signifie aucunement que les échanges soient interdits entre clouds de cercle différent.

Impact sur les applications

La doctrine d'utilisation de l'informatique en nuage par l'Etat a des impacts importants sur l'hébergement d'une application. Le positionnement d'une application sur un cloud de 1er 2nd ou 3ème cercle dépend avant tout du niveau de sensibilité des données qu'il manipule. La décision peut aussi varier en fonction d'éléments contextuels comme des accords commerciaux ou des tensions diplomatiques.

Mise en place d'un hébergement

Sachant que les conventions de service de ministère à ministère sont appelées à se multiplier, cette fiche CCT de l'hébergement prend le parti de d'aligner l'offre de service d'hébergement ministérielle à l'offre de service inter-ministérielle telle qu'elle est décrite dans le schéma directeur des infrastructures d'hébergement inter-ministériel. Celui-ci a été réalisé sous l'égide de la DINSIC / DINUM avec les DSI ministérielles et une participation notable du MI. L'un des documents les plus structurant de ce schéma directeur en est son catalogue de service. Ce catalogue décrit les types de prestations assurées dans le cadre d'une convention entre l'offreur de service et sont bénéficiaire. Cette description couvre les domaines suivants :

- la description du service
- le périmètre de la prestation
- la responsabilité des acteurs
- les modalités de mise en œuvre et de gestion des services considérés
- les engagements sur les niveaux de qualité de service.

Ce document de référence, reconnu au niveau inter-ministériel (CINUM), décrit des engagements de service standard, susceptibles d'être complétés par chaque offreur. La présente fiche, comme le catalogue dont elle s'inspire, est structurée selon une vue « bénéficiaire ». Elle adresse plusieurs types de bénéficiaires : des maîtrises d'oeuvre, consommatrice de services d'infrastructure (offre IaaS d'un cloud par exemple), des responsables de projets SI, et finalement des utilisateurs finaux (offres de type SaaS).

Remarque : cet hébergement peut ne concerner qu'une partie de l'application concernée.

Service offert par les hébergeurs

Les services d'hébergement et d'exploitation offerts au sein du ministère sont structurés par le catalogue sus-nommé qui en établit le cadre, et complétés par les services propres à chaque hébergeur. Ces offres s'appuient sur des infrastructures techniques dont l'architecture est exposée par chaque offreur de service.

Qui sont les hébergeurs du ministère

Le ministère possède aujourd'hui deux instances d'hébergement centrales ainsi que des instances d'hébergement zonales. Les instances d'hébergement centrales :

- Celui du centre d'hebergement (CH) de la DNUM, qui héberge les plateformes ISOCELE et CLOUD PI et opère trois sites :
  - le **SIR (Service informatique de Rosny)**, qui opère les salles B021 et B015 qui a une vocation interministérielle,
  - le **SIL (Service informatique de Lognes)**
  - et le **SIVM (Service informatique du Val Maubouée)**.
- Celui du STIG, avec les centres de Rosny et Nogent.
  Le STIG a aujourd'hui une forte orientation sécurité intérieure.

Les instances d'hébergement zonales : les SGAMI, dont la préfecture de police de Paris et le SGAMI EST.

Outre leur centre d'hébergement zonal, Les SGAMI peuvent être Centre de Compétence national (CCN) sur des compétences qui leur sont spécifiques. Le chapitre des informations utiles liste les fonctions d'hébergement et d'exploitation des SGAMI et de leurs CCN.

Cycle de vie d'un hébergement et convention

La mise en place d'un hébergement est matérialisée par une demande d'hébergement, puis par l'élaboration et la signature d'une convention avec un hébergeur. Cf liens en fin de fiche. Ces actions s'intègrent dans un cycle de vie de l'hébergement

1. le bénéficiaire évalue ses besoins fonctionnels, les services nécessaires
2. le bénéficiaire fait une demande d'hébergement (cf formulaire en fin de fiche)
3. mise au point de la convention et de ses annexes et signature de la convention (cf conventions type en fin de fiche)
4. mise en place de l'hébergement et mise en production
5. fonctionnement courant
6. phase de réversibilité ou de décommissionnement

Processus de consommation d'une offre SaaS (à venir)

A terme, les environnements de cloud pourront offrir une « boutique » d'offre SaaS (Software as a Service). Permettant par exemple de mettre rapidement en place un wiki, un site web (cms), une plateforme de réalisation de questionnaire ...etc. Le processus de demande et de conventionnement tel qu'il est décrit au dessus ne convient alors pas. Ce type de consommation nécessite :

- un conventionnement accéléré, via un système de conditions générales d'utilisation (CGU)
- un système de facturation simple et rapide

Règles et recommandations

La section règles et recommandations va être prochainement mise à jour et simplifiée.

Recommandation

L'hébergement et l'exploitabilité d'une application sont à prendre en compte dès la phase amont du projet. En effet, ces deux problématiques conditionnent fortement la conception même de l'application. En d'autres termes, le centre d'hébergement doit être impliqué en amont du projet pour pouvoir assurer l'hébergement dans de bonnes conditions.

Règle

Les DBA des hébergeurs ne sont pas habilités à répondre à des demandes d'extraction de données. Il appartient au concepteur de l'application de prévoir ses propres mécanismes d'extraction de données en conformité avec la loi ou les règlements européens.

Règle

Les demandes d'hébergement d'application nationale sont traitées par le BPAH (DNUM/SDAIT) . Les demandes sont à adresser au BRM (à l'adresse dnum-brm-contacts@interieur.gouv.fr)

Règle

Conformément aux règles stratégiques élaborées lors de la démarche Action Publique 2022, les hébergements doivent être pensés « Cloud First ».

Ref	Statut	Intitulé
1347	RG	La journalisation doit être prévue dès la conception de l'application en indiquant notamment les personnes autorisées à y accéder, le mode d'administration et la durée de conservation.
1000	RG	Lorsque l'application comporte des chemins différents entre deux composants, le fichier de paramètres doit systématiquement contenir les éléments nécessaires à l'établissement du chemin principal, mais également à l'établissement d'un chemin de secours.
1008	RG	Une application utilisant un socle technique donné doit être développée dans un souci de compatibilité avec les autres applications utilisant ce même socle.
1009	RG	Les chefs de projets des services techniques centraux doivent respecter les dispositions relatives à la gestion de la plate-forme de production centralisée décrites en annexe du CCT.
1012	RG	La sauvegarde des données applicatives s'appuie sur des solutions mutualisées mises en œuvre par le ministère.

1014	RG	Les outils d'ordonnancement ne doivent pas être utilisés à des fins d'orchestration de processus métier.
1019	RG	Les journaux doivent respecter le format défini par le ministère conformément aux « Normes d'exploitation » dont les éléments nécessaires seront fournis aux titulaires.
1020	RG	"L'application doit disposer d'un mode trace, 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). Ce mode trace doit ainsi permettre : - 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) - de fournir le contenu des données liées aux opérations précédentes - d'indiquer précisément la position de l'opération dans le programme - de détailler précisément toutes les erreurs, ou problèmes, même internes - de fournir un niveau d'importance aux fonctions tracées, et aux erreurs - d'être activé, et de ne garder que le niveau d'information choisi (niveau du point précédent) - d'archiver les informations sur une période assez longue (compte tenu du niveau choisi), de l'ordre de plusieurs jours à plusieurs semaines - d'archiver ces informations et de les purger, ceci de manière automatique."
1021	RG	Le mode trace ne doit pas être dépendant d'un outil de développement particulier. Il doit être intégré dans le produit final, comme une option de fonctionnement.
1022	RG	Le mode trace doit pouvoir être activé/supprimé dynamiquement. Le niveau de détail du mode trace doit pouvoir être spécifié/modifié dynamiquement.
1023	RG	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.
1051	RG	Les journaux doivent être stockés sur les disques locaux des serveurs. L'application doit permettre de les dupliquer vers un système externe.
1052	RG	La journalisation technique repose aujourd'hui sur : l'association NAGIOS/application PROLOG ou SYSLOG. Le cahier des charges techniques précisera,en fonction du centre d'hébergement retenu, les spécifications .
1053	RG	Les environnements virtualisés doivent se faire sur les produits référencés au CCT.
1054	RG	Les disques d'un serveur connectés en architecture DAS ont pour vocation de n'accueillir que le système d'exploitation et les logiciels de base.
1349	RG	Toute application (ou sous-application) doit: - être identifiée par un trigramme; - correspondre à une arborescence normalisée par environnement (production, développement, ...) sur un espace de stockage dédié; - l'espace de stockage peut comprendre un à plusieurs groupes de volumes (ou disques) et systèmes de fichiers.
1007	RG	Les informations/traitements sensibles doivent être hébergés sur des serveurs physiquement distincts des serveurs hébergeant des informations/traitements non sensibles.
1015	RG	Les opérations de télémaintenance par un prestataire externe, quand elles sont autorisées doivent systématiquement être réalisées avec le système SPAN
1002	rc	La répartition des flux est assurée par les équipements réseaux en frontalité de la ferme des serveurs de présentation.
1003	rc	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.
1004	rc	Pour le 'tiers' serveur base de données, les solutions de haute disponibilité unifiées, standard, et industrielles à disposition dans les centres de service sont privilégiées. A défaut les solutions fournies par les moteurs SGBD seront utilisées.
1010	rc	Les bases de données et les fichiers, doivent pouvoir (si le système de gestion de données le permet), être sauvegardés dynamiquement (sauvegardes dites bases «ouvertes»). L'application doit offrir la possibilité de verrouiller les mises à jour, tout en maintenant les consultations actives.
1013	rc	"La sauvegarde des bases des données - soit sensibles et volumineuses - soit accessibles 24h/24

1013	rc	s'effectue à chaud en utilisant l'une des technologies suivantes : - les snapshots des solutions de stockage disque - l'agent spécifique du logiciel de sauvegarde lorsqu'il est disponible."
1018	rc	Dans le cas de journaux applicatifs répartis, il faut garantir le respect de la chronologie des opérations (exemples : horodatage, numéro de séquence, ...).
1099	RG	Toutes les actions contribuant au lancement ou à l'arrêt de l'application, doivent pouvoir être déclenchées par une commande unique et s'enchaîner ensuite automatiquement.
1220	RG	L'application ne doit ni imposer, ni embarquer de solution d'ordonnancement liées aux travaux d'exploitation et d'administration.
1289	RG	L'application doit permettre les points de synchronisation assurant une cohérence fonctionnelle pour les sauvegardes de contextes entiers.
1297	RG	Tous les paramètres de l'application doivent être regroupés dans un fichier.
1299	RG	L'application doit fournir une commande permettant d'interdire toute nouvelle connexion utilisateur, sans perturber les connexions en cours.
1300	RG	L'application doit fournir une commande permettant l'arrêt de toutes les connexions utilisateur en cours.
1302	RG	"Toutes les actions d'exploitation et de pilotage de l'application doivent pouvoir être déclenchées : - manuellement en mode «expert» (mode commande) ou en mode «novice» (interface graphique), - et automatiquement par un automate (soumission de scripts sans aucune intervention humaine)."
1303	RG	Le fonctionnement normal et quotidien d'une application ne doit pas solliciter une intervention directe d'un opérateur.
1304	RG	Tous les logs des applications doivent être tracés dans un fichier au format ASCII.
1319	RG	L'application ne doit pas imposer des composants logiciels qui seraient incompatibles avec la solution de sauvegarde mutualisée mise en oeuvre par le service d'exploitation.
1301	rc	L'application doit fournir une commande permettant de passer, à tout moment, en mode «consultation».
1035	RG	Dans les centres d'exploitation, les données ne sont pas stockées sur les serveurs mais sur des systèmes partagés (exemple SAN/NAS).

Informations utiles

Contacts utiles

Demandes d'hébergement centraux : dnum-brm-contacts@interieur.gouv.fr

Hébergement en SGAMI : la demande doit être qualifiée par la DNUM, puis possiblement orientée vers le SGAMI EST.

Offres de service

Demande d'hébergement interne

Les demandes d'hébergement central sont instruites par la DNUM/SDAIT/BPAH qui les traite dans un délai de 15 jours. Elles sont émises par le RSIMM de la direction concernée, ou par le chef de projet.

- Le formulaire de demande d'hébergement est téléchargeable : Demande d'hébergement
- Adresse fonctionnelle : dnum-brm-contacts@interieur.gouv.fr

Catalogue des offres de service d'hébergement et d'exploitation

Catalogue de service et modèle de convention de service de la DINSIC / DINUM et du GT interministériel hébergement : voir zone ressources

Offre de service d'hébergement de la DSIC : Catalogue en ligne

Offres SaaS avec mise en place accélérée (dans le futur)

- Adresse de la boutique
- Conditions générales d'utilisation - A venir
- Méthode de facturation - A venir

Ressources

Schéma Directeur des infrastructures d'hébergement

- Source - DINSIC / DINUM et GT hébergement interministériel
- Périmètre : les services d'hébergement interministériels
- Catalogue des services d'hébergement
- Modèle de convention de services
- Modèle d'annexe technique
- Modèle d'annexe financière
- Modèle de plan d'assurance qualité - Source Laurent Le-Blay

Les deux premiers documents, à savoir le catalogue et le modèle de convention de service, maintenus et portés par la DINSIC / DINUM, peuvent être utilisés sur un périmètre intra ministériel

Dossiers d'architecture des hébergeurs centraux :

- Dossier d'architecture technique de la DNUM - A venir
- Dossier d'architecture technique du STIG, version 3.3 datée de décembre 2019 : Infrastructure de production mutualisée et secourue (IPMS).
- Dossier d'architecture technique du STIG, résumé de la politique V1 : IPMS - Résumé de la politique

Zone d'entraide

A fournir

Service de supervision

Contexte

La présente fiche est en cours d'écriture à la date de publication du CCT V3.0.

Impact sur les applications

Règles et recommandations

Recommandation

Règle

Informations utiles

>

> **Contacts utiles**
>
> **Offres de service**
>
> **Ressources**
>
> **Zone d'entraide**
>
> A fournir

Pilier services transverses

Le pilier des services transverses offre un choix synthétique des offres exposées par les différents acteurs SIC du ministère, que ce soit les services centraux ou les services déconcentrés que sont les SGAMI. Par ailleurs il faut signaler le nombre croissant d'offres qui débordent du cadre strictement ministériel.

Services transverses

Contexte

Avertissement : la présente fiche est embryonnaire. Elle est appelée à être complétée dans les versions ultérieures du CCT.

Il est nécessaire de rappeler ici que la consultation des offres de services existantes est nécessaire dans le cadre de la conception de nouveaux produits ou de nouvelles applications. La mise en oeuvre des offres de service existantes, bien sûr sous réserve de leur adéquation au besoin, est un facteur important de cohérence du SI de l'État, de non redondance, et d'économie des deniers publics.

Les DSI centrales proposent toutes des offres de service nationales. Certaines d'entre elles ont même un périmètre élargi au SI de l'État, comme par exemple le service d'horodatage, ou certains services de supervision. Ces offres de service sont présentées dans les catalogues de services des DSI et le CCT n'a pas vocation à se substituer à ces catalogues de service (cf chapitre ressources ci-dessous).

Les SGAMI peuvent eux aussi déployer des offres de services nationales. Ils le font sous le pilotage de l'une des deux DSI centrales (DSIC ou ST(SI)²), avec un statut reconnu de Centre de Compétences Nationales (CCN).

Offres de service

La liste qui suit met le focus sur quelques offres de services structurantes et ne se substitue pas aux catalogues de services, plus exhaustifs, et présentés par les différents acteurs SIC.

- DSIC / SDI - Service de signature électronique
- DSIC / SDI - Service d'horodatage (périmètre interministériel)
- DSIC / SDA / SGAMI Sud-Ouest - Gestion électronique de courrier (GEC) basée sur Maarch et déployée dans les préfectures ou les directions centrales
- DSIC / SDA / SGAMI Sud-Ouest - Production de démarches en ligne / Saisine par voie électronique (SVE)
- DINSIC - Production de démarches en ligne / Démarches simplifiées
- DSIC / SDA / SGAMI Sud-Ouest - Service d'archivage intermédiaire (avec Maarch RM)
- DSIC / SDA - Service d'analyse de performance applicative, basé sur Dynatrace
- DICOM - Web Analytics
- ANTS - 2D-DOC - Solution de sécurisation de document à l'aide d'un code barre 2D
- SGAMI Est : référentiels cartographiques

Ressources

- Catalogue de service de la DSIC
- Catalogue de service du SGAMI Ouest
- Directives Nationales Opérationnelles ou DNO SIC de 2019

Liste des Centres de Compétences Nationales (CCN) :

CCN	Sous direction porteuse	SGAMI chef de file	Commentaire
Référent outil de supervision LAN Télémétrobox	DSIC/SDI	SGAMI Ouest	Lettre de mission du 29 juin 2016
Outils CMS - Content Management Systems (logiciel de gestion de contenus destinés à la création de sites Web Internet ou Intranet	DSIC/SDA	SGAMI Ouest	Lettre de mission du 26 juillet 2017
Virtualisation en environnement WINDOWS	DSIC/SDI	SGAMI Ouest	Lettre de mission du 7 mai 2018
Système d'information INPT (GOTI)	ST(SI)²/SDR²	SGAMI Est	Lettre de mission du 16 février 2016
Cartographie : référentiel grande échelle (RGE)	DSIC/SDA	SGAMI Est	Lettre de mission du 1er juillet 2016
Expertise outillage Gestion de parc (OCS-GLPI)	DSIC/SDI	SGAMI Est	Lettre de mission du 3 octobre 2016
Cellule ingénierie et servitudes (CCNIS)	ST(SI)²/SDR²	SGAMI Sud	Note du 14 janvier 2016
Expertise Réseaux Air/Sol – réseaux radio	ST(SI)²/SDR²	SGAMI Sud	Lettre de mission du 9 janvier
Système d'information de sûreté de sites	DSIC/SDSU	SGAMI Nord	Lettre de mission du 19 décembre 2016
Système d'information de sûreté de sites	DSIC/SDSU	SGAMI Nord	Lettre de mission du 19 décembre 2016
Centre d'exploitation et de supervision de l'INPT (CESI)	ST(SI)²/SDR²	SGAMI Sud-Est	Note du 19 février 2016
Renvoi d'images / flux vidéo	ST(SI)²/SDAC	SGAMI Sud-Est	Lettre de mission du 27 avril 2016
Expertise Bureau distant (terminaux légers)	DSIC/SDI	SGAMI Sud-Est	Lettre de mission du 27 juin 2016
Offre de gestion électronique de courrier Maarch	DSIC/SDA	SGAMI Sud-Ouest	Lettre de mission du 13 juin 2016
Maarch	DSIC/SDA	SGAMI Sud-Ouest	A finaliser à date de parution des DNO SIC 2019 Présentation du CCN et des offres Maarch
CESAR	ST(SI)²/SDR²	PP/SDSICIF	Formalisé depuis 2014. À actualiser dans le cadre du secours mutuel avec le CESI. En cours de finalisation par la PP/SDSICIF à date de parution des DNO 2019
Expertise Moyens de transmissions	ST(SI)²	PP/SDSICIF	A finaliser par la PP/SDSICIF à date de parution des DNO 2019