

Cadre de cohérence technique des systèmes d'information et de communication du ministère des armées

CCT 2023-2024 (Version 3.5 Edition 2)

Version non protégée diffusable hors ministère de façon réfléchie

[CCT-MinArm 2023-2024-3.5-Edition 2-30/06/2024]

Rédaction	Contributions : DGNUM, CASID, DIRISI, DGA, EMA, SGA Coordination : sous-comité de cohérence des architectures [SC ² A]	AND, DIRISI, DGNUM, CASID, EMA, SGA
Commentaires Contributions	Experts du ministère	DGA (AND, DT-IP/MI, S2NA), DIRISI (EMO, SDCS, POENT, PODEV-CDAD, POHEB, SERVPROJ), DGNUM (SDTN, SDSN, SDGN), CASID, EMA/SNA, COMCYBER, SGA (DTPM, MAP, SMSIF-RH), DPID, DSI Domaine
Validation	Sous-comité de cohérence des architectures	SC ² A
Validation	Olivier GANIS, sous-directeur de la transformation numérique DGNUM	DGNUM /SDTN
Approbation	Vincent TEJEDOR, directeur général DGNUM	DGNUM

SOMMAIRE

1 GENERALITES	12
1.1 Objet du document	12
1.2 Périmètre	12
1.3 Domaine d'application – Acteurs concernés	13
1.4 Gestion et gouvernance du CCT	14
1.5 Prise en compte dans le cadre des cahiers des charges	14
1.6 Organisation du document	15
1.6.1 Organisation générale du document	15
1.6.2 Pile logicielle et environnements d'exécution	15
1.7 Codification des références du CCT	15
1.7.1 Références documentaires – Typologie de documents	16
1.7.2 Règles et recommandations additionnelles	16
1.7.3 Normes et standards	17
1.7.4 Produits et solutions	17
1.8 Critères d'éligibilité des produits et solutions	18
1.8.1 Contraintes à respecter et critères d'appréciation	18
1.8.2 Évolutions	18
1.8.3 Le CCT et l'innovation	19
1.9 Conformité au CCT	19
1.9.1 Validation des architectures des SI	19
1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT	19
2 CADRES REFERENTIELS GENERAUX	21
2.1 Les référentiels internationaux	21
2.1.1 OTAN	21
2.1.1.1 Référentiel NISP	21
2.1.1.2 Démarche FMN (Federated Mission Networking)	21
2.1.2 Européen	23
2.2 Le cadre interministériel	24
2.2.1 La stratégie du SI de l'État – Doctrine cloud	24
2.2.2 Politique de la donnée - Logiciels Libres – ouverture des codes	24
2.2.3 Les référentiels interministériels	26
2.2.3.1 Référentiels généraux (RGI, RGS, RGAA, R2GA, RGESN)	26
2.2.3.2 Communication gouvernementale - Charte Internet de l'État – Charte graphique	28
2.2.4 Les outils et l'offre de service au niveau interministériel	29
2.2.4.1 L'offre de services communs	29
2.2.4.2 Le socle de logiciels libres SILL – Marché de support LL	29
2.2.4.3 Les données ouvertes	29
2.2.4.4 Conception de site Internet	30
2.3 Le cadre ministériel	30
2.3.1 Politique SIC ambition numérique	30
2.3.2 Architecture générale, politique logicielle	30
2.3.3 Socle numérique	31

2.3.4	SIC opérationnels – FrOpS	31
2.3.4.1	Politique et concepts d'emploi	31
2.3.4.2	COTS OTAN / SIC Multinationaux	31
2.3.5	Sécurité	32
2.3.6	Gouvernance	32
2.3.6.1	Outils de gouvernance	35
2.3.6.1.1	Gestion du patrimoine	35
2.3.6.1.2	Gestion du patrimoine – Données	36
2.3.7	Relation client – Offre de service - DIADEME	36
3	SERVICES COMMUNS	37
3.1	Services à l'utilisateur	38
3.1.1	Environnement de travail	38
3.1.1.1	Poste de travail - CCB [SU-PC]	38
3.1.1.2	Critères d'éligibilité d'un package	40
3.1.1.3	Recours à la machine virtuelle Java sur le terminal utilisateur	41
3.1.1.4	Postes de travail autonomes ou en mode déconnecté	41
3.1.1.5	Socle technique logiciel du poste de travail	42
3.1.1.6	Offre logicielle du poste de travail [SU-STORE]	43
3.1.1.7	Messagerie	45
3.1.1.7.1	Messagerie non officielle [SU-MEL]	45
3.1.1.7.2	Messagerie officielle [SU-MOF]	46
3.1.1.8	Agenda, contacts [SU-AGE]	46
3.1.1.9	Portail personnalisable [SU-GPE]	47
3.1.2	Collaboratif	47
3.1.2.1	Communication instantanée	47
3.1.2.1.1	Dialogue en ligne, gestion de présence [SU-PRE], messagerie instantanée [SU-MIN]	47
3.1.2.1.2	Réunion virtuelle [SU-REV], audioconférence [SU-AUD], visioconférence [SU-VIS], vidéoconférence [SU-VID]	48
3.1.2.1.3	Solutions logicielles client	48
3.1.2.2	Espace de travail collaboratif [SU-EDT]	49
3.1.2.3	Wiki [SU-WKI]	49
3.1.2.4	Tableau blanc - Rédaction synchrone	50
3.1.2.5	Forum [SU-FOR]	50
3.1.2.6	Listes de diffusion	50
3.1.2.7	Réseau social [SU-RSE]	50
3.1.3	Vie courante	51
3.1.3.1	Portail intranet [SU_PIN]	51
3.1.3.2	Annuaire pages blanches, pages jaunes [SU-PJB]	51
3.1.3.3	Impression – édition multifonction [SU-IMP]	52
3.1.3.4	Moteur de recherche [SU-RMR]	52
3.1.3.5	Enquête et sondage [SU-ENQ]	53
3.1.3.6	Réservation de salles [SU-RDS]	53
3.1.4	Gestion des données	54
3.1.4.1	Stockage des données [SU-REP]	54
3.1.4.2	Transfert de données volumineuses [SU-TFV]	54
3.1.5	Sécurité [SU-SSO, SU-CHI, SU-SIG]	55
3.1.6	Mobilité [SU-AN, SU-ITN]	55
3.1.7	Accès réseaux extérieurs	57
3.1.7.1	Internet sur le poste de travail [SU-WEB]	57
3.1.7.2	Accès aux réseaux interministériels [SU-RMI] et autres réseaux extérieurs [SU-REX]	58
3.1.8	Téléphonie	59
3.1.9	E-formation	59
3.1.10	Services divers	59

3.1.10.1 Traduction [SU-TRL]	59
3.1.10.2 Traitement de la parole	60
3.2 Socle des applications	60
3.2.1 Généralités	60
3.2.1.1 Concepts fondamentaux	60
3.2.1.2 Démarche et principes liés aux solutions en nuage (cloud)	61
3.2.1.3 Transformation numérique	65
3.2.1.3.1 Agilité	65
3.2.1.3.2 Stratégie API – corpus documentaire API	65
3.2.1.4 Hébergement mutualisé	66
3.2.2 Hébergement d'applications	67
3.2.2.1 Services Web / Serveur de présentation [HSW]	67
3.2.2.2 Serveurs d'application et environnements d'exécution	68
3.2.2.2.1 Environnement d'exécution Java	68
3.2.2.2.2 Environnement d'exécution PHP	71
3.2.2.2.3 Environnement d'exécution .Net	72
3.2.2.2.4 Environnement d'exécution JavaScript	72
3.2.2.2.5 Environnement d'exécution Python	72
3.2.2.2.6 Environnement d'exécution R	73
3.2.2.2.7 Environnement d'exécution Ruby	73
3.2.2.2.8 Environnement propriétaire	73
3.2.3 Portail des applications métiers	74
3.2.3.1 Moteur de workflow [WFL]	74
3.2.3.2 Process robotisés (RPA)	74
3.2.3.3 Chatbot	75
3.2.3.4 Moteur de règles	75
3.2.3.5 Services de gestion des rôles et profils	75
3.2.3.6 Services de gestion des règles d'accès	75
3.2.3.7 Portail des applications mobiles sur Internet – Milistore	75
3.2.4 Échanges entre applications	76
3.2.4.1 Généralités	76
3.2.4.1.1 Cas des échanges Intradef avec l'extérieur	77
3.2.4.2 Échanges inter-systèmes	77
3.2.4.3 Architectures SOA - Orchestration et logique métier	78
3.2.4.4 Architectures API – REST – PEM	79
3.2.4.4.1 Architecture API REST - PEM	79
3.2.4.4.2 « Route API »	80
3.2.4.5 Extraction et transformation (ETL) [TRF]	83
3.2.4.6 Gestion de processus et de règles métiers	83
3.2.4.7 Annuaire des applications et services [ANA]	84
3.2.5 Données et contenu	84
3.2.5.1 Formats de données	84
3.2.5.1.1 Encodage des caractères	84
3.2.5.1.2 Formats audio et vidéo	85
3.2.5.1.3 Outils de conversion de format	85
3.2.5.2 Gestion des accès aux données	85
3.2.5.3 Gestionnaire des données [HBD]	86
3.2.5.3.1 Les SGBDR	86
3.2.5.3.2 Les SGBD sous la dénomination NoSQL	88
3.2.5.3.3 Les SGBD en mémoire	90
3.2.5.3.4 Les agents de messages	90
3.2.5.4 Gestion des données de référence (MDM) – management de la qualité des données (DQM)	91
3.2.5.5 Gestion électronique de documents [GED]	93
3.2.5.6 Masquage / Anonymisation / Pseudonymisation des données	93

3.2.6	Informatique « décisionnelle », Big Data, analyse prédictive	93
3.2.6.1	Introduction et orientations ministérielles	93
3.2.7	Datavisualisation, BI Corporate ou BI self-service	94
3.2.7.1	Données massives ou « Big Data »	96
3.2.7.1.1	Plateformes exploratoires et d'innovation DATA360 – POCEAD – ARTEMIS-IA	96
3.2.7.1.2	Plateforme POCEAD – ouverture des données	98
3.2.7.1.3	Plateforme ARTEMIS.IA	99
3.2.7.2	Analyse prédictive et statistique	99
3.2.8	Cadres particuliers	100
3.2.8.1	ERP	100
3.2.8.2	Moteur de génération de rapports	101
3.2.8.3	Archivage	101
3.2.8.3.1	Documents de portée générale OTAN	101
3.2.8.3.2	Documents de portée générale nationale	102
3.2.8.3.3	Documents de portée générale Ministérielle	102
3.2.8.3.4	Documents techniques MinArm	103
3.2.8.3.5	Solution ministérielle Archipel	103
3.2.8.4	Informations géographiques, hydrographiques, océanographiques et météorologiques (GHOM)	103
3.2.8.4.1	GEODE 4D	104
3.2.8.4.2	Moteur cartographique OSM sur Intradef	104
3.2.9	Démarche simplifiée (DS) – Dossier numérique de l'agent (DNA)	105
3.2.9.1	Démarches simplifiées (DS)	105
3.2.9.2	Dossier numérique de l'agent (DNA)	105
3.2.10	Intelligence artificielle	106
3.2.11	Internet des objets – IOT	107
3.3	Services d'infrastructure	107
3.3.1	Messagerie / Agenda / Tâches / Listes de diffusion	107
3.3.1.1	Messagerie non officielle – Agenda [MEL-AGE]	107
3.3.1.2	Gestion de tâches [GTA]	108
3.3.1.3	Liste de diffusion [LDF]	108
3.3.2	Partage d'information et publication	109
3.3.2.1	Portail personnalisable [GPE]	109
3.3.2.2	Portail d'information [PIN]	109
3.3.2.3	Création de sites Web [CSW]	110
3.3.2.4	Gestionnaire de métadonnées [GMD]	110
3.3.2.5	Syndication de contenu [ASY]	110
3.3.2.6	Répertoires partagés [REP]	111
3.3.2.7	Moteur de recherche [RMR]	111
3.3.2.8	Gestion des communautés d'intérêt [COI]	111
3.3.2.9	Réseau social d'entreprise [RSE]	112
3.3.2.10	Enquête et sondage [ENQ]	112
3.3.3	Travail de groupe	112
3.3.3.1	Messagerie instantanée – Réunion virtuelle – Vidéoconférence - Rédaction collaborative synchrone [MIN-REV-VIH-RCS]	112
3.3.3.2	Wiki [WKI]	113
3.3.3.3	Forum [FOR]	114
3.3.4	Services d'annuaires [ANN]	114
3.3.4.1	Annuaires / référentiels	114
3.3.4.2	Annuaires techniques de ressources	116
3.3.4.3	Outils de « <i>provisionning</i> » d'annuaires	116
3.3.5	Utilitaires d'infrastructure	116
3.3.5.1	Serveurs d'impression – numérisation [IMP]	116
3.3.5.2	Diffusion audio-video [DAV]	117
3.3.6	Services communs réseau	117

3.3.6.1	Nommage DNS[NOM]	117
3.3.6.2	Synchronisation horaire [SYN]	118
3.3.6.3	Adressage - DHCP [ADR]	118
3.3.6.4	Marquage des flux réseaux [MQR]	118
3.3.6.5	Transfert fichiers volumineux [TFV]	118
3.3.6.6	Autres [MFI]	119
3.3.7	Systèmes d'exploitation [OS]	119
3.4	Services de sécurité	119
3.5	Services d'administration et de gestion	119
4	SECURITE	120
4.1	Documents de référence	120
4.1.1	Document généraux	120
4.1.1.1	Politiques de sécurité des systèmes d'information	120
4.1.1.2	OIV/OSE	121
4.1.1.2.1	Opérateur d'importance vitale	121
4.1.1.2.2	Opérateur de services essentiels	121
4.1.1.3	Droits et obligations des usagers et des administrateurs	121
4.1.1.4	Protection du secret	121
4.1.1.5	Protection des données à caractère personnel (RGPD, CNIL ...)	122
4.1.2	Références pour le non classifié (NP-DR-sensible) et le NR	123
4.1.3	Références pour le niveau Secret (ex CD)	123
4.1.4	Référence pour le SO	124
4.1.5	Références pour le SUE	124
4.1.6	Références pour la protection des informations avec les Nations Unies	124
4.1.7	Accès à la documentation technique	125
4.2	Démarche de sécurité	125
4.2.1	Homologation	125
4.2.1.1	Généralités	125
4.2.1.2	Principes	126
4.2.1.3	Homologation nationale	126
4.2.1.4	Homologation interalliée	128
4.2.1.5	Cas particuliers des systèmes industriels (dont SCADA)	128
4.2.2	Maintien en condition de sécurité	129
4.2.3	Audits	129
4.3	Cryptographie et gestion des ACSSI	130
4.4	Protection contre les signaux compromettants	130
4.5	Sécurisation des COTS	131
4.6	Services de sécurité	132
4.6.1	Sécurisation des accès	132
4.6.1.1	Démarche INA : RIN – RIA-Def - MindefConnect	132
4.6.1.2	Identification / Authentification des personnes [CAU]	134
4.6.1.2.1	Authentification sur Internet	134
4.6.1.2.2	Authentification sur Intradef	135
4.6.1.2.3	Authentification sur intranets classifiés	136
4.6.1.2.4	Authentification mutualisée et SSO	136
4.6.1.3	Habilitation et gestion des profils	138
4.6.1.4	Supports matériels – Cartes à puces	139
4.6.1.5	Authentification Machines [CAR]	140

4.6.1.6	Authentification Services [CAR]	140
4.6.1.7	Relais (messagerie, services web, services utilisateurs) [Rxx]	141
4.6.2	Gestion des clés – certificats électroniques [IGC]	141
4.6.3	Gestion de la preuve	143
4.6.3.1	Horodatage [HOR]	143
4.6.3.2	Signature [SGN]	143
4.6.4	Surveillance - Outils LID, détection d'intrusion [SUR] [DEA]	144
4.6.5	Utilitaires de sécurité	144
4.6.5.1	Antivirus – codes malveillants [ANV] [SSV]	144
4.6.5.2	Contrôles d'intégrité [CIN]	145
4.6.5.3	Chiffrement	145
4.6.5.3.1	Chiffrement de fichiers [CHI]	145
4.6.5.3.2	Effacement sécurisé	146
4.6.5.4	Pare-feux	146
4.6.6	Supports de stockage sécurisés	147
4.6.7	Équipements de chiffrement	148
4.7	Interconnexions, passerelles et solutions de sécurité iso/multi niveaux	148
4.7.1	Passerelles d'échanges	148
4.7.2	Passerelles transdomaines	149
4.7.3	Autres passerelles	151
4.8	Administration de la sécurité	152
4.8.1	Gestion des utilisateurs et des droits	152
4.8.2	PCA-PRA	152
4.8.3	Gestion des journaux d'évènements applicatifs ou système	152
4.8.4	Maintien en condition de sécurité (MCS) - composant technique	153
4.8.5	Sécurisation des flux réseaux	154
4.8.6	Sécurisation des supports de stockage	154
4.8.7	Hébergement / Virtualisation	154
4.8.8	Supervision de la sécurité, LID	154
4.8.9	Télémaintenance	155
4.8.10	Sauvegardes	155
4.8.11	Gestion de configurations de sécurité	155
4.9	Divers	156
5	INFRASTRUCTURE	157
5.1	Matériels, OS, virtualisation et conteneurisation	157
5.1.1	Système d'exploitation [OS]	157
5.1.1.1	Système d'exploitation client	157
5.1.1.2	Système d'exploitation serveur	157
5.1.1.3	Autres (équipement réseau)	159
5.1.2	Virtualisation	159
5.1.3	Conteneurisation	160
5.1.4	Poste terminal : fixe / mobile (portable, smartphone, tablette)	165
5.1.5	Communication	165
5.1.5.1	Voix et Vidéoconférence Secret	165
5.1.6	Impression et scanners	165
5.1.7	Stockage	165
5.1.8	Téléphonie	166
5.1.8.1	Téléphonie classique	166
5.1.8.2	Téléphonie chiffrée	167
5.1.8.3	Radiotéléphonie (INPT)	167
5.1.9	Solutions 'packagées' : SIA-Box	167

5.2 Réseaux	168
5.2.1 Généralités	168
5.2.1.1 Architecture des réseaux, IPV6	168
5.2.1.2 Adressage IP	168
5.2.1.3 Bout en bout : QoS – Contrats de services – interconnexion – métrologie	168
5.2.1.4 Problématique des réseaux contraints	169
5.2.2 Réseaux de transport WAN et routage	169
5.2.3 Services de réseaux de desserte	170
5.2.3.1 Maîtrise des flux réseau [MFR]	170
5.2.4 Services des réseaux étendus : filtrage - passerelles [FIL-PAS]	170
5.2.5 ToIP / VoIP	170
5.2.6 Réseaux sans fils	171
5.2.6.1 Technologies sans fil (WIFI, Bluetooth, RFID, ZIGBEE, Lorawan)	171
5.2.6.2 RFID	171
5.2.7 Liaison satellitaires	171
5.2.8 Équipements : Lan, Routage, Switch, Pare feu, accélérateurs...	172
5.2.9 Équipements de chiffrement	172
5.2.10 VPN	172
5.2.11 Baies	172
5.2.12 Câblage	172
6 CADRE FONCTIONNEL ET TECHNIQUE D'HEBERGEMENT	173
6.1 Plateformes d'hébergement	173
6.1.1 Références générales sur l'hébergement	173
6.1.2 Typologie d'environnements sur les plateformes	174
6.1.3 Les niveaux de service d'hébergement	175
6.1.4 Processus d'hébergement	176
6.1.5 Le dossier d'architecture technique est un prérequis essentiel et structurant de tout échange avec la DIRISI (deux modèles sont disponibles pour ce document sur le portail hébergement de la DIRISI) Hébergement sur Intradef	176
6.1.5.1 Aspect réseaux	177
6.1.5.1.1 Gard	177
6.1.5.1.2 SARDAc	177
6.1.5.1.3 Netscaler	177
6.1.5.2 Hébergement Infogérance DR	178
6.1.5.3 Hébergement C1 DR	179
6.1.5.4 Offre VPS DR	180
6.1.5.5 Hébergement des données de santé (HDS)	180
6.1.5.6 Hébergement Salle Blanche DR (réservé aux besoins en matériel spécifique)	181
6.1.5.7 Hébergement sur SIE (Intradef Embarqué)	181
6.1.5.8 Hébergement de développement	182
6.1.6 Hébergement sur Internet	183
6.1.6.1 Hébergement Internet mutualisé – HELISS-NG	183
6.1.6.2 Hébergement C1 NP	184
6.1.6.3 Hébergement PHEBIA sur Internet	185
6.1.6.4 Recours offre C3 Internet	185
6.1.7 Hébergement mutualisé sur les intranets classifiés	186
6.1.8 Informatique décisionnelle	186
6.2 Opérations – processus	186
6.2.1 Gestion des configurations	186
6.2.1.1 Base de connaissance de gestion CMDB [BCA]	187
6.2.1.2 Inventaire [INV]	187
6.2.1.3 Dépôt d'artefacts	187

6.2.2	Gestion des demandes	188
6.2.3	L'hébergement d'un nouveau SI fait l'objet d'une demande dématérialisée dans le catalogue de service de la DIRISI.Déploiement / Distribution / Orchestration	188
6.2.4	Gestion du stockage	190
6.2.5	Synchronisation / RéPLICATION / Déduplication	190
6.2.6	Sauvegarde / restauration	190
6.2.7	Observabilité	191
6.2.7.1	Journaux d'événements applicatifs et système	192
6.2.7.2	Métriques	193
6.2.7.3	Traces	193
6.2.7.4	Dépendances (C1-NP et C1-DR)	194
6.2.7.5	Sur les réseaux classifiés	194
6.2.8	PCA/PRA – PCI/PRI - Gestion de crise	194
6.2.9	Gestion d'exploitation et des capacités	195
6.2.10	Hypervision	195
6.2.11	Administration réseaux, performance réseaux et Télécommunications	195
6.2.12	Surveillance et métrologie des salles	195
7	CONCEPTION – DEVELOPPEMENT	196
7.1	Règles générales	196
7.2	Analyse, modélisation	196
7.2.1	Modélisation métier	196
7.3	Développement	198
7.3.1	Outils de développements internes	198
7.3.1.1	Environnement DevSecOps ministériel	198
7.3.1.1.1	Ambitions et orientations DEVSECOPS	198
7.3.1.1.2	Plateforme de développement PICSEL	199
7.3.1.2	Safr@n	199
7.3.2	Développement en Java	200
7.3.3	Développement en PHP	201
7.3.4	Développement en C# et .NET	202
7.3.5	Développement HTML5-Javascript-CSS	202
7.3.6	Réalisation d'applications mobiles	205
7.3.7	Développement à l'aide d'outils « low-code » ou « no-code »	206
7.3.8	Autres langages	208
7.3.9	Sécurisation du code	208
7.4	Test et intégration (pré-intégration, intégration continue)	209
7.4.1	Tests unitaires	210
7.4.2	Tests d'intégration des composants	210
7.4.3	Intégration continue	210
7.4.4	Tests de performance	211
7.5	Qualité logicielle	212
7.5.1	Performance - Métrologie	213
7.6	Gestion des anomalies	214
8	ANNEXES	216
8.1	Glossaire / liens utiles	216
8.2	Produits / Piles logicielles d'exécution	216
8.2.1	Pile logicielle : liste des produits	216

8.2.2	Modules pour CMS Drupal, Joomla ! et Wordpress	270
8.3	Piles logicielles du développement	270
8.3.1	Pile PICSEL	270
8.4	Règles de nommage	271
8.4.1	Nommage des fichiers	271
8.4.2	Annuaire - Identifiant unique - Adresse messagerie	271
8.4.3	Nommage DNS	271
8.4.4	Nommage des serveurs	271
8.4.5	Nommage composants d'infrastructure de télécommunication	272
8.4.6	Nommage VLAN	272
8.4.7	Adressage IP	273
8.4.8	Marquage de la sensibilité des informations numériques	273
8.5	Référentiels / Nomenclatures	273
8.5.1	Cartographie des services	273
8.5.2	Catalogue des OID	274
8.5.3	Trigrammes de sites géographiques	274
8.5.4	Mots clés d'attribution (MCA)	274
8.6	Critères d'éligibilité des produits et solutions	275
8.6.1	Objectifs et contraintes	275
8.6.2	Critères généraux d'appréciation	275
8.6.3	Critères d'éligibilité pour des modules de CMS	277
8.7	Modèles d'architecture	278
8.7.1	Introduction aux modèles d'architecture	278
8.7.1.1	Qu'est-ce qu'un modèle d'architecture ?	278
8.7.2	Modélisation des SI avec Archimate	279
8.7.2.1	Qu'est-ce que archimate ?	279
8.7.2.2	Les concepts Archimate utilisés pour les modèles d'architecture CCT	280
8.7.2.3	Les relations Archimate utilisées pour les modèles d'architecture CCT	281
8.7.3	Modèles d'architectures logiques de référence	281
8.7.3.1	Définition et intérêt d'une architecture logique	281
8.7.3.2	Modèle de référence	282
8.7.4	Catalogue des modèles d'architecture applicatives	285
8.7.4.1	Le modèle d'architecture PHP	285
8.7.4.2	Le modèle d'architecture Javascript	286
8.7.4.3	Le modèle d'architecture Java	287
8.7.4.4	Le modèle d'architecture de modernisation progressive d'un SI « historique » Java	288
8.7.4.5	Le modèle d'architecture « Client-léger » permettant un mode déconnecté	289

Table des illustrations

<i>Figure 1 : Cycle de vie d'un projet SIC</i>	33
<i>Figure 2 : Route API</i>	81
<i>Figure 3 : Typologie des environnements sur les plateformes</i>	174
<i>Figure 4 : Description d'un SI dans ARCHIMATE</i>	280
<i>Figure 5 : Architecture applicative</i>	282
<i>Figure 6 : Architecture applicative (modèle logique)</i>	284

<i>Figure 7 : Modèle d'architecture PHP</i>	286
<i>Figure 8 : Modèle d'architecture Javascript.....</i>	287
<i>Figure 9 : Modèle d'architecture applicative Javascript sur le Frontend et Java en Backend.....</i>	288
<i>Figure 10 : Modèle d'architecture applicative de transition permettant d'assurer la modernisation progressive d'un SI « historique » Java</i>	289
<i>Figure 11 : Modèle d'architecture « client-léger » permettant un mode déconnecté</i>	289

1 GENERALITES

1.1 Objet du document

Ce document constitue le référentiel ministériel des préconisations et choix techniques relatifs au socle du système d'information du ministère des armées et aux grands composants d'architecture technique.

Il s'inscrit dans le cadre documentaire technique du ministère dont le document d'architecture technique générale des SIC du ministère des armées [ATG] est le cadre de référence et complète le référentiel d'architecture technique décrivant les principaux motifs d'architecture technique mis en œuvre.

Il précise les vues « applicative », « logicielle » et « infrastructure » liées à la démarche d'urbanisation du ministère en déclinaison de la politique ministérielle relative aux SIC.

Conformément au décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication [DGNUM], celle-ci définit les dispositions d'architecture générale et le cadre de cohérence du système d'information et de communication de la défense et en contrôle la mise en œuvre.

Conformément au mandat du sous-comité de cohérence des architectures (SC²A)¹, l'animation et la réalisation du présent document sont effectuées par le SC²A qui soumet annuellement une nouvelle version à la validation du CECNUM et à la signature du DGNUM.

La conformité au cadre de cohérence technique [CCT] constitue un des critères d'appréciation dans les revues d'approbation de projets de systèmes d'information relevant de l'instruction ministérielle 2476 [IM2476] portant sur la conduite des projets SIC, et dans l'instruction pour avis conforme prévu à l'article 5 du décret du 28 juin 2018 précité.

1.2 Périmètre

De façon globale, le CCT est un référentiel des choix techniques du ministère des armées dans le domaine des SIC. Il concerne essentiellement le domaine technique SIC ayant trait aux intranets du ministère² (Intradef, Intranets Secret-SF, FrOpS, hébergement Internet sur les plateformes ministérielles Heliss NG, PHEBIA (remplacées en 2024 par la plateforme C1NP), initiatives Cloud internes et externes, hébergements SaaS sur Internet, réseaux spécifiques dont IST et Très Secret,... et plus globalement, l'usage et l'empreinte du ministère sur et au travers d'Internet). Le CCT peut le cas échéant être amené à couvrir des segments en couplage même lâche avec les Intranets IP du ministère dès lors que cela présente un intérêt pour l'ensemble de la communauté SIC.

Il décline les chapitres du document [ATG] relatifs aux services communs (services à l'utilisateur, services techniques, socle applicatif), aux services et outils de sécurité, à l'hébergement, l'administration et l'exploitation, à l'infrastructure (réseau, téléphonie, configuration logicielle et matérielle standard), dont il précise les choix techniques. Il couvre également les règles de conception et de développement du ministère.

¹ Mandat diffusé par note n°252/ARM/DGNUM/DG/NP du 7 juillet 2020

² Les systèmes d'information hébergés par des sous-traitants doivent respecter les règles de l'intranet auquel ils sont raccordés.

Il a vocation à préciser les préconisations et choix relatifs aux services communs des intranets décrits dans la cartographie des services communs du ministère des armées [CARTO]³.

1.3 Domaine d'application – Acteurs concernés

Ce référentiel doit être pris en compte par les projets de SIC et référencé dans le cadre des marchés publics (**cf. 1.5**). Tout système d'information ou composant logiciel proposé pour une utilisation tant sur les réseaux du MinArm que sur Internet doit respecter les recommandations du CCT en vigueur au début de sa réalisation et en suivre les évolutions tout au long de son cycle de vie (cette conformité constitue une condition préalable à tout passage en environnement de préproduction ou de production, notamment pour les plateformes C1NP et C1DR). En conséquence, **les évolutions du CCT devront notamment être prises en compte pendant la réalisation des travaux** et dans le cadre de la tierce maintenance d'administration / d'exploitation, a minima pour ce qui concerne les correctifs de sécurité et la gestion de l'obsolescence. Le processus de révision annuelle du CCT tient compte de cette contrainte et s'attache à éviter toute modification brutale toutes les fois que c'est possible.

Le CCT s'adresse principalement :

- **Aux directions des systèmes d'information et aux directions d'application⁴** pour leur présenter les choix et orientations du ministère pour l'accueil, l'hébergement, et l'environnement des systèmes d'information et les aider dans la conduite de leur projet, notamment dans la prise en compte dans les marchés du contexte technique ministériel ; le non-respect du CCT nécessitera pour les directions d'application de justifier leur choix et d'initier des demandes de dérogation (cf. 1.9.2).
Par défaut, toute direction d'application doit s'efforcer d'en respecter les parties qui peuvent lui être applicables ;
- **Aux acteurs techniques de la communauté SIC** aux fins de partage, de cohérence et de pilotage de l'évolution des compétences techniques nécessaires au ministère, le CCT :
 - est un outil de partage permettant à des acteurs techniques parfois dispersés de partager une même vision des composants d'architecture et des choix techniques du ministère ;
 - est un levier de cohérence du corpus documentaire technique du ministère permettant d'identifier des références redondantes ou en recouvrement, d'identifier des obsolescences ou des lacunes et d'en tirer un plan de travail de mise en cohérence ;
 - constitue un outil utile dans le cadre d'une démarche visant à assurer l'adéquation entre les compétences techniques existantes ou prévues et les besoins, notamment dans le cadre d'une GPEC⁵ sur les compétences techniques ;
- **Aux acteurs en charge de développements internes** au ministère (CDAD, Fabrique Numérique, SMSIF-RH, S2NA, centres de proximité des armées (ESIOC, CCIAT, CEPN, CSD/M, ...), etc.) dont il constitue le cadre de référence ;
- **Aux partenaires** étatiques, alliés ou industriels à titre d'outil de communication et de partage, le

³ Cf. 8.5.1 Cartographie des services

⁴ Par direction d'application, on entend ici l'ensemble des acteurs travaillant au sein ou au profit d'une direction de projet ou de programme (responsable de conduite de projet, responsable fonctionnel, experts techniques ou métier, rédacteurs de marché...).

⁵ Gestion prévisionnelle des Emplois et Compétences.

CCT :

- permet de faire connaître et de positionner efficacement les choix du ministère en interministériel notamment dans le cadre des travaux pilotés par la DINUM, comme en interallié ;
- permet d'informer les fournisseurs et industriels travaillant au profit des SIC du ministère et d'orienter leurs travaux pour une meilleure prise en compte du contexte ministériel ;

Afin de répondre au mieux à ces besoins de communication du CCT vis-à-vis d'entités externes au ministère, deux versions du CCT sont proposées, l'une DR à usage d'abord interne, l'autre NP permettant une diffusion plus large mais qui doit demeurer encadrée et maîtrisée.

1.4 Gestion et gouvernance du CCT

Conformément aux textes en vigueur, la gouvernance des architectures technique et applicative s'appuie sur le sous-comité de cohérence des architectures (SC²A) pour valider les architectures des systèmes d'information du ministère.

Le CCT est un document vivant, prenant en compte les besoins projets qui seront exprimés au travers de leur DSI de rattachement. L'ensemble du CCT est mis à jour annuellement.

Depuis la version 3.5, l'annexe 8.2 du CCT est mis à jour à mi année ainsi que les corrections d'erreurs relevées dans la version annuelle majeure (notamment cohérence entre 8.2 et corps du document).

1.5 Prise en compte dans le cadre des cahiers des charges

Le présent CCT doit être référencé dans les CCTP⁶, en tout ou partie⁷. Une formulation possible⁸ est donnée ci-après :

« L'architecture et la pile logicielle du système doivent respecter/être conformes au CCT (à mettre en document applicable dans le marché). Tout écart devra faire l'objet d'une justification et d'une demande de dérogation auprès du SC²A.

Il est précisé que l'obtention de celle-ci demeure de la responsabilité de la direction de projet qui pour ce faire, s'appuiera autant que de besoin sur son titulaire.

Les évolutions du CCT devront être prises en compte pendant la réalisation des travaux et la période de MCO/MCS. »

Si pour un contexte donné, le chef de projet juge qu'une règle ou recommandation du CCT est incontournable, il doit alors la transférer dans son CCTP et préciser son caractère obligatoire. Cette exigence sera alors reprise dans la grille de conformité et évaluée en tant qu'élément de conformité de l'offre, c'est-à-dire qu'une proposition ne respectant pas cette exigence sera automatiquement rejetée.

Toute difficulté rencontrée lors de la mise en œuvre du cadre de cohérence technique devra être signalée au

⁶ Cahier des Charges Techniques Particulières

⁷ En particulier l'annexe « pile logicielle »

⁸ Formulation adaptée de clauses analogues du CCT du ministère de l'Intérieur

1.6 Organisation du document

1.6.1 Organisation générale du document

La structure du document est cohérente avec le document d'architecture technique générale des SIC du ministère des armées et, pour les chapitres en relevant, avec la cartographie des services des Intranets des armées [CARTO]. Cette structure est compatible avec les NRI⁹/NRA¹⁰ du Cadre Commun d'Urbanisation (CCU) du SI de l'État entretenu par la DINUM (cf. 8.5).

Ce CCT est composé :

- d'une partie principale référençant les documents normatifs, guides de paramétrage, règles additionnelles éventuelles ne se retrouvant pas dans un document référencé, ainsi que les principaux choix logiciels ou interfaces normatives et tout élément ayant vocation à rejoindre le référentiel commun technique du ministère ;
- d'un ensemble d'annexes complétant ce corpus dont principalement :
 - le catalogue des produits et solutions autorisés dans le ministère, et notamment la pile logicielle soutenue ou exploitée par la DIRISI selon les environnements ainsi que les piles d'exécution ;
 - le référentiel de l'environnement de développement ;
 - la liste des bibliothèques applicables à certaines technologies.

Les références identifiées dans ce cadre (références documentaires, règles additionnelles, normes/standards et produits/solutions) sont répertoriées dans des cartouches dont les modèles et la codification sont précisés ci-dessous.

1.6.2 Pile logicielle et environnements d'exécution

Le présent CCT détaille les solutions et produits mis en œuvre à des degrés divers au sein du ministère des armées, soutenus ou pas par l'opérateur Défense. La récapitulation des produits est annexée au CCT sous le vocable « Pile logicielle ».

Par ailleurs, il existe des services constitués d'un assemblage de composants intégrés qui seront à privilier vis-à-vis des briques technologiques sous-jacentes. On y trouve par exemple la pile d'exécution des structures d'hébergement, la pile de la plateforme décisionnelle, l'environnement de développement interne, des services de socle...

Certains de ces environnements techniques sont également détaillés dans le CCT.

1.7 Codification des références du CCT

⁹ NRI : Nomenclature de Référence d'Infrastructure

¹⁰ NRA : Nomenclature de Référence Applicative

1.7.1 Références documentaires – Typologie de documents

Document	Date	Origine	Type doc	Portée
(1)	(2)	(3)	(4)	(5)
<i>Commentaire : périmètre, recouvrement, manque, toilettage à opérer, imprécisions, niveau d'application (difficulté, application non avérée, ...) (+ auteur)</i>				

- (1) : **Document**: titre + éventuelle référence (timbre)
- (2) : **Date du document** : sous la forme : JJ Mois AAAA
- (3) : **Origine** : Autorité signataire ou chargée de l'entretien
- (4) : **Type de document** : Directive / Note / ITE/ Guide / Concept d'emploi / Livrable industriel/Projet
- (5) : **Portée** : peut être de nature différente suivant la référence :
- Organisation : OTAN, UE, France, Interministériel, MinArm, Organisme ;
 - Déploiement : Intradef, Intraced niveau Secret-SF (S-SF), Très Secret (TS), FrOpS, Internet, SIE (segment Intradef embarqué), IST, PICSEL, ... ;
 - Confidentialité: NP, DR, Secret-SF, Secret, Très Secret (TS)... ;
 - Métier : SIAG, SIOC, SIST, ... ;
- (6) : **Commentaire** : périmètre, recouvrement, difficulté(s) ou subtilité(s) de mise en œuvre, évolution proposée ou à venir, ...

Typologie de documents :

Globalement, les documents de ce référentiel peuvent être classés en 4 grandes catégories :

- Cadre juridique applicable : traités ou accords internationaux, textes européens (règlement/directive), loi, ordonnance, décret, arrêté, circulaire, instruction interministérielle ou ministérielle, référentiels généraux ;
- Cadre général ministériel : politique, stratégie, doctrine ou concept d'emploi, SLR ;
- Cadre technique normatif ou référentiel : STANAG, politique de sécurité, directive, cadre technique, ITE, référentiel ;
- Cadre technique d'accompagnement : guide, note technique, manuel, rapport technique ; documents ou livrables projets...

À titre d'information, pour les documents techniques nouvellement produits sous son égide, la DGNUM a adopté une typologie en 4 classes dont le périmètre et le niveau de signature, d'applicabilité, de dérogation sont de nature différente. Ces 4 niveaux sont les directives, cadres techniques, notes techniques ou guides. Cette typologie peut constituer une base de réflexion pour une adoption par les armées, directions et services aux fins d'homogénéiser les références techniques du ministère.

1.7.2 Règles et recommandations additionnelles

De façon générale les règles recommandées ont vocation à être incluses dans des documents référencés (exemple : les directives) par le CCT. Cependant, lorsque cela présente un intérêt particulier, et si la règle n'est encore présente dans aucun autre document, il est possible de référencer une telle règle directement dans le CCT.

Règle	Énoncé	Statut	Portée
(1)	(2)	(3)	(4)

(1) **Règle** : CCT_RN : N numéro

(2) **Énoncé** de la règle

(3) **Statut** : Obligatoire / Recommandé / Déconseillé / Interdit (cf. ci-dessous)

(4) **Portée** : cf. 1.7.1

Les niveaux de recommandation sont conformes à la [RFC 2119] :

- **OBLIGATOIRE** : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ; ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive
- **RECOMMANDÉ** : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;
- **DÉCONSEILLÉ** : ce niveau de préconisation signifie que la règle édictée indique une contre-indication qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé ;
- **INTERDIT** : ce niveau de préconisation signifie que la règle édictée indique une interdiction absolue de la directive.

Toute demande de dérogation à ces règles doit être présentée au SC²A pour instruction, validation et recommandations (cf. 1.9.2).

1.7.3 Normes et standards

Le CCT n'a pas vocation à recenser l'ensemble des normes et standards du domaine couvert. Cependant, lorsque cela présente un intérêt particulier, il est possible d'inclure dans ce document une norme.

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
(1)	(2)	(3)	(4)

(1) **Norme/standard** : nom commun de la norme ou du standard

(2) **Description** de l'usage et de ses conditions d'utilisation au sein du MinArm

(3) **Statut** : Obligatoire / Recommandé / Déconseillé / Interdit (cf. 0)

(4) **Portée** : cf. 1.7.1

1.7.4 Produits et solutions

NOTA : ce document référence les solutions ou produits logiciels principaux, ainsi que les orientations principales. Pour plus de détails (version, sous-version...), on se référera à l'annexe détaillée de la pile logicielle dont la structure est calquée sur le sommaire du CCT. Par ailleurs, généralement et sauf contraintes liées à leur mise à disposition sur les réseaux ministériels, les versions indiquées sont les versions minimales autorisées.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
(1)	(2)	(3)	(4)	(5)	(6)

Commentaire : éventuel pour préciser le cadre d'emploi, l'usage...

(1) **Solution** : exemple : grand composant : messagerie, bureautique, MCS, virtualisation...

(2) **Produit** : nom du produit ou du service logiciel (ou matériel ou nom de la solution si celle-ci est packagée) / version majeure. L'insertion d'un tel produit dans le CCT est soumis à une présentation préalable, suivi d'un avis, en SC²A (cf. 1.9.2).

(3) **Fournisseur** : éditeur / communauté libre ... S'il s'agit d'une solution interne : nom ou organisme point de contact

(4) **Utilisation / restriction** : conditions éventuelles d'utilisation dans le ministère

(5) **Statut** : sur deux lettres :

- La première relative au niveau de **recommandation** :
 - **R** : Recommandé (usage général par défaut) ;
 - **E** : Émergent (il est envisagé de recommander la solution à une date à indiquer en commentaire si connue ou produit à l'étude en vue d'une possible recommandation) ;
 - **A** : Assujetti (à un usage particulier ou nécessitant une autorisation ou une justification, détail fourni en commentaire) ;
 - **D** : Déconseillé (obsolescence, abandon par l'éditeur ou autre) ;
 - **Interdit** (formellement interdit) ;
 - - : aucune politique sur le produit n'a encore été définie au niveau du ministère ;
 - * : cela dépend de la version, il faut se référer à l'annexe 8.2.
- La seconde relative à la nature du **soutien** par l'opérateur :
 - **S** : soutenu : conditions particulières éventuellement préciser en commentaires ;
 - **E** : soutien envisagé à une date à indiquer, si connue, en commentaire ;
 - **O** : obsolescent bien qu'encore soutenu (retrait futur à anticiper) ;
 - **N** : non soutenu (en cas d'autorisation d'emploi du produit concerné, son soutien devra être assuré par la direction d'application) ;
 - - : le niveau de soutien reste à définir ;
 - * : cela dépend de la version, il faut se référer à l'annexe 8.2

Une solution ayant le statut ‘E’, ‘O’, ‘N’, ou ‘-’ ne pourra pas prétendre à une offre infogérance de la DIRISI. En conséquence, la direction d'application devra assumer seule l'exploitation technique (l'application des correctifs de sécurité restant obligatoire dans les délais prescrits).

(6) Portée cf 1.7.1

Nota : les portées SIA S-SF et SIA FrOpS renvoient par défaut au périmètre SIA, il existe encore des bulles historiques Intraced Air, SICF ou FrOpS qui n'utilisent pas forcément le produit ou la solution.

1.8 Critères d'éligibilité des produits et solutions

1.8.1 Contraintes à respecter et critères d'appréciation

Le domaine de l'informatique évolue à un rythme extrêmement rapide. L'introduction d'une nouvelle technologie ou d'un nouveau produit dans le CCT est toujours le fruit d'une équation complexe prenant en compte des besoins et contraintes s'opposant par nature comme l'avantage opérationnel procuré, la maîtrise ou la sécurité du SI, la souveraineté, l'exploitabilité ou encore la rationalisation des choix.

Aussi les demandes d'intégration de nouveaux produits ou solutions dans le CCT comme les demandes de dérogation sont appréciées sur la base d'une grille de critères en termes fonctionnels, de support, de sécurité, de qualité ou encore d'intégration dans le système d'information du ministère.

Les contraintes prises en compte ainsi que les critères d'appréciation sont détaillés en annexe 8.6.

1.8.2 Évolutions

Compte tenu de la nature très évolutive des technologies, le statut associé est susceptible d'évoluer à chaque édition du CCT.

En conséquence, la gouvernance technique (cf. 1.4) passe en revue régulièrement les technologies recensées et celles qui lui sont soumises par le biais des saisines et demandes de dérogations. Pour ce faire, elle s'appuie

sur des expertises identifiées en interne ou en externe (études industrielles, RETEX de nos partenaires, forums, prestations sur mesures, etc).

Toute sollicitation ou contribution spontanée est également bienvenue pour attirer l'attention de la gouvernance technique sur une nouvelle technologie ou une évolution dans un domaine susceptible de faire évoluer une position antérieure.

1.8.3 Le CCT et l'innovation

L'innovation n'a de valeur que dans sa capacité à améliorer durablement le fonctionnement du ministère. Ceci passe avant tout par la mise en œuvre de nouveaux procédés ou l'amélioration des procédés existants en utilisant au besoin les leviers offerts par l'informatique.

Plusieurs outils peuvent répondre à un besoin donné, il convient de choisir celui qui répondra le mieux au besoin dans sa globalité même s'il peut s'avérer être sous optimal pour un aspect spécifique.

Refuser un outil particulier ne signifie donc pas s'opposer à une innovation, mais orienter de manière raisonnée et argumentée vers un autre choix jugé globalement plus efficient.

1.9 Conformité au CCT

1.9.1 Validation des architectures des SI

Afin de préparer et de réduire le risque à l'atterrissement du système d'information sur les infrastructures du ministère, les directions d'application doivent solliciter l'avis du SC²A. Son avis est requis a minima pour le jalon 3 permettant de lancer la réalisation prévu dans l'IM 2476 relatif à la conduite des projets de SIC (cf. 1.4).

En cas de besoin et sous réserve de la passation de prestations d'assistance, des capacités d'appui, ne se substituant pas aux architectes du projet ou aux DSI domaine, existent pour accompagner le projet dans la consolidation et la vérification de la conformité d'une architecture avant passage du projet en SC²A (UO DIRISI, offre de service du bureau d'architecture de la DIRISI, appui DGA, ...).

La validation des architectures par le SC²A ne préjuge pas de la validation physique de l'hébergement visé qui est du ressort de l'opérateur (validation des matériels physiques, raccordements réseaux, offre de services ou d'hébergement validée, ...).

En complément de l'avis de principe du SC²A, la prise en charge effective en infogérance par la DIRISI nécessite un passage en comité d'affaires (plan de charges, ressources, planning...).

1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT

Les demandes de saisine pour avis et validation d'architecture et les demandes de dérogations aux recommandations du CCT doivent être présentées à la gouvernance technique (cf. 1.4) qui instruit ou fait instruire les demandes. Sont concernés notamment :

- la liste de composants logiciels avec leur version ;
- la liste des bibliothèques employées et leurs versions (Java, Javascript, Python, PHP, Drupal, ...) dans les formats demandés ;
- les adhérences à des services tiers (DNS, annuaires, messagerie, PEM, MindefConnect, ...) ;
- les écarts avec les règles prévues par le corpus de directives du ministère ;

- les références des fiches SICLADE SI et Projet .

Toute demande d'étude de projet devra être validée par la DSI de rattachement avant d'être planifié.

Pour éviter tout report de session, il est rappelé que la direction de projet doit s'assurer de la présence du représentant de la DSI et des compétences nécessaires pour être en mesure de répondre aux questions techniques et d'architecture du SC²A (industriels, responsable de réalisation, ...).

2 CADRES REFERENTIELS GENERAUX

Le ministère des armées inscrit sa démarche technique dans un objectif d'interopérabilité tant avec les alliés qu'en interministériel, ainsi que dans sa relation avec le citoyen. Suivant le contexte, les principaux référentiels à privilégier sont :

2.1 Les référentiels internationaux

2.1.1 OTAN

2.1.1.1 Référentiel NISP

En termes de cadre technique SIC (relevant du périmètre de ce CCT), le référentiel principal d'interopérabilité avec les alliés est le NISP qui fixe les règles d'interopérabilité et les profils d'emploi applicables aux systèmes concourant à la conduite des opérations en réseau NNEC (NATO Network Enabled Capability).

Document	Date	Origine	Type doc	Portée
NATO Interoperability Standard and Profiles (NISP) V14 (STANAG 5524) AdatP-34(N) - V1 du 26 mai 2021	26 mai 2021	NC3Board	Référentiel	OTAN SIO en interface avec l'OTAN

Commentaire : applicable aux systèmes concourant au NNEC (NATO Network Enabled Capability). Cette version du NISP a été raccourcie et simplifiée. Le NISP contient dorénavant 3 volumes :

- Volume 1 : introduit les concepts de base, et définit les modalités de gestion du NISP ; il inclut aussi un guide sur le développement de profils d'interopérabilité
- Volume 2 : contient les standards et profils d'interopérabilité approuvés et applicables actuellement
- Volume 3 : contient les standards et profils d'interopérabilité candidats, applicables aux programmes sous 1 ou 2 ans (dont le profil FMN, répondant à la démarche décrite ci-après).

Cette nouvelle version introduit la notion de Base-Standards Profile (BSP) qui renvoie à un profil des meilleures pratiques n'appartenant pas à des profils spécifiques.

2.1.1.2 Démarche FMN (Federated Mission Networking)

La mission de la démarche FMN est de développer et de maintenir une capacité C3¹¹ interalliée au travers de l'établissement commun d'un référentiel de normes d'interopérabilité et de procédures de mise en œuvre de ce référentiel. Cette capacité s'articule autour de la préparation collaborative par les Affiliés (Nations ou organisations) de forces :

- interconnectées par un réseau de mission constitué suivant des normes et des principes identifiés et expérimentés dans le cadre de l'initiative FMN ;
- dont les capacités d'interopérabilité ont été validées d'un point de vue opérationnel.

Le périmètre technique du FMN couvre ainsi l'interconnexion des réseaux et des moyens de communication, les services communs, les applicatifs C2 (Command & Control) et les fonctions associées : renseignement,

¹¹ Command, Control and Communications

appui-feu, ciblage, logistique, médical, ...

Plus globalement, l'initiative multinationale *FMN* s'imposant comme le vecteur principal d'interopérabilité des systèmes d'information et de communication en environnement interalliés, la France a choisi d'y adhérer et de revendiquer le statut **d'affilié de type A (Nation cadre)**. Trente-cinq nations ou entités participent en 2021 à l'initiative *FMN*. L'OTAN est un affilié de l'initiative *FMN* via NCS (NATO Command Structure), ACO (Allied Command for Operations) indique que la conformité au référentiel *FMN* est obligatoire pour les prises de tour NRF.

La démarche *FMN* s'organise en spirales capacitaires suivant un calendrier¹² contraint et ambitieux.

State	Spiral 1	Spiral 2	Spiral 3	Spiral 4	Spiral 5	Spiral 6
Preferred operational use	2017-2018	2019-2021	2022-2024	2025-2027	2028-2029	2030-2031

Entre le jalon "Final Specifications" et le jalon "Preferred operational use", les affiliés doivent réaliser l'acquisition des capacités définies au titre de la spirale, valider les tests techniques *FMN* de conformité des composants choisis et réussir les tests de mise en œuvre opérationnelle des dites capacités.

L'enjeu pour la France est double, il s'agit :

- de valider sa capacité technique et humaine à respecter les spécifications *FMN* et donc d'établir sa crédibilité à assumer ses ambitions opérationnelles,
- d'influencer l'initiative *FMN* afin qu'elle prenne en compte les intérêts nationaux en termes de doctrine, de procédures opérationnelles et de politique industrielle.

Le statut d'affilié de type A impose à la France **certains engagements** dont la participation active à la gouvernance *FMN* et à l'animation de ses travaux, le respect des spécifications *FMN*¹³ élaborées par les affiliés sous pilotage OTAN/ACT et des exigences d'entrainement aux processus en coalition et de mise en œuvre de laboratoires de test à distance des systèmes nationaux.

Afin d'accompagner ce changement de paradigme, une organisation idoine a été mise en place. Il a donc été décidé de :

- créer une gouvernance de cohérence inter-programmes et intra-ministère vis à vis de cet enjeu *FMN* par le biais de la mise en place d'une revue de cohérence capacitaire *FMN* (en conformité avec l'Instruction Ministérielle 1618) sous la responsabilité de EMA/COCA et DGA/SASD. Cette revue a en charge de définir la feuille de route *FMN*.
- créer une équipe projet FRISE *FMN* (type Manager/OP) qui doit instruire et coordonner la prise en compte de la feuille de route capacitaire au sein des programmes d'armement.

Document	Date	Origine	Type doc	Portée
Déclaration des Autorités Militaires Françaises au secrétariat FMN de leur volonté de devenir affilié du FMN, avec le niveau d'ambition Mission Network Element (Affilié de type A) diffusée par note N°193/REPDEF OTAN/C3/NU du 11 mars 2016	11 mars 2016	REPDEF OTAN	Note	MinArm

¹²"Proposed Specifications" – Jalon de spécifications initiales de la spirale

" Final Specifications" – Jalon de validation des spécifications

" Emerging operational use" – Jalon de début de confirmation des nations sur les spécifications de la spirale

" Preferred Operational use" - Phase de mise en œuvre du référentiel de la spirale en contexte interalliés *FMN*

¹³ Spécifications traitant des composantes procédurales et techniques du système d'information de la coalition

Document	Date	Origine	Type doc	Portée
Mise en place de plateforme FMN, note D6-19-007236/ARM/EMA/MGA/NCPI/NP du 19/12/2019	19 décembre 2019	EMA	Note	MinArm
Mandat de la Revue de Cohérence Capacitaire (RCC) diffusé par note sous double timbre : D-20-00377/ARM/EMA/SC/PLANS/COCA/NP DGA01090024720/ARM/DGA/SASD/NP	20 juillet 2020	EMA DGA	Note	MinArm
Contexte et mandat de l'équipe projet FRISE FMN Présentation des missions et de l'organisation de l'EDPI FRISE FMN diffusé par note sous double timbre : D-20-002452/ARM/EMA/SNA/NP DGA01D20A-8017/ARM/DGA/DO/UM ESIO/NP	29 mai 2020	EMA DGA	Note	MinArm

2.1.2 Européen

Document	Date	Origine	Type doc	Portée
Règlement e-IDAS – electronic Identification And Signature : Règlement (UE) 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur	23 juillet 2014	Union Européenne	Règlement applicable directement	UE
Commentaire : Tout comme le Référentiel Général de Sécurité (RGS) pour la France, e-IDAS a proposé de donner un cadre juridique aux échanges électroniques ayant lieu sur le marché communautaire. e-IDAS propose trois niveaux d'authentification : faible, substantiel, élevé (3 pour le RGS). Ce règlement est applicable depuis le 1er juillet 2016. Le règlement e-IDAS fait actuellement l'objet d'une refonte.				
RGPD : règlement général sur la protection de la donnée : Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données	27 avril 2016	Union Européenne	Règlement applicable directement	UE
Commentaire : le règlement européen RGPD voté en 2016 est applicable depuis le 25 mai 2018. Il vise à renforcer la protection des données à caractère personnel en harmonisant la législation à l'ensemble de l'Union européenne. En pratique, la plupart des déclarations préalables CNIL disparaissent au profit d'une logique de responsabilisation a priori des acteurs et de conformité continue. Les organismes qui traitent des données personnelles doivent veiller au respect des textes tout au long du cycle de vie de la donnée. Les pouvoirs de sanction des CNIL nationales sont renforcés.				
Directive NIS : Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union	14 décembre 2022	Union Européenne	transposée en droit national	UE
Commentaire : La présente directive établit des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur. Elle s'applique aux opérateurs de services essentiels – Entités du ministère a priori non concernés, mais certains industriels : oui. Ce texte fait actuellement l'objet d'une refonte. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC				
RÈGLEMENT (UE) 2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne	14 novembre 2018	Union Européenne	Règlement applicable directement	UE
Commentaire : Le présent règlement s'applique au traitement de données électroniques autres que les données à caractère personnel dans l'Union qui est: a) fourni en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'Union, par un fournisseur de services établi ou non dans l'Union; ou b) effectué par une personne physique ou morale résidant ou disposant d'un établissement dans l'Union pour ses propres besoins.				

2.2 Le cadre interministériel

2.2.1 La stratégie du SI de l'État – Doctrine cloud

Document	Date	Origine	Type doc	Portée
Cadre stratégique commun du système d'information de l'État : diffusé par circulaire du Premier ministre du 7 mars 2013	7 mars 2013	PM	Circulaire	Toute administration
<i>Commentaire : ce cadre est un document d'orientation fixant les objectifs de transformation du système d'information de l'État sous forme de cibles à atteindre et de dispositifs à mettre en œuvre à l'échéance de 5 ans, en partant des principaux enjeux de l'État.</i>				
Décret n°2019-1088 relatif au système d'information et de communication de l'état et à la direction interministérielle du numérique [DINUM] en date du 25 octobre 2019 et publié au JO du 27 octobre 2019	25 octobre 2019	PM	Décret	Toute administration
<i>Commentaire : Ce décret définit le système d'information de l'État placé sous la responsabilité du Premier ministre ainsi que les attributions de la direction interministérielle du numérique (DINUM). Il introduit l'examen pour avis conforme (article 3) des projets de SI importants (montant prévisionnel global actuellement fixé à 9M€ par arrêté du 5 juin 2020 publié au JO du 26 juillet 2020). Les systèmes opérationnels et de communication et les systèmes d'information scientifiques et techniques n'entrent pas dans le cadre du champ de ce décret, de même que les systèmes comportant des supports ou informations classifiés qui restent sous la responsabilité des ministères concernés.</i>				
Arrêté du 5 juin pour l'application de l'article 3 du décret n°2019-1088 du 25 octobre 2019 (cf. ci-dessus) publié au JO du 26 juillet 2020	5 juin 2020	PM	Arrêté	Toute administration
Directive DGSIC n°37 relative au traitement d'un dossier éligible à l'article 3 du décret n°2014-879 du 1er août 2014 relatif au système d'information et de communication de l'État modifié par le décret 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique.	8 février 2016	DGSIC	Directive	MinArm
<i>Commentaire : cette directive qui doit être réactualisée décrit le contenu du dossier qu'il convient de constituer pour l'avis de conformité en DINUM et les modalités de traitement de ce dossier au niveau du MinArm.</i>				
Circulaire n° 6404-SG relative à la doctrine d'utilisation de l'informatique en nuage par l'État	31 mai 2023	PM	Circulaire	Toute administration
Doctrine "Cloud au Centre" et offre Office 365 de Microsoft diffusée par note DINUM-DIR-210901 du 15 septembre 2021	15 septembre 2021	DINUM	Note	Toute administration

2.2.2 Politique de la donnée - Logiciels Libres – ouverture des codes

Document	Date	Origine	Type doc	Portée
Circulaire n°6264/SG relative à la politique publique de la donnée, des algorithmes et des codes sources	27 avril 2021	PM	Circulaire	Toute administration
<i>Commentaire : La circulaire met en œuvre une politique publique de la donnée :</i>				
<ul style="list-style-type: none"> • <i>constituant une priorité stratégique de l'État dans ses relations avec tous ses partenaires, en particulier les collectivités territoriales, et dont le suivi sera assuré par des RIM régulières (RIM de suivi, RIM transverses, RIM thématiques, dites « Bothorel »)</i> 				

Document	Date	Origine	Type doc	Portée
<ul style="list-style-type: none"> une orientation marquée sur l'ouverture et la transparence des informations publiques, avec un axe sur le partage des données entre administrations avec une gouvernance à la main de l'administrateur général des données (AGD) et des administrateurs ministériels (AMD) dont le périmètre de responsabilités est désormais étendu aux algorithmes et aux codes sources (ex : création du Comité Interministériel des AMDAC – CIAD)) <p>La circulaire fixe un ensemble d'actions à la charge des ministères et pose des axes stratégiques pilotés au niveau interministériel, et qui seront à décliner par chaque ministère</p> <ul style="list-style-type: none"> Désignation d'un AMDAC (15 mai) Élaboration et publication d'une feuille de route (15 juillet – 15 septembre 2021) Gratuité totale des données publiques d'ici 2023 				
Article L. 311-5 du code des relations entre le public et l'administration modifié par ordonnance n°2016-1360 du 13 octobre 2016 art 51	13 octobre 2016	PM	Loi	Toute administration
Commentaire : cet article permet de limiter l'accès aux documents administratifs dont la consultation ou la communication porterait atteinte notamment au secret de la défense nationale ou à la sécurité des systèmes d'information des administrations.				
Politique ministérielle des données édition approuvée le 05/04/2022 diffusée par la note n°117/ARM/DGNUM/DG/NP du 5/04/2022	5 Avril 2022		Politique	MinArm
Commentaire : La politique ministérielle des données définit le cadre pour la valorisation des données du ministère (elle a vocation à être déclinée par les grands subordonnées et les organismes rattachés au ministre), en précisant :				
<ul style="list-style-type: none"> la vision à long terme du ministère sur la valorisation des données ; 6 principes directeurs (s'appliquant aux organisations comme aux produits en projet et en exploitation/production) : Valeur, Partage, Efficience, Maîtrise en sécurité, Gouvernance et Acculturation ; 21 ambitions déclinant les principes directeurs (précisant les objectifs à atteindre pour chaque principe) ; des rôles à instancier par les états-majors, directions et services du ministère (directeur des données, directeur des données délégué, administrateur des données de zone fonctionnelle, architecte de données, référent métier) ; Des instances de décision et d'animation (Comité des Administrateurs des données de la défense (CADD), Forum ministériel des données (FMD), Commission ministérielle des données (CMD)). 				
Orientations pour l'usage des logiciels libres dans l'administration : circulaire du Premier ministre adressée le 19 septembre 2012 à tous les ministères.	19 sept. 2012	PM	Circulaire	Toute administration
Commentaire : cette circulaire précise les contextes d'usage des logiciels libres favorables au sein de l'administration, décrit l'organisation et les objectifs des instances « logiciel libre » interministérielles (sous l'égide de la DINUM (ex-DINSIC)), incite les ministères à contribuer à cet effort et préconise de considérer désormais le logiciel libre à égalité avec les autres solutions pour répondre aux besoins métiers.				
Conseils à la rédaction de clauses de propriété intellectuelle pour les marchés de développement et de maintenance de logiciels libres	26 fév. 2014	DINSIC	Guide	Toute administration
Commentaire : Ce guide pratique à destination des administrations a été élaboré sous l'égide de la DINSIC par un groupe de travail regroupant le SAE et diverses administrations de l'état pour faciliter la rédaction des cahiers des charges (notamment les CCAG-TIC) permettant de couvrir des marchés de :				
<ul style="list-style-type: none"> - maintenance corrective et adaptative portant sur un logiciel libre ; - maintenance évolutive portant sur un logiciel libre ; - développement de logiciels spécifiques destinés à être mis à disposition de tiers par l'administration sous un régime de licence de logiciel libre. https://www.economie.gouv.fr/apie/actualites/conseils-redaction-clauses-propriete-intellectuelle				
Politique de contribution aux logiciels libres de l'État	15 février 2018	DINSIC	Politique	Toute administration
Commentaire : cette politique publiée provisoirement sur le site github de la DINSIC (https://www.numerique.gouv.fr/publications/politique-logiciel-libre/) a été validée par l'ensemble des DSIs des administrations le 15 février 2018. Elle précise :				
<ul style="list-style-type: none"> - les règles et principes à respecter pour l'ouverture des codes sources - les bonnes pratiques à respecter par les ministères 				

Document	Date	Origine	Type doc	Portée
<p>- la gouvernance des politiques de contribution de l'État.</p> <p>Sont concernés l'ensemble des <u>nouveaux</u> développements de codes sources développés soit en interne soit pour le compte d'une administration dans le cadre du système d'information de l'État tel que défini par le décret du 1^{er} août 2014 n°2014-879 relatif au système d'information et de communication de l'État (cf. 2.2.1)</p>				

Offre de services en matières de logiciels libres : cf 2.2.4.2

2.2.3 Les référentiels interministériels

2.2.3.1 Référentiels généraux (RGI, RGS, RGAA, R2GA, RGESN)

Il s'agit des référentiels touchant à l'interopérabilité, la sécurité, l'accessibilité, l'archivage et l'écoconception.

Document	Date	Origine	Type doc	Portée
Interopérabilité				
Référentiel Général d'Interopérabilité [RGI] V2 approuvé par arrêté du Premier ministre du 20 avril 2016	20 avril 2016	DINSIC	/Arrêté	Toute administration
<p><i>Commentaire : règles d'interopérabilité (format, protocoles, encodages, ...) rentrant dans le champ d'application de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.</i></p> <p><i>Sous pilotage de la DINSIC, cette version a été co-construite par les DSI des administrations centrales et a fait l'objet d'un appel à commentaires auquel le ministère a contribué en 2015.</i></p> <p><i>La version de référence est publiée sur le site de modernisation de la vie publique http://references.modernisation.gouv.fr/interoperabilite.</i></p> <p><i>Par rapport au RGI V1, cette version permet d'actualiser sous une forme claire et ramassée la liste de formats d'interopérabilité retenus, et introduit la notion de profils d'interopérabilité correspondant à des cas d'usage : le profil d'interopérabilité État Plateforme est notamment mis en exergue.</i></p>				
Sécurité				
Référentiel Général de Sécurité [RGS] V2.0 du 13 juin 2014 approuvé par arrêté du Premier ministre du 13 juin 2014	13 juin 2014	PM	Arrêté	Toute administration

Document	Date	Origine	Type doc	Portée
<i>Commentaire : le RGS précise des règles de sécurité s'imposant aux autorités administratives dans la sécurisation de leur SI et notamment sur les dispositifs de sécurité relatifs aux mécanismes cryptographiques et à l'utilisation de certificats électroniques et contremarques de temps. Le RGS propose également des bonnes pratiques en matière de SSI.</i>				
<i>Le RGS découle de l'application de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.</i>				
<i>Une évolution est prévue pour assurer une meilleure articulation du RGS vers le règlement européen eIDAS</i>				
<i>Le RGS V2 (https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents) est constitué :</i>				
- d'un corps principal				
- de 5 annexes relatives à l'utilisation de certificats électroniques :				
- RGS A1 : règles de mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques ;				
- RGS A2 : politique de certification type « certificats personne » ;				
- RGS A3 : politique de certification type « services applicatifs » ;				
- RGS A4 : profils de certificats, CRL, OCSP et algorithmes cryptographiques ;				
- RG A5 : politique d'horodatage ;				
- de 3 annexes relatives à l'utilisation de mécanismes cryptographiques (RGS B1 à B3) :				
- RGS B1 : règles concernant le choix et le dimensionnement des mécanismes cryptographiques ;				
- RGS B2 : règles concernant la gestion des clés utilisées dans des mécanismes cryptographiques ;				
- RGS B3 : règles concernant les mécanismes d'authentification ;				
- d'une annexe relative aux prestataires d'audits SSI (RGS C) :				
- RGS C : référentiel d'exigences applicables aux prestataires d'audits SSI.				
Accessibilité				
Décret n°2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne	24 juillet 2019	PM	Décret	Toute administration
<i>Commentaire : le décret détermine les obligations relatives à l'accessibilité des services de communication au public en ligne aux personnes handicapées, comprenant les applications mobiles et le mobilier urbain numérique, à mettre en œuvre selon un référentiel d'accessibilité. Il précise les modalités de mise en œuvre (déclaration d'accessibilité, procédures, sanctions applicables, exemptions)...</i>				
Référentiel Général d'Amélioration de l'Accessibilité [RGAA] V 4.1	mis à jour 16 février 2021	DINUM	Arrêté	Toute administration
<i>Commentaire : ce référentiel, anciennement Référentiel Général de l'Accessibilité pour les administrations, découle de l'article 47 de la loi n°2005-102 du 11 février 2005 sur l'égalité des droits et des changes, la participation et la citoyenneté des personnes handicapées.</i>				
<i>Cette version est structurée en 2 parties. La première présente les obligations à respecter : elle s'adresse aux juristes, aux gestionnaires et à tous les professionnels du web et de l'accessibilité. La deuxième contient une liste de critères pour vérifier la conformité d'une page web : elle s'adresse aux auditeurs RGAA. Cette version est accessible en ligne : https://www.numerique.gouv.fr/publications/rgaa-accessibilite/</i>				
Archivage				
Référentiel Général de Gestion des Archives [R2GA] publié par le comité interministériel aux Archives de France	Octobre 2013	PM	Référentiel	Toute administration
<i>Commentaire : ce référentiel précise les notions relatives à l'archivage, le périmètre, et les règles précises découlant du livre II du code du patrimoine. Ce référentiel publié sous l'égide du comité interministériel aux archives de France (CIAF) est le fruit d'un travail piloté par le ministère de la culture en étroite collaboration avec les directions des archives des ministères en charge de la Défense et des Affaires étrangères.</i>				
<i>Voir également corpus lié à l'archivage §3.2.7.4 Archivage</i>				
Ecoconception				

Document	Date	Origine	Type doc	Portée
Référentiel général d'écoconception de service numérique [RGESN] (version beta)	A venir	PM	Référentiel	Toute administration
<p><i>Commentaire : Le référentiel général d'écoconception de service numérique (RGESN) est un document interministériel édité par la direction interministérielle du numérique (DINUM).</i></p> <p><i>Dans une perspective de sobriété numérique, le RGESN présente une grille d'analyse qui s'applique aux SI dans leur phase de développement, dès la phase d'idéation. Les objectifs poursuivis à travers cette approche sont de mettre en service, in fine, un SI qui consomme moins de ressources informatiques et énergétiques et des équipements dont l'obsolescence est retardée, qu'il s'agisse des équipements utilisateurs ou des équipements réseau ou serveur.</i></p> <p><i>L'écoconception des services numériques n'est pas uniquement une recherche d'optimisation, d'efficience ou de performance mais une réflexion plus globale sur l'usage des technologies. Il est important d'intégrer les impacts environnementaux du numérique dans la conception des services numériques en visant directement ou indirectement à allonger la durée des vies des équipements numériques, à réduire la consommation de ressources informatiques et énergétiques des terminaux, des réseaux et des centres de données.</i></p> <p><i>Le RGESN est accessible via https://ecoresponsable.numerique.gouv.fr/publications/</i></p>				

2.2.3.2 Communication gouvernementale - Charte Internet de l'État – Charte graphique

Document	Date	Origine	Type doc	Portée
Internet de l'état : circulaire du Premier ministre n°5574/SGG du 16 février 2012	16 février 2012	PM	Circulaire	Toute administration Internet
<p><i>Commentaire : cette circulaire contient notamment :</i></p> <ul style="list-style-type: none"> - <i>Une charte de l'internet applicable à tous les sites des administrations centrales et des services déconcentrés de l'état</i> - <i>Les procédures d'agrément auxquelles tout projet Internet et numériques de l'État, en refonte ou en création doit se plier et ce quelle que soit l'extension du nom de domaine concerné (.gouv, .org, .com, .fr...).</i> 				
Communication gouvernementale : circulaire du Premier ministre n°6120/SG du 14 octobre 2019 relative l'organisation et la coordination de la communication gouvernementale	14 octobre 2019	PM	Circulaire	Toute administration Internet
<p><i>Commentaire : cette circulaire renforce le pilotage de la communication gouvernementale par le SIG (Service d'Information du Gouvernement) sur 3 axes :</i></p> <ul style="list-style-type: none"> - <i>le respect des procédures de demande d'agrément (opération de communication, site internet, réseaux sociaux...)</i> ; - <i>les actions relatives à l'analyse de l'opinion</i> ; - <i>la planification des actions de communication.</i> 				
Charte graphique : circulaire du Premier ministre n°6144/SG du 17 février 2020 relative à la nouvelle stratégie de marque de l'État.	17 février 2020	PM	Circulaire	Toute administration Internet
<p><i>Commentaire : cette stratégie se décline en 3 modalités :</i></p> <p><i>Une charte graphique ;</i></p> <p><i>Une charte des grands principes rédactionnels ;</i></p> <p><i>Une charte des réseaux sociaux.</i></p> <p><i>Ces documents sont accessibles sous : https://www.gouvernement.fr/marque-Etat</i></p>				

2.2.4 Les outils et l'offre de service au niveau interministériel

2.2.4.1 L'offre de services communs

Des travaux engagés depuis plusieurs années sous l'égide de la DINUM, ont donné lieu à des réalisations, des offres de service ou des projets encore en cours parmi lesquels :

- le réseau interministériel de l'état (RIE) ;
- la transformation des centres informatiques ;
- le socle interministériel des logiciels libres (SILL) ;
- la démarche open.data.gouv.fr : relative à l'ouverture des données de l'état ;
- la démarche d'API donnant lieu à un portail de publication des API ;
- la démarche FranceConnect dont une des principales réalisations est FranceConnect, permettant l'authentification des particuliers (voir description) ; les composants AgentConnect en déploiement sur le RIE peuvent être étudiés alors que ProConnect n'est qu'à envisager ultérieurement ; Le dispositif FranceConnect est désormais renforcé par l'usage de la carte nationale d'identité électronique (Décret SGIN du 22 avril 2022).
- la solution de messagerie instantanée interministérielle Tchap ;
- le service de « démarches simplifiées » ;
- des nouveaux outils collaboratifs pour les agents de l'Etat permettant d'aider au télétravail (<https://www.numerique.gouv.fr/outils-agents>) : webconference, audioconference, et en complément le Webinaire de l'état, plateforme collaborative Resana, plateforme des communautés professionnelles de l'État Osmose.

2.2.4.2 Le socle de logiciels libres SILL – Marché de support LL

Attention : la présence d'un logiciel dans ce socle ne présuppose pas de son acceptabilité sur les réseaux du Ministère.

Document	Date	Origine	Type doc	Portée
Socle interministériel de logiciels libres (SILL)	mise à jour en continu	DINUM	Référentiel	Toute administration

Commentaire : ce catalogue constitue un référentiel de logiciels libres préconisés au niveau interministériel et couvrant, dans sa version actuelle, le poste de travail, la gestion de parc, l'exploitation de serveurs, les bases de données, les environnements de virtualisation et les environnements de développement. Chaque logiciel du SILL est suivi par un ministère référent. Le SILL fait désormais l'objet d'une actualisation en continu consultable sur le site web : <https://catalogue.numerique.gouv.fr/catalogue>.

2.2.4.3 Les données ouvertes

L'utilisation des données ouvertes exposées sur Internet doit tenir compte des principes suivants :

- Pour les données de référence, le recours à l'utilisation d'une donnée ouverte n'est autorisé que si celle-ci n'est pas déjà exposée au sein du ministère par la zone fonctionnelle en ayant la responsabilité. En effet, la donnée de référence peut déjà être consommable au sein du ministère, soit par reprise de la donnée ouverte ainsi exposée de manière synchronisée à l'ensemble des SI, soit par exposition de la donnée par un abonnement auprès de la source officielle (cet abonnement apportant

un enrichissement vis-à-vis de la donnée ouverte).

- Pour les données de production, il est préconisé de s'assurer en amont, qu'un contrat de service puisse être établi avec la source des données, certains jeux de données ne faisant pas l'objet de mises à jour dans le temps.

2.2.4.4 Conception de site Internet

Dans sa mission de « pilote de la transformation digitale de la communication gouvernementale », et dans la lignée de la charte graphique de l'État, le Service d'information du Gouvernement [SIG] met à disposition sous le vocable de « Système de Design » (Design System) un ensemble de composants réutilisables, répondant à des standards et à une gouvernance, pouvant être assemblés pour créer des sites Internet accessibles et ergonomiques.

Le système de design est accessible sous <https://www.systeme-de-design.gouv.fr>.

2.3 Le cadre ministériel

Les références suivantes ne sont pas uniquement techniques mais sont nécessaires à la compréhension du cadre général global des SIC du ministère, sans pour autant le décrire de façon exhaustive.

2.3.1 Politique SIC ambition numérique

Document	Date	Origine	Type doc	Portée
Instruction ministérielle n°2476 CC6 IM SIC du 29 avril 2019	29 avril 2019	DGSIC	Politique	MinArm
<i>Commentaire : Cette politique vise à fixer les grandes orientations capacitaire déclinées en une feuille de route à 5 ans.</i>				
Ambition numérique du ministère des armées approuvée par le ministre le 30 novembre 2017 et diffusée par note n° 490/ARM/DGSIC/DG/NP du 11 décembre 2017)	30 nov.2017	Ministre	Politique	MinArm
<i>Commentaire : Ce document définit une approche globale et cohérente de la transformation numérique du ministère des armées, en cohérence avec le chantier « Transformation numérique de l'État » de la démarche « Action publique 2022 », lancé par le Premier Ministre le vendredi 13 octobre 2017</i>				
Schéma directeur de la transformation numérique volet stratégique approuvée par le ministre et diffusée sous timbre n°735/ARM/DGSIC/DG/NP du 19 avril 2018	19 avril 2018	CEMA, DGA, SGA, DGSIC	Politique	MinArm
<i>Commentaire : ce document décline en grands chantiers l'ambition numérique du ministère. Il doit être complété par des feuilles de route plus précises qui formeront le volet opérationnel du schéma directeur</i>				

Dans le cadre de la transformation numérique du ministère, certaines opérations phare sont de nature à contribuer à enrichir le cadre technique du ministère et à asseoir la notion de socle ministériel numérique mutualisé (C1NP/C1DR/PICSEL, INA, Artemis.IA, SI Connect@ero, SCORPION, Axonav, ...).

2.3.2 Architecture générale, politique logicielle

Document	Date	Origine	Type doc	Portée
Politique générale sur le logiciel au ministère des Armées diffusée par note n°44/ARM/DGNUM/DG/NP du 11 février 2019	8 février 2019	DGNUM	Politique	MinArm

*Commentaire : cette politique remplace la directive DGSIC n°1 portant sur les logiciels du 17 octobre 2006
Dans le contexte de transformation numérique de l'État et du ministère, elle réactualise sa politique sur le logiciel, autour de 3 principes majeurs (architecture modulaire orientée services, standardisation des échanges, indépendance vis-à-vis de l'infrastructure sous-jacente), et 9 objectifs (dont recours aux standards ouverts, souveraineté, diminution des adhérences, rationalisation des choix, partage et réutilisation, architecture modulaire, principes d'APIsation).*

Dossier de définition d'architecture des intranets du SIA (v2.01)	04 juin 2019	DGA	Dossier d'architectur e	S-SF FrOpS Instances DR projetable s
---	--------------	-----	-------------------------	---

Commentaire : Ce dossier décrit les principes d'architecture retenus au titre des travaux sur les intranets concernés par le programme SIA. Il constitue le dossier de définition de l'architecture des Intranets, présente la vue générale cible de l'architecture des Intranets dans le cadre du SIA.

2.3.3 Socle numérique

Vision du socle numérique ministériel mutualisé 2025-2030 : Cf. §2.3.1 Politique SIC ambition numérique

Feuille de route du socle pour la modernisation des réseaux : Cf. §5.2 Réseaux

Schéma directeur du socle pour l'hébergement/cloud diffusée : cf. §6.1 Plateformes d'hébergement

Note portant organisation du pilotage du socle numérique : cf. §2.3.6 Gouvernance

2.3.4 SIC opérationnels – FrOpS

2.3.4.1 Politique et concepts d'emploi

Document	Date	Origine	Type doc	Portée
Note n°508/DEF/EMA/PAC/NP relative à la politique des armées en matière de sensibilité des informations opérationnelles	9 juin 2009	EMA	Note	Armées
Doctrine Interarmées relative aux SIC en opération : DIA-6_SI-OPS (2020) sous timbre n°138/ARM/CICDE/NP du 16 décembre 2020	16 décembre 2020	CICDE	Doctrine	MinArm
<i>Commentaire : Ce document précise les principes et l'emploi des SIC dans la conduite des opérations. Il présente les grands principes des SIC et définit les différents niveaux de responsabilité dans la conception, la mise en œuvre et la conduite des SIC, enfin il présente l'emploi des SIC en opération.</i>				

2.3.4.2 COTS OTAN / SIC Multinationaux

La liste des SI et COTS OTAN est entretenue et actualisée par EMA/SNA. La liste exhaustive des piles OTAN est toujours tenue à jour par l'agence NCIA. Les détails sont à demander auprès des RSIO.

De même l'EMA/SNA identifie et répertorie tous les besoins et les synoptiques de raccordements pour les SIC multinationaux (OTAN, Européens, bilatéraux ou multilatéraux).

Document	Date	Origine	Type doc	Portée
SI/COTS OTAN – Gouvernance et plan pluriannuel à cinq ans, diffusé par note n°D-21-003071/ARM/EMA/MGA/SNA/NP du 10 juin 2021	10 juin 2021	EMA	Note	MinArm
<i>Commentaire : Cette note liste les principaux produits (SI/COTS) livrés par l'agence NCIA pour la réalisation des activités opérationnelles en contexte national ou multinational</i>				

2.3.5 Sécurité

Pour une meilleure cohérence du document, l'ensemble des références relatives à la sécurité sont regroupées au chapitre associé (cf 4.1).

2.3.6 Gouvernance

Dans le cadre des comités exécutifs (COMEX) ministériels¹⁴ de 2020 et 2021, une nouvelle organisation de la conduite et du suivi des projets numériques a été décidée. Elle s'appuie sur :

- DSIs TRANSVERSES A VOCATION MINISTERIELLE :
 - DSIs Groupe (DGNUM),
 - DSIs Socle (DIRISI), DSIs Cyber (COMCYBER) ;
- 17 DSIs Domaines (dont 11 relevant du périmètre EMA, 4 du périmètre du SGA, 1 du périmètre DGA et 1 de celui de la DRSD) ;
- Responsables de segments : EMA/SNA, SGA/DTPM, DGA/S2NA ;
- l'Agence du numérique de défense (DGA/AND).

Pour accompagner la mise en place des DSIs, un guide relatif aux missions d'une DSIs Domaine a été émis par la note n° 443/ARM/DGNUM/DG/NP du 9 novembre 2021.

La mise en place de cette nouvelle organisation s'est accompagnée d'une rénovation de la gouvernance numérique, notamment par la publication de deux textes structurants en 2022 :

- l'arrêté du 9 septembre 2022 portant création et organisation d'instances relatives au système d'information et de communication de la défense,
- l'instruction n° ARM/CAB du 9 septembre 2022 fixant la gouvernance ministérielle du numérique et des systèmes d'information et de communication.

La gouvernance ministérielle du numérique et des SIC s'appuie sur :

- les instances de gouvernance générale :
 - la gouvernance des segments (CSIOC, CS3E, CSIAG¹⁵) ;
 - la gouvernance du socle avec le COF¹⁶ ;
- les instances de gouvernance thématique :
 - la gouvernance des fréquences avec la CMF¹⁷ ;
 - la gouvernance de l'urbanisation - avec la commission ministérielle d'urbanisation et le

¹⁴ Cf. comités exécutifs ministériels du numérique des 17 juillet 2020, 27 novembre 2020 et 17 novembre 2021.

¹⁵ CSIOC : commission des systèmes d'information opérationnels et de communication ; CS3E : commission des systèmes d'expertise, essais et expérimentations ; CSIAG : commission des systèmes d'information, d'administration et de gestion.

¹⁶ COF : Comité d'orientation fonctionnel.

¹⁷ CMF : Commission ministérielle des fréquences.

- comité ministériel d'urbanisation ;
- la gouvernance de l'architecture technique avec le SC²A¹⁸ ;
 - la gouvernance des données avec la CMD¹⁹.

L'instruction fixant la gouvernance ministérielle du numérique et des SIC définit les jalons de gouvernance (de J0 à J6), en tant que modalités d'examen des projets et systèmes.

Les visuels suivants illustrent le cycle de vie d'un projet SIC :

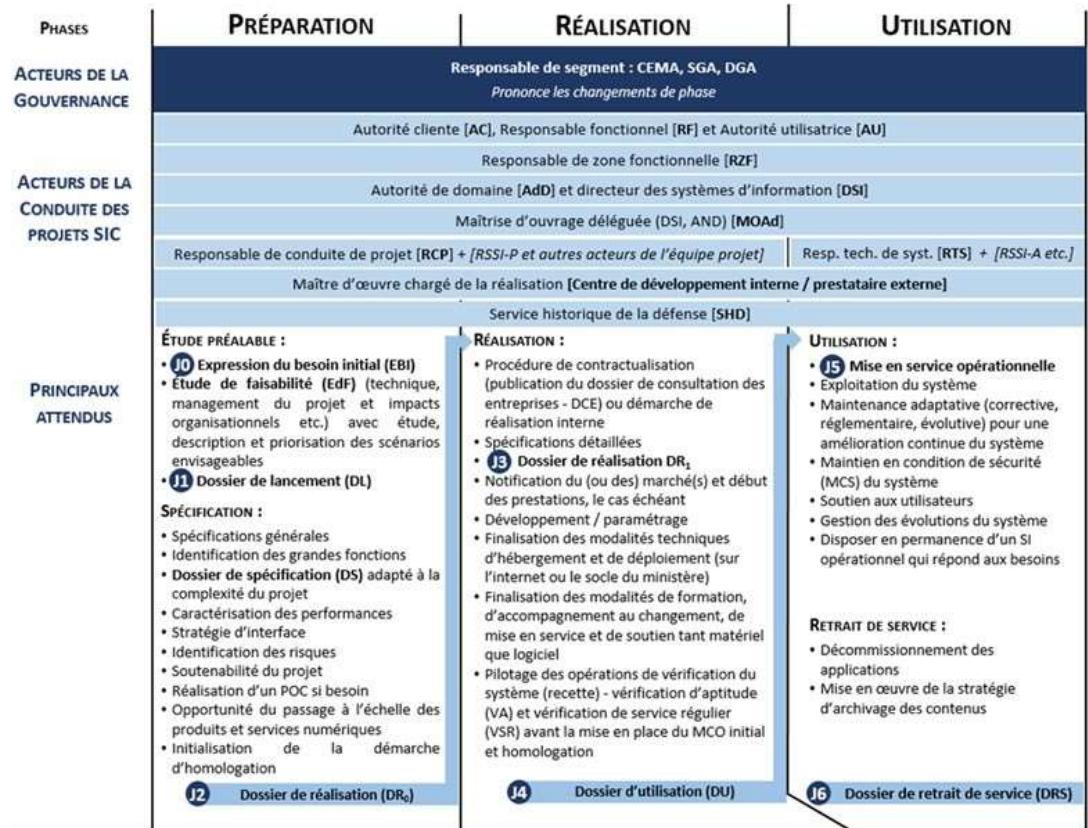


Figure 1 : Cycle de vie d'un projet SIC

Document	Date	Origine	Type doc	Portée
Décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication	28 juin 2018	MinArm	Décret	Toute administration
<i>Commentaire : Ce décret destiné à renforcer la cohérence globale des SIC crée la DGNUM, direction succédant à la DGSI avec des attributions élargies.</i>				
Arrêté du 28 juin 2018 portant organisation de la DGNUM	25/01/2023	MinArm	Arrêté	Toute administration

¹⁸ SC²A : Sous-comité de cohérence des architectures.

¹⁹ CMD : Commission ministérielle des données.

Document	Date	Origine	Type doc	Portée
<i>Commentaire : Cet arrêté définit les conditions dans lesquels l'article 5 du précédent décret s'applique (avis obligatoire du DGNUM pour tout SI à fort enjeu ministériel ou dont le montant est supérieur à 5M €). Il est actuellement en cours de modification (publication annoncée d'ici T4 2022).</i>				
Arrêté du 23 avril 2021 portant création de l'agence du numérique de Défense (AND)	23 avril 2021	MinArm	Arrêté	MinArm
Arrêté du 9 septembre 2022 portant création et organisation d'instances relatives au système d'information et de communication de la défense et publié au BOA	9 septembre 2022	MinArm	Arrêté	MinArm
<i>Commentaire : Cet arrêté introduit les segments SIOC, SIST et SIAG selon une définition fonctionnelle. Le segment SIOC comprend le socle numérique ministériel mutualisé, conçu et opéré au bénéfice des trois segments. Il définit les instances de gouvernance SIC de haut niveau du ministère (CNUM conseil du numérique et des SIC, CECNUM comité exécutif du conseil du numérique et des SIC, CSIOC, CS3E, CSIAG¹⁵, COF¹⁶).</i>				
Instruction du 9 septembre 2022 fixant la gouvernance ministérielle du numérique et des SIC et publiée au BOA	9 septembre 2022	Ministre	Instruction	MinArm
<i>Commentaire : Cette instruction décrit les rôles et responsabilités de gouvernance des acteurs de l'écosystème numérique et SIC au MINARM, définit les instances de gouvernance et traite de l'examen des projets et systèmes (articulation avec le capacitaire ; modalités d'examen des projets et systèmes introduisant les jalons de gouvernance). Il existe des instances de gouvernance générale (gouvernance des segments ; gouvernance du socle numérique ministériel mutualisé), et d'autres de gouvernance thématique (gouvernance des fréquences avec la CMF17 ; la gouvernance de l'urbanisation - avec la commission ministérielle d'urbanisation - et de l'architecture technique avec le SC²A ; la gouvernance des données avec la CMD19).</i>				
Directive DGNUM N° 43 portant sur la gouvernance et la conduite du socle numérique du ministère : diffusée par note n° 111/ARM/DGNUM/DG du 28 mars 2019	27 mars 2019	DGNUM	Directive	MinArm
<i>Commentaire : Cette directive définit les modes de gouvernance et les rôles et responsabilités des différents acteurs du ministère en matière de gouvernance et de conduite des projets relevant du périmètre du socle numérique. Cette directive instaure trois comités en charge des orientations fonctionnelles, de la sécurité et de l'architecture technique des services du socle du numérique. Cette directive a été complétée par l'arrêté du 9 septembre 2022 portant création et organisation d'instances relatives au SIC de la défense et son IM d'application, l'IM fixant la gouvernance ministérielle du numérique.</i>				
Mandat relatif au sous-comité de cohérence des architectures du ministère (SC²A) diffusé par note n° 252/ARM/DGNUM/DG/NP du 7 juillet 2020	7 juillet 2020	DGNUM	Note	MinArm
Mandat provisoire du comité d'orientation fonctionnel (COF) du socle numérique diffusé en annexe de la note n°397/ARM/DGNUM/DG/NP du 02 novembre 2020	02 novembre 2020	DGNUM	Note	MinArm
Guide relatif aux missions d'une DSU Domaine diffusé par la note n° 443/ARM/DGNUM/DG/NP du 9 novembre 2021	9 novembre 2021	DGNUM	Guide	MinArm
<i>Commentaire : Les principales missions d'une DSU Domaine se structurent autour de quatre « grands axes » :</i> <i>- Axe 1 : Stratégie et pilotage</i> <i>- Axe 2 : Architecture et données</i> <i>- Axe 3 : Sécurité du numérique et protection des données</i> <i>- Axe 4 : Conduite de projets et appui aux SIC en service du portefeuille</i>				
Mémento « Présentation des grands principes de gouvernance et de conduite de projet SIC au MINARM »	28/11/2022	DGNUM	Mémento	MinArm
<i>Commentaire : Document destiné à toute personne (autorité, acteur d'un projet...) souhaitant disposer d'une vision d'ensemble de la gouvernance et de la conduite de projet SIC au MINARM. Il s'adresse notamment aux équipes dont les projets et SIC en service sont régis par l'IM n° 2476 portant sur la conduite des projets de SIC</i>				
IM n°2476 ARM/CAB portant sur la conduite des projets SIC diffusée par courrier n°002476/ARM/CC6/NP du 29 avril 2019	29 avril 2019	Ministre	Instruction	MinArm

Document	Date	Origine	Type doc	Portée
<i>Commentaire : cette instruction définit les modalités de conduite, de vérification, de contrôle et d'approbation des projets SIC du ministère hors opération d'armement. Le processus s'articule autour de trois phases : préparation, réalisation et utilisation.</i>				
<i>Cette instruction ministérielle doit faire l'objet d'une déclinaison au travers d'un guide. Elle abroge les IM 2007 de 2014 et 2008 de 2013.</i>				
IM n°1618/ARM/CAB sur les déroulement des programmes d'armement	15 février 2019	Ministre	Iinstruction	SIOC Programme
<i>Commentaire : Cette instruction qui abroge l'ancienne instruction 1516 décrit l'ensemble du processus de conduite d'un programme d'armement autour de 3 phases : préparation, réalisation, et utilisation.</i>				
<i>Cette instruction s'accompagne d'un guide d'application de cette nouvelle instruction.</i>				
IM provisoire n°1/ARM/DGNUM portant sur la conduite agile des services et produits digitaux approuvée le 5 octobre 2018	5 octobre 2018	DGNUM	Instruction	MinArm
<i>Commentaire : L'instruction ambitionne d'apporter un cadre souple aux porteurs d'initiatives digitales afin de leur permettre d'éprouver une nouvelle méthodologie de conduite de projets, incrémentale et intégrant le droit à l'échec. Le parcours s'articule en trois phases : idéation, incubation, et développement de PMV (produits minimum viables). À l'issue, si une décision de passage à l'échelle est prise, les PMV intègrent le processus de conduite normale de projets SIC.</i>				

Document	Date	Origine	Type doc	Portée
Note portant organisation du pilotage du socle numérique n° 407060/ARM/DIRISI/SP/DIS SOCLE/NP	13/12/2022	DIRISI	Note	MinArm
<i>Commentaire : ce document est publié sur la communauté de travail de la DSI Socle Numérique.</i>				

2.3.6.1 Outils de gouvernance

2.3.6.1.1 Gestion du patrimoine

SICLADE : l'outil de gestion du portefeuille ministériel applicatif

Tout système d'information, tout équipement comportant au moins un logiciel doit obligatoirement être enrôlé dès son initialisation dans l'outil SICLADE DR ou SICLADE Secret (pour les systèmes de niveaux S et TS). Cela permet d'initialiser son processus d'homologation, de recensement, au besoin de rattachement budgétaire et, le cas échéant, de permettre de constituer son dossier d'hébergement par la DIRISI.

Cet enrôlement se décompose à minima en une fiche SICLADE, voire une fiche de traitement en cas de manipulation de données à caractère personnel, pour le RGPD.

Le registre de traitement du MinARM (article 30 du RGPD) est produit à partir de SICLADE. L'instance SICLADE Secret sera aussi utilisée dans le cadre de l'élaboration de la cartographie ministérielle de Cybersécurité. Pour de plus amples informations, se référer à SYNOPTIC.

Document	Date	Origine	Type doc	Portée
Directive d'emploi de SICLADE	2024	DGNUM	Note	MinArm
<i>Commentaire : La directive d'emploi permettra de définir précisément l'emploi de l'outil de gestion du portefeuille applicatif du ministère.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion de patrimoine	SICLADE Version en vigueur sur Intradef	Minarm	Outil de gestion de portefeuille applicatif du ministère	R / S	MinArm
Gestion de patrimoine	CAST Highlight	Cast Software	Pour l'observation de la qualité applicative du portefeuille des SI du ministère. Destiné à la gouvernance. Son utilisation est recommandée pour les ZF, DSI et segments. Sont analysés les SI métiers (hors COTS, portails) en production afin d'évaluer les forces et faiblesses potentielles du portefeuille.	R / -	MinArm
Gestion de patrimoine	Diademe	MinArm	CMDB DIRISI	- / S	Intradef

2.3.6.1.2 Gestion du patrimoine – Données

Conformément à la directive n°35/DEF/DGSIC du 11 juin 2015 portant sur la gouvernance de la qualité des données du ministère, les administrateurs de données de zone fonctionnelle (ADD-ZF) tiennent à jour la Cartographie des Objets Métier (COM) précisant les données placées sous la responsabilité des zones fonctionnelles ainsi que la Cartographie des Données de Référence et des Référentiels de Données (CD2RD) précisant les données de référence identifiées au ministère et leurs référentiels de données associés. Ces cartographies, dans leur version en vigueur, sont disponibles sur SynopTIC, univers « Données ».

Cette identification des objets métier et des données de référence, sera complétée de l'identification des données de production au sein des SI, au travers d'un catalogue de données permettant de valoriser l'ensemble des données du ministère par leur recensement auprès de tous les gisements de données, et par l'exposition de ces jeux de données pour consultation par leurs clients potentiels. Cet inventaire centralisé et détaillé des données du ministère permettra de comprendre leur sémantique, leur format, et leur(s) source(s) afin d'identifier rapidement les données pouvant être utilisées dans le cadre de nouveaux cas d'usage exprimés par les métiers.

Ainsi, le ministère se dote du catalogue de données dans le cadre du projet MetadatARM, pour les données NP/DR. Celui-ci est composé :

- d'un glossaire permettant de recenser les données métier, de les définir en termes de sémantique et de partager cette définition ;
- du catalogue de données proprement dit (aussi appelé dictionnaire des données) permettant de lister et de décrire en termes de métadonnées les données existants dans les SI ;
- d'une fonction permettant d'analyser le parcours des données et d'identifier leur transformation.

Ce service commun du socle ministériel est en cours de réalisation dans le cadre de la feuille de route de l'offre de services « données » confiée à l'AND. La perspective calendaire de mise en production de la plateforme cible est une mise en service progressive en 2024.

2.3.7 Relation client – Offre de service - DIADEME

Depuis 2018, la DIRISI a mis en place le système d'information DIADEME (Digitalisation Intégrée et Agile pour une DIRISI évolutive et modernisée) qui s'enrichit chaque année de nouveaux services.

Pour les clients de la DIRISI, DIADEME est l'accès unique et fédéré au catalogue de services de la DIRISI contenant :

- l'ensemble de l'offre de services de l'opérateur ;
- le DIRISI-store, magasin de logiciels librement installables sur Intradef ;
- les articles et la documentation stockée dans les espaces professionnels des bases de connaissances DIADEME ;
- la déclaration des incidents de production comme cyber (en remplacement du formulaire FOURMI) et aux réclamations dans le cas de non résolution ;
- le suivi des demandes dont les formulaires ont été implémentés ;
- le suivi des demandes professionnelles [FEB] dans le cadre du recueil du besoin et du processus de suivi du plan de charge DIRISI.

Pour l'opérateur DIRISI, DIADEME est l'outil de gestion des services IT de la DIRISI.

3 SERVICES COMMUNS

Les services communs recouvrent l'ensemble des services, hors métiers, nécessaires au fonctionnement du système d'information des armées. Les éléments référentiels ci-dessous précisent les composants de ce socle et fixent un cadre mutualisé permettant aux applications de s'y intégrer.

Le socle technique commun mis en œuvre par la DIRISI apporte les logiciels des serveurs et des postes de travail de l'infrastructure d'intranet (notamment les systèmes d'exploitation et tous les outils associés).

Intranet Secret-SF / FrOpS

Sur l'intranet Secret-SF (ex CD-SF), les services déployés issus des programmes d'armement, de l'opération d'ensemble Intraced, et des services déployés par les armées sont pris en compte dans le cadre du programme SIA. Les services communs déployés sont ceux du SIA S-SF.

La démarche est identique pour l'intranet SIA FrOpS : à terme les services communs déployés seront également ceux de SIA S-SF sur l'ensemble du réseau en métropole.

SIA- S-SF destiné aux théâtres d'opérations et aux bâtiments est en cours de déploiement tous niveaux de confidentialité confondus.

Intradef²

Une refonte de l'Intradef est confiée à la MOA et la DSI Socle et opérée par l'AND dans le double objectif de forte sécurisation et d'adaptation aux évolutions majeures liées à la transformation numérique au sein du ministère.

Par ailleurs, la DIRISI exerce un rôle renforcé d'administrateur technique de l'Intradef.

Intradef-SIE : Sur les bâtiments de la Marine nationale, les services d'usage courant du réseau DR sont prolongés et adaptés aux contraintes apportées par le Segment Intradef Embarqué (SIE), dans la continuité des services de l'« Intramar bateau ». Le SIE version « Baltique » est en service depuis l'été 2021. Le SIE apporte :

- la disponibilité des services communs à bord y compris en mode déconnecté (autonomie) ;
- l'optimisation des échanges sur les réseaux contraints ;
- la gestion des doubles équipages et des états-majors embarqués (embarquement et débarquement).

L'architecture du SIE comprend :

- les infrastructures embarquées et plateformes d'entraînement (CSC) et de formation (Pôle Ecoles Méditerranée) ;
- une infrastructure nationale à terre, hébergée en datacenter et portant notamment la gestion de configuration centralisée des infrastructures et services embarqués et des plateformes;

- des serveurs de bordure à terre, hébergés en datacenter, assurant le relais des services communs (DNS, LDAP, SMTP, NTP, DECOS, etc.) ;
- des services du socle SIE à terre (portails, etc.), hébergés en datacenter, au bénéfice des équipages des bâtiments « en préparation » (à terre) dont les données sont interchangeables avec les services de l'infrastructure embarquée via un support de stockage dédié.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°87 d'exploitation du STC-IA (V0.2) version 2.0 du 30 juin 2013	30 juin 2013	DIRISI	Directive	Intradef
<i>Commentaire : Cette directive décrit l'architecture globale et les principaux services ainsi que les modalités d'exploitation du STC-IA (V0.2) sur l'Intradef. Différents travaux DIRISI (MISHUCO, ...) ont depuis modernisé cette architecture.</i>				
Directive DIRISI n°210 d'exploitation du STC-IA sur Intraced CD-SF version 2.4 du 2 mars 2017	1er mars 2017	DIRISI	Directive	S-SF
<i>Commentaire : Cette directive décrit l'architecture globale et les principaux services ainsi que les modalités d'exploitation du STC-IA sur l'Intraced Secret-SF.</i>				

3.1 Services à l'utilisateur

Ce paragraphe renvoie à des services utilisables par les applications mais également visibles directement par les utilisateurs. Ces services font partie du catalogue de services opérés principalement par la DIRISI.

La gouvernance des services du socle du numérique, est décrite en §2.3.6 **Gouvernance**. La gouvernance des services à l'utilisateur s'est mise en place au travers d'un comité d'orientation fonctionnelle (COF animé par la DGNUM) et d'une gouvernance technique assurée par le SC²A décrits au §1.4 **Gestion et gouvernance du CCT**

3.1.1 Environnement de travail

3.1.1.1 Poste de travail - CCB [SU-PC]

Ce chapitre n'évoque que les postes de travail d'organismes dont le soutien incombe à la DIRISI.

Concept d'emploi : Le service « Poste de travail » décrit par le concept d'emploi « Environnement de travail » définit une offre matérielle et logicielle répondant aux besoins informatiques standards de l'ensemble des utilisateurs du ministère des armées. Il couvre la définition des différents types de matériel/configuration, les outils logiciels nécessaires à la production/consultation de certains formats de fichiers et l'ensemble des dispositifs de base permettant à l'agent de travailler quel que soit son environnement (sur site, en mobilité), en accédant à l'ensemble des ressources, et selon les normes ministérielles de sécurité en vigueur, notamment la politique de sécurité des Intranets.

Matériels - COBALT : l'acquisition, le renouvellement, la configuration ou la réforme du poste de travail sont désormais assurés de façon standardisée au sein du ministère des armées par la DIRISI/SICL. Ce processus couvre tous les postes bureautiques utilisés en France métropolitaine, quel que soit le niveau de classification (NP-DR, Secret, OTAN...), à l'exception des postes dont le soutien n'incombe pas à la DIRISI (programmes d'armement, renseignement, hôpitaux...) et qui bénéficient de services restreints par rapport aux postes standardisés.

L'aspect matériel est géré au travers d'une régie « rationalisée » connue sous le nom de COBALT.

Logiciels – CCB : la DIRISI assure la gestion de configuration des postes et des smartphones de tous les Intranets qu'elle infogère. Pour les réseaux Intradef, SIA S-SF, IntraCed S-SF et SIA FrOps, le comité de configuration bureautique (CCB) présidé par la DIRISI en valide les évolutions, en conformité avec le CCT.

Dans ce contexte, toute création/modification de masters, de logiciels ou d'applications en vue d'un déploiement est instruite par le CCB.

Pour répondre aux contraintes opérationnelles ou aux difficultés techniques, le CCB peut autoriser le déploiement de logiciels en mode manuel (installation par un technicien de la DIRISI). En raison des contraintes de charge, ce cas doit demeurer exceptionnel.

La conception des masters Intradef, SIA S-SF, IntraCed S-SF et SIA FrOps relève de l'AND qui intègre les préconisations de la DGA-MI pour les stratégies de configuration et de sécurité. La réalisation des masters de ces réseaux incombe à la DIRISI qui les télédéploie.



La présence d'un logiciel dans un marché cadre ne présuppose pas de son acceptabilité sur les réseaux opérés par le Ministère. Il est hautement recommandé de s'en assurer avant de procéder à son acquisition. À défaut l'installation pourra être refusée au moment de la demande de déploiement.



Outre les masters, la DIRISI réalise les packages logiciels correspondant :

- à des services communs répondant à un besoin générique ;
- à des besoins « métier » nécessaires à des emplois spécifiques ;
- à des pilotes permettant le bon fonctionnement de périphériques.

Préalablement à leur instruction par la DIRISI, les demandes de réalisation de masters et de logiciels font l'objet d'une validation de leur DSI respective.

Le master Intradef est adapté par la DIRISI aux spécificités embarquées du SIE. Les logiciels validés en CCB et packagés par le CNCI peuvent y être déployés avec les outils spécifiques du SIE dans des conditions spécifiques d'emploi.

Logiciels à licences payantes faisant l'objet d'un contrat cadre : l'offre de logiciels à licences payantes repose essentiellement sur des contrats-cadres gérés par la DIRISI ou par la DGA :

- - marchés multi-éditeurs : Ouranos, UGAP et PROGIST (porté pour ce dernier par la DGA) ;
- - marchés-cadres éditeurs.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°8 définissant les règles à appliquer au système de postes terminaux : directive publiée au Bulletin Officiel des Armées	29 juin 2009	DGSIC	Directive	MinArm
<i>Commentaire : Règles d'usage et d'interopérabilité des postes terminaux du ministère des armées. Périmètre : tous les intranets.</i>				
Concept d'emploi « environnement de travail » : note conjointe : n°6691/DEF/EMA/CPI/AUT/NP / n°1261/DEF/SGA/ADJ	6 juillet 2012 10 juillet 2012	SC1	Concept Emploi	MinArm/ NP/DR
<i>Commentaire : Concept d'emploi "environnement de travail": ce document couvre les notions de poste de travail, de son environnement physique (impression, partage de ressources, accès réseaux, matériels en option), de ses ressources logicielles (bureautique, gestion de fichier, messagerie, navigateur, multimédia,...), de la capacité pour l'utilisateur en fonction de son profil de rechercher et demander des services dans le catalogue de services (D-store) et de l'environnement de sécurité du poste de travail. Il s'applique uniquement au monde NP/DR.</i>				
SLR du service « environnement de travail » : note conjointe : n°1114/DEF/EMA/CPI/AUT/NP / n°201/DEF/SGA/ADJ	26 janvier 2013 29 janvier 2013	SC1	SLR	MinArm/ NP/DR

Document	Date	Origine	Type doc	Portée
<i>Commentaire : SLR relatif au service de l'"environnement de travail"</i>				
EMO.GUI.R4.003 - Constitution et rôle du Comité de Configuration Bureautique (CCB) Directive DIRISI n°151 de gestion des changements et des configurations logicielles sur le poste de travail	12 janvier 2022	DIRISI/SCO E	Directive	MinArm métropole, Intradef, S-SF, SIA FrOps
<i>Commentaire : cette directive précise les modalités de gestion de configuration du poste de travail. Elle précise notamment le processus d'évolution des socles, ainsi que des demandes logicielles, des mises en production et de déploiement.</i>				
Directive DIRISI n°143 relative au maintien en condition de sécurité des postes de l'Intradef du 15 novembre 2015	15 novembre 2015	DIRISI	Directive	Intradef,
<i>Commentaire : cette directive décrit les modalités de maintien en condition de sécurité des postes sur l'Intradef et notamment les processus de préparation et de déploiement des patchs de sécurité</i>				
Directive DIRISI COBALT	30/11/2020	DIRISI/SCO E	Directive	MinArm métropole, Intradef, S-SF FrOpS
<i>Commentaire : Cette directive est un document cadre décrivant la totalité du processus bureautique au sein du ministère des Armées et servant de référence pour en assurer le bon fonctionnement. Elle précise le périmètre, les rôles et modes de fonctionnement du processus bureautique mis en œuvre en déclinaison de COBALT.</i>				

3.1.1.2 Critères d'éligibilité d'un package

L'inéligibilité d'un package du point de vue de la sécurité est déterminée par la mise en évidence d'une des vulnérabilités suivantes (liste non exhaustive) :

- absence de soutien par l'éditeur (notamment au regard du MCS) ; si d'aventure un logiciel packagé ne dispose plus de MCS, alors ce dernier est retiré du déploiement et ne peut plus être demandé en installation même au titre d'un renouvellement du poste (sauf dérogation officielle accordée, pour une durée donnée, par le COMCYBER) ;
- incompatibilité avec le socle technique ou une installation non compatible avec les standards du ministère ;
- initialisation ou fonctionnement nécessitant une connexion Internet (exemple : Internet Sur le poste de travail ISPT) ;
- application fonctionnant en mode serveur (se reporter notamment au chapitre **3.1.1.4 Postes de travail autonomes ou en mode déconnecté**) ;
- installation sur la partition C, en dehors du dossier « Program Files » ou « Program Files(x86) » ;
- application qui, par fonctionnement, nécessite ou crée une élévation de privilège ;
- application ou logiciel qui donne à un utilisateur authentifié des droits à la fois en écriture et en exécution sur un même dossier (règle dite W^X ou W xor X, respect de la règle de moindre privilège) ;
- logiciels de virtualisation, de paravirtualisation ou d'émulation ;
- dépendance d'un SI non enregistré dans SICLADE ou ne disposant pas d'une homologation, ou, à défaut, d'une autorisation provisoire d'exploitation (APE) ;
- logiciels de type freeware à usage privé sauf accord explicite de l'éditeur ;

- identification d'un comportement suspect ou malveillant du logiciel ;
- mécanisme interne au logiciel (non désactivable) cherchant à se connecter à un serveur sur Internet ;
- dépendance Java non compatible avec AdoptOpenJDK devenu Eclipse Temurin (voir ci-dessous) ;
- installation ne pouvant se faire par les mécanismes du réseau support (package MECM, ex-SCCM).

3.1.1.3 Recours à la machine virtuelle Java sur le terminal utilisateur

Document	Date	Origine	Type doc	Portée
Orientations ministérielles suite à l'évolution de la politique de la société Oracle relative au composant JAVA (Cf 3.2.2.2.1)	25 juillet 2019	DGNUM	Note	MinArm

Certains logiciels nécessitent pour fonctionner qu'une machine virtuelle Java (JVM) soit installée sur le poste utilisateur. Du fait des changements successifs de politique de soutien et de licence de l'éditeur Oracle, il y a 3 licences différentes désormais : Oracle TNLA ([Oracle Technology Network License Agreement for Java SE](#)), Oracle NFTC ([Oracle No-Fee Terms and Conditions License](#)) et GPL2 ([GPLv2+CPE](#)).

Les OpenJDK sont en licences GPL2 (licence GNU).

Pour les Oracle JDK (version LTS) :

- Versions 8 et 11 ont la licence Oracle TNLA (droit d'utilisation restreint au développement et au RUN d'une application personnelle (ne s'applique pas à un usage professionnel). Pour cela il faut souscrire à « Oracle Java SE Universal Subscription ». Cette souscription payante donne accès aux services de « My Oracle Support » ([My Oracle Support](#)) dont un support téléphonique) ;
- Versions 17 et 21, c'est la licence Oracle NFTC qui permet un usage gratuit y compris professionnel. Pour avoir un support, il faut comme pour les version 8 et 11, souscrire à « Oracle Java SE Universal Subscription » ;

Dans tous les autres cas, une JVM Oracle déjà déployée sur un réseau soutenu par la DIRISI, ainsi que les outils propriétaires associés doivent être désinstallés et les mises à jour automatiques désactivées sur le poste de travail ;

La solution recommandée est la JVM HotSpot incluse dans Eclipse Temurin (ex AdoptOpenJDK) avec une préférence pour cette dernière selon la version de Java utilisée. Le recours à une autre JVM doit être dûment justifiée et nécessite une validation du SC²A et du COMCYBER.

L'installation doit impérativement se faire via les mécanismes du réseau support (package MECM). En particulier, le recours à un déploiement Java Webstart ou équivalent est interdit.

La JVM ne doit pas être incluse dans le package d'un logiciel métier mais indiquée en dépendance (afin de faciliter le MCS de la JVM).

3.1.1.4 Postes de travail autonomes ou en mode déconnecté

Certains cas d'usage peuvent nécessiter de recourir à des postes de travail autonomes (i.e. jamais raccordés à un réseau du ministère) ou déconnectés (i.e. raccordés seulement de manière épisodique à un réseau du ministère).

Les postes de travail autonomes présentent un risque moindre de sécurité (seules les données qu'ils contiennent nécessitent une attention particulière) mais imposent une gestion spécifique coûteuse pour en assurer le maintien en condition opérationnelle ou de sécurité. C'est pourquoi il convient d'en limiter l'usage au strict nécessaire et d'essayer, autant que possible, de ne recourir qu'à des technologies maîtrisées utilisées

sur les autres types de postes de travail.

Les postes de travail en mode déconnecté répondent à deux cas d'usage :

- Travail nomade sans possibilité de connexion à un réseau du ministère pendant ce temps ;
- Nécessité impérative (pour des raisons légales ou opérationnelles) de maintenir le fonctionnement en cas de coupure réseau, malgré le risque infime d'occurrence d'un tel incident de nos jours.

L'usage de ces postes doit présenter les garanties de sécurité nécessaires permettant une reconnexion au réseau support. En conséquence :

- Aucun service ne doit y fonctionner en mode serveur ;
- Les logiciels installés doivent suivre les mêmes règles que celles des autres postes dudit réseau.

Pour ce type de postes, le recours à des technologies faiblement adhérentes dont PWA²⁰ ou un sous-ensemble (stockage local, service worker, ...) est particulièrement recommandé. À défaut, une application en technologie Electron reste préférable à un client lourd classique, malgré le cycle particulièrement rapide de mise à jour de cette solution qui impose un repackaging semestriel.

Une attention particulière devra être portée à l'authentification – si elle est nécessaire – afin qu'elle soit opérante avec les conditions de sécurité requises pour les 2 modes de fonctionnement.

3.1.1.5 Socle technique logiciel du poste de travail

Ci-dessous la liste des principaux composants logiciels constituant le socle technique du poste de travail nécessaire au fonctionnement, au maintien en condition de sécurité et de configuration du terminal.



Le Navigateur IE 11 est en cours de décommissionnement : les directions d'applications doivent faire en sorte que leur SI ne soient plus adhérents à ce navigateur ni à un navigateur particulier.

Navigateurs recommandés : Firefox ESR et EDGE Chromium



Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Système d'exploitation	Windows	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	*
<i>NOTA : Le déploiement débutera en 2024 pour les postes clients compatibles et se poursuivra en 2025 pour les postes renouvelés au PRB. Cible de fin de déploiement octobre 2025.</i>					
Déploiement	Agent Configuration Manager (ex SCCM) Current Branch	Microsoft	Agent MECM de déploiement - Cf. 6.2.3	R / S	Intradef
<i>Commentaire : Tout autre outil d'installation sur un système d'exploitation Microsoft (tels que ClickOnce, Java Webstart, InstallAnyware par ex.) ou le recours aux exécutables portables est interdit.</i>					

²⁰ Progressive web application : les applications web progressives utilisent des API web modernes ainsi qu'une stratégie d'amélioration progressive pour créer des applications web multiplateformes qui fonctionnent partout et possèdent des fonctionnalités qui donnent aux utilisateurs les mêmes avantages que les applications natives. Cette technologie est de mieux en mieux supportée et intégrée aux navigateurs et notamment EDGE. Par ailleurs, les mobiles sous Android sont compatibles des applications PWA.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
	LAPS	Microsoft	Gestion du mot de passe local des machines	R/S	Tous réseaux
<i>Nota : remplacement par Windows LAPS à partir du build Windows 10 22H2. Nécessite version Windows Server 2019 car non compatible Windows Server 2016.</i>					
	Sysmon	Microsoft	Gestion de l'activité système		
Environnement exécution	.NET Framework	Microsoft	<i>Framework d'exécution des applications sur OS Windows</i>	R / S	MinAr m
Environnement exécution	.NET Core	Microsoft	<i>Framework d'exécution des applications sur OS Windows.</i>	A / S	MinAr m
Environnement exécution	Eclipse Temurin (ex AdoptOpenJDK)	Eclipse Adoptium	Machine java virtuelle : suite à changement de politique de Oracle, la version de Java déployée est Eclipse Temurin, déployé hors master en tant que dépendance d'un composant logiciel (cf ci-dessus 3.1.1.3 Recours à la machine virtuelle Java)	R / S	MinAr m
<i>Commentaire : Tout autre environnement devra faire l'objet d'une demande de dérogation dûment et rigoureusement justifiée.</i>					

3.1.1.6 Offre logicielle du poste de travail [SU-STORE]

La DIRISI met à disposition des utilisateurs (du domaine DR-CPT) des logiciels déjà packagés en libre-service (DIRISI STORE).

Par ailleurs, les utilisateurs peuvent demander un logiciel présent dans l'offre de service logiciel à partir du catalogue DIADEME.

Enfin les utilisateurs peuvent exprimer un besoin dûment motivé et validé par leur tête de chaîne. Ce dernier fera l'objet d'une instruction par le CCB (cf. §3.1.1.1).

Pour les logiciels soumis à licence, les packages distribués sur les postes de travail nécessitent la saisie du numéro de licence pour que le logiciel soit installé.

Ci-dessous, la liste des principaux logiciels de bureautique du master ou en accès « libre » :

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Bureautique	Office: incluant Word, Excel, Outlook, PowerPoint, OneNote, Visio Viewer	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	*
Bureautique	Modules Office: Skype for Business, Project, Visio	Microsoft	<i>Assujetti : sur demande (payant ou pour VIP/VOP)</i>	A / S	Intradef
Bureautique	Nemo		<i>Plugin Outlook</i>	R / S	Intradef S-SF SIA FrOps

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Bureautique	Libre Office	The Document Foundation	Master : Déploiement sur simple demande pour Windows 7	R / S	Intradef
Bureautique	Adobe Reader DC	Adobe	Master	R / S	Intradef
Bureautique	7-Zip	Igor Pavlov (logiciel libre)	Master : Compression	R / S	Intradef
Navigateur	Firefox ESR	Mozilla	Master <i>cf.4.5 Sécurisation des COTS</i> * pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits	* / *	Intradef S-SF SIA FrOps
Navigateur	EDGE Chromium	Microsoft	Version anaheim basée sur le noyau Chromium	R / S	Intradef
Navigateur	Internet Explorer	Microsoft	Master <i>cf.4.5 Sécurisation des COTS</i> NB : produit déprécié par l'éditeur.	I / N	Intradef S-SF SIA FrOps
<i>Commentaire : Le navigateur Microsoft Edge basé sur le noyau Chromium remplace IE. Les directions d'application DOIVENT faire en sorte que leurs SI ne soient plus adhérents à ce navigateur et pour ce faire, peuvent, si nécessaire et de manière transitoire, recourir au mode de compatibilité proposé par EDGE</i>					
Multimedia	VLC	Videolan	Master	R / S	Intradef
Multimedia	Flash player	Adobe	Statut : <u>Interdit</u> / Plus de soutien NB : retiré du socle et du navigateur début 2021	I / N	Intradef
<i>Commentaire : pour des raisons de sécurité, tous les navigateurs interdisent désormais ce plugin. Le ministère en interdit l'usage. Microsoft a bloqué Flash via la mise à jour de juillet 2021 (KB4577586)</i>					
Sécurité	ACID Cryptofiler	Capgemini Abak Systèmes	Master : Chiffrement des données de niveau DR <i>Cf. 4.6.5.3.1 Chiffrement de fichiers [CHI]</i> Cette solution est soumis à un agrément ANSSI	R / S	Intradef

3.1.1.7 Messagerie

On distingue deux types de service de messagerie : messagerie officielle et messagerie non officielle. Un même concept d'emploi recouvre ces deux types :

Document	Date	Origine	Type doc	Portée
Concept d'emploi de messagerie électronique note conjointe : n°2859/DEF/EMA/CPI/AUT/NP / n°2202/DEF/SGA/ADJ/NP :	21 déc. 2010 15 déc. 2010	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi de messagerie électronique officielle et non officielle</i>				
SLR des services "messagerie officielle" et "messagerie non officielle" : note conjointe : n°1619/DEF/EMA/CPI/AUT/NP / n°304/DEF/SGA/ADJ/NP	11 février 2013 15 février 2013	SC1	SLR	MinArm
<i>Commentaire : SLR relatif au service de messagerie</i>				

3.1.1.7.1 Messagerie non officielle [SU-MEL]

Ce service permet à l'utilisateur de disposer d'une solution de messagerie électronique (personnelle ou de groupe) permettant d'échanger des messages non officiels tels que définis dans le concept de messagerie non officielle.

Ce service inclut des fonctions d'envoi-réception (de message depuis l'interne et l'externe) / archivage automatique / accusé de réception / carnet d'adresse / protection contre le courrier indésirable / envoi à des listes de diffusion.

Cas d'usage :

- Messagerie individuelle ou pour un groupe d'utilisateur, liée ou non à une fonction ;
- Utilisation possible de plusieurs comptes de messagerie ;
- Utilisation tolérée pour des besoins non professionnels dans la limite du respect des règles de sécurité et de non gêne du service professionnel ;
- Comptes techniques de messagerie à destination des systèmes d'information.

Voir partie back office §3.3.1.1 Messagerie non officielle – Agenda

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Messagerie (Client)	Client Outlook	Microsoft	Client de messagerie <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	* / *	S-SF SIA FrOps
Messagerie (Client)	Client Thunderbird	Mozilla	Client de messagerie alternatif. Ce client est également déployé sur les postes CLIP-HESTIA.	A / N	Tout intranet
Messagerie (Client)	Outlook Web Access (OWA)	Microsoft	Webmail simulant un client Outlook	<u>R</u> / S	Tout intranet
Messagerie (Client)	SOGO		Assujetti au contexte SIE : Webmail pour le SIE (Baltique/Celtique), connectable avec le client Outlook et offrant des fonctions de partage de calendriers et de carnets d'adresses.	A / S	SIE
Messagerie (serveur)	<i>Partie serveur : Cf. 3.3.1 Messagerie / Agenda / Tâches / Listes de diffusion</i>				

3.1.1.7.2 Messagerie officielle [SU-MOF]

Ce service permet à l'utilisateur de disposer d'une solution de messagerie électronique (personnelle ou de groupe) permettant d'échanger des messages officiels tels que définis dans le concept d'emploi de messagerie. (Les messages sont considérés comme officiels, si et seulement s'ils sont émis à partir d'une adresse d'organisme et s'ils respectent un certain formalisme.)

Ce service est assuré de façon principale par NEMO.

NEMO :

La trajectoire des messageries officielles de l'État-Major des Armées en relation avec le nouveau concept de messagerie fait de NeMO (Nouvelle Messagerie Officielle) la messagerie officielle de l'Itradef.

Document	Date	Origine	Type doc	Portée
Nommage des adresses électroniques (cf. §.3.3.4.1 Annuaires / référentiels)				
<i>Commentaire : défini par la directive de nommage des annuaires</i>				
Gestion de la liste unique des mots clés d'attribution (MCA) <i>Cf. 8.5.4 Mots clés d'attribution (MCA)</i>				
Emploi de la messagerie officielle (NeMO) sur le réseau Intradef de l'EMA diffusé par note I-14-000549/DEF/EMA/ESMG/NP du 7 février 2014	7 février 2014	EMA	Note	MinArm
<i>Commentaire : cette note décrit l'emploi de NEMO dans le cadre des cellules de management de l'information de l'EMA.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Messagerie (client)	NEMO Addon client Outlook	MinArm		R / S	IntradefS-SF FrOpS
Messagerie (serveur)	NEMO	MinArm	Système d'information sur une base Exchange + compléments logiciels	R / S	Intradef S-SF SIA FrOps

3.1.1.8 Agenda, contacts [SU-AGE]

Ce service recouvre l'accès à la gestion d'un ou plusieurs agendas personnels, depuis tout type de terminal, et ce de façon synchronisée (en cible), la planification d'événement et la réservation éventuelle de toutes ressources associées (salles, moyens techniques...), la gestion des invitations, et toutes les fonctions classiques de configuration et de gestion d'agenda.

Document	Date	Origine	Type doc	Portée
Concept d'emploi agenda : Note conjointe : n°11299/DEF/EMA/CPI/AUT/NP / n°1758/DEF/SGA/ADJ :	22 octobre 2012 23 octobre 2012	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi agenda</i>				
SLR du service "agenda" : note conjointe : n°1117/DEF/EMA/CPI/AUT/NP / n°202/DEF/SGA/ADJ/NP	28 janvier 2013 29 janvier 2013	SC1	SLR	MinArm
<i>Commentaire : SLR relatif au service d'agenda</i>				

Les solutions d'agenda, de gestion de contacts et de gestion de tâches personnelles sont intégrées aux solutions logicielles de client de messagerie (*cf. 3.1.1.7 Messagerie*)

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Partage calendriers, contacts, messages	SOGO	OpenSource	Solution spécifique à SIE voir : <i>§3.1.1.7.1 Messagerie non officielle [SUEMEL]</i>	A / S	SIE
Partage calendriers, contacts, messages	Outlook Web Access (OWA)	Microsoft	Webmail simulant un client Outlook	R / S	Tout intranet
Partage calendriers, contacts, messages	Outlook	Microsoft	Master	R / S	Intradef

3.1.1.9 Portail personnalisable [SU-GPE]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "portail personnalisable" : note conjointe : n°1351/DEF/EMA/CPI/AUT/NP / n°248/DEF/SGA/ADJ	4 février 2013 6 février 2013	SC1	Concept Emploi	MinArm Intradef
<i>Commentaire : Concept d'emploi "portail personnalisable"</i>				
SLR du service "portail personnalisable" : note conjointe : n°1771/DEF/EMA/CPI/AUT/NP / n°319/DEF/SGA/ADJ	12 février 2013 15 février 2013	SC1	SLR	MinArm Intradef
<i>Commentaire : SLR du service de " portail personnalisable "</i>				

Au niveau client, le service est accessible via le navigateur. [Voir partie back office §3.3.2.1](#) Portail personnalisable [GPE]

3.1.2 Collaboratif

3.1.2.1 Communication instantanée

Pas de référence identifiée à ce jour.

3.1.2.1.1 Dialogue en ligne, gestion de présence [SU-PRE], messagerie instantanée [SU-MIN]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "discussion en ligne" : note conjointe : n°11230/DEF/EMA/CPI/AUT/NP / n°1759/DEF/SGA/ADJ	22 octobre 2012 23 octobre 2012	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi discussion en ligne : ce concept d'emploi couvre les notions de messagerie instantanée, de gestion de présence et de discussion en ligne</i>				
SLR des services de "discussion en ligne" : note conjointe : n°701/DEF/EMA/CPI/AUT/NP / n°151/DEF/SGA/ADJ/NP	18 janvier 2013 22 janvier 2013	SC1	SLR	MinArm
<i>Commentaire : SLR relatif au service de discussion en ligne</i>				

3.1.2.1.2 Réunion virtuelle [SU-REV], audioconférence [SU-AUD], visioconférence [SU-VIS], vidéoconférence [SU-VID]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "réunion virtuelle" : note conjointe : n°12477/DEF/EMA/CPI/AUT/NP / n°2033/DEF/SGA/ADJ	26 nov. 2012 30 nov. 2012	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "réunion virtuelle" : ce concept d'emploi couvre les notions d'audioconférence, de visioconférence, et de réunion virtuelle avec les fonctions associées au travail collaboratif synchrone : partage de bureau, de fichiers, tableau blanc, sondages auprès des participants, présentation 3D, ...</i>				
SLR des services "audioconférence " et « visioconférence » : note conjointe : n°1116/DEF/EMA/CPI/AUT/NP / n°200/DEF/SGA/ADJ/NP				
<i>Commentaire : SLR relatif aux services d'audioconférence et visioconférence</i>				
Politique de la messagerie instantanée sécurisée de l'Etat « TCHAP » pour le ministère des armées Diffusée par note n°98/ARM/DGNUM/DG/NP du 21 mars 2019	21 mars 2019	DGNUM	Politique d'emploi	MinArm
<i>Commentaire : cette politique décrit le cadre d'emploi de la messagerie TCHAP. Cette messagerie est utilisée pour des échanges de confiance des agents du ministère entre eux, avec d'autres agents étatiques ou, sur invitation, avec des partenaires extérieurs, via des téléphones « grand public » non sécurisés, privés ou professionnels de type Android ou Apple.</i>				
<i>Initialement, deux services étaient prévus (TCHAP Agent et TCHAP Secure), TCHAP Secure a depuis été abandonné au profit de TCHAP Agent.</i>				

3.1.2.1.3 Solutions logicielles client

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Communications instantanées	Prosody	SIE (Baltique et Celtique)	Solution de chat	R / S	SIE
Communications instantanées	Lync (client couplé au serveur)	Microsoft	Son remplacement est à l'étude sur les réseaux classifiés.	D / O	S-SF SIA FrOps
Communications instantanées	Skype for business	Microsoft		R / S	MinArm
Communications instantanées	JChat (client couplé au serveur TCS)	OTAN	Solution de chat opérationnelle nativement interopérable avec l'OTAN	R / S	S-SF SIA FrOps
Communications instantanées	JChat (client couplé au serveur TCS)	OTAN	Solution de chat opérationnelle uniquement pour les cas d'usage Guyane, JO2024 et coupe du monde de rugby, non soutenu DIRISI au-delà (CR SP-COF N°2023/407 du 07/07/23)	A / S	Intradef
Communications instantanées	Audioconf DIRISI	DIRISI	Pour des échanges NP	R / S	NP
Communications instantanées	Audioconf de l'état	DINUM	Pour des échanges NP	R / -	NP
Communications instantanées	Tchap	DINUM	Solution de chat sécurisé interministériel	R / S	Etat Internet
<i>Commentaire : voir politique d'emploi ci-dessus.</i>					

Communications instantanées	Webconf de l'Etat	DINUM	Solution interministérielle basée sur JITSI	R / S	Internet
<i>Commentaire : fonctionne sur des postes internet à partir d'un navigateur mais pas au travers d'ISPT, en utilisant le service interministériel.</i>					
Communication instantanée (serveur)	Partie back-office serveur : Cf. 3.3.3.1 Messagerie instantanée – Réunion virtuelle – Vidéoconférence - Rédaction collaborative synchrone [MIN-REV-VIH-RCS]				
Communications instantanées	VVIPER		Mis en œuvre avec Jabber et assujetti aux seuls cas d'emploi VViper	A / E	S-SF
Communications instantanées	Jabber		Communication OTAN (Cf. WEBEX partie serveur)	A / E	SIA FrOps

3.1.2.2 Espace de travail collaboratif [SU-EDT]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "espace de travail collaboratif" : note conjointe : n°11231/DEF/EMA/CPI/AUT/NP / n°1760/DEF/SGA/ADJ	22 octobre 2012 23 octobre 2012	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "espaces de travail collaboratif" : ce concept d'emploi couvre la gestion d'espaces de travail collaboratif et leur accès ainsi que des outils associés : partage de ressources, workflow de travail, production de documents en communs, gestion de version, assignation et suivi des tâches, partage d'agenda, outils d'échange ou de partage internes à la communauté (discussion en ligne, wiki, enquêtes, mind mapping, ...)</i>				
SLR du service "espace de travail collaboratif" : note conjointe : n°699/DEF/EMA/CPI/AUT/NP / n°200/DEF/SGA/ADJ/NP	26 janvier 2013 29 janvier 2013	SC1	SLR	MinArm
<i>Commentaire : SLR relatif au service d' "espaces de travail collaboratif"</i>				

L'accès à ce service à l'utilisateur se fait via le navigateur du poste client.

Solutions : [Voir partie back office - serveur §3.3.2.8](#) Gestion des communautés d'intérêt [COI]

3.1.2.3 Wiki [SU-WKI]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "wiki" : note conjointe : n°6352/DEF/EMA/CPI/AUT/NP / n°960/DEF/SGA/ADJ/NP	3 juin 2013 5 juin 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "wiki"</i>				
SLR du service "wiki" : note conjointe : n°1626/DEF/EMA/CPI/AUT/NP / n°1199/DEF/SGA/ADJ	2 juillet 2013 9 juillet 2013	SC1	SLR	MinArm
<i>Commentaire : SLR relatif au service de "wiki"</i>				

L'accès à ce service à l'utilisateur se fait via le navigateur du poste client.

Solutions : Voir partie back office - serveur §3.3.3.2 Wiki [WKI]

3.1.2.4 Tableau blanc - Rédaction synchrone

Pour l'instant, les fonctions collaboratives s'arrêtent aux fonctions de tableau blanc et sont essentiellement amenées par le client Skype.

Solutions : Voir partie back office - serveur

§3.3.3.1 Messagerie instantanée – Réunion virtuelle – Vidéoconférence - Rédaction collaborative synchrone [MIN-REV-VIH-RCS]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Tableau blanc (client)	Lync	Microsoft		D / N	S-SF SIA FrOps
Tableau blanc (client)	Skype for business	Microsoft		R / S	Intradef S-SF SIA FrOps
Rédaction synchrone (client)	Navigateur ou Suite bureautique interfacé avec Sharepoint ou Alfresco		Dans le cadre des espaces de travail collaboratif	R / S	Intradef S-SF SIA FrOps

3.1.2.5 Forum [SU-FOR]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "forum" : note conjointe : n°3814/DEF/EMA/CPI/AUT/NP / n°555/DEF/SGA/ADJ	26 mars 2013 28 mars 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "forum"</i>				
SLR du service "forum" : note conjointe : n°4582/DEF/EMA/CPI/AUT/NP / n°686/DEF/SGA/ADJ/NP	12 avril 2013 15 avril 2013	SC1	SLR	MinArm
<i>Commentaire : SLR du service "forum"</i>				

L'accès à ce service à l'utilisateur se fait via le navigateur du poste client.

Solutions : Voir partie back office - serveur §3.3.3.3 Forum [FOR]

3.1.2.6 Listes de diffusion

Cf §3.3.1.4 Liste de diffusion [LDF]

3.1.2.7 Réseau social [SU-RSE]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "réseau social MinDef" : note conjointe : n°3817/DEF/EMA/CPI/AUT/NP / n°557/DEF/SGA/ADJ	26 mars 2013 28 mars 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "réseau social" : ce document couvre essentiellement les fonctions d'animation de communautés, de recherche ou de suivi de publications de communautés d'utilisateurs</i>				

Document	Date	Origine	Type doc	Portée
SLR du service "réseau social MinDef" : note conjointe : n°4583/DEF/EMA/CPI/AUT/NP / n°687/DEF/SGA/ADJ/NP	12 avril 2013 15 avril 2013	SC1	SLR	MinArm
<i>Commentaire : SLR du service "réseau social"</i>				

L'accès à ce service à l'utilisateur se fait via le navigateur du poste client.

Solutions : Voir partie back office - serveur §3.3.2.9 Réseau social d'entreprise [RSE]

3.1.3 Vie courante

3.1.3.1 Portail intranet [SU_PIN]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "portail intranet" : note conjointe : n°529/DEF/EMA/CPI/AUT/NP / n°152/DEF/SGA/ADJ	16 janvier 2013 22 janvier 2013	SC1	Concept Emploi	MinArm Tout intranet
<i>Commentaire : Concept d'emploi "portail intranet"</i>				
SLR du service "portail intranet" : note conjointe : n°1349/DEF/EMA/CPI/AUT/NP / n°247/DEF/SGA/ADJ	4 février 2013 6 février 2013	SC1	SLR	MinArm Tout intranet
<i>Commentaire : SLR des services de "portail intranet"</i>				
Compte rendu du CODIR restreint des Intranets n°24 du 3 avril 2014 diffusé par note conjointe : n°D-14-004992 /DEF/EMA/PSIOC/NP du 19 mai 2014 n°316/DEF/DGSIC/NP du 20 mai 2014	19 mai 2014 20 mai 2014	CODIR Intranets	Note	MinArm Internet Intradef
<i>Commentaire : le compte rendu porte décision relative au choix des outils pour les portails de communications pour le NP-DR.</i>				

L'accès à ce service à l'utilisateur se fait via le navigateur du poste client.

Solutions : Voir partie back office - serveur §3.3.2.2 Portail d'information [PIN]

3.1.3.2 Annuaire pages blanches, pages jaunes [SU-PJB]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "pages jaunes – pages blanches" : Note conjointe : n°10710/DEF/EMA/CPI/AUT/NP / n°1687/DEF/SGA/ADJ	9 octobre 2012 11 octobre 2012	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi pages jaunes / pages blanches</i>				
SLR du service "pages jaunes – pages blanches" : note conjointe : n°591/DEF/EMA/CPI/AUT/NP / n°145/DEF/SGA/ADJ/NP	17 janvier 2013 22 janvier 2013	SC1	SLR	MinArm
<i>Commentaire : SLR relatif au service de pages jaunes- pages blanches</i>				

Voir aussi §3.3.4.1 Annuaires / référentiels et § 3.3.4.3 Outils de « provisionning » d'annuaires

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Annuaire Pages blanches	Solution Annudef	MinArm	Ce service est réalisé sur développement interne	R / S	Intradef
Annuaire Pages blanches	Annuaire de référence OpenLDAP provisionné via MEIBO	MinArm	Service packagé IntraCed S-SF et SIA S-SF	R / S	S-SF SIA FrOps
Annuaire Pages blanches	Annubat	MinArm	Interface permettant la consultation du LDAP embarqué.	R / S	SIE

3.1.3.3 Impression – édition multifonction [SU-IMP]

Ces services renvoient essentiellement à des fonctions d'impression, de copies et de numérisation de documents.

En cible, et sauf pour répondre à des besoins très spécifiques, ces services sont assurés par des photocopieurs multifonctions réseaux mutualisés entre services et activés via une identification par badge (carte CIMS par défaut ou une carte subsidiaire si l'utilisateur ne possède pas encore de carte CIMS) et une authentification par un code numérique. Ces services de proximité doivent être également accessibles en itinérance interne.

L'enrôlement s'opère en fonction du compte Active Directory pour les postes du domaine considéré. S'il n'y a pas de lecteur de badge ou si celui ne fonctionne pas, l'authentification en fonction du compte Active Directory reste toujours possible, si la fonction est disponible. L'authentification sur les photocopieurs multifonctions réseaux mutualisés est obligatoire pour les fonctions copie, impression et numérisation pour permettre l'imputabilité et la traçabilité.

Les photocopieurs multifonctions sont des objets partagés dans l'Active Directory et peuvent être recherchés et installés depuis le poste de travail, en fonction des droits dont dispose l'utilisateur.

L'authentification par badge et code est centralisée par défaut, mais elle est peut-être locale à un unique photocopieur multifonction pour des besoins spécifiques.

Par défaut, l'acquisition d'imprimantes multifonctions passe par le marché SOLIMP pour les intranets sous responsabilité de l'opérateur DIRISI.

Le SIE met en œuvre le serveur d'impression CUPS sur son domaine local.

Document	Date	Origine	Type doc	Portée
Politique d'impression au ministère des armées diffusé par note n°703/ARM/DGNUM/DG/NP	27 novembre 2023	DGNUM	Politique	MinArm
Concept d'emploi "point d'édition multifonction" : diffusée par note conjointe : n°5441/DEF/EMA/CPI/AUT/NP / n°827/DEF/SGA/ADJ	? mai 2013 13 mai 2013	SC1	Concept Emploi	MinArm NP/DR
<i>Commentaire : Concept d'emploi " point d'édition multifonction " : ce document couvre les fonctions d'impression, de copie de documents, de numérisation, de télécopie pour un utilisateur, ainsi que les fonctions de découverte, de paramétrage et de gestion des imprimantes.</i>				
SLR du service "point d'édition multifonction" : note conjointe : n°5955/DEF/EMA/CPI/AUT/NP / n°908/DEF/SGA/ADJ	24 mai 2013 27 mai 2013	SC1	SLR	MinArm/ NP/DR
<i>Commentaire : SLR relatif au service de " point d'édition multifonction "</i>				

3.1.3.4 Moteur de recherche [SU-RMR]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "moteur de recherche" : note conjointe : n°4584/DEF/EMA/CPI/AUT/NP / n°683/DEF/SGA/ADJ	12 avril 2013 15 avril 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "moteur de recherche"</i>				
SLR du service "moteur de recherche" : note conjointe : n°5155/DEF/EMA/CPI/AUT/NP / n°769/DEF/SGA/ADJ	26 avril 2013 29 avril 2013	SC1	SLR	MinArm
<i>Commentaire : SLR relatif au service de "moteur de recherche"</i>				

Les moteurs de recherche sont accessibles via le navigateur du poste client. [Voir partie back office §3.3.2.7 Moteur de recherche \[RMR\]](#)

3.1.3.5 Enquête et sondage [SU-ENQ]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "enquêtes et sondages" : note conjointe : n°7558/DEF/EMA/CPI/AUT/NP / n°1164/DEF/SGA/ADJ	1 ^{er} juillet 2013 1 ^{er} juillet 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "enquêtes et sondages" : ce document couvre les fonctions de création, envoi, réponse, exploitation et analyse de résultats de questionnaires.</i>				
SLR du service "enquêtes et sondages" : note conjointe : n°8487/DEF/EMA/CPI/AUT/NP / n°1295/DEF/SGA/ADJ	12 juillet 2013 13 juillet 2013	SC1	SLR	MinArm
<i>Commentaire : SLR du service de "enquêtes et sondages"</i>				
Rationalisation des logiciels de questionnaires, sondages et enquêtes : note n°294/DEF/DGSIC/SDMA/BGAI du 16 mars 2011	16 mars 2011	DGSIC	Note	Intradef
<i>Commentaire : note DGSIC préconisant l'usage de LimeSurvey</i>				

Ce service à l'utilisateur est accessible via le navigateur du poste client. Voir partie back office §3.3.2.10 Enquête et sondage [ENQ].

3.1.3.6 Réservation de salles [SU-RDS]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "réservation de salles" : note conjointe : n°8889/DEF/EMA/CPI/AUT/NP / n°1270/DEF/SGA/ADJ	18 juillet 2013 18 juillet 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi "réservation de salles"</i>				
SLR du service "réservation de salles" : note conjointe : n°8888/DEF/EMA/CPI/AUT/NP / n°1269/DEF/SGA/ADJ	18 juillet 2013 18 juillet 2013	SC1	SLR	MinArm
<i>Commentaire : SLR du service de "réservation de salles"</i>				

Ce service est adossé au service d'agenda. Sur l'Intradef sauf à Balard, les salles sont des ressources enregistrées dans l'annuaire technique Active Directory DR-CPT.

Sur Balard, le service fait l'objet d'un service séparé OPALE non intégré au service d'agenda et nécessitant le report manuel de la salle réservée dans le service d'agenda.

3.1.4 Gestion des données

3.1.4.1 Stockage des données [SU-REP]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "stockage de données" : note conjointe : n°4140/DEF/EMA/CPI/AUT/NP / n°640/DEF/SGA/ADJ	2 avril 2013 5 avril 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi " stockage de données " : ce document couvre :</i>				
<ul style="list-style-type: none"> - le stockage des données professionnelles d'un utilisateur (<i>support amovible, poste de travail, via l'intranet</i>), - le stockage des données professionnelles partagées par des utilisateurs, - le stockage des données de personnalisation du poste de travail permettant la mobilité, - le stockage des données privées d'un utilisateur 				
SLR du service "stockage de données" : note conjointe : n°4688/DEF/EMA/CPI/AUT/NP / n°713/DEF/SGA/ADJ	18 avril 2013 18 avril 2013	SC1	SLR	MinArm
<i>Commentaire : SLR du service de " stockage de données "</i>				

Chaque utilisateur du DR-CPT dispose :

- d'un espace de stockage individuel sur son poste ;
- d'un espace de stockage à vocation temporaire sur Defense-Drive ;
- de droits sur des espaces de stockage partagés (avec des membres de son unité d'appartenance) ou publics : ces espaces de stockage sont gérés par la DIRISI (ou l'opérateur dont ils dépendent).

Sur SIE, chaque utilisateur dispose d'un espace de stockage privé et public.

Partie BackOffice :

Cf. 3.3.2.5 Syndication de contenu [ASY]

Cf. 3.3.2.6 Répertoires partagés [REP]

3.1.4.2 Transfert de données volumineuses [SU-TFV]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "transfert de données volumineuses" : note conjointe : n°444/DEF/EMA/CPI/AUT/NP / n°153/DEF/SGA/ADJ	14 janvier 2013 22 janvier 2013	SC1	Concept Emploi	MinArm
<i>Commentaire : Concept d'emploi " transfert de données volumineuses "</i>				
<i>SLR du service "transfert de données volumineuses" : note conjointe : n°1350/DEF/EMA/CPI/AUT/NP / n°249/DEF/SGA/ADJ</i>				
<i>Commentaire : SLR du service de " transfert de données volumineuses "</i>				

La solution Defense Drive (Intradef) permet de mettre en œuvre les dispositions principales du concept d'emploi transfert de données volumineuses de niveau NP/DR ainsi que du concept d'emploi "Stockage de données".

France Transfert doit également être utilisé au travers d'ISPT pour des échanges de niveau NP et prendra la suite de la solution Merlin que sera décommissionnée au 1^{er} mars 2024.

Des solutions sont également envisagées pour les intranets classifiés.

3.1.5 Sécurité [SU-SO, SU-CHI, SU-SIG]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "services de sécurité de l'usager" : note conjointe : n°D12-013027/DEF/EMA/CPI/AUT/NP / n°2090/DEF/SGA/ADJ	7 déc. 2012 10 déc. 2012	SC1	Concept Emploi	MinArm Intradef S-SF
<i>Commentaire : Ce document traite des services de sécurité relatifs à l'utilisateur et couvre les besoins attendus en cible :</i>				
<ul style="list-style-type: none"> - <u>pour l'authentification</u> : authentification simple en fonction de son besoin, aussi unique que possible (SSO), authentification forte ciblée ; - <u>la signature électronique et le cachet serveur</u> : signature répondant au besoin de confiance et de durée de conservation dans le temps, assurant la non-répudiation, garantissant l'intégrité visuelle et sémantique du contenu, assurant des preuves d'envoi et de réception via un service d'horodatage, pouvant faire office de preuve ; ce service doit couvrir tous les besoins d'échanges entre autorités administratives, avec les partenaires et la société civile, les besoins d'échanges impliquant les agents ; - <u>le chiffrement pour protéger les documents (documents et messages, les échanges, les postes terminaux notamment en situation de mobilité, les données transitant sur un réseau, accéder à des ressources en situation de mobilité</u> ; 				
SLR des services de "sécurité de l'usager" : note conjointe : n°D13-004806/DEF/EMA/CPI/AUT/NP / n°726/DEF/SGA/ADJ/NP	18 avril 2014 22 avril 2014	SC1	SLR	MinArm Intradef
Cadre d'emploi de la signature électronique au ministère des Armées – Ed 2 <i>Cf. 4.6.3.2 Signature [SGN]</i>	8 juillet 2021	DGNUM	Concept emploi	MinArm

Cf. § 4.6 Services de sécurité

3.1.6 Mobilité [SU-AN, SU-ITN]

Deux solutions ministérielles de mobilité (nomadisme) permettant depuis l'extérieur d'accéder à l'Intradef sont actuellement en service au sein du ministère : SMOBI et téléphonie mobile.

SMOBI est la solution proposée par la DIRISI avec :

- un volet « ordiphone » (certains smartphones et tablettes Android de la marque Samsung) basé sur une sécurisation du terminal et de l'accès jusqu'au niveau DR par la suite CRYPTOSMART (société ERCOM) pour mobile ; une solution complémentaire de gestion de flotte (Mobile Iron) est installée sur les terminaux en vue du déploiement d'applications depuis un magasin d'applications dédié du Ministère ;
- un volet poste de travail (sous Microsoft Windows) : il s'agit d'un poste de travail portable standard de l'Intradef équipé d'une sécurisation de l'accès par la suite CRYPTOSMART pour PC, d'une pile logicielle complémentaire dédiée (chiffrement du disque dur, détection automatique de l'environnement LAN/mobilité) et éventuellement d'une connexion 4G ;
- l'accès à l'Intradef se fait via une passerelle dédiée SMOBI. La navigation Internet sur le poste se fait via ISPT (Internet sur le poste de travail) sous réserve, pour le volet poste de travail, de disposer de ce service.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°25 portant sur la mobilité publiée au Bulletin Officiel des Armées modifiant la Directive DGSIC n°12 portant sur la mobilité du 1^{er} juin 2010	29 mars 2012	DGSIC	Directive	Réseaux non classifiés
<i>Commentaire : Règles applicables au nomadisme et à la mobilité externe sur les réseaux non classifiés. Cette directive liste notamment les fonctions de sécurité que les solutions de mobilité doivent respecter en priorité.</i>				
Concept d'emploi des services de mobilité : note conjointe : n°D11-4204/DEF/EMA/CPI/AUT/NP / n°878/DEF/SGA/ADJ	13 mai 2011 19 mai 2011	SC1	Concept Emploi	MinArm Intradef S-SF
<i>Commentaire : Ce document traite des services relatifs aux services d'itinérance (mobilité interne) et de nomadisme pour les postes de travail ainsi qu'aux services liés aux Smartphones sur l'Intradef. Le réseau S-SF n'est concerné que par des services d'itinérance.</i>				
SLR des "services de mobilité" : note conjointe : n°D12-134/DEF/EMA/CPI/AUT/NP / n°79/DEF/SGA/ADJ	06 janvier 2012 16 janvier 2012	SC1	SLR	MinArm Intradef
<i>Commentaire : SLR relatifs aux accès en itinérance (BS09) et en nomadisme (BS10)</i>				
Directive DIRISI n° 89 d'exploitation des solutions de mobilité de l'Intradef version 1.0 du 02/04/2013	2 avril 2013	DIRISI	Directive	Intradef
<i>Commentaire : cette directive porte sur les solutions techniques de mobilité actuellement en service au sein du ministère, notamment SMOBI.</i>				
Directive DIRISI n° 86 de soutien de la solution de mobilité SMOBI	2 avril 2013	DIRISI	Directive	Intradef
Directive d'emploi des services de mobilité SMOBI Note n°123 /DEF/SGA/ADJ du 31 janvier 2014	31 janvier 2014	SGA	Note	Intradef
SMOBI – Dérogation à l'étranger diffusé par NEMO UM SNUM 2020/225 du 21 juillet 2020	21 juillet 2020	UM SNUM	Note	Intradef
<i>Commentaire : Ce NEMO porte un avis technique sur les conditions d'utilisation d'un SMOBI à l'étranger</i>				
Plan de management des services de mobilité sécurisée de l'Intradef (Solution de mobilité de l'Intradef – SMOBI) diffusé par note n° 501272/DEF/DIRISI/SCI/SI/NP version 1.0 du 1er juin 2014	4 juin 2014	DIRISI	Note	Intradef
Spécification d'interface SMOBI à l'attention des SI : Cadre d'architecture et contraintes de configuration pour un système d'information accessible sur un terminal SMOBI	1 ^{er} décembre 2020	UM SNUM / DIRISI	Note technique	Intradef
<i>Commentaire : cette note technique s'adresse aux directions d'applications ayant vocation à être accédées en mobilité via SMOBI. Elle définit les conditions pour une bonne intégration des applications dans l'écosystème SMOBI.</i>				
Mise en œuvre de la téléphonie mobile au sein des bases de défense <i>Cf. 5.1.8.1 Téléphonie classique</i>	4 février 2014	EMA	Note	Intradef

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Mobilité « poste de travail »	SMOBI Solution ministérielle basée sur les produits CRYPTOSMART	DIRISI	Utilisation de la station de travail de l'Intradef (poste unique) en situation de nomadisme avec Cryptosmart PC Suite et éventuellement une connexion type réseaux mobiles civils. Infrastructures d'accueil basées sur Cryptosmart Gateway	R / S	Intradef
Mobilité « ordiphone »	SMOBI Solution ministérielle	DIRISI	Utilisation d'un ordiphone du commerce (smartphones et tablettes de marque Samsung fournis par	R / S	Intradef

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
	basée sur les produits CRYPTOSMART et Mobile Iron		l'administration) sécurisé par la solution Cryptosmart Mobile Suite Infrastructures d'accueil basées sur Cryptosmart Gateway.		

3.1.7 Accès réseaux extérieurs

3.1.7.1 Internet sur le poste de travail [SU-WEB]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "internet sur le poste de travail" : diffusé par note conjointe : n°9065/DEF/EMA/CPI/AUT/NP / n°2249/DEF/SGA/ADJ	22 nov. 2011 30 nov. 2011	SC1	Concept Emploi	MinArm Intradef
<i>Commentaire : Concept d'emploi " internet sur le poste de travail " : ce document couvre les fonctions d'accès depuis le poste de travail à la messagerie et à la navigation sur le réseau internet.</i>				
SLR du service "internet sur le poste de travail" : note conjointe : n°2810/DEF/EMA/CPI/AUT/NP / n°664/DEF/SGA/ADJ	29 mars 2012 4 avril 2012	SC1	SLR	Intradef
<i>Commentaire : SLR relatif au service de " internet sur le poste de travail "</i>				
Transmission de données sensibles par Internet : par note n°D-12-002601/DEF/EMA/CPI/SSI/NP /	23 mars 2012	EMA	Note	Intradef
<i>Commentaire : cette note précise les obligations faites dans l'usage de SISMEL pour la transmission d'informations sensibles : pas de redirection automatique, chiffrement préalables des données sensibles.</i>				

Conformément au concept d'emploi de l'internet sur le poste de travail qui prévoit un poste unique NP/DR relié à l'Intradef (pour rappel, l'accès aux services de l'internet sur un poste classifié de défense est interdit) et disposant d'accès à l'internet, le catalogue de service du ministère propose deux services :

SISMEL : service de messagerie (SISMEL) permettant d'émettre/recevoir des messages vers/ de l'internet directement depuis la boîte aux lettres hébergée sur l'Intradef: l'usage de ce service est actuellement limité aux messages non officiels ; les pièces jointes de niveau DR, DR-SF et autre niveau de confidentialité spécifique (personnel, médical, etc.) ne peuvent être émises que si elles ont été préalablement chiffrées par un logiciel adapté à leur niveau de sensibilité (par exemple ACID ou Zed ! pour le niveau DR).

Document	Date	Origine	Type doc	Portée
Directive DIRISI d'exploitation de SISMEL V2 : sous timbre n°1100318/DEF/DIRISI/SCOL/B.EMP/Intranets du 26 février 2008	26 février 2008	DIRISI	Directive	Intradef

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Échanges mail Internet	SISMEL	MinArm	Passerelle de messagerie sécurisée mise en place par le MinArm entre la messagerie de l'Intradef et l'Internet	R / S	Intradef

ISPT – Internet Sur le Poste de Travail : service de navigation sur l'internet depuis le navigateur du poste Intradef ;

Document	Date	Origine	Type doc	Portée

Directive DIRISI n°232 d'exploitation et de soutien du service Internet sur le poste de travail (ISPT) V8.2	10 décembre 2018	DIRISI	Directive	Intradef
--	------------------	--------	-----------	----------

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Accès Web Internet	ISPT : Internet sur le Poste de Travail	MinArm	Passerelle assurant l'accès au service de navigation sur l'Internet depuis le poste de travail de l'Intradef. Le nombre de postes et d'utilisateurs bénéficiant du service ISPT est limité	R / S	Intradef

Le service ISPT fonctionne en mode :

- « liste noire » : un site référencé par le CALID dans cette liste noire est interdit d'accès via ISPT ;
- « liste blanche » : un site nécessite d'être autorisé pour être accédé. La demande d'autorisation d'accès à un site non encore connu se fait automatiquement.

Ces deux services (SISMEL et ISPT) mettent en œuvre des politiques de filtrage de flux et de contenus ainsi que de protection contre les codes malveillants. Ces services sont exclusivement à l'usage des utilisateurs finaux et n'ont pas vocation à être consommés via des robots ou des mécanismes d'automatisation. Pour de tels usages, il est recommandé le recours à la route API.

A noter que la DGA est dotée d'une solution ISPT qui lui est propre (cf. 4.7.3 Autres passerelles)

Par ailleurs, pour des besoins particuliers, des boîtes aux lettres fonctionnelles ou nominatives (adresse en @def.gouv.fr) hébergées directement sur l'Internet peuvent être mises à disposition dans le cadre du marché ASTEL-I en remplacement de MIM3.

Les anciennes adresses en @defense.gouv.fr ont été supprimées mi-septembre 2018.

3.1.7.2 Accès aux réseaux interministériels [SU-RMI] et autres réseaux extérieurs [SU-REX]

Document	Date	Origine	Type doc	Portée
Concept d'emploi "accès réseaux extérieurs" : note conjointe : n°D14-002653/DEF/EMA/CPI/AUT/NP / n°389/DEF/SGA/ADJ	10 mars 2014 12 mars 2014	SC1	Concept Emploi	MinArm Intradef S-SF
<i>Commentaire : Ce document traite des accès aux réseaux extérieurs de même niveau de confidentialité ou de niveau de confidentialité différente via des passerelles et des besoins cibles relatifs à ces passerelles : accès à des applications, échanges de données et besoins de services à l'utilisateur, dans le respect de la réglementation et du droit d'en connaître.</i>				
SLR des services "d'accès aux réseaux extérieurs" : note conjointe : n°D14-003482/DEF/EMA/CPI/AUT/NP / n°687/DEF/SGA/ADJ/NP	27 mars 2014 14 mai 2014	SC1	SLR	MinArm Intradef

Ces accès sont réalisés au travers de passerelles : cf. 4.7 Interconnexions, passerelles et solutions de sécurité iso/multi niveaux

3.1.8 Téléphonie

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°7 portant sur la téléphonie sur le protocole internet publiée au Bulletin Officiel des Armées	13 janvier 2009	DGSIC	Directive	MinArm
<i>Commentaire : Règles applicables à la ToIP.</i>				

Voir aussi : §5.1.7

Téléphonie et 5 ToIP / VoIP §5.2.

3.1.9 E-formation

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
e-formation	ILIAS	www.ilias.de	Learning Management System (LMS) : plateforme d'enseignement à distance/ DR	R / S	Intradef Internet
e-formation	Suite SCENARI	Université Technologique de Compiègne (UTC) et société KELIS	Logiciel libre. Atelier de production de chaîne éditoriale	R / S	MinArm
e-formation	Moodle	Moodle HQ	Learning Content Management System (LCMS) : système de création et de gestion de contenu pédagogique pour alimenter un LMS. Logiciel libre sous licence GNU GPL.	R / S	MinArm

3.1.10 Services divers

3.1.10.1 Traduction [SU-TRL]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
traduction	REVERSO			D / -	S-SF SIA FrOps
traduction	CRISTAL	AND		I / -	S-SF SIA FrOps
traduction	- SYSTRAN Pure Neural Server (SPNS 9) ou - SYSTRAN Translate Server (STS 10)	Systran SAS (FR)	- Traduction neuronale disponible pour 55 langues, portail de traduction, web services (API REST) - OS : RHEL/Almalinux pour STS10 (RHEL/Centos 7 ou 8 pour SPNS9) - Intègre nativement un OCR, en option connecteur possible vers un outil de transcription de la parole - Mode SaaS (souverain européen OVH) ou on-premise (CPU ou GPU) - Outil non soumis à des restrictions export ni à des juridictions extra-européennes - Intégré dans ARTEMIS.IA	A / S	MinArm

3.1.10.2 Traitement de la parole

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Transcription de la parole	Vocapia (VoxSigma TRANS)	Vocapia Research (FR)	- 25 langues disponibles dont langues d'intérêt MINARM, outils d'adaptation disponibles, API REST, OS Linux - Mode SaaS ou on-premise - Déployé dans FCR-M (SIA-rents)	A / S	SIA SF
Identification de la langue parlée	Vocapia (VoxSigma LID)	Vocapia Research (FR)	Brique unique intégrant l'identification de plus de 120 langues, variantes et dialectes (dont langues d'intérêt MINARM), API REST, OS Linux, mode SaaS ou on-premise	E / E	MinArm

3.2 Socle des applications

3.2.1 Généralités

3.2.1.1 Concepts fondamentaux

Les applications réalisées, aussi bien en interne qu'en externe, au profit du ministère des armées répondent aux critères principaux suivants :

- **Indépendance technologique** : l'application doit pouvoir s'exécuter indépendamment de son environnement (système d'exploitation virtualisé ou non) et du mode d'accès (client léger, client riche, etc.), en évitant autant que faire se peut tout déploiement spécifique sur le poste client ;

Client léger, la règle / client lourd, l'exception

Lors de la validation des architectures, le recours à un client lourd devra être dûment justifié.

Compatibilité des navigateurs

Les projets doivent être compatibles avec tous les navigateurs recommandés, les autres navigateurs étant susceptibles d'être désactivés sans préavis ou d'entraîner des limitations sur le poste utilisateur (accès ISPT, ...). Pour les fonctionnalités conformes à des normes (notamment HTML, ...), il est recommandé d'éviter de prendre ce qu'un éditeur de navigateur aurait pu ajouter en surcouche d'une norme, quelles que soient les justifications légitimes ou non de l'éditeur, au risque qu'en cas de retrait futur de cette fonctionnalité par l'éditeur, cela perturbe le fonctionnement des applicatifs qui y auraient eu recours.

- **Rationalisation des techniques utilisées** : limiter le spectre des compétences des architectes, des développeurs mais aussi des exploitants permet de circonscrire les éventuels surcoûts liés à l'acquisition, puis à la maintenance, de compétences trop dispersées ;
- **Interopérabilité native** : anticiper l'interopérabilité, notamment en facilitant l'accès à la couche métier dans un contexte « SOA²¹ », permet de diminuer les efforts ultérieurs nécessaires à

²¹ Service Oriented Architecture, architecture orientée services.

l'intégration de l'application dans le socle ministériel.

En termes d'architecture :

L'architecture générique d'un système d'information doit répondre à de multiples contraintes (sécurité, maintenabilité, mise à l'échelle, exploitabilité ...). Ceci induit *a minima* un découpage en couches (présentation HTML5, CSS3, moteur exposant des services au travers d'API et stockage).

Afin d'éviter un système d'information monolithique difficilement maintenable au fil du temps, il est recommandé de l'organiser en services (granularité à adapter en fonction des besoins et des performances attendues), de s'appuyer sur les services et les données de références existants (API), d'offrir en retour des services/données à valeur ajoutée susceptible d'intéresser d'autres services sous forme d'API (*cf. 3.2.1.3.2 Stratégie API – corpus documentaire API.*)

★★★★★
Faire valider en SC²A le plus en
amont possible l'architecture du SI.
★★★★★

Le système d'information doit s'appuyer sur des services mutualisés mis en place sur les réseaux supports : service d'authentification, service de temps, service de nommage...

Afin de fluidifier le processus d'hébergement, les directions d'application doivent faire valider leur architecture (architecture applicative, spécifications techniques, intégration sur le/les réseaux supports, déploiement) par les instances de gouvernance technique (*cf. 1.4 Gestion et gouvernance du CCT*) (sur dossier ou en présentation) au moment de la revue de conception générale. À tout moment, sur expression de besoin auprès de la sous-direction client de la DIRISI (FEB), le bureau architecture amont (Service projets) peut également être utilement sollicité par les directions d'application afin d'évaluer la conformité de leur solution avec le cadre de cohérence technique.

3.2.1.2 Démarche et principes liés aux solutions en nuage (cloud)

Le ministère a repensé son architecture d'hébergement afin de se doter des outils nécessaires permettant de répondre à son ambition numérique. Se concentrant en premier lieu sur les environnements Intradef et Internet, il a lancé un chantier de « cloudification » qui vise à transformer ses plateformes techniques d'hébergement de sites et applications en une offre de service d'hébergement standardisée et maîtrisée dans la durée.

Cet investissement est réalisé afin de :

- permettre des mises en service rapides et fiables sur les différents environnements grâce aux apports de la simplification des processus, de l'automatisation et de la standardisation (DevSecOps)
- assurer une continuité de service et une résilience accrues apportées in fine par une redondance locale (deux salles d'un même datacenter) et régionale (entre deux datacenter)
- disposer d'une capacité d'enrichissement des services au fur et à mesure grâce à des plateformes évolutives par conception et aptes à offrir les technologies les plus récentes dans ses prochaines versions (orchestration de conteneurs, capacité GPU pour l'IA, Zero Trust, Data Centric Security ...)
- assurer une sécurité et une maîtrise accrues via la mise en œuvre de mécanismes d'observation de bout en bout et d'audit durant tout le cycle de vie des applications
- disposer de plateformes maîtrisées par le Ministère, conformes aux normes et standards modernes et opérables en autonomie

Cette offre de service cloud s'appuie sur 3 plateformes :

- PICSEL : première étape du parcours cloud, la plateforme PICSEL apporte des outils de développement et de tests modernes conformes à l'état de l'art. La mise à disposition de services

représentatifs des différents environnements facilite les tests. Le contrôle qualité et le mécanisme de livraison automatisé (CI/CD orientée GitOps) fiabilisent et accélèrent la mise à disposition aux utilisateurs ;

- C1DR : partie du cloud destinée à la mise en œuvre rapide et automatisée de sites et d'applications au profit du personnel du Ministère. La plateforme C1DR s'intègre pleinement aux services du socle numérique tout en offrant des garanties de sécurité et de résilience adaptées. Chaque application y dispose de son espace dédié et protégé, mais reste capable d'échanger de manière maîtrisée avec les autres applications ou services, y compris ceux hébergés sur Internet ;
- C1NP : partie du cloud destinée aux sites et applications exposés sur Internet. Bâtie sur le même modèle et les mêmes standards que C1DR et PICSEL et disposant des mêmes services que ces derniers, cette plateforme est dotée de mécanismes de sécurité complémentaires adaptés à cet environnement plus exposé.

La capacité d'hébergement avec orchestration de conteneurs sera progressivement ouverte sur PICSEL au dernier trimestre 2023 et doit être opérationnelle sur C1DR fin 2024. Le SC²A vérifiera la pertinence technique du recours à ce type de technologie pour les systèmes d'informations concernés ainsi que l'acceptabilité des composants utilisés (notamment par examen des dockerfiles et du SBOM).

Parallèlement, ces offres d'hébergement seront enrichies de façon à fournir des capacités de CPU haute fréquence et GPU aux systèmes d'information (sous le nom « offre GPU »). En vue de garantir la capacité des Datacenter à répondre aux besoins importants induits par ce type de technologie (énergie et refroidissement notamment), le matériel mis en place devra se conformer aux spécifications suivantes :

CPU		
Type processeur	Intel Xeon 6338N – 32 coeurs	AMD Epyc 9354 32 coeurs
Fréquence	2,2 Ghz	3,25 Ghz
Extension aux jeux d'instructions	MMX – SSE – SSE2 – SSE 3 – SSE 4.2 – AVX – AVX2 – AVX 512 – FMA3 – F16C	MMX – SSE – SSE2 – SSE 3 – SSE 4.2 – AVX – AVX2 – AVX 512 – FMA3 – F16C
Usages	Courant Type : Bdd, Portail applicatif, Web, etc	A justifier Application monothread ou à processus séquentiels
Infrastructure	SHSM, C1DR, ISHM	Clustet fréquentiel C1DR
GPU		
Type GPU	L40S	H100
Capacité Mémoire	48 Go	80 Go
Bande passante	864 Gbit/s	2 Tbit/s
FP64	NA	26 Tflops
FP64 Tensor Core	NA	51 Tflops
FP32	91,6 Tflops	51 Tflops
TF32 Tensor Core	366 Tflops *	1513 Tflops *
FP16 Tensor Core	733 Tflops *	1513 Tflops *
FP8 Tensor Core	1466 Tflops *	3026 Tflops *
Usages	Intelligence Artificielle	A justifier

* Avec dispersion structurelle. Sans dispersion, les spécifications sont deux fois moins élevées

Les niveaux de service de ces nouvelles offres sont identiques aux offres historiques.

A date, l'offre d'hébergement reste à dessein adossée aux mêmes technologies (machines virtuelles, systèmes d'exploitation, déploiement automatisé Ruche, authentification MindefConnect ...) que celles utilisées au

sein des hébergements actuels (SHSM DR, Heliss NG), ce qui permet à une application conforme au CCT d'être rapidement et facilement migrable.

Plus précisément, pour être éligible C1NP ou C1DR, une application doit :

- disposer d'une pile logicielle à jour et soutenue en MCO/MCS
- disposer de scripts de déploiements Ruche conformes (ceux de C1NP sont identiques à ceux d'Itradef)
- s'adosser à l'authentification MinDefConnect de l'environnement support
- exporter ses journaux d'évènements applicatifs dans le puits de log (C1NP dans un premier temps)
- instancier à minima l'API REST d'observabilité (l'instrumentation pourra être enrichie via développement mais c'est laissé à l'appréciation du projet de ses besoins en la matière)
- gérer ses secrets et ses certificats via le service de socle Gestion des secrets (C1NP pour les secrets et les certificats non exposés sur Internet dans un premier temps)

Les 3 premiers points sont des exigences de conformité préexistantes, non spécifiques au cloud et rappelées systématiquement aux projets concernés dans les avis SC²A.

L'export des journaux d'évènements applicatifs ne nécessite que la configuration d'un agent et le raccordement à la gestion des secrets se limite le plus souvent à une opération technique simple.

L'implémentation de l'API d'observabilité (cf. 6.2.7.4) requiert quant à elle un petit travail de développement complémentaire, pour partie automatisable en utilisant le fichier OpenAPI de description fourni. En retour, la direction d'application ou de projet (ainsi que l'exploitant) bénéficie d'un suivi fiable de l'état effectif de bon fonctionnement de l'application incluant sa capacité à interagir correctement avec les services socles et autres applications avec lesquels elle est en interaction.

Ces exigences constituent le socle minimum requis pour s'assurer que l'application pourra être hébergée avec le bon niveau de sécurité, de maintenabilité, de disponibilité et de résilience sans obérer les capacités d'exploitation de l'opérateur. En conséquence, elles sont désormais requises pour tout nouveau projet et doivent également être prises en compte dans la feuille de route des systèmes d'information existants.

Règle	Énoncé	Statut	Portée
CCT_R1	<p>Il est OBLIGATOIRE que tout système d'information déployé sur les environnements C1NP et C1DR :</p> <ul style="list-style-type: none"> - soit déployé et mis à jour via des playbooks et collections ansibles conformes à celle définies dans le cadre du projet Ruche, - s'adosse à la seule authentification MinDefConnect de l'environnement, - exporte ses journaux d'évènements applicatifs dans le puits de logs de l'environnement, - instancie l'API REST d'observabilité du Ministère, - gère ses secrets et les certificats X509 qui peuvent l'être via le service Gestion des secrets du socle. 	O	C1NP Intradef (Legagy et C1DR)

CCT_R2	<p>Il est RECOMMANDÉ que tout système d'information déployé :</p> <ul style="list-style-type: none"> - soit déployé et mis à jour via des playbooks et collections ansibles conformes à celle définies dans le cadre du projet Ruche, - s'adosse au service d'authentification du socle disponible dans l'environnement, - soit en capacité d'exporter ses journaux d'évènements applicatifs dans le puits de logs de l'environnement, - instancie l'API REST d'observabilité du Ministère, - soit en capacité de gérer ses secrets et les certificats X509 qui peuvent l'être via un service Gestion des secrets du socle. 	R	MinArm
--------	---	---	--------

A noter que sur les environnements autres que C1NP et Intradef (C1DR et Legacy), l'infrastructure Ruche n'est pas disponible à date. Le déploiement nécessitera donc que le projet instancie une machine virtuelle hébergeant un moteur ansible pour utiliser ses playbooks et collections.

Mais pour tirer la quintesse des bénéfices du cloud, notamment en cas de recours à un hébergement en conteneurs orchestrés, une application devra être conçue sous forme de services et respecter dans sa conception un certain nombre de principes, notamment les 12 facteurs (<https://12factor.net/fr>):

- disposer d'une source de code unique. Ce n'est que lors du déploiement que les paramètres spécifiques à l'environnement sont injectés.
- ses dépendances devront être explicitement déclarées, l'application ne devant pas se reposer sur la présence supposée d'une bibliothèque ou exécutable du système d'exploitation. Les dépendances devront être disponibles dans l'instance MEDUSA de l'environnement cible.
- les éléments de configurations devront être communiqués via variables d'environnement ou récupérés dans un service (données standards ou secrets, ces derniers étant gérés par GDS).
- toutes les ressources externes (bases de données, caches, messagerie, file de messages) seront accédées via des URL ou équivalent, en utilisant des protocoles sécurisés et les authentifications associées.
- l'assemblage sera réalisé sur PICSEL avant la publication, et non lors de l'exécution, avec la capacité de revenir immédiatement à une version précédente en cas de problème.
- l'application sera conçue sous forme de processus sans états et indépendants, les données persistées devant se trouver dans une ressource externe, typiquement une base de données. Le système de fichier local ou la mémoire ne pourront être utilisés que de manière locale, temporaire et ponctuelle, leur persistance n'étant jamais garantie. Aucun mécanisme de session persistante ne sera mis en œuvre. Un processus doit pouvoir s'exécuter sur des machines physiques différentes à tout moment. De plus, ils ne doivent pas s'exécuter comme des démons mais s'appuyer sur le gestionnaire de processus du système. Enfin, les journaux d'évènements doivent être émis sur le flux de sortie standard, gérer proprement les signaux d'arrêts, les redémarrages et la reprise après plantage.
- les services seront exposés uniquement via une URL et un port, sans présupposer de l'existence d'un service d'exposition tiers (type serveur web).
- les services doivent être considérés comme jetables et disposer d'API interrogeables pour indiquer leur bon fonctionnement (heartbeat, ce qu'apporte l'API d'observabilité, cf. 6.2.7.4) et leur capacité à traiter des requêtes (readiness).
- les éventuels processus d'administration doivent se lancer dans des environnements identiques à ceux des autres processus et faire partie des livraisons de l'application.

- les applications devront disposer de tests automatisés permettant d'en vérifier le bon fonctionnement après une installation ou une mise à jour automatisée ainsi que de la capacité de revenir rapidement à la version précédente en cas d'anomalie (application et base de données, notamment).

La conception de ce type d'applications implique en outre que les développements se fassent avec les mêmes briques logicielles et ressources que celles de production et disposer d'une couverture de tests suffisante et adaptée (unitaires, fonctionnels, métiers, IHM), exécutés dans un environnement d'intégration continue afin de prémunir au maximum des incidents découverts en production.

3.2.1.3 Transformation numérique

3.2.1.3.1 Agilité

Document	Date	Origine	Type doc	Portée
Guide DGSIC n°15 portant sur l'agilité dans le cadre de la transformation numériques diffusé par note N°209/ARM/DGSIC/DG/NP du 4 mai 2018 <i>Commentaire : Dans ce cadre de la transformation numérique, le guide ministériel relatif à l'agilité a vocation à aider les usagers, les collaborateurs métiers, les acheteurs et les différentes équipes de projets et de programmes à mettre en œuvre une démarche agile. Ce guide propose une articulation autour de 5 thèmes :</i> - l'incubation de services numériques - les méthodes agiles - l'agilité et les aspects marchés - l'agilité et la réalisation technique - la sécurité numérique en démarche agile	4 mai 2018	DGSIC	Guide	MinArm

3.2.1.3.2 Stratégie API – corpus documentaire API

Dans le cadre de sa transformation numérique, le ministère des Armées doit pouvoir bénéficier d'un SI plus modulaire, plus ouvert et aux composants facilement réutilisables. L'enjeu des prochaines années est de mettre en œuvre une stratégie d'« API-sation » cohérente et standardisée à l'échelle du ministère des Armées et s'intégrant pleinement à la démarche interministérielle.

Déployée d'abord sur Intradef et Internet, la mise en œuvre de cette orientation s'appuie sur un corpus documentaire en cours de production devant être cohérent de documents existants ou produits par ailleurs.

Le corpus API est constitué :

- d'un document d'orientation générale : la politique générale relative aux API ;
- d'un ou plusieurs documents relatifs au « management des API » et notamment une directive relative à la gouvernance des API ;
- de documents de normalisation et notamment la directive DGSIC 19 rénovée, le cadre technique de mise en œuvre des API REST et le guide de conception des API (*cf. §3.2.4*) ;
- de documents techniques relatifs aux composants d'architecture mis en place (passerelle API, plateforme d'exposition et de management (PEM) des API REST dite API Gateway, démarche simplifiée...) au fur et à mesure de la disponibilité des services associés ;
- Un site de publication des données mises à disposition par l'intermédiaire de la PEM.

Document	Date	Origine	Type doc	Portée
Politique générale sur les API version 1 diffusée par note n°276/ARM/DGNUM/DG/NP du 24 juillet 2020	24 juillet 2020	DGNUM	Politique	MinArm
Directive DGNUM n°48 relative à la gouvernance des API au sein du ministère des armées diffusée par note n°276/ARM/DGNUM/DG/NP du 24 juillet 2020	24 juillet 2020	DGNUM	Directive	MinArm

3.2.1.4 Hébergement mutualisé

L'opérateur de défense exploite, via les CNMO-SI²², un socle d'exécution permettant la rationalisation et la mutualisation des ressources techniques, tels que locaux techniques, serveurs, licences, socles applicatifs et déchargeant les directions de projet des problématiques d'acquisition de ces moyens. De plus, l'homogénéité de la plate-forme permet une rationalisation et une maîtrise des compétences à détenir par l'hébergeur.

Cet hébergement mutualisé, en environnement NP maîtrisé/DR zone de confiance comme en environnements classifiés est structuré autour de 3 offres de prestation de service (salle blanche, serveur privé virtuel (VPS), infogérance, selon les réseaux) et, pour chacun, 4 niveaux de services (Bronze, Argent, Or, Platine) (*cf. détails §6.1.1 Références générales sur l'hébergement*) .

Une opération d'investissement « hébergement » actuellement en cours vise à faire évoluer ces hébergements vers une offre de service cloud standardisée :

- sur Intradef (C1 DR) en remplacement des SHSM DR début 2024 pour les environnements d'intégration, de pré-production et de production ;
- sur Internet (C1 NP) début 2024 en remplacement de PHEBIA et Heliss NG dont les décommissionnements interviendront respectivement fin avril et fin décembre 2024 ;
- Partie intégrante de cette offre cloud, la plateforme de développement, d'expérimentation et de qualification PICSEL permet aux centres de développements, aux TMA dotées de comptes Intradef et aux directions de projet de s'assurer de la qualité et de l'intégrabilité de leurs applications sur les deux environnements précédents.

Ces hébergements reprennent les technologies utilisées précédemment, les performances et les services actuellement offerts et vont y apporter progressivement une part croissante d'automatisation. Cette dernière qui s'appuie notamment sur le projet Ruche (technologie ansible) aura pour premier bénéfice de réduire les délais de mise à disposition des hébergements pour les systèmes d'information sur système d'exploitation durci et le raccordement à différents services d'infrastructure (DNS, NTP, antivirus, sauvegarde, comptes de service, gestion des licences mais aussi supervision, puits de journaux d'évènements applicatifs). Plusieurs outils assureront une plus grande maîtrise et une plus grande sécurité : aux outils précédemment cités et au durcissement des systèmes d'exploitation installés, s'ajoutent les dépôts de logiciels sécurisés via le projet MEDUSA, le suivi de conformité tout au long de la vie du système d'information via le SI Conformité et un gestionnaire des secrets (mot de passe des comptes applicatifs, certificats) via le projet GDS. De plus, chaque application est installée dans un espace cloisonné (technologie NSX-T) la préservant des attaques latérales en cas de compromission d'une autre application hébergée sur la plateforme.

Dans un second temps, C1 NP apportera également des environnements d'intégration accessibles de manière contrôlée depuis Internet. En attendant, l'intégration sera réalisée par la TME sur les environnements de préproduction.

Des capacités complémentaires telles qu'une extension du stockage de masse (réseau DR, NP et S-SF) ont également été ajoutées. Vont suivre fin 2024 une capacité d'hébergement de conteneurs orchestrés ainsi la possibilité de disposer de capacités de calcul supérieures recourrant à des processeurs graphiques (GPU).

²² Centres nationaux de mise en œuvre des systèmes d'information.

Voir 3.2.1.2 pour les prérequis s'imposant aux applications afin qu'elles soient éligibles à cette offre de service cloud et puissent en tirer pleinement parti.

La migration des systèmes d'informations vers ces hébergements cloud est l'objet de la manœuvre dite « move to cloud », actuellement focalisée sur le domaine Internet et qui nécessite l'investissement des directions d'application et de projet et de leurs DSI Domaine pour la mener à bien dans les temps impartis²³ avec l'appui de dispositifs mis en place par l'opération (centre de compétence cloud, appui DGNUM/DIRISI/AND et support PICSEL).

La plateforme de développement et d'expérimentation PICSEL sera systématiquement utilisée pour valider la conformité et la qualité des adaptations réalisées.

3.2.2 Hébergement d'applications

3.2.2.1 Services Web / Serveur de présentation [HSW]

Document	Date	Origine	Type doc	Portée
Recommandations pour la sécurisation des sites Web <i>cf.4.5 Sécurisation des COTS</i>	22 avril 2013	ANSSI	Note technique	Toute administration
Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur <i>cf.4.5 Sécurisation des COTS</i>	28 avril 2021	ANSSI	Note technique	Toute administration

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Serveur de présentation	Apache HTTP Server	Apache Foundation		R / S	MinArm
Serveur de présentation	IIS (inclus dans Windows Server)	Microsoft	Si environnement Microsoft retenu	R / S	MinArm
Serveur de présentation	Tomcat	Apache Software Foundation		R / S	MinArm
<i>Commentaire : RedHat, après l'avoir retiré de sa distribution Linux, vient de réintégrer Tomcat aux paquets (tout comme AlmaLinux), il n'est donc plus nécessaire ni autorisé d'utiliser des distributions binaires tar.gz.</i>					
Serveur de présentation	NGINX	NGINX (racheté par F5 Networks)	Ce serveur est très largement utilisé sur l'internet.	R / S	MinArm
<i>Commentaire : Dans la plupart des cas, un httpd Apache correctement configuré répondra au moins aussi bien et apportera plus de richesse fonctionnelle grâce à ses modules. NGINX sera en revanche bien adapté pour servir des ressources statiques sous forte charge.</i>					
Proxy et équilibrEUR de charge	HAProxy	HAProxy Technologies	Solution recommandée hors infogérance pour assurer les fonctions de haute disponibilité, de répartition de charge et de proxy HTTP et TCP,	A / S	MinArm

²³ Pour mémoire, la plateforme PHEBIA sera décommissionnée fin avril 2024 et la plateforme Heliss NG fin décembre 2024. Les plateformes SHSM DR actuelles doivent arriver en fin de vie vers 2028.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
<i>Commentaire : Dans le cas d'un système déjà en infogérance sur SHSM DR, ces fonctions sont assurées par les équipements réseaux matériels du Datacenter (type NetScaler) et pas par HAProxy. Pour les SI hébergés en VPS sur SHSM DR et CIDR, la fonction LB doit être portée au niveau logiciel par le SI (HA Proxy à inclure dans son architecture) dans l'attente de la mise en place, pour les SI hébergés sur CIDR, d'une répartition de charge basée sur l'outil VMWARE NSX.</i>					

3.2.2.2 Serveurs d'application et environnements d'exécution

Un serveur d'applications est un logiciel offrant un contexte d'exécution pour des composants applicatifs. Le terme est apparu dans le domaine des applications web. Dans un sens strict les composants hébergés par le serveur d'applications ne sont pas de simples procédures ou scripts mais de réels composants logiciels conformes à un modèle de composants.

S'assurer que les dépendances ou librairies liées à l'environnement d'exécution font l'objet d'un suivi en sécurité au travers des dépôts ministériels DECOS (MEDUSA en cible) ou y sont éligibles (cf. 8.6 Critères d'éligibilité des produits et solutions) ou alors font l'objet d'une contractualisation d'un suivi de sécurité et de traitement des obsolescences par la direction d'application.

Par ailleurs, de tels environnements nécessitent parfois des piles logicielles d'exécution non soutenues.

Numéro	Énoncé de la règle	Statut	Portée
RT_DEV_03	L'usage <u>de bibliothèques adhérentes à des outils de développement propriétaires</u> est fortement INTERDIT	D	MinArm

Ces recommandations sont valables pour un développement réalisé en interne au ministère comme pour des développements réalisés par des prestataires externes : le maintien en condition de sécurité de ces bibliothèques ou composants d'exécution embarqués doit être un critère d'homologation, et, pour des réalisations externalisées, doit faire l'objet d'une exigence auprès de l'industriel.

3.2.2.2.1 Environnement d'exécution Java

3.2.2.2.1.1 Composant binaire d'exécution Java (JRE / JDK)

En raison de l'évolution de la politique commerciale de la société ORACLE vers un modèle de licence contraignant et payant sur le composant binaire d'exécution des applications Java, dès la version 9, des orientations ministérielles fortes ont été prises sur ce sujet. Ces orientations ont fait l'objet d'une présentation en CECNUM du 9 avril 2019 et d'une note d'orientations ministérielles.

Les systèmes du ministère doivent systématiquement recourir à une instanciation binaire JRE²⁴ de l'OpenJDK comme suit :

- Sur un serveur Linux (Redhat, Centos, Debian et AlmaLinux), l'instanciation binaire JRE d'OpenJDK fournie par la distribution ;
- Sur un serveur Windows, l'instanciation binaire JRE d'OpenJDK fournie par Eclipse Temurin (ex AdoptOpenJDK).

²⁴ Le JRE est le composant nécessaire à l'exécution d'applications Java compilées, contrairement au JDK qui y ajoute des outils de développements qui n'ont pas leur place en environnement de production.

Pour les cas où un support serait nécessaire :

- Sur un serveur Linux, utiliser une distribution RedHat qui apportera ce support ;
- Sur un serveur Windows, utiliser une instanciation binaire JRE OpenJDK non Oracle apportant ce support (Azul, IBM, RedHat ...).

Seules les versions LTS de JRE d'OpenJDK soutenues peuvent être utilisées (actuellement 8, 11 et 17).

Dans les situations où le JRE Oracle ne pourrait pas être remplacé, la direction de projet, après obtention d'une dérogation, devra :

- Selon la situation, demander au fournisseur du système d'information adhérent de mettre en place une feuille de route de migration vers un JRE conforme aux orientations ministérielles ou de faire réaliser la migration de son système d'information pour le rendre conforme ;
- Financer et faire mettre en œuvre une infrastructure matérielle pour l'hébergement des composants serveurs utilisant le JRE Oracle ;
- Financer les licences Oracle correspondant à cette infrastructure, ainsi que leur renouvellement.

Document	Date	Origine	Type doc	Portée
Orientations ministérielles suite à l'évolution de la politique de la société Oracle relative au composant JAVA, diffusées par note n°301 /ARM/DGNU/DG/NP du 25 juillet 2019	25 juillet 2019	DGNU	Note	MinArm
<i>Commentaire : cette note définit les modalités d'application des orientations relatives au composant Java suite à l'évolution de la société ORACLE. (cf supra)</i>				
Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows (cf. §4.5 <u>Sécurisation des COTS</u>)		ANSSI	Note technique	Toute administration

Composant binaire JAVA

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement java serveur	Oracle JRE ou Oracle OpenJDK	Oracle	Lorsqu'aucun autre JRE ne peut être utilisé. Le recours à cette solution implique systématiquement un hébergement sur machine physique dédiée.	A/S	MinArm
Environnement java serveur	JRE OpenJDK	OpenJDK Développeur	Toutes les distributions certifiées partagent le même code source et l'intégralité des fonctionnalités nécessaires à la certification Java. Elles se distinguent potentiellement par des compléments et par une offre de service du distributeur.	R/S (en lien avec l'OS utilisé)	Minarm
<i>Commentaire</i>					
	- sous Linux, utiliser l'instanciation binaire JRE de l'OpenJDK 8,11 ou 17 fournie par la distribution. Si un support est nécessaire, utiliser la distribution Linux RedHat ;				
	- sous Windows, utiliser Eclipse Temurin (ex AdoptOpenJDK) ou une autre JRE non Oracle si un support est nécessaire.				
Environnement java serveur	Java Standard Edition	tous éditeurs	Strictement interdit si hors versions LTS	I/-	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
<i>Commentaire : Ces versions non LTS, qui n'offrent pas de plus-value démontrée, ont une durée de vie de 6 mois (hors souscription pour celles d'Oracle) impliquant des coûts humains de mise à jour non compatibles avec la durée de vie des projets du Ministère et non pris en compte dans la démarche d'automatisation en cours.</i>					
Environnement Java serveur	Jakarta Edition	Enterprise Eclipse	Fondation Eclipse	Cf. section suivante sur les serveurs d'application Java et section 7.4.2 sur les versions. (ex. Java EE)	A/S MinArm

3.2.2.2.1.2 Serveurs d'application Java

Sur Intradef, les serveurs d'application et d'EJB mentionnés ci-dessous sont tous sous statut Assujetti : il est demandé aux directions d'application de se rapprocher de la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT).

L'architecture recommandée au Ministère des Armées privilégie le développement avec les framework Spring et Spring Boot plutôt que Jakarta EE (cf. plus bas) tant pour la productivité et la performance qu'ils apportent que pour la qualité de leur documentation.

La technologie Jakarta EE (anciennement Java EE) se décline version complète, avec le profil « Jakarta EE Platform », ou bien en versions allégées avec soit : le profil « Jakarta EE Core Profile » qui offre un runtime réduit par rapport au profil complet, ou bien le profil « Jakarta EE Web Profile » qui est adapté aux sites WEB.

Une initiative complémentaire, mieux adaptée à une architecture micro-services que Jakarta EE, a conduit à spécifier le « MicroProfile » (actuellement en version 6.0) qui intègre le profil « Jakarta EE Core Profile » plus quelques API java, non présentes dans Jakarta EE, mais pertinentes pour des micro-services (par exemple pour gérer la tolérance ou panne, ou interroger l'état de santé d'un micro-service). Du fait de sa complexité et des coûts potentiellement induits en exploitation, une architecture micro-services doit être réservée à des cas d'usages pertinents et reste donc assujetti à une validation par le SC²A.

La complexité de l'édition Entreprise de Java a longtemps été causée par la multiplicité des modèles de composants et des conteneurs d'exécution spécifiques à chacun (composants Servlet, JSF, EJB session, EJB Entité, etc...) qui rendait le code peu portable et nécessitait une mécanique d'exécution complexe et donc moins performante et fiable qu'une architecture à base de classes Java standard (nommée POJO). C'est pourquoi les composants EJB ont été fortement décriés et ne sont pas recommandés au Ministère. Conçu pour offrir une alternative, le Framework Spring qui a largement fait ses preuves depuis utilise un mécanisme dit « d'injection de dépendances » qui a finalement été implémenté dans Jakarta EE, sous le nom de « Contexts and Dependency Injection (CDI) ».

En résumé, l'emploi de Jakarta EE reste assujetti à une validation du SC²A afin d'éviter l'emploi d'un serveur d'application supportant cette spécification autant que possible. Il est recommandé une architecture plus simple basée sur un simple serveur de servlet comme Tomcat qui saura répondre au besoin dans la plupart des cas tout en allégeant les charges de développement, de maintien en condition opérationnelle et d'exploitation.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Serveurs d'applications	Tomcat	Fondation Apache	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits	* / *	MinArm

Commentaire : Tomcat est suffisant pour supporter Jakarta EE Web Profile. C'est l'option à privilégier pour les nouveaux développement avec Spring et Spring Boot Framework.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Serveurs d'applications et d'EJB	TomEE	Fondation Apache	Serveur d'application pour Jakarta EE	A / S	Intradef
Serveurs d'applications et d'EJB	Enterprise Application Platform JBOSS EAP	RedHat	Serveur d'applications JEE	A / S	Intradef Internet
<i>Commentaire : Ces deux serveurs ont un statut « Assujetti » car Jakarta EE est globalement assujetti. Cela dit parmi tous les autres serveurs certifiés Jakarta EE (par exemple Glassfish, Payara ou Wildfly), TomEE est la solution à privilégier si un support n'est pas nécessaire (avec une installation sur AlmaLinux par exemple) et JBoss EAP est à privilégier si un support est souhaité (avec l'OS RHEL du même éditeur RedHat). Dans les deux cas, le micro-profil est disponible. Les autres solutions sont déconseillées pour réduire le nombre de solutions à maîtriser en exploitation.</i>					
Serveurs d'applications et d'EJB	Glassfish	Eclipse Foundation	Serveur d'applications JEE8 en production, centralisé.	D / S	MinArm
Serveurs d'applications et d'EJB	Payara Server	Payara Services Ltd	Serveur d'applications JEE	D / S	MinArm
Serveurs d'applications et d'EJB	WildFly	RedHat	Serveur d'applications JEE	D / S	Intradef Internet S-SF SIA FrOps
<i>Commentaire : Le SC²A attire, par ailleurs, l'attention des projets sur le cycle de vie particulièrement court de cette solution (une nouvelle version majeure tous les 3 mois) qui va imposer à minima au projet une charge de MCO/MCS conséquente afin de la maintenir à jour et dans des versions supportées par leurs communautés ou éditeurs respectifs</i>					
Serveurs d'applications	Jetty	Fondation Eclipse	Serveur embarqué pour applications légères à réserver aux travaux de développement.	A / -	MinArm

Les dépendances complémentaires (jar) non présentes dans les dépôts de développement sur MEDUSA sont soumises à demande d'autorisation préalable et devront satisfaire les critères décrits en 8.6.

À noter que les déploiements d'applications Java doivent se faire en production par livraison d'archive war (ou ear pour les cas justifiés) : ce mode de livraison garantit la maîtrise de l'exploitant sur le serveur d'application et lui permet par exemple de procéder si besoin et de façon autonome à l'application d'une mise à jour de sécurité sans devoir attendre la mise à disposition d'une nouvelle version de l'application entière. En conséquence, la réalisation de « fat jar » embarquant un serveur est à réservé aux seuls travaux de développement.

3.2.2.2 Environnement d'exécution PHP

Document	Date	Origine	Type doc	Portée
Cadre technique relatif au développement PHP au sein du ministère de la Défense : Cf. §7.3.3 Développement en PHP				MinArm
<i>Commentaire : ce document essentiellement orienté développement contient des préconisations et règles techniques applicables dans la mise en œuvre d'un environnement d'exécution PHP.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement PHP	PHP	PHP Group	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	MinArm
Environnement PHP	PHP-FPM	PHP Group	Pour des sites en PHP devant subir des charges importantes (inclus avec PHP)	R / S	MinArm
<i>Commentaire :</i> En s'appuyant sur le cadre technique de développement PHP, tout nouveau développement voulant utiliser un Framework PHP doit utiliser une version de PHP récente et maintenue.					

Les modules complémentaires non présents dans les dépôts de développement sur MEDUSA sont soumis à demande d'autorisation préalable et devront satisfaire les critères décrits en 8.6.

3.2.2.2.3 Environnement d'exécution .Net

.Net est, à l'instar de Jakarta EE pour le langage Java, la plateforme associée au langage C# de Microsoft.

Dans un environnement Windows, il n'est pas nécessaire de disposer d'un serveur d'application pour héberger un programme, qui s'exécute alors comme un service Windows. Il est néanmoins possible d'utiliser IIS (Internet Information Service). Le recours à cet environnement d'exécution sur un serveur doit toutefois n'être envisagé que lorsque des spécificités ou effets recherchés ne sont pas atteignables à l'aide des environnements Java, JavaScript ou PHP et qu'une capacité de MCS et de MCO est durablement disponible.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
.NET	.NET, .NET Core	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	MinArm

3.2.2.2.4 Environnement d'exécution JavaScript

Dans le cadre de développement « backend » le recours à node.js est nécessaire. Il offre une alternative au développement d'un backend Java ou PHP et permet de réaliser un SI entièrement en Javascript.

Il est cependant nécessaire que les librairies et dépendances Javascript satisfassent aux critères décrits en 8.6 Critères d'éligibilité des produits et solutions et puissent être maintenues, suivies en configuration de sécurité. De plus, Javascript est une technologie foisonnante offrant souvent, parmi ceux qui sont éligibles, plusieurs frameworks ou bibliothèques différentes pour répondre à un même besoin : afin de garantir la capacité du Ministère à en garantir sa maîtrise et sa capacité à assurer le MCO des SI qui les utilisent, seul un nombre limité d'entre elles pourra être recommandé (cf. 7.3.5 Développement HTML5-Javascript-CSS). Les directions d'application peuvent se rapprocher de la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT) pour exprimer et faire valider leurs besoins.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement JS	Node.js	OpenJS foundation	Restreint aux versions paires soutenues [LTS]	R / S	MinArm

3.2.2.2.5 Environnement d'exécution Python

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement Python	Python	Python Software Foundation	Restreint au domaine de la science des données, à l'emploi d'outils d'administration, aux usages	* / *	MinArm

			scientifiques (IST) ou comme dépendance d'un autre logiciel sur étagère. * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>		
Framework Web	Django	Django Software Foundation (License BSD)	Les applications MVC doivent s'appuyer sur les technologies recommandées du CCT. Le langage python n'est pas interdit pour réaliser des applications WEB.	I / N	MinArm

L'environnement d'exécution Python est déjà requis par un certain nombre d'outils, notamment d'administration (dont Ansible). Son emploi est par ailleurs adéquat dans le domaine de la science des données.

En environnement d'exécution, les bibliothèques et dépendances devront satisfaire les critères décrits en **8.6 Critères d'éligibilité des produits et solutions**.

3.2.2.2.6 Environnement d'exécution R

Le langage et l'environnement d'exécution R sont autorisés pour un emploi dans les domaines des statistiques et de la science des données à condition de disposer d'une ressource de MCO pérenne.

Le recours à des bibliothèques complémentaires non présentes dans les dépôts de développement MEDUSA est soumis à demande d'autorisation préalable ; elles devront satisfaire les critères décrits en 8.6 Critères d'éligibilité des produits et solutions.

3.2.2.2.7 Environnement d'exécution Ruby

Déjà présent dans les distributions Linux en vigueur au ministère, l'environnement d'exécution Ruby est déjà requis par un certain nombre d'outils, notamment d'administration (dont Puppet). Son emploi pour des solutions dépassant ce cadre n'est pour le moment pas envisagé, notamment, du fait d'une popularité en amorce de déclin, de l'absence de facteurs suffisamment différentiant de Java, PHP, Javascript ou Python, d'un cadre ministériel de développement, de ressources de développement interne formées, du manque de compétences externes disponibles et d'une solution outillée de dépôts et de suivi des multiples bibliothèques complémentaires.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement Ruby	Ruby	Ruby Licence	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	* / *	MinArm
Framework Web	Ruby on Rails	Licence MIT	Les applications MVC doivent s'appuyer sur les technologies recommandées du CCT, et non sur le langage Ruby	I / N	MinArm

Commentaire : le langage Ruby n'a pas été retenu dans le portefeuille de technologies du Ministère qui n'investira pas dans son intégration au sein du processus de cloudification et d'automatisation. En conséquence, le recours à cette technologie ne sera pas autorisé pour un nouveau projet (développement interne et acquisition sur étagère).

3.2.2.2.8 Environnement propriétaire

Certains outils propriétaires (Windev, Webdev, FileMaker, ...) proposent en intégré et à titre de "meilleure productivité" des bibliothèques propriétaires ou nécessitent des environnements d'exécution, ou des serveurs

d'application propriétaires : ces bibliothèques ou composants ne font pas l'objet d'un suivi en sécurité tout le temps de vie de l'outil, et peuvent donc générer des failles de sécurité sur les systèmes construits à partir de ces bibliothèques ou composants d'environnement d'exécution, et, au-delà faire peser un risque de sécurité systémique sur l'écosystème dans lequel ils sont déployés (Intradef, Internet C1NP ...). Ils entraînent de surcroît une dépendance à leurs éditeurs commerciaux sur les plans financier, technologiques et fonctionnels allant à l'encontre de la recherche de souveraineté du Ministère en la matière.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement propriétaire	Windev Webdev Filemaker			I / N	MinArm
<i>Commentaire : tout nouveau développement sous Windev, Webdev ou Filemaker est interdit. Pour tous les projets déjà existants, une montée de version régulière est exigée jusqu'à la transition vers un nouveau système d'information ou une nouvelle technologie.</i>					

Voir aussi §7.3.7 Développement à l'aide d'outils « low-code » ou « no-code »

3.2.3 Portail des applications métiers

3.2.3.1 Moteur de workflow [WFL]

Cf. 3.2.4.6 Gestion de processus et de règles métiers

3.2.3.2 Process robotisés (RPA)

La RPA (Robotic Process Automation) consiste en l'automatisation de tâches, répliquant l'activité humaine. Elle permet d'effectuer des actions, identifiées comme simples et répétitives, plus rapidement et plus précisément que l'homme. Cette technologie s'articule autour de 3 grandes fonctions :

- le studio, qui permet de designer les robots,
- le robot, qui joue le rôle d'assistant, autonome ou interactif (stand-alone),
- l'« orchestrator », plateforme serveur, qui permet de piloter l'ensemble des robots.

Cette technologie doit être perçue comme une capacité temporaire d'automatisation de dispositifs anciens pour en améliorer le fonctionnement en attente de leur refonte basée sur des technologies plus récentes, robustes et maintenables, conformes à la politique ministérielle.

Document	Date	Origine	Type doc	Portée
Cadre des activités de Robotic Process Automation (RPA) du MINARM , diffusé par lettre n°197/ARM/DGNUM/DG/NP du 19 mai 2020	19 mai 2020	DGNUM	Cadre	MinArm
<i>Commentaire : Ce cadre précise les bonnes pratiques à respecter au sein du ministère des armées dans la mise en place d'un RPA.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
RPA (Process robotisés)	UiPath	UiPath		A / S	Intradef

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
<i>Commentaire :</i> Cette technologie devant être considérée comme un moyen temporaire d'amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d'une rejointe vers un environnement non dérogatoire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n'exonère pas du respect des règles de l'Intradef et de facto, n'autorise pas son emploi au travers d'ISPT.					
RPA (Process robotisés)	OpenRPA	OpenIAP	<i>Alternative opensource</i>	A / S	Intradef
<i>Commentaire :</i> Déploiement uniquement sur les postes de travail en automatisation d'actions manuelles réalisées par l'utilisateur de la session. Dans ce cadre, et sous réserve du maintien d'une action manuelle de validation des informations transmises, l'utilisation d'ISPT depuis un poste de travail pourra faire l'objet d'une demande de dérogation temporaire.					

3.2.3.3 Chatbot

Un chatbot, étymologiquement dialogue (chat) automatisé (bot) est un agent conversationnel permettant d'apporter des réponses à des demandes d'un utilisateur de façon automatisée.

On distingue :

- des chatbots simples reposant sur un dialogue basé sur des mots-clés dans un cadre préétabli et des bases de données préexistantes ;
- des chatbots plus complexes qui apprennent et s'améliorent en continu et reposent sur des mécanismes d'apprentissage automatique (machine learning).

Un outil de génération de chatbots a été élaboré avec la fabrique numérique. Il permet de créer facilement, via un playbook ansible, un service de chatbot pour une application basée sur des briques open source dont RASA constitue le cœur.

3.2.3.4 Moteur de règles

Pas de référence identifiée à ce jour.

3.2.3.5 Services de gestion des rôles et profils

Pas de référence identifiée à ce jour.

3.2.3.6 Services de gestion des règles d'accès

Pas de référence identifiée à ce jour.

3.2.3.7 Portail des applications mobiles sur Internet – Milistore

Document	Date	Origine	Type doc	Portée
Directive d'emploi MILISTORE version 1 diffusée par la note N°506418/ARM/EMAT/PNI/NP du 06/07/2022	2022	EMAT	Directive	MinArm

Commentaire : Milistore est la solution de l'Armée de Terre pour accéder depuis un téléphone personnel (BYOD) au catalogue d'applications ou de ressources ministérielles, et au besoin, interministérielles telles que TCHAP. Elle est accessible uniquement aux utilisateurs authentifiés par FranceConnect ou MindefConnect : les utilisateurs accéderont alors à un catalogue filtré selon leur profil, l'accès aux applications de Milistore pourra ainsi être restreint en fonction du rôle, de l'organisation ou de l'emplacement géographique de l'utilisateur.

La transposition de MILISTORE au sein du ministère des armées a fait l'objet d'une étude portée par la DGNUM au premier semestre 2020. Il en est ressorti une proposition de refonte de l'architecture technique. Aucune suite n'a pour autant été donnée à ce stade. Cette étude ne remet toutefois pas en cause la feuille de route de MILISTORE de l'Armée de Terre.

Chacune de ces applications devra avoir fait l'objet en préalable d'une déclaration complète dans SICLADE, d'une homologation, d'un visa du SC²A ainsi que d'un visa SaaS délivré par la DGNUM.

Les applications devront être prioritairement développées en Progressive Web App (PWA).

3.2.4 Échanges entre applications

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°19 édition 2 portant sur les échanges inter-applicatifs du ministère de la Défense diffusée par lettre n°72/ARM/DGNU/DG/NP du 8 mars 2019	8 mars 2019	DGNU	Directive	MinArm
<i>Commentaire : <u>À</u>cette 2^{ème} édition abroge la première version de 2011 en prenant en compte l'évolution technologique : sans écarter définitivement les technologies plus anciennes (SOAP...), ne serait-ce qu'au titre du legacy ou de certains besoins spécifiques, la nouvelle version préconise des architectures orientées services autour du modèle REST, en déclinaison de la stratégie API de l'état et du ministère et en conformité avec le RGI V2. Cette directive est complétée d'un cadre technique de mise en œuvre API (cf. 3.2.4.4)</i>				
Référentiel général d'interopérabilité [RGI] <i>Cf. 2.2.3 Les référentiels interministériels</i>				

Commentaire : Règles applicables aux échanges inter-applicatifs du système d'information du ministère des armées.

3.2.4.1 Généralités

Toute application s'inscrit aujourd'hui dans un contexte plus large que son seul périmètre fonctionnel. Les échanges inter-applicatifs permettent l'économie d'une saisie multiple, dispendieuse en temps et en personnel et source d'erreurs.

La mise en relation des applications s'effectue dans le cadre d'une approche Service Oriented Architecture (SOA). Dans cette approche, les besoins opérationnels sont définis en services et sont satisfaits par des systèmes et des moyens répartis qui s'exécutent et coopèrent dans un environnement réseau.

Cette approche impose une phase préalable d'analyse indépendante de l'implémentation, pour faire émerger une liste de services à partir des besoins opérationnels. Ces services sous-tendent la couche applicative et apportent modularité et une évolutivité accrue à l'application tout en la découplant des autres applications et services avec lesquels elle interagit.

L'économie est alors double, puisque s'ajoute à l'économie des données déjà évoquée une économie d'écriture des fonctions (services) déjà réalisées au travers d'autres SI. Il faut donc inciter à la réutilisation des composants et des services distants en facilitant les échanges de flux inter-applicatifs.

L'approche orientée service impose une grande rigueur de conception aux fournisseurs de services afin de garantir le découplage entre spécification du service et implémentation du service, ceci afin de ne pas compromettre l'évolutivité de l'implémentation. Ceci disqualifie notamment toute API générée automatiquement et calquée sur le schéma de données sous-jacent, ainsi que les outils et frameworks présentant cette approche.

Il en va de même des approches Capture Data Change (CDC) qui visent à propager des modifications apportées au niveau de la base de données vers des systèmes d'information tiers : en effet, un changement en base de données est avant tout la conséquence d'un événement métier qui implique (ou impliquera dans une évolution ultérieure) d'autres actions métier (une notification vers un utilisateur ou un autre service ou application par exemple). La modification en base de données ne pouvant refléter l'événement métier dans sa globalité, la technologie CDC doit être réservée aux seuls besoins purement techniques (réPLICATION par exemple).

3.2.4.1.1 Cas des échanges Intradef avec l'extérieur

Dans le cas des systèmes présents à la fois sur Internet et Intradef (ou Intradef et RIE), la sécurité des données sensibles (données à caractère personnel de personnel militaire, données sur l'état de santé, ...) conduit à promouvoir l'architecture suivante :

- un frontal accessible hors zone de confiance Intradef ne doit afficher que des données éphémères récupérées d'Intradef via des appels REST au travers de la passerelle API ;
- un stockage hors zone de confiance Intradef doit se limiter aux données non sensibles nécessaires à la résilience et à la performance du service ; les autres données sensibles étant stockées sur l'Intradef.

Les échanges de fichiers non protégés entre le frontal et la partie traitement Intradef se font :

- de manière asynchrone au travers de la passerelle Acheron (à noter que ce mode d'échange est déprécié et ne doit plus être utilisé pour les nouveaux projets, tandis que ceux qui l'utilisent déjà doivent d'ores et déjà préparer une évolution pour recourir à la passerelle API v2.1).
- de manière synchrone au travers de la passerelle API v2.1.

3.2.4.2 Échanges inter-systèmes

Ce chapitre fait référence aux prescriptions en matière d'échanges entre systèmes d'information de différentes administrations, entre domaines de sécurité ou bien encore pour des échanges massifs.

Profils d'interopérabilité recommandés par le Référentiel Général d'Interopérabilité (RGI)

Le RGI a introduit la notion de profils d'interopérabilité : un profil d'interopérabilité est un ensemble limité de standards, un groupe de spécifications à utiliser dans un contexte opérationnel, un usage déterminé. Dans sa version V2, le RGI a identifié 9 profils d'interopérabilité dont notamment 2 profils génériques dans des contextes d'échanges applicatifs :

Profil d'interopérabilité	Description / Utilisation / Restriction	Statut	Portée
Profil « Fondations État Plateforme »	Il constitue le socle de base en matière d'interopérabilité pour tous les échanges de type entre administrations, et entre les administrations et le citoyen ou l'entreprise. Il concerne plus particulièrement les échanges entre : les usagers, les « fournisseurs de services », les « fournisseurs de données », et la brique mutualisée « FranceConnect » tels que définis dans la stratégie État Plateforme. Le style d'architecture préconisé dans ce cadre est l'architecture REST . <i>(cf. description détaillée du profil RGI V2 p73)</i>	R	Toute administration
Profil « Web Service SOAP »	Ce profil répond aux mêmes types d'échanges que le précédent mais dans le cadre d'une architecture de services SOAP . Sa mise en œuvre est plus complexe, mais peut être nécessaire notamment dans	A	MinArm

	<p>le cadre d'échanges nécessitant une gestion transactionnelle (par exemple : transaction longue).</p> <p>Ce format de Web Service est toutefois en forte perte de vitesse au profit des architectures REST.</p> <p><i>(cf. description détaillée du profil RGI V2 p 74)</i></p>		
--	---	--	--

D'autres profils plus particuliers sont par ailleurs recommandés dans le cadre des échanges du monde de la protection sociale (INTEROPS), de l'archivage ou de la géomatique.

Échanges inter-applicatifs entre administrations

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
PRESTO V2	<p>« Protocole d'échanges standards ouverts ». Il pose les bases d'un protocole d'échange de messages informatiques entre applications pour servir les besoins de l'administration électronique.</p> <p>A n'utiliser que pour les cas d'utilisation en cours.</p> <p><i>Commentaire : PRESTO est un protocole d'échange de fichiers défini par l'administration française pour ses besoins propres. Ce protocole n'est plus entretenu et est classé « fin de vie » par le RGI. Une évolution ouverte vers REST de ce standard permettrait de le repasser à « recommandé ».</i></p> <p><i>Seule la version 2.0 peut encore être conservée pour les cas d'utilisation en cours (les versions antérieures font appel à des protocoles de sécurité dépassés)</i></p>	O	Toute administration

Échanges d'informations liées aux processus d'authentification et d'autorisation

Cf. §4.6.1 Sécurisation des accès

Moniteur de transfert

Un moniteur de transfert permet le transport sécurisé de grands volumes d'information entre sites distants.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Moniteur de transfert	CFT	Axway	Assujetti aux cas d'usage ne pouvant être couverts par une brique recommandée (ex : Camel, Talend) pour les échanges en interministériel	A / S	Intradef

3.2.4.3 Architectures SOA - Orchestration et logique métier

L'objectif d'une architecture SOA est d'exposer les fonctionnalités métier mutualisables sous forme de services accessibles à toutes les applications qui peuvent en nécessiter le traitement sous-jacent.

L'architecture SOA offre les moyens de mettre en phase rapidement et régulièrement le système informatique et l'ensemble des règles métiers utilisées, au rythme des évolutions imposées par les travaux d'urbanisation du système d'informations (changements techniques et fonctionnels). En conséquence, elle offre un moyen efficace d'aligner le système informatique sur l'expression du besoin fonctionnel en liaison avec les faisabilités et les contraintes techniques.

Le RGI V2 définit un profil d'interopérabilité pour ces architectures (cf. ci-dessus §3.2.4.2 Échanges inter-systèmes).

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Enterprise Service Bus	Open Studio for ESB ou version commerciale suivant les besoins ESB v5	Talend	Lorsque le recours à un ESB est justifié, il est RECOMMANDÉ d'utiliser l'ESB Talend pour les échanges de flux inter-applicatifs	A / E	MinArm
Enterprise Service Bus	ServiceMix	Apache	Assujetti au seul périmètre des applications s'appuyant sur le framework du SIA (échanges avec Fuse).	A / O	Intraced SIA FrOps
<i>Commentaire : Il est recommandé de directement recourir aux versions à jour des librairies historiquement embarquées dans ServiceMix (KARAF, CAMEL, CXF, ...), ce projet ne présentant aucune activité depuis plusieurs années (https://servicemix.apache.org/community/board-reports.html cf. Community Health... https://servicemix.apache.org/community/releases-schedule.html)</i>					

3.2.4.4 Architectures API – REST – PEM

3.2.4.4.1 Architecture API REST - PEM

Le cadre de réalisation de l’État Plateforme constitue un modèle d’ouverture des SI à travers les interfaces de type API et du style d’architecture REST. Un profil d’interopérabilité « État plateforme » est d’ailleurs défini dans le RGI V2 (cf. ci-dessus §3.2.4.2 Échanges inter-systèmes)

Document	Date	Origine	Type doc	Portée
Cadre technique de mise en œuvre des API au sein du ministère des armées, diffusé par lettre n°72/ARM/DGNUM/DG/NP du 8 mars 2019	Février 2019	DGNUM	Guide	MinArm
<i>Commentaire : Ce cadre décline et précise la directive DGNUM n°19 sur les échanges inter-applicatifs pour des API de type REST. Il décrit la manière de concevoir, sécuriser et développer des API et précise les bonnes pratiques à observer dans leur réalisation. La documentation est accessible (après authentification) sur le portail du SAND.</i>				
Guide de bonnes pratiques API : de la conception des APIs à l’exposition contrôlée des ressources	Avril 2015	SGMAP	Guide	Toute admin.
<i>Commentaire : Ce document cherche à recenser les principes directeurs associés à la conception, au développement et à l’exposition d’API. Les principes rassemblés dans ce guide sont applicables au ministère des Armées dans son propre environnement.</i>				
Guide de conception des APIs 1.0	16 avril 2021	DGNUM	Guide	Toute admin.
<i>Commentaire : Ce guide définit un cadre de développement des API en les rendant homogènes, cohérentes et conformes aux standards en vigueur ainsi qu'à l'état de l'art dans ce domaine. Ce document complète et précise, en fonction des sujets traités, certaines règles inscrites dans le "Cadre technique de mise en œuvre des API au sein du Ministère des Armées" v1.0 du 21/02/2019.</i>				

Afin de permettre la gestion et la gouvernance des API, le ministère met en place une « plateforme d’exposition et de médiation » (PEM)²⁵. Ce type de composant :

- fournit aux développeurs une plateforme permettant d’enregistrer et documenter les API (côté fournisseur d’API), de consulter la documentation des API, de les tester (côté consommateur d’API), de gérer des droits d'accès aux API (fonction de gestion) et d'obtenir des statistiques et indicateurs

²⁵ Composant dénommé passerelle API ou API Gateway dans la littérature informatique. Mais le terme « passerelle » est réservé au sein du Ministère aux dispositifs permettant des échanges de données entre réseaux de confiances ou de confidentialités différentes.

d'usage (fonction de pilotage) ;

- est médiateur des échanges entre des applications fournissant des services sous forme d'API et des applications les consommant. Le composant s'assure des autorisations d'accès à l'API, de la conformité des appels d'API en fonction des descriptions et droits d'accès enregistrés. Enfin il procède au routage de l'API vers le serveur ad hoc et protège le service exposé en assurant la mise en œuvre de politiques de sécurité (quotas d'appels, droits d'accès et d'usage...).

3.2.4.4.2 « Route API »

Le standard d'échanges API RESTful²⁶ s'impose dans les orientations interministérielles comme moyen de communication entre les systèmes d'informations de zones de confiance différentes pour consommer ou exposer des ressources conformément à la politique générale sur les API DGNUM.

Ces échanges inter-applicatifs entre l'Itradef et l'internet maîtrisé et non maîtrisé adressent les trois zones de confiance suivantes :

- L'Itradef ;
- L'internet maîtrisé (*Heliss-NG puis CINP*), c'est-à-dire une zone exposée à l'Internet **mais fortement sécurisée et infogérée par l'opérateur DIRISI** ;
- L'internet non maîtrisé (public) ;

Le ministère instancie cette technologie de PEM pour construire progressivement l'offre de service **Route API** permettant des échanges inter-applicatifs B2B²⁷ à l'intérieur de chaque zone et entre chaque zone :

- **Une PEM Intradef** pour mettre en relation via API RESTful des SI exclusivement à l'Itradef (donc jusqu'à niveau DR) ;
- **Une passerelle API [P.API]** pour mettre en relation via API RESTful des SI Internet maîtrisé avec des SI Intradef. La P.API repose sur les sous-systèmes suivants :
 - Une PEM P.API côté Intradef exposant des API NP pour des SI Internet maîtrisé ;
 - Une PEM P.API côté internet maîtrisé exposant des API uniquement NP pour des SI Intradef ;
 - Des moyens de sécurité entre les deux PEM (SAS API) permettant de sécuriser les échanges via API pour faire transiter des données structurées et des fichiers.
- **Une PEM Internet** pour mettre en relation via API RESTful des SI Internet non maîtrisé avec des SI Internet maîtrisé.

²⁶ Une API REST est une API qui respecte les principes de conception de REST, ou le style architectural de transfert d'état de représentation. Pour cette raison, les API REST sont parfois appelées API RESTful.

²⁷ B2B Business to Business désigne une relation d'entreprise qui fournit des biens ou des services à d'autres entreprises.

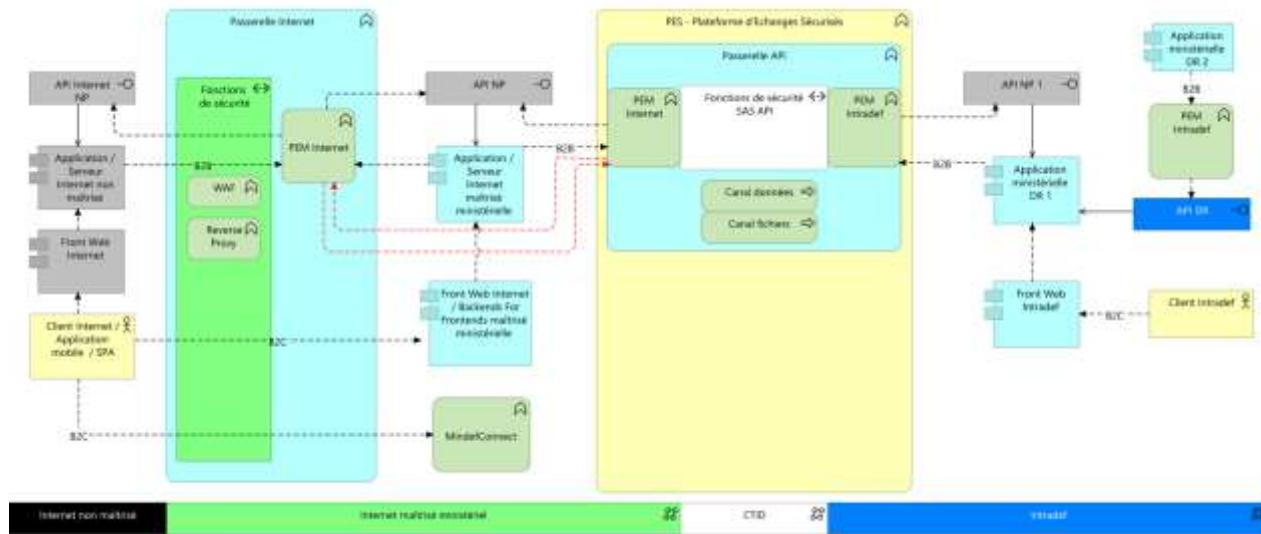


Figure 2 : Route API

Chacune de ces instances PEM suit des règles communes (standard de description, homologation de l’API, contrat d’usage entre consommateurs et fournisseurs de ressources) du cadre de mise en œuvre des API (cf. paragraphe précédent 3.2.4.4.1), ainsi que certaines spécificités liées à leur positionnement et leur rôle par exemple (une API susceptible de véhiculer des données de type DR ne pourra se trouver exposée que sur la PEM Intradef).

Des moyens seront progressivement mis en œuvre pour simplifier auprès des directions d’application la constitution de ces routes API tout en permettant à l’opérateur DIRISI d’avoir une supervision unifiée du dispositif.

Pour l’internet maîtrisé, le cadre d’hébergement très strict et très contraint induit par ces environnements particulièrement exposés impose aux applications des exigences complémentaires en matière de sécurité, et notamment pour celles dont le rendu est effectué côté client²⁸ (applications SPA²⁹, mobiles …) :

- Dans le cas d’échanges B2C³⁰, le client (qui n’est, par nature, pas maîtrisable par le ministère) ne peut pas faire appel directement aux API exposées par la passerelle API³¹ : il doit s’adresser à un serveur front web ou un SI rebond (pattern BFF³²) sur l’internet maîtrisé qui, seul, est ensuite autorisé à relayer les appels API via une PEM après contrôle, d’éventuels enrichissements et transformation de la base de l’URL³³. La consommation d’API par ce type de client depuis la PEM Internet n’est pas autorisée pour des raisons de sécurité (la protection du secret pour des appels API n’étant pas assurée) ;
- Les échanges API de type B2B entre l’internet maîtrisé et l’internet non maîtrisé doivent l’être

²⁸ Client Side Render (CSR) par opposition au rendu côté serveur ou Server Side Render (SSR) qui ne s’impose donc pas.

²⁹ Une application monopage ou SPA (« Single-page application » en anglais) est une implémentation d’application web qui ne charge qu’un seul document web, puis met à jour le contenu du corps de ce document via des API JavaScript.

³⁰ B2C Business to Consumer désigne une relation d’entreprise qui fournit des biens ou des services à des particuliers.

³¹ Les identifiants et mots de passe nécessaires – aucune API n’étant publique - pour consommer une API de la passerelle API (ou d’une PEM), sont uniquement attribués à des serveurs et donc aucunement à des clients.

³² Le pattern Backends For Frontends (BFF) consiste à créer des services « passerelles » adaptés aux besoins spécifiques de chaque client. Ces clients peuvent être des applications frontend ou des interfaces externes.

³³ Cette transformation, bien que peu contraignante, a pour avantage de ne pas divulguer à l’extérieur l’API telle qu’elle est exposée par la passerelle API en entrée d’Intradef.

exclusivement au travers de la PEM Internet. Des équipements de sécurité complémentaires portés par les services d'infrastructure ajouteront d'autres règles de sécurité ;

- Aucune API exposée par la passerelle API ne peut être consommée directement par un serveur hébergé en dehors de l'internet maîtrisé. Pour consommer une API de la passerelle API depuis l'internet non maîtrisé un serveur hébergé sur l'internet maîtrisé reste obligatoire jusqu'à l'ouverture de la Route API qui permettra sous certaines modalités d'échange de s'affranchir de celui-ci ;
- Les serveurs hébergés sur l'internet maîtrisé peuvent actuellement consommer directement des API externes (internet public), du moins après configuration des éléments de sécurité (les équipements de sécurité en sortie de plateforme permettant de suivre et de sécuriser les échanges) ;
- Les serveurs hébergés sur Intradef ne peuvent pas consommer directement des API externes (internet public) via la passerelle API. Pour consommer une API externe depuis l'Intradef un serveur hébergé sur l'internet maîtrisé reste obligatoire jusqu'à l'ouverture de la Route API qui permettra sous certaines modalités d'échange de s'affranchir de celui-ci.

Il est rappelé ici, que dans le cadre des échanges B2C, l'authentification de l'utilisateur doit reposer sur MinDefConnect Internet, exclusivement selon l'« authorization code flow » et que la gestion des droits incombe à l'application (via son serveur hébergé sur Heliss NG et à terme sur C1 NP).

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Exposition et médiation d'API [PEM]	PEM Intradef Instance ministérielle mutualisée basée sur le produit WSO2	MinArm WSO2	pour les échanges inter-applicatifs internes à Intradef via API	R / S	Intradef
Exposition et médiation d'API [PEM]	PEM pour la passerelle API Instances ministérielles mutualisées basée sur le produit WSO2	MinArm WSO2	Pour les échanges inter-applicatifs de l'Intradef avec la passerelle API Pour les échanges interapplicatifs de l'internet maîtrisé (Heliss-NG puis C1NP) avec la passerelle API	R / S	Intradef / Internet maîtrisé
<i>Commentaire : le ministère a mis en place des instances de PEM mutualisées en interne à l'Intradef (PEM Intradef) qui seront complétées fin S1 2025 par d'autres pour gérer la Route API entre internet et Intradef (composants de la passerelle API Intradef-Internet).</i>					
Exposition et médiation d'API [PEM]	PEM Internet Instance ministérielle mutualisée basée sur le produit WSO2	MinArm WSO2	Pour les échanges inter-applicatifs entre Internet maîtrisé (Heliss-NG puis C1NP) et Internet non maîtrisé (internet public)	E / -	Internet maîtrisé / Internet non maîtrisé
<i>Commentaire : actuellement en préproduction, la PEM Internet doit passer en production expérimentale fin 2024 puis en production opérationnelle fin S1 2025</i>					
Exposition et médiation d'API [PEM]	PEM pour environnement de développement et de validation	MinArm WSO2		R / S	PICSEL
	WSO2 API Manager version	WSO2	Si nécessité d'instances dédiées	A / N	MinArm
<i>Commentaire : lorsque le recours à une PEM dédiée est nécessaire en lieu et place des instances mutualisées ministérielles évoquées ci-dessus, et sous réserve de le justifier en dérogation, l'usage de WSO2 est recommandé, mais son support est à la charge de la direction d'application.</i>					

3.2.4.5 Extraction et transformation (ETL) [TRF]

Un outil d'ETL³⁴ permet l'extraction, la transformation et le chargement des données depuis des sources, et des cibles diverses par l'intermédiaire de connecteurs : base de données, fichiers, ERP, etc. Les principaux domaines d'emploi sont l'alimentation ou l'échange entre systèmes opérationnels et l'extraction des données de systèmes opérationnels à l'usage des systèmes dédiés au décisionnel.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
ETL	Talend Open Studio for data integration	Talend (open source)	Il est recommandé d'utiliser Talend Open Studio dans les cas suivants : - synchronisation et transfert en masse de données entre SI ; - traitement de données embarqué dans le SI. - reprise de données	R / S	MinArm, Intradef
ETL	Talend Plateform pour Data integration	Talend	Il est recommandé d'utiliser cette solution si une équipe de 3 développeurs ou plus est dédiée à la création de tâches.	R / S	MinArm, Intradef
ETL	Talend Plateform Data Management	Talend	Il est recommandé d'utiliser cette solution pour les projets devant implémenter la gestion de qualité des données et si une équipe de 3 développeurs ou plus est dédiée à la création de tâches. <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	R / S	MinArm Intradef
<i>Commentaire : la mise en production des tâches doit se faire par livraison de jar, invoqués par un ordonnanceur type cron et il appartient au projet de se doter dans tous les cas d'une solution de supervision fonctionnelle des échanges.</i>					
ETL	Data Integrator	Oracle	<i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	* / *	MinArm
ETL	SSIS	Microsoft	Assujetti à l'alimentation d'un infocentre en technologie Microsoft. <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	* / *	MinArm
ETL	Logstash	Elastic (Open source)	Assujetti à l'alimentation de nœuds Elastic Search	R / S	MinArm
DELDT ³⁵	Spark	Apache	Outil d'ingestion, de traitement et d'accès	A / N	MinArm
<i>Commentaire : cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.</i>					

3.2.4.6 Gestion de processus et de règles métiers

La gestion des processus (« Business Process Management » ou BPM) consiste à modéliser les processus métiers. L'objectif de cette démarche est d'aboutir à une meilleure vue globale de l'ensemble des processus métiers et de leurs interactions afin d'être en mesure de les optimiser et, si possible, de les automatiser au maximum à l'aide d'applications métier.

³⁴ Extract, Transform, Load : extraction, transformation, chargement.

³⁵ Discover, Extract, Load, Discover, Transform

Dans un deuxième temps, permettre de modifier simplement ces processus en fonction des besoins passe par l'établissement de règles métiers.

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
BPMN V2	Le Business Process Model and Notation (BPMN) est un modèle de processus métier et une notation graphique standardisée par l'Object Management Group (OMG).	R	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
BPMN	Bonita	BonitaSoft	Déconseillé à cause de son usage Low-Code et rythme de mise à jour élevé, AngularJS spécifique maintenu dans la solution.	D / N	MinArm
BPMN	Camunda	Camunda	Assujetti	A / N	MinArm
BPMN	Flowable	Flowable	Assujeti	A / E	Intradef
<i>Commentaires : Pour la majorité des cas développés en Java, le recours à un framework de l'écosystème Spring (WebFlow, StateMachine) peut amplement suffire. Pour les cas plus complexes, l'embarquement d'un framework Camunda peut s'avérer une alternative opportune. Concernant des développements en PHP, il est préconisé le recours à Symfony-Workflow ou Laravel-Workflow.</i>					

Les outils de modélisation BPM, de processus, de workflow et d'architecture sont évoqués au chapitre 7.2.1 Modélisation métier.

3.2.4.7 Annuaire des applications et services [ANA]

Pas de référence identifiée à ce jour.

3.2.5 Données et contenu

3.2.5.1 Formats de données

Document	Date	Origine	Type doc	Portée
Référentiel Général d'Interopérabilité [RGI]				
<i>Commentaire : (cf.2.2.3 Les référentiels interministériels). Le RGI, dans sa partie syntaxique effectue les recommandations en matière de formats élémentaires et de formats composites. Il s'applique au ministère.</i>				

L'attention des directions d'applications est attirée sur l'encodage des caractères et des formats audio et vidéo.

3.2.5.1.1 Encodage des caractères

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
UTF-8	Norme de codage des caractères sur plusieurs octets. Il est recommandé d'utiliser UTF-8 pour l'encodage des caractères, notamment pour éviter un affichage « exotique » des caractères accentués. L'utilisation de tout autre encodage doit être justifiée par un besoin technique.	R	MinArm
<i>Commentaire : UTF-8 peut être mis en œuvre sur Windows 10 à partir de la version 1903, là où ce n'est pas possible utiliser par défaut CP65001.</i>			
UTF-16, UTF-32	l'usage de UTF-16 ou UTF-32 est réservé à l'encodage des caractères pour les besoins d'échange démonstrativement plus efficaces en UTF-16 ou	A	

	UTF-32, ou si l'usage d'UTF-8 est interdit par une disposition normative.		
ASCII	Codage historique de caractères sur 7 bits.	D	
ISO-8859-x	Normes de codage de caractères sur 8 bits. Ces normes très répandues sont entrées en obsolescence. L'usage pour les nouveaux systèmes est très fortement déconseillé et nécessite l'obtention d'une dérogation.	D	
Autres encodages	Notamment les jeux de caractères Windows-1252 ou CP1252, CP437, CP850	I	

Voir aussi les règles de nommage des fichiers enfermant des contenus numériques (chapitre 8.4.1).

3.2.5.1.2 Formats audio et vidéo

Les données vidéo et audio sont susceptibles d'avoir un impact significatif sur les réseaux du ministère. Par ailleurs, certains formats ne sont pas ou plus pris en charge nativement par les navigateurs. Il convient donc d'utiliser des formats tenant compte de ces contraintes.

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
WebM	Conteneur vidéo	R	MinArm
MKV	Conteneur vidéo	R	MinArm
VP8	Codec vidéo pour le conteneur WebM	R	MinArm
VP9	Codec vidéo pour le conteneur WebM	R	MinArm
H264	Codec vidéo pour le conteneur MKV	R	MinArm
H265	Codec vidéo pour le conteneur MKV	R	MinArm
<i>Commentaire : La résolution doit être limitée à 720P au maximum, le fullHD ne s'impose pas sur les réseaux MinArm dont les capacités doivent être préservées.</i>			
Vorbis	Codec audio	R	MinArm
Opus	Codec audio	R	MinArm

3.2.5.1.3 Outils de conversion de format

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Conversion de format	PANDOC	opensource	Outil de conversion de documents multi-format utilisable par les applications en tant que de besoin préférentiellement à l'installation niveau serveur de LibreOffice ou MS-Office.	R / -	MinArm

3.2.5.2 Gestion des accès aux données

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
CSV ³⁶	Format de transfert de données en volume, dit « à plat » ou texte. Recommandé uniquement pour les échanges entre application et utilisateur (cf. RGI v2). Pour tous les autres cas, utiliser XML.	A	MinArm
XML ³⁷	Format et échange de documents structurés, standard du W3C. C'est un méta langage permettant de définir des langages (format de données)	R	MinArm

³⁶ Comma separated values. Valeurs séparées par des virgules (ou des points-virgules lorsque les données contiennent elles-même des virgules).

³⁷ Extensible markup language. Langage de balisage extensible.

	notamment en vue de faciliter l'échange automatisé de contenus complexes entre système informatiques hétérogènes. Il peut cependant être un peu « verbeux » pour des volumétries importantes.		
XSD	Format de description d'un document XML, standard du W3C. Il est recommandé d'utiliser la syntaxe XSD (XML schema definition) pour décrire le contenu et la structure d'un document XML et en vérifier la validité.	R	MinArm
XSLT et XPath	Il est recommandé d'utiliser les langages XSLT pour formater et transformer des documents XML et XPath pour localiser une portion d'un document XML et ainsi requêter sur un document.	R	MinArm
JSON	Usage recommandé pour les protocoles optimisés méga-données (Big Data) et pour les échanges de données en architecture Web.	R	MinArm

3.2.5.3 Gestionnaire des données [HBD]

Il existe principalement deux grandes familles de moteurs de base de données ayant chacune des limites :

- Les bases de données relationnelles où les données, en général fortement typées et très structurées sont reliées entre elles par une algèbre relationnelle, permettant d'en vérifier rapidement l'intégrité : on leur délègue communément la responsabilité de vérifier le respect des règles métiers exprimables sous forme de contraintes et de relations (cas des ERP, ou du reporting pour le décisionnel en mode OLAP). C'est aussi une couche d'abstraction prenant en charge les contraintes du stockage physique de la donnée et de la concurrence des accès. Cependant elles sont limitées en performances (capacité, temps de réponse) par le respect du modèle d'E. F. Codd et l'implémentation de transactions aux propriétés ACID (Atomicité, Cohérence, Isolation, Durabilité).
- Les moteurs NoSQL qui s'affranchissent d'une partie de ces contraintes. Il y a deux grands cas d'utilisation du NoSQL. Le premier, permet de développer rapidement des applications simples utilisant des données faiblement structurées par essence (et non par manque de conception). Le second, permet de satisfaire des exigences essentiellement techniques, tout particulièrement sur les aspects volumétrie, passage à l'échelle (temps de réponse constant malgré la charge et la volumétrie) et résilience (disponibilité malgré les pannes). Ces moteurs ne sont pas adaptés lorsque des relations existent dans le modèle de données et doivent être exploitées (problèmes de performance voire d'intégrité notamment).

3.2.5.3.1 Les SGBDR

★★★★★

Les choix de SGBDR non recommandés doivent systématiquement faire l'objet d'une demande de dérogation dûment justifiée auprès de la gouvernance technique (§ 1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT)

★★★★★

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°5 relative aux systèmes de gestion de bases de données relationnelles publiée au Bulletin Officiel des Armées	7 avril 2008	DGSIC	Directive	MinArm
Note DGSIC relative au choix du SGBDR dans les systèmes d'information diffusée sous timbre n°468/ARM/DGSIC/DG/NP du 24 novembre 2017	24 novembre 2017	DGSIC	Note	MinArm

Document	Date	Origine	Type doc	Portée
<i>Commentaire : Cette note soumet tout choix de SGBDR non recommandé dans le CCT à une demande systématique de dérogation auprès de la gouvernance technique (cf. 1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT)</i>				
Configuration sécurisée de PostgreSQL <i>(cf. 4.5 Sécurisation des COTS)</i>	5 avril 2011	DGA MI	Guide technique	MinArm

NOTA : Résumé de la politique en matière de SGBDR

- Pour tout nouveau projet ou évolution majeure, le choix des solutions PostgreSQL et MariaDB est systématiquement à étudier (MySQL doit être réservée aux cas où MariaDB ne disposerait pas de la fonctionnalité équivalente nécessaire.)
- A défaut, SQL Server à dûment justifier si aucune solution opensource recommandée ne peut convenir
- A défaut, SGBD Oracle, si aucune solution opensource recommandée et si SQL server impossible, à strictement justifier : dans ce cas, sur Intradef, étudier l'offre d'hébergement refacturée Exadata particulièrement sollicitée aujourd'hui, ou, à défaut disposer d'une licence spécifique pour environnement virtualisé, ou, à défaut, mettre en place un hébergement sur machine physique dédiée.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
SGBD	PostgreSQL	The PostgreSQL Global Development Group	Solution à privilégier pour les nouveaux développements et les migrations. Elle permet des architectures offrant haute disponibilité et scalabilité. <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits</i>	* / *	MinArm
<i>Commentaire : Le recours à un framework ou outil d'exposition REST tel POSTGREST est déconseillé, et nécessite une dérogation dûment justifiée en SC2A. L'exposition d'API de type CRUD n'est pas conforme à la stratégie API du ministère au sens où elle induit un couplage fort entre le schéma de la base de données et l'API générée.</i>					
SGBD	MariaDB	MariaDB Foundation	Ce SGBD, « fork » de MySQL depuis 2012, est la solution référencée par le socle interministériel de logiciels libres (SILL). Solution à privilégier par rapport à MySQL à fonctionnalités équivalentes. <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits</i>	* / *	MinArm
SGBD	Galera Cluster	Galeracluster	Solution de clusterisation multi-maitre synchrone pour MariaDB	R / S	MinArm
<i>Commentaire : Depuis la version 10.1, MariaDB inclut Galera Cluster</i>					
SGBD	MySQL	Oracle	<i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits</i>	* / *	MinArm
<i>Commentaire : La version 5.7 de MySQL sera la dernière soutenue par le Ministère (fin de support officiel annoncée à T4 2023), les alternatives recommandées demeurent, dans cet ordre, PostgreSQL et MariaDB.</i>					
SGBD	SQL Server	Microsoft	Assujetti : Utilisation à justifier dans le cas où aucune solution opensource recommandée au CCT ne peut convenir. <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits</i>	* / *	MinArm
<i>Commentaire : MS SQL Server est en assujetti, toutes versions et licences confondues (Express, standard ou enterprise)</i>					

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
SGBD	Oracle Database Standard Edition One	Oracle	Assujetti : Utilisation à dûment justifier, si impossibilité de recourir ni un SGBDR recommandé ni, à défaut, à SQL Server * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	A / S	MinArm
SGBD	SQLite	SQLite	Librairie en langage C qui implémente un moteur de BD relationnelle. Elle est petite, rapide et performante. C'est une solution pertinente en mode « embedded » c'est-à-dire embarquée dans une application sans avoir besoin de l'installation et du management d'un SGBDR. Cette librairie est utilisable sur un nombre très importants d'OS et de langages de programmation. Son usage principal est sur terminaux mobiles (smartphone et tablette). A ne pas utiliser toutefois dans le cadre d'un service cloud, notamment conteneurisé.	A / N	MinArm
SGBD	PostGIS	PostGIS	Surcouche PostgreSQL permettant d'en faire un SGBD spatial ou de cartographie	A / N	MinArm

3.2.5.3.2 Les SGBD sous la dénomination NoSQL

Les cas d'utilisation sont volontairement incomplets. Les caractéristiques trop techniques sont exclues. Ne sont présentés que les critères les plus sélectifs qui peuvent être déterminés durant une analyse de besoins.

Les bases de données NOSQL mentionnées ci-dessous sont quasi-toutes sous statut Assujetti : il est demandé aux directions d'application de se rapprocher de la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT) aux fins de capitalisation sur les usages de ces solutions.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Base de données NOSQL	Elasticsearch	Elastic	Moteur de recherche et d'analyse sans état éventuellement distribué basé sur Apache Lucene. Pour des recherches rapides avec évaluation de pertinence y compris full text. Traditionnellement utilisé avec Logstash pour l'ingestion des données et Kibana pour la visualisation. * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	MinArm

Commentaire : () : A priori le récent changement de mode de licence (passage Apache 2.0 -> licence SSPL) n'impacte pas les usages qu'en fait le ministère. Il existe aussi une version entreprise payante.*

Compte tenu du cycle de vie, il n'y a pas véritablement de version LTS mais plutôt deux versions maintenues en parallèle, une stable et une dite « current » ayant un cycle rapide de mises à jours techniques et fonctionnelles. La version recommandée est la version LTS.

Base de données NOSQL	OpenSearch	AWS	Alternative à Elasticsearch/Kibana apportant les fonctionnalités de sécurité (authentification) et alerting	A / N	MinArm
-----------------------	------------	-----	---	-------	--------

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Base données NOSQL	Cassandra	Apache ou distribution commerciale DataStax	Base de données orientée colonnes avec un ressenti proche d'un SGBDR. Grands volumes de données et des besoins de bases distribuées hautement disponibles et décentralisées, sous réserve de prendre en compte les impacts réseau <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	A / S	MinArm
Base données NOSQL	MongoDB	MongoDB	Indexes et requêtes simples sur un modèle changeant et des données peu structurées (textes plus ou moins longs, données saisies avec peu de contraintes) ; applications de type blog À envisager après étude des fonctionnalités JSON de PostgreSQL <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	A / S	MinArm
Base données NOSQL	Memcached	Danga Interactive	Hautes performances d'écriture et de restitution (accès inférieur à la ms) dans une base clef/chaîne de caractère en mémoire.	R / S	MinArm
Base données NOSQL	Redis	Redis Labs	Hautes performances d'écriture et de restitution (accès inférieur à la ms) dans une base clef/valeur en mémoire plus riche fonctionnellement et éventuellement persistée. <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	A / S	MinArm
Base données NOSQL	Neo4j	Neo4j	Pure base de données graphe. Traitement rapide d'ensembles de nombreuses données fortement en relation les unes avec les autres en grand nombre (ou dont le nombre de relations est variable). Neo4J doit être utilisé en version entreprise, la version communautaire n'ayant pas de gestion de droits. Si cette gestion de droit est nécessaire, utiliser ArangoDB.	A / N	MinArm
Base données NOSQL	ArangoDB	ArangoDB	BD multi-modèles (graphes, documents, clés-valeurs) open-source sous licence Apache. Son langage de requêtes AQL déclaratif permet des combinaisons de différents patterns d'accès dans une même requête.	Base de données NOSQL	ArangoDB
Base données NOSQL	InfluxDB	InfluxData	Orienté pour un besoin de traitement hautes performances de séries chronologiques qu'une autre base de données présente au CCT ne pourrait satisfaire (Postgres ou Elastic par exemple). Et son écosystème immédiat : -Telegraf (proxy BDD InfluxDB), -Kapacitor (analyse streaming des données entrant dans InfluxDB)	E / N	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Base de données NOSQL	SOLR	Fondation Apache	Pour implémenter des moteurs de recherche évolués.	A / S	MinArm
Base de données NOSQL	PouchDB	Fondation Apache (Apache License 2.0)	PouchDB est principalement utilisé pour le stockage de données côté client, ce qui signifie qu'il peut être utilisé pour stocker des données localement dans un navigateur web ou dans un environnement Node.js. PouchDB est conçu pour la réPLICATION bidirectionnelle de données entre la base de données locale et une base de données distante. Cela permet de maintenir les données synchronisées entre différentes instances de l'application, même en cas de déconnexion.	A / *	MinArm
Base de données NOSQL	CouchDB	Fondation Apache (Apache License 2.0)	CouchDB offre une réPLICATION multi-master, ce qui signifie que plusieurs bases de données CouchDB peuvent se synchroniser entre elles de manière bidirectionnelle. Cela permet une grande tolérance aux pannes et la distribution des données sur plusieurs serveurs.	A / N	MinArm

3.2.5.3.3 Les SGBD en mémoire

Les bases de données en mémoire (in-memory) visent à accélérer l'accès aux données en les stockant directement en RAM (mémoire temporaire rapide) plutôt que sur les disques durs (mémoire persistante lente).

3.2.5.3.4 Les agents de messages

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Agent de messages	RabbitMQ	Pivotal Software	Logiciel libre sous licence Mozilla Public License permettant l'échange de message. À utiliser pour découpler des systèmes d'information notamment ; <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	* / *	MinArm
Agent de messages	ActiveMQ	Apache Software Foundation	Logiciel libre sous licence Apache 2.0 de serveur de message multi protocoles (AMQP, MQTT, STOMP) ; <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	R / S	MinArm
Agent de messages	Redis	Redis Labs	Base clef/valeur en mémoire qui peut aussi être utilisée comme agent de message. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	A / S	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Agent de messages	Kafka	Apache Software Foundation	Logiciel libre sous licence Apache 2.0 pour la mise en place de pipeline de messages, la supervision temps réel, l'IoT quand RabbitMQ n'est pas suffisant, qu'il y a un besoin de persistance ou qu'un cluster est nécessaire ; <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	R / S	MinArm

3.2.5.4 Gestion des données de référence (MDM) – management de la qualité des données (DQM)

Gestion des données de référence (MDM : master data management)

La gestion des données de référence ou gestion des données maîtres (GDR, plus connue sous le vocable anglais de master data management ou MDM) est une branche des technologies de l'information qui définit un ensemble de concepts et de processus visant à définir, stocker, maintenir, distribuer et imposer une vue complète, fiable et à jour des données de référence au sein d'un système d'information.

Management de la qualité des données (DQM : data quality management)

La mise en qualité des données est un prérequis indispensable à l'optimisation et à l'efficience des métiers. La maîtrise de la qualité des données est donc un enjeu important au sein des organisations. Il s'agit de fournir des données correctes, complètes, à jour et cohérentes aux acteurs métiers. Une réponse technologique à cette problématique est apportée par la brique de management de la qualité des données.

La mise en œuvre de ces deux concepts au sein du ministère se concrétise au travers des travaux menés par la DGNUM sur la gouvernance de la qualité des données et la mise en place d'une plateforme technique implémentant les briques MDM et DQM et Service Adresse.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°35 portant sur la gouvernance de la qualité des données du ministère de la Défense, diffusée sous timbre n° 314/DEF/DGSIC/SDS/NP du 11 juin 2015	11/06/2015	DGSIC	Directive	MinArm
<i>Commentaire : Cette directive définit les règles relatives à la gouvernance de la qualité des données des systèmes d'information et de communication (SIC) du ministère des armées. Elle abroge l'ancienne directive DGSIC n°14 portant sur l'administration des données du ministère des armées. Elle est complétée par un guide (ci-dessous).</i>				
Guide DGSIC n°10 portant sur la gouvernance de la qualité des données du ministère de la Défense	11/06/2015	DGSIC	Guide	MinArm
<i>Commentaire : Le présent guide a pour objectif de présenter les principes fondateurs de la gouvernance de la qualité des données, en définissant le périmètre puis en établissant pour chaque démarche relevant de cette gouvernance les objectifs, les concepts, les principes de mise en œuvre et les moyens associés.</i>				

La solution retenue au niveau ministériel est celle mise en œuvre par le projet « Plateforme de gestion des données de référence » (PGDR). Pour mémoire, la gestion des métadonnées est couverte par METADATARM (cf 2.3.6.2.2)

Concernant le MDM, l'offre de service de PGDR concerne les données de référence NP/DR du ministère ; elle est constituée de :

- La réalisation de référentiels de données par le CASID (selon le plan de charge) ou l'industriel (sur financement) ;
- La délégation de capacités de réalisation de référentiels de données à un organisme du ministère (sur ressources humaines et financières de son ressort).

En conformité avec la politique API, les données de référence sont exposées sous forme d'API sur la PEM via POCEAD. Néanmoins des flux complets sont envisageables pour répondre au besoin des SI consommant historiquement les données de référence sous cette forme.

Concernant le DQM, l'offre de service de PGDR se décline en services de qualité des données (diagnostics de la qualité des données, et propositions de correction lorsqu'elles sont automatisables) pour l'ensemble des données des SI NP/DR du ministère (et pas seulement les données de référence), prenant la forme de :

- La réalisation de services qualité des données par le CASID (selon le plan de charge) ou l'industriel (sur financement) ;
- La délégation de capacités de réalisation de services qualité des données à un organisme du ministère (sur ressources humaines et/ou financières de son ressort).

Le DQM est complété d'un service « clef en main » dédié au contrôle et au redressement des adresses postales et/ou géographiques au périmètre France métropolitaine et DROM COM, certifié SNA (Service Nationale de l'Adresse). Ce service est utilisable selon deux modes :

- un mode batch permettant d'effectuer des mesures de qualité, des traitements de normalisation ainsi que des redressements d'adresses sur des lots de fichiers volumineux (traitement de masse) ;
- un mode API permettant d'intégrer directement aux sein d'applications métiers une interface de saisie et de contrôle et de redressement en temps réel des adresses.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Composant MDM	PGDR	MinArm	Basé sur le logiciel IBM Product Master V12 À vocation ministérielle, l'offre de service concerne tout référentiel de données NP/DR quel que soit le domaine métier.	R / E	Intradef
Composant DQM	PGDR	MinArm	Basé sur le logiciel IBM InfoSphere Information Server 12 (Information Analyzer et Quality Stage) À vocation ministérielle, l'offre de service concerne tout SI dont les données sont NP/DR et ceci quel que soit le domaine métier.	R / E	Intradef

Commentaires : pour l'usage de cette plateforme, s'adresser au bureau Données de la DGNUM.

Composant Service Adresse	PGDR	MinArm	Basé sur les solutions Capency Batch : CAP RNVP API : CAP ADRESS <ul style="list-style-type: none"> - CAP SAISIE (saisie des adresses en « entonnoir ») - CAP LINE (saisie des adresses sur un seul champ) CAP VERIF (intégralité d'une adresse quel que soit son mode de saisie) À vocation ministérielle, l'offre de service concerne tout SI dont les données sont NP/DR et ceci quel que soit le domaine métier.	R	Intradef
---------------------------	------	--------	--	---	----------

3.2.5.5 Gestion électronique de documents [GED]

La gestion électronique des documents (GED, ou EDM pour Electronic Document Management) désigne un procédé informatisé visant à organiser et gérer des informations essentiellement non structurées comme des documents électroniques au sein d'une organisation.

Elle met principalement en œuvre des systèmes d'acquisition (numérisation de masse de documents papiers, par exemple), d'indexation, de classement, de gestion et de stockage, d'accès (navigation et recherche) et de consultation des documents.

L'aspect publication des documents est traité dans le chapitre 3.1.3.1 Portail intranet [SU_PIN], et partie back-office 3.3.2.2 Portail d'information [PIN].

Le travail collaboratif présidant à leur élaboration est traité en 3.1.2.2 Espace de travail collaboratif [SU-EDT] et, partie back-office 3.3.2.8 Gestion des communautés d'intérêt [COI] et 3.3.3 Travail de groupe.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
GED	Sharepoint	Microsoft	<i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	A / S	Tout intranet
GED	Alfresco community edition	Alfresco Software		R / S	Intradef
GED	Alfresco community edition	Alfresco Software	S-SF (non inclus dans l'offre STC-IA 0.5, mais peut être embarqué dans une application dédiée)	A / S	S-SF SIA FrOps

3.2.5.6 Masquage / Anonymisation / Pseudonymisation des données

Le masquage des données est une technologie visant à prévenir la manipulation de données à caractère personnel ou dites « sensibles » pour le ministère (exemple : site) en fournissant aux utilisateurs des données fictives mais réalistes au lieu des données réelles. Il s'appuie sur les principes d'anonymisation et de pseudonymisation des données en fonction de l'objectif recherché.

L'anonymisation des données est le processus par lequel les données sont rendues anonymes, et à l'issue duquel elles ne peuvent plus être rattachées à un individu en particulier. Le procédé doit ainsi être irréversible dans le but de rendre impossible la ré-identification.

La pseudonymisation (ou pseudo-anonymisation), en revanche, est un processus technique consistant à remplacer la valeur d'une donnée par une autre valeur. Ce procédé est nécessairement réversible, les deux processus techniques étant utilisés pour des cas d'usage différents.

3.2.6 Informatique « décisionnelle », Big Data, analyse prédictive

3.2.6.1 Introduction et orientations ministérielles

Jusqu'ici l'informatique décisionnelle couvrait traditionnellement l'ensemble de la chaîne décisionnelle depuis l'extraction des données, leur hébergement dans un entrepôt de données, leur transformation, la gestion de leur qualité et la restitution d'analyses statiques.

Le ministère a ainsi été amené à mettre en place la ferme de stockage Fasttrack servant d'infocentres et la plateforme décisionnelle SAP Business Object BI. Ces plateformes traditionnelles sont opérationnelles depuis plusieurs années et destinées à être remplacées. Actuellement dimensionnées au juste besoin pour les systèmes existants, la ferme Fasttrack ne prendra plus en compte de nouveaux besoins. Les nouveaux outils

de « datavisualisation » permettent de naviguer dans des tableaux de bord de façon dynamique. Le ministère a fait le choix de la technologique QlikSense pour mettre en place une plateforme ministérielle de « datavisualisation » qui à terme remplacera l'ensemble des univers et requêtes SAP BI. Les autres outils de datavisualisation ou de tableaux de bord sont soumis à dérogation.

Les nouveaux outils dits de « big data » permettent de traiter un volume de données beaucoup plus important, d'exploiter leur potentiel par des techniques de « science de la donnée », comme l'analyse prédictive et des algorithmes d'intelligence artificielle.

Au niveau du ministère, le traitement des cas d'usage en mode innovation ou expérimental (« proof of Concept ») peut être assuré par le Labo BI de la DTPM au travers de sa plateforme Data360 ou par le SAND au travers de POCEAD.

POCEAD est aujourd'hui positionné comme le seul outil ministériel de traitement BigData pour des données NP-DR en environnement de production.

Progressivement, un catalogue de solutions s'enrichira d'autres options adaptées en fonction des catégories de besoins. Ainsi, devraient émerger à moyen terme (2024) des offres autour de briques et services mis à disposition par le projet ARTEMIS.IA sur le réseau S-SF SIA.

La feuille de route ministérielle des données, document qui sera officialisé en 2024, puis remis à jour tous les ans, portera les stratégies de cohérence en cohérence avec la politique ministérielle des données (Note n°117/ARM/DGNUM/DG/NP du 5 avril 2022).

Document	Date	Origine	Type doc	Portée
Politique ministérielle des données Note n°117/ARM/DGNUM/DG/NP du 5 avril 2022	05/04/2022	DGNUM	Note	MinArm

3.2.7 Datavisualisation, BI Corporate ou BI self-service

L'utilisation des données venant de SI opérationnels se fait avec des outils de restitution allant du simple rapport au tableau de bord composé d'indicateurs complexes.

L'informatique décisionnelle agile permet de créer des tableaux de bord dynamiques. Ces outils permettent de **couvrir le cycle de création d'un tableau de bord de la collecte des données, de leur préparation, de leur nettoyage et de leur visualisation**. Ils se caractérisent en général par une simplicité d'usage, et une interface graphique plus conviviale que celle que l'on retrouve dans l'informatique décisionnelle traditionnelle. Elle permet de s'affranchir d'une phase de restructuration des données.

Pour tout nouveau projet ou toute évolution majeure de projet décisionnel, et conformément à la décision n°4 du CECNUM du 9 juillet 2019, la plateforme ministérielle basée sur l'outil Qlik Sense doit être utilisée.

Dans les autres cas, envisager les outils d'analyse et de visualisation des données mentionnés au §3.2.6.3 Datavisualisation (ou BI self-service).

→ **Une stratégie de migration de l'ensemble des solutions de BI (SAP-BO, Power BI, Cohéris Liberty, etc.) est actuellement à l'étude.**

SAP a annoncé la fin de SAP Business Object en 2027 au profit de sa solution cloud SAP Analytics Cloud. Le support (*mainstream maintenance*) de la version 4.3 s'achèvera fin 2025 (2027 en souscrivant un *priority support*). La version SAP Business Object 2024 recentrée sur les outils les plus utilisés (Web Intelligence, .unx universes et platform BI) prolongera le support jusque fin 2027 et est destinée à faciliter la migration vers la solution Cloud. Cette dernière sera également déclinée en version "on premise" sous le nom SAP BO Enterprise, private cloud edition (PCE) opérée par SAP

ce qui la rend impropre à un usage sur les réseaux du Ministère.

En conséquence, la migration des rapports existants vers la solution ministérielle Qlik Sense doit être planifiée en fonction de cette échéance de fin 2025.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Décisionnel traditionnel	Plateforme basée sur l'Appliance décisionnelle (matériels et logiciels) Fast track	DIRISI Bull	Plateforme mutualisée Intradef. <i>Implique le recours à SQL Server (Assujetti)</i>	D / S	Intradef
Décisionnel traditionnel	Business Objects BI	SAP	Outil de restitution et d'analyse des données (WEBI). <i>Implique le recours à SQL Server (Assujetti)</i>	D / S	Intradef
<i>Commentaire : interdit en dessous de la version 4. 3. Déconseillé pour les nouveaux projets ayant recours par ailleurs à une technologie SAP et interdit pour tout autre nouveau projet.</i>					
Décisionnel traditionnel	SQL Server BI SSRS and SSAS.	Microsoft	Outil de restitution et d'analyse des données (WEBI).	D / N	Intradef
Décisionnel agile Analyse et de visualisation de données	Plateforme ministérielle QlikSense (Serveur) Enterprise	Qlik		R / S	Intradef
	KIBANA	Elastic	Assujetti à l'écosystème ElasticSearch et Logstash et à la justification que les outils recommandés de datavisualisation ne satisfont pas.	R / S	MinArm
	GRAFANA	Grafana labs	Pour des besoins non couverts par Kibana, cf ci-dessus	A / N	Intradef
	TABLEAU	Tableau Software	Doit migrer vers la plateforme QlikSense	D / N	Intradef
	POWERBI Server	Microsoft	Doit migrer vers la plateforme QlikSense	D / N	Intradef
<i>Commentaires :</i>					
<i>- La plateforme ministérielle QlikSense est installée par la DIRISI.</i>					
Décisionnel traditionnel	SAP Crystal Report	SAP	Permet de créer des rapports de masse avec des graphiques et des tableaux de données. Permet la disposition des objets aux pixels près. N'est pas interactif et visualisable via la plateforme SAP ou via un export pdf.	D / S	Intradef
Décisionnel traditionnel	SAP BO LUMIRA	SAP	Permet de développer des tableaux de bord interactifs	D / S	Intradef
<i>Commentaire : Ces logiciels sont installés sur la plateforme ministérielle décisionnelle, leur partie cliente est packagée par le CNCI.</i>					
Décisionnel traditionnel	Pentaho (version communautaire)	Hitachi Vantara	Solution Open Source en Java. Suite logicielle complète (de la création à la diffusion via une interface web. Assujetti à des emplois simples	D / -	Intradef
Décisionnel traditionnel	Jaspersoft BI (version communautaire)	Tibco	Plateforme BI Open Source Assujetti à des emplois simples.	D / -	Intradef

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Préparation et analyse des données	Dataiku	Dataiku	Le cadre d'emploi de la solution n'est pas défini et les risques cyber ne sont pas encore entièrement identifiés. L'utilisation de l'outil doit être soumise à l'autorisation du COMCYBER	E / -	MinArm

La plateforme Business Object BI opérée par la DIRISI reste maintenue pour permettre aux projets existants ou intégrés à un écosystème SAP de continuer à pouvoir faire fonctionner les outils d'informatique décisionnelle déjà mis en place en attendant une migration vers la plateforme Qlik Sense.

Pour la collecte et transformation des données (ETL), se référer au § 3.2.4.5.

3.2.7.1 Données massives ou « Big Data »

Le terme de « Big Data » (parfois appelées « données massives » en français) est au croisement de plusieurs domaines : statistiques, technologies, bases de données et métiers (finances, RH, renseignement, etc.). Le « Big Data » vise à exploiter des données souvent complexes de structures et de sources très diverses, à croissance exponentielle. Ce type de données est difficile à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information.

Les technologies « Big Data » s'appuient essentiellement sur des solutions open source :

- un système de fichiers distribué permettant de stocker des données plus ou moins structurées sur un ensemble de serveurs distribués y compris géographiquement (Hadoop Distributed File System par exemple) ;
- un framework de requêtage sur ces agrégats de données distribuées (les calculs sont effectués au plus près des données puis consolidés en central : MapReduce et son évolution YARN notamment) ;
- des traitements en temps réels réalisés par des moteurs d'indexation temps réel distribués (ElasticSearch, pile ELK, par exemple).

Les approches, architectures et outils diffèrent selon qu'il s'agit de traiter ces données en temps réel ou pas, Dans tous les cas, il est recommandé une approche en deux temps : l'expérimentation (« proof of concept ») validée par un expert de type « Data Scientist » et l'industrialisation.

3.2.7.1.1 Plateformes exploratoires et d'innovation DATA360 – POCEAD – ARTEMIS-IA

Il y a trois plateformes disposant d'une capacité d'exploration de données et de POC (proof of Concept).

La plateforme DATA360 est une plateforme d'expérimentation du Labo BI de la DTPM. Dédiée uniquement à l'innovation, elle est composée des fonctionnalités suivantes :

- collecte des données ;
- stockage indexé des données massives ;
- analyse des données (fouille via un moteur de recherche très puissant) ;
- datavisualisation via la plateforme ministérielle QlikSense ;
- sécurisation (gestion des droits d'accès jusqu'à la donnée) ;
- datascience (mise en œuvre d'algorithme).

La plateforme POCEAD dispose d'une capacité d'exploration et d'incubation d'un besoin (Data Lab) et développement d'un POC (proof of concept). Cette plateforme qui permet également de réaliser des cas

d'usage en environnement de production est décrite dans le paragraphe suivant.

La plateforme ARTEMIS.IA dispose :

- D'un bac à sable permettant :
 - Le développement en vue de la mise à disposition de nouveaux modules et applications,
 - L'accès aux données opérationnelles sans nuire à leurs disponibilités pour les applications en cours d'utilisation,
 - La mise à disposition des outils pour explorer les données disponibles, et pour entraîner, tester et qualifier des algorithmes basés sur de l'IA.
- D'un kit de développement logiciel permettant (disponible sur PICSEL ou de manière autonome) :
 - De doter un tiers d'une suite logicielle autonome, indépendante d'une instance ARTEMIS.IA,
 - De réaliser la conception, l'implémentation et les tests unitaires de modules dans les langages Python, R, Java.

Pour des cas d'usage au stade exploratoire ou d'innovation et la réalisation de POC concernant le « Big Data et/ou l'analyse prédictive », la gouvernance orientera au Pitch 0 vers l'une des plateformes ayant cette capacité DATA360, POCEAD ou KDL ARTEMIS.IA sur PICSEL. Pour tout autre cas, se référer au §3.2.6.4.2Plateforme POCEAD – ouverture des données.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Big Data – IA phase exploratoire et POC	POCEAD basée sur la plateforme SAAGIE	MinArm	En phase exploratoire et d'innovation pour la réalisation de POC et de cas d'usage en production pour des données qui peuvent être réutilisées (open data) avec contractualisation selon les catégories de données utilisées. (*) : soutenu par le CASID/SAND	R / S	Intradef
Big Data – IA phase exploratoire et POC	DATA360 Basé sur Elastic Cloud Enterprise	Elastic	En phase exploratoire et d'innovation et pour la réalisation de POC. Pour avoir une vision 360 des données pour l'aide à la décision. Les données peuvent être croisées entre elles et avec d'autres données provenant de POCEAD ou provenant de data.gouv.fr via des API (*) : soutenu par SGA/MAP	R / S	Intradef
Big Data – IA phase exploratoire et POC	Bac à sable ARTEMIS IA (cf. 3.2.6.4.3 Plateforme ARTEMIS.IA)	Minarm	Disponible sur environnement de production pour aider au développement, explorer les données, pour entraîner tester et qualifier des algorithmes basés sur de l'IA.	R / S	Minarm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Big Data – IA phase exploratoire et POC	Kit de Développement ARTEMIS.IA	MinArm	Kit de développement logiciel ARTEMIS.IA permettant de développer et de packager des applicatons métier pour intégration sur le socle ARTEMIS.IA Disponible sur PICSEL ou de manière autonome	R / S	Minarm

3.2.7.1.2 Plateforme POCEAD – ouverture des données

La **Plateforme d’Ouverture, de Centralisation, d’Exposition et d’Analyse des Données (POCEAD)** est dédiée à l’ouverture et à la mise à disposition des données du ministère des armées. Son objectif est d’offrir un ensemble de services permettant d’analyser, de traiter et d’exposer des données aux directions d’application et aux services numériques du ministère.

Les services offerts par POCEAD se composent du stockage et du traitement Big Data (données NP/DR uniquement), de la visualisation et de l’API-sation des données :

- Exploration/ Incubation d’un besoin (Data Lab) : Découverte des outils de Big Data + Exploration de jeux de données, Développement d’un POC (proof of concept)
- Réalisation de cas d’usage, du développement à la production : Data visualisation via QlikSense, Data analyse – BI, Data science – IA
- Exposition d’API via la PEM : Données de référence, Données métier

Par ailleurs, l’équipe assure un conseil à la rédaction d’un CCTP dans le cadre d’un marché public ou d’une FEB pour une UO DIRISI sur les questions relatives aux fonctions couvertes par POCEAD.

POCEAD est en production depuis avril 2019 et permet de développer des cas d’usage jusqu’à leur mise en production.

La Direction d’Application (DA) ou le porteur du cas d’usage est ensuite dirigé vers la BU DATA (Business Unit Data à BRUZ) pour le développement et/ou la mise en production du cas d’usage :

- **Réalisation clef en main** permet de faire développer une maquette ou un produit par l’équipe de développement POCEAD
- **Accompagnement à la carte** permet de développer une maquette ou un produit pérenne par les équipes internes au client en s’appuyant sur l’écosystème POCEAD et avec le soutien de l’équipe de développement POCEAD.
- **Développement en autonomie** permet de développer une maquette ou un produit pérenne par un prestataire en s’appuyant sur l’écosystème POCEAD.

Quelle que soit l’offre d’accompagnement décidée, la DA ou le porteur du cas d’usage dispose d’une documentation disponible sur **Synoptic** (cf. ci-dessous).

POCEAD est aujourd’hui positionnée comme l’outil ministériel de traitement BigData pour des données NP-DR en environnement de production. (cf. §3.2.6.1 *Introduction et orientations ministérielles* pour la stratégie d’évolution).

Document	Date	Origine	Type doc	Portée
Note relative au traitement des données (POCEAD diffusée par courrier N°210/ARM/DGNUM/DG/NP du 8 juin 2020)	8 juin 2020	DGNUM	Note	Intradef
<i>Commentaire : Cette note positionne POCEAD et son articulation avec la plateforme ministérielle de datavisualisation QlikSense</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Big Data – IA Environnement de prod	POCEAD basée sur la plateforme SAAGIE	MinArm		R / S(*)	Intradef

3.2.7.1.3 Plateforme ARTEMIS.IA

Le programme ARTEMIS.IA (ARchitecture de Traitement et d'Exploitation Massive de l'Information multi-sourceS Intelligence Artificielle) a pour objectifs de fournir une infostructure unifiée et souveraine d'analyse et de traitement de données massives (Big Data) et d'Intelligence Artificielle (IA) issues de technologies civiles adaptée aux spécificités du MINARM, de mutualiser les développements tout en permettant d'accueillir la variété des cas d'usages des armées, directions et services (ADS) et de capter l'innovation issue du monde civil au profit des Armées.

L'opération ARTEMIS.IA a démarré en 2017 dans le cadre d'un partenariat d'innovation en 3 phases et est en phase d'industrialisation en 2022 avec un premier déploiement sur le réseau Secret-SF SIA.

L'offre de service sera constituée :

- D'un bac à sable permettant :
 - Le développement en vue de la mise à disposition de nouveaux modules et applications,
 - L'accès aux données opérationnelles sans nuire à leurs disponibilités pour les applications en cours d'utilisation,
 - La mise à disposition des outils pour explorer les données disponibles, et pour entraîner, tester et qualifier des algorithmes basés sur de l'IA.
- D'un kit de développement logiciel permettant :
 - De doter un tiers d'une suite logicielle autonome, indépendante d'une instance ARTEMIS.IA,
 - De réaliser la conception, l'implémentation et les tests unitaires de modules dans les langages Python, R, Java.
- D'une plateforme ARTEMIS.IA permettant de réaliser les tests d'intégration des cas d'usage et de les mettre ensuite en production. Cette plateforme sera utilisée en mode mutualisé c'est-à-dire qu'elle portera les cas d'usage des directions d'application.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Big Data - IA	ARTEMIS IA (cf. 3.2.6.4.3 <i>Plateforme ARTEMIS.IA</i>)	MinArm		R / S	MinArm

3.2.7.2 Analyse prédictive et statistique

Alors que les solutions d'analyse et de génération de rapports classiques appartiennent au domaine du constaté et permettent d'analyser la situation à un moment donné, l'analyse prédictive permet au contraire de répondre au pourquoi de la situation en se focalisant sur les variables explicatives.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Analyse prédictive	POCEAD (cf. 3.2.6.4.2 <i>Plateforme POCEAD – ouverture des données</i>)	MinArm	Cette plateforme offre des fonctions d'analyse prédictive et statistique. (*) soutenu par le CASID/SAND	R / S	Intradef

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Analyse prédictive	ARTEMIS IA	MinArm		A / S	MinArm
Analyse prédictive	- SAS Analytic Pro server - SAS IML - SAS ETS - SAS Access to ODBC - SAS Access to PC Files - SAS Visual Analytics 7.3	SAS	Cette plateforme offre une solution simple d'utilisation, couvrant toutes les fonctionnalités depuis l'alimentation en self-service jusqu'au déploiement de l'analytique en temps réel. SAS sont les pionniers dans le domaine des statistiques et de la prédiction.	D / S	Intradef
<i>Commentaire : Ces solutions sont hébergées sur une plateforme SAS hébergée au CNMO-SI pour des besoins RH (DRH-MD, OSD) et devront migrer dans le cadre de la feuille de route évoquée au §3.2.6.1 Introduction et orientations ministérielles.</i>					
Analyse prédictive	Predictive Analysis	SAP	Cette plateforme offre une solution simple d'utilisation, couvrant toutes les fonctionnalités depuis l'alimentation en self-service jusqu'au déploiement de l'analytique.	D / -	Intradef
Analyse Prédictive	Elastic Search module Machine Learning	Elastic	Cas d'usage spécifique (analyse prédictive sur certaines séries temporelles uniquement)	A / -	

3.2.8 Cadres particuliers

3.2.8.1 ERP

Les ERP³⁸, ou PGI³⁹ en français, sont des logiciels de gestion suffisamment génériques pour convenir à une clientèle élargie. Ils comprennent généralement une base générique et une partie paramétrable.

On parle d'ERP ou de PGI dès lors que le produit considéré couvre au moins deux domaines fonctionnels distincts de l'entreprise (logistique et ressources humaines, par exemple). Cette famille de logiciels peut aller jusqu'à couvrir l'ensemble des besoins de gestion d'une entreprise. Les domaines fonctionnels peuvent être déclinés sous forme de modules optionnels.

Un ERP est efficace lorsqu'il est utilisé pour les processus natifs de la solution. Les personnalisations successives d'un ERP obèrent la possibilité de suivre la feuille de route éditeur et entraîne des coûts de traitement des obsolescences supplémentaires.

Un ERP doit pouvoir s'intégrer dans le socle et doit ouvrir ses données aux applications qui le demandent.

SAP : à titre d'information, le nouvel accord cadre, porté par le MinArm (pilotage par DRHMD/SRSI/SMSIF-RH) a été notifié en juillet 2022, pour 3 ans et renouvelable 1 an.

³⁸ Enterprise Resource Planning.

³⁹ Progiciel de gestion intégré.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
ERP	SAP ECC	SAP	ERP complet utilisé notamment pour les SIRH d'armées (CONCERTO, RHAPSODIE, ORCHESTRA, etc.), la finance (CHORUS) ou la logistique (SINAPSE, ARES, SCALP...)	D / N	Intradef
<i>Commentaire : La suite SAP ECC (ERP Central Component) sera formellement interdite dans les nouveaux projets dont la mise en production se fera à partir du 1er janvier 2023. A l'heure actuelle le support de cette suite est assuré par la société SAP jusqu'en 2030.</i>					
ERP	SAP HANA S/4HANA	SAP	Assujetti à une justification du cadre d'emploi	A / N	Intradef
<i>Commentaire : Il est indispensable de pleinement prendre en compte les fortes contraintes imposées par ces ERP, à la fois pour leur hébergement, leur exploitation, leur MCO, leur encapsulation des données que pour leur intégration au sein du SI du Ministère avant d'y recourir.</i>					
ERP	HR Access Suite	HR Access Solutions (Sopra)	Progiciel utilisé pour les RH et la finance, utilisé pour ALLIANCE et SOURCE Solde	A / N	Intradef
<i>Commentaire : Il est indispensable de pleinement prendre en compte les fortes contraintes imposées par ces ERP, à la fois pour leur hébergement, leur exploitation, leur MCO, leur encapsulation des données que pour leur intégration au sein du SI du Ministère avant d'y recourir.</i>					

Nota : Les produits présentés sont actuellement utilisés au sein du ministère. Ils ne contraignent pas les évolutions à venir.

⚠ L'obtention d'une dérogation pour mettre un oeuvre un de ces produits n'exempte pas de la nécessité de respecter les normes, standards et directives du Ministère, dont la nécessité de recourir aux briques du socle, pour l'authentification via MinDefConnect ou la consommation et l'exposition des données via API Rest par exemple.

3.2.8.2 Moteur de génération de rapports

Cf. 3.2.6 Informatique « décisionnelle », Big Data, analyse prédictive.

3.2.8.3 Archivage

3.2.8.3.1 Documents de portée générale OTAN

Document	Date	Origine	Type doc	Portée
Politique relative à la gestion des archives courantes et intermédiaires de l'OTAN (C-M(2011)0043)	17 juin 2011	NATO	Politique	MinArm
Directive sur la gestion des archives courantes et intermédiaires de l'OTAN (C-M(2012)0014)	27 février 2012	NATO	Directive	MinArm
Stratégie OTAN pour la conservation à long terme des informations numériques (AC/324-D(2012)0003)	8 août 2012	NATO	Stratégie	MinArm
Directive sur la conservation des informations numériques OTAN pérennes (AC/324-D(2014)0008)	3 juillet 2014	NATO	Directive	MinArm

3.2.8.3.2 Documents de portée générale nationale

Document	Date	Origine	Type doc	Portée
Code du patrimoine livre II	15 juillet 2008	Ministères	Loi	Toute administration
Référentiel Général de Gestion des Archives [R2GA] publié par le comité interministériel aux Archives de France Cf 2.2.3.1 Référentiels généraux (RGI, RGS, RGAA, R2GA, RGESN)	Octobre 2013	PM	Référentiel	Toute administration

Le RGI V2 définit par ailleurs un profil d'archivage

Profil d'interopérabilité	Description / Utilisation / Restriction	Statut	Portée
Profil « Archivage »	Ce profil, entretenu par le Service Interministériel des Archives de France (SIAF), identifie les normes de modélisation conceptuelle et les standards techniques intervenant dans les échanges, liés à la gestion de l'archivage, la consultation ou la conservation de documents. <i>(cf. description détaillée du profil RGI V2 p74)</i>	R	Toute administration

3.2.8.3.3 Documents de portée générale Ministérielle

Document	Date	Origine	Type doc	Portée
Instruction ministérielle 101 relative à la politique et à l'organisation de générale de l'archivage du ministère de la défense, IM n°101/DEF/SGA/DMPA/DPC du 29 juillet 2011	29 juillet 2011	DMPA	Instruction	MinArm
Directive DGSIC n°30 portant sur la mise en œuvre de la démarche d'archivage des contenus dans les projets de SI publiée au Bulletin Officiel des Armées	5 déc. 2013	DGSIC	Directive	MinArm
<i>Commentaire : Recommandations sur la prise en compte de l'archivage dans la conduite des projets de SI, notamment pour la conception, les évolutions et le retrait du SI Point de contact : DMPA / DP Archivage</i>				
Guide ministériel relatif à l'intégration de la démarche d'archivage dans les projets de systèmes d'information V1.0 approuvé le 30 septembre 2013	30 septembre 2013	DMPA	Guide	MinArm
Manuel pour élaborer la stratégie d'archivage d'un SI V1.0 approuvé le 30 septembre 2013	30 septembre 2013	DMPA	Manuel	MinArm
Positionnement des outils collaboratifs dans le cycle de vie du document, sous double-timbre n°394/DEF/DGSIC/SDAU/NP du 8 juillet 2015 n°D-15-004558/DEF/EMA/CPI/NP du 8 juillet 2015	8 juillet 2015	DGSIC EMA	Note	MinArm
<i>Commentaire : Cette note issue du comité directeur des Intranets précise pour rappel que les outils de travail collaboratif n'ont pas vocation à être utilisés à des fins d'archivage de documents validés et rappelle les principaux éléments de la démarche d'archivage au sein du ministère des armées.</i>				

3.2.8.3.4 Documents techniques MinArm

Document	Date	Origine	Type doc	Portée
Préconisations pour la pérennisation de l'information : validées en CECSIC du 22 juin 2012	28 juin 2012	DGSIC DMPA	Recommandations	MinArm
<i>Commentaire : Ce document est un livrable d'un GT archivage piloté par la DGSIC et la DMPA, dont les annexes principales ont été présentées et validées lors du conseil exécutif des SIC (CECSIC) du 28 juin 2012. Le document émet des recommandations concernant :</i>				
<ul style="list-style-type: none"> - les métadonnées essentielles pour la maîtrise du cycle de vie de l'information ; - les formats pérennes pour les documents électroniques. 				

3.2.8.3.5 Solution ministérielle Archipel

Le projet Archipel a pour objet de mettre en place le système d'archivage du ministère en s'appuyant sur le progiciel Everteam (front office) et la solution d'archivage interministériel Vitam ([back office](#)) qui apportent une garantie de sécurité et de disponibilité pour les archives papiers et électroniques, quel qu'en soit le niveau de protection. Le projet est en production pour la partie NP/DR et gestion du classifié papier depuis 2021.

Ses principales caractéristiques sont :

- La prise en compte des besoins utilisateurs métier par l'apport des **fonctionnalités nécessaires au fonctionnement des services publics d'archives** : entrées, recherches, consultation, communication, administration et gestion, structurations arborescentes, référentiels... ;
- La **gestion unitaire de fortes volumétries** de données et l'accès à la pièce par des requêtes riches ;
- La **garantie de la valeur probante** des archives par le respect des normes et standards en vigueur (NF Z 42-013, Z 42- 020, Z 44-022, SEDA...), par la traçabilité des opérations et du cycle de vie des objets et leur journalisation sécurisée ;
- La sécurité et la robustesse : la gestion applicative du stockage permet une **réPLICATION** des données, métadonnées, index et journaux d'évènements sur plusieurs sites et plusieurs offres contrôlées ; l'architecture interne du stockage assure la **capacité de reconstruire** le système à partir d'une seule offre, en une fois ou au fil de l'eau ;
- La possibilité d'une **utilisation mutualisée** grâce à la gestion multi-tenant de Vitam.

Document	Date	Origine	Type doc	Portée
Documentation technique relative à VITAM accessible sur http://www.programmavitam.fr		DINUM	Documentation technique	Interministériel
<i>Commentaire : VITAM est la couche back office de l'archivage développé en interministériel par la DINUM.</i>				
Documentation relative à au télé-service de versement aux archives [TSV]	Octobre 2019	DMCA	Documentation technique	Intradef
<i>Commentaire : TSV est un outil de versement au service des archives de ministère des armées mis en service en mai 2018.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Archivage	<i>ARCHIPEL solution ministérielle</i>	MinArm		R / S	Intradef

3.2.8.4 Informations géographiques, hydrographiques, océanographiques et météorologiques (GHOM)

Un système d'information géographique (SIG) est un système d'informations permettant de créer, d'organiser

et de présenter des données géo référencées, ainsi que de produire des plans et des cartes. Ses usages couvrent les activités géomatiques de traitement, de partage et de diffusion de l'information géographique.

Document	Date	Origine	Type doc	Portée
Directive DGNUM n°9 portant sur les données géographiques, hydrographiques, océanographiques et météorologiques de Défense sous forme numérique diffusée par note n°298 /ARM/DNUM/DG/NP du 23 juillet 2019	22 juillet 2019	DNUM	Directive	MinArm
<i>Commentaire : La nouvelle version actualise et précise les règles d'exploitation des données géographiques, hydrographiques, océanographiques et météorologiques de Défense et les formats associés</i>				
Guide DGA S-CAT n°14107 de spécifications fonctionnelles pour la composante géographique des systèmes de la défense 3 ^{ème} édition entretenue par DT/ST/DGA IP/ASC/ENV	10 octobre 2012	DGA IP	Guide	MinArm SIO
<i>Commentaire : Ce guide traite des données à caractère géographique de l'espace aéroterrestre, hors renseignement et à l'exclusion notamment des données hydrographiques utilisées notamment pour les cartes marines de navigation, des données météo et aéronautiques. Il précise les spécificités fonctionnelles liées aux formats des données choisies. Le guide DGS-SCAT n°14109, même édition, même date, en constitue une version synthétique.</i>				

Le RGI V2 définit un profil géométrique pour l'échange de données géographiques entre administration :

Profil d'interopérabilité	Description / Utilisation / Restriction	Statut	Portée
Profil « Géométrique »	Ce profil, entretenu par le Conseil National de l'Information Géolocalisée (CNIG), identifie les principaux standards recommandés pour les échanges d'informations géographiques entre les administrations pour localiser notamment des événements, des données, des activités, des objets. <i>(cf. description détaillée du profil RGI V2 p74)</i>	R	Toute administration

3.2.8.4.1 GEODE 4D

Le SI GEODE 4D apportera un portail WEB qui permettra de consulter les situations d'environnement, de télécharger les produits GHOM (données géographie uniquement), de demander des prestations de soutien GHOM et de faire remonter des informations. Pour le domaine géographique, le Portail GEODE 4D remplacera le catalogue EGI actuel.

Des services web majoritairement basés sur les standards de l'OGC (Open Geospatial Consortium) seront en outre disponibles sous condition pour les applications intégrées dans une configuration SIA.

3.2.8.4.2 Moteur cartographique OSM sur Intradef

Le moteur cartographique OSM, en cours de réalisation, offrira un service de mise à disposition de fonds de carte, basés sur OpenStreetMap, et un service de visualisation de données géo-référencées, autorisant la recherche d'une ville, d'une adresse et la récupération des coordonnées géographiques associées.

Ces éléments seront accessibles par des API de type REST inscrits dans le catalogue de la PEM Intradef.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Moteur cartographique	Solution ministérielle basée sur OpenStreetMap	MINARM		E / E	Intradef
Partage de données	GeoServer	Open Source	url : geoserver.org	A / N	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
geospatial					

3.2.9 Démarche simplifiée (DS) – Dossier numérique de l'agent (DNA)

3.2.9.1 Démarches simplifiées (DS)

Ce service fonctionnel commun permet de dématérialiser des démarches administratives grâce à un générateur de formulaires et une plateforme d'instruction de dossiers. Il permet de gérer le cycle de vie d'un formulaire, de sa conception jusqu'à son intégration dans les traitements applicatifs, à la main complète des métiers. Cette application est construite sur la solution « [demarches-simplifiees.fr](https://www.demarches-simplifiees.fr) » co-développée par la DINUM et le ministère des Armées. Le service offre une API permettant l'intégration réactive (Webhook en GraphQL) avec des systèmes tiers. Sur les instances ministérielles, le service est intégré avec le service DNA pour permettre la simplification administrative et le DNLUF (« [Dites-Le Nous Une Fois](#) »), il s'appuie sur les référentiels ministériels pour les données de référence, et fait appel à des notifications par mail pour la gestion des étapes de validation (INA / POCEAD / système de cartographie Open Street Map, API tierces...).

Il existe trois instances :

- **Sur Internet**, la DINUM héberge et maintient le service qui bénéficie de l'interconnexion à de nombreux services de l'État plateforme, notamment France Connect, API Entreprise, API Géo et BAN.
- **Sur Intradef**, le ministère des Armées en a assuré un portage sur Intradef, opérationnel et homologué au printemps 2019.
- **Sur l'Internet Maitrisé** : le service, en cours de déploiement, permettra une continuité Internet / Intradef et s'appuie sur les capacités de fédération d'identités de MindefConnect Internet.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Dématérialisation de procédures	demarches-simplifiees.fr	DINUM	Solution développée et soutenue par la DINUM https://www.demarches-simplifiees.fr/	R / S	Internet
Dématérialisation de procédures	Solution de la DINUM portée sur Internet	MINARM	Solution maîtrisée par le ministère https://demarches-simplifiees.defense.gouv.fr/	E / N	Internet
Dématérialisation de procédures	Solution de la DINUM portée dans l'environnement Intradef	MINARM	Soutien par le projet DS au profit du ministère	R / S	Intradef
<i>Commentaire : Sur Intradef, la solution est opérationnelle et homologuée depuis avril 2019. La documentation du service se trouve sur le portail de la DINUM / https://doc.demarches-simplifiees.fr/</i>					

3.2.9.2 Dossier numérique de l'agent (DNA)

Le DNA est un service en cours de réalisation. Il offrira un espace de stockage et de mise à disposition de documents et justificatifs à des fins de simplification administrative. Le service sera disponible sur l'Internet maîtrisé et l'Intradef.

Les documents et justificatifs fournis pourront être mis à disposition des applications après autorisation de l'administré. Les documents et justificatifs sur le DNA sur Internet peuvent être déposés seuls sur Internet, puis être ensuite basculés sur Intradef si besoin st (cas du recrutement ou des pensionnés).

Pour l'administré, le DNA offre un point d'accès unique à ses données tant sur Internet que sur l'Itradef, lui permet de solliciter des rectifications, si nécessaire, et de partager simplement de la donnée avec un tiers.

Pour les directions d'application, le DNA permet, au travers d'une API, de déposer et récupérer un document (notification type A/R à l'administré). Afin d'être en conformité avec le RGPD, la direction d'application doit établir un contrat d'usage accompagné d'un protocole d'échange entre son application et le DNA.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Simplification administrative	DNA Internet	MINARM	NP	E / S	Internet
Simplification administrative	DNA Intradef	MINARM	NP/DR <i>(*) soutenu par le projet au profit du ministère</i>	E / S	Intradef
<i>Commentaire : Solution développée en mode agile.</i>					

3.2.10 Intelligence artificielle

Document	Date	Origine	Type doc	Portée
Dossier relatif aux risques de sécurité et aux bonnes pratiques portant sur l'intelligence artificielle	Avril 2022	CNIL	Dossier	
Guide de recommandations pour la spécification et la qualification de systèmes intégrant de l'intelligence artificielle V2	30 octobre 2020	DGA	Guide	MinArm
<i>Le guide de la DGA présente les principaux enjeux techniques liés à l'intégration d'intelligence artificielle (IA) dans les systèmes opérationnels et propose une méthodologie pour leur mise en œuvre, de la spécification à la qualification des systèmes, mais aussi tout au long de la vie du système déployé.</i>				
<i>Le dossier de la CNIL présente les différentes attaques possibles sur un système IA, détaille une méthodologie d'analyse de risques et présente les bonnes pratiques pour la sécurisation d'un système IA.</i>				

Les IA génératives ne sont pas complètement maîtrisées dans le secteur civil notamment par les GAFAM, qu'elles rendent d'ors et déjà des services pour les cadres de tous les secteurs d'activités.

Le milieu militaire n'est pas exclu (+ de 10 millions de requête au MINARM selon la DPID) et l'emploi de ces outils génère des risques métier et de sécurité.

Dans le cadre de la mission du laboratoire Big Data et IA visant à faciliter l'expérimentation rapide des nouvelles fonctionnalités offertes par les IA génératives ouvertes (génération de texte, d'images et de sons), le SGA a mis en place une plateforme d'expérimentation de l'IA Générative texte à texte sur PICSEL.

A la suite de la réunion d'éclairage et d'anticipation stratégique (REAS) du 7 juin 2023, le CEMA a demandé une expérimentation sur les IA génératives afin d'acquérir une première capacité expérimentale d'IA générative spécifique aux métiers de l'état-major stratégique. Les principes retenus sont une réutilisation des projets existants et l'usage d'outils perfectibles tout en l'améliorant durant son utilisation.

L'EMA a donc rejoint la plateforme du Labo Big Data et IA dans le cadre de son projet. Cette plateforme accueille simultanément deux expérimentations cadrées :

- celle du SGA conduite par le Labo Big Data et IA (GenIAI) ;
- celle de l'EMA sur la partie DR conduite par le C2LAB (Projet VAUBAN / cas d'usage PILACTI).

Il s'agit donc de proposer une alternative aux IA génératives du secteur civil pour réduire le risque de fuite d'informations.

Egalement, cela consiste à évaluer l'intérêt opérationnel et d'intégrer progressivement, et au plus tôt lorsque

c'est possible, des outils d'IA générative au sein de nos organisations en identifiant et en développant des cas d'usage qui pourront être ensuite reproduits ou étendus. Cette expérimentation vise à :

- Tester la pertinence des modèles d'IA générative open source (test du modèle Mistral.AI prévu) ;
- Affiner la définition des besoins de ce type de solutions ;
- Calibrer les travaux pour anticiper les futures capacités pour passer à l'échelle ;
- Préparer l'organisation et les procédures pour utiliser et maintenir ce type de solution.

3.2.11 Internet des objets – IOT

Document	Date	Origine	Type doc	Portée
Guide ANSSI de recommandations relatives à la sécurité des (systèmes d') objets connectés	27 août 2021	ANSSI	Guide	Toute administration

Commentaire : Ce guide présente des recommandations de sécurité pour un système d'objets connectés. Il peut être utilisé pour concevoir un tel système ou pour en faciliter l'analyse sécuritaire. Ce guide comprend deux parties, l'architecture d'un système connecté et les propriétés de sécurité attendues, puis les recommandations techniques.

3.3 Services d'infrastructure

3.3.1 Messagerie / Agenda / Tâches / Listes de diffusion

Le service utilisateur associé est décrit en §3.1.1.7 *Messagerie* ainsi que la partie client.

3.3.1.1 Messagerie non officielle – Agenda [MEL-AGE]

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°3 définissant les règles de la messagerie électronique publiée au Bulletin Officiel des Armées.	08 janvier 2008	DGSIC	Directive	MinArm

Commentaire : Mécanismes permettant la mise en œuvre d'une messagerie électronique. Périmètre : tous les intranets. (À noter que dans la RT11, XIMF est à choisir de préférence à XSMTP, que la RT20 relative à Thunderbird n'est plus la solution recommandée par le ministère)

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°53 « Gestion des adresses fonctionnelles et listes de diffusion dans l'Annudef » du 28/08/2013	28 août 2013	DIRISI/SCO E	Directive	Intradef

Commentaire : la directive précise notamment les modalités d'association des adresses fonctionnelles aux adresses personnelles sur l'Intradef, ainsi que les modalités de gestion des listes de diffusion de l'Annudef.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Messagerie (Serveur)	Serveur Exchange	Microsoft	Service déployé sur tout l'Intradef	R / S	Intradef

Commentaire : Les protocoles à utiliser pour l'émission et la réception sont respectivement SMPTPs et IMAPs avec authentification..

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Messagerie (Serveur)	Serveur Exchange Interface Web (OWA) et WebService (EWS)	Microsoft		R / S	Intradef

Commentaire : ces interfaces permettent l'accès aux fonctions du serveur via un navigateur ou en Webservice

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Messagerie (Serveur)	Serveur Exchange	Microsoft	Service déployé sur SIA S-SF, IntraCed S-SF et SIA FrOpS	R / S	S-SF SIA FrOpS
Messagerie (Serveur)	Serveur Exchange Interface Web (OWA) et WebService (EWS)	Microsoft	Service déployé sur SIA S-SF / SIA FrOpS	R / S	S-SF SIA FrOpS
Messagerie (Serveur)	Solution basée sur composants Postfix, Cyrus IMAP)			A / N	S-SF
Messagerie (Interop)	Serveur Postfix	Postfix.org, licence IBM Public Licence	Utilisé pour assurer un relais de messagerie en bordure de système (NEMO).	A / S	Intradef S-SF SIA FrOpS
Messagerie (Interop)	Serveur Cyrus IMAP	Carnegie Mellon University, licence BSD	Utilisé en serveur SMTP/IMAP d'appoint, assujetti à uncadre d'emploi ne relevant pas des services communs	A / S	Intradef S-SF SIA FrOpS

3.3.1.2 Gestion de tâches [GTA]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion de tâches	La gestion de tâche personnelle est intégrée dans les solutions de messagerie <i>Cf. 3.3.1.1 Messagerie non officielle – Agenda [MEL-AGE]</i>			R / S	Intradef S-SF SIA FrOps

3.3.1.3 Liste de diffusion [LDF]

Document	Date	Origine	Type doc	Portée
Gestion des listes de diffusion dans l'Annudef (cf. 3.1.1.7.1 Messagerie non officielle)				
Commentaire : décrite par la directive DIRISI n°53. Cette directive définit le processus de gestion de liste statiques et dynamiques.				
Gestion des listes de diffusion dans l'Annudef (cf. 3.1.1.7.1 Messagerie non officielle)				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Listes diffusion	Produit annuaire défense	MinArm	Gestion de liste de diffusion gérée suivant la directive DIRISI n°53 (cf. 3.3.1.1 ci-dessus)	R / S	Intradef

3.3.2 Partage d'information et publication

3.3.2.1 Portail personnalisable [GPE]

Le service utilisateur associé est décrit en §3.1.1.9 Portail personnalisable [SU-GPE].

Document	Date	Origine	Type doc	Portée
Portail collaboratif des armées, note diffusée sous timbre D-19-004391/ARM/EMA/ESMG/NP	26 juillet 2019	MGA	Note	Ministère
<i>Commentaire : Cette note fait état d'une décision de l'EMA d'un portail collaboratif unique pour le besoin des armées, dénommé PC@, sur la base de la technologie mise en œuvre sur le portail des opérations existant.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Portails	Liferay	Liferay	Pour les applications en usage dans le cadre du STC-IA	R / S	Intradef S-SF SIA FrOps
Portails	Sharepoint	Microsoft		R / S	Intradef
Portails	PC@ (sur base Sharepoint)	MinArm	Portail des opérations	R / S	Intradef S-SF SIA FrOps
<i>Commentaire : Le déploiement isolé de l'outil Sharepoint Designer, désormais intégré dans les nouvelles versions de Sharepoint (à partir de 2016), n'est plus nécessaire.</i>					

3.3.2.2 Portail d'information [PIN]

Le service utilisateur associé est décrit en §3.1.3.1 Portail intranet [SU_PIN].

Document	Date	Origine	Type doc	Portée
Compte rendu du CODIR restreint des Intranets n°24 du 3 avril 2014 diffusé par note conjointe : n°D-14-004992 /DEF/EMA/PSIOC/NP du 19 mai 2014 n°316/DEF/DGSIC/NP du 20 mai 2014	19 mai 2014 20 mai 2014	CODIR Intranets	Note	Internet Intradef
<i>Commentaire : le compte rendu porte décision relative au choix des outils pour les portails de communications pour le NP-DR.</i>				



Pour les CMS, la conformité des modules retenus aux critères d'éligibilité doit être vérifiée dans le processus d'homologation ou validée en gouvernance technique (§ 1.9.2 Processus de saisine pour validation d'architecture ou dérogation au CCT)



Les écosystèmes des systèmes de gestion de contenu (CMS) sont riches et disposent de nombreux modules complémentaires pour étendre leurs fonctionnalités mais non nécessairement qualifiés par l'éditeur. Afin d'en assurer la maintenabilité, il convient, d'une part, d'en limiter le nombre au juste besoin, et, d'autre part, de ne retenir que des modules présentant des critères de confiance tels que définis au §8.6.3 Critères d'éligibilité pour des modules de CMS.

Les modules autorisés pour les CMS recommandés et soutenus sont référencés au paragraphe 8.2.2 Modules pour CMS Drupal, Joomla ! et Wordpress L'ajout d'un nouveau module est soumis à vérification préalable

des critères évoqués ci-dessus.

→ En conséquence, pour les CMS non infogérés, la conformité des modules aux critères d'éligibilité doit avoir été vérifiée dans le processus d'homologation ou validée en gouvernance technique.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Portails	Joomla!	Joomla!	Pour une utilisation orientée portail de communication <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u></i>	* / *	Tout intranet Internet
Portails	Drupal	Opensource	Pour une utilisation orientée portail de communication	R / S	Tout intranet Internet
<i>Commentaire : Drupal permet la mise en place d'un CMS de type Headless Ce type de solution vise à découpler le système front-office de présentation des données à l'utilisateur, des données créées et stockées en back-office. Dans cette logique, le back-office expose une API susceptible d'être consommée par différents front-office, permettant ainsi de faciliter la diffusion d'un même contenu sur différents types de canaux et supports.</i>					
Portails	WordPress	Opensource	Pour une utilisation orientée portail de communication	A / N	Intradef Internet (hors Heliss-NG)
<i>Commentaire : Le recours à WordPress est assujetti à une demande de dérogation justifiant d'usages non couverts par les produits listés ci-dessus. Le choix des modules déployés doit respecter les critères affichés au chapitre 8.6.2</i>					
Portails	Alfresco Community Edition	Alfresco	Pour une utilisation nécessitant des fonctionnalités avancées de travail collaboratif ou d'intégration applicative	A / S	Intradef Internet
Portails	Alfresco Community Edition	Alfresco	Pour une utilisation nécessitant des fonctionnalités avancées de travail collaboratif ou d'intégration applicative	A / S	S-SF SIA FrOps
Portails	SharePoint	Microsoft	Pour une utilisation nécessitant des fonctionnalités avancées de travail collaboratif ou d'intégration applicative NB : embarque nécessairement une base de données SQL Server	A / S	Tout intranet Internet

Se reporter également à l'annexe 8.6.3 *Critères d'éligibilité pour des modules de CMS*

3.3.2.3 Crédit de sites Web [CSW]

Pas de référence identifiée à ce jour.

3.3.2.4 Gestionnaire de métadonnées [GMD]

Complément sur METADATARM en 2024.

3.3.2.5 Syndication de contenu [ASY]

Pas de référence identifiée à ce jour.

3.3.2.6 Répertoires partagés [REP]

Ce service est fourni sur l’Intradef ainsi que sur le S-SF et le SIA FrOps (métropole et configuration projetable). Un recours aux répertoires partagés demeure possible dans la mesure où elles autorisent des fonctionnalités avancées de gestion des droits, de recherche et d'affichage n'impliquant pas le recours à des actes techniques d'administration. Compte tenu du coût de maintenance, d'infogérence, cette solution n'est pas à privilégier.

3.3.2.7 Moteur de recherche [RMR]

Le service utilisateur associé est décrit en §3.1.3.4 *Moteur de recherche [SU-RMR]*

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Moteur recherche	Qwant	Qwant	Moteur de recherche préservant les données utilisateurs dont l'usage est encouragé par le gouvernement.	R / -	Internet
Moteur recherche	SYRIARM	AND	Solution ministérielle basée sur Sinequa	R / S	Intradef
Moteur recherche	SINEQUA	Sinequa	Toute solution utilisant SINEQUA en dehors de la solution ministérielle est soumise à dérogation.	A / S	Intradef S-SF SIA FrOps

3.3.2.8 Gestion des communautés d'intérêt [COI]

Le service utilisateur associé est décrit en §3.1.2.2 Espace de travail collaboratif [SU-EDT]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Travail collaboratif	SharePoint Server 2016 Enterprise	Microsoft		R / S	MinArm
Travail collaboratif	Alfresco Community Edition	Alfresco		R / S	Intradef
Travail collaboratif	Alfresco Community Edition	Alfresco	Dans le cas où les instances Sharepoint ne seraient pas utilisables	A / S	S-SF SIA FrOps
Travail collaboratif	OSMOSE	DINUM	Proposée par la DINUM, la plateforme Osmose permet aux agents de l’État et de ses établissements publics d'animer en ligne une communauté professionnelle. URL : https://osmose.numerique.gouv.fr	R / S	Internet
Travail collaboratif	RESANA	DINUM	Destinée aux agents de l’État, la plateforme collaborative interministérielle Resana leur offre un espace numérique complet pour faciliter le stockage, le partage et la coédition de documents, mais aussi le travail en équipe et en mode projet, y compris en mobilité grâce à une	R / S	Internet

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
			application dédiée. URL : https://resana.numerique.gouv.fr		

3.3.2.9 Réseau social d'entreprise [RSE]

Le service utilisateur associé est décrit en §3.1.2.7 Réseau social [SU-RSE]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Réseau social	Solution Synoptic Basé sur Drupal	MinArm	Cette solution permet la mise en œuvre d'espaces thématiques et l'animation en réseau de ces espaces Contact à prendre avec la DGNUM (*) Soutien assuré par le CASID au profit du ministère.	R / S(*)	Intradef

3.3.2.10 Enquête et sondage [ENQ]

Le service utilisateur associé est décrit en §3.1.3.5 Enquête et sondage [SU-ENQ]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Enquêtes-Sondages	SHERLOCK		Solution ministérielle basée sur limesurvey	R / S	Intradef
Enquêtes-Sondages	Limesurvey		En cas d'impossibilité d'utiliser la plateforme ministérielle *pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits	* / *	Intradef
Enquêtes-Sondages	Isidate	DGA	Outil de sondage pour recherche d'une date	R / S	Intradef

3.3.3 Travail de groupe

Service utilisateur associé : cf. 3.1.2.1 Communication instantanée ainsi que la partie client.

3.3.3.1 Messagerie instantanée – Réunion virtuelle – Vidéoconférence - Rédaction collaborative synchrone [MIN-REV-VIH-RCS]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Communications instantanées	Skype for business Server	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits	R / S	Intradef
Communications instantanées	Lync (serveur couplé au client Lync)	Microsoft	Solution obsolescente (remplacement par Skype)	D / O	S-SF SIA FrOps
Communications instantanées	Skype for business Server	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits	R / E	S-SF SIA FrOps

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Communications instantanées	TCS (solution serveur basé sur openfire, couplé au client JChat)	NCIA	Solution de chat opérationnelle nativement interopérable avec l'OTAN	A / S	Intradef S-SF SIA FrOps
Communications instantanées	Jitsi		Utilisé par exemple dans le service interministériel (webconf.numerique.gouv.fr) (*)Soutien DINUM	A / S(*)	Internet
Communications instantanées	Prosody	Equipe Prosody	Assujetti au contexte SIE : Serveur XMPP sous licence libre MIT utilisée dans le cadre du SIE	A / S(*)	SIE
Communications instantanées	Tchap	DINUM	Solution de chat sécurisé interministériel (*)Soutien DINUM	R / S(*)	État Internet
Communications instantanées	WEBEX Version entreprise	Cisco	Solution de visio/toip (S-SF / SIA FrOps / Mission Secret...). S'adosse à des équipements de télé/visioconférence. (Client Jabber standard).	A / N	S-SF SIA FrOps
Communications instantanées	VVIPER	AND	Solution de visio/toip (S-SF). Déploiement envisagé sur SIA FrOps (échéance non consolidée à date) <i>Soutien via une TME</i>	E / S	S-SF
Plateforme de collaboration	NextCloud	NextCloud GmbH	L'assujettissement porte sur les plugins NextCloud	A / N	MinArm
Communications instantanées	Mattermost	Mattermost	Restriction au client web <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	* / *	MinArm

3.3.3.2 Wiki [WIKI]

Le service utilisateur associé est décrit au §3.1.2.3 *Wiki /SU-WKI/*. La gouvernance technique ne recommande aucun produit particulier, cependant il est désormais préconisé de recourir aux solutions de wiki compatibles du langage Markdown pour ses possibilités de normalisation et d'interopérabilité. Les solutions mentionnées ci-après demeurent celles principalement déployées au sein du Ministère.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Wiki	Mediawiki		Déployé pour wikidefense et dans TULEAP, recommandé dans le SILL 2020	- / N	Intradef
Wiki	DokuWiki	Communauté DokuWiki	Assujetti au contexte SIE : Déployé dans le cadre du SIE	A / S	SIE
Wiki	xWiki	xWiki SAS	Version de jQuery employée désormais obsolète et non soutenue	A / N	Intradef
Wiki	xWiki	xWiki SAS	Version de jQuery employée désormais obsolète et non soutenue	R / N	Hors Intradef

3.3.3.3 Forum [FOR]

Le service utilisateur associé est décrit au §3.1.2.5 *Forum [SU-FOR]* ainsi que la partie clientUn forum pouvant être mis en place, de façon intégrée avec les outils collaboratifs.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Forum	PhpBB		Déployé actuellement assez largement (marine, armée de terre...) En l'absence d'autres portages	A / N	Intradef

3.3.4 Services d'annuaires [ANN]

Les annuaires s'inscrivent dans la démarche menée au niveau ministériel autour de la « gestion des identités numériques et des accès », plus connue sous l'acronyme anglais IAM (pour identity and access management). Cette démarche est portée par le projet d'ensemble « Identités Numériques et Autorisations » [INA] (*cf. §4.6.1.1 Démarche INA : RIN*) présentant une architecture à trois niveaux :

- au niveau ministériel, un référentiel des identités numériques [RIN] contenant les données communes à tous les intranets du ministère relatives aux données d'identités des personnes ; l'Annudef sur l'Intradef fait aujourd'hui fonction de référentiel ministériel ;
- sur chaque intranet, le RIN sert de base à la constitution d'un référentiel d'intranet (RIAXXX) avec l'adjonction de données spécifiques au niveau d'intranet (adresse électronique, certificats, organisation...) ou de données permettant aux applications de gérer les autorisations ;
- enfin ces référentiels d'intranet servent de point d'alimentation et d'adossement des annuaires techniques nécessaires au fonctionnement des services, des applications et du composant MindefConnect de l'intranet concerné.

La constitution de ces annuaires fait l'objet du projet SI INA mené dans le cadre de la démarche INA.

A date, seuls le RIN et le RIADef sont en cours de réalisation.

3.3.4.1 Annuaires / référentiels

Document	Date	Origine	Type doc	Portée
Directive DGSIC n° 2 portant sur le système d'annuaires du ministère de la Défense (publié au BOA sous la référence BOC N°17 du 19 juillet 2007, texte 1)	9 mars 2007	DGSIC	Directive	MinArm
<i>Commentaire : directive de portée générale (LDAP, schéma d'annuaire,...)</i>				
Directive de nommage des annuaires : note n°D-12-005368/DEF/EMA/CPI/SIA/NP du 12 juin 2012	12 juin 2012	EMA	Note	MinArm
<i>Commentaire : mise en forme des informations d'annuaire et des adresses de messagerie électronique.</i>				
<i>⚠️ plusieurs textes définissent les règles de nommage d'annuaire notamment pour la levée d'homonymie, les notions d'organisme (directive DGSIC, n°2 et n°3, directive de nommage des annuaires EMA, RGI, concept d'emploi pages jaunes/pages blanches...). Un travail de mise en cohérence de ces textes doit être mené pour lever toute ambiguïté et préciser le texte applicable.</i>				
Directive DIRISI/SCOE n° 53 « Gestion des adresses fonctionnelles et listes de diffusion dans l'Annudef » version 2 (<i>cf. 3.1.1.7.1 Messagerie non officielle</i>)	28 aout 2013	DIRISI	Directive	MinArm
<i>Commentaire : déjà cité dans le chapitre sur les messageries, la directive précise notamment les modalités d'association des adresses fonctionnelles aux adresses personnelles sur l'Intradef</i>				

Document	Date	Origine	Type doc	Portée
Schéma d'annuaire des Intranets de la Défense v2.3 N°2012/263131/DGA MI/SDT/ASC/TIE/1000305 du 26/11/2012 approuvé par SC2 le 23 novembre 2012	26 nov. 2012	SC2 ⁴⁰	Référentiel	MinArm
Catalogue des OID de la défense v2.5 (n° 2012/263135/DGA MI/SDT/ASC/TIE/1000305 du 21/11/2012)	9 mars 2023	DIRISI sous couvert SC ^{2A}	Référentiel	MinArm
<i>Commentaire : catalogue des OID spécifiques défense associés.</i>				
ACP133 (D) Common Directory Services and Procedures – Juillet 2009	Juillet 2009	OTAN/CCE B	Référentiel	OTAN
ACP 133 SUPP-1 (A) Common Directory Services and Procedures Supplement – Juillet 2009				
<i>Commentaire : décrit tous les éléments en termes d'annuaire (services d'annuaire, architecture, protocole, schéma d'annuaire, procédures), nécessaires à l'interopérabilité au sein de l'OTAN et entre les alliés et notamment pour gérer les communications alliées incluant des services (messagerie, pages blanches/pages jaunes, infrastructures de clés publiques...). Cette normalisation repose largement sur les standards du monde civil.</i>				

Référentiel d'Identités Numériques [RIN]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Annuaire	RIN : référentiel ministériel des Identités Numériques	MinArm	À terme, le ministère disposera d'un seul référentiel d'identités entretenu par le SI INA pour tous les intranets	R / E	Intradef

Référentiel d'annuaires par intranet

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Annuaire	Annudef	MinArm	Le rôle du RIN est tenu actuellement par l'annuaire référent de l'intranet sensible (Annudef). À terme l'Annudef sera remplacé par le RIADef , extraction du RIN pour l'Intradef.	R / S	Intradef
Annuaire	RIADef : Référentiel d'Identités et d'Autorisations du ministère	MinArm	À terme, le ministère disposera d'un référentiel d'identités et des données d'autorisations entretenu par le SI INA sur Intradef	R / E	Intradef
Annuaire	OpenLDAP : annuaire de référence Annubat : interface de consultation	MinArm	Solution déployée dans le cadre du SIE	R / S	SIE
Annuaire	OpenLDAP : Annuaire de référence MEIBO : gestion de contenu (+ développements)	MinArm	Solution SIA S-SF pour la métropole. Solution également pour le fédérateur Intraced	R / S	S-SF SIA FrOps

⁴⁰ sous-comité architecture et service de l'ancien comité directeurs des intranets

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Annuaire	OpenLDAP : Annuaire de référence	Open Source	(*)Solution SIA S-SF pour le théâtre	R / S(*)	S-SF SIA FrOps

3.3.4.2 Annuaires techniques de ressources

Document	Date	Origine	Type doc	Portée
Directive technique sur la gestion des comptes dans un annuaire et application à un Active Directory V1.0	28 juin 2012	DGSIC	Directive	MinArm
<i>Commentaire : directive relative aux règles de sécurité à observer dans la gestion des comptes Active Directory</i>				
Points de contrôle Active Directory du 02 juin 2020 : "CERTFR-2020-DUR-001" https://www.cert.ssi.gouv.fr/dur/CERTFR-2020-DUR-001/	16/11/2022	CERT	Note technique	Toute admin.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Annuaire technique	Active Directory	Microsoft		R / S	Tout intranet
Annuaire technique	OpenLDAP		Attention, cette solution n'est plus portée par les distributions RedHat et AlmaLinux.	R / S	Tout intranet

3.3.4.3 Outils de « provisioning » d'annuaires

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Provisionning Annuaire	MEIBO	ILEX	SIA S-SF métropole	A / S	S-SF SIA FrOps
Provisionning Annuaire	SI INA, solution ministérielle de gestion des identités numériques basée sur le produit USERCUBE	MinArm	Cette solution est en cours de réalisation et doit permettre de constituer le RIN et les RIAXXX d'intranets.	R / E	Intradef
Provisionning Annuaire	USERCUBE	USERCUBE	Assujetti dans le cadre d'autres contexte d'emploi que SI INA *pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	MinArm

3.3.5 Utilitaires d'infrastructure

3.3.5.1 Serveurs d'impression – numérisation [IMP]

Cf. 3.1.3.3 Impression – édition multifonction [SU-IMP]

3.3.5.2 Diffusion audio-video [DAV]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Streaming Video	Deftube	MinArm	Solution ministérielle construite autour des produits Ubicast	R / E	Intradef
<i>Commentaire : Par défaut, seule l'instance Deftube est autorisée pour publier sur l'intradef des supports vidéo.</i>					

3.3.6 Services communs réseau

3.3.6.1 Nommage DNS⁴¹[NOM]

Nommage sur l'Internet : la DIRISI exploite pour les besoins ministériels sur Internet deux domaines DNS : « intradef.gouv.fr » et « defense.gouv.fr ». La gestion des sous-domaines se fait au travers du marché ASTEL-I. À noter que les adresses professionnelles sur Internet sont en def.gouv.fr et gérées au travers d'un lot du marché ASTEL-I.

Document	Date	Origine	Type doc	Portée
Compte-rendu de la quarantième réunion du sous-comité « emploi et besoins » du comité directeur des intranets diffusées par note sous double timbre : n°D-18-002794/ARM/EMA/CPI/AUT/NP	1er juin 2018	SC1	Compte-Rendu	
n°0001D18015707/ARM/SGA/ADJ/NP	14 juin 2018	EMA SGA		
<i>Commentaire : cette note permet de faire le point sur le marché MIM3 Lot 3 concernant les boîtes aux lettres Internet professionnelles</i>				
Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine v1.3	10 novembre 2017	ANSSI	Note technique	Toute administration

Nommage sur l'Intradef : La mise en place de l'Intradef modernisé a conduit à la création d'un nouveau domaine « intradef.gouv.fr » autorisé par le SIG (Service d'Information du Gouvernement) en 2009. L'ancien domaine « defense.gouv.fr » perdure pour des cadres d'emploi spécifiques

Document	Date	Origine	Type doc	Portée
Guide EMO.GUI.R4.016 « Nommage DNS » V1.0	01/09/2022	DIRISI	Guide	Intradef S-SF SIA FrOps
<i>Commentaire : Ce guide abroge et remplace la directive DIRISI n°31 relative au nommage des DNS Intradef du 8/07/2016.</i>				
Directive DIRISI n°101 d'exploitation du DNS (Intradef) v1.0 diffusée par note n°923571/DEF/DIRISI/SCOE/EXP/NP du 12 juillet 2013	12 juillet 2013	DIRISI	Directive	Intradef
<i>Commentaire : cette directive présente l'architecture technique globale du service DNS ainsi que les éléments relatifs à l'exploitation des services du DNS de l'Intradef. Cette directive ne traite que de l'exploitation du DNS dans l'espace de confiance (Intradef modernisé) tant dans le domaine « intradef.gouv.fr » que « defense.gouv.fr ». Elle ne traite pas de l'exploitation des chaînes DNS historiques des organismes, ni des organismes hors de l'espace de confiance.</i>				

⁴¹ DNS : Domain Name System

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
DNS	Windows Server (service DNS)	Microsoft	Dans le cadre de STC-IA, utilisé pour la résolution des adresses de ressources référencées dans Active Directory.	R / S	Tout Intranet
DNS	Bind	ISC	Pour la résolution des adresses des composants hors STC-IA.	R / S	Tout Intranet

3.3.6.2 Synchronisation horaire [SYN]

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°24 portant sur le service de synchronisation horaire au standard IP publiée au Bulletin Officiel des Armées	09 mars 2012	DGSIC	Directive	MinArm
<i>Commentaire : Règles d'usage et de mise en œuvre de la synchronisation horaire des réseaux IP de la défense. Périmètre : tous les intranets.</i>				

Pour les directions d'application : les applications doivent se synchroniser sur l'architecture de synchronisation horaire ministérielle mise en place par la DIRISI (pour l'Intradef, cf. la directive supra).

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Synchro Horaire	NTP client & serveur Meinberg	Meinberg	Sur les configurations projetables.	A / N	Intradef S-SF SIA FrOps
<i>Commentaire : mise en œuvre dans le cadre de STC-IA et sur certains réseaux isolés</i>					
Synchro Horaire	Ntpd/Chronyd	Natif	Sur les OS Linux	R / S	MinArm

3.3.6.3 Adressage - DHCP [ADR]

Cf §4.6.1.5

3.3.6.4 Marquage des flux réseaux [MQR]

Cf. 5.2.1.3

3.3.6.5 Transfert fichiers volumineux [TFV]

Le service utilisateur associé est décrit au §3.1.4.2 Transfert de données volumineuses [SU-TFV].

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Transfert de données volumineuses	Defense Drive	MinArm	Solution DIRISI sur la base du produit OODRIVE	R / S	Intradef
Transfert de données volumineuses (serveur)	Skype	MinArm	<i>Assujetti à l'usage de la messagerie instantanée</i>	A / S	Intradef

Transfert données volumineuses	Pydio	Pydio	Solution de partage de fichiers en web.	R / S	Internet
Transfert données volumineuses	MERLIN	MinArm	Arrêt du service au 1 ^{er} mars 2024	I / N	Internet Intradef
Transfert données volumineuses	France Transfert	Dinum	Echanges Internet-Internet de fichiers NP uniquement entre individus	R / N	Internet

3.3.6.6 Autres [MFI]

Sans objet.

3.3.7 Systèmes d'exploitation [OS]

Cf. §5.1.1 Système d'exploitation [OS]

3.4 Services de sécurité

Cf. §4.6 Services de sécurité

3.5 Services d'administration et de gestion

Cf. §6.2 Opérations – processus

4 SECURITE

4.1 Documents de référence

4.1.1 Document généraux

4.1.1.1 Politiques de sécurité des systèmes d'information

Document	Date	Origine	Type doc	Portée
Circulaire n°6095/SG relative à l'organisation gouvernementale pour la gestion des crises majeures	01/07/2019	PM	Circulaire	Toute admin.
Circulaire n° 6290/SG relative aux actions à engager pour renforcer la cybersécurité de l'État.	15/07/2021	PM	Circulaire	Toute admin.
Décret n°2022-513 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics	08/04/2022	PM	Décret	Toute admin.
Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle no 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics	26/10/2022	PM	Arrêté	Toute admin.
Politique de sécurité des systèmes d'information du ministère de l'État (PSSIE) diffusée par circulaire du premier ministre n°5725/SG du 17 juillet 2014	17 juillet 2014	PM	Circulaire	Toute admin.
Politique de sécurité des systèmes d'information du ministère de la défense [PSSIM] : instruction ministérielle n°7326/DEF/CAB du 25 juin 2018	25 juin 2018	DEF/CAB	IM	MinArm Tutelles
<i>Commentaires : La PSSIM prend en compte la PSSI de l'État. Ce document fixe les orientations stratégiques de la SSI, et définit les règles techniques et opérationnelles de SSI à respecter en les renvoyant éventuellement à des instructions et directives techniques correspondantes. Elle est complétée d'un volet technique (cf. ci-dessous) dont des mises à jour sont actuellement en préparation.</i>				
<i>Par ailleurs, la nouvelle politique ministérielle de sécurité numérique est actuellement en cours de rédaction. Elle sera composée de trois volets : stratégique, organisationnel et technique.</i>				
Volet technique de la politique de sécurité des systèmes d'information [PSSIM-T] : instruction ministérielle n°7326-2/DEF/CAB Edition 2 diffusée par note n°2475 du cabinet le 21 juillet 2021	21 juillet 2021	DEF/CAB	IM	MinArm Tutelles
<i>Commentaire : ce document définit un socle de mesures répondant aux orientations stratégiques de la PSSI ministérielle. Il tient compte notamment de la PSSIE, de l'IGI1300 et de II901.</i>				
Politique de sécurité du système d'information des opérations – FrOpS v1.0, diffusée par lettre D-14-006866/DEF/EMA/CPI/SSI/ DR-SF du 11 juillet 2014	11 juillet 2014	EMA	Politique SSI	Armées-OIA
Politique de sécurité système de l'intranet sensible de défense (PSS Intradef)	Septembre 2009	DGSIC	Note	OIA - EMA
<i>Commentaire : Cette politique de sécurité a pour objet de fixer les règles générales de sécurité qui régissent la façon dont les informations et les services de l'Intradef sont gérés.</i>				
Politique de sécurité de l'information de l'autorité qualifiée SGA version 2 diffusée par note n°10116023516 /DEF/SGA du 24 octobre 2016	24 octobre 2016	SGA	Note	SGA
<i>Commentaire : ce document est applicable à tous les organismes relevant du SGA. Ce document a vocation à être transposé en une (ou plusieurs) directive d'application de la PSSIM et de son volet technique (lorsqu'il sera mis à jour).</i>				

4.1.1.2 OIV/OSE

4.1.1.2.1 Opérateur d'importance vitale

Document	Date	Origine	Type doc	Portée
Arrêté du premier ministre du 2 juillet 2018 portant approbation de la directive nationale de sécurité applicable aux activités militaires de l'État (DNS AME)	02/07/2018	MINARM	Arrêté	AME
Arrêté du 22 mars 2021 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité, relatives au sous-secteur d'activités d'importance vitale « Activités militaires de l'État ».	22/03/2021	PM	arrêté	AME
Arrêté du 8 septembre 2017 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Activités industrielles de l'armement	08/09/2017	PM	arrêté	ID
Vigipirate – Objectifs de cybersécurité	27/02/2014	ANSSI	Guide	Tout

4.1.1.2.2 Opérateur de services essentiels

Document	Date	Origine	Type doc	Portée
Décret 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des OSE et des fournisseurs de service numériques	23/05/2018	PM	Décret	Toute admin
Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n°2018-384 du 23 mai 2018	14/09/2018	PM	Arrêté	Toute admin

4.1.1.3 Droits et obligations des usagers et des administrateurs

Document	Date	Origine	Type doc	Portée
Instruction n°2003/DEF/DGSIC portant code de bon usage des systèmes d'information et de communication du ministère de la Défense.	20 novembre 2008	DGSIC	Instruction	MinArm
Instruction n°2004/DEF/DGSIC relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la Défense	14 décembre 2009	DGSIC	Instruction	MinArm

4.1.1.4 Protection du secret

Document	Date	Origine	Type doc	Portée
Instruction générale interministérielle n°1300 portant sur la protection du secret de la défense nationale	09 août 2021	ARM/CAB	Arrêté	Toutes administrations
<i>Commentaire : Cette nouvelle IGI 1300 remplace l'IGI1300 du 13 novembre 2020.</i>				
Instruction ministérielle 900/ARM/CAB portant sur la protection du secret et des informations diffusion restreinte et sensibles	15 mars 2021	ARM/CAB	Instruction	MinArm
<i>Commentaire : Une nouvelle version est à la publication.</i>				

Document	Date	Origine	Type doc	Portée
Note n°508/DEF/EMA/PAC/NP relative à la politique des armées en matière de sensibilité des informations opérationnelles <i>(Cf. 2.3 Le cadre ministériel)</i>	9 juin 2009	EMA	Note	Armées
Circulaire n°3415 du 7 novembre 2012 de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation	7 novembre 2012	PM	Circulaire	Toutes administrations

4.1.1.5 Protection des données à caractère personnel (RGPD, CNIL ...)

Différents fichiers informatiques sont soumis au régime juridique de protection des données à caractère personnel. Ces données sont celles qui concernent les personnes physiques et celles qui permettent de l'identifier directement ou indirectement (informations nominatives, images, voix notamment).

La plupart de ces références se trouvent aussi sur le portail de la DAJ.

Document	Date	Origine	Type doc	Portée
RGPD : règlement général sur la protection de la donnée : Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (cf.2.1.2 Européen)	27 avril 2016 (application à compter du 25 mai 2018)	Union Européenne	Règlement	Union européenne
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	6 janvier 1978	Ministères	Loi	Toutes administrations
Dispositions relatives à l'agrément « hébergement des données de santé » : - article L. 1111-8 du code de la santé publique ; - articles R. 1111-8-8 et suivants du code de la santé publique.		MSS	Loi et décret	Toute administration
Décret n°2019-536 du 29 mai 2019 en application de la loi Informatique et Libertés Décret n°2007-914 du 15 mai 2007 en application de la loi Informatique et Libertés Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification	29 mai 2019 15 mai 2007 19 avril 2019	PM	Décrets	Toutes administrations
<i>Commentaire : Le 2ème décret liste les traitements automatisés de données à caractère personnel intéressant la sûreté de l'État, la défense ou la sécurité publique. Le 1er explicite l'ensemble du dispositif CNIL et les procédures afférentes en déclinaison du RGPD. Le 3eme décret apporte des précisions concernant les conditions spécifiques de traitement du numéro d'identification au RNIPP (répertoire national d'identification des personnes physiques) ou numéro de sécurité sociale et notamment les catégories de responsables de traitement et les finalités des traitements qui sont autorisés à l'utiliser par principe, les acteurs qui ne sont pas dans cette liste ne peuvent pas l'utiliser.</i>				
Note n°20236 ARM/CAB relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère des armées	18 juillet 2018	MinArm/	Note	
Décret n°2018-932 du 29 octobre 2018 modifiant les dispositions du code de la défense relatives à la sécurité des traitements de données à caractère personnel comportant la mention de la qualité de militaire	29 octobre 2018	MinArm	Décret	Toutes administrations
<i>Ce texte entré en vigueur le 1er avril 2019, porte modification du code de la défense, et décline des dispositions du RGPD pour les traitements de données à caractère personnel dont la finalité exige, outre les données d'identification, la collecte d'au moins une donnée révélant, à sa seule lecture, la qualité de militaire.</i>				

Document	Date	Origine	Type doc	Portée
Arrêté du 7 avril 2011 relatif au respect de l'anonymat de militaires et de personnels civils du ministère de la défense <i>Commentaire : Cet arrêté précise la liste des services ou unités dont les missions exigent le respect de l'anonymat des militaires et civils qui y sont affectés.</i>	7 avril 2011		Arrêté	MinArm
Arrêté du 26 juillet 2013, portant création, par le ministère de la défense, d'un traitement automatisé de données à caractère personnel relatif à la gestion des traces générées par l'utilisation des moyens informatiques. <i>Commentaire : Il s'agit d'un arrêté « générique » actualisant la déclaration CNIL sur l'intranet défense et s'appliquant à l'ensemble du ministère pour la gestion des traces en déclinaison de la directive DGSIC n°29 précitée et la mise en place des outils de surveillance de ses réseaux. Il permet également de couvrir les activités de lutte informatique défensive. L'arrêté identifie le type de données à caractère personnel susceptibles d'être conservées, et les catégories de personnel susceptibles d'y accéder dans le cadre de leur mission. Les devoirs de ces personnels sont rappelés dans l'instruction ministérielle n°2004 (cf.4.1.1.3 Droits et obligations des usagers et des administrateurs).</i>	26 juillet 2013	MinArm	Arrêté	Tout intranet

4.1.2 Références pour le non classifié (NP-DR-sensible) et le NR

Document	Date	Origine	Type doc	Portée
Instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles	11 février 2015	ANSSI	Instruction	Toutes administrations
<i>Commentaire : cette instruction ministérielle complète l'IGI 1300 et la PSSIE en instaurant des règles relatives à la protection des systèmes d'information sensibles ou diffusion restreinte. Elle doit être rendue applicable dans les contrats d'externalisation.</i>				
Document AC/35-D/1034 relatif à la protection des informations NATO RESTRICTED : document diffusé le 25 mai 2005.	25 mai 2005	OTAN	Document international	Toutes administrations
<i>Commentaire : Ce document décrit les éléments de politique de sécurité, les orientations et exigences à appliquer aux informations « NATO RESTRICTED »</i>				

4.1.3 Références pour le niveau Secret (ex CD)

Document	Date	Origine	Type doc	Portée
Guide n°972/SCSSI/SI relatif à la protection des supports classifiés de défense.	9 avril 1998	PM	Guide	Toutes administrations
<i>Commentaire : Ce document traite de la protection, manipulation et destruction des supports d'information tels que disques durs, clé USB, carte à puce,</i>				
Guide technique 972-1 pour la confidentialité des informations enregistrées sur disque dur à recycler ou exporter sous timbre n°972-1/SGDN/DCSSI du 17 juillet 2003	17 juillet 2003	PM	Guide	Toutes administrations
<i>Commentaire : Ce guide précise le guide 972 dans son chapitre 8 relatif à l'effacement d'un support pour recyclage interne. Il s'applique aux supports magnétiques d'informations classifiées de défense ou d'informations sensibles non classifiées de défense.</i>				

4.1.4 Référence pour le SO

Document	Date	Origine	Type doc	Portée
Instruction générale interministérielle n°2100/SGDSN/SSD portant sur l'application en France du système de sécurité de l'Organisation du Traité de l'Atlantique Nord.	1 ^{er} décembre 1975	PM	Instruction	Toutes administrations
<i>Commentaire : texte en cours de révision</i>				
Document AC35-D1002-REV5 Liste des équivalents nationaux des classifications de sécurité OTAN : document diffusé le 6 octobre 2010	6 octobre 2010	OTAN	Document international	Toutes administrations
Accord entre l'Union Européenne et l'Organisation du Traité de l'Atlantique Nord sur la sécurité des informations du 14 mars publié au JOUE du 27 mars 2003	14 mars 2003	UE-OTAN	Accord international	Toutes administrations

4.1.5 Références pour le SUE

Document	Date	Origine	Type doc	Portée
Instruction générale interministérielle n°2102/SGDSN/PSE/PSD portant sur la protection en France des informations classifiées de l'union européenne.	12 juillet 2013	PM	Instruction	Toutes administrations
Accord relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne publié au journal officiel de l'union européenne du 8 juillet 2011	4 mai 2011	UE	Accord	Toutes administrations
<i>Commentaire : Aux termes de cet accord, les États membres prennent toutes les mesures appropriées pour que le niveau de protection accordé aux informations classifiées de l'UE soit équivalent à celui qui est accordé par la décision 2011/292/UE du Conseil de l'UE</i>				

4.1.6 Références pour la protection des informations avec les Nations Unies

Il n'existe pas d'accord de sécurité avec les Nations Unies pour la protection des données classifiées. L'échange de données classifiées n'est donc en théorie pas possible.

D'un point de vue pratique, en l'absence d'accord de sécurité, il est difficile de définir des équivalences de classification. Si un traitant doit utiliser ou transmettre des informations sensibles de l'ONU, il lui appartient de déterminer le niveau de protection à accorder aux informations, en fonction de leur nature.

Il pourra également se référer aux instructions relatives à la sensibilité, à la classification et à la gestion des informations de la section des archives de l'ONU, pour la protection des données classifiées de l'ONU.

Document	Date	Origine	Type doc	Portée
Boîte à outils consacrée à la gestion de l'information confidentielle	26 avril 2010	SARM – DM (ONU)	/	Toutes administrations
<i>Commentaire : Document édité et réalisé par la Section des Archives et du Records Management (arms@un.org) et l'unité de gestion de l'information relative au maintien de la paix (peacekeepingimu@un.org).</i>				
<i>Remarque : la même version en langue anglaise intitulée Information Sensitivity Toolkit éditée le 24 février 2010 est également disponible.</i>				

4.1.7 Accès à la documentation technique

Les réglementations techniques internationales (OTAN, UE) sont soumises à des traités et des accords de sécurité particuliers.

Pour faciliter la diffusion des documents correspondants, une communauté d'intérêt a été ouverte sur l'Intraced S-SF pour accéder, dans le respect du droit d'en connaître à la réglementation relative aux niveaux classifiés jusqu'aux niveaux Secret, que ce soit dans le domaine souverain, OTAN ou UE.

4.2 Démarche de sécurité

Document	Date	Origine	Type doc	Portée
Guide des clauses de sécurité des systèmes d'information types à intégrer dans les marchés publics , diffusé par lettre n°DAE-2019-10-11495 du 13 novembre 2019	Juillet 2019	DAE - ANSSI	Guide	Toutes administrations
Guide d'achat de produits de sécurité et de services de confiance conformément à la politique de sécurité des SI du ministère de la défense , diffusé par lettre n° 732/DEF/DGSIC/FSSI/NP du 17 novembre 2014	17 novembre 2014	DGSIC	Guide	MinArm
<i>Commentaire : la PSSI ministérielle en déclinaison de la PSSI de l'État fait obligation à l'autorité d'homologation de la sécurité d'un système d'information d'identifier les produits et services qui doivent être de confiance. Ce guide expliquer les modes de mise en application de ces dispositions.</i>				
Guide DGSIC n°14 sur la typologie des attaques informatiques et les contre-mesures possibles , diffusé par lettre n° 113/ARM/DGSIC/DG/NP du 7 mars 2018	7 mars 2018	DGSIC	Guide	MinArm
<i>Commentaire : Ce guide a pour objectif d'aider un responsable de la sécurité des systèmes d'information (RSSI) ou un responsable de conduite de projet (RCP) à mieux comprendre les menaces qui pèsent sur leur SI, en présentant les différentes méthodes d'attaques génériques qui viennent ponctuer l'actualité du numérique et en explicitant les liens avec les menaces types de la méthode d'analyse de risques du ministère.</i>				
Directive DGSIC n°40 portant sur le développement des applications informatiques et des logiciels robustes du ministère de la Défense [DIR DEV.SEC] diffusée par note n° 195/DEF/DGSIC/DG/NP du 17 mai 2017	17 mai 2017	DGSIC	Directive	MinArm
<i>Commentaire : Il s'agit d'un ensemble d'exigences et de règles permettant de réaliser au profit du ministère des armées des développements d'applications informatiques ou des logiciels robustes capables de fonctionner correctement en présence d'événements inattendus. Cette directive ne se substitue pas aux normes qualité déjà existantes mais les complètent. Elle adresse toutes les phases d'élaboration d'un logiciel : spécification, conception, développement, tests, intégration, et déploiement.</i>				
Guide ministériel de bonnes pratiques contractuelles afférentes au droit du numérique v2	Janvier 2023	DGNUM	guide	MinArm, acheteurs
<i>Commentaire : Le guide constitue une aide de référence pour les acteurs de l'achat, tant pour les acheteurs que les conseillers juridiques. Il ne se substituera toutefois pas aux guides de bonnes pratiques adoptés par la voie réglementaire. Il traite notamment de la propriété intellectuelle, la protection des données (à caractère personnel et non personnelles).</i>				

4.2.1 Homologation

4.2.1.1 Généralités

L'autorité nationale de sécurité en matière de systèmes internationaux est le secrétariat général de la défense et de la sécurité nationale (SGDSN). Le SGDSN assure, en application des accords internationaux, la sécurité des informations classifiées confiées à la France (article 10 de l'IGI 1300). Les homologations de sécurité des systèmes d'information correspondantes relèvent ainsi de sa responsabilité et sont instruites par l'Agence nationale des systèmes d'information (ANSSI). Toutefois, pour permettre au ministère des armées un

fonctionnement amélioré, le SGDSN a délégué au CEMA un pouvoir d'homologation pour certains systèmes traitant des informations. Fondamentalement même si le formalisme et les réglementations à appliquer diffèrent, le principe reste toutefois le même, à savoir qu'une autorité responsable (SAA pour Security Accreditation Authority) atteste formellement que le niveau de sécurité requis pour le système d'information est atteint.

Le SGDSN, en tant qu'ANS⁴², émet les instructions générales interministérielles relatives à la mise en application des dispositions des différents organismes internationaux. En matière de hiérarchie des normes, un traité international a valeur supérieure à la législation nationale.

4.2.1.2 Principes

La démarche d'homologation est une composante de la gestion de la sécurité réalisée tout au long du cycle de vie d'un système d'information. **Tout système doit être homologué.**

L'homologation est une des responsabilités de l'Autorité Qualifiée en SSI (AQSSI). Une AQ peut déléguer le suivi de la démarche ou les décisions d'homologation à une ou plusieurs Autorités d'Homologations (AH). La décision d'homologation de sécurité est l'acte formel par lequel l'AH certifie, après évaluation des risques et analyse des mesures de sécurité mises en œuvre, que la protection des informations du système est assurée au niveau requis. Elle est un préalable à l'autorisation d'exploitation.

4.2.1.3 Homologation nationale

Tout système d'information ne présente pas les mêmes enjeux de sécurité en matière de confidentialité des données, d'intégrité, de disponibilité et de criticité pour les missions du ministère. De plus, de nombreux SI ou applications sont hébergés sur les Intranets du ministère bénéficiant, par héritage, des services de sécurité apportés par ces réseaux.

Dans ces conditions, la DGNUM a développé, en complément de la démarche d'homologation standard, deux méthodes d'homologation qui permettent d'alléger le processus d'homologation : la démarche sommaire d'homologation et la démarche d'homologation simplifiée.

Document	Date	Origine	Type doc	Portée
Décision du 22 décembre 2010 n°15979/DEF/CAB/CM14 relative à la désignation des autorités qualifiées du ministère de la Défense et des anciens combattants	22 décembre 2010	EMA	Note	Armées
<i>Commentaire : directive relative à toute homologation de tout système d'information relevant du MinArm.</i>				
Directive DGNUM n°27 portant sur l'homologation des systèmes d'information du ministère des Armées, 3ème édition diffusée par note n°DEP-00337/2022/ARM/DPID/NP du 7 juin 2022	07 juin 2022	DPID	Directive	MinArm
<i>Commentaire : Cette directive définit la politique à mettre en œuvre en matière d'homologation de sécurité pour les systèmes d'information (SI) au sein du ministère des armées. Elle fournit les critères de décision pour mener à terme toute démarche d'homologation, permettant ainsi d'identifier, d'atteindre, puis de maintenir un niveau de risque acceptable, tant du point de vue de la sécurité que des coûts. Elle concerne tous les systèmes d'information du ministère, quel que soit le niveau de sensibilité des informations traitées.</i>				
<i>La présente édition n°3 permet d'optimiser la documentation attendue et étend les cas d'usage présentés pour faciliter l'appropriation du dispositif d'homologation 2022.</i>				

⁴² ANS : Agence Nationale de Sécurité

Document	Date	Origine	Type doc	Portée
Guide ministériel n°6 Ed.2 relatif aux données de caractérisation d'un système d'information diffusé par note n°372/DEF/DGSIC/SDSSI du 4 avril 2013	2 avril 2013	DGSIC	Guide	MinArm
<i>Commentaire : Ce guide fixe le cadre sémantique et documente la liste des valeurs permises pour les données chargées de caractériser un système d'information. Ce guide s'adresse principalement aux différentes directions de projet faisant appel à ces différents types de données.</i>				
Guide ministériel n°7 relative à l'intégration de la sécurité des systèmes d'information dans les projets de systèmes d'information, Ed-4. Diffusé par note 355/ARM/DGNUM/SDSN/NP accessible sur Synoptic	30 septembre 2022	DGNUM	Guide	MinArm
<i>Commentaire : Ce guide fournit aux RSSI, aux équipes de projets et aux centres d'experts des autorités d'homologation les éléments nécessaires à l'intégration de la sécurité numérique dans la vie des systèmes d'information, du stade d'initialisation, jusqu'au stade d'utilisation, puis de retrait de service. Cette 3ème édition se présente sous forme d'un recueil de fiches évolutives, propose des modèles de livrables et des outils, ainsi que de liens vers des référentiels utiles. Remarque : le présent guide ne concerne pas les opérations d'armement, les systèmes industriels ou les SI relevant de l'OTAN ou de l'UE. Cependant, les responsables de programmes d'armement peuvent s'y référer. La DGA dispose de son propre guide (Guide S-CAT n° 15 002)</i>				
Guide S-CAT n°15002 : Démarche de prise en compte de la sécurité dans les programmes, guide pour les experts.	1er octobre 2007	DGA/DET/ CELAR/SSI	Guide	DGA
<i>Commentaire : Ce guide présente la démarche de prise en compte de la sécurité des systèmes d'information (SSI), pour les projets et programmes d'armement relatifs aux systèmes d'information (des forces ou de la DGA) ou aux systèmes d'armes traitant ou non des données classifiées de défense et qui feront l'objet d'une homologation par une autorité qualifiée.</i>				
Questionnaire d'évaluation initiale (QEI)	1er décembre 2021	DGNUM	Formulaire Excel	MinArm
<i>Commentaire : Ce questionnaire, actualisé en 2021, constitue la toute première étape d'analyse de risque SSI recommandée par la directive ministérielle relative aux homologations. Par le biais d'une auto-évaluation, il offre un moyen simple de déterminer rapidement si un SI présente des enjeux de sécurité importants ou non. Cette auto-évaluation prend la forme de 15 questions attendant une réponse graduée de 0 à 3. La méthode de calcul proposée, quoique simple, applique les principes de la méthode d'analyse de risque EBIOS. Les 15 questions proposées couvrent globalement tous les aspects d'une analyse de risque EBIOS à savoir :</i>				
1/ Les besoins de sécurité ; 2/ Les impacts potentiels ; 3/ l'importance des menaces potentielles ; 4/ L'importance des vulnérabilités				
Instruction D-MAN n°119 relative à l'homologation des systèmes d'information traitant des informations classifiées ou sensibles	31 mars 2011	DGA	Directive	DGA
<i>Commentaire : L'objet de la présente instruction est :</i>				
<ul style="list-style-type: none"> - de définir l'organisation mise en œuvre au sein de la Direction générale de l'armement (DGA), de préciser les principes et règles qui s'imposent pour procéder à l'homologation (autorisant la mise en exploitation) des systèmes d'information traitant des informations classifiées ou sensibles ; - d'organiser le contrôle des conditions d'exploitation des systèmes ainsi que le suivi des actions correctrices en découlant. 				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Pilotage des risques.	MAITRISK Solution ministérielle de conduite des analyses de risques basée sur la suite EGERIE Risk Manager	MinArm		R / S(*)	MinArm

4.2.1.4 Homologation interalliée

Document	Date	Origine	Type doc	Portée
AC35-D2004 (NSC)/ AC322-0052 (C3B) Rev 3 diffusée conjointement par le Nato Security Committee et le C3Board le 15 novembre 2013	15 nov. 2013	OTAN	Directive	Toutes administrations
<i>Commentaire : directive principale sur l'INFOSEC [Nato Unclassified]</i>				
AC/35-D/1021-REV3 - Lignes directrices pour l'homologation de sécurité des systèmes d'information et de communication (SIC) : document diffusé le 31 janvier 2012	31 janvier 2012	OTAN	Guidelines	Tout SIC traitant d'infos. OTAN.
<i>Commentaire : ce document donne les orientations sur les modalités requises et les processus mis en œuvre pour remplir la fonction d'homologation de sécurité des SIC traitant d'informations OTAN classifiées ou non. [Nato Non classifié]</i>				
AC35-D1014-REV3 – Lignes directrices concernant la structure et le contenu de la procédure d'exploitation et de sécurité (SecOPS) des systèmes d'information et de communication : document diffusé le 31 janvier 2012	31 janvier 2012	OTAN	Guidelines	Toutes administrations
<i>Commentaire : ce document précise la structure et le contenu attendu d'une SecOPS et les attendus pour les catégories d'agents et de personnes concernés par l'utilisation des SIC (utilisateurs sur réseaux locaux, utilisateurs de moyens portables, utilisation par les visiteurs, autorités d'exploitation ou responsables de la gestion de la sécurité) [Nato Non classifié]</i>				
AC/35-D/1015-REV3 - Lignes directrices pour l'établissement des énoncés des impératifs de sécurité (SRS) : document classifié NR diffusé le 31 janvier 2012	31 janvier 2012	OTAN	Guidelines	Tout SIC traitant d'infos. OTAN.
<i>Commentaire : Lignes directrices pour l'élaboration des SSRS (Security Requirement Statements), SEISRS (System-specific Electronic Information Security Requirement Statement), SISRS (System Interconnection SRS) et CSRS (Community SRS).</i>				
<i>Ce document classifié NR peut être obtenu sur le portail de l'Intraced (cf. §4.1.7 Accès à la documentation technique)</i>				
SDIP 29- REV1 Jan. 2011- Critères de conception des installations et mise en place de l'équipement de traitement de l'information classifiée : document classifié NR de janvier 2011	Janvier 2011	OTAN	Directive	Tout SIC traitant d'infos. OTAN.
<i>Commentaire : Ce document définit les politiques, responsabilités et procédures présidant à l'installation d'équipements permettant le traitement d'informations classifiées OTAN.</i>				
<i>Ce document classifié NR peut être obtenu sur le portail de l'Intraced (cf. §4.1.7 Accès à la documentation technique)</i>				

4.2.1.5 Cas particuliers des systèmes industriels (dont SCADA)

Un système industriel est un système d'informations commandant ou contrôlant automatiquement des dispositifs physiques à partir des données collectées par des capteurs. Il existe ainsi une interaction entre le monde virtuel et le monde réel.

Les systèmes industriels se sont rapprochés tardivement mais progressivement des standards du monde numérique et notamment du standard IP. Des systèmes hétérogènes ont ainsi été interconnectés dans un souci majeur de productivité, tout en cherchant à préserver la sûreté de fonctionnement mais sans attention pour la sécurité des systèmes d'information.

Davantage exposés, ces systèmes constituent désormais une cible privilégiée pour des cyber-attaquants car leurs actions peuvent avoir un impact direct sur nos intérêts vitaux (électricité, nucléaire, sanitaire, transport, ...) voire porter atteinte à l'intégrité des personnes.

Document	Date	Origine	Type doc	Portée
Directive n°39 relative à la sécurité des systèmes industriels (DIR S.INDUS)	9 juin 2023	DPIP	Directive	MinArm

Document	Date	Origine	Type doc	Portée
<i>Commentaire : Cette directive s'adresse principalement à tous les acteurs participant à la conception, la réalisation, l'exploitation des systèmes industriels, en particulier les personnes en charge des projets, les responsables d'opérations d'infrastructures mais également aux acteurs participant à leur maintien en condition de sécurité. Ces acteurs peuvent être du domaine cybersécurité ou de tous les domaines concourant à la vie des systèmes industriels.</i>				
<i>Directive révisée en cours de publication par DPID</i>				
Guide ANSSI relatif à la doctrine de détection pour les systèmes industriels	3 décembre 2020	ANSSI	Guide	Toute admin.
<i>Commentaire : Ce guide présente :</i>				
<ul style="list-style-type: none"> - les grands principes de la supervision de la sécurité d'un système numérique ; - les particularités des systèmes industriels ; - la définition des périmètres de détection ; - les principes généraux de détection ; - la définition des points de détection. 				

4.2.2 Maintien en condition de sécurité

Le maintien en condition de sécurité (MCS) a pour objectif d'établir les procédures permettant de traiter les vulnérabilités ou incidents de SSI.

4.2.3 Audits

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°15 relative à la réalisation des audits de sécurité des systèmes d'information au sein du ministère de la Défense diffusée par note n°1182/DEF/DGSIC/SDSSI du 10 novembre 2010	10 nov. 2010	DGSIC	Directive	MinArm
<i>Commentaire : Directive définissant le processus d'audit SSI au sein du ministère.</i>				
Référentiel d'exigences applicable aux prestataires d'audit de la sécurité des systèmes d'information V2.1[PASSI] (cf. 2.2.3 Les référentiels interministériels).	6 octobre 2015	ANSSI	Référentiel	Toutes administrations
<i>Commentaire : Le référentiel PASSI est constitutif du référentiel général de sécurité (RGSV2), cosigné de l'ANSSI et du SGMAP. Il est devenu applicable à la diffusion de celui-ci (1^{er} juillet 2014). Les autorités administratives doivent recourir, notamment dans leurs appels d'offres à des prestataires d'audit conformes aux exigences de ce référentiel.</i>				
Directive DGSIC n°28 portant sur l'exécution des audits SSI diffusée par lettre n°100/DEF/DGSIC/SDSSI/NP du 17 octobre 2013	17 octobre 2013	DPID	Directive	MinArm
<i>Commentaire : L'objectif de ce document est de définir les aspects techniques des audits SSI, en complément de la directive ministérielle n°15 relative à leur organisation. Elle vise à une uniformisation des processus communs aux équipes procédant à des audits. Cette directive peut également servir de cadre de référence pour contractualiser avec une société d'audit extérieure au ministère.</i>				
Directive relative à la réalisation des audits SSI par le CASSI et les organismes d'audit SSI des armées diffusée par la note n° D-16-001314/DEF/EMA/CPI/NP	Février 2016	EMA	Directive	Armées
<i>Commentaire : Cette directive aborde tous les aspects qui se rapportent aux modalités pratiques de réalisation d'un audit SSI, conformément aux directives DGSIC 15 et 28.</i>				

4.3 Cryptographie et gestion des ACSSI

Cryptographie :

Document	Date	Origine	Type doc	Portée
RGS_B_1 Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. V2.03 (cf. 2.2.3 <i>Les référentiels interministériels</i>)	21 février 2014	ANSSI	Directive	Toutes administrations
<i>Commentaire : Document constitutif du RGS V2. Les règles et recommandations contenues s'adressent à un lecteur familier des concepts cryptographiques. Les concepts de base ne sont donc pas systématiquement rappelés.</i>				
RGS_B_2 Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. V2 (cf. 2.2.3 <i>Les référentiels interministériels</i>)	8 juin 2012	ANSSI	Directive	Toutes administrations
<i>Commentaire : Document constitutif du RGS V2. L'objectif de ce document est de présenter le cycle de vie d'une clef cryptographique et les différentes architectures de gestion de clés possibles. Ce document complète le document RGS_B_1 ci-dessus</i>				

Gestion des ACSSI – ACSSI non classifiés (anciennement ASGLI) :

Document	Date	Origine	Type doc	Portée
Instruction interministérielle n°910 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI) sous timbre n°910/SGDSN/ANSSI du 22 octobre 2013	22 octobre 2013	ANSSI	Instruction	Toutes administrations
<i>Commentaire : La directive 34 décline cette instruction sur le périmètre MINARM.</i>				
Transport des ACSSI NP-DR par conteneurs sécurisés (Note D-20-005942) sous timbre n°D-20-005942/ARM/EMA/DSA/NP du 10 novembre 2020	10 novembre 2020	EMA	Note	MinArm
Directive centrale ministérielle n°34 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI) du ministère des armées	20 juin 2023	DPID	Directive	MinArm
<i>Commentaire : cette directive définit au sein du ministère des armées les responsabilités et les règles de gestion des ACSSI, en application de l'instruction interministérielle n°910.</i>				

Cryptophonie :

Cf. 5.1.8.2 Téléphonie chiffrée : téléphonie chiffrée, télécopie chiffrante, cryptophonie

Equipements de chiffrement

Cf. 4.6.7 Équipements de chiffrement

4.4 Protection contre les signaux compromettants

Document	Date	Origine	Type doc	Portée
Instruction interministérielle n°300/SGDSN/ANSSI du 23 juin 2014 relative à la protection contre les signaux compromettants	23 juin 2014	SGDSN	Instruction	Toutes admin.
Répertoire n°490 des matériels évalués au plan de la protection contre l'émission SPC	20 juin 2016	ANSSI	Répertoire	Toutes admin.
<i>Commentaires : ce document répertorie l'ensemble des matériels ou systèmes satisfaisant aux exigences de la norme SDIP-27 niveau A (TEMPEST), B ou C (raisonnement et conduction), ou zone 1 ou 2 en rayonnement au sens du zonage TEMPEST.</i>				

4.5 Sécurisation des COTS

Document	Date	Origine	Type doc	Portée
Procédure « Certification de sécurité de premier niveau des produits des technologies de l'information » (CSPN) diffusée sous timbre n°86/ANSSI/SDE/PSS/CCN du 13 janvier 2020	13/01/2020	ANSSI	Directive	MinArm
Processus de qualification d'un produit v1.0	12/01/2017	ANSSI	Directive	Toutes administrations
Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection v3.3	13/01/2020	ANSSI	Directive	Toutes administrations
<i>Commentaire : Les présentes procédures décrivent l'ensemble du processus de certification et de qualification de sécurité d'un produit, depuis la demande officielle par un commanditaire jusqu'à l'attribution d'un certificat pour le produit évalué, ainsi que le rôle de chacun des acteurs.</i>				

La sécurisation des systèmes d'information nécessite une bonne maîtrise de la configuration des composants logiciels qui les constituent. La mise en service d'un composant logiciel basé sur les options de configuration par défaut est déconseillée. Le déploiement de composants logiciels qui n'auraient pas fait, au préalable, l'objet de la réalisation d'un guide de configuration est à analyser comme une vulnérabilité potentielle dans le cadre de la démarche d'homologation.

Guides de paramétrage liés à des produits technologiques précis :

Document	Date	Origine	Type doc	Portée
Guides de sécurité « produits »	2016	DGSIC	Guide	MinArm

Une liste des guides de sécurité disponibles qui ont été identifiés dans le cadre du chantier de production des guides de configuration est accessible sur le site des SIC du ministère (cf. lien ci-dessus)

La liste des guides accessibles sont ceux utilisés par le CASSI durant les phases d'audit.

Cette liste contient de nombreux guides de configuration relatifs à des produits référencés dans le CCT dont (liste non exhaustive) : Apache http Server, Adobe Acrobat reader, Microsoft Windows 10, Exchange Server, IIS, SQL Server, Office, Kerberos, Oracle MySQL, Oracle Database, PostgreSQL, VMWare, Éléments actifs réseau CISCO, pare-feu, Environnement GNU/Linux.

Cette liste contient également des guides relatifs à des produits qui ne sont pas référencés dans le CCT soit parce qu'ils n'entrent pas dans le cadre de la politique du ministère, soit parce qu'ils correspondent à des produits jugés obsoletes voire proscrits. **L'attention est attirée sur le fait que la présence de ces guides dans cette liste ne vaut pas approbation de ces produits.**

Guides et notes techniques (ANSSI, DGA, etc.) :

Document	Date	Origine	Type doc	Portée
Guides et notes techniques ANSSI liés à des bonnes pratiques ou des solutions technologiques https://cyber.gouv.fr/publications		ANSSI	Guides	Toute admin.

Document	Date	Origine	Type doc	Portée
<i>Commentaires : Ces guides de bonnes pratiques, notes techniques ou méthodologiques sont en général liés à des thématiques. A titre d'exemple pour les 3 dernières années :</i>				
<ul style="list-style-type: none"> - Recommandations de sécurité relatives aux déploiements de conteneur Docker (décembre 2019) - Profil de fonctionnalités et de sécurité – SAS et stations blanches (août 2020) ; - Guide des mécanismes cryptographiques (janvier 2020) ; - Guide de sélection d'algorithmes cryptographiques (mars 2021) ; - Recommandations pour la mise en oeuvre d'un site web : maîtriser les standards de sécurité côté navigateur (avril 2021) ; - Recommandations relatives à la sécurité des (systèmes d') objets connectés (août 2021) ; - Recommandations relatives à l'authentification multifacteur et aux mots de passe (octobre 2021) ; - Recommandations de sécurité pour l'architecture d'un système de journalisation (janvier 2022) ; - Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory (janvier 2022).; 				
<i>Certains guides adressent des produits plus ciblés : commutateurs industriels Hischmann et Siemens Scalance (février 2022), pare-feu Stormshield (avril 2021)...</i>				

4.6 Services de sécurité

4.6.1 Sécurisation des accès

4.6.1.1 Démarche INA : RIN – RIA-Def - MindefConnect

L'authentification a pour but de vérifier l'identité dont une personne se réclame. L'authentification est généralement précédée ou combinée avec une identification qui permet à cette personne de se faire reconnaître du système par un élément - l'identifiant - dont on l'a précédemment dotée.

Le référentiel d'identités du ministère est actuellement porté par Annudef sur Intradef mais se limite aux seules personnes ayant un accès à ce réseau. Il offre des services de pages blanches et de pages jaunes (il dispose également d'un webservice SOAP d'authentification désormais obsolète, non pérennes et par conséquent déconseillé : les projets y ayant recourt doivent planifier rapidement les travaux nécessaires pour basculer sur une authentification MindefConnect Intradef) et de webservices SOAP d'accès aux informations sur ces personnes dans le respect du besoin d'en connaître.

Le projet d'ensemble INA vise à dégager une vision homogène et construite de la problématique de gestion des identités et des accès (IAM/IAG pour Identity and Access Management/Governance) pour le ministère des armées. INA vise à :

- rationaliser et sécuriser la gestion des identités numériques, dans le respect du RGPD, par la construction d'un Référentiel d'identités numériques (**RIN**) commun étendu aux agents civils, gendarmes, réservistes, candidats, pensionnés, ayant-droits, partenaires, militaires étrangers n'ayant pas vocation à disposer d'un compte Intradef ;
- simplifier l'administration des comptes utilisateurs en réduisant la charge administrative ;
- automatiser et centraliser la gestion de ces données afin d'en garantir l'exactitude et de minimiser les délais de mise à jour ;
- pour chaque intranet, simplifier la gestion des accès par l'installation d'un dispositif de fédération des moyens d'authentification (**MinDefConnect**) et d'un Single Sign On (SSO) ;
- pour chaque intranet, disposer d'un Référentiel des Identités et Accès de l'intranet considéré, à terme Référentiel des Identités et Autorisations (RIA-xxx) permettant de gérer et maîtriser les droits d'accès

des utilisateurs aux applications, sous la forme de macro droits⁴³ selon le cycle de vie de l'identité numérique (entrée, parcours, sortie) : **RIA-Net** pour l'internet, **RIA-Def** pour l'Intradef, **RIA-Ced** pour le Secret-SF, **RIA-FrOpS** pour le SIA FrOps.

Référentiel d'identités numériques (RIN) : Base fédérée d'identités, le RIN contient un référentiel des liens entre les identités d'une personne. Cette base de données commune contient l'ensemble des attributs de type RH et organisationnel (au sens CREDO) pour tout le personnel du ministère. Le RIN contient également les identités provenant des chaînes de confiance (pour les extérieurs, les identités protégées, les ayants droits...). Enfin, ces données sont complétées avec les informations d'emploi locales renseignées par le réseau de proximité Employeur. Ce RIN dont le rôle est assuré aujourd'hui en partie par l'annuaire référent de l'intranet sensible (Annudef), est en cours de consolidation et de fiabilisation. Il sera constitué :

- des données d'identité dites « pivot » du type nom de naissance, prénom(s), sexe, date, ville et pays de naissance ;
- de données d'identité complétées par les SIRH pour les agents du ministère des armées et renseignées via une interface dédiée pour les personnes extérieures et employées au ministère des armées ;
- des attributs techniques permettant l'identification des personnes au sein du système d'information : nom de connexion unique, numéro d'employé...

Référentiel d'identités et d'autorisations de l'Intradef (RIA-Def) : Alimenté par le RIN et complété de données propres à l'Intradef, le RIA-Def doit permettre de gérer les données d'autorisations associées à ces identités dans le contexte de l'Intradef. Il provisionnera les annuaires techniques, et fournira à terme les identités et autorisations d'accès de haut niveau (macro droits) aux SI Clients par l'intermédiaire du composant MindefConnect Intradef.

MindefConnect Intradef : Service centralisé d'authentification des utilisateurs et de contrôle d'accès aux ressources. Il permet aux SI Clients de :

- déléguer l'authentification de leurs utilisateurs,
- déléguer les contrôles d'accès de leurs utilisateurs (il ne gère pas les droits applicatifs),
- disposer du support de différents mécanismes d'authentification et des protocoles OpenId Connect et, en cas d'impossibilité technique justifiée auprès de la gouvernance technique, SAMLv2.

Il permet aux utilisateurs de bénéficier d'une authentification unique (SSO).

Document	Date	Origine	Type doc	Portée
Gestion des identités numériques et des accès : architecture d'ensemble cible : note conjointe DGSIC-EMA : n°40/DEF/DGSIC/SDAU/NP du 21 janvier 2014 n°D14-000925/DEF/EMA/CPI/NP du 23 janvier 2014	23 janvier 2014	DGSIC EMA	Note	MinArm
<i>Commentaire : Cette note présente l'architecture cible à atteindre en matière d'IAM au sein du ministère des armées.</i>				
Gouvernance du domaine « référentiel des identités et annuaires » (INA) diffusée par la note conjointe DGSIC-EMA n°435 DEF/DGSIC/DG/NP du 5 août 2015	6 août 2015	DGSIC EMA	Note	MinArm
<i>Commentaire : Cette note présente la gouvernance, le périmètre et les enjeux de la problématique de la gestion des identités et des accès pour le ministère des armées.</i>				

⁴³ Les macro-droits seront calculés sur la base des modalités d'accès et de profils métiers dits « Profils Filière Métier Applicatif » (PFMA). Les droits fins (micro droits) et la gestion des profils des utilisateurs restent de la responsabilité des applications

Document	Date	Origine	Type doc	Portée
Instruction ministérielle relative à l'identité numérique et autorisations au ministère des armées	Prévue 2024	DGNUM	IM	MinArm
<i>Commentaire : cette instruction précise les concepts et définitions liées à l'identité numérique, ainsi que les principes retenus. L'organisation, les acteurs en jeu et leurs rôles dans la gestion des identités numériques au sein du ministère seront définis dans un document de politique ministérielle et une directive de gouvernance. Dès parution, cette note abrogera la note sur le document précédent de janvier 2014</i>				

4.6.1.2 Identification / Authentification des personnes [CAU]

Pour mémoire, la PSSI-A fixe un certain nombre de règles concernant l'identification et l'authentification des personnes, et notamment :

- l'accès à un système ou un réseau du ministère ne doit être possible qu'après un processus d'identification/authentification.
- chaque utilisateur doit disposer d'un identifiant unique.
- pour les SI jusqu'au niveau DR inclus, des comptes fonctionnels peuvent être autorisés par le chef d'organisme dans le cas des centres opérationnels (CO) et des postes de permanence, si des mesures organisationnelles garantissent la traçabilité des usagers :
 - une note de service décrivant ces mesures est signée par le chef du CO ou d'organisme. Les mesures peuvent aussi être intégrées dans la note d'organisation SSI de l'organisme ;
 - une main courante conserve les noms des personnes utilisant ces comptes fonctionnels ;
 - ces comptes fonctionnels sont «attachés» à la machine désignée dans la note de service. Cette règle n'est pas imposée dans le cas d'une authentification forte.

4.6.1.2.1 Authentification sur Internet

Sur Internet, le ministère a développé une capacité d'identification et d'authentification sur internet. Cette capacité qui est construite sur les composants MinDefConnect Internet et Fournisseur d'identité Intradef est obligatoire sur Heliss-NG et C1NP et offre :

- un mécanisme de réconciliation de l'identité Internet avec l'identité Intradef (impliquant le système d'information utilisant le service incluant un composant sur Intradef, la passerelle API, le fournisseur d'identité Intradef et Annudef) ;
- la possibilité d'utiliser une authentification à double facteur en ajoutant un mot de passe à usage unique (one time password ou OTP) sans connexion à un service ;
- la possibilité d'utiliser FranceConnect.

En application des critères du CCT, le SC²A ne recommande pas l'emploi des clients FreeOTP (ne bénéficiant pas de mises à jour suffisantes) et de Google Authenticator (solution GAFAM). Il préconise les alternatives suivantes pour les appareils disposant d'un système d'exploitation Android : Aegis Authenticator, FreeOTP+ (version dérivée de FreeOTP).

Ces deux solutions disposent par ailleurs de fonctionnalités d'export et d'import des données et autorise un fonctionnement en mode déconnecté (hors connexion réseau).

Le SC²A préconise les alternatives suivantes pour les appareils disposant d'un système d'exploitation iOS : Tofu Authenticator, Authenticator.

MinDefConnect Internet n'est pas destiné à gérer les droits fins des applications pour lesquelles il assure l'identification et l'authentification.

Les protocoles supportés sont OpenIdConnect (mode *confidential* seulement) à privilégier et, par défaut, et sur demande de dérogation dûment justifiée à la gouvernance technique, SAMLV2.

Document	Date	Origine	Type doc	Portée
Spécification d'interface générique MindefConnect Internet / Si clients V1.0.7	19 juillet 2022	AND	Guide	MinArm

En interministériel, a été lancée la démarche FranceConnect, premier composant de la stratégie « État Plateforme », dispositif permettant de garantir l'identité d'un usager en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée.

Cette démarche s'est scindée en plusieurs volets :

- « FranceConnect» pour les usagers d'internet : le système, en service depuis janvier 2016 et opéré par la DINUM, a vocation à être reconnu à terme par l'ensemble des services publics numériques sur Internet, dont il propose de fédérer les comptes ; MinDefConnect Internet permet aux systèmes d'informations hébergés sur Heliss NG puis C1NP de recourir à ce service ;
- « AgentConnect » pour les agents de l'Etat sur le réseau interministériel RIE et mis à disposition sur Internet. Le projet vise à déterminer les moyens d'identification et d'authentification des agents du service public, agents des ministères et des collectivités territoriales dans le cadre de l'usage d'applications entre les collectivités et les S.I. de l'État ;
- « MonComptePro» pour les entreprises et autres personnes morales.

4.6.1.2.2 Authentification sur Intradef

Sur l'Intradef, l'authentification sur le poste de travail repose en standard sur un mécanisme technique « login / mot de passe » relié au jeton d'authentification Kerberos sur Active Directory.

MinDefConnect sur Intradef est désormais le mode d'authentification imposé aux systèmes d'information. Il pourra également permettre d'utiliser le dispositif FranceConnect. Il permettra la mise en œuvre de fédérations d'identité avec d'autres ministères au travers du Réseau Ministériel d'Etat RIE.

MinDefConnect Intradef offre aux applications la gestion des accès et des éléments génériques permettant aux applications de gérer des droits mais n'est pas destiné à gérer les droits eux-mêmes des applications pour lesquelles il assure l'identification et l'authentification.

Les protocoles supportés sont OpenIdConnect à privilégier et, par défaut, et sur demande de dérogation dûment justifiée à la gouvernance technique, SAMLV2.

Pour les applications nécessitant une authentification forte est mise en place au moyen de la carte à puce CIMS⁴⁴ contenant un certificat électronique d'authentification issu de l'IGC CIMS. En revanche, l'adossement au web service d'authentification de l'Annufed ou à l'authentification directe sur l'Active Directory sont des modes d'authentification fortement déconseillés.

⁴⁴ CIMS : Carte d'Identité Multi-Services

Document	Date	Origine	Type doc	Portée
Modalités d'authentification pour l'accès aux applications par note conjointe DGSIC-EMA n°447/DEF/DGSIC/SDAU/NP du 22 juillet 2016 n°D-16-008130/DEF/EMA/CPI/NP du 26 août 2016 [abrogée]	26 août 2016	DGSIC - EMA	Note	MinArm
Spécifications d'interface générique MindefConnect IntraDef v2.6	29/01/2021	UMSNUM	Rapport	MinArm

Pour rappel, la spécification d'interface relative à MindefConnectIntradef mentionne la règle suivante :

Règle	Énoncé	Statut	Portée
CCT_R3	Il est OBLIGATOIRE que les applications utilisant le composant MinDefConnect Intradef/Internet traitent l'authentification côté serveur en implémentant l'« authorization code flow » à l'exclusion de tout autre « flow ».	O	Intradef Internet

4.6.1.2.3 Authentification sur intranets classifiés

Sur les intranets classifiés de défense, l'accès est protégé par « carte à puce et code PIN » généralement au niveau du poste, sinon au niveau du portail ; il équivaut donc à une authentification forte. La carte est aujourd'hui fournie par le projet IGCg NG.

Les mises en œuvre des **RIA-Ced** et **RIA-FrOpS** sont à l'étude (voir document de référence [« DASS des services de gestion des identités numériques et des autorisations SIA »](#)).

Document	Date	Origine	Type doc	Portée
DASS des services de gestion des identités numériques et des autorisations SIA » V0.7 du 22 novembre 2019	22 nov 2019	DGA	Rapport	S-SF SIA FrOps

4.6.1.2.4 Authentification mutualisée et SSO

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
RFC 4120	The Kerberos Network Authentication Service : standard décrivant le mécanisme d'authentification via le protocole Kerberos	R	MinArm
SAML v2	Security assertion markup language (SAML) est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Basé sur le langage XML, SAML a été développé par le consortium OASIS. SAML propose l'authentification unique (en anglais single sign-on ou SSO) sur le web permettant à un utilisateur de naviguer sur plusieurs sites différents en ne s'authentifiant qu'une seule fois, sans pour autant que ces sites aient accès à des informations trop confidentielles.	A	Toutes administrations
OpenIDConnect 2.0	OpenID Connect est une couche d'identification basée sur le protocole OAuth 2.0, qui autorise les clients à vérifier l'identité d'un utilisateur final en se basant sur l'authentification fournie par un serveur d'autorisation, suivant le processus d'obtention d'une simple information du profil de l'utilisateur final. Ce processus est basé sur un dispositif interopérable de type REST.	R	Toutes administrations
<i>Commentaire : OpenID Connect v2 et SAML v2 sont tous deux recommandés par le RGI. OpenID Connect v2 est par ailleurs le protocole retenu par la démarche FranceConnect et celui privilégié par le Ministère des Armées. Pour le ministère, ces protocoles sont adaptés à des applications partagées en interministériel aux fins de fédération d'identité : chaque organisme gère ses propres identités (fournisseur d'identité), l'accès à l'application se fait au travers d'une fédération d'identité, sphère de confiance reposant sur l'un de ces protocoles. Bien qu'aucune politique ministérielle n'ait encore été arrêtée sur ce sujet, le ministère est amené dès maintenant à mettre en œuvre chacun de ces protocoles : - SAML v2 sera utilisé pour la fédération d'identité avec la DGFIP dans le cadre du projet AGIR (Application de Gestion Interne des Risques - Contrôle interne de gestion de la DGFIP proposée au SGA)</i>			

- OpenID Connect sera utilisé pour la fédération d'identité dans le cadre du projet OASIS (partage des événements aériens au sein du MINARM)..

Document	Date	Origine	Type doc	Portée
Modalités d'authentification pour l'accès aux applications cf. §4.6.1.2.2 Authentification sur Intradef			Note	MinArm
Spécification d'interface générique MindefConnect Intradef / Si clients V2.7	21 juin 2021	UM SNUM	Guide	Intradef
Spécification d'interface générique MindefConnect Internet / Si clients V1.0.7	19 juillet 2022	AND	Guide	

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
SSO	MindefConnect Intradef v2	MinArm	Solution d'authentification sur Intradef. Cette solution de fédération d'identité prend en charge les protocoles OpenID Connect (en priorité) et SAML V2 (par défaut).	R / S	Intradef
SSO	KEYCLOAK	REDHAT	Solution open source de fédération d'identité. Lorsque des besoins spécifiques non rendus par les solutions ministérielles nécessitent une instantiation particulière. (exemple : Axone...). Ce besoin particulier doit être justifié. <i>* pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	* / *	Intradef Internet
<i>Commentaires : Vu la rapidité des évolutions sur ce logiciel et la durée de vie très courte des versions (3 mois), il peut être intéressant d'utiliser la version soumise à licence REDHAT SSO ou disposer d'un maintien en condition de sécurité adapté à ce rythme très rapide de mises à jour.</i>					
<i>Le SC²A constate une tendance de certains intégrateurs à recourir, par facilité plus que par besoin technique, à cette solution, par conséquent, en dehors d'une logique de mutualisation de la gestion des rôles et droits d'un écosystème logiciel donné, le SC²A préconisera l'intégration des ces mécanismes au sein même des projets (via potentiellement certaines librairies proposées par les frameworks de développement tels que Spring Security).</i>					
SSO	REDHAT SSO	REDHAT	Solution packagée faisant l'objet d'une offre de service de REDHAT sur la base de Keycloak	A / N	Intradef
Authentification mutualisée	WebService Annudef	DIRISI	Ce mode est interdit pour tout nouveau projet.	I / S	Intradef
<i>Commentaire : Ce mode d'authentification obligeant les utilisateurs à disposer d'un second jeu d'identifiant et de mot de passe, moins intégré et communiqué au système d'information l'utilisant ne doit désormais plus être utilisé. Il est de plus obsolète et non pérenne. L'usage des autres WebServices reste possible pour accéder à des données utilisateurs contenues dans l'Annudef</i>					
<i>l'interrogation directe de l'annuaire LDAP n'étant pas autorisée. A noter toutefois que ces webservices ont vocation à être remplacés par des API Rest à interroger depuis la PEM Intradef. Enfin, il convient de signaler qu'au moment de l'authentification, MindefConnect Intradef renvoie systématiquement un certain nombre d'informations pivot relative à l'utilisateur identifié.</i>					
SSO	Windows Server reposant sur le protocole Kerberos	Microsoft	Si MindefConnect Intradef ne peut pas être utilisé. Cela devra être justifié.	R / S	Intradef
<i>Commentaire : Pour les smartphones SMOBI (sous OS Android), Kerberos n'est pas encore pris en charge. Les serveurs doivent alors ajouter un mécanisme complémentaire, se déclenchant en cas d'échec de l'authentification automatique et demandant à l'utilisateur de saisir son identifiant et son mot de passe de session.</i>					

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
SSO	Windows Server reposant sur le protocole Kerberos	Microsoft	En cours de généralisation.	R / S	S-SF SIA FrOps
<i>Commentaire : Pour le théâtre, il s'agit de Kerberos sur Windows Server 2012/2016.</i>					
SSO	MindefConnect Internet v2 (reposant sur RedhatSSO de Redhat)	MinArm	Solution d'authentification sur Internet Cette solution de fédération d'identité prend en charge OpenID Connect, l'OTP, FranceConnect Particuliers ainsi qu'une réconciliation d'identité avec Intradef pour les ressortissants du MinArm.	R / S	Internet
<i>Commentaire : L'utilisation de cette brique s'impose désormais aux systèmes d'information hébergés sur Heliss NG ainsi que sur CINP. Ces derniers doivent, pour des raisons de sécurité et conformément à l'homologation de MinDefConnect Internet, impérativement implémenter l'authorization code flow à l'exclusion de tout autre « flow », y compris lorsque le client est une application web SPA ou une application mobile.</i>					
SSO	FranceConnect Particulier	DINUM	Dispositif préconisé par l'État (État plateforme) pour garantir l'identité d'un usager en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée.	R / -	Internet
<i>Commentaire : Certaines démarches administratives en ligne requièrent davantage qu'une authentification simple, reposant sur un identifiant et un mot de passe. La DINUM étudie donc la piste d'un « second facteur » à utiliser par les fournisseurs de services. Autrement dit un système supplémentaire de vérification reposant sur ce que possède l'usager, ce qu'il sait ou ce qu'il est. Cette authentification renforcée est nécessaire dans un cas d'usage sensible tel que la modification d'un RIB préenregistré. L'ensemble de la documentation technique concernant FranceConnect est accessible sur le site dédié : https://partenaires.franceconnect.gouv.fr/</i>					

4.6.1.3 Habillement et gestion des profils

Actuellement la sécurisation de la gestion des profils de comptes utilisateurs et des accès des utilisateurs aux services de l'Intradef se fait au travers de stratégies de groupes ou GPO (Group Policy Object) déployées dans l'annuaire Active Directory DR-CPT.

Règle	Énoncé	Statut	Portée
CCT_R4	Il est OBLIGATOIRE que les applications assurent la gestion des droits fins à leur niveau.	O	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion des profils	Gestion des GPO sur Active Directory (GPMC : Group Policy Management Console ou AGPM : Advanced Group Policy Management)	Microsoft	AGPM est lié au pack MDOP (Microsoft Desktop Optimization Pack) et n'est pas disponible depuis les sites VisualStudio ou MAC (ex VLSC) il doit faire l'objet d'une FEB.	R / S	MinArm

4.6.1.4 Supports matériels – Cartes à puces

Document	Date	Origine	Type doc	Portée
e-IDAS – electronic Identification And Signature : règlement européen <i>Cf. §2.1.2 Européen) ce texte fait actuellement l'objet d'une refonte.</i>	23 juillet 2014	Union Européenne	Règlement	UE
RGS B3 – Mécanismes d'authentification version 1.0 : annexe du référentiel général de sécurité (RGS) <i>Cf. 2.2.3 Les référentiels interministériels</i>	13 janvier 2010	ANSSI	RGS	Toutes administrations

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Carte à puce	CIMS	MinArm	<p>La carte CIMS est la carte d'identité professionnelle et militaire pour les agents du ministère. Les données apposées sur et contenues dans la puce de la carte proviennent des SI RH et de l'Annudef.</p> <p>La carte est équipée d'une puce qui offre plusieurs interfaces :</p> <ul style="list-style-type: none"> - Une interface sans contact (Mifare DESFire) utilisée notamment pour du contrôle d'accès, la restauration et l'utilisation de l'impression sécurisée - Une interface avec contact : des certificats électroniques (un d'authentification, un de signature et un de chiffrement) délivrés par l'IGC CIMS. <p>Les certificats électroniques CIMS sont utilisés par exemple pour :</p> <ul style="list-style-type: none"> - l'authentification forte auprès d'applications le nécessitant sur l'Itradef (CHORUS, SI CIMS, Source Solde, MindefConnect ...) - la signature électronique (SOSIE, SI CIMS, ...) <p>Plusieurs générations de puce sont en circulation</p> <p>Un logiciel tiers (middleware) est nécessaire pour utiliser les certificats électroniques</p>	R / S	Intradef

Les enceintes cryptographiques autonomes (Hardware Security Module – HSM) offrent des services cryptographiques à un serveur ou à un réseau complet (LAN) via TCP/IP pour effectuer la cryptographie symétrique et asymétrique. Toutes les données critiques de sécurité sont manipulées uniquement dans l'enceinte sécurisée du HSM et ne sont jamais exposées dans l'environnement non sécurisé des serveurs, pour en garantir la non-compromission. Ces outils peuvent être utilisés pour les applications critiques comme les infrastructures de gestion de clés, les serveurs d'autorité de certification, les serveurs d'horodatage, le chiffrement de la base de données. Nécessitant le recours à des API de programmation relativement complexes disponibles que dans quelques langages de programmation, il est également possible d'utiliser des outils logiciels (tel que le service de socle Gestion des secret ou le logiciel Vault de Hashicorp sur lequel il s'appuie) s'intercalant entre l'application et le HSM et proposant à la place des API Rest, simplifiant drastiquement les développements et ouvrant leur utilisation à tout langage de programmation.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion des	TrustWay Proteccio	ATOS	TrustWay Proteccio est le nouvel HSM	R / S	MinArm

clefs			à usage général de Bull. De conception et de fabrication européenne, il s'inscrit comme le successeur des HSM TrustWay Crypto PCI et TrustWay box. Produit certifié Critères Communs EAL4+. Produit qualifié niveau Renforcé par l'ANSSI en mars 2020		
-------	--	--	--	--	--

4.6.1.5 Authentification Machines [CAR]

Avant l'ouverture d'une session, les machines peuvent s'identifier via le protocole 802.1x.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°88 « Implémentation du 802.1x sur les réseaux de desserte » : version V1.0 du 27 mars 2013	27 mars 2013	DIRISI	Directive	Intradef S-SF SIA FrOps
<i>Commentaire : Cette directive décrit l'architecture et la mise en œuvre de l'infrastructure 802.1x d'authentification des équipements d'extrémité (ordinateurs, portables, téléphones, imprimantes, etc...) déployée au sein du Ministère des armées. Cette architecture permet de répondre partiellement au besoin d'itinérance et de sécurisation des services communs du STC-IA, ainsi qu'au dialogue entre l'infrastructure mise en œuvre par la DIRISI et celles mises en œuvre dans le cadre de partenariats public privé (Balard, RDIP...).</i>				
Recommandations de l'ANSSI relatives au déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux	07 août 2018	ANSSI	Guide	Administration
<i>Commentaire : Ce document détaille le fonctionnement d'un réseau à accès contrôlé, qu'il soit filaire ou sans fil et présente les recommandations de la technologie reposant sur le protocole 802.1X, ainsi que l'architecture et les composants principaux d'un tel réseau. Il détaille les fonctions de sécurité et les bonnes pratiques à appliquer pour augmenter le niveau d'un tel réseau.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
802.1x	Architecture basée sur l'infrastructure Microsoft	DIRISI	Cette infrastructure est basée sur l'infrastructure Microsoft avec : - l'architecture de certification sous PKI Windows - les groupes de sécurité dédiés à l'architecture 802.1x sous Active Directory - les services Radius déployés en configurant des serveurs NPS (Network Policy Serveur) sous Windows.	R / S	MinArm

4.6.1.6 Authentification Services [CAR]

Dans le cadre des chantiers de transformation et de sécurisation des socles non classifiés, le déploiement d'un gestionnaire de secrets accessible par API est en cours (C1NP puis C1DR).

Ce gestionnaire de secrets offre deux catégories de fonctionnalités :

- Une infrastructure de gestion de clefs automatisée avec :
 - Un service de création et de renouvellement de certificats finaux X509 HTTPS. Le gestionnaire de secrets se positionne en tant qu'Autorité de Certification Déléguée d'une ACR issue d'IGC-G-NG ;

- Un service de production de certificats de type client SSH (authentification d'un client SSH par certificat) ;
- Des fonctionnalités de stockage de secrets (mots de passe de comptes de service, jetons...) avec :
 - Un service de stockage de secrets avec gestion de versions ;
 - Un service de création et de renouvellement automatique de mots de passe de bases de données.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestionnaire de secrets	Service GDS	MinArm	Basé sur la solution Hashicorp Vault, gestion et mise à disposition d'éléments secrets via API REST et la fourniture de certificats serveur	R / S	Intradef

4.6.1.7 Relais (messagerie, services web, services utilisateurs) [Rxx]

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Relais messagerie	Postfix	Postfix.org	Dans le cadre de SIA et SIE	R / S	S-SF SIA FrOps SIE
Relais Web	Apache HTTP Server	Apache Foundation	Dans le cadre de SIA	R / S	S-SF SIA FrOps

4.6.2 Gestion des clés – certificats électroniques [IGC]

RGS

Le référentiel général de sécurité (RGS) définit un ensemble de règles de sécurité (authentification, horodatage, confidentialité, signature électronique...) qui s'imposent aux administrations et aux collectivités territoriales pour sécuriser leurs systèmes d'information. Certaines annexes du RGS concernent les IGC.

L’arrêté du 13 juin 2014 porte approbation du RGS et précise les modalités de mise en œuvre de la procédure de validation des certificats électroniques. Cet arrêté rend applicable la deuxième version du RGS au 1^{er} juillet 2014.

Document	Date	Origine	Type doc	Portée
e-IDAS – electronic Identification And Signature : règlement européen <i>Cf. §2.1.2 Européen</i> <i>Ce texte fait actuellement l'objet d'une refonte.</i>	23 juillet 2014	Union Européenne	Règlement	UE
RGS A1 – Fonctions de sécurité basées sur l’emploi de certificats électroniques version 3.0 RGS A2 – Politique de certification type « certificats électroniques de personne » version 3.0 RGS A3 – Politique de certification type « services applicatifs », version 3.0 RGS A4 – Profils de certificats, CRL, OCSP et algorithmes cryptographiques, version 3.0 RGS A5 – Politique de certification type « services applicatifs », version 3.0 <i>Cf. 2.2.3 Les référentiels interministériels (Annexes du RGS)</i>	27 février 2014	ANSSI	RGS	Toutes administrations

MINARM

Document	Date	Origine	Type doc	Portée
Politique ministérielle des IGC au MINARM diffusée par la note n°194/ARM/DGNUM/SDSN/NP	18 mai 2022	DGNUM	politique	Minarm
<i>Commentaire : ce document définit les grands principes d'utilisation des IGC au sein du ministère des armées.</i>				
Directive DGSIC n°21 edition 4 portant sur les certificats électroniques employés au sein du ministère des armées diffusée par la note n°194/ARM/DGNUM/SDSN/NP du 18/05/2022	18 mai 2022	DGNUM	Directive	MinArm
<i>Commentaire : Cette directive décrit les besoins du ministère en services de confiance, ainsi que les modalités de délivrance et le concept d'emploi des certificats électroniques. Règles pour tout niveau de confidentialité découlant du RGS (hors algorithmes gouvernementaux).</i>				
Mémento pour l'utilisation des certificats électroniques diffusé par note n°1367/DEF/DGSIC/SDSSI du 22 novembre 2012	19 nov. 2012	DGSIC		MinArm
<i>Commentaire : Ce mémento émis par la DGSIC limité volontairement à une page recto-verso décrit succinctement ce que sont les certificats électroniques, leur utilisation, les supports utilisés pour les stocker, l'organisation mise en place pour les déployer et l'apport en termes de sécurité.</i>				
Rapport technique définissant les exigences pour l'intégration de l'IGC Générique dans un système	22 février 2011	DGA MI	Rapport technique	DGA
<i>Commentaire : Ce document fournit des exigences types pour l'intégration de l'IGC Générique dans un système et l'utilisation des certificats correspondants.</i>				
Cadre de gouvernance des infrastructures de gestion de clés diffusée par note n° 194/ARM/DGNUM/SDSN/NP du 18/05/2022	18 mai 2022	DGNUM		MinArm
Organisation du PSCE IGCg-NG diffusée par note n° D-22-003046/ARM/EMA/COMCYBER/NP du 14/06/2022	14 juin 2022	COMCYBER		MinArm

L'IGC-G (IGC générique) n'est plus à l'état de l'art Cyber. Son obsolescence matérielle et logicielle ne permet plus d'apporter un soutien à la hauteur des enjeux.

L'IGCg-NG est le système, de référence, à utiliser par l'ensemble des projets.

Les services IGCg restent en production afin que les programmes dont la transition vers l'IGCg NG est difficile puissent continuer à fonctionner et restent sécurisés à minima. Son utilisation nécessite l'instruction de dérogations auprès du COMCYBER pour continuer à être utilisé au-delà du 31 mars 2024.

Contrairement à l'IGCg qui met en œuvre une instance par niveau (IGCg Intradef, IGCg IntraCed S-SF et IGCg IntraCed S), l'IGCg NG met en œuvre un unique centre de production alimentant ces mêmes Intranet via des passerelles dédiées. Le service comprend la fourniture des cartes à puces, ainsi que l'ensemble des services liés au cycle de vie des certificats (génération, renouvellement, révocation, déblocage de supports, séquestration et recouvrement de clés de confidentialité).

Sur l'Intradef, l'IGCg NG est employée pour les certificats machines. Les certificats personnes sont fournis par l'IGC CIMS, apportée dans le cadre de la délivrance de la carte CIMS (Carte d'identité Multi-Services).

Sur l'internet et pour les échanges interministériels :

- les certificats machines exposés vers l'Internet public peuvent être obtenus via le lot 3 du marché ASTEL-I géré par la DIRISI ;
- Les certificats machines utilisés en interne sur la plateforme d'hébergement C1NP seront délivrés par le service socle gestion des secrets disposant d'une autorité de certification déléguée ;
- les certificats de personne (conformes aux RGS***) sont fournis par l'IGC dite IGC CIMS, apportée dans le cadre de la délivrance de la carte CIMS (Carte d'identité Multi-Services).

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
IGC	Certificats machine Internet	Marché DIRISI ASTEL-I	Certificats machines pour Internet à acquérir via le marché ASTEL-Imis en service par la DIRISI.	R / S	Internet
<i>Commentaire : attention, la durée des certificats est imposée.</i>					
IGC	IGC CIMS	ANTS	IGC opérée par l'ANTS ⁴⁵ dans le cadre du déploiement de la carte CIMS ⁴⁶ sur l'Itradef. Les certificats sont portés par la carte à puce. Ces certificats peuvent être utilisés pour des échanges avec d'autres administrations sur Internet ou le RIE. <i>(*) Soutien assuré l'opérateur Imprimerie Nationale</i>	R / S (*)	Intradef Internet-RIE
IGC	IGCg	MinArm	IGC remplacée par IGCg NG et ne doit plus être utilisée par les projets (dérégulation déléguée au COMCYBER).	I / S	Intradef S-SF SIA FrOps
IGC	IGCg NG	MinArm	Unique service de gestion de certificats du MinArm. IGC opérée par la DIRISI permet de délivrer des certificats logiciels et sur les réseaux classifiés, des certificats sur cartes à puce.	R / S	Intradef S-SF SIA FrOps

L'étude de convergence IGC pilotée par la DGNUM (fin 2020-début 2021) a permis de poser les principes de rationalisation de l'offre IGC et de la réduction du nombre d'autorités de certification racine. En perspective, il s'agira également, lorsque cela est possible de rattacher à des autorités de certification déléguée, les nombreuses PKI techniques – souvent intégrées aux solutions éditeurs - délivrant des certificats machine nécessaires au fonctionnement de l'infrastructure. La mise en œuvre d'une PKI Technique demeure soumise à la validation du SC²A et à l'attribution d'OID spécifiques.

4.6.3 Gestion de la preuve

4.6.3.1 Horodatage [HOR]

Pas de référence identifiée à ce jour.

4.6.3.2 Signature [SGN]

Document	Date	Origine	Type doc	Portée
Cadre d'emploi de la signature électronique au ministère des Armées – Ed 2 diffusée par note n° 313/ARM/DGNUM/SDSN/NP du 8 juillet 2021	8 juillet 2021	DGNUM	Concept Emploi	MinArm

⁴⁵ Agence National des Titres Sécurisés

⁴⁶ Carte d'Identité Multi-Services

Document	Date	Origine	Type doc	Portée
<i>Commentaire : Ce document précise les aspects techniques, juridiques et organisationnels à prendre en compte pour intégrer le processus de signature électronique dans un projet. Il détaille les trois offres de signature électronique susceptibles d'adresser les besoins du ministère.</i>				

Sur l’Intradef, La solution ministérielle pour la signature électronique est SOSIE.

SOSIE offre les services suivants :

- la signature sur poste depuis un portail applicatif (navigateur) ;
- la signature cachet serveur accessible pour les SI ayant un besoin de cachet ;
- un service de vérification de signature ;
- un service d’archivage des preuves de signature (et non du document signé).

Sur les intranets classifiés de défense, la solution est un socle de signature apporté par le SIA.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Signature	SOSIE	MinArm	Solution de signature sur l’Intradef	R / S	Intradef
Signature	SSIG (socle de signature)	MinArm-SIA		R / S	S-SF SIA FrOps

4.6.4 Surveillance - Outils LID, détection d'intrusion [SUR] [DEA]

Document	Date	Origine	Type doc	Portée
D directive DGSIC n°10 sur la prévention contre les codes malveillants <i>Cf. 4.6.5.1 Antivirus – codes malveillants [ANV] [SSV]</i>	05 novembre 2009	DGSIC	Directive	MinArm
<i>Commentaire : Cette directive définit les règles du ministère des armées en matière de prévention contre les codes malveillants (PCM). Ce processus est prolongé par des processus opérationnels, dans le cadre plus général de la lutte informatique défense (LID), qui ne sont pas traités dans cette directive</i>				

4.6.5 Utilitaires de sécurité

4.6.5.1 Antivirus – codes malveillants [ANV] [SSV]

Document	Date	Origine	Type doc	Portée
D directive DGSIC n°10 sur la prévention contre les codes malveillants	5 nov. 2009	DGSIC	Directive	MinArm
<i>Commentaire : Cette directive définit les règles du ministère des armées en matière de prévention contre les codes malveillants (PCM). Elle en précise les principes, les objectifs et les moyens généraux pour y parvenir. La lutte contre les codes malveillants repose sur deux types de processus différents. La PCM est le processus amont de cette lutte, et fait l'objet de cette directive. L'effet majeur recherché de la PCM du ministère est de minimiser les impacts des codes malveillants, dans le cadre d'une analyse de risques globale des systèmes d'information. Ce processus est prolongé par des processus opérationnels, dans le cadre plus général de la lutte informatique défense (LID), qui ne sont pas traités dans cette directive</i>				
Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows <i>cf.4.5 Sécurisation des COTS</i>	06 déc. 2013	ANSSI	Note	Toute admin.

Le projet **DARMA** (Défense Antivirus et Résilience contre les codes Malveillants) doit être mis en œuvre

sur tous les réseaux. Ce projet consiste à la mise en œuvre d'un système de défense en profondeur contre les codes malveillants à partir de trois antivirus différents conformément à la PSSI-A (règle PSD 20) (*cf. § 4.1.1.1 Politiques de sécurité des systèmes d'information*).

4.6.5.2 Contrôles d'intégrité [CIN]

Pour s'assurer de l'intégrité d'un fichier ou d'une livraison, il est possible de recourir aux utilitaires Microsoft CertUtil ou Get-FileHash présents en standard sur les postes et serveurs. A l'identique, les utilitaires MD5sum et SHA1sum peuvent être utilisés sur les environnements de type Linux. Cependant pour des raisons de sécurité, l'utilitaire sha256sum sera préféré.

4.6.5.3 Chiffrement

4.6.5.3.1 Chiffrement de fichiers [CHI]

ACID⁴⁷ Cryptofiler : L'opération de chiffrement des données sensibles doit être effectuée dans un environnement de confiance soit validé pour traiter des informations du niveau visé. C'est la raison pour laquelle le logiciel ACID Cryptofiler n'est pas installé sur des postes Internet en libre-service.

Certains produits agréés, ou certains systèmes ayant reçu une homologation, peuvent disposer d'un chiffrement ACID alors qu'ils disposent d'un accès à internet filtré (ISPT, CLIP). Les mesures de protection face à la menace liée à Internet sont alors jugées suffisantes.

Document	Date	Origine	Type doc	Portée
Concept d'Emploi de Zed! diffusé par note n°170/ARM/DGNUM/DG/NP du 15 mai 2019	14 mai 2019	DGNUM	Concept d'emploi	MinArm
Procédure de transmission d'informations sensibles de niveau Confidentiel Personnel avec le logiciel ZED! diffusée par message officiel n°2020/286 du 4 juin 2020	4 juin 2020	COMCYBER	Procédure	MinArm
Recommandations pour une utilisation sécurisée de Zed! diffusée par note n°ANSSI-PG-068 du 14/11/2019 (v1.1)	14 novembre 2019	ANSSI	Note technique	Toute admin.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Chiffrement	ACID Cryptofiler	Capgemini-Abak Systèmes	Permet le chiffrement au niveau DR. Plugin pour Outlook 2016 disponible dans le Store DIRISI DR-CPT.	R / S	MinArm
<i>Commentaire : Solution agréée par l'ANSSI.</i>					
Chiffrement	ACID Eleonore	MinArm - DGA	Permet le chiffrement au niveau Secret.	D / S	MinArm
<i>Commentaire : Cette solution est désormais déconseillée (liste C ANSSI)</i>					

⁴⁷ ACID : Automate de Chiffrement des Informations de Défense

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Chiffrement	Zed! (à ne pas confondre avec « Zed! Free » qui est interdit)	Prim'X	Assujetti aux échanges à l'interministériel jusqu'au niveau DR-SF, à l'exception des échanges avec l'UE au niveau RUE où il est autorisé ainsi qu'avec les industriels qui ne disposent pas d'ACID	A / S	Toute administration
<i>Commentaire : Cette solution qualifiée au niveau standard par l'ANSSI dans sa version Q.2020.1 jusqu'au 15 septembre 2024 permet de combler un périmètre que le logiciel ACID ne peut pas couvrir. Il ne doit être utilisé qu'avec des personnes physiques ou morales, publiques ou privées, hors du ministère ou avec les industriels n'ayant pas ACID. ACID reste, par ailleurs, le seul outil de chiffrement de documents autorisé au sein du ministère dans le cadre d'échanges avec les industriels disposant du logiciel ACID.</i>					
<i>Zed ! est accessible sur le DIRISI Store.</i>					

4.6.5.3.2 Effacement sécurisé

Document	Date	Origine	Type doc	Portée
Guide technique 972-1 pour la confidentialité des informations enregistrées sur disque dur à recycler ou exporter	17 juillet 2003	SGDN		Toutes administrations
<i>Commentaire : Ce guide précise le guide 972 dans son chapitre 8 relatif à l'effacement d'un support pour recyclage interne. Il a valeur de circulaire.</i>				
Directive DIRISI n°117 relative au traitement des supports ayant contenu des informations sensibles ou classifiées sous timbre n°400757/DEF/DIRESI/SDSSI/NP du 13 février 2014	13 février 2014	DIRISI	Directive	DIRISI
Directive DIRISI n°119 relative à l'obfuscation sécurisée des données sous timbre /DEF/DIRESI/SDSSI/NP du 17 février 2014	17 février 2014	DIRISI	Directive	DIRISI

Le logiciel Blanchir, qui a été développé par DGA MI, est retiré du CCT car il n'est plus soutenu.

Ce logiciel n'était adapté que pour les disques durs de technologie classique (plateaux à revêtement ferromagnétique), hors mémoire FLASH ou clés USB. L'effacement de données par réécriture demeure une technologie peu fiable et est réservée à des cas d'emploi particulier.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Effacement de fichiers sécurisé	Fonction d'effacement sécurisé d'ACID	Capgemini-Abak Systèmes	Permet d'effacer des fichiers ou répertoires sur un poste sur lequel Acid est installé. Il ne permet pas de blanchir un disque entier. ACID ne permet pas de déclassifier le support effacé.	R / S	MinArm

Bien que des solutions d'effacement sécurisé soient recommandées dans le CCT, il est préférable d'appliquer des solutions de chiffrement de disque ou de fichier (ACID, etc.).

4.6.5.4 Pare-feux

Règle	Énoncé	Statut	Portée
CCT_R5	Par défaut, il est OBLIGATOIRE de laisser actif le pare-feu logiciel intégré aux OS et de le configurer.	O	MinArm

Document	Date	Origine	Type doc	Portée
Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu cf.4.5 Sécurisation des COTS	30 mars 2013	ANSSI	Note technique	Toutes administrations
Recommandations de sécurisation d'un pare-feu Stormshield Network Security cf.4.5 Sécurisation des COTS	02 avril 2021	ANSSI	Guide	Toutes administrations
Guide PA-044 « Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à internet »	22 janvier 2018	ANSSI	Guide	Toutes administrations

Concernant les OS Windows, il est interdit de désactiver le service associé, et ce, même en cas de recours à un pare-feu tiers, en effet, le service « pare-feu » ne gère pas que le pare-feu mais gère également tout l'aspect « hardening de service » de Windows. Aussi, dans le cas où l'on ne souhaite pas utiliser le pare-feu de Windows au profit d'un pare-feu tiers, il faut désactiver le pare-feu en tant que composant pour les différents profils (privé-public et domaine) mais ne pas désactiver le service.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Pare-feu	PALO ALTO	PALO ALTO		R / S	Intradef Internet S-SF SIA FrOps
Pare-feu applicatif Web (WAF)	Securesphere	IMPERVA	Sur Heliss-NG	R / S	Internet
Pare-feu applicatif Web (WAF)	UBIKA WAF	UBIKA	Sur C1NP	R / S	Internet

4.6.6 Supports de stockage sécurisés

GLOBULL :

L'ANSSI a publié un nouvel agrément du disque dur externe GLOBULL dans lequel elle impose une mise à jour des équipements vers la nouvelle version. Cette mise à jour nécessite un retour des équipements en station de personnalisation pour assurer le remplacement de la carte à puce, une mise à jour des logiciels de sécurité et une personnalisation des équipements.

La parution de cet agrément implique donc que les équipements actuellement en service au sein des armées doivent être mis à jour dans les meilleurs délais afin de conserver leur capacité de stocker avec un niveau de sécurité acceptable des informations jusqu'au niveau confidentiel défense.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Transport / Stockage de données sécurisés	GLOBULL V1	BULL	Transport et stockage transitoire de données de type disque dur amovible permettant le transport jusqu'au niveau S.	D / S	MinArm
<i>Commentaire : La décision d'homologation par l'EMA pour l'usage des Globull VI est désormais caduque, l'ANSSI considère que les Globull VI ne sont plus agréés depuis le 1er juin 2020. Voir pour utiliser les futurs Globull V2</i>					
Transport / Stockage de données sécurisés	ECLYPT CORE 600	VIASAT (UK)	Disque dur chiffrant agréé niveau NATO SECRET. Capacité HDD 120 ou 320 GB et SDD 128 ou 256 GB	R / S	OTAN

4.6.7 Équipements de chiffrement

OTAN

Document	Date	Origine	Type doc	Portée
SDIP 293- REV1 de mars 2011- Instructions for the Control and Safeguarding of NATO Cryptomaterial Document classifié NR	Mars 2011	OTAN	Document international	Systèmes OTAN
<i>Commentaire : ce document définit le socle minimum de règles applicables pour la sécurité physique, la distribution et la gestion de tous les matériels de chiffrement utilisés dans le cadre de l'OTAN.</i>				
<i>Ce document classifié NR peut être obtenu sur le portail de l'Intraced S-SF (cf. §4.1.7 Accès à la documentation technique)</i>				

Adressage équipements de chiffrement

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°134 relative à l'adressage IPV4 des réseaux protégés : version 2.1 du 25 juin 2014 <i>Cf. § 8.4.7 Adressage IP</i>	25 juin 2014	DIRISI	Directive	MinArm Réseaux Classifiés de défense
<i>Commentaire : Cette directive porte sur les équipements agréés Diffusion Restreinte ainsi que les équipements relevant du classifié de défense (Echinops, TCE621,...) en métropole, OME, ... mais hors des chiffreurs du réseau du centre de gestion (Socrate, Rtran) et hors RIFAN.</i>				

4.7 Interconnexions, passerelles et solutions de sécurité iso/multi niveaux

4.7.1 Passerelles d'échanges

Document	Date	Origine	Type doc	Portée
Concept d'emploi « accès réseaux extérieurs » SLR des services "d'accès aux réseaux extérieurs": cf. 3.1.7.2 Accès aux réseaux interministériels [SU-RMI] et autres réseaux extérieurs [SU-REX]		SC1	Concept Emploi SLR	MinArm Tout réseau
Guide « Recommandations pour les architectures des systèmes d'information sensibles ou diffusion restreinte » réf. PG-075	28 déc. 2020	ANSSI	Guide	Toutes administrations NP-DR
Guide « Recommandations relatives à l'interconnexion d'un système d'information à Internet » V3.0 du 19 juin décembre 2020	19 juin 2020	ANSSI	Guide	Toutes administrations NP-DR
<i>Commentaire : Ce document adresse des interconnexions entre un réseau privé hébergeant des informations sensibles non classifiées de défense et un réseau ouvert type Internet. Ce document n'édicte pas de règle impérative, mais décrit un ensemble de concepts ou de recommandations à adapter en fonction des contraintes et enjeux du contexte.</i>				
Recommandations relatives à l'interconnexion d'un système d'information à Internet : guide ANSSI-PA-066 du 19 juin 20	19/06/2020	ANSSI	Guide	Toutes administrations
Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu <i>cf.4.5 Sécurisation des COTS</i>	30 mars 2013	ANSSI	Note technique	Toutes administrations
Recommandations de sécurité concernant l'analyse des flux HTTPS <i>cf.4.5 Sécurisation des COTS</i>	9 octobre 2014	ANSSI	Note technique	Toute admin.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°13 sur la sécurité des accès aux services de l'Internet et de l'hébergement des services Internet du ministère <i>Cf. 6.1.3.2 Hébergement Internet</i>	30 juin 2010	DGSIC	Directive	MinArm
<i>Commentaire : Règles applicables aux accès au réseau et aux services de l'Internet ainsi qu'en matière d'hébergement de services internet.</i>				
AC/322-D/0030-REV5 – Directives complémentaires du 23 février 2011 sur les aspects techniques et la mise en œuvre de l'INFOSEC pour l'interconnexion des systèmes d'information et de communication (SIC) document classifié NR de février 2011	Février 2011	OTAN	Guidelines	OTAN
<i>Commentaire : Cette directive précise les principes de base à appliquer et les exigences minimales de sécurité pour la mise en œuvre d'interconnexion entre SIC de l'OTAN, entre SIC de l'OTAN et SIC nationaux de l'OTAN, et entre SIC OTAN et SIC d'entités hors OTAN.</i>				
<i>Ce document classifié NR peut être obtenu sur le portail de l'Intraced S-SF (cf. §4.1.7 Accès à la documentation technique)</i>				

4.7.2 Passerelles transdomaines

Passerelles ministérielles génériques

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Passerelle	PES	DIRISI	Plateforme d'échange sécurisée Internet/Intradef composée de : - SISMEL, - ACHERON (obsolet), - Passerelle API v2.1 décrits ci-dessous.	R / S	Intradef Internet
Passerelle	ACHERON	DIRISI	Passerelle d'échange de fichiers asynchrone (entre 2 et 15 mn) entre SI Intradef/Internet utilisant le protocole WebDav et les mécanismes de filtrage ISPT. Soumise à des restrictions de volumétrie, de formats et restreinte aux fichiers NP non chiffrés.	D / S	Intradef/ Internet
<i>Commentaire : cette passerelle en voie d'obsolescence ne doit plus être utilisée pour les nouveaux projets (lui préférer la passerelle API v2.1 pour les échanges de fichiers de taille inférieure à 8Mo – la version 2.2 attendue pour 2025 permettra de s'affranchir de cette limitation dans la limite des quotas alloués). Ceci implique d'utiliser des API Rest plutôt que le protocole WebDav. Le recours à des échanges asynchrones de gros blocs de données ne constitue pas une bonne pratique d'architecture : échanger des données unitaires en mode synchrone présente de meilleures qualités de fiabilité et de résilience, raison pour laquelle le recours à la PAPI v2.1 doit systématiquement être recherché.</i>					
Passerelle	PASSERELLE API v1	DIRISI	Passerelle API RESTful entre des SI Intradef et Internet offrant des fonctions de gestion des API, des droits associés, de publication, de documentation et de sécurité. Limitée aux seuls systèmes d'informations hébergés sur des plateformes opérées par la DIRISI (Intradef et Heliss NG). Pas de possibilité d'échange de fichiers (même encodés en base 64 par exemple). Homologuée jusqu'en juin 2023, elle est remplacée par la version 2.1	D / S	Intradef Internet (Heliss NG)
Passerelle	PASSERELLE API v2.1	DIRISI	Passerelle API RESTful entre des SI Intradef et Internet offrant des fonctions de gestion des API, des	R / S	Intradef Internet (Heliss

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
			<p>droits associés, de publication, de documentation et de sécurité. Limitée aux seuls systèmes d'informations hébergés sur des plateformes opérées par la DIRISI (Intradef et Heliss NG puis C1NP). Cette nouvelle version de la passerelle API RESTful inclut la capacité d'échange des fichiers de manière synchrone avec des fichiers limités en taille à 8 Mo.</p> <p>Mise en production en octobre 2023.</p>		NG)
Passerelle	PASSERELLE API v2.2	DIRISI	<p>Service en cours d'étude : reprend les fonctions de la passerelle API et inclut la capacité d'échange des fichiers tel qu'envisagé initialement pour une version synchrone de la passerelle ACHERON. A l'issue la passerelle ACHERON devrait être décommissionnée.</p>	E / -	Intradef Internet (Heliss NG)
Passerelle	ISPT	DIRISI	<p>Passerelle Web permettant d'accéder à la navigation Web Internet depuis les postes Intradef.</p> <p>Système homologué jusqu'au 13 juin 2024</p> <p>(cf. 3.1.7.1 Internet sur le poste de travail)</p>	R / S	MinArm Intradef
Passerelle	DMZ IRD	DGA	<p>Interconnexion des Réseaux de Défense : permet l'interconnexion des sociétés avec la DGA. Permet également le raccordement avec des collectivités territoriales.</p> <p>(*) soutien assuré par la DGA</p>	R / S (*)	DGA
Passerelle	SIMS DR	DIRISI SGDSN	Relais de messagerie pour envoyer des messages officiels (échanges entre les ambassades)	O / -	MinArm

PES : Plateforme d'Échanges Sécurisés est un composant de la transformation numérique pour les échanges entre l'Intradef et l'internet : cette plateforme regroupe actuellement :

- la passerelle API d'échanges de données sous forme d'API de type REST et d'échanges synchrones de fichiers de taille inférieure à 8Mo ;
- la passerelle SISMEL d'échanges de mails,
- la passerelle ACHERON d'échanges asynchrones de fichiers via protocole WebDav.

Document	Date	Origine	Type doc	Portée
Passerelle API : spécification d'interface générique de la passerelle API avec les SI clients V1.2	16 Septembre 2022	SAND	Spéc. Technique	MinArm
<i>Commentaire : Ce document fournit aux directions de projets, maîtrises d'ouvrage et maîtrises d'œuvre toutes les informations fonctionnelles et techniques nécessaires à l'utilisation du service « passerelle API » mis en œuvre par la DIRISI entre les segments Intradef & Internet maîtrisé (Heliss NG puis C1NP). Le développement des API doit suivre le cadre technique de mise en œuvre des API du ministère [cf. 3.2.4.4]</i>				
Directive DIRISI n°195 relative à l'exploitation et au soutien du système ACHERON	1 ^{er} mars 2017	DIRISI	Directive	MinArm

Document	Date	Origine	Type doc	Portée
<i>Commentaire : Cette directive a pour but de fournir les éléments relatifs à l'exploitation du système ACHERON. Elle précise les responsabilités de l'opérateur DIRISI, de ses clients, et les modalités de mise en œuvre du système ACHERON.</i>				
Passerelle ACHERON : Spécifications d'interface générique de la passerelle ACHERON	10 février 2017	DIRISI	Spéc Technique	MinArm
<i>Commentaire : Ce document fournit aux directions de projets, maîtrises d'ouvrage et maîtrises d'œuvre toutes les informations fonctionnelles et techniques nécessaires à l'utilisation du service « passerelle ACHERON » mis en œuvre par la DIRISI entre les segments Intradef & Internet maîtrisé (Heliss NG).</i>				

Passerelles et moyens d'accès spécifiques

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Passerelle	SMOBI	DIRISI	Solution de MOBilité de l'Intradef Service permettant un accès sécurisé à l'Intradef en mobilité	R / S	MinArm

4.7.3 Autres passerelles

Un travail de recensement et de rationalisation du GT passerelles piloté par la DIRISI/MOA Socle a déjà recensé plus de 160 passerelles.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Passerelle	ADER	DIRISI	Permet l'accès des administrations au réseau ADER (Administration En RESeau). Le support utilisé est le RIE (Réseau Internet d'État)	R / S	Intradef Interministériel
Passerelle	Espace Partenaires (voir IRD)	DIRISI - DGA	L'espace partenaires offre un espace de confiance permettant un échange entre le ministère des armées et ses partenaires. Il repose sur l'utilisation du réseau ENX, d'une politique de sécurité définie et maîtrisée par le ministère. Point de contact : direction du projet Espace Partenaire (DGA) (*) Soutien DGA	R / S(*)	Intradef Partenaires

4.8 Administration de la sécurité

4.8.1 Gestion des utilisateurs et des droits

Cf. aussi §4.6.1.3 Habilitation et gestion des profils

Document	Date	Origine	Type doc	Portée
Directive technique sur la gestion des comptes dans un annuaire et application à un Active Directory (cf. 3.3.4.2 Annuaires techniques de ressources)	04 avril 2013	DGSIC	Directive	MinArm

Commentaire : Ce document définit les règles de sécurité du ministère des armées pour la gestion des comptes dans un Active Directory.

4.8.2 PCA-PRA

Document	Date	Origine	Type doc	Portée
Guide DGSIC n°4 portant sur la rédaction des plans de continuité d'activité (PCA) et plan de reprise d'activité (PRA) diffusé par note n°771 /DEF/DGSIC du 26 juillet 2010	23 juillet 2010	DGSIC	Guide	MinArm

Commentaire : aide à la réflexion pour la rédaction de PCA-PRA au sein du ministère peu adapté à des entités éphémères (comme les structures liées aux OPEX).

Guide pour réaliser un plan de continuité d'activité	12 juin 2013	SGDSN	Guide	Etat
<i>Commentaire : Ce guide élaboré par le SGDSN présente une démarche méthodologique permettant l'élaboration concrète d'un PCA. Il est destiné aux organismes relevant de l'État, aux collectivités territoriales ainsi qu'aux entreprises.</i>				
Guide DGSIC n°5 « dispositions pratiques et techniques de continuité informatique » diffusée par note n°1323/DEF/DGSIC/SDSSI du 10 décembre 2010	10 déc. 2010	DGSIC	Guide	MinArm
<i>Commentaire : éléments d'aide issus de retours d'expérience pour la mise en place de PCA/PRA et plus particulièrement de PCI/PRI.</i>				
Directive DGSIC n°17 portant sur l'identification et le suivi des systèmes critiques (DIR-ISSC) diffusée par note n°805/DEF/DGSIC/ du 7 juillet 2011	6 juillet 2011	DGSIC	Directive	MinArm
<i>Commentaire : Cette directive définit la méthode à mettre en œuvre par des organismes du ministère des armées en matière de systèmes critiques, les critères d'identification et de caractérisation de ces systèmes, et les dispositions de suivi de leur état de préparation. Le premier objectif est de cartographier les systèmes critiques du ministère, de les caractériser et de maintenir à jour la cartographie ainsi réalisée. Un système d'information est dit critique dès lors qu'il remplit ou supporte une ou plusieurs mission(s) essentielle(s) du ministère. Il s'agit ensuite d'établir des plans d'action et calendriers de progrès vers les objectifs de sécurité retenus et de suivre leur application. Cette démarche d'amélioration continue et itérative implique de réviser régulièrement les résultats.</i>				

4.8.3 Gestion des journaux d'évènements applicatifs ou système

La gestion des journaux d'évènements applicatifs ou système ou « logs » (précédemment désignés en tant que « traces », terme non approprié qui renvoie à un autre aspect de l'observabilité, cf. 6.2.7) issus des équipements des réseaux informatiques du ministère (serveurs, postes de travail, pare-feux, sondes, ...) et portant sur des données multiples (données à caractère personnel, données de trafic, de localisation, de systèmes d'informations...) est couverte par plusieurs textes de portée globale engageant le ministère, notamment au regard des données à caractère personnel.

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°29 portant sur les traces et leur gestion au sein du ministère de la Défense diffusée par note n°1065/DEF/DGSIC/SDSSI/NP du 12 novembre 2013 <i>Commentaire : La directive n°29 a pour objet la définition des principes, des buts et des objectifs ainsi que des moyens généraux pour parvenir à une gestion des traces efficiente au ministère des armées. Elle stipule notamment que la mise en œuvre des traces répondant au juste besoin est obligatoire et que le format doit être celui de la RFC 5424 (syslog).</i>	12 nov.2013	DGSIC	Directive	MinArm
Arrêté du 27 janvier 2023 autorisant la mise en œuvre de traitements automatisés de gestion des traces relatives aux systèmes d'information et de communication du ministère de la défense https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047089467	27 janvier 2023	MinArm	Arrêté	MinArm
Directive DIRISI n°270 relative à la mise sous supervision de sécurité	1 décembre 2018	DIRISI	Directive	Armées

4.8.4 Maintien en condition de sécurité (MCS) - composant technique

DECOS-S : Sur l’Intradef, le service DECOS-S⁴⁸ opéré par la DIRISI permet le déploiement des correctifs de sécurité de systèmes soutenus sur l’Intradef : le périmètre couvert concerne les systèmes et produits Microsoft, les produits Adobe et les distributions LINUX soutenus par la DIRISI (incluant les produits RedHat) au travers des mécanismes techniques idoines et adaptés (WSUS pour les serveurs Windows, dépôts LINUX, suite RedHat Satellite pour les serveurs RHEL rattachés, ...).

Courant 2024, DECOS-S sera progressivement remplacé par MEDUSA, dépôt généralisé d’artefacts binaires en cours de réalisation par l’AND (cf. §6.2.1.3 Dépôt d’artefacts)

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°111 d’emploi DECOS-S diffusée par note n°400954/DEF/DIRISI/DIR	25 février 2014	DIRISI	Directive	Armées
<i>Commentaire : Cette directive d’emploi décrit le périmètre et l’organisation relative au projet DECOS-S et liste les produits et systèmes couverts.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Correctifs de sécurité	Projet DECOS-S	DIRISI	Ce système opéré par la DIRISI permet le déploiement de correctifs de sécurité pour : - les systèmes et produits Microsoft - les systèmes Centos 7, AlmaLinux 8+ et RedHat 7+ (ainsi que Debian et Ubuntu) - les produits d’Adobe - des middlewares et bibliothèques logicielles non présents dans les dépôts précédents	R / S	Intradef
<i>Commentaire : Les systèmes d’exploitation Centos (obsolète en juin 2024), Debian (assujetti principalement à un usage SIE en voie d’extinction et Ubuntu non autorisé) ne sont mentionnés que par complétude de description d’usages historiques en cours de suppression. Cela signifie que leur présence dans le dépôt DECOS-S ne vaut pas recommandation d’utilisation.</i>					

⁴⁸ DECOS-S : Déploiement des Correctifs de Sécurité sur l’intranet Sensible

4.8.5 Sécurisation des flux réseaux

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité relatives à IP Sec pour la protection des flux réseau (cf.4.5 Sécurisation des COTS)	3 août 2015	ANSSI	Note technique	Toutes administrations
Recommandations de sécurité relatives à TLS, édition 1.2	26 mars 2020	ANSSI	Note technique	Toutes administrations
<i>Commentaire : se reporter à l'annexe 8.2 pour connaitre la dernière version recommandée pour TLS</i>				

4.8.6 Sécurisation des supports de stockage

Supports classifiés de défense

Document	Date	Origine	Type doc	Portée
Guide n°972/SCSSI/SI relatif à la protection des supports classifiés de défense. (Cf. 4.1.3 Références pour le niveau Secret (ex CD))	9 avril 1998	PM	Circulaire	Toutes administrations
Guide technique 972-1 pour la confidentialité des informations enregistrées sur disque dur à recycler ou exporter (Cf. 4.1.3 Références pour le niveau Secret (ex CD))	17 juillet 2003	PM	Circulaire	Toutes administrations
<i>Commentaire : Ce document traite de la protection, manipulation et destruction des supports d'information tels que disques durs, clé USB, carte à puce, etc.</i>				

Supports amovibles sur l'Itradef

Document	Date	Origine	Type doc	Portée
Concept d'emploi des stations blanches NG sur l'Itradef sous timbre n°403275 /DEF/DIRISI/SDSSI du 18 juin 2013 diffusé par note n°403277/DEF/DIRISI/DIR du 18 juin 2013	18 juin 2013	DIRISI	Concept d'emploi	Intradef

4.8.7 Hébergement / Virtualisation

Document	Date	Origine	Type doc	Portée
Directive DGSIC n° 32 portant sur la sécurité de l'hébergement des SI au sein du ministère diffusée par note n°170/DEF/DGSIC/SDSSI/NP du 11 mars 2014	11/03/2014	DGSIC	Directive	MinArm
<i>Commentaire : Cette directive définit les exigences de sécurité que doivent respecter les opérateurs du ministère en matière d'hébergement. Les règles se décomposent en deux grandes parties :</i>				
<ul style="list-style-type: none"> • celles applicables à l'opérateur et à son système d'information • celles applicables aux systèmes informatiques hébergés, classées en fonction du niveau d'hébergement. <i>Lorsque le système informatique ou l'application est hébergé à l'extérieur du ministère, les directions de projet peuvent s'inspirer des règles qui y sont contenues afin de rédiger le contrat avec l'opérateur. Elle n'a pas pour but d'imposer des architectures aux opérateurs au sein des datacenters, ni de traiter des réseaux de transit.</i>				

Cf. aussi 5.1.2 Virtualisation

4.8.8 Supervision de la sécurité, LID

Pas de référence identifiée à ce jour.

4.8.9 Télémaintenance

La disponibilité de fonctionnalités de plus en plus riches au niveau du poste de travail, combinée à la diminution des ressources humaines techniques, entraînent un recours généralisé à des opérations d'assistance ou de maintenance à distance.

Constatant que la sécurité n'est pas toujours bien appréhendée pour réaliser ce type d'interventions et que les solutions utilisées amènent des vulnérabilités et octroient aux intervenants des droits importants, l'ANSSI a publié un certain nombre de notes techniques permettant de mieux sécuriser le recours à la téléassistance.

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité relatives à la téléassistance (MS-RDP et VNC) (cf.4.5 Sécurisation des COTS)	13 janvier 2017	ANSSI	Guide technique	Toute admin.
Recommandations de sécurité relatives à IP Sec pour la protection des flux réseau (cf.4.5 Sécurisation des COTS)	3 août 2015	ANSSI	Note technique	Toutes admin.
Recommandations pour un usage sécurisé d'(Open)SSH (cf.4.5 Sécurisation des COTS)	17 août 2015	ANSSI	Note technique	Toutes admin.

4.8.10 Sauvegardes

Cf. §6.2.6 Sauvegarde / restauration

4.8.11 Gestion de configurations de sécurité

Le format **SCAP** (Security Content Automation Protocol) est le protocole préconisé par le ministère pour mettre en œuvre des outils de gestion et de contrôle des configurations de sécurité.

C'est une **synthèse interopérable de spécifications ouvertes énumérant** les noms des produits utilisés, **les défauts des logiciels et les problèmes de configuration**. Dans certains cas il permet, grâce notamment à des mécanismes de classement, d'évaluer l'impact de la découverte des problèmes de sécurité.

SCAP offre un moyen :

- d'évaluer la sécurité des failles et les erreurs de configuration des logiciels dans l'entreprise de manière transparente, interopérable, reproductive et automatisable ;
- d'évaluer à chaque instant la posture de sécurité du système d'information ;
- de gagner du temps en orientant le travail des équipes d'administration ou d'audits sur des aspects plus importants de la sécurité.

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
SCAP	Security Content Automation Protocol. Ensemble de spécifications entretenues par le NIST ⁴⁹ et accessibles sur le site http://scap.nist.gov . Le ministère retient essentiellement les spécifications suivantes : <ul style="list-style-type: none">• CVE (pour Common Vulnerability Enumeration), permet d'associer un numéro unique à chaque nouvelle vulnérabilité (indépendamment de la référence donnée par l'éditeur). Cette norme est aujourd'hui incontournable dans le domaine de gestion de vulnérabilités.	R	MinArm

⁴⁹ NIST : National Institute of Standards and Technology

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
	<ul style="list-style-type: none"> • CCE (pour Common Configuration Enumeration), fournit un identifiant standard et un dictionnaire des problèmes de configuration liés à la sécurité. • CPE (pour Common Platform Enumeration), fournit un système de nommage permettant de désigner de façon non ambiguë des composants informatiques tels que machine, système d'exploitation ou paquetage logiciels. • XCCDF (pour eXtensible Checklist Configuration Description Format), fournit un standard XML pour la spécification des listes de tests et la publication des résultats des tests. • oval (pour Open Vulnerability Assessment Language), fournit un standard XML pour les procédures de test des défauts liés à la sécurité des logiciels, des problèmes de configuration et des correctifs. • CVSS (pour Common Vulnerability Scoring System), fournit un système de notation compris entre 0 et 10 pour évaluer la dangerosité d'une vulnérabilité. 		

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion de conformité	OpenSCAP	Opensource	Chaines CI/CD mises en place par l'AND	E / N	Intradef

« Conformité serveurs et postes de travail » : Le système de gestion de la Conformité serveurs et postes de travail a pour objectif de pouvoir réaliser un contrôle automatique et périodique de la conformité (conformité aux référentiels de sécurité et à l'annexe 8 du CCT) des serveurs et des postes de travail. Il utilise le standard SCAP. Il propose de plus un affichage des vulnérabilités associées à la pile logicielle détectée.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion de conformité	Conformité Serveurs et postes de travail	MinArm	Intradef Solution ministérielle en cours de déploiement sur les serveurs et totalement déployé sur les postes de travail	R / S	Intradef

4.9 Divers

La sécurité est transverse à tous les segments couverts par le CCT. Des préconisations relatives à la sécurité se retrouvent notamment dans les chapitres listés ci-après :

3.1.1.5 Socle technique logiciel du poste de travail

3.1.5 Sécurité [SU-SSO, SU-CHI, SU-SIG]

3.1.6 Mobilité [SU-AN, SU-ITN]

5.1.1 Système d'exploitation [OS]

5.1.2 Virtualisation

5.1.8.1 Téléphonie classique

5.1.8.2 Téléphonie chiffrée

5.2.5 ToIP / VoIP

5.2.6 Réseaux sans fil

6.1.1 Références générales sur l'hébergement

7.4 Conception et codage

5 INFRASTRUCTURE

5.1 Matériels, OS, virtualisation et conteneurisation

Ce paragraphe décrit les matériels, OS et composants.

5.1.1 Système d'exploitation [OS]

5.1.1.1 Système d'exploitation client

Document	Date	Origine	Type doc	Portée
Configuration sécurisée de Windows 7 : <i>(cf.4.5 Sécurisation des COTS)</i>	23 mars 2011	DGA MI	Guide technique	MinArm
Configuration sécurisée de Windows 10 V3.1 : <i>(cf.4.5 Sécurisation des COTS)</i>	18 mars 2022	DGA MI	Guide technique	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
OS Client	Windows Mobile	Microsoft	Ces OS ne sont plus maintenus et ne doivent en aucun cas être utilisés (y compris les versions 6.5 et 10)	I / N	MinArm
OS Client	Windows	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	S-SF SIA FrOps
OS Client	Android version	Google	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	*
OS Client	Autres OS		Tablettes/... Soumis à stricte dérogation suivant cas d'usage.	D / N	

5.1.1.2 Système d'exploitation serveur

CENTOS : Suite au changement de stratégie annoncé en décembre 2020 par REDHAT/IBM, le soutien de CentOS 8 s'est arrêté en novembre 2022, le soutien de CentoS 7.9 s'arrêtera quant à lui mi-2024.

ALMA LINUX : Suite à l'instruction du sujet et sa validation en CECNUM de juin 2022, Alma Linux devient la distribution Linux communautaire de substitution à CentOS sur les Intranets ministériels. Ceci a été confirmé depuis, après vérification de la capacité d'AlmaLinux à poursuivre ses activités dans la durée suite à la limitation d'accès aux sources des paquets par RedHat à ses seuls clients sous licence. AlmaLinux, qui conserve son principe de compatibilité binaire avec RedHat Enterprise Linux, mais ne recherche plus le principe d'identité parfaite en matière de correctifs, ce qui lui permet de les appliquer sans attendre que RedHat le fasse (RedHat n'appliquant d'ailleurs pas systématiquement tous les correctifs).

REDHAT ENTERPRISE LINUX : L'option RedHat reste disponible et recommandée pour les SI pour lesquels le support de l'application hébergée ou les conditions d'infogérance l'imposent.

WINDOWS SERVER : Ce système d'exploitation n'est utilisable que pour les systèmes d'informations ne pouvant techniquement pas être opérés sur une distribution Linux, compte-tenu des investissements en matière de maîtrise des dépôts binaires (MEDUSA), d'automatisation (RUCHE) et de standardisation menés par le Ministère pour ses hébergements de systèmes d'information. Ceci inclut le cadre d'un hébergement VPS ou salle blanche. La migration vers Linux sera systématiquement demandée lors de toute évolution

majeure ou migration vers le C1DR d'un système d'information éligible. Le personnel en charge de l'administration devra être formé en conséquence.

Le Ministère s'est doté d'une capacité à fournir rapidement des templates d'OS durcis, et leurs mises à jour successives, pour les réseaux Intradef et NP. Ces templates sont ceux mis en œuvre dans les machines virtuelles fournies par la DIRISI. Ces templates sont les mêmes que ceux mis à disposition des équipes projets sur PICSEL.

STRATEGIE EN MATIERE DE VERSIONS DES SYSTEMES D'EXPLOITATION :

- afin de pourvoir maîtriser ses hébergements, le Ministère se limite volontairement à maintenir au plus 2 versions majeures de systèmes d'information simultanément (par exemple Windows Server 2016 et 2019, Redhat Enterprise Linux ou AlmaLinux 8 et 9) ; Windows Server 2022 pourra toutefois être autorisé après obtention de dérogation pour des services d'infrastructures et hors des structures d'hébergement de systèmes d'information opérées par la DIRISI.
- Redhat Enterprise Linux et AlmaLinux possèdent des cycles de version majeures et mineures identiques (du moins pour les versions 8 et 9, la politique retenue par Redhat pour la version 10 n'étant pas encore connue), le second se conformant au premier :
 - Chaque version majeure dispose d'un support complet pendant 5 ans suivi d'une période de maintenance de 5 ans supplémentaires, RedHat apportant une possibilité d'une extension de support de 3 ans supplémentaires sur souscription, option non retenue par le Ministère (cf. <https://access.redhat.com/support/policy/updates/errata/>)
 - Chaque version mineure (numéroté de 8.0 à 8.9 ou 9.0 à 9.9) est maintenue 6 mois (RedHat propose une extension de support 18 mois supplémentaires pour les versions x.1, x.2, x.4, x.6 et x.8 sur souscription de l'Extended Update Support, option non retenue par le Ministère). Ceci couvre une période de 4 ans et demi, la version 8.10 ou 9.10 ajoutant les 6 mois manquant pour atteindre les 5 ans de support complet indiqués précédemment.
 - La dernière version mineure (8.10 ou 9.10) dispose donc de 6 mois de support complet puis de 5 ans de maintenance complémentaires.

En conséquence, un système d'information utilisant une version 8 inférieure à la version 8.10 devra suivre le cycle des mises à jour tous les 6 mois jusqu'à atteindre la version 8.10. Attendu que les dépôts de la version mineure n-1 restent disponibles jusqu'à ce que la version n+1 devienne disponible, cette montée de version mineure devra s'achever au plus tard à ce moment (un système d'information en version 8.6 doit migrer au plus tard quand la version 8.8 est disponible, idéalement lorsque la version 8.7 est mise à disposition).

Une fois la version 8.10 utilisée, le système d'information peut adopter deux stratégies différentes :

- rester en version 8.10 (en effectuant les mises à jour régulièrement) jusqu'à ce que la version 9.10 soit disponible (environ 2 ans ½ après) : le projet dispose alors de 2 ans ½ pour effectuer cette montée de version majeure ;
- poursuivre le cycle des versions mineures 9.x tel que décrit plus haut pour les versions 8.x.

A noter que la seconde stratégie implique des opérations plus fréquentes de mises à jour mais beaucoup plus faciles à mener, le changement d'une version mineure à l'autre ne présentant qu'un risque faible de dysfonctionnement.

De plus, l'obligation de MCS souscrite dans le cadre de l'homologation du système d'information impose de toute façon des mises à jour très régulières, et que vont faciliter les services et les automatismes mis en place dans le cadre de la cloudification des hébergements du Ministère.

La première stratégie, qui impose également ces mises à jour régulières, conduira à des travaux beaucoup plus

conséquents, et d'autant plus difficiles qu'ils sont espacés dans le temps (maintien de la connaissance, campagne de tests de non régression d'envergure ...)

Dans tous les cas, **il est impératif que les projets prévoient des tests fonctionnels de non régression** : ces travaux indispensables dans un contexte de cloudification et d'automatisation des déploiements s'avèrera en outre un investissement extrêmement rentable pour mener les indispensables campagnes de tests, lors du déploiement initial puis à chaque mise à jour mineure ou majeure, qu'il s'agisse de MCO, MCS ou d'évolution.

Pour appuyer cette démarche et renforcer sa maîtrise en la matière, le Ministère met en œuvre une usine d'images de système d'exploitation durcis afin de pouvoir les générer, les tester et les mettre régulièrement et rapidement à disposition sur PICSEL, C1DR et C1NP.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
OS Server	Windows Server	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	* / *	*
OS Serveur	Redhat Enterprise Linux RHEL	Redhat	Préférer la distribution AlmaLinux si un support REDHAT n'est pas requis. * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	* / *	*
OS Serveur	Debian	Debian	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	* / *	*
OS Serveur	CentOS	Redhat	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	* / *	*
OS Serveur	AlmaLinux	Alma	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	* / *	*
OS Serveur	Autres distributions LINUX		Soumis à stricte dérogation après démonstration d'impossibilité d'utiliser une distribution Linux recommandée et mise en œuvre d'un durcissement équivalent. Les travaux d'automatisation de déploiement seront également à la charge du projet.	D / N	

5.1.1.3 Autres (équipement réseau)

Pas de référence identifiée à ce jour.

5.1.2 Virtualisation

Document	Date	Origine	Type doc	Portée
Directive DIRISI 80 « de nommage des VLAN » v1.1 Cf. 8.4.6 Nommage VLAN	11 juin 2013	DIRISI	Directive	Intradef S-SF
Recommandations de sécurité pour les architectures basées sur VMware vSphere ESXi cf.4.5 Sécurisation des COTS	25 mai 2016	ANSSI	Note	Toute admin.
Problématiques de sécurité associées à la virtualisation des systèmes d'information cf.4.5 Sécurisation des COTS	26 sept. 2013	ANSSI	Note technique	Toute admin.

Recommandations pour la sécurisation des commutateurs Ethernet et l'utilisation des VLAN cf.4.5 Sécurisation des COTS	22 février 2010	DGA MI	Guide technique	MinArm
---	-----------------	--------	-----------------	--------

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Virtualisation serveur	VMWare	VMWare	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	* / *	*
Virtualisation serveur	Hyper-V	Microsoft	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i> A ce jour, seul le type 1 est recommandé (BARE METAL)	* / *	*

Pas de référence identifiée à ce jour pour les sujets suivants :

- *Virtualisation applications*
- *Virtualisation poste de travail*
- *Virtualisation stockage, sauvegarde*
- *Virtualisation réseau*

5.1.3 Conteneurisation

Les avantages généralement reconnus de la technologie des conteneurs sont :

- rapidité de démarrage: un conteneur démarre en quelques secondes, là où une machine mettra généralement plusieurs minutes, ce qui induit une capacité d'adapter en temps réel la capacité face à un pic de charge.
- légèreté et optimisation de la consommation des ressources : parce que les conteneurs utilisent le système d'exploitation de leur hôte, contrairement aux machines virtuelles qui ont chacune le leur, ils possèdent une **empreinte réduite** (RAM et CPU).
- immutabilité⁵⁰ : par principe, le conteneur est un composant généralement sans états : les modifications sont réalisées par génération d'un nouveau conteneur qui vient remplacer l'ancien, simplifiant drastiquement les actes d'exploitation.
- facilité de déploiement : un conteneur prédéfini est auto-suffisant et isolé de son hôte et peut donc être directement déployé en production sur celui-ci en s'affranchissant de tout problème de dépendance logicielle.

Les qualités évoquées ci-dessus font de la technologie de la conteneurisation un outil tout à fait adapté pour répondre à certains besoins engendrés par la transformation numérique qui anime actuellement le ministère.

Il convient néanmoins de rappeler que l'emploi de ces solutions n'est pas sans incidence sur les pratiques en vigueur au sein du ministère tant en termes d'hébergement, de pratiques d'exploitation et de maintien en

⁵⁰ Infrastructure immuable (immutable infrastructure) : les images de machines virtuelles ou de conteneurs sont générées à partir de rôles ansible et d'un dépôt de composants logiciels maîtrisé ; une fois testées, ces images servent à instancier le système d'information en production. Toute modification de ces instances nécessite de regénérer de nouvelles images et de les instancier en production pour remplacer les anciennes. Aucune modification directe des instances en production n'est permise.

condition de sécurité.

Au niveau de l'exploitation de ces solutions, la remise en cause de certains paradigmes et approches en la matière nécessite un accompagnement et une évolution des mentalités et pratiques en matière d'administration, de gestion et d'exploitation de ces structures et des applications qui en dépendent. De même, il s'agit pour le ministère d'accompagner la montée en compétences du personnel qui va être associé à cette évolution. Enfin, ces nouveaux modes de travail doivent s'intégrer avec ceux des systèmes classiques (nombre de systèmes d'informations ne tireraient aucun bénéfice à adopter une architecture conteneurisée) et avec la démarche DevSecOps actuellement en cours de mise en place par le ministère dans l'opération de cloudification de ses hébergements Intradef et Internet.

Concernant la sécurité de l'information, les conteneurs présentent, par défaut, une étanchéité moindre qu'une VM : des règles de conception (rootless), de durcissement et des frameworks de sécurité devront être choisis pour assurer le niveau de sécurité requis. L'approche « boîte noire » des conteneurs pose la problématique de la gestion des images, de leur source, de leur sécurité, de leur maintien en condition opérationnelle et de sécurité et de leur gestion. Le modèle à l'échelle est en train d'être construit afin d'offrir les garanties nécessaires au déploiement d'images externes sur les intranets ministériels (fourniture du dockerfile ou équivalent, vérification des règles de construction et des dépendances, contrôle de la composition via des outils d'analyse introspectifs ou via fourniture du SBOM⁵¹, ...).

Techniquement, l'éclatement du système d'information dans de multiples conteneurs et l'absence de visibilité directe sur leur composition et leur fonctionnement intra et inter conteneurs va entraîner une complexification significative de la tâche des exploitants qu'il faudra au préalable contrebalancer par le recours à des outils d'orchestration et de supervision adéquats.

Le paragraphe 3.2.1.2 Démarche et principes liés rappelle les grands principes d'architecture logicielle à mettre en œuvre afin de concevoir une application éligible à ce type d'hébergement.

Le ministère se prépare désormais à fournir cette capacité : disponible dès fin 2023 sur PICSEL à des fins de développement et d'expérimentations, elle sera mise en production sur Intradef (dans l'environnement C1DR) fin 2024.

Les systèmes d'information hébergés en orchestration de conteneur sous soumis aux mêmes exigences de gouvernance que ceux hébergés en machines virtuelles. En particulier, leur architecture et leur pile logicielles doivent être soumises au SC²A pour validation. A cet effet, les fichiers dockerfile ou équivalents, ainsi que les SBOM devront être transmis.

Règle	Énoncé	Statut	Portée
CCT_R6	Il est OBLIGATOIRE que les solutions retenues en matière de conteneurisation ou d'outillage de la conteneurisation respectent les standards OCI (à titre d'exemple sur les runtime, containerd, cri-o, runc seront envisageables, lxc/lxd ou docker seront refusés)	O	Intradef Internet
CCT_R7	Il est RECOMMANDÉ que les solutions retenues en matière de conteneurisation ou d'outillage de la conteneurisation respectent les standards OCI (à titre d'exemple sur les runtime, containerd, cri-o, runc seront envisageables, lxc/lxd ou docker seront déconseillées)	R	MinArm Hors Intradef Hors Internet

⁵¹ SBOM : Software Bill of Material : liste de l'exhaustivité des composants logiciels utilisés et livrés, toutes dépendances comprises, dans un format normalisé comprenant également les versions précises associées.

Les travaux menés cette année ont conduit le Ministère à sélectionner les technologies suivantes, dans le respect des standards OCI.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Hébergement en orchestration de conteneurs	CaaS C1DR	MinArm	Service d'orchestration de conteneurs sur base de Kubernetes (distribution RKE2)	E / S	Intradef
<i>Commentaire : service attendu fin 2024 sur la plateforme C1DR, notamment pour héberger l'instance diffusion restreinte d'ARTEMIS.IA. Un service équivalent est déjà mis en place à des fins de développement et d'expérimentations sur la plateforme PICSEL et sera progressivement ouvert d'ici à fin 2023. Lorsque le service sera ouvert sur C1DR, il s'imposera à tout système d'information conteneurisé sur Intradef. Il appartient aux directions de projet concernés de prendre les mesures nécessaires pour y migrer dès que cela sera requis.</i>					
Hébergement en orchestration de conteneurs	CaaS C1NP	MinArm		E / S	C1NP
<i>Commentaire : un service identique à celui mis en place sur la plateforme C1DR sera mis en œuvre ensuite sur la plateforme C1NP. Dans l'attente, cette plateforme ne permettra pas de recourir à la technologie des conteneurs.</i>					
Hébergement en orchestration de conteneurs	CaaS IST-C	MinArm	Service d'orchestration de conteneurs sur base de Kubernetes (distribution RKE2)	R / S	I3E – IST
<i>Commentaire : L'hébergement en conteneur est mis en œuvre au sein des SI d'hébergement et métier de l'intranet IST secret du site de Bruz. Les applications/SI candidats sont soumis aux règles d'hébergement émises par l'intranet d'accueil. Les travaux de l'intranet IST-C seront reconduits sur les SI nationaux RI3E DR et S. Le S2NA a une capacité à déployer et utiliser des solutions d'orchestration de conteneurs sur la base Kubernetes.</i>					
Orchestrator	Kubernetes	CNCF	Orchestrator de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	A / N	MinArm
<i>Commentaire : une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.</i>					
Distribution	RKE2	CNCF/SUSE	Ou « RKE Government » : ensemble de composants assemblés en vue de répondre aux besoins induits par l'orchestration de conteneurs. Distribution retenue pour les offres de conteneurisation cloud C1 du Ministère. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	A / N	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
<i>Commentaire : RKE2 a été retenue pour son adéquation à l'environnement de déploiement hors connexion Internet (dite « air gap ») et le niveau de sécurisation nativement intégré dont l'application du durcissement CIS (v1.6 ou v1.23) avec un minimum d'intervention des exploitants. Chaque version est maintenue environ 1 an, la fin de vie survenant environ 2 mois après. Les projets doivent s'organiser en conséquence pour assurer des montées de version sur une base annuelle et assurer l'application des mises à jours dans l'intervalle (https://www.suse.com/lifecycle#rke2). C'est pourquoi, il est recommandé d'utiliser un gestionnaire de cluster afin d'être capacité d'assurer le MCS et le MCO.</i>					
Moteur de containerisation	Containerd	CNCF	Par extension, tout moteur s'appuyant sur cet exécutable. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits.</i>	A / N	MinArm
Gestion de clusters	Rancher	CNCF/SUSE	Permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits</i>	A / N	MinArm
<i>Commentaire : Rancher embarque un grand nombre de produits prépackagés sous formes de charts Helm disponibles dans le catalogue de l'application. En cas de déploiement via Rancher, la version à privilégier est la version proposée par Rancher. Toutefois les modules sont tous installables de façon indépendantes, ce qui permet de remédier à une vulnérabilité. Dans le cas où aucune version n'est spécifiée pour un produit du fait d'un cycle d'évolution trop rapide, il conviendra de se reporter directement à la documentation du produit.</i>					
<i>Commentaire 2 : Rancher est une application en conteneur qui s'exécute dans un cluster dédié avec des composants imposés (INGRESS NGINX comme composant CNI par exemple). En conséquence, les composants listés ci-après ne sont utilisables que dans les autres clusters.</i>					
Interface réseau pour conteneurs	Cilium	CNCF/Isovalent	Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits</i>	A / N	MinArm
<i>Commentaire : Apporte la gestion des network policies sur les noms de domaine contrairement à Calico (à vérifier)</i>					
Interface réseau pour conteneurs	Calico	CNCF/Tigera	Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1_Pile logicielle : liste des produits</i>	A / N	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Contrôle d'admission	Kyverno	CNCF / Nirmata	Moteur de contrôle d'admission (gestion de la conformité et de la configuration) <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	A / N	MinArm
Gestionnaire de backup	Velero	CNCF / SUSE	Solution de sauvegarde et restauration de clusters Kubernetes Choisir la version en fonction du support de la version Kubernetes (cf documentation Velero) <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	A / N	MinArm
Gestionnaire de backup	Kasten	CNCF / VEEAM	Solution de sauvegarde très fin et restauration de clusters et ressources Kubernetes. Permet d'offrir du « Backup as a service » en fonction de l'implémentation choisie. Permet également la migration simple de clusters.	A / N	MinArm
Gestionnaire de backup	Px Backup	Pure Storage	Solution de gestion de stockage sur baies Pure Storage.	A / N	MinArm
Stockage	Plugin CSI vSphere	VMWare	Permet de monter des disques vSphere sur les nœuds d'un cluster Kubernetes afin de créer des volumes persistants <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	A / N	MinArm
<i>Commentaire : Infra hors cloud C1, requis quand sous-jacent VMWare notamment pour Kasten et Velero</i>					
Stockage	Portworx	Pure Storage	Solution de gestion de stockage sur baies Pure Storage. <i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	A / N	MinArm
<i>Commentaire : Infra hors cloud C1 (pour du ad hoc, pas prévu pour les C1 d'interagir directement avec les baies PureStorage)</i>					

Les systèmes et projets quel que soit leur domaine d'application (big data, projets applicatifs, ...) ne disposant pas dans l'environnement concerné d'une offre de service d'hébergement en orchestration de conteneurs et souhaitant mettre en œuvre ces technologies devront donc soumettre au préalable au SC²A une demande de dérogation. Ceci permettra de recenser les usages envisagés et de vérifier, avec les équipes concernées, la pertinence du recours à la conteneurisation. Une attention toute particulière sera systématiquement portée sur la gestion et la maîtrise des images utilisées.

Document	Date	Origine	Type doc	Portée
Guide ANSSI de recommandations de sécurité relatives aux déploiements de conteneur docker <i>cf.4.5 Sécurisation des COTS</i>	23 septembre 2020	ANSSI	Note technique	Toute admin.
<i>Commentaires : Ce document présente les bonnes pratiques de sécurité relatives au déploiement et à l'exécution de conteneur Docker (le Docker daemon et la gestion des images Docker sont hors de périmètre de ce guide)</i>				

L'intérêt de la technologie d'orchestration des conteneurs réside également dans son intégration de la chaîne DevSecOps mise en place pour assurer un cycle rapide de déploiement des applications et de leurs mises à

jour. Cet aspect, partie intégrante de la démarche de cloudification en cours, s'appuie sur des capacités GitOps côté production et un outillage CI/CD DevSecOps adossé à la plateforme PICSEL.

En attendant la mise en place de l'offre de service d'hébergement en orchestration de conteneurs (prévue fin 2024 sur le C1DR) à même de garantir une exploitation maîtrisée de conteneurs en production, le recours aux conteneurs, demeure soumis à une demande de dérogation, notamment afin de s'assurer du bon emploi de la technologie et de la capacité à rejoindre les offres ministérielles dès lors qu'elles seront disponibles.

Par ailleurs, le recours à des conteneurs mis en œuvre sur serveurs lors des phases de développement et de test pour lesquelles ils sont parfaitement adaptés est pleinement autorisé. La capacité actuellement en test sur PICSEL va être ouverte progressivement à compter de la fin 2023.

Enfin, l'utilisation de conteneurs sur le poste client (PC, tablette, ...) est, quant à elle, interdite (fonctionnement en mode serveur proscrit, complexité de l'exploitation du poste). Depuis la migration Windows 10 des postes clients, il n'est désormais plus permis (et par configuration, rendu techniquement impossible) d'y faire fonctionner une machine virtuelle.

5.1.4 Poste terminal : fixe / mobile (portable, smartphone, tablette)

Configuration logicielle : cf. §3.1.1.5 Socle technique logiciel du poste de travail

Configuration matérielle : pas de référence identifiée à ce jour

Document	Date	Origine	Type doc	Portée
Recommandations de configuration matérielle de postes clients et serveurs x86 (cf.4.5 Sécurisation des COTS)	25 mars 2015	ANSSI	Note technique	Toute admin.
<i>Commentaires : Ce document traite essentiellement de mécanismes matériels présents ou prévus sur architecturex86 et de recommandations quant à leur usage. Il aborde également des éléments de configuration qu'il convient de vérifier lors du paramétrage du BIOS d'un ordinateur.</i>				

5.1.5 Communication

5.1.5.1 Voix et Vidéoconférence Secret

Paragraphe laissé vide intentionnellement.

5.1.6 Impression et scanners

Cf. 3.1.3.3 Impression – édition multifonction [SU-IMP]

5.1.7 Stockage

Document	Date	Origine	Type doc	Portée
Concept d'emploi et SLR sur le stockage des données (cf. §3.1.4 Gestion des données)				
<i>Commentaire : le service utilisateur est décrit en §3.1.4 Gestion des données</i>				
D directive DIRISI n°245 relative à l'exploitation et au soutien d'IRIS V1.0 (cf. §3.1.4 Gestion des données)	2 mai 2018	DIRISI	Directive	Intradef
<i>Commentaire : cette directive précise le service offert par IRIS, l'organisation et le fonctionnement de l'infrastructure IRIS ainsi que les éléments relatifs à l'exploitation, le soutien et les responsabilités des acteurs.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Stockage	IRIS Sur une base de Scality	DIRISI	Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde)	R / S	Intradef
<i>Commentaire :</i> cette solution (Infrastructure Résiliente et Intègre de Stockage) est un service d'infrastructure de stockage extensible de données non structurées (de taille supérieure à 60 ko) offrant plusieurs pétaoctets pour les besoins de l'infrastructure (sauvegardes, journaux d'évènements applicatifs, ...) et des d'applications à travers différents protocoles (NFS, SMB v3 et S3), qu'il s'agisse de données froides (dépôt d'archives, de sauvegardes, d'images ISO, de vidéos...) ou non (stockage objet via le protocole S3).					
Stockage	IRIS-S-SF Sur une base de Scality	DIRISI	Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde) en cours d'intégration avec le programme SIA	E / S	S-SF
Stockage	MinIO	MinIO	Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde). Assujetti à des cas d'emploi ne permettant pas de recourir aux instances IRIS existantes	A / N	MinArm

Présente sur l'Intradef, cette capacité est en cours de déploiement sur le réseau S-SF (SIA) et également prévue dans l'environnement C1NP ainsi que PICSEL pour faciliter les travaux de développement des systèmes d'information devant y avoir recours. Ce stockage n'est en revanche pas adapté aux cas d'usage suivants :

- hébergement de bases de données relationnelles (du fait des taux I/O élevés que cela nécessiterait) ;
- exécution de machines virtuelles.

5.1.8 Téléphonie

5.1.8.1 Téléphonie classique

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°7 portant sur la téléphonie sur le protocole internet publiée au Bulletin Officiel des Armées Cf 3.1.8 Téléphonie	13 janvier 2009	DGSIC	Directive	MinArm
Directive DGSIC n°11 du 8 janvier 2010 portant sur la sécurisation des autocommutateurs diffusée par lettre n°15/DEF/DGSIC/SDSSI du 8 janvier 2010	8 janvier 2010	DGSIC	Directive	MinArm

Commentaires : Cette directive définit la politique à mettre en œuvre par les organismes du ministère des armées responsables d'un service de téléphonie classique.

Elle fournit les critères de décision pour l'acquisition, la réalisation, la mise en œuvre, le maintien en condition et la sortie de service d'un service de téléphonie classique.

Cette directive est applicable aux systèmes d'information et de communication non classifiés de défense supports d'un service de téléphonie classique et à tous leurs composants, notamment leurs éléments actifs.

Directive DIRISI n°256 du 13 août 2018 relative à l'emploi et la configuration de la téléphonie professionnelle du ministère de la défense (TPDM)	8 janvier 2010	DGSIC	Directive	MinArm
--	----------------	-------	-----------	--------

Commentaires : Cette directive a pour but de définir un cadre d'emploi des différentes fonctionnalités de téléphonie professionnelle au sein du ministère et de standardiser au maximum les configurations des PABX métropolitains ou non.

Directive de mise en œuvre de la téléphonie mobile au sein des bases de défense Note N° D-14-001374/DEF/EMA/CPCS/B.SOUT/SIC-SSI/NP du 04 février 2014	4 février 2014	EMA	Note	Intradef
---	----------------	-----	------	----------

5.1.8.2 Téléphonie chiffrée

Cf 4.6.8

5.1.8.3 Radiotéléphonie (INPT)

Le réseau radio du futur (RRF) constitue un projet de réseau commun aux acteurs de la gestion de crise. Il a vocation à se substituer aux réseaux radios RUBIS et INPT actuellement utilisés, qui reposent sur des infrastructures détenues et exploitées par l'État et qui offrent des services rudimentaires.

Le RRF vise à remédier à ces limites en offrant une solution hybride, qui consiste à utiliser les réseaux 4G et 5G des opérateurs de réseaux mobiles, tout en bénéficiant d'une qualité de service différenciée par rapport à leurs autres clients

Le RRF bénéficiera à de nombreux services de l'État (forces de sécurité intérieure, armées, services de secours, administration pénitentiaire, services douaniers, services de la navigation maritime ou aérienne, etc.), comme à certains opérateurs d'importance vitale et aux collectivités territoriales (police municipale, services départementaux d'incendie et de secours (SDIS)).

Le RRF devait être employé de manière opérationnelle lors des J0 (2024) en France.

Les armées pourraient donc être conduites, à brève échéance, à devenir clientes RRF et/ou à interfaçer leurs propres systèmes avec le RRF

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°133 d'exploitation et de soutien de l'INPT /DIPAD : V1.0 du 16 juin 2014	16 juin 2014	DIRISI	Directive	MinArm
<i>Commentaire : L'INPT (Infrastructure Nationale Partageable des Transmissions) est un réseau globalisé de radiotéléphonie numérique, de couverture nationale, offrant des services de voix et de données, et opéré par le ministère de l'intérieur. Cette directive décrit les modalités d'exploitation du sous-réseau de l'INPT attribué au ministère des armées (DIPAD : Desserte Interarmées en PMR Accessibles à la Défense). A terme, la défense est concernée par 10000 terminaux.</i>				

5.1.9 Solutions 'packagées' : SIA-Box

Cf. §2.3.1 Politique SIC ambition numérique

5.2 Réseaux

Pas de référence identifiée à ce jour.

5.2.1 Généralités

Paragraphe laissé vide intentionnellement.

5.2.1.1 Architecture des réseaux, IPV6

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°20 portant sur l'architecture des réseaux 'internet Protocol' publiée au Bulletin Officiel des Armées	24 août 2011	DGSIC	Directive	MinArm
<i>Commentaire : Règles relatives essentiellement aux réseaux de transit global IP (hors passerelles et enclaves), et ne concernent que la seule couche IP (hors réseaux supports, ou couches de transport ou applicatives).</i>				
Directive DGSIC n°22 portant sur la transition IPv6 publiée au Bulletin Officiel des Armées	20 déc. 2011	DGSIC	Directive	MinArm
<i>Commentaire : Directive relative à la stratégie de migration vers l'IPv6 et règles relatives aux acquisitions et évolutions majeures de tous les systèmes d'information et de communication au regard de la transition vers IPv6</i>				

5.2.1.2 Adressage IP

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°129 portant sur l'adressage IPV4 du ministère de la défense : version 2.1 Cf. 8.4.7 Adressage IP	7 mai 2014	DIRISI	Directive	MinArm
Directive DIRISI n°109 portant sur la politique de routage des flux IP DEFENSE Cf. 8.4.7 Adressage IP	26 mai 2018	DIRISI	Directive	MinArm
Directive DIRISI n°134 relative à l'adressage IPV4 des réseaux protégés Cf. 8.4.7 Adressage IP	25 juin 2014	DIRISI	Directive	MinArm Réseaux Classifiés de défense

5.2.1.3 Bout en bout : QoS – Contrats de services – interconnexion – métrologie

Marquage – qualité de service

Document	Date	Origine	Type doc	Portée
Directive n°36 DGSIC relative au marquage des flux IP pour la qualité de service sur les réseaux IP au sein du ministère de la Défense	3 juillet 2015	DGSIC	Directive	MinArm

Routage inter-systèmes

Document	Date	Origine	Type doc	Portée
Directive n°38 relative au « routage inter-systèmes » [DIR-RIS] , approuvée le 29 mars 2016 et diffusée par note n°173/DEF/DGSIC/DG/NP du 30 mars 2016	29 mars 2016	DGSIC	Directive	MinArm Tout Intranet

Commentaire : Cette directive énumère des modèles d'interconnexion de réseaux IP et traite de règles de bon usage ainsi que des aspects liés à la sécurisation des interconnexions aussi bien dans le domaine des connexions de type unicast que multicast. Elle concerne les aspects techniques et organisationnels relatifs aux équipements matériels de réseaux, aux éléments de sécurité, et aux applications.

Bonnes pratiques de configuration de BGP	Sept. 2013	ANSSI	Guide	Toutes admin.
---	------------	-------	-------	---------------

Commentaire : ce document de l'ANSSI réalisé avec la coopération d'opérateurs français, décrit les bonnes pratiques de configuration du protocole BGP (Border Gateway Protocol), protocole natif des routeurs. Il édicte des recommandations suivant les types d'interconnexions et de relations entre AS (Autonomous System).

Métrologie – indicateurs

Document	Date	Origine	Type doc	Portée
Directive DGNUM n°42 relative à la métrologie réseau (DIR-METRO)	15 janvier 2019	DGNUM	Directive	MinArm
Directive DIRISI n°145 relative à l'exploitation de la fonction métrologie réseau, V1	07 janv. 2015	DIRISI	Directive	MinArm

Commentaire : Cette directive décrit l'ensemble des outils de métrologie des réseaux de la DIRISI, en particulier l'exploitation des outils de métrologie des réseaux du CNMO-R Maisons Laffitte (réseaux noirs et réseau DR). Elle décrit les modalités de demandes de mise en surveillance métrologie réseaux.

5.2.1.4 Problématique des réseaux contraints

Document	Date	Origine	Type doc	Portée
Recommandations à destination des responsables d'applications devant déployer leur système sur des théâtres d'opération et bâtiments de la Marine, sous timbre n° 759/DEF/DGSIC/SDAU du 27 novembre 2014	27 novembre 2014	DGSIC	Note	MinArm

Commentaire : cette note fournit un ensemble de recommandations générales en matière de conception, d'architecture et de qualification des systèmes d'information pour la prise en compte de leur déploiement sur les théâtres d'opération, les bateaux et implantations outre-mer (limites des réseaux, liaisons satellitaires...)

5.2.2 Réseaux de transport WAN et routage

DESCARTES (DEploiement des Services de Communications et Architectures des Réseaux de TElécommunications Sécurisés) : les réseaux de transport du ministère des Armées s'appuient sur plusieurs composantes fonctionnelles s'appuyant sur la technologie IP :

- d'un réseau de transport IP d'usage général, opéré par un opérateur civil (OPERA, migration vers le RIE en cours d'étude) ;
- d'un réseau de transport métropolitain résilient et maîtrisé capable de fonctionner même en cas de crise grave (composante SOCRATE du programme DESCARTES portée par le marché SCR, rénovation du réseau historique résilientSOCRATE) ;
- Une architecture de routage et de sécurité (composante POINCARE du programme DESCARTES portée par le marché ISR) constituée d'un système de points d'interconnexion (PI) sur les sites offrant les capacités de raccordement des réseaux de desserte, de chiffrement des flux (au niveau DIFFUSION RESTREINTE) et leur aiguillage selon leur classe et la résilience requise pour transiter sur le réseau d'usage général et/ou le réseau résilient ; cette composante standard est doublée d'une composante ATM (Air Trafic Management) sur les sites contribuant au contrôle aérien pour le routage spécifique de ces flux dédiés, qui est ségrégée pour pouvoir répondre aux exigences réglementaires liées à l'ATM

- d'un secours par satellite (COMCEPT) pour le transport vers les sites nécessitant de la résilience et n'ayant qu'un accès au réseau de transit IP d'usage général ;
- de divers supports tiers et Internet, notamment pour les sites OME ;
- d'une architecture de routage et de sécurité (POINCARE), constituée d'un système de points d'interconnexion (PI) sur les sites offrant les capacités de raccordement des réseaux de desserte, d'aiguillage et de chiffrement des flux.

Dans le cadre du programme DESCARTES, une spécification d'interface pour les clients au réseau DESCARTES a été établie. Elle définit les spécificités techniques du raccordement IP au réseau DESCARTES et les contraintes et exigences d'interconnexion à prendre en compte par les systèmes client.

Il est important de prendre en compte le MTU (Maximum Transmission Unit) pour les clients raccordés au réseau DESCARTES (ce MTU est de 1330 octets). Il s'agit également du MTU appliqué à l'Intradef.

Tout client / application se raccordant au réseau DESCARTES doit renseigner le fichier CAR (Canevas des besoins Réseau) qui caractérise le type d'échange et les flux entre les différents sites et la QoS envisagée.

Pour une demande de DIMA (Durée d'Indisponibilité Maximale Acceptée) supérieure à I2 ou une priorisation opérationnelle supérieure à P3 (au sens de la directive DGSIC n°36 relative au marquage des flux IP), le directeur d'application doit également fournir le besoin en communication à l'ARR (Autorité de Régulation des Réseaux) qui décide de la DIMA et de la priorité opérationnelle associées à l'application (voir ci-dessous)

Document	Date	Origine	Type doc	Portée
CAR (Canevas des besoins Réseaux)	19 sept. 2013	DGA	Spécification d'interface	MinArm et hors MinArm (sites partenaires)
ARR (Autorité de Régulation des Réseaux)				MinArm

5.2.3 Services de réseaux de desserte

5.2.3.1 Maîtrise des flux réseau [MFR]

Pas de référence identifiée à ce jour.

5.2.4 Services des réseaux étendus : filtrage - passerelles [FIL-PAS]

Cf 5.2.12 Câblage

5.2.5 ToIP / VoIP

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°7 portant sur la téléphonie sur le protocole internet : directive du 13 janvier 2009 publiée au Bulletin Officiel des Armées	13 janvier 2009	DGSIC	Directive	MinArm

<p><i>Commentaire : Cette directive définit la politique à mettre en œuvre avant le déploiement d'un service de téléphonie sur le protocole internet (ToIP) par les organismes du ministère des armées. Elle fournit les critères de décision pour l'acquisition, la réalisation et la mise en œuvre d'un service de ToIP.</i></p> <p><i>Elle est applicable aux systèmes d'information et de communication non classifiés de défense support d'un service de ToIP et à leurs composants, notamment leurs éléments actifs.</i></p> <p><i>Cette directive tient compte du projet de référentiel général d'interopérabilité prescrit par l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives et du projet de référentiel général de sécurité.</i></p>	<p>Recommandations de sécurisation d'une architecture de téléphonie sur IP (cf.4.5 Sécurisation des COTS)</p>	<p>23 déc. 2013</p>	<p>ANSSI</p>	<p>Note technique</p>	<p>Toute admin.</p>
--	--	---------------------	--------------	-----------------------	---------------------

5.2.6 Réseaux sans fils

5.2.6.1 Technologies sans fil (WIFI, Bluetooth, RFID, ZIGBEE, Lorawan)

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°23 portant sur la sécurité de réseaux sans fil diffusée par note n°54/ARM/DGNUM/DG/NP du 2 février 2021	2 février 2021	DGSIC	Directive	MinArm
<i>Commentaire : Règles sur l'emploi et la mise en œuvre de technologies sans fil : Wi-Fi, Bluetooth, RFID, ZIGBEE, LORAWAN. Cette directive abroge l'ancienne version restreinte au Wifi du 6 février 2012 et le guide n°9 sur la mise en œuvre des réseaux Wifi</i>				
Recommandations de sécurité relatives aux réseaux WIFI (cf.4.5 Sécurisation des COTS)	9 septembre 2013	ANSSI	Note technique	Toutes administrations

5.2.6.2 RFID

Document	Date	Origine	Type doc	Portée
Politique interarmées pour l'emploi de systèmes d'identification par radiofréquences [PIA RFID] diffusée par note sous double timbre : N°D-17004828 ARM/EMA/SC N°DGA01D17025073/ARM/DGA/DO/SMCO	06 octobre 2017	EMA DGA	Politique	MinArm
Directive technique interarmées pour la mise en œuvre des technologies RFID [DTIA RFID] diffusée par note : N°D-18005592 ARM/EMA/DSA/MCO/NP N°DGA01D18054469/ARM/DGA/DO/SMCO/NP	15 octobre 2018 15 octobre 2018	EMA DGA	Directive	MinArm
Vademecum sur la RFID entretenu par DGA/DO/SMCO	14 nov. 2016	DGA	Guide	MinArm

Commentaire : ce guide RFID fournit une aide aux spécificateurs sur l'utilisation de cette technologie pour le soutien des opérations d'armement. Il peut aider soit en phase amont lors de la rédaction des documents contractuels (STB, CCTP, ...) ou en phase de réception des offres et de négociation avec les industriels afin de vérifier tous les aspects (questions, normes, ...) des solutions RFID proposées.

5.2.7 Liaison satellitaires

Pas de référence identifiée à ce jour.

5.2.8 Équipements : Lan, Routage, Switch, Pare feu, accélérateurs...

Document	Date	Origine	Type doc	Portée
Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu (cf.4.5 Sécurisation des COTS)	30 mars 2013	ANSSI	Note technique	Toutes administrations
Recommandations pour la sécurisation des commutateurs Ethernet et l'utilisation des VLAN cf.4.5 Sécurisation des COTS	22 février 2010	DGA MI	Guide technique	MinArm

5.2.9 Équipements de chiffrement

Cf 4.6.7 Équipements de chiffrement

5.2.10 VPN

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité relatives à IP Sec pour la protection des flux réseau (cf.4.5 Sécurisation des COTS)	3 août 2015	ANSSI	Note technique	Toutes administrations

5.2.11 Baies

Pas de référence identifiée à ce jour.

5.2.12 Câblage

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°15 « infrastructure des réseaux de desserte du ministère de la défense V2.0 sous timbre n°502688/DEF/DIRISI/SCP du 21 octobre 2010	21 octobre 2010	DIRISI	Directive	MinArm
<i>Commentaire : cette directive identifie les éléments du câblage générique, les normes et modalités de câblage des réseaux de desserte du ministère. Elle est constituée de deux parties :</i>				
<ul style="list-style-type: none"> - partie 1 : relative à l'état de l'art en cours au ministère sur le câblage, les locaux techniques, les armoires techniques, le câblage du fédérateur, le câblage capillaire (postes terminaux) ainsi que les règles sur le cheminement, le repérage et le marquage de l'infrastructure et les procédures de contrôles ; - partie 2 : les normes retenues en matière de câblages, de résistance au feu, de courants forts et les normes techniques réseaux. Cet ensemble normatif est entretenu sous l'égide du Centre de Normalisation de la Défense (CND) via son site « Intranormes ». (http://intranormes.dga.defense.gouv.fr/, accès restreint) 				

6 CADRE FONCTIONNEL ET TECHNIQUE D'HEBERGEMENT

6.1 Plateformes d'hébergement

6.1.1 Références générales sur l'hébergement

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°32 portant sur la sécurité de l'hébergement des SI au sein du ministère Cf. 4.8.7 Hébergement / Virtualisation	11/03/2014	DGSIC	Directive	MinArm
<i>Commentaire : applicable à l'opérateur, et aux systèmes informatiques hébergés, en recommandation pour les applications ayant vocation à être hébergées à l'extérieur du ministère.</i>				
Document Cadre DIRISI n°61 portant sur la mise en production des Systèmes d'Information et de Communication dans les infrastructures informatiques de la DIRISI V3.0	11/08/2023	DIRISI	Document Cadre	MinArm (infra DIRISI)
<i>Commentaire : définit le processus de mise en production d'un SI dans les infrastructures d'hébergement de la DIRISI (dont CINP et CIDR et en orchestration de conteneurs) pour tout type de projet (sous IM 2476 ou 1618, cycle en V ou agile, adapté selon le niveau de service : infogérance, VPS ou salle blanche).</i>				

La mise en production des systèmes d'informations et services hébergés sur les infrastructures de la DIRISI régit par le Document Cadre n°61 référencé ci-dessus a été amendée et allégée. Elle s'effectue selon 3 étapes :

- **Pré-production** : premier jalon lançant la phase d'installation en environnement de préproduction du socle d'infrastructure pour y vérifier la bonne intégration du SI (dont l'installation automatisée via Ruche) et mener la VABF (validation d'aptitude au bon fonctionnement) conformément aux conditions restrictives fixées par l'autorité d'homologation au travers de l'AfT (Approval for Testing, i.e. Autorisation pour tests), notamment en matière de données utilisées ;
- **Production expérimentale** : deuxième jalon après acceptation de la VABF, lançant la phase de VSR (vérification en service régulier) en environnement de production pour une durée inférieure à 6 mois et un panel d'au plus 10% du nombre total d'utilisateurs prévus avec des données réelles et nécessitant une homologation (au minimum une APE : Autorisation Provisoire d'Emploi) ; la VSR doit permettre d'apprécier la performance du SI en conditions normales d'utilisation et d'effectuer les ajustements qui pourraient s'avérer nécessaires ;
- **Production opérationnelle** : troisième et dernier jalon après acceptation de la VSR et obtention d'une homologation ferme et qui marque la mise en service opérationnelle.

Ce document cadre couvre également le cas des mises à jour sans et avec modification de périmètre ou d'architecture et celui des déploiements multi sites.

Règle	Énoncé	Statut	Portée
CCT_R8	Il est INTERDIT d'héberger à des fins d'intégration, de pré-production ou de production un service ou un système d'information en dehors des plates-formes de socle dès lors qu'une offre de service adaptée est disponible dans l'environnement considéré.	I	MinArm
CCT_R9	Pour le cas où une plateforme de socle n'est pas disponible ou pour des activités d'expérimentation ou de développement non réalisables sur PICSEL, il est OBLIGATOIRE d'obtenir une dérogation du SC ² A.	O	MinArm

Le SC²A appréciera la nécessité d'opérer des hébergements hors plates-formes du socle, sur des infrastructures en salle blanche et opérées par des tiers :

- les plates-formes d'hébergement du S2NA sont considérées comme appartenant au socle ;
- les activités de réalisation d'infocentre, de tableaux de bord ou d'entraînement de modèles d'intelligence artificielle sont assimilées à des activités de production, à mener dans un environnement destiné à ce type d'activité, les instances de production du service utilisé devant prévoir ce cas d'usage et mettre à disposition les espaces et les ressources nécessaires (ex : instance de « développement » du service de visualisation de données Qlik Sense)
- l'utilisation de la SHEMDEV à des fins de développement nécessite une dérogation du SC²A qui vérifiera l'incapacité de PICSEL à répondre au besoin et fera programmer les évolutions requises pour y remédier : la dérogation sera en conséquence nécessairement bornée dans le temps.

Hors activité de développement, les hébergements sur des plates-formes tierces restent assujettis aux autorisations de la gouvernance et à une homologation. Il en est de même des plates-formes elles-mêmes.

6.1.2 Typologie d'environnements sur les plateformes

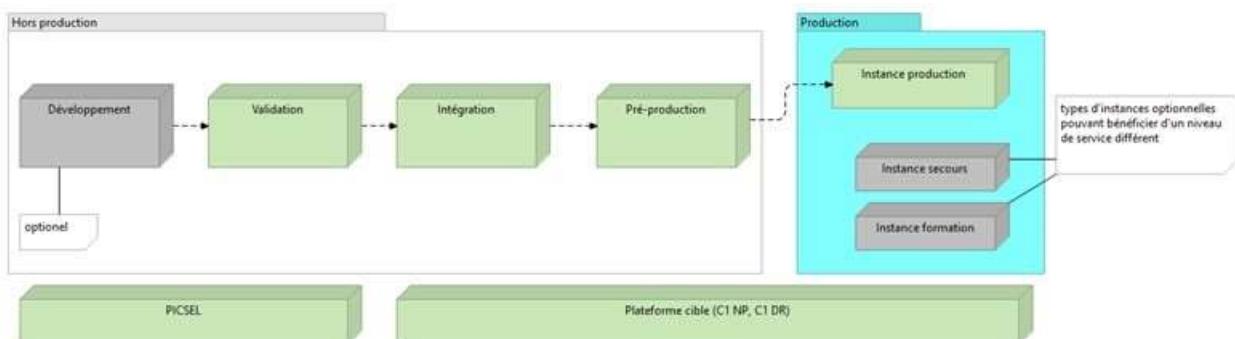


Figure 3 : Typologie des environnements sur les plateformes

Pour chaque SI déployé, différents environnements sont envisageables en fonction des visées et phases du projet.

Environnements SI dits « Hors production » :

- **Environnement de développement** : il est destiné aux projets pour implémenter leurs systèmes et est porté hors dérogation par la plate-forme PICSEL, quel que soit le niveau de classification visé au déploiement. Il porte également une logique de bac-à-sable ou d'expérimentation. C'est dans cet environnement que sera réalisé le contrôle qualité requis avant déploiement vers l'environnement cible ; ce contrôle qualité est destiné à valider avant déploiement la conformité du système aux contraintes et attendus d'hébergement (playbooks Ansible, conformités au CCT, pile maintenue et à

jour, ...).

- **Environnement « Intégration SI »** : il est destiné aux équipes du SI (équipe projet et de développement qui ont la charge du déploiement et de l'exploitation de cet environnement, même en infogérance) pour tester les procédures de déploiement en environnement représentatif sur plateforme d'hébergement cible et valider le bon fonctionnement technique du SI (dans le cas d'une primo installation, d'évolutions ou d'application de correctifs de sécurité).

Environnement « Préproduction SI » : il est destiné aux équipes du RCP/RTS et aux infogérants pour tester les procédures d'exploitation et valider le bon fonctionnement du SI (VABF). L'équipe projet procède aux tests fonctionnels (dans le cas d'une primo installation ou d'évolutions du SI). Elle permet d'effectuer la mise en œuvre de tous les changements sans impacter le SI de production (cf. étape éponyme du Document Cadre n°61 décrite ci-dessus)

Environnement SI « Production » : il s'agit de l'environnement d'hébergement cible qui peut lui-même se voir adjoindre deux types d'instances complémentaires, dont le niveau de service apporté peut être différent de celui de l'instance de production principale. C'est sur cet environnement qu'est réalisé la VSR (cf. étapes de production expérimentale et de production opérationnelle du Document Cadre n°61 décrites ci-dessus).

Instance SI « Secours » : elle permet la reprise ou la continuité du système (éventuellement en mode dégradé) de l'instance principale de production, dont elle est l'image y compris pour la partie « données », en cas d'incident majeur. Il convient de noter que le mécanisme de réPLICATION des données devra être étudié et mis en place par le projet. Le PCI/PRI reste également de la responsabilité du bénéficiaire. L'instance de secours est nécessairement déployée sur un DataCenter différent de l'instance de production principale ;

Instance SI « Formation » : ce type d'environnement, éventuellement à accès restreint, permet d'offrir un espace de formation aux utilisateurs finaux du SI, éventuellement pour préparer la mise en production d'une nouvelle version sur l'instance de production principale.

6.1.3 Les niveaux de service d'hébergement

Pour chaque offre, l'opérateur s'engage à mettre en œuvre tous les moyens disponibles pour assurer aux environnements de production le niveau de services découlant directement de la catégorisation DIMA du système d'information attribuée le cas échéant par l'Autorité de Régulation des Réseaux :

- Bronze : SI non catégorisé par l'Autorité de Régulation des Réseaux (ARR) ou catégorisé I2 par l'ARR ;
- Argent : SI catégorisé I3bis par l'ARR ;
- Or : SI catégorisé I3 par l'ARR ;
- Platine : SI catégorisé I4 par l'ARR.

Sont concernées la disponibilité, les sauvegardes et restaurations ainsi que la prise en compte des incidents et des demandes de changements.

6.1.4 Processus d'hébergement

Après expression du besoin d'hébergement par le bénéficiaire auprès de la DIRISI, le processus d'hébergement se déroule en 5 phases successives : attribution de l'hébergement une fois les pré-requis acquis, qualification du SI sur l'infrastructure DIRISI, mise en pré-production, mise en production expérimentale puis opérationnelle et, à terme, arrêt des services d'hébergement.

Lors de la demande d'hébergement, il convient de prendre en compte l'ensemble de ses contraintes, besoins et services consommés (débits réseaux nécessaires, certificats, entrées DNS, NTP, supervision et supervision de sécurité, services d'authentification, de messagerie, passerelles, archivage ...). Des agents seront installés concomitamment pour répondre à certains besoins (supervision, sécurité, sauvegarde, gestion et contrôle de configuration ...). Selon le cas, des tests de montée en charge pourront en outre être demandés.

Enfin, pour être mis en production, il est rappelé qu'un système doit être homologué et faire l'objet d'une validation d'architecture de la part du SC²A, être homologué et satisfaire aux exigences du Comité de mise en production (cf. 6.1.1 ci-dessus)

6.1.5 Le dossier d'architecture technique est un prérequis essentiel et structurant de tout échange avec la DIRISI (deux modèles sont disponibles pour ce document sur le portail hébergement de la DIRISI)Hébergement sur Intradef

Périmètre	Offre	Utilisation/Restriction	Statut	Portée
Hébergement de production / pré-production	Infogérance	L'offre C1 DR se substituera à cette offre pour les nouveaux projets	R / S	Intradef
Hébergement de pré-production / production	VPS/VPSc	L'offre C1 DR se substituera à cette offre pour les nouveaux projets	R / S	Intradef
Hébergement de production / pré-production	Salle blanche	Réservé aux besoins en matériel spécifique	A / N	Intradef
Hébergement de production / pré-production / intégration	C1 DR	Primo-accédants courant fin 2023	E / S	Intradef
Hébergement de production	HDS	Réservé aux données de santé	R / S	Intradef
Hébergement de production	SIE	Intradef embarqué uniquement	R / S	Intradef
Hébergement de développement/expérimentation/validation	PICSEL	Les systèmes d'information doivent réaliser un contrôle qualité sur cette plate-forme pour évaluer leur aptitude à un hébergement en production.	R / S	Intradef

6.1.5.1 Aspect réseaux

6.1.5.1.1 Gard

Sur Intradef, le réseau interne des datacenter (Bordeaux, Rennes, Suresnes, Six-Fours en service ; Toulon dispose d'une architecture hautement résiliente de type IP Fabric. Le projet Gard apporte une connectivité à l'accès de 10 et 25 Gbit/s et une automatisation de la configuration sur base de logiciel (SDN).

6.1.5.1.2 SARDaC

De plus, les flux entrant/sortant dits « Nord-Sud » des datacenter sont désormais filtrés (fin du déploiement début 2024) et ne laisseront dèsormer circuler par défaut que (projet SARDaC⁵²) :

- HTTPs : exposition des sites, applications web et API REST ou SOAP ;
- S3 : flux d'accès aux stockages objet ;
- SMTPs : flux de messagerie sécurisé ;
- DNS : flux d'interrogation des serveurs de nommage ;
- NTP : flux de synchronisation horaire ;
- LDAPs : flux d'authentification des postes de travail ;
- flux de réPLICATION des infrastructures (Active Directory, réPLICATION asynchrone des baies de stockage, réPLICATION des bucket IRIS, SRM et vSphere)

Les flux existant sont examinés sur Bordeaux, Six-Fours, Suresnes et le seront à Rennes et Toulon fin premier trimestre 2024. Les flux non conformes et non justifiés seront ensuite progressivement coupés.

6.1.5.1.3 Netscaler

La politique d'emploi des Netscaler d'entrée des datacenter a également fait l'objet d'une harmonisation entre les différents centre. Ces équipements portent actuellement trois fonctions principales :

- Equilibrage de charge (Loadbalancing ou LB),
- Chiffrement/déchiffrement des flux TLS,
- Authentification.

A l'avenir, ces fonctions seront assurées uniformément comme suit.

6.1.5.1.3.1 Equilibrage de charge

Les Netscalers assurent l'équilibrage de charge :

- Pour les systèmes d'information « historiques » infogérés par la DIRISI,
- Pour les seuls composants du socle (portefeuille de la DSI Socle) concourrant à l'activité d'hébergement ou à la sécurité après avis favorable du SC²A

Pour les systèmes d'information hébergés en VPS sur l'offre VPS DR, cette fonction de répartition de charge doit être portée au niveau de leur couche logicielle et incluse dans leur architecture, en utilisant des solutions

⁵² Sécurisation Accès Réseau DataCenter

référencées et recommandées (HAProxy, httpd, NGINX, ...).

Dans un second temps, les systèmes d'information hébergés sur C1DR pourront bénéficier de la répartition de charge apportée par la technologie VMWare NSX-T.

6.1.5.1.3.2 Chiffrement des flux

Le chiffrement des flux TLS consiste à la conversion du http vers le https dans le sens sortant, le certificat étant porté par l'équipement Netscaler. Cette fonction est maintenue pour :

- Tous les systèmes d'information « historiques » qui ne peuvent pas assurer eux-mêmes cette fonction, et après obtention d'une dérogation du SC²A ;
- Tous les systèmes d'information en https en infogérance DR et bénéficiant actuellement de ce service ;
- Tous les systèmes d'information en https en infogérance sur le C1DR le temps que la fonction soit reprise par la technologie VMWare NSX-T ou la brique de socle gestion des secrets dès qu'elle sera en production opérationnelle.

6.1.5.1.3.3 Authentification

Les équipements mutualisés Netscaler ne doivent porter aucune fonction spécifique d'un système d'information spécifique, au premier rang desquelles l'authentification qui est, sauf dérogation obtenue auprès du SC²A, de la responsabilité exclusive de la brique de socle MindefConnect Intradef.

En conséquence, les systèmes d'information « historiques » en infogérance DR ou non et utilisant ce mode d'authentification le conserveront jusqu'à leur migration vers le C1DR. Aucun nouveau système ne sera autorisé à utiliser ce mode d'authentification non conforme.

6.1.5.2 Hébergement Infogérance DR

Cet hébergement sera remplacé par C1DR à compter de 2024. Les systèmes d'informations qui bénéficient de ce service doivent intégrer la démarche « move to cloud » pour y être transférés d'ici à environ 5 ans, échéance prévisionnelle d'arrêt du service.

La DIRISI assure l'administration technique et la supervision de la couche technique applicative (systèmes d'exploitation, serveurs applicatifs, serveurs de présentation, bases de données) sous réserve que ses composants soient déclarés soutenus par la DIRISI dans le présent Cadre de Cohérence Technique.

La DIRISI assure une administration technique restreinte de la pile logicielle non déclarée comme « soutenue » dans le CCT, limitée à des actions réflexes telles que l'arrêt et relance des services, sous réserve de fourniture par le bénéficiaire d'une documentation technique suffisante.

L'administration fonctionnelle du SI incombe entièrement au bénéficiaire.

L'ensemble des enregistrements d'exécution (traces, journaux d'évènements applicatifs et systèmes, ...) doit être rendu accessible à la DIRISI à des fins d'exploitation de la sécurité.

Document	Date	Origine	Type doc	Portée
Conditions Générales d'Hébergement DIRISI de SI DR EMO.GUI.R4.014 v2.0	01 juillet 2022	DIRISI	Guide	Intradef
<i>Commentaire : cette note décrit les conditions générales d'hébergement d'un système d'information DR dans le cadre de l'offre de service de la DIRISI, la sécurité et les obligations liées à cet hébergement.</i>				
Directive DIRISI n°239 d'administration de l'Intradef : v1 du 3 avril 2018, directive entretenue par la DIRISI	3 avril 2018	DIRISI	Note	Intradef
<i>Commentaire : Cette directive fait suite à la désignation du DC-DIRISI comme administrateur de l'Intradef. Elle décline les axes sur lesquels cette fonction s'exerce.</i>				
Directive n°193 Urbanisation des équipements dans les centres informatiques de la DIRISI V2.0 du 01/10/2016	1 octobre 2016	DIRISI	Note	Intradef

6.1.5.3 Hébergement C1 DR

Document	Date	Origine	Type doc	Portée
Conditions Générales d'Hébergement DIRISI de SI C1 DR	fin 2023	DIRISI	Guide	Intradef
<i>Commentaire : cette note décrira les conditions générales d'hébergement d'un système d'information DR dans le cadre de l'offre de service C1 DR de la DIRISI, la sécurité et les obligations liées à cet hébergement.</i>				

Partie intégrante de l'offre de service Cloud (cf. 3.2.1.2 Démarche et principes liés), C1DR est destiné à remplacer au premier semestre 2024 les hébergements Infogérance DR (cf. 6.1.4.2 ci-dessus), VPS DR et VPS-c DR (cf. 6.1.4.4 ci-dessous). Dès lors, tous les nouveaux systèmes d'information requerrant ce niveau de service y seront hébergés.

Construit dans une recherche de maîtrise, de standardisation et d'automatisation, C1 DR vise avant tout à simplifier et accélérer la mise en production des systèmes d'information mais ne modifie pas fondamentalement les principes et le cadre technologique en vigueur en œuvre sur les hébergements Infogérance et VPS DR : hébergement en machines virtuelles avec les systèmes d'exploitation durcis du Ministère.

Il apporte toutefois un raccordement automatisé aux services du socle dont certains devaient précédemment être demandés séparément (NTP, DNS, sauvegarde, dépôts de mise à jour MEDUSA, antivirus, gestion des licences Windows et RedHat, supervision, contrôle de conformité, orchestrateur Ruche, inventaire, comptes de services). D'autres services seront progressivement ajoutés à la liste (gestion des secrets et des certificats, stockage objet IRIS, puits de journaux d'événements applicatifs et système ...).

La démarche de cloudification impose au système d'information de respecter quelques exigences qui sont rappelées ci-après et qui sont destinées à faciliter les automatisations et l'exploitabilité, donc améliorer le niveau de service offert, et d'en conserver la maîtrise dans la durée :

- disposer d'une pile logicielle à jour et soutenue en MCO/MCS (condition d'homologation et par conséquent exigence déjà en vigueur pour les hébergements actuels)
- disposer de scripts de déploiements Ruche conformes (ceux de C1NP sont identiques à ceux d'Intradef, exigence déjà en vigueur pour l'hébergement infogérance DR actuel, étendue au VPS)
- s'adosser à l'authentification MindefConnect de l'environnement support (exigence déjà en vigueur)
- exporter ses journaux d'événements applicatifs dans le puits de log dès disponibilité (revient à produire des journaux d'événements qui seront exportés ensuite automatiquement par un agent installé à cet effet)
- instancier à minima l'API REST d'observabilité (l'instrumentation pourra être enrichie via

développement mais c'est laissé à l'appréciation du projet de ses besoins en la matière)

- gérer ses secrets et ses certificats via le service de socle Gestion des secrets (dès disponibilité du service dans cet environnement)

Les services offerts sur la plate-forme PICSEL ont été mis en place pour faciliter le développement et le test des quelques adaptations nécessaires et d'en contrôler la conformité avant déploiement sur C1 DR.

6.1.5.4 Offre VPS DR

Cet hébergement a vocation à être remplacé par C1DR (cf. 6.1.4.3 ci-dessus) à compter de 2024. Compte-tenu des délais courts de mise à disposition des environnements VPS qui la rende inutile, l'offre VPS circuit court n'y sera plus proposée. Les systèmes d'informations qui bénéficient de ce service doivent intégrer la démarche « move to cloud » pour y être transférés d'ici à environ 5 ans, échéance prévisionnelle d'arrêt du service.

Les prestations de la DIRISI concernent la fourniture et l'administration technique des couches basses : machines virtuelles ou physiques (le choix de matériel et d'architecture est à la charge de la DIRISI en fonction de l'analyse du SI), réseau, stockage, sauvegarde du SI (sous réserve de document d'exploitation de sauvegarde compatible fourni par le bénéficiaire), installation et mises à jour anti-virus, serveur de temps, agent d'inventaire logiciel, agents de sécurisation et accès au service de mise à jour de sécurité.

Les serveurs sont initialement livrés avec un système d'exploitation préconfiguré de manière générique par la DIRISI. Des droits restreints sur le VCENTER (arrêt/relation des machines virtuelles) seront fournis au besoin au bénéficiaire.

L'administration technique et fonctionnelle de l'ensemble de la couche applicative (système d'exploitation, logiciels et bases de données) reste à la charge de la direction du projet du bénéficiaire. La MOE (ou TME) agissant pour le bénéficiaire doit recevoir les habilitations nécessaires pour l'accès aux réseaux concernés.

L'ensemble des enregistrements d'exécution (traces, journaux d'événements applicatifs et système, ...) doit être rendu accessible à la DIRISI à des fins d'exploitation de la sécurité.

Document	Date	Origine	Type doc	Portée
Nouvelle offre d'hébergement « Serveur Privé Virtuel circuit court » (VPS circuit court) de la DIRISI diffusée par note 406395 /ARM/DIRISI/SCOE/EXP/NP du 24 avril 018	24 avril 2018	DIRISI	Note	Intradef
<i>Commentaire : Cette note décrit les modalités de la nouvelle offre permettant de disposer de machines virtuelles en délai rapide inférieur à un mois.</i>				

6.1.5.5 Hébergement des données de santé (HDS)

La plateforme Hébergement des Données de Santé (HDS) a été mise en place par la DIRISI pour assurer l'hébergement de données de santé (données à caractère personnel dites sensibles) et l'infogérance des systèmes d'information du SSA qui les produisent. Cette plateforme hébergée au CNMO-SI de Suresnes est un sous-ensemble sécurisé de l'Intradef ayant obtenu la certification ISO 27001 puis la certification HDS.

Le périmètre de la certification HDS couvre toutes les activités métiers d'hébergement et d'infogérance du CNMO-SI Suresnes jusqu'au routeur d'entrée du Datacenter :

- Les machines physiques et bases de données hébergeant le(s) futur(s) SI et les données de santé ;
- Les éléments de l'infrastructure technique concourant à l'hébergement des SI qui accèdent aux données de santé ;

- Le processus de sauvegarde et de conservation des données de santé ;
- L'exploitation technique ;
- Les plateformes de production, de recette et d'essais.

Document	Date	Origine	Type doc	Portée
Directive CNMO-SI S n°142 relative aux conditions générales d'hébergement des systèmes d'information de santé	18 juin 2019	DIRISI/ CNMO-SI S	Directive	Intradef - Données de santé

Commentaire : cette directive décrit les modalités d'hébergement d'un SI de santé dans le cadre du CNMOS- SI de Suresnes, hébergeur de données de santé certifié. Elle précise les procédures opérationnelles, les rôles des acteurs en accord avec le cadre réglementaire d'hébergement de données de santé. Elle décrit l'offre d'infogérance mis en œuvre par la DIRISI.

6.1.5.6 Hébergement Salle Blanche DR (réservé aux besoins en matériel spécifique)

Sous réserve d'obtention d'une dérogation permettant le recours à un tel hébergement, les prestations Salle Blanche de la DIRISI consistent en la fourniture d'un emplacement au sein d'une architecture matérielle DIRISI existante, dans une salle serveur climatisée avec accès aux réseaux électriques et informatiques.

L'achat, la livraison, l'installation, la maintenance et l'administration technique et fonctionnelle du matériel et des logiciels (y compris la sauvegarde, la restauration et le soutien en cas de défaillance) incombent entièrement au bénéficiaire.

Il incombe également au bénéficiaire de prendre attaché avec la DIRISI afin de bénéficier de l'installation de l'agent d'inventaire.

Le matériel fourni par le bénéficiaire doit obligatoirement être compatible avec les structures DIRISI. La DIRISI agissant pour le bénéficiaire doit recevoir les habilitations nécessaires pour l'accès aux datacenters et aux réseaux concernés.

L'ensemble des enregistrements d'exécution (traces, journaux d'évènements applicatifs et systèmes, ...) doit être rendu accessible à la DIRISI à des fins d'exploitation de la sécurité.

Cette offre de service reste soumise à l'approbation technique de la DIRISI dont les modalités sont décrites dans le guide et les conditions générales d'hébergement.

6.1.5.7 Hébergement sur SIE (Intradef Embarqué)

Les infrastructures embarquées du SIE permettent l'hébergement d'applications locales depuis la version Baltique. Ces infrastructures apportent des ressources limitées lié aux contraintes d'environnement (espace en baie, énergie, refroidissement, réseau contraint).

Le SIE offre 2 niveaux d'hébergement :

- intégré (mutualisation des services : frontal web, bases de données, télé-déploiement, etc.) ;
- hébergé (mise à disposition d'un espace pour une machine virtuelle entièrement gérée par la direction d'application).

Les directions d'application sont invitées à contacter l'équipe SIE pour connaître les spécifications à jour de l'hébergement sur SIE à prendre en compte.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°236 – Exploitation et soutien des systèmes d'hébergement mutualisé embarqué (SHeMe)	01 mars 2018	DIRISI	Doc	SIE

Commentaire : cette directive sera mise à jour en 2024 et complétée d'un guide de gouvernance et de recommandation au développement des applications embarquées.

6.1.5.8 Hébergement de développement

Partie intégrante de l'offre de service Cloud (cf. 3.2.1.2), la composante PICSEL (Plateforme Interarmées pour héberger la production Continue sécurisée des SI Et Logiciels) met à disposition des Responsables de conduite de Projet, des Responsables Technique de Système et des Responsables de Réalisation de Projet des Directions d'application (DA), de projet (DP) ou de programme numérique une infrastructure Diffusion restreinte (DR) hors espace de confiance.

Ceci permet de répondre aux enjeux de maîtrise induits par les activités de développement et d'expérimentation tout en donnant plus de libertés aux équipes projet et en facilitant l'accès aux partenaires industriels dans les locaux du MinArm. Elle met enfin le contrôle qualité indispensable au projets et programmes numériques du Ministère des Armées (MinArm) avant leur installation sur les environnements cibles.

PICSEL permet d'accélérer les étapes de développements, de validation / qualification et de mise à jour des applications (dont le move to cloud) avant le passage en intégration, pré-production et production de leurs applications sur C1DR ou C1NP. PICSEL doit également dérisquer et banaliser ces opérations et alléger les charges d'exploitation dans la durée.

Les standardisations et les contrôles effectués doivent enfin, par les garanties qu'ils apportent, permettre d'alléger les processus de gouvernance actuels associés à ce passage.

PICSEL propose des ressources informatiques sous forme de moyens, d'outils et d'espaces de développement (dénommés « zones projet ») :

- accès rapide à des ressources et en libre-service pour mener des travaux de développement, d'expérimentation ou de qualification dans le cadre d'un projet préalablement validé par la DSI d'appartenance ;
- mise à disposition d'outils et de services représentatifs des services de la production C1DR et C1NP paramétrés selon les normes du Ministère, administrés et exploités pour mener ces travaux ;
- des moyens et outils aux directions d'application pour réaliser un premier niveau de validation et d'intégration ;
- des moyens et outils aux exploitants et aux RSSI-A de s'assurer de la qualité des applications et services (qualité, sécurité, exploitabilité) avant qu'ils ne soient déployés dans les environnements cibles et in fine en production ;
- une chaîne CI/CD DevSecOps vers les environnements cibles (C1NP et C1DR et environnement historique DR dans une moindre mesure, travaux en cours) ;
- mutualisation (en cours) de la gestion des dépôts de binaires de développement ;
- support à l'utilisation des services via une base de connaissance et une équipe support.

Cette plateforme est par nature en constante évolution : son catalogue de services s'enrichit au fur et à mesure des décisions et des orientations techniques de la DSI Socle en réponse aux besoins exprimés par les DA/DP et l'ensemble des entités de développement du Ministère. Elle évolue également pour intégrer les évolutions et amélioration des services cloud offerts par les plateformes C1NP et C1DR qui y sont développés. Elle doit notamment reprendre l'ensemble du périmètre couvert par les SHEM Dev en ce qui concerne les activités de développement. L'intégration des capacités de tests de charges menées par le BEEI du Service projets de la DIRISI est également en cours d'étude.

Bien qu'il soit possible d'exposer sur Intradef les systèmes d'information et services qui y sont développés ou expérimentés, ceci doit se limiter à quelques utilisateurs à des fins de tests et de validation. PICSEL (comme toute plateforme de ce type) n'est pas destinée à héberger ou exposer des systèmes d'information ou des services en production utilisés en situation réelle depuis Intradef, même si l'accès est limité à une population restreinte.

6.1.6 Hébergement sur Internet

Périmètre	Offre	Utilisation/Restriction	Statut	Portée
Hébergement de production / pré-production / intégration / développement	HELISS NG	HELISS NG va être remplacé par C1 NP. Les SI hébergés seront progressivement migrés sur C1 NP dès son ouverture. HELISS NG sera décommissionnée fin 2024.	D / S	Internet
<i>Commentaire : les systèmes d'information visant un hébergement Internet sur plate-forme ministérielle sont désormais programmés pour être déployés sur C1NP dès disponibilité.</i>				
Hébergement de production / pré-production / intégration / développement	PHEBIA	Sera dé-commissionnée fin avril 2024. N'est plus ouverte aux nouveaux SI à partir de janvier 2023.	I / N	Internet
Hébergement de production / pré-production	C1 NP	Deviendra recommandé dès la mise en production en 2024.	R / S	Internet
Hébergement de production	C3 Internet	Soumis à visa Cloud DGNUM	A / N	Internet

Document	Date	Origine	Type doc	Portée
Instruction ministérielle n°2010 /DEF/DGSIC/NP relative à la mise en œuvre de services en ligne ou de sites internet par le ministère de la défense diffusée par note n°458//DEF/DGSIC/DG/NP du 2 août 2016	2 août 2016	DGSIC	IM	MinArm
<i>Commentaire : cette IM précise les modalités de demande ou de renouvellement d'agrément pour tout site internet du ministère des armées, réseaux sociaux inclus, en déclinaison de la circulaire du Premier ministre n° 5574/SG du 16 février 2012 relative à l'Internet de l'État.</i>				
Politique d'hébergement des SI et des données sur INTERNET Edition approuvée le 18/07/2022 et diffusée par la note N°255/ARM/DNUM/SDTN/NP	18 juillet 2022	DNUM	Politique	Internet
<i>Commentaire : Cette politique abroge les directives provisoires précédentes (Offres IaaS/PaaS et SaaS)</i>				
Directive DGSIC n°13 sur la sécurité des accès aux services de l'Internet et de l'hébergement des services Internet du ministère	30 juin 2010	DGSIC	Directive	MinArm
<i>Commentaire : Règles applicables aux accès au réseau et aux services de l'Internet ainsi qu'en matière d'hébergement de services internet. La partie hébergement des services Internet sur l'internet maîtrisé est traitée plus spécifiquement par la Directive DNUM n°44.(voir ci-dessous)</i>				

6.1.6.1 Hébergement Internet mutualisé – HELISS-NG

Cet hébergement est remplacé par C1NP (cf.6.1.5.2 ci-dessous) à compter de 2024. Les systèmes d'informations qui bénéficient de ce service doivent intégrer la démarche « move to cloud » pour y être transférés d'ici à fin 2024, échéance d'arrêt du service.

Document	Date	Origine	Type doc	Portée
Conditions générales d'hébergement d'un SI NP (Internet) par la DIRISI diffusées par note n°414370/ARM/DIRISI/SCOE/EXP/NP du 08 novembre 2017	8 nov. 2017	DIRISI	Note	Internet
<i>Commentaire : cette note décrit les conditions générales d'hébergement d'un système d'information NP Internet dans le cadre de l'offre de service Heliss NG de la DIRISI, la sécurité et les obligations liées à cet hébergement.</i>				
Directive DGSIC n°32 portant sur la sécurité de l'hébergement des SI au sein du ministère <i>Cf. 4.8.7 Hébergement / Virtualisation</i>	11/03/2014	DGSIC	Directive	MinArm
<i>Commentaire : applicable à l'opérateur, et aux systèmes informatiques hébergés, en recommandation pour les applications ayant vocation à être hébergée à l'extérieur du ministère.</i>				
Directive DGSIC n°13 sur la sécurité des accès aux services de l'Internet et de l'hébergement des services Internet du ministère <i>(Cf. 6.1.5 ci-dessus)</i>	30 juin 2010	DGSIC	Directive	MinArm

6.1.6.2 Hébergement C1 NP

Partie intégrante de l'offre de service Cloud (cf. 3.2.1.2 Démarche et principes liés), C1NP est destiné à remplacer au premier semestre 2024 l'hébergement en infogérance NP (cf. 6.1.5.1 ci-dessus). Dès lors, tous les nouveaux systèmes d'information requerrant ce niveau de service y seront hébergés.

Construit dans une recherche de maîtrise, de standardisation et d'automatisation, C1 NP, tout comme C1 DR, vise avant tout à simplifier et accélérer la mise en production des systèmes d'information mais ne modifie pas fondamentalement les principes et le cadre technologique en vigueur en œuvre sur Heliss NG : hébergement infogéré de machines virtuelles avec les systèmes d'exploitations durcis du Ministère. Les services d'authentification et d'échanges avec Intradef y seront également disponibles (PAPI v2.1, PEM Internet, Acheron, messagerie, MindefConnect Internet).

Il apporte toutefois une extension des technologies acceptées et un raccordement automatisé à un panel de services du socle étendu (NTP, DNS, sauvegarde, dépôts de mise à jour MEDUSA, antivirus, gestion des licences Windows et RedHat, supervision, orchestrateur Ruche identique à celui du C1DR, inventaire, comptes de services ainsi que gestion des secrets et des certificats non exposés sur Internet, puits de journaux d'évènements applicatifs et système). D'autres services seront progressivement ajoutés à la liste en cohérence avec C1 NP et PICSEL (stockage objet type IRIS, contrôle de conformité, hébergement en orchestration de conteneurs ...).

La démarche de cloudification impose au système d'information de respecter quelques exigences qui sont rappelées ci-après et qui sont destinées à faciliter les automatisations et l'exploitabilité, donc améliorer le niveau de service offert, et d'en conserver la maîtrise dans la durée :

- disposer d'une pile logicielle à jour et soutenue en MCO/MCS (condition d'homologation et par conséquent exigence déjà en vigueur pour les hébergement actuels)
- disposer de scripts de déploiements Ruche conformes (ceux de C1NP sont identiques à ceux d'Intradef)
- s'adosser à l'authentification MindefConnect Internet (exigence déjà en vigueur)
- exporter ses journaux d'évènements applicatifs dans le puits de log
- instancier à minima l'API REST d'observabilité (l'instrumentation pourra être enrichie via développement mais c'est laissé à l'appréciation du projet de ses besoins en la matière)
- gérer ses secrets et ses certificats non exposés sur Internet via le service de socle Gestion des secrets.

Les services offerts sur la plate-forme PICSEL ont été mis en place pour faciliter le développement et le test des quelques adaptations nécessaires et d'en contrôler la conformité avant déploiement sur C1 NP.

6.1.6.3 Hébergement PHEBIA sur Internet

Cette offre est actuellement en fin de vie et sera dé-commissionnée fin avril 2024. Elle n'est plus proposée aux nouveaux SI depuis janvier 2023 qui, conformément à la stratégie Cloud du ministère, sont orientés soit vers l'offre C1 NP soit vers l'offre C3 Internet. Les systèmes d'informations qui bénéficient encore de ce service doivent intégrer la démarche « move to cloud » pour rejoindre l'offre C3 Internet ou, éventuellement C1NP d'ici à fin avril 2024, date à laquelle le service sera définitivement arrêté.

Cette plateforme était de type Cloud en libre-service. Elle est physiquement hébergée dans le datacenter de Suresnes de la DIRISI et est exploitée à distance par un sous-traitant de la DIRISI.

La DIRISI n'assure ni l'infogérance, ni l'administration de la sécurité des différents SI hébergés sur PHEBIA.

6.1.6.4 Recours offre C3 Internet

Le recours à un service cloud de type IaaS/PaaS est subordonné à un visa de la DGNUM. Ce recours doit se faire via le vecteur contractuel interministériel UGAP. La DIRISI est seule habilitée à activer ce levier pour le ministère des armées.

Le recours à un service cloud en mode SaaS, que ce soit via le contrat OURANOS ou via les contrats d'unité d'œuvre, ou tout autre mode de contractualisation, est subordonné à une demande de visa auprès de la DGNUM. Un tel hébergement doit remplir certaines obligations liées à la souveraineté et la sécurité, RGPD inclus.

Dans ce cadre, un avis du SC²A est obligatoire pour tout système déployé en offre C3 internet mettant en œuvre des interfaces avec des systèmes d'informations ou composants déployés sur des hébergement MinArm (utilisation de passerelles d'échanges, mise en œuvre de flux de données inter segments, accès depuis des postes ISPT intradef, consommation ou exposition de services). Pour les autres systèmes d'information, un avis contradictoire du SC²A pourra être demandé par la DGNUM à fin d'obtention du visa Cloud requis. Ce processus n'exonère pas le projet de conduire une démarche d'homologation.

Document	Date	Origine	Type doc	Portée
Politique d'hébergement des SI et des données sur INTERNET Edition approuvée le 18/07/2022 et diffusée par la note N°255/ARM/DNUM/SDTN/NP	18 juillet 2022	DNUM	Politique	Internet
<i>Commentaire : Cette politique abroge les directives provisoires précédentes (Offres IaaS/PaaS et SaaS)</i>				
Circulaire n° 6282/SG du 5 juillet 2021 portant la doctrine d'utilisation de l'informatique en nuage de l'Etat	5 juillet 2021	PM	Circulaire	Toute administration
<i>Commentaire : cette circulaire prévoit que l'administration en charge du système choisit la solution adaptée en fonction de ses propres critères et qu'elle doit privilégier une offre qualifiée et immunisée aux réglementations extracommunautaires</i>				
Référentiel d'exigence Prestataires de services de l'information en nuage (SecNumCloud) de l'ANSSI (version 3.2 du 8 mars 2022)	8 mars 2022	PM	Référentiel	Toute administration

6.1.7 Hébergement mutualisé sur les intranets classifiés

L'architecture de tout système d'information (architecture applicative et intégration sur le/les réseaux supports) doit être validée par la gouvernance technique (cf. 1.4 Gestion et gouvernance du CCT) (sur dossier ou en présentation) au moment de la revue de conception générale.

Document	Date	Origine	Type doc	Portée
Conditions générales d'hébergement de systèmes d'information par la DIRISI sur les réseaux classifiés (CD-SF) : v2 du 1 ^{er} janvier 2021.	1 ^{er} janvier 2021	DIRISI	Guide	S-SF
Directive DIRISI n°216 relative à l'exploitation et au soutien du Module d'Hébergement Sécurisé sur le niveau CD-SF	4 juillet 2017	DIRISI	Directive	S-SF

Hors cas dérogatoire, l'hébergement d'applications et de systèmes d'information au sein du SIA est structuré autour des moyens ISHM/MHS et permet ainsi aux applications de venir consommer l'offre de services proposée par le SIA (services communs, sauvegarde, stockage, ...). La consommation des services du SIA ne présume pas du niveau d'infogérance proposé par l'opérateur à la direction d'application (Infogérance ou VPS).

L'hébergement d'une application au sein du SIA doit respecter certaines contraintes et consignes :

- l'application doit respecter le Référentiel d'hébergement, document mis à jour à minima annuellement. Ce document est disponible auprès du programme SIA ;
- l'application peut consommer l'ensemble des services communs du socle étendu fourni par le SIA.
- l'application est hébergée sur un OS basé sur un « *template* » fourni par le SIA.

Hors dérogation du programme SIA et de l'opérateur DIRISI, il n'est pas prévu d'offre Salle Blanche sur les intranets SIA classifiés en dehors du déploiement des instances d'hébergement du SIA.

6.1.8 Informatique décisionnelle

Voir aussi §3.2.6 Informatique décisionnelle traditionnelle (ou BI Corporate)

6.2 Opérations – processus

6.2.1 Gestion des configurations

La mise en place de processus et d'outils de gestion des configurations doit permettre de connaître la composition exacte et à tout moment du parc informatique de responsabilité DIRISI et d'établir des analyses d'impact avant chaque changement.

Pour être efficace, la gestion de configuration doit définir :

- les éléments de configuration qui doivent être inventoriés et suivis en regard des services et processus qu'elle alimente ;
- les processus qui permettront de maintenir à jour les configurations ;
- les acteurs du processus.

La DIRISI met en œuvre une gestion des configurations sur le périmètre des systèmes d'informations métiers hébergés par la DIRISI.

Le contrôle qualité opéré sur PICSEL et l'API d'observabilité (cf. 6.2.7.4) désormais requis pour les hébergements C1NP et C1DR ainsi que le SI Conformité ont vocation à contribuer à cette gestion de configuration.

6.2.1.1 Base de connaissance de gestion CMDB [BCA]

La base de gestion des configurations (CMDB) a vocation à intégrer tous les systèmes d'informations métiers et services hébergés par la DIRISI. Elle permettra d'établir la photo du parc matériel et applicatif, de mener des campagnes de rationalisation, d'améliorer la gestion des obsolescences logicielles et le suivi des évolutions.

Document	Date	Origine	Type doc	Portée
GUIDE EMO.GUI.R4.012 Description des systèmes d'Information dans la CMDB version 1.0	01/08/2022	DIRISI	Guide	MinArm

6.2.1.2 Inventaire [INV]

Afin d'alimenter la CMDB de l'hébergement, la DIRISI collecte les informations logicielles et matérielles sur les serveurs Windows et Linux.

L'alimentation de la CMDB Bureautique utilise quant à elle les remontées MECM pour les postes utilisateurs.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Inventaire	MECM	Microsoft	Limité aux clients WINDOWS depuis 2019	R / S	MinArm
Inventaire	ServiceNow	ServiceNow	Utilisé par l'opérateur pour alimenter sa CMDB	R / S	Intradef
Inventaire	OCS Inventory	OCS Inventory Team	-Dans le cas de réseaux non opérés par la DIRISI et ne disposant pas d'une infrastructure d'inventaire déjà en place. -pour les réseaux opérés ou sous la responsabilité de la DIRISI (notamment l'intradef), soumis à la stricte approbation de la DIRISI	A / S	MinArm
Inventaire	GLPI	GLPI	Uniquement sur des parcs non gérés par la DIRISI. Les versions antérieures à la 10.0.3 sont interdites car présentant 2 vulnérabilités critiques.	A / S	MinArm

6.2.1.3 Dépôt d'artefacts

Le ministère doit disposer d'un service qui centralise et sécurise ses artefacts binaires. Ce service a également vocation à faciliter sur l'Intradef la récupération et la mise à jour des binaires, bibliothèques et packages issus d'internet ou mis à disposition suite à des développements internes ou de MOI Tiers. Il permettra de cartographier les binaires utilisés dans les SI afin d'alerter les responsables des SI en cas d'utilisation de composants obsolètes, interdits ou considérés comme dangereux.

C'est la brique de socle MEDUSA qui doit porter ce service. Elle reprendra l'ensemble du périmètre couvert actuellement par DECOS et l'étendra progressivement, tant en termes d'environnement (PICSEL, C1NP et Intradef en 2024) qu'en termes de binaires proposés, les premiers ajoutés étant les templates d'OS durcis.

Pour ces derniers, en attendant l'ouverture du service MEDUSA, ils seront transitoirement disponibles viaRUCHE.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Dépot correctif de sécurité	DECOS-S	DIRISI	<i>Cf. 4.8.4 Maintien en condition de sécurité (MCS) - composant technique</i>	R / S	MinArm
Dépot	MEDUSA	MinArm	Mise à jour Et Dépôt Unifié de Systèmes et Applicatifs	E / E	MinArm
Reperoire d'artefacts	Artifactory	JFrog	Assujetti à tout autre cadre d'emploi que MEDUSA-RUCHE - nécessité de justifier le cadre d'emploi	A / E	MinArm
<i>Commentaire : L'objectif pour le Ministère est d'acquérir la maîtrise des binaires de toutes natures mis en œuvre sur ses réseaux et de se constituer une source de vérité unique dans ce domaine. En conséquence, ajouter un autre dépôt vient à l'encontre de cette démarche et ne peut s'entendre que dans des environnements non couverts actuellement et dans l'optique d'une rejointe à terme. En conséquence, ceci nécessite d'être dûment justifié.</i>					

6.2.2 Gestion des demandes

6.2.3 L'hébergement d'un nouveau SI fait l'objet d'une demande dématérialisée dans le catalogue de service de la DIRISI.Déploiement / Distribution / Orchestration

Dans un objectif de maîtrise des hébergements et des postes de travail, de réduction des délais et des coûts humains d'installation, de mise à jour et d'exploitation, le ministère s'oriente vers une automatisation et une orchestration des déploiements et de la distribution des logiciels.

Sur les systèmes Windows, elle s'appuie principalement sur WSUS et MECM (excluant de facto le recours aux technologies de type Java Webstart par exemple). Dans le cadre de la démarche de cloudification et dans la poursuite du projet Ruche, les installations manuelles des systèmes d'informations sont remplacées par une orchestration à base de technologie ansible et de dépôts de binaires maîtrisés.

Ceci a pour objet d'éviter les actions manuelles, sujettes à erreurs, en suivant une documentation lourde à réaliser et difficile à fiabiliser, à standardiser les pratiques entre Datacenter notamment, à rendre reproductibles ces opérations délicates et à réduire drastiquement les délais de mise à disposition.

Ce mode de distribution s'applique aux durcissements de sécurité, aux briques logicielles standards du CCT et au déploiement des systèmes d'information.

Ce mode de déploiement est désormais obligatoire pour les systèmes d'information en infogérance sur le réseau DR. Il le sera également dans les hébergements cloudifiés C1NP et C1DR, y compris pour les systèmes en VPS. Pour les niveaux VPS actuel et salle blanche, il devient recommandé hors dérogation du SC²A : outre les gains pour les TME, ceci vise à préparer la migration inéluctable vers les hébergements cloudifiés.

Limitée dans un premier temps aux seuls systèmes en infogérance sur le réseau DR, l'infrastructure Ruche va désormais être également accessible aux équipes projets de ces systèmes sur les plates-formes d'intégration ainsi qu'aux exploitants des systèmes d'information en VPS via demande officielle (NEMO) vers la DSI Socle. Les autres devront avoir recours à une machine virtuelle dédiée destinée à exécuter un moteur ansible dédié (exécutable ansible seul, AWX si nécessaire).

Ce mode de déploiement s'appuie notamment sur :

- une bibliothèque de « collections Ansible » ministérielle qui sera progressivement enrichie et disponible en libre service sur Intradef ;

- un kit de développement contenant la structure attendue pour le projet ;
- le « guide d'utilisation du modèle de projet Gitlab » associé et deux projets de démonstration est également disponible.

Une liste synthétique des collections, des versions de middleware prises en charge et leur état sont disponibles sur la page de la météo des collections Ruche.

Une collection développée par un projet peut être proposée pour intégrer la bibliothèque : elle pourra alors être validée, adaptée à une utilisation mutualisée et intégrée.

Cette démarche de standardisation et d'automatisation, alignée sur les principes de l'infrastructure as code sera poursuivie notamment dans les domaines du provisionnement des ressources de type machines virtuelles via, par exemple, le recours à Terraform (dans le cadre du SIA ou des C1 DR et C1 NP) ou dans celui de l'orchestration de conteneurs.

Document	Date	Origine	Type doc	Portée
GUIDE « offre d'automatisation des déploiements de SI) EMO.GUI.R4.017 version 1.0	01/10/2022	DIRISI	Guide	MinArm
GUIDE « utilisation du modèle de projet Gitlab pour la plateforme RUCHE » EMO.GUI.R4.015 version 1.0	01/08/2022	DIRISI	Guide	Intradef

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Déploiement	MECM / WSUS	Microsoft		R / S	Intradef
Déploiement	MECM / WSUS	Microsoft		A / S	S-SF SIA Frops
Déploiement	OCS Inventory	OCS Inventory Team	Assujetti aux configurations projetables SIA et dans le cas de réseaux non opérés par la DIRISI et ne disposant pas d'une infrastructure de déploiement déjà en place. Toute autre utilisation est soumise à la stricte approbation de la DIRISI	A / S	MinAr m
Orchestration	Puppet	Apache	Sur SIE (version Baltique), pour la distribution des configurations. A titre transitoire, sur environnement S2NA	A / -	Intradef dont SIE et S2NA
<i>Commentaire : assujetti au titre de l'existant actuel, dans une optique à terme de rejointe d'une cible Ansible.</i>					
Déploiement	RUCHE	Minarm		R / S	MinAr m
<i>Commentaire : RUCHE a pour vocation à fournir des services et une plateforme autour de la solution Ansible pour l'automatisation des déploiements de SI. Il vise un service optimisé aux exploitants et un changement dans le mode de livraison des SI infogérés. (cf. ci-dessous pour un premier niveau d'offre de service)</i>					
Orchestration	Ansible	REDHAT	Pour l'automatisation de l'installation et du déploiement de tout nouveau SI	R / S	Intradef Internet
<i>Commentaire : Ansible (au travers de Ruche, à chaque fois que le service est disponible sur le réseau support) est désormais le mode requis d'installation et de mise à jour des nouveaux systèmes d'information sur les plateformes de la DIRISI comme pour celles de l'AND.</i>					
Provisionnement	Terraform	HashiCorp	Pour l'automatisation du provisionnement des ressources de type VM	A / -	Minarm

Génération d'images	Packer	HashiCorp	Génération d'images machine identiques multi plateformes	R / -	MinArm
---------------------	--------	-----------	--	-------	--------

6.2.4 Gestion du stockage

Dans les structures d'hébergement de l'Intradef, la gestion du stockage est actuellement assurée par les outils déployés dans chaque Infrastructure d'hébergement.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Stockage SAN	Pure Storage	Pure Storage	Structures d'hébergement	R / S	Intradef
Stockage SAN	Hitachi	Hitachi	Structures d'hébergement	R / S	Intradef
Stockage NAS	Hitachi	Hitachi	Structures d'hébergement	A / S	Intradef
Stockage NAS	Netapp	NetApp	Structures d'hébergement	A / S	Intradef
Stockage Objet	Scality Ring	Scality	Assujetti à IRIS	A / S	Intradef

6.2.5 Synchronisation / RéPLICATION / Déduplication

Pas de référence identifiée à ce jour.

6.2.6 Sauvegarde / restauration

Sur Intradef, les structures d'hébergement et serveurs de proximité peuvent avoir deux types de données à sauvegarder : les bases de données et les fichiers. Les premières sont sauvegardées sur bande au moyen du logiciel Time Navigator d'ATEMPO. Les seconds sont sauvegardés via ADA d'ASG.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Sauvegarde	Time Navigator (TINA)	ATEMPO	Structures d'hébergement : Pour les données structurées avec sauvegarde sur bandes Par défaut pour l'offre d'hébergement VPS	R / S	Intradef
Sauvegarde	MIRIA (ADA)	ASG	Sauvegarde serveur de proximité	R / S	Intradef
Sauvegarde	VEEAM	VEEAM Software	<i>pour les recommandations sur les versions voir le détail en annexe 8.2.1 Pile logicielle : liste des produits</i>	R / S	Intradef S-SF SIA FrOps
Sauvegarde	Bareos	Bareos	Assujetti au contexte SIE : Outil sous licence libre AGPL v3, utilisé sur le SIE Baltique.	A / S	SIE
Sauvegarde	Elastic Curator	Elastic	Gestionnaire de snapshots Elasticsearch/Opensearch	A/N	Intradef S-SF SIA FrOps

Sauvegarde du poste de travail :

Pour la sauvegarde du poste de travail, certains organismes (DGA, SIMMT...) ont mis en place une solution basée sur la solution LINA de la société ATEMPO.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Sauvegarde	Live Navigator (LINA)	ATEMPO	Solution de sauvegarde des postes de travail sur le périmètre DGA	A / S	Intradef

6.2.7 Observabilité

L'un des enjeux de la démarche de cloudification (cf. 3.2.1.2) est l'accroissement de maîtrise sur les infrastructures et systèmes d'information hébergés. Outre les aspects de conformité et de sécurité, la visibilité sur leur fonctionnement est également un axe qui doit être développé.

La capacité d'un système d'information à fournir des informations sur son fonctionnement interne à partir d'éléments qu'il émet s'appelle **l'observabilité**. Elle facilite la supervision et permet une identification et une résolution des problèmes plus rapides voire automatisées en vue de répondre aux attentes des utilisateurs et d'atteindre les niveaux de services (SLA ou Service Level Agreements) et autres exigences métier.

Le bénéfice principal de l'observabilité est qu'un système plus observable est plus facile à comprendre (en général et en détails), plus facile à superviser, plus facile et plus sûr à mettre à jour et plus facile à réparer.

Par extension, l'observabilité fait également référence aux outils logiciels et aux pratiques permettant d'agréger, de corrélérer et d'analyser un flux continu de données de fonctionnement des applications associées à celles du matériel et du réseau sur lesquels elles s'exécutent.

L'observabilité applicative se concentre sur 4 types principaux de données, dont les 3 communément désignés comme étant **les 3 piliers de l'observabilité** : les journaux d'évènements applicatifs, les métriques et les traces applicatives auxquels s'ajoutent les dépendances :

- **journaux d'évènements applicatifs** (ou **logs**) : enregistrements granulaires, horodatés, complets et immuables des événements applicatifs qu'on peut trouver sous 3 formats : texte, structuré ou binaire. Parmi tant d'autres, les journaux d'événements applicatifs peuvent être utilisés pour créer des enregistrements haute fidélité, milliseconde par milliseconde de chaque événement, complets avec le contexte associé que les développeurs peuvent « rejouer » à des fins de recherche de panne ou de débogage.
- **métriques** : appelées parfois métriques « *time series* », ce sont des mesures fondamentales de la santé de l'application et du système sur une période de temps donnée, par exemple combien de mémoire ou de capacité de calcul une application utilise sur une période de 5 minutes ou encore avec quel délai de réponse une application répond lors d'un pic d'utilisation.
- **traces** : les traces enregistrent le « voyage » de bout en bout de chaque requête utilisateur, depuis son interface ou son application mobile via toute l'architecture distribuée jusqu'au retour de la réponse.
- **dépendances** : également appelées cartes de dépendances, elles indiquent de quelles autres composantes, applications ou ressources technologiques dépend une application.

Une fois collectées, ces informations sont agrégées en temps réel pour fournir une **information complète et contextuelle** : le **quoi**, **où** et le **pourquoi** de chaque événement. Ces informations multiples peuvent être découvertes automatiquement par des systèmes qui, pour traiter cette masse de données, peuvent s'appuyer sur de l'intelligence artificielle (AIOps) afin d'extraire des signaux – l'indication d'un problème réel – au milieu du bruit.

L'observabilité et la supervision, qu'elle soit applicative⁵³ ou réseau⁵⁴, sont deux concepts distincts mais complémentaires. La supervision collecte et analyse des données connues comme étant liées à des problèmes de performance de l'application, du système ou du réseau (les **knows unknowns**: des conditions exceptionnelles qu'on sait devoir surveiller) alors que l'observabilité donne aux équipes des informations contextuelles nécessaires pour identifier et résoudre au plus tôt des problèmes dont elles n'étaient pas conscientes (**unknown unknowns**) et permettre des infrastructures de remédiation automatique et des infrastructures d'auto réparation des applications.

Le Ministère, disposait déjà de capacités de supervision grâce au projet PISARO :

- **PISARO Supervision** (aspect *métriques*) : surveillance de l'état des infrastructures des SI hébergés par la DIRISI,
- **PISARO Métrologie** (aspect *traces*) : suivi précis et proactif du fonctionnement des SI à fort enjeu de disponibilité.

En capitalisant sur ces capacités, le Ministère va étendre la démarche afin de prendre en compte :

- l'ensemble des dimensions de la supervision et de l'observabilité,
- toutes les plateformes composant le cloud (C1NP, C1DR et PICSEL – y compris pour l'hébergement en orchestration de conteneurs - ainsi que l'hébergement historique DR pour partie).

Pour marquer cette extension de périmètre, l'ensemble des composantes contributrices (dont celles de PISARO) est regroupé au sein du projet « Observabilité ».

6.2.7.1 Journaux d'événements applicatifs et système

Document	Date	Origine	Type doc	Portée
Recommandations de sécurité pour l'architecture d'un système de journalisation ANSSI-PA-012/ANSSI/SDE du 28/01/2022 https://www.ssi.gouv.fr/uploads/2022/01/anssi-guide-recommandations_securite_architecture_systeme_journalisation.pdf	28/01/2022	ANSSI	Guide	Toute administration

Dans le cadre de la cloudification en général et du projet « Observabilité » en particulier, une infrastructure adossée à Elastic a été mise en place sur PICSEL et sera intégrée à la composante C1NP. Son déploiement est également planifié pour 2024 sur la composante C1DR. Les systèmes d'information et services y déverseront leurs journaux d'événements applicatifs et système, permettant ainsi une consultation et une interrogation centralisée. L'adossement au stockage IRIS permettra de les conserver conformément aux délais requis par la réglementation. Enfin, il alimentera les outils de supervision de sécurité.

Plusieurs solutions du socle vont s'appuyer sur cette capacité (dont RUCHE et SARDaC).

⁵³ APM ou Application Performance Monitoring

⁵⁴ NPM ou Network Performance Monitoring

6.2.7.2 Métriques

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
PISARO Supervision	Shinken Enterprise	Shinken	Mise en place pour la supervision des structures d'hébergement et des SI hébergés par la DIRISI. Intégrée à la solution Observabilité.	R / S	Intradef
Supervision/Hypervision	GSYS Solution basée sur Shinken		Solution de supervision apportée (et soutenu) par le SIA	A / S	S-SF SIA FrOps
Supervision/Hypervision	Shinken Enterprise	Shinken		A / N	MinArm
Sonde NRPE	NRPE	Daemon Linux	Agent de supervision NRPE	R / S	MinArm
Sonde NRPE	NSClient ++	NSClient	Agent de supervision NRPE Périmètre de déploiement restreint aux serveurs Windows	A / S	MinArm

S'adressant à l'ensemble des SI des réseaux NP, alimenté par les métriques qu'il collecte, PISARO supervision (intégré à la solution Observabilité) couvre la surveillance du bon fonctionnement d'un système afin de s'assurer de la disponibilité des services, de prévenir les défaillances et de détecter les anomalies. Cette offre s'adresse à l'ensemble des SI du réseau Intradef de la DIRISI.

L'utilisation de PISARO supervision (intégré à la solution Observabilité) permet d'améliorer la disponibilité des SI hébergés en :

- disposant d'une **vue globale** du système d'information et de l'infrastructure IT en **temps réel** ;
- **centralisant** l'ensemble des indicateurs dans une seule console ;
- **rendant compte** des événements impactant la **performance** et la **disponibilité** des services ;
- **prévenant les défaillances** et menant des actions de correction ;
- **aidant au diagnostic** pour l'identification de l'origine des défaillances ;
- **optimisant la disponibilité** des services.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°263 relative à l'exploitation et au soutien PISARO (supervision)	01/11/2019	DIRISI	Directive	Intradef
<i>Commentaire : La directive présente l'architecture générale de la partie supervision de PISARO (métropole et outre-mer). Elle fournit à tous les acteurs des éléments quant à l'exploitation et au soutien de PISARO dans sa fonction de supervision. Elle précise les responsabilités et fonctions accessibles des différents acteurs.</i>				

6.2.7.3 Traces

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
PISARO Métrologie	Dynatrace	DynaTrace	- mise en place pour monitorer les applications identifiées comme critiques par la DIRISI - utilisé aussi par le CASID lors des audits ou assistances des SI confrontés à des problèmes de performances (en	A / S	Intradef

			collaboration avec le BEEI). Intégrée à la solution Observabilité.		
--	--	--	---	--	--

Les traces permettent de mesurer la performance des sessions utilisateurs via le suivi des temps de réponse et la performance des processus métiers via le suivi des transactions, etc.

En complément de la PISARO supervision, l'utilisation de PISARO métrologie (intégrée à la solution Observabilité) offre à la chaîne d'exploitation DIRISI de nouvelles capacités proactives, qui lui permettent notamment de :

- **Mesurer dans le temps la performance** et la disponibilité des systèmes d'information identifiés par le Pôle hébergement comme étant sensibles (en termes de criticité ou de charge d'exploitation induite par un manque de fiabilité) et obtenir une vision du **ressenti utilisateur**
- Fournir matière à des **analyses et rapports approfondis** du comportement de ces systèmes d'information et leur impact du point de vue des utilisateurs
- Suivre les **engagements de service et anticiper** d'éventuels dysfonctionnements.

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°257 relative à l'exploitation et au soutien PISARO (métrologie)	01/11/2018	DIRISI	Directive	Intradef
<i>Commentaire : La directive fournit à tous les acteurs des éléments quant à l'exploitation et au soutien de PISARO dans sa fonction de métrologie. Elle précise les responsabilités des différents acteurs. Elle précise les critères d'éligibilité d'une mise sous métrologie d'un SI et le processus de mise en place. PISARO est intégrée à la solution Observabilité..</i>				

6.2.7.4 Dépendances (C1-NP et C1-DR)

Le suivi des dépendances est adressé travers des informations collectées dans la CMDB de la DIRISI ainsi que, de façon plus dynamique, à l'aide de l'API d'observabilité. Cette dernière a pour objet de :

- Faciliter la récupération d'informations relative à la gouvernance ayant un impact sur les hébergements (trigramme, version, niveau ARR, DSI d'appartenance ...) ;
- Améliorer l'observabilité des systèmes d'information en mettant à disposition un état synthétique de bon fonctionnement et de leur capacité à utiliser les services et autres systèmes d'information dont ils dépendent.

6.2.7.5 Sur les réseaux classifiés

Pas de référence identifiée à ce jour.

6.2.8 PCA/PRA – PCI/PRI - Gestion de crise

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.010 Tests périodiques des Plans de Continuité d'Activité & Plans de Continuité Informatique version 2.0	20/04/2022	DIRISI	Guide	MinArm

Commentaire : Ce guide remplace la directive n°251 et a pour but de fixer les conditions de mise en œuvre des tests périodiques des Plans de Continuité d'Activité (PCA) de l'EMO DIRISI, des pôles opérationnels et des centres nationaux de la DIVOPS, d'une part ; des Plans de Continuité Informatique (PCI) des systèmes d'information (SI) critiques, exploités par la DIRISI au profit de ses clients ou à son propre bénéfice, d'autre part. Il vise donc à décrire les différents types de tests, leur fréquence, le rôle des acteurs, les modalités d'établissement du calendrier des tests et les procédures de compte rendu. Il n'a pas vocation à fournir les modes opératoires de réalisation ni les modèles de rédaction des PCA et PCI.

Voir également § 4.8.2 PCA-PRA

6.2.9 Gestion d'exploitation et des capacités

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion incidents	DIADME	Service Now	Gestion des incidents Basé sur la version UTAH de Service Now	R / S	MinArm

6.2.10 Hypervision

Pas de référence identifiée à ce jour.

6.2.11 Administration réseaux, performance réseaux et Télécommunications

Pas de référence identifiée à ce jour.

6.2.12 Surveillance et métrologie des salles

Pas de référence identifiée à ce jour.

7 CONCEPTION – DEVELOPPEMENT

7.1 Règles générales

Les applications conçues et développées aujourd’hui structurent le système d’information ministériel de demain. La conception d’une nouvelle application doit s’effectuer dans le cadre des concepts fondamentaux définis au §3.2.1.1 *Concepts fondamentaux* (indépendance technologique, rationalisation des techniques utilisées, interopérabilité native).

Dans le cas où le choix s’oriente vers un développement externalisé ou l’acquisition d’un progiciel « sur étagère », outre les concepts ci-dessus, de nombreux principes restent valables.

Cela se traduit par les recommandations suivantes :

- L’approche silo est proscrite, le choix doit être fait dans un contexte global, en tenant notamment compte de l’intégration du nouveau produit dans son environnement applicatif au sein du SI du ministère ;
- Pour les développements externalisés, afin de permettre aux industriels postulants de s’inscrire dans la démarche de rationalisation technique du ministère, le présent CCT (dans sa version NP à diffusion réfléchie) doit être joint au CCTP, en tout ou partie selon les modalités proposées au §1.5 *Prise en compte dans le cadre des cahiers des charges* ;
- Pour les développements internes et externes un passage par le chaîne de pré intégration de PICSEL est requis ;
- Des règles de gouvernance, de conduite de projet ou de prise en compte de la SSI et d’hébergement s’appliquent aux maîtres d’ouvrage faisant réaliser des applications, qu’elles soient ou non basées sur des progiciels du commerce. Des règles d’autres domaines (archivage, etc.) peuvent également s’appliquer.

7.2 Analyse, modélisation

7.2.1 Modélisation métier

La modélisation métier est un préalable à toute démarche d’informatisation. Au sein du ministère des armées, cette démarche, qui s’inscrit dans un cadre étatique, repose sur la description d’un modèle d’entreprise conformément au langage retenu Archimate, et qui couvre quatre axes : Stratégique, Métier, Applicatif et Technique (contre 5 jusqu’à présent, la couche fonctionnelle se retrouvant dans les axes métier, applicatif et technique).

Cette démarche de modélisation est cadrée par un guide destiné aux architectes du ministère des armées.

L’utilisation de ce guide s’accompagne de la mise en œuvre d’outils ministériels accessibles localement sur chaque poste de travail :

- Archi (pour les représentations d’architecture, respect natif du langage Archimate), certains patterns seront fournis au travers de bibliothèques ;;
- CAMUNDA (pour les modélisations des processus, selon le BPMN) ;
- Modélio (pour les diagrammes de données, selon UML) ;
- Draw.IO (pour les phases d’idéation).

Ces outils sont disponibles via le [DIRISI Store sur DIADME](#).

Les travaux de modélisation réalisés dans le cadre d'un projet, de rédaction de schémas directeurs, etc. peuvent être importés dans le référentiel d'architecte d'entreprise (AE). L'alimentation du référentiel AE central se fera en conséquence selon un processus de gouvernance avec des contrôles de cohérence, l'analyse de la pertinence du contenu, notamment au regard des interfaces. La gestion de ce référentiel sera sous MEGA HOPEX.

Le référentiel AE central sera restreint en modification aux urbanistes DGNUM/CASID, un accès sera ouvert aux architectes d'entreprise des DSI Domaines (un par DSI). Les modélisations seront toutefois accessibles en lecture au ministère via un site web généré avec MEGA HOPEX.

Par ailleurs, l'annexe 8.7 Modèles d'architecture du présent CCT présente un catalogue des architectures recommandées, modélisées à l'aide d'un sous-ensemble simplifié et adapté aux besoins du Ministère de la spécification Archimate.

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
ARCHIMATE	Langage de modélisation ouvert d'architecture d'entreprise. Norme technique de l'OpenGroup. Choisi comme un standard recommandé pour décrire les architectures dans le référentiel Otan NAF v4	R	MinArm

Document	Date	Origine	Type doc	Portée
Guide ministériel n°3 « export documentaire du plan d'occupation des sols du ministère de la défense » : édition POS v4.03 mise à jour approuvée le 22 novembre 2017 et diffusée par note n°463/ARM/DGSIC/DG/NP du 22 novembre 2017	22 nov. 2017	DGSIC	Guide POS	MinArm
<i>Commentaire : Ce document décrit l'ensemble de secteurs qui composent le POS.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Modélisation métier	MEGA	MEGA	HOPEX	R	MinArm
Modélisation métier	ARCHI	Archi	Implémente Archimate 3.2, préconisé pour la modélisation d'ensemble des SI.	R	MinArm
Modélisation métier	CAMUNDAMODELER (Open Source Desktop Modeler)	CAMUNDA	Logiciel permettant de modéliser les processus métier au format BPMN 2.0 et les modèles de décision au format DMN 1.1.	R	MinArm
Modélisation métier	MODELIO	MODELIO	Logiciel permettant de modéliser en UML 2.5 (préconisé pour les modèles de classes ou d'activités) 2.5 mais aussi en BPMN 2.0, Archimate 3.2.	R	MinArm
Modélisation métier	DRAW.IO	Diagrams.net (JGraph)	Logiciel permettant de modéliser librement (mode idéation), qui est une alternative à Microsoft Visio avec en natif des artefacts de différents langages de modélisation (UML, BPMN, etc.).	R	MinArm

7.3 Développement

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du ministère. Néanmoins, les documents référencés constituent des guides de règles et bonnes pratiques pour tout développement, à ce titre il est possible d'y faire référence dans les documents contractuels.

Par ailleurs, il est rappelé que de nombreux usages reposent sur le passage par des réseaux contraints, spécificité qu'il importe de prendre en compte dès les phases de développement (cf 5.2.1.45.2.1.4).

7.3.1 Outils de développements internes

7.3.1.1 Environnement DevSecOps ministériel

7.3.1.1.1 Ambitions et orientations DEVSECOPS

Différents travaux sont en cours de réalisation pour consolider la plateforme de développement dotée d'une chaîne DEVSECOPS pérenne au profit de l'ensemble du ministère des armées.

Dans un premier temps, une capacité de déploiement automatisé et d'intégration automatisée a été mise en place sur PICSEL.

Dans un deuxième temps, mise en place progressive d'une capacité d'intégration et de déploiement continu vers les composantes C1NP et C1DR du cloud attendue pour fin 2023.

En parallèle une primo capacité CI/CD sur base d'orchestration de conteneurs a été réalisée sur PICSEL et va être progressivement mise à disposition en attendant l'ouverture du service d'hébergement en orchestration de conteneurs sur C1DR prévu pour fin 2024.

Finalement, une capacité DevSecOps complète sera mise en place.

L'AND participe à ces activités au travers de différents projets dont la plateforme d'intégration (PICSEL⁵⁵) permettant la mise en place d'un IaaS, puis d'un PaaS, à l'usage des équipes de développement et des directeurs d'application. Ces travaux sont réalisés en étroite interaction avec RUCHE, le référentiel unifié de code source mis en place en relation avec le pôle hébergement. RUCHE est le dépôt git national (a minima pour les collections ansible et autres éléments propres aux déploiements).

Offrant une première capacité de CI/CD⁵⁶, la chaîne actuelle comprend :

- La génération à la demande et le management de VPC (Virtual Private Cloud), appelés Zones Projets, permettant aux équipes projet (ou centre de développement / exploitation) d'avoir un environnement de développement, d'expérimentation et à terme de pré-intégration (plateforme PICSEL)
- La mise à disposition d'un orchestrateur de déploiement (Ansible) permettant aux équipes projet d'automatiser leurs déploiements en réutilisant et en spécialisant les productions du pôle hébergement (collections de RUCHE)
- La mise à disposition d'un orchestrateur d'intégration continue (Jenkins en cours de remplacement par Gitlab CI), associé à l'écosystème habituel des chaînes de développement (Analyse statique SonarQube, tests de conformité et de sécurité SCAP...)

⁵⁵ Plateforme InterArmées pour héberger la production Continue Sécurisée des SI Et les Logiciels

⁵⁶ Continuous Integration/Continuous Delivery

- La mise à disposition de dépôts sécurisés et mis à jour (MEDUSA) permettant le déploiement des applications et des machines à utiliser.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement de développement	PICSEL	MinArm	Plateforme DevSecOps de développement et d'expérimentation, assurant le contrôle qualité requis pour un hébergement sur C1DR et C1NP Cf. 6.1.1.86.1.4.8	R / S	MinArm
Environnement de développement	ShemDev	MinArm	Capacité résiduelle de fournitures de ressources à des fins de développement assujettie aux cas d'usage non encore couverts par PICSEL	D / -	MinArm
Gestionnaire de version	Gitlab	Gitlab		A / -	MinArm
Gestionnaire de version	Gitea	Gitea	Gestionnaire de version pour des besoins modestes	A / N	MinArm
Intégration Continue	Jenkins	Licence MIT	Bascule en cours vers GitlabCI sur PICSEL	D / -	MinArm
Intégration Continue	GitlabCI	Gitlab	Assujetti au besoin d'une instance dédiée hors PICSEL ou RUCHE	A / S	Intradef
Qualimétrie	SonarQube	SonarSource	Assujetti au besoin d'une instance hors PICSEL	A / -	MinArm
Orchestration	RedHat automation controller	Red Hat	Assujetti au besoin d'une instance dédiée hors PICSEL ou RUCHE	A / -	MinArm
Orchestration	Molecule	opensource	Utilisation pour test des collections Ansible	A / -	MinArm
<i>Commentaire : Dès lors que la plateforme ministérielle de déploiement automatisé est en capacité d'opérer dans l'environnement considéré, celle-ci doit être utilisée. Les composants ci-dessus complète le dispositif sur les environnements non équipés.</i>					

7.3.1.1.2 Plateforme de développement PICSEL

Pile logicielle : Annexe 8.3 (Cf 8.3.1)

7.3.1.2 Safr@n

SAFR@N est un système de développement pour les applications de type client web, client riche, client nomade encore mis à disposition des entités de réalisation du ministère des Armées (CDAD⁵⁷), autres centres de développement). Cette plateforme est destinée au maintien de SI legacy et interdite pour tout nouveau projet. SAFR@N est maintenu en exploitation en attendant le portage de ses fonctionnalités sur PICSEL.

⁵⁷ Centre de développement des applications de la défense.

7.3.2 Développement en Java

Document	Date	Origine	Type doc	Portée
Guide de règles et de recommandations relatives au développement d'applications de sécurité en Java, https://cyber.gouv.fr/publications/securite-et-langage-java	2009	ANSSI	Guide	MinArm
<i>Commentaire : Ce guide élaboré dans le cadre du projet JAVASEC sous l'égide de l'ANSSI présente des règles et recommandations pour le développement d'applications JAVA avec un bon niveau de prise en compte de la sécurité. Même si ce guide date un peu, nombre de préconisations de développement restent d'actualité. Les éléments de ce guide sont sur le site de l'ANSSI : https://cyber.gouv.fr/publications/securite-et-langage-java</i>				

Le framework Spring est recommandé pour le développement backend en Java. Il est très complet et permet une très grande variété d'intégration avec d'autres framework si besoin. Les principaux composants à privilégier sont : Spring MVC (pour le développement d'applications web), Spring Security (pour gérer l'authentification, les habilitations et la protection contre diverses attaques), Spring Data (qui simplifie l'accès aux bases de données en fournissant une abstraction pour travailler avec différentes sources de données, telles que les bases de données relationnelles et NoSQL). Sur le plan de l'architecture, Spring fournit un conteneur IoC (pour la gestion des objets et de leur cycle de vie. Il prend en charge l'injection de dépendances, la configuration des beans, et la gestion des transactions). Enfin, Spring prend en charge la programmation par aspect (AOP) ce qui permet de séparer la logique métier des aspects techniques et transverses comme par exemple la gestion de la sécurité, des transactions, de la sécurité, ou encore de la journalisation d'événements.

Spring Boot est un projet Spring qui simplifie et accélère la création d'applications Java en fournissant une configuration automatique (avec différents profils possibles qui définissent des dépendances préconfigurées appelées « starters ») qui réduit fortement la complexité d'une configuration manuelle.

JHipster (Java Hipster) est un générateur d'applications Spring Boot. Ses principaux avantages pour améliorer la productivité des développeurs sont :

1. Configuration : JHipster génère une configuration initiale complète pour une application Spring Boot comprenant notamment la structure du projet, la configuration de la base de données, la sécurité avec Spring Security (supporte OpenID Connect), la gestion des utilisateurs (gestion de profils utilisateurs), Elasticsearch, et bien d'autres. JHipster intègre également la configuration du Frontend et supporte Vue.js, React et Angular (supporte également la création d'application PWA) ;
2. Scaffolding : JHipster peut générer automatiquement le code source de l'application, les entités, les contrôleurs et services REST, les modèles de vues ;
3. Base de données : JHipster prend en charge plusieurs systèmes de gestion de base de données, notamment MariaDB, MySQL, PostgreSQL, MongoDB. Il génère également des scripts de migration pour les modifications de schéma de base de données (supporte les outils Liquibase, Flyway ou le très simple dbDeploy qui peut s'intégrer dans le code en tant que Spring Bean) ;
4. Outils de développement : JHipster intègre divers outils de développement, tels que des outils de test, de gestion de base de données et de génération de code. Il possède également, avec le « JHipster Domain Language » (JDL), un langage de description pour l'application, ses entités et relations utilisable dans un IDE (pe. Eclipse, IntelliJ ou VS Code) ;
5. Déploiement : JHipster génère des fichiers de configuration pour le déploiement y compris pour des conteneurs (par exemple pour un cluster Kubernetes).

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Environnement Java	Jakarta EE	Eclipse (Licence Publique Eclipse 2.0)	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / *	MinArm
Framework de développement	Spring	VMWare (licence Apache 2.0)	Framework d'infrastructure pour les applications d'entreprise Java à utiliser préférentiellement avec l'OpenJDK 8/17.	R / -	MinArm
<i>Commentaire : A noter que la fin du support de la version 5.3 est annoncée au 31/12/2024⁵⁸ (une extension de 2 ans supplémentaires est possible au travers d'un support commercial) et que la prochaine version majeure de Spring nécessitera d'utiliser au minimum le JDK 17. De plus, la version 5.3 prend en charge les versions 7 et 8 de Java EE sous namespace javax tandis que la version 6 passe aux version 9 et 10 de Jakarta EE sous namespace jakarta. Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route en 2024.</i>					
Framework de développement	Spring Boot	VMWare (licence Apache 2.0)	Outil d'aide à la création d'application Spring, simplifiant la gestion des dépendances et la configuration ; La fonction permettant d'embarquer un serveur d'application Tomcat, Jetty ou Undertow ne <u>doit pas</u> être utilisée (hors des environnements de développement ou d'hébergement en orchestration de conteneurs). * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / -	MinArm
Framework de développement	JHipster	Projet communautaire (Licence Apache 2.0)	Générateur de projet d'application Spring Boot intégrant la réalisation d'un frontend avec Vue.js, React ou Angular.	R / -	MinArm

7.3.3 Développement en PHP

Document	Date	Origine	Type doc	Portée
Cadre technique relatif au développement PHP au sein du ministère de la Défense, diffusé sous timbre n° 185 /DEF/DGSIC/DG/NP du 6 avril 2016	6 avril 2016	DGSIC	Cadre technique	MinArm
<i>Commentaire : Ce document cadre, désormais obsolète, précise les conditions de réalisation technique d'applications développées en PHP au sein du ministère : il précise les règles techniques à respecter, émet des préconisations en matière d'outils de développement et énonce les bonnes pratiques en conformité avec l'état de l'art. Il est applicable aux centres de développement du ministère.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Framework de développement	Symfony	Symfony SAS (licence MIT)	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / -	MinArm

⁵⁸ <https://spring.io/projects/spring-framework#support>

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Framework de développement	Laravel	Communauté (licence MIT)		R / -	MinArm
Framework de développement	Drupal	(licence GNU GPL 2)	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <i>Pile logicielle : liste des produits</i>	R / -	MinArm

7.3.4 Développement en C# et .NET

Le framework .Net, ainsi qu'un système d'exploitation Windows, font partie des prérequis pour développer en C#. L'environnement de développement est Microsoft Visual Studio, auquel il est possible d'ajouter des plugins, et la gestion du cycle de vie peut se faire via TFS (Team Foundation Server) qui gère le versioning des sources, la réservation de code, la gestion des tâches, les builds, etc. Une instance de SQL Server est indispensable au fonctionnement de TFS. Enfin, la gestion des dépendances nécessite Nuget.

7.3.5 Développement HTML5-Javascript-CSS

Pour ce type de développement, il est recommandé de privilégier la réalisation d'application SPA (*single page application*). Ceci afin d'améliorer la performance de l'application en réduisant les sollicitations vers un serveur de présentation et donc de la bande passante réseau.

Règle	Énoncé	Statut	Portée
RT_DEV_10	Pour la réalisation d'applications web, il est RECOMMANDÉ de privilégier un développement de <i>Single Page Application</i> [SPA].	R	MinArm

Il est également recommandé de réaliser le rendu des pages côté serveur plutôt que côté client (SSR) pour améliorer la performance de l'application et la mise en cache des pages. Cette approche est nécessaire pour améliorer le référencement d'un site si nécessaire (SEO). La génération de sites statiques (SSG) est également à privilégier à l'installation lorsque c'est envisageable pour améliorer la performance et la sécurité.

Règle	Énoncé	Statut	Portée
RT_DEV_11	Pour la réalisation d'applications web, il est RECOMMANDÉ de réaliser le rendu des pages côté serveur [SSR].	R	MinArm

La génération de sites statiques (ou *Static Site Generator* : SSG) est également à privilégier lorsque c'est envisageable pour améliorer la performance et la sécurité.

Règle	Énoncé	Statut	Portée
RT_DEV_12	Pour la réalisation de pages web globalement statiques, il est RECOMMANDÉ de recourir à la génération de sites statiques [SSG].	R	MinArm

La technologie PWA (« progressive web app ») est recommandée pour permettre le fonctionnement en mode temporairement déconnecté d'un SI réalisé en client-léger.

Règle	Énoncé	Statut	Portée
RT_DEV_13	Pour les besoins de fonctionnement en mode temporairement déconnecté d'un système d'information en client léger, il est RECOMMANDÉ de recourir au développement d'une progressive web app [PWA].	R	MinArm

Actuellement, 2 frameworks pérennes s'imposent pour le développement d'application en Javascript : Vue.js et React. Le premier est à privilégier car il est le plus simple à maîtriser tout en étant suffisamment complet pour la plupart des SI du Ministère. React est aussi complet et bénéficie d'un bon support éditeur sur les vulnérabilités critiques.

Angular, précédemment recommandé, est dorénavant assujetti à la maintenance des SI existants en production et à des développements réalisés par des équipes internes déjà formées et expérimentées sur Angular. Il est assujetti à condition de disposer d'une capacité pour assurer les mises à jour du fait du rythme très soutenu de sortie des versions majeures⁵⁹ (tous les 6 mois), ce qui rend très difficile et coûteux le MCS des SI réalisés avec Angular. De surcroît, c'est un framework qui est plus complexe et exigeant à maîtriser que Vue.js ou React sans qu'il apporte des fonctionnalités majeures qui ne seraient pas réalisables avec Vue.js ou React (avec si besoin des librairies complémentaires disponibles dans les écosystèmes de ces framework, voire des framework tels que Nuxt.js ou Next.js).

Le développement en JavaScript pour le backend nécessite l'environnement d'exécution Node.js (*cf. 3.2.2.2.4 Environnement d'exécution JavaScript*). Pour la partie web associée, le framework recommandé est Express. Son remplacement par le framework Fastify est assujetti à un besoin de très fortes performances ou de traitements complexes en mode asynchrone. Express est un framework simple et performant qui dispose d'un écosystème très important de librairies et framework complémentaires permettant d'apporter des fonctionnalités prêtes à l'emploi. Parmi celles-ci, et pour éviter une trop grande diversité de framework, il est conseillé de privilégier les frameworks Parse Server (à la condition express de découpler les API REST servies du schéma de base de données et de les rendre conformes au cadre technique des API REST du Ministère) ou Nest.js. Leur utilisation reste assujettie car il est préférable de privilégier la simplicité d'Express qui est suffisante dans la plupart des applications WEB.

Il est de plus recommandé de réaliser les développements en Typescript qui apporte un typage statique permettant de renforcer la qualité et la robustesse du code face à des erreurs qui peuvent être détectées dès la compilation du code Typescript en Javascript plutôt qu'à l'exécution.

Règle	Énoncé	Statut	Portée
RT_DEV_14	Il est RECOMMANDÉ de réaliser les développements en Typescript plutôt que directement en Javascript.	R	MinArm

Enfin, JQuery, dont seule la version 3 est encore maintenue a vu les fonctions offertes reprises par les API Javascript des navigateurs ou par des microframeworks. Malgré les immenses services rendus par le passé, cette technologie est désormais sans réelle plus-value, en fin de vie et ne doit plus être utilisée. Les greffons ou frameworks qui l'utilisent doivent être identifiés et progressivement remplacés par des équivalents n'ayant pas d'adhérence avec JQuery.



Pour la réalisation d'applications mobiles, **privilégier** le développement de PWA (progressive Web Apps)
Développement en mode natif soumis à dérogation



Document	Date	Origine	Type doc	Portée
Recommandations pour la mise en œuvre d'un site Web : maîtriser les standards de sécurité côté navigateur <i>cf.4.5 Sécurisation des COTS</i>	28 avril 2021	ANSSI	Note technique	Toute administration

⁵⁹ <https://angular.io/guide/releases>

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Framework de développement	JQuery	JQuery Foundation	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / -	MinArm
Framework de développement	Angular	Google (licence MIT)	* pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / -	MinArm
Framework de développement	React	Meta (licence MIT)		R / -	MinArm
Framework de développement	Next.js	Vercel (licence MIT)	Assujetti à la réalisation avec React de SI exposés sur Internet et pour lesquels l'optimisation du référencement par les moteurs de recherche (SEO) est un besoin métier majeur. * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	A / -	MinArm
Framework de développement	Vue.js	Evan You (licence MIT)	Solution à privilégier pour les nouveaux projets * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	* / -	MinArm
Framework de développement	Nuxt.js	NuxtJS (licence MIT)	Version en fonction de la version Vue utilisée. Assujetti à la réalisation avec Vue.js de SI exposés sur Internet et pour lesquels l'optimisation du référencement par les moteurs de recherche (SEO) est un besoin métier majeur. * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	A / -	MinArm
Framework de développement	Electron	OpenJS Foundation	Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an). * pour les recommandations sur les versions voir le détail en annexe 8.2.1 <u>Pile logicielle : liste des produits</u>	A / -	MinArm
Commentaire : Le SC ² A attire l'attention des projets sur le cycle de vie particulièrement court de la solution Electron qui va imposer a minima au projet une charge de MCO/MCS conséquente afin de la maintenir à jour et dans une version supportée. Avec une nouvelle version toutes les 8 à 10 semaines et un support de 6 mois, un nouveau package CNCI est donc à refaire au moins tous les 6 mois.					
Framework de développement	Express.js	OpenJS Foundation	Framework WEB pour développement Javascript	R / S	MinArm
Framework de développement	Fastify	OpenJS Foundation	Framework WEB assujetti à des enjeux de performance ou de traitements complexes en mode asynchrone.	A / -	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Framework de développement	Parse server	Parse-community (License BSD)	Framework complémentaire à Express. Assujetti à un développement d'application mobile pour faciliter la gestion des utilisateurs, la communication en temps réel par websockets et les notifications Push aux appareils mobiles.	A / -	MinArm
Framework de développement	Nest.js	Open collective (Licence MIT)	Pour un développement backend métier important, plutôt que d'utiliser Express et un nombre conséquent de modules complémentaires dont la liste varierait d'un SI à l'autre, il est préférable de choisir un framework intégré et suffisamment complet pour réaliser un SI métier complexe entièrement en Javascript. Nest.js est le framework à privilégier dans ce cas d'utilisation. Il fonctionne avec Express ou Fastify et est agnostique au framework frontend. Il peut être utilisé avec Vue.js, React ou Angular.	A / -	MinArm

7.3.6 Réalisation d'applications mobiles

Le cadre relatif à la réalisation des applications mobiles identifie trois manières de réaliser des applications mobiles :

- Webapp en faisant appel à un navigateur
- Application développées en natif
- Application dites hybrides.

L'évolution technologique, et notamment les capacités actuelles des navigateurs et des protocoles sur lesquels ils reposent, incitent désormais à recommander fortement l'usage de « progressive web apps » (PWA)⁶⁰ pour la réalisation d'applications mobiles.

Les applications web progressives utilisent des API web modernes ainsi qu'une stratégie d'amélioration progressive pour créer des applications web multiplateformes qui fonctionnent partout et possèdent des fonctionnalités qui donnent aux utilisateurs les mêmes avantages que les applications natives, y compris pour un fonctionnement en mode déconnecté.

Les solutions développées en natif ou dites hybrides restent envisageables dès lors que l'approche PWA ne permet pas de répondre au besoin.

Lorsque l'accès aux SDK natifs est nécessaire, le framework ionic associé à Capacitor ou Cordova et qui est compatible avec les frameworks Angular, React et Vue pourra être utilisé.

⁶⁰ À noter que l'annonce de l'arrêt du support des PWA sur Firefox ne concerne que la version Desktop, et pas les versions sur Android qui, elles, continuent à fonctionner.

Règle	Énoncé	Statut	Portée
CCT_R10	Pour la réalisation d'applications mobiles, il est RECOMMANDÉ de privilégier un développement de Progressive Web Apps [PWA] plutôt qu'un développement en mode natif.	R	MinArm

Document	Date	Origine	Type doc	Portée
Cadre technique relatif à la réalisation des applications mobiles au sein du ministère de la Défense , diffusé par note n°141 /DEF/DGSIC/DG/NP	3 mars 2016	DGSIC	Cadre technique	MinArm
<i>Commentaire : ce document précise les conditions de réalisation technique des applications mobiles au sein du Ministère: il en définit les cas d'usage retenus par le ministère des armées, précise les règles techniques à respecter, et émet des préconisations en matière de choix technologiques.</i>				
Spécification d'interface SMOBI à l'attention des SI Cadre d'architecture et contraintes de configuration pour un système d'information accessible sur un terminal SMOBI Cf. 3.1.6 Mobilité [SU-AN, SU-ITN]	Décembre 2020	UMSNUM/DIRISI	Note technique	Intradef
<i>Cf. 3.1.6 Mobilité [SU-AN, SU-ITN]</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Framework de développement	Ionic	Licence MIT	Développement d'applications mobiles nécessitant un accès aux SDKs natifs.	A / -	MinArm
Framework de développement	Capacitor		Développement d'applications s'appuyant sur Ionic	A / -	MinArm
Framework de développement	Cordova		Développement d'applications s'appuyant sur Ionic	A / -	MinArm

7.3.7 Développement à l'aide d'outils « low-code » ou « no-code »

Document	Date	Origine	Type doc	Portée
Directive n°49 encadrant l'emploi des solutions peu de code / sans code au Ministère des armées édition v1.0, diffusée par note n° 564/ARM/DGNUM/SDTN/NP	28/09/2023	DGNUM	Directive	MinArm Hors projets sous IM 1618
<i>Commentaire : ce document a pour objet de fixer les règles d'emploi des solutions de Low Code / No Code au sein du Ministère des armées, en lien avec le cadre de cohérence technique et la gouvernance associée des projets de systèmes d'information. S'applique aux plates-formes qui ont vocation à mutualiser différentes expérimentations et applications ainsi que leur MCO/MCS sur une même solution.</i>				
Feuille de route ministérielle des données	Mise à jour de décembre 2023.	DGNUM	Feuille de route	MinArm
<i>Commentaire : La plateforme applicative simplicité est identifiée comme une capacité permettant de faciliter la captation de données métiers aujourd'hui inaccessible et de faciliter l'ouverture de données mises en qualité.</i>				

Le *no-code* ou *low-code* consiste à développer des applications sans avoir besoin d'écrire de code (*no-code*) ou avec peu de code (*low-code*). Les outils *no-code* sont généralement pensés dès leur conception pour générer des applications sans avoir à écrire de code, alors que les outils *low-code* sont plus souvent des extensions d'outils existants, davantage orientés vers le monde de l'entreprise. Tous mettent en avant la simplicité avec laquelle il est possible de développer une application.

L'utilisation de tels produits permet de masquer la complexité technique en se focalisant sur la partie métier. Ces outils nécessitent des formations spécifiques à la solution utilisée mais permettent ensuite à un acteur

fonctionnel d'être relativement autonome pour réaliser des cas d'usage peu complexes.

Ainsi, selon les objectifs et les besoins du projet il peut être pertinent d'utiliser un outil de type « *low-code* » ou « *no-code* » lors de la phase d'idéation ou de cadrage fonctionnel afin de réaliser des POC. Cela peut permettre de mieux inclure les acteurs métier dans la réalisation et de faire mûrir le besoin fonctionnel, dans le cadre d'une démarche centrée sur l'utilisateur.

Néanmoins, ces produits ne permettent pas toujours d'obtenir la maîtrise nécessaire de l'application ainsi créée. La structuration du code sous-jacent, son éclatement au sein des différents des ateliers et son suivi en version, tous spécifiques, obèrent les capacités d'appropriation et de MCO par les équipes de développement du Ministère, mêmes formées sur ces produits. Aussi, même si les promesses de simplicité de l'approche *low-code / no-code* peuvent sembler tentantes, notamment du point de vue fonctionnel, ce mode de production des applications n'est pas adapté à tous les cas d'usage.

L'utilisation de ces outils est assujettie aux projets fonctionnellement très simples, aux POC et aux phases d'idéation sur une durée déterminée avant un passage à l'échelle hors d'outils *low-code / no-code*. De plus, lorsque les applications créées sont destinées à la production, le MCS de l'ensemble de la pile logicielle doit être assuré sur toute leur durée de vie.

Par conséquent, la réalisation d'une solution basée sur un outil de *low-code / no-code* est soumise à une dérogation préalable dûment justifiée auprès du SC²A afin de garantir le MCO et le MCS sur toute la durée d'utilisation du produit. Le recours à des plateformes de *low-code / no code* pour des applications structurantes du ministère ou ayant un besoin de disponibilité supérieur à I2 (classification ARR) est jugé risqué et fortement déconseillé. Il est même interdit pour réaliser des applications critiques qui nécessitent une sécurité renforcée et une haute fiabilité.

Pour mémoire, il existe des services du socle numérique (Démarche Simplifiée, Tuleap) et des outils de développements référencés dans le présent CCT (Drupal WebForm, Jhipster, chaîne CI/CD et outillage PICSEL) qui permettent de mener rapidement des développements maîtrisables dans la durée.

Au-delà de ces considérations, la directive référencée ci-dessus énonce un certain nombre de règles de gouvernance des plates-formes et des développements, organisationnelles, de sécurité et techniques dont :

- Limiter aux expérimentations et aux applications non critiques de taille réduite, ne requérant pas plus qu'une disponibilité I2 et sans besoin de sécurité renforcée ou de haute fiabilité ;
- Calculer le retour sur investissement et élaborer un document de justification ;
- Conformité au RGAA, ainsi qu'avec le CCT, quel que soit le type d'hébergement et recours à des frameworks standards si possible OpenSource ;
- Effectuer les échanges interapplicatifs via API Rest, utiliser des certificats IGCg NG ;
- Absence de développements spécifiques ;
- Mise en œuvre par du personnel formé maîtrisant la technologie ;
- Plate-forme distincte de celle de production pour les activités de développement ;
- Suivre une démarche d'homologation standard.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Plateforme applicative centrée données	Simplicité	Simplicité	- Une instance dédiée à un projet Ou - Une plateforme applicative permettant à une DSI d'héberger plusieurs applicatifs métier	E / -	MinArm

Parmi les différentes solutions expérimentées ou en service, la solution Simplicité présente de multiples intérêts comme plateforme applicative orientée données au profit d'une DS1.

C'est une solution déjà maîtrisée par le ministère, plusieurs instances de la plateforme Simplicité sont déjà en service, chacune étant dédiée à un projet. Au-delà cet usage, employer Simplicité comme plateforme applicative permet faciliter la création de cas d'usages dans un environnement maîtrisé et apportant nativement des interconnexions avec les briques du socle telle que Mindefconnect, démarche simplifiée et les plateforme API.

Par ailleurs, la création des applicatifs repose sur la description préalable des objets métiers et il permet d'interroger et d'exposer nativement des API. C'est ainsi une plateforme pertinente pour outiller la feuille de route ministérielle des données sur les fonctions « capter/collecter » et « ouvrir ».

Déployable dans une architecture cloud, il faut évaluer son potentiel pour accélérer le portage d'application anciennes dans le mouvement vers le cloud, dans une démarche data-centrée.

7.3.8 Autres langages

Document	Date	Origine	Type doc	Portée
Guide S-CAT n°517 : Règles de codage pour l'implémentation de logiciels en langage Python	05/03/2015	DGA MI	Guide	MinArm
<i>Commentaire : Ce document est un guide de règles et de recommandations à utiliser pour le développement de logiciels dans le langage Python. Ce guide a pour objectifs de :</i>				
<ul style="list-style-type: none"> - Augmenter la qualité et la fiabilité du code source produit, en mettant en avant les bonnes pratiques de programmation, et en interdisant les constructions dangereuses ou fréquemment sources d'anomalies ; - Faciliter le travail d'évaluation logicielle (évaluation en mode boîte blanche) en définissant un cadre commun pour le code source fourni. Le but est de gagner en homogénéité dans les développements produits, et également permettre l'analyse statique outillée des logiciels produits 				
Guide S-CAT n°518 : Règles de codage pour l'implémentation de logiciels en langage C	24/03/2015	DGA MI	Guide	MinArm
<i>Commentaire : Ce document est un guide de recommandations contenant un certain nombre de règles à utiliser pour le développement de logiciels dans le langage C. Ce guide a pour objectifs de :</i>				
<ul style="list-style-type: none"> - Augmenter la qualité et la fiabilité du code source produit, en mettant en avant les bonnes pratiques de programmation, et en interdisant les constructions dangereuses ou fréquemment sources d'anomalies ; - Faciliter le travail d'évaluation logicielle (évaluation en mode boîte blanche) en définissant un cadre pour le code source fourni. 				
Guide S-CAT n°521 : Règles de codage pour l'implémentation de logiciels en langage C++	24/11/2015	DGA MI	Guide	MinArm
<i>Commentaire : Ce document est un guide de recommandations contenant un certain nombre de règles à utiliser pour le développement de logiciels dans le langage C++. Ce guide a pour objectifs de :</i>				
<ul style="list-style-type: none"> - Augmenter la qualité et la fiabilité du code source produit, en mettant en avant les bonnes pratiques de programmation, et en interdisant les constructions dangereuses ou fréquemment sources d'anomalies ; - Faciliter le travail d'évaluation logicielle (évaluation en mode boîte blanche) en définissant un cadre pour le code source fourni en entrée d'évaluation. 				
Règles de programmation pour le développement sécurisé de logiciels en langage C – v1.4 https://www.ssi.gouv.fr/uploads/2020/07/anssi-guide-regles_de_programmation_pour_le Developpement_securise_de_logiciels_en_langage_c-v1.4.pdf	24/03/2022	ANSSI	Guide	Toutes administrations

7.3.9 Sécurisation du code

Les données que traitent nos applications font l'objet de convoitises plus ou moins aiguës selon leur criticité ou l'intérêt qu'elles présentent, et le risque de vol d'informations ou de données sensibles est réel. La façon

dont un programme informatique est conçu peut impacter sa disponibilité, compromettre l'intégrité et la confidentialité des données traitées, et ainsi engager la responsabilité pénale de son propriétaire, de son promoteur ou des équipes qui en ont assuré la conception et la réalisation.

Les mesures de sécurisation des réseaux et des serveurs ne sont pas absolues et la surface d'attaque représentée par un code mal conçu (cf. top 10 de l'OWASP⁶¹) doit être considérée comme critique. La démarche de sécurisation du code doit en conséquence être pleinement intégrée au cycle de vie des applications, de leur conception à leur retrait de service. La robustesse du code doit être testée et vérifiée avant toute mise en production, ainsi qu'à chaque évolution.

Ces contrôles sont par exemple rendus disponibles dans la chaîne d'intégration continue de PICSEL.

La sécurisation du code ne doit pas être confondue avec la démarche, réglementairement obligatoire, d'homologation, pour laquelle il convient de se référer au § 4.2.1.

L'ensemble des acteurs impliqués, maîtrise d'ouvrage comme équipes de conception, réalisation et maintien en condition opérationnelle, doit comprendre les enjeux de cette démarche et mettre correctement en œuvre les recommandations en la matière, ou faciliter cette mise en œuvre : bonnes pratiques de codage (génériques et spécifiques aux technologies et langages employés), utilisation d'interfaces de programmation connues, documentées et soutenues, utilisation d'outils de vérification de qualité du code, etc.

Des travaux de veille et d'animation sur la robustesse du code sont réalisés par le CASID⁶².

Document	Date	Origine	Type doc	Portée
Directive DGSIC n°40 portant sur le développement des applications informatiques et des logiciels robustes du ministère de la Défense [DIR DEV.SEC]	17/05/2017	DGSIC	Directive	MinArm

7.4 Test et intégration (pré-intégration, intégration continue)

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du ministère et est fortement recommandé pour les développements réalisés à l'extérieur.

Document	Date	Origine	Type doc	Portée
<u>Guide des bonnes pratiques de la mise en œuvre du test logiciel à l'usage des centres de développement du ministère de la défense</u>	14/06/2017	CASID	Guide	MinArm
<i>Commentaire : Ce document est un guide des bonnes pratiques des tests à réaliser lors du développement d'une application logicielle. Il couvre les tests unitaires, d'intégration, tests système, et tests d'acceptation. Ce document est le fruit d'un groupe de travail ad hoc d'acteurs du développement en interne au ministère.</i>				

Dans un cadre professionnel, et d'autant plus au ministère des Armées, tout développement implique la réalisation de tests logiciels automatisés. La démarche de cloudification renforce encore cet impératif en rendant tout système d'information qui n'en serait pas doté inapte à tirer un quelconque bénéfice des nouveaux environnements de développement (déploiement automatisé fiable et rapide notamment).

Ces tests automatisés s'organisent sous forme d'une pyramide :

⁶¹ Open web association security project (<http://owasp.org/www-chapter-france/>) : communauté, libre et ouverte à tous, travaillant sur la sécurité des applications web. Le « top ten » est un projet visant à lister les 10 risques de sécurité applicative les plus critiques. Ce classement fait référence et est aujourd'hui cité par de nombreuses organisations, dont certaines gouvernementales

- tests unitaires: ne testent qu'une seule fonction ou méthode, en isolation de tout composant externe à celle-ci;
- tests d'intégration et d'API ;
- tests d'IHM, tests de bout en bout, tests fonctionnels ;
- tests de sécurité, de charge et tests métiers.

Les premiers sont les nombreux, les plus simples, robustes et rapides à exécuter, les derniers sont les moins nombreux, les plus complexes, fragiles et lents à exécuter.

Ils doivent être intégrés et joués dans une chaîne d'intégration continue, typiquement celle de PICSEL.

Le développement dirigé par les tests (TDD ou Test Driven Development) et dirigé par le comportement (BDD ou Behaviour Driven Development) sont des pratiques fortement recommandées qui permettent d'améliorer significativement la qualité du code produit, son adéquation au besoin et de calibrer au juste besoin le nombre de tests à produire.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
BDD Testing	Cucumber	OpenSource		R / -	MinArm
<i>Commentaire : Le recours à Gherkin comme langage de spécification des tests constitue en la matière une bonne pratique.</i>					
TDD Testing	Cypress	Cypress.io		R / -	MinArm
Automatisation de tests d'IHM	Selenium IDE	SeleniumHQ	Pour la production de scripts servant à la mesure des métriques associées à un scénario fonctionnel complet à travers une IHM Web.	R / -	MinArm

7.4.1 Tests unitaires

Un test unitaire (ou de composants) vérifie le fonctionnement individuel de logiciels, modules, composants ou autres unités de code (classes, méthodes, programmes) testables séparément. Le test unitaire doit se faire de manière isolée du reste du système (en utilisant éventuellement des bouchons, pilotes et simulateurs).

7.4.2 Tests d'intégration des composants

L'intégration est un processus combinant des composants ou systèmes avec une interaction. Le terme intégration doit toujours être précisé. Il peut concerner entre autres :

- l'intégration de composants dans une application ;
- l'intégration d'une application dans son environnement;
- l'intégration logiciel-matériel d'un SI dans son environnement physique.

7.4.3 Intégration continue

L'intégration continue est un ensemble de pratiques utilisées en génie logiciel consistant à vérifier à chaque modification de code que le résultat est conforme aux standards de développement et que les modifications ne produisent pas de régression dans l'application développée.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Intégration continue	PICSEL (Gitlab)	MinArm	Outil retenu dans le cadre de la cloudification (PICSEL, C1DR et C1NP)	R / S	MinArm
Intégration continue	Jenkins	Jenkins	Assujetti à des cas d'usages hors PICSEL	D / -	MinArm
<i>Commentaire : Jenkins demeure un excellent outil, il est en cours de retrait de PICSEL à des fins de rationalisation des outils, Gitlab permettant de mutualiser plusieurs fonctions au sein d'un même service (CI/CD, gestion des dépôts git, gestion des tickets de développement, Wiki ...).</i>					

7.4.4 Tests de performance

Les tests de performance, de montée en charge peuvent être mis en œuvre par le BEEI⁶³ (DIRISI). Ce bureau a vocation à rejoindre à terme l'environnement PICSEL afin d'alléger les opérations d'installation des systèmes d'information à tester et de bénéficier d'instances représentatives de services socle des environnements C1DR et C1NP.

Document	Date	Origine	Type doc	Portée
Description de l'offre de performance du BEEI diffusée par courrier n°402629/ARM/DIRISI/SP/DASM/NP du 27 avril 2021	27/04/2021	DIRISI	Note	MinArm
<i>Commentaire : Cette note, à destination des RCP et CAT projet, a pour objectif de présenter l'offre de service performance du Bureau Expertise pour l'Évaluation et l'Intégration, en rappelant quelques principes nécessaires au bon déroulement des projets performance.</i>				

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Tests de charge	JMeter	Apache Software Foundation	Sollicitation intensive et parallélisée de services simples : - webservices ; - tests JUnit ; - méthode d'un bean managé ; - SQL ; - navigation simple dans une IHM Web.	R	MinArm
<i>Commentaire : à utiliser uniquement sur un environnement dédié aux tests de charge</i>					
Tests de charge	Gatling	Gatling Corp	Tests de charge et de performance pour applications web (sous licence Apache 2.0). Disponible sur PICSEL.	R	MinArm
<i>Commentaire : à utiliser uniquement sur un environnement dédié aux tests de charge</i>					

⁶³ Bureau Expertise pour l'Évaluation et l'Intégration

7.5 Qualité logicielle

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du ministère et est fortement recommandé pour les développements réalisés à l'extérieur.

Qualité du code

La qualité logicielle est un ensemble d'indicateurs portant sur des critères multiples : qualité du code source, facilité de maintenance, qualité perçue, facilité d'apprentissage, etc.

Pour les logiciels, la qualité ne se mesure pas. C'est la non-qualité qui sert de base aux calculs des indicateurs. On mesure de fait le nombre de dysfonctionnements rencontrés impactant un des critères de qualité et le logiciel est considéré comme étant « de qualité » si ces dysfonctionnements ne dépassent pas un seuil fixé selon les attentes du projet ou du Ministère vis-à-vis de ce logiciel ou de cette typologie de développement.

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
ASCRM V1.0 (OMG Document Number : formal/2016-01-03)	Automated Source Code Reliability Measure. Janvier 2016 <i>cette norme de l'OMG définit les éléments de mesure de la qualité interne du code dans le domaine de la fiabilité (disponibilité, tolérance aux pannes et capacité de récupération).</i> https://www.omg.org/spec/ASCRM/1.0/PDF	R	MinArm
ASCSM V1.0 (OMG Document Number : Formal/2016-01-04)	Automated Source Code Security Measure. Janvier 2016 <i>Cette norme de l'OMG définit les éléments de mesure de la qualité interne du code dans le domaine de la sécurité (fondé sur le Top 25 du CWE).</i> https://www.omg.org/spec/ASCSM/1.0/PDF	R	MinArm
ASCPEM V1.0 (OMG document Number : formal/2016-01-02)	Automated Source Code Performance Efficiency Measure. Janvier 2016 <i>Cette norme de l'OMG définit les éléments de mesure de la qualité interne du code dans le domaine de la performance.</i> https://www.omg.org/spec/ASCPEM/1.0/PDF	R	MinArm
ISO/IEC 25010 :2011	System and software quality models <i>Cette norme (actuellement en statut « à réviser ») complète et remplace la norme ISO/IEC 9126-1.</i> Réf : https://www.iso.org/standard/35733.html	R	MinArm
ISO-5055	Nouvelle norme fournissant un ensemble de règles permettant d'évaluer les systèmes logiciels selon quatre facteurs : sécurité, fiabilité, maintenabilité et efficience. Réf : https://www.iso.org/standard/80623.html Téléchargeable ici.	R	MinArm
CWE	Common Weakness Enumeration, liste des vulnérabilités logicielles maintenue par le MITRE (organisation à but non lucratif américaine). Réf : https://cwe.mitre.org	R	MinArm
NIST Risk Management Framework	Ensemble de critères visant à sécuriser les systèmes informatiques du gouvernement américain. Réf : https://csrc.nist.gov/projects/risk-management/sp800-53-controls	R	MinArm

Norme/standards	Description / Utilisation / Restriction	Statut	Portée
OWASP top 10 2021	Liste des failles de sécurité les plus courantes et les plus exploitées. Réf : https://owasp.org/www-project-top-ten	R	MinArm
<i>Commentaire : 2021 est à date (fin 2023) le dernier top ten disponible. Il existe sur le site OWASP d'autres Top Ten d'intérêt (Kubernetes, Machine Learning, Large Language Model Applications, AI, API, mobile, CI/CD ...)</i>			
Modèle qualimétrique du CISQ	Standard pour mesurer les critères de qualité des logiciels, développé par le Consortium for IT Software Quality. Réf : https://www.it-cisq.org	R	MinArm
<i>Commentaire : les 5 dernières références sont mesurées par la plateforme CAST mise en œuvre par le CASID.</i>			

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Qualité du code	SonarQube LTS	Open Source	Composants logiciels open source faisant partie de la plateforme d'intégration continue PICSEL, à utiliser conjointement.	R / S	MinArm
Qualité du code	CAST AIP	CAST SOFTWARE	Outil particulièrement adapté à l'évaluation du code des prestataires extérieurs ou aux opérations de transférabilité / réversibilité. A réservé en priorité aux SI structurants, selon arbitrage DGNUM. Les principaux intégrateurs disposant de cette plateforme, il est opportun de prévoir dans les marchés la communication des résultats de l'analyse. La version souhaitable est celle du ministère afin de pouvoir effectuer éventuellement des mesures contradictoires en s'appuyant sur la norme ISO 5055.	R / -	MinArm
<i>Commentaire : il est recommandé de contrôler en continu la qualité du code avec SonarQube et de réservé les mesures avec CAST AIP aux livraisons majeures. CAST AIP nécessite un temps de traitement plus long mais offre des résultats plus poussés avec des mesures de remédiation qui peuvent être complétées par un plan d'amélioration et un accompagnement du CASID.</i>					

7.5.1 Performance - Métrologie

La supervision permet de s'assurer du bon fonctionnement permanent d'un service ou d'une application en fonction d'indicateurs définis par le client. La métrologie de la performance ajoute la notion de mesures dans le but d'optimiser l'infrastructure d'hébergement, le code et les performances vis-à-vis de l'utilisateur final. Il est possible de faire appel aux outils ministériels de traces (outils Dynatrace dans le cadre de l'observabilité : « PISARO métrologie »).

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Performance-métrie	Vmstat : Version fournie par le système d'exploitation	Open source	Pour l'observation ponctuelle d'un serveur. Limité aux systèmes Linux.	R	MinArm

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Performance-métrologie	sar – ksar :	Open source	Version fournie par le système d'exploitation Pour : - historiser l'activité de plusieurs serveurs ; - effectuer des mesures durant une campagne de tests ; - faire des comparaisons dans le temps. Limité aux systèmes Linux.	R	MinArm
Performance-métrologie	perfmon	Microsoft	Version fournie par le système d'exploitation Même cas d'utilisation que sar et ksar mais pour un serveur Windows.	R	MinArm
Performance-métrologie	XDebug	Open source	Mesure des performances des applications PHP https://xdebug.org/	R	MinArm
Performance-métrologie	JavaMelody	Open Source	Composant logiciel open source, dédié au monitoring d'applications Java.	R	MinArm

7.6 Gestion des anomalies

Dans sa version actuelle, ce paragraphe s'applique aux développements internes du ministère et est fortement recommandé pour les développements réalisés à l'extérieur.

Les anomalies peuvent notamment être caractérisées par :

- des règles de gestion mal comprises ou interprétées ;
- de mauvais comportements ergonomiques ;
- des erreurs de charte graphique ;
- des erreurs de libellés ou d'affichage.

Niveaux de criticité

On distingue trois niveaux de criticité :

- MINEUR : les anomalies de ce niveau n'entraînent pas le fonctionnement de l'application. Ce peut être par exemple des erreurs d'affichage, de libellé, de message ou d'affichage graphique ;
- MAJEUR : ces erreurs, plus graves, touchent le bon fonctionnement de l'application, par exemple une règle de gestion erronée sans toutefois bloquer la recette du produit ;
- CRITIQUE : ce sont les erreurs les plus graves, qui bloquent la recette du produit.

Cette définition de criticité permet :

- de donner un bilan global de la qualité de la livraison ;
- de pouvoir prioriser les corrections, et planifier le travail de correction.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestion d'anomalies	Tuleap	Tuleap		R / S	Intradef

<i>Commentaire : Soutenu et exploité par le CASID</i>					
Gestion d'anomalies	DooNAF-Mantis Bug Tracker	DGA	Assujetti au contexte des programmes d'armement (DGA).	A / S (*)	MinArm
<i>Commentaires : (*) DooNAF est l'atelier d'ingénierie système (IS) mis à disposition par la DGA. Il regroupe un ensemble d'outils d'ingénierie système utilisés lors du déroulement d'une opération d'armement. Mantis Bug Tracker personnalisé pour la DGA fait partie de la suite d'outils soutenus sur le plan fonctionnel par la communauté IS et sur le plan système par le S2NA.</i>					
Gestion d'anomalies	JIRA	Atlassian		D	MinArm
<i>Commentaire : nécessite désormais une licence Data Center pour pouvoir disposer du MCO/MCS pour un hébergement sur les plateformes du Ministère.</i>					

8 ANNEXES

8.1 Glossaire / liens utiles

- Le Guide n°7 DGNUM – intégration de la sécurité numérique dans les projets comprend un glossaire portant sur les termes en matière de sécurité numérique

8.2 Produits / Piles logicielles d'exécution

8.2.1 Pile logicielle : liste des produits

Cette annexe reprend et précise les choix de produits logiciels cités dans le présent CCT.

Pour une meilleure lisibilité, la structuration de l'annexe suit strictement les numéros de chapitres du CCT.

Légende :

Reco SC2	Soutien
Recommandé	Soutenu
Emergent	Envisagé
Assujetti	Observé
Déconseillé	Non soutenu
Interdit	-
-	-

Annexe CCT v3.5.1 - 2024- Pile logicielle générale					Intradef		SIA S-SF		SIA FrOpS		Interne t					
Catégorie	Logiciel	Éditeur	Version		Recom. SC²A	Soutien DIRISI	Date de fin de support	Date de fin de support étendu	Commentaire							
Agent de messages	ActiveMQ	Apache Software Foundation	5.16	I N I N I N I N									19/04/23		N'est plus soutenu au 20/04/2023	
Agent de messages	ActiveMQ	Apache Software Foundation	5.17	R S R S R S R S											Compatible Java 11+ Utilise Spring 5.x, Log4j 2.x	
Agent de messages	ActiveMQ	Apache Software Foundation	5.18	R S R S R S R S											Compatible Java 11+ Utilise Spring 5.3, Log4j 2.x	
Agent de messages	Kafka	Apache Software Foundation	3.4	I N I N							I N				Fin de vie : lors de la sortie de la 3.7	
Agent de messages	Kafka	Apache Software Foundation	3.5	R S R S					R S						Fin de vie : lors de la sortie de la 3.8	
Agent de messages	Kafka	Apache Software Foundation	3.6	R S R S					R S						Fin de vie : lors de la sortie de la 3.9	
Agent de messages	Kafka	Apache Software Foundation	3.7	R S R S					R S						Fin de vie : lors de la sortie de la 3.9	
Agent de messages	RabbitMQ	Pivotal Software	3.11.x	I N							I N	30/12/23			Version obsolète. Le support étendu jusqu'au 31/07/2024 est payant.	

Agent de messages	RabbitMQ	Pivotal Software	3.12.x	D	O				D	O	22/02/24	31/12/24	Soutenu après accompagnement et assistance par premiers projets pour montée en compétence. Le support étendu jusqu'au 31/12/2024 est payant.
Agent de messages	RabbitMQ	Pivotal Software	3.13.x	R	S				R	S		31/12/25	Soutenu après accompagnement et assistance par premiers projets pour montée en compétence. Le support étendu est possible jusqu'au 01/09/2025 sous réserve d'acquittement d'une licence payante.
Annuaire - Provisionning	Usercube	Usercube	5.x	I							31/12/22		
Annuaire - Provisionning	Usercube	Usercube	6.X	A									
Annuaires	Active Directory	Microsoft		R	S	R	S	R	S				Aligné sur le support des versions windows server
Annuaires	Meibo	Ilex	4.0			A	S	A	S				
Annuaires	OpenLDAP	OpenLDAP project	2.5.x	R	S	R	S	R	S	A	S		2.5.16 à la date du 31/7/23 LTS, en principe supportée 5 ans
Base de données NOSQL	ArangoDB	ArangoDB	3.10	I	N	I	N	I	N	I	N	03/10/23	
Base de données NOSQL	ArangoDB	ArangoDB	3.11	A	N	A	N	A	N				BD multi-modèles (graphes, documents, clés-valeurs) open-source sous licence Apache. Version communautaire https://arangodb.com/subscriptions/end-of-life-notice/

Base de données NOSQL	Cassandra	Apache Software Foundation	3.0.X	D	O			I	N			Date de fin de vie approximative : fin d'année 2023, avec la sortie de la v5.0.	
Base de données NOSQL	Cassandra	Apache Software Foundation	3.11.X	D	O			I	N			Date de fin de vie approximative : fin d'année 2023, avec la sortie de la v5.0.	
Base de données NOSQL	Cassandra	Apache Software Foundation	4.0.X	A	S					30/06/24		Cas d'usage : Grands volumes de données et des besoins de bases distribuées hautement disponibles et décentralisées, sous réserve de prendre en compte les impacts réseau	
Base de données NOSQL	Cassandra	Apache Software Foundation	4.1.X	D	O			I	N			Même status pour les versions 4.x hors 4.0.	
Base de données NOSQL	CouchDB	Apache Software Foundation	2	A	N	A	N	A	N			CouchDB offre une réplication multi-master, ce qui signifie que plusieurs bases de données CouchDB peuvent se synchroniser entre elles de manière bidirectionnelle. Cela permet une grande tolérance aux pannes et la distribution des données sur plusieurs serveurs.	
Base de données NOSQL	Elasticsearch	Elastic	6.X	I	N	I	N	I	N	I	N	09/08/22	
Base de données NOSQL	Elasticsearch	Elastic	7.17.X	R	S	R	S	R	S	R	S	30/04/24	Actuelle version LTS - 7.17.X - Sera maintenue jusqu'à la version 9.0.0 Il faut utiliser le JDK fournit pas la distribution linux plutôt que le JDK

Base de données NOSQL	Neo4J	Neo4j	5.X	D	N			I	N			Base de type graphe . En version entreprise car la version communautaire n'a pas de gestion de privilège (un seul rôle d'admin)
Base de données NOSQL	OpenSearch	AWS	2.x	A	N							Alternative Elasticsearch
Base de données NOSQL	PouchDB	Apache Software Foundation	8	A	A	A	A	A				PouchDB est principalement utilisé pour le stockage de données côté client, ce qui signifie qu'il peut être utilisé pour stocker des données localement dans un navigateur web ou dans un environnement Node.js. PouchDB est conçu pour la réplication bidirectionnelle de données entre la base de données locale et une base de données distante. Cela permet de maintenir les données synchronisées entre différentes instances de l'application, même en cas de déconnexion.
Base de données NOSQL	Redis	Redis Labs	6.2	I	N			I	N			Une version majeure tous les ans recommandée comme base clé/valeur
Base de données NOSQL	Redis	Redis Labs	6.4	D	O			I	N	28/02/25		Une version majeure tous les ans recommandée comme base clé/valeur
Base de données NOSQL	Redis	Redis Labs	7.0	A	S			A	S	31/08/25		Une version majeure tous les ans recommandée comme base clé/valeur
Base de données NOSQL	Redis	Redis Labs	7.2	A	S	A	S	A	S			Une version majeure tous les ans recommandée comme base clé/valeur

Base de données NOSQL	Solr	Apache Software Foundation	8.x	I	N			I	N			Les versions 8.10 et inférieures sont en fin de vie, et interdites.
Base de données NOSQL	Solr	Apache Software Foundation	9.x	A	S			A	S			8.11 : D/O. Elle peut encore recevoir des correctif de bugs critiques.
BPM	Bonita	Bonitasoft	2022.2	D	D	D	I					Nécessite java 11 ou +. Compatible OIDC. Déconseillé parce qu'outils de low code, et du fait de la fréquence élevée des mises à jours.
BPM	Bonita	Bonitasoft	2023.1	D	D	D	I					Nécessite java 11 ou +. Compatible OIDC. Déconseillé parce qu'outils de low code, et du fait de la fréquence élevée des mises à jours.
BPM	Camunda	Camunda	7.24 CE	A	N	A	N	A	N	30/09/25	31/03/30	Version LTS
BPM	Camunda	Camunda	8.x	A	N	A	N	A	N			
BPM	Flowable	Flowable	7	A	E							
Bureautique	7-zip	Igor Viktorovitch Pavlov	23.x	R		R		R				
Bureautique	Acrobat Reader	Adobe	2020	R		R		R		05/01/25		
Bureautique	Acrobat Reader	Adobe	DC (2017)	I		I		I		05/06/22		Cycle de vie identique à celui d'Acrobat Standard 2017.
Bureautique	Libre Office	The Document Foundation	24.2.x	D		D		D		29/11/24		

Bureautique	Libre Office	The Document Foundation	24.8.x	R					E	12/06/25		
Bureautique	Libre Office	The Document Foundation	7.6.x	I	I	I	I	I	I	11/06/24		
Bureautique	Office	Microsoft	2007	I	I	I	I	I	I	08/10/12	09/10/17	Même statut pour les versions antérieures.
Bureautique	Office	Microsoft	2010	I	A	A	A	I	I	12/10/15	12/10/20	Assujetti : A la demande et aux postes sous Windows 7
Bureautique	Office	Microsoft	2013	I	I	I	I	I	I	09/04/18	10/04/23	
Bureautique	Office	Microsoft	2016	R	R	R	R			12/10/20	13/10/25	
Chiffrement	ACID Cryptofiler	MinArm	V7	R								Chiffrement sur poste au niveau max DR-SF
Chiffrement	ACID Eleonore	MinArm			D	O						Chiffrement au niveau max CD
CI/CD	Gitlab		16.6.x	I	N	I	N	I	N		14/02/24	Gestion du code source et des images localement construites Version CE ou EE identiques sauf niveau de support
CI/CD	Gitlab		17.x	A	N	A	N	A	N		15/08/24	Gestion du code source et des images localement construites Version CE ou EE identiques sauf niveau de support
Communication instantanée	JChat	OTAN		A		A		A				Assujetti au contexte : Interop OTAN / FrOps À utiliser avec le JRE Temurin.
Communication instantanée	Jitsi Meet	Jitsi							A			Utilisé par exemple dans le service interministériel webconf.numerique.gouv.fr
Communication instantanée	Lync	Microsoft	2010	I	D	D	D	I		11/04/16	12/04/21	Cf Microsoft Office 2010

Communication instantanée	Skype for business	Microsoft	2016	R	R	R	I		12/10/20	13/10/25	
Communication instantanée	Tchap	DINUM					R				
Communication instantanée / réunion virtuelle	TCS	OTAN		A	S	A	S	A	S		
Communication instantanée / réunion virtuelle	WEBEX	MinArm				A	N	A	N		
Contrôle d'admission	Kyverno	CNCF/Nirmata	1.10	A	N	A	N	A	N		Moteur de contrôle d'admission (gestion de la confirmité et de la configuration)
Conversion de format	Pandoc	John MacFarlane	2	I	N	I	N	I	N	17/01/23	Outil de conversion mutli-format à préférer à l'installation niveau serveur d'une suite bureautique
Conversion de format	Pandoc	John MacFarlane	3	R	S	R	S	R	S		Outil de conversion mutli-format à préférer à l'installation niveau serveur d'une suite bureautique Dernière version : 3.1.8 (8/09/2023)
Data visualisation	Kibana	Elastic	6.X	I	N	I	N	I	N	09/08/22	
Data visualisation	Kibana	Elastic	7.17.X	R	S	R	S	R	S	30/04/24	Actuelle version LTS - 7.17.X - Sera maintenue jusqu'à la version 9.0.0
Data visualisation	Kibana	Elastic	8.X	A	N	A	N	A	N	09/08/24	Version non recommandée. Cycle de vie rapide. Assujetti à la capacité à le maintenir en version. Privilégier la version 7.17.X considérée comme stable.
Décisionnel Agile / Analyse et visualisation	Grafana	Grafana Labs	10.0.x	I	N				I	23/10/23	

Décisionnel Agile / Analyse et visualisation	Grafana	Grafana Labs	10.1.x	A	N				I	N			
Décisionnel Agile / Analyse et visualisation	Grafana	Grafana Labs	10.2.x	A	N				I	N			
Décisionnel Agile / Analyse et visualisation	Grafana	Grafana Labs	8.x (8.5.27)	I	N	I	N	I	N	I	N	12/06/22	Malgré la règle, encore soutenue en sécurité à date (4/10/23)
Décisionnel Agile / Analyse et visualisation	Grafana	Grafana Labs	9.x	A	N				I	N			
Décisionnel Agile / Analyse et visualisation	Plateforme Ministerielle QlickSense	QlikSense		R	S								
Décisionnel Agile / Analyse et visualisation	PowerBI Server	Microsoft		D	N	I	N	I	N	I	N		
Décisionnel Agile / Analyse et visualisation	QlikSense	QlikSense	May 2021	A	N								
Décisionnel Agile / Analyse et visualisation	Tableau	Tableau Software		D	N				I	N			
Décisionnel Analyse prédictive	Elasticsearch module machine learning	Elastic		A	S								
Décisionnel Analyse prédictive	POCEAD	MinArm		R	S								
Décisionnel Analyse prédictive	Predictive Analysis	SAP		D	O				I	N			
Décisionnel Analyse prédictive	Suite SAS	SAS	9.4	D	O				I	N	30/06/25		

Décisionnel traditionnel	BO Lumira	SAP	2.x	D	O			I	N			
Décisionnel traditionnel	Business Object	SAP	4.1	I	N			I	N	30/11/18	30/11/20	
Décisionnel traditionnel	Business Object	SAP	4.2	I	N			I	N	30/11/22	30/11/24	Déconseillé pour tout nouveau projet. Interdit pour tout projet hors écosystème SAP Maintenu pour les anciens projets en attendant migration vers QlikSense Patch critique seulement jusqu'en décembre 2024
Décisionnel traditionnel	Business Object	SAP	4.3	D	O			I	N	30/11/25	30/11/27	Déconseillé pour tout nouveau projet. Interdit pour tout projet hors écosystème SAP Maintenu pour les anciens projets en attendant migration vers QlikSense
Décisionnel traditionnel	Crystal Report	SAP	2016	D	O			I	N			fin de support 2024. SAP a planifié la fin de ce produit au plus tard fin 2027 SP9
Décisionnel traditionnel	Fast Track	Bull		A	S							
Décisionnel traditionnel	Jaspersoft BI	Tibco		D	N			I	N			Édition Communautaire
Décisionnel traditionnel	Pentaho	Hitachi		D	N			I	N			Édition Communautaire
Décisionnel traditionnel	SQL Server BI SSRS and SAAS	Microsoft		D	N			I	N			Outil de restitution et d'analyse des données (WEBI)

Déploiement	GLPI	Teclib	10.0.x	A	N				I	N				Uniquement pour les parcs non gérés par la DIRISI.
Déploiement	GLPI	Teclib	9.5.x	I	N				I	N	30/06/23			Uniquement pour les parcs non gérés par la DIRISI.
Déploiement	OCS Inventory	OCS Inventory Team	2.11.1	A	N	A		A	I	N				En alternative ou complément à SCCM, pour utilisation particulière hors administration technique DIRISI.
Déploiement / Distribution	MECM	Microsoft	2207	I	N	I	N	I	N	I	11/02/24			
Déploiement / Distribution	MECM	Microsoft	2211	I	N	I	N	I	N	I	18/07/24			
Déploiement / Distribution	MECM	Microsoft	2303	D	O	D	O	D	O	I	23/10/24			
Déploiement / Distribution	MECM	Microsoft	2309	R	S	R	S	R	S		09/04/25			
Déploiement / Distribution	MECM	Microsoft	2403	R	S	R	S	R	S		22/10/25			
Déploiement / Distribution	ORCIDE	MinArm				A	S	A	S					Assujetti : aux configurations projetables du SIA sur théâtres et bâtiments
Déploiement / Distribution	SCCM	Microsoft	2017	I	N	I	N	I	N	I	07/10/23			Dernière version obsolète : passer sur MECM
Distribution	RKE2	CNCF/SUSE	1.27	I	N	I	N	I	N		27/06/24			
Distribution	RKE2	CNCF/SUSE	1.28	D	N	D	N	D	N		27/08/24			
Distribution	RKE2	CNCF/SUSE	1.29	D	N	D	N	D	N		28/02/25			
Distribution	RKE2	CNCF/SUSE	1.30	A	N	A	N	A	N		28/06/25			
DNS	Bind	Internet Systems Consortium	9.16	I	N	I	N	I	N	I	30/04/24			
DNS	Bind	Internet Systems Consortium	9.18	R	S	R	S	R	S	I	30/04/26			
E-formation	ILIAS	Ilias		R	S					R	S			

E-formation	Moodle	Moodle HQ	4.0	I	N				I	N	11/06/23	10/12/23		
E-formation	Moodle	Moodle HQ	4.1	R	S				R	S	10/12/23	09/11/25	Version LTS	
E-formation	Suite SCENARI	UTC		R	S				R	S				
Enquêtes et Sondages	Isidate	DGA		R	S								Sondage sur une date	
Enquêtes et Sondages	LimeSurvey	LimeSurvey	5.X	I	N				I	N	31/05/23	31/05/24	remplace la 5.4 du dernier CCT (maj de sécurité)	
Enquêtes et Sondages	LimeSurvey	LimeSurvey	6.X	R	S				R	S	31/05/25	31/05/26	dernière version	
Enquêtes et Sondages	Sherlock	SGA		R	S									
Environnement Java	Jakarta Enterprise Edition	Oracle	7	I		I		I	I				Même status pour les versions antérieures	
Environnement Java	Jakarta Enterprise Edition	Oracle	8	D		D		D	I				Uniquement pour des systèmes historiques en maintenance. Interdit pour un nouveau développement.	
Environnement Java	Jakarta Enterprise Edition	Oracle	9.0	I		I		I	I				Version de transition, rapidement remplacée par la 9.1 pour un support de Java 11 LTS.	
Environnement Java	Jakarta Enterprise Edition	Oracle	9.1	A		A		A	A				Version actuellement à privilégier pour le framework Jakarta EE mais reste assujetti car l'usage du Framework Spring reste la solution Java backend recommandée	
Environnement Java	JDK	Oracle	11	I	N	I	N	I	N	I	N			
Environnement Java	JDK	Oracle	17	A	S	A	S	A	S	A	S			
Environnement Java	JDK	Oracle	21	A	S	A	S	A	S	A	S			
Environnement Java	JDK	Oracle	8	I	N	I	N	I	N	I	N	30/03/22	30/12/30	
Environnement Java	OpenJDK	Oracle	11	A	S					I	N	29/09/23	30/01/32	Assujetti : Suite à modification politique Oracle sur Java : composant soumis à licence (pour le MCS et le support) et environnement dédié à prévoir pour l'hébergement ou dans le cadre d'une licence l'autorisant. Uniquement pour bénéficier du

Environnement Java	OpenJDK	Oracle	20	I N I N I N I N	31/08/23		Même statut pour les versions non-LTS, ie celles non inscrites au CCT.
Environnement Java	OpenJDK	Eclipse Adoptium	20	I N I N	19/07/23		Même statut pour les versions non-LTS, ie celles non inscrites au CCT.
Environnement Java	OpenJDK	Oracle	21	A S A S A S A S	29/09/28	29/09/31	Lorsqu'aucun autre JDK ne peut être utilisé.
							Cette version LTS a un support exceptionnel de 16 ans du fait de l'étendue du parc logiciel qui utilise cette version. Composant soumis à licence (pour le MCS et le support) Pour un usage serveur : nécessite donc une licence, ainsi qu'un environnement physique dédié à prévoir pour l'hébergement. Uniquement pour bénéficier du support d'un éditeur de solution refusant d'assurer le soutien sur une autre version binaire de ce JDK. Pour un usage client : java 8 est **déconseillé** pour un usage client. Les outils propriétaires doivent être désactivés ainsi que toute mise à jour automatique
Environnement Java	OpenJDK	Oracle	8	A S I N	30/03/22	30/12/30	Pour un usage serveur : Pour système Linux : fournie par la distribution Pour Windows : Eclipse Adoptium (Temurin) Sinon : à justifier
Environnement Java	OpenJDK	Eclipse Adoptium	8	R S R S R S R S	29/11/26		

Environnement Python	Python	Python Software Foundation	3.11	A S	A S	A S	A S	A S	23/10/27		Emploi à justifier.
Environnement Python	Python	Python Software Foundation	3.12	A S	A S	A S	A S	A S	01/10/28		Emploi à justifier.
Environnement Python	Python	Python Software Foundation	3.7	I N	I N	I N	I N	I N	26/06/23		Même statut pour les versions 3.0 à 3.6.
Environnement Python	Python	Python Software Foundation	3.8	D O	D O	D O	D O	I N	13/10/24		Emploi à justifier.
Environnement Python	Python	Python Software Foundation	3.9	A S	A S	A S	A S	A S	04/10/25		Emploi à justifier.
Environnement Ruby	Ruby		3.1	I N	I N	I N	I N	I N	30/03/25		
Environnement Ruby	Ruby		3.2	A N	A N	A N	A N	A N	30/03/26		Assujetti au seul cas de mise en œuvre du service de socle Démarche Simplifié et à l'outil Puppet dans l'attente d'une migration vers Ruche
Environnement Ruby	Ruby		3.3	A N	A N	A N	A N	A N	31/03/27		Assujetti au seul cas de mise en œuvre du service de socle Démarche Simplifiée et à l'outil Puppet dans l'attente d'une migration vers Ruche
ERP	HR Access Suite (Sopra)			A N				I N			
ERP	SAP ECC	SAP		D N				I N			
ERP	SAP HANA / SAP S/4HANA	SAP		A N				I N	18/01/38		

ESB	ServiceMix	Apache Software Foundation	7		D	O	D	O							Uniquement pour les applications s'appuyant sur le framework du SIA
ESB	Talend Open Studio for ESB	Talend	7.2	I	N					I	N	31/12/20	31/05/22		
ESB	Talend Open Studio for ESB	Talend	7.3	D	O					I	N	30/04/23	31/10/24		
ESB	Talend Open Studio for ESB	Talend	8	A	E										Assujetti : lorsque le recours à un ESB se justifie Au besoin version commerciale
ETL	Data Integrator	Oracle	12.1	I	N					I	N	30/11/17	30/11/19		Assujetti aux SI déjà déployés et aux cas d'usage ne pouvant pas être satisfaits par des briques recommandées.
ETL	Data Integrator	Oracle	12.2	A	N					I	N	30/11/26	30/11/27		Assujetti aux SI déjà déployés et aux cas d'usage ne pouvant pas être satisfaits par des briques recommandées.
ETL	Logstash	Elastic	6.X	I	N	I	N	I	N	I	N	09/02/22			Même statut pour les versions précédentes
ETL	Logstash	Elastic	7.17.X	R	S	R	S	R	S	R	S				Actuelle version LTS - 7.17.X - Sera maintenue jusqu'à la version 9.0.0
ETL	Logstash	Elastic	8.X	A	N	A	N	A	N			09/08/23			Version non recommandée. Cycle de vie rapide. Assujetti à la capacité à le maintenir en version. Privilégier la version 7.17.X considérée comme stable.
ETL	SQL Server Integration Services (SSIS)	Microsoft	2012	I	N					I	N	10/07/17	11/07/22		Bull Fast Track (Assujetti à un infocentre en MS)
ETL	SQL Server Integration Services (SSIS)	Microsoft	2016	A	S					I	N	12/07/21	13/07/26		Bull Fast Track (Assujetti à un infocentre en MS). L'actuel

													infocentre opéré par la DIRISI n'intègre plus de nouveaux SI)
ETL	SQL Server Integration Services (SSIS)	Microsoft	2019	A	S				I	N	27/02/25	07/01/30	
ETL	Talend open studio for Data Integration	Talend	7.3	D	O				I	N	30/04/23	31/10/24	
ETL	Talend open studio for Data Integration	Talend	8	R	S								
ETL	Talend Platform Data Management (TPDM)	Talend	6.5.1	I	N				I	N			
ETL	Talend Platform Data Management (TPDM)	Talend	7.3	D	O				I	N	31/10/24		
ETL	Talend Platform Data Management (TPDM)	Talend	8	R	S				A	S			
Forum	PhpBB	phpBB limited	3.3		N								Pas de recommandation du SC2A, assez largement déployé dans les armées recommandé dans le SILL
Framework de développement	.NET	Microsoft	5.0	I	I	I	I	I			07/05/22		Même status pour les versions antérieures
Framework de développement	.NET	Microsoft	6.0	D	D	D	D	D			12/11/24		Version courante 6.0.22 https://dotnet.microsoft.com
Framework de développement	.NET	Microsoft	7	I	I	I	I	I			14/05/24		Attention version non LTS - déconseillée

Framework de développement	.NET Framework	Microsoft	4.7	R S R S R S R S								Le support de .NET 4.7 suit la même politique de cycle de vie que le système d'exploitation parent.
Framework de développement	.NET Framework	Microsoft	4.8	R S R S R S R S								Le support de .NET 4.8 suit la même politique de cycle de vie que le système d'exploitation parent.
Framework de développement	Adobe Integrated Runtime (AIR)		50	D I I I								Migration vers des technologies web recommandé. Sera refusé pour toutes nouvelles applications.
Framework de développement	Angular	Google	15	I I I I						02/05/23	17/05/24	Assujetti à la maintenance des applications déjà en production ou aux projets réalisés par des équipes internes dotés d'une capacité au bon niveau de compétence apte à assurer le MCO et le MCS sur tout la durée du système d'information (1 nouvelle version majeure tous les 6 mois avec un support de 18 mois)
Framework de développement	Angular	Google	16	D D D D						07/11/23	07/11/24	Assujetti à la maintenance des applications déjà en production ou aux projets réalisés par des équipes internes dotés d'une capacité au bon niveau de compétence apte à assurer le MCO et le MCS sur tout la durée du système d'information (1 nouvelle version majeure tous les 6 mois avec un support de 18 mois)
Framework de développement	Angular	Google	17	D D D D						08/05/24	15/05/25	Assujetti à la maintenance des applications déjà en production ou aux projets réalisés par des équipes internes dotés d'une capacité au bon niveau de compétence apte à assurer le MCO et le MCS sur tout la durée du système d'information (1

											nouvelle version majeure tous les 6 mois avec un support de 18 mois)	
Framework de développement	Angular	Google	18	A	A	A	A		22/11/24	22/11/25	Assujetti à la maintenance des applications déjà en production ou aux projets réalisés par des équipes internes dotés d'une capacité au bon niveau de compétence apte à assurer le MCO et le MCS sur tout la durée du système d'information (1 nouvelle version majeure tous les 6 mois avec un support de 18 mois)	
Framework de développement	Bootstrap		4	I	N	I	N	I	N	I	N	Dernière version : 4.6.2
Framework de développement	Bootstrap		5	R		R		R		R		Dernière version sortie 5.3.0 (30/05/2023)
Framework de développement	Capacitor		4	I		I		I		I		02/11/23 02/05/24
Framework de développement	Capacitor		5	D		D		D		I		15/10/24 15/04/25
Framework de développement	Capacitor		6	A		A		A		A		
Framework de développement	Cordova	Apache Software Foundation	12	A	A	A	A	A			Développement d'applications s'appuyant sur Ionic	
Framework de développement	Django		3.2	I	N	I	N	I	N	I	N	Les applications MVC doivent s'appuyer sur les technologies recommandées du CCT. Le langage python n'est pas recommandé pour réaliser des applications WEB.

Framework de développement	Django		4.2	I N I N I N I N		03/12/23	31/03/26	Les applications MVC doivent s'appuyer sur les technologies recommandées du CCT. Le langage python n'est pas recommandé pour réaliser des applications WEB.
Framework de développement	Django		5.2	I N I N I N I N		30/11/25	31/03/28	Les applications MVC doivent s'appuyer sur les technologies recommandées du CCT. Le langage python n'est pas recommandé pour réaliser des applications WEB.
Framework de développement	Electron		29	I I I I		20/08/24		Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an).
Framework de développement	Electron		30	D D D D		15/10/24		Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an).
Framework de développement	Electron		31	D D D D		07/01/25		Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an).
Framework de développement	Electron		32	A A A A		04/03/25		Assujetti aux cas nécessitant impérativement le développement d'un client lourd et une capacité à réaliser un MCS très fréquent (au moins 2 fois par an).
Framework de développement	Ionic		6	I I I I		28/09/23	28/03/24	Développement d'applications mobiles nécessitant un accès aux SDKs natifs.

Framework de développement	Ionic		7	D	D	D	I		17/04/24	17/04/25	Développement d'applications mobiles nécessitant un accès aux SDKs natifs.
Framework de développement	Ionic		8	A	A	A	A				Développement d'applications mobiles nécessitant un accès aux SDKs natifs.
Framework de développement	JHipster		8	R	R	R	R				Générateur de projet d'application Spring Boot intégrant la réalisation d'un frontend avec Vue.js, React ou Angular.
Framework de développement	jQuery		2	I	I	I	I				
Framework de développement	jQuery		3	D	D	D	I				Technologie en obsolescence qui ne doit plus être utilisée pour les nouveaux projets. Les composants associés sont dépréciés les uns après les autres (jquery Mobile par exemple) tandis que jquery-ui (1.13) est en mode restreint à la maintenance.
Framework de développement	Laravel	Laravel	10	D	D	D	D		06/08/24	06/02/25	Compatible PHP 8.1-8.3
Framework de développement	Laravel	Laravel	11	R	R	R	R		05/08/25	03/02/26	Compatible PHP 8.2 et 8.3
Framework de développement	Laravel	Laravel	9	I	I	I	I		07/08/23	07/02/24	Dernière version 9.52.9
Framework de développement	NestJS		10	A	A	A	A				
Framework de développement	Next.js		14	A	A	A	A				Assujetti à la réalisation avec React de SI exposés sur Internet et pour lesquels l'optimisation du référencement par les moteurs de recherche (SEO) est un besoin métier majeur.

Framework de développement	Node.js	OpenJS Foundation	18	I N I N I N I N	29/04/25		
Framework de développement	Node.js	OpenJS Foundation	20	R S R S R S R S	29/04/26		
Framework de développement	Node.js	OpenJS Foundation	21	I N I N I N I N	29/04/26		Version interdite en raison du cycle de vie très court (soutien des versions impaires inférieur à 1 an). Même statut pour les autres versions impaires.
Framework de développement	Node.js	OpenJS Foundation	22	R S R S R S R S	29/04/26		
Framework de développement	Nuxt.js		2	I I I I	30/12/23		
Framework de développement	Nuxt.js		3	A A A A			Assujetti à la réalisation avec Vue.js de SI exposés sur Internet et pour lesquels l'optimisation du référencement par les moteurs de recherche (SEO) est un besoin métier majeur.
Framework de développement	React		18	R R R R			
Framework de développement	Ruby on Rails		6.1	I N I N I N I N			
Framework de développement	Spring	VMWare	5.2	I I I I	30/12/21	30/12/23	Attention support étendu disponible uniquement sur souscription d'une offre commerciale.
Framework de développement	Spring	VMWare	5.3	R R R R	30/12/24	30/12/26	Attention support étendu disponible uniquement sur souscription d'une offre

													commerciale.
													Compatibilité java 8 - 11 et 17 et javaEE 7 et 8.
Framework de développement	Spring	VMWare	6.0	D	D	D	I						Attention support étendu disponible uniquement sur souscription d'une offre commerciale.
Framework de développement	Spring Boot	VMWare	2.6	I	I	I	I						Compatibilité java 17 et jakartaEE 9 et 10. Il est donc recommandé aux projets utilisant cette technologie en v5.3 de planifier une montée de version majeure dans leur feuille de route en 2024.
Framework de développement	Spring Boot	VMWare	2.7	D	D	D	I						Nécessite l'acquisition d'un support étendu disponible uniquement sur souscription d'une offre commerciale.
Framework de développement	Spring Boot	VMWare	3.0	D	D	D	I						Compatibilité java 8 - 20

Framework de développement	Spring Boot	VMWare	3.1	D	D	D	D	17/05/24	17/08/25	Compatibilité java 17 - 20	<p>La fonction permettant d'embarquer un serveur d'application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs).</p> <p>Nécessite également de monter un certain nombre de versions de frameworks en dépendance (Elasticsearch client 8.7, SLF4J 2.0 ... par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route en 2024.</p> <p>Attention support étendu disponible uniquement sur souscription d'une offre commerciale.</p>
Framework de développement	Spring Boot	VMWare	3.2	D	D	D	D	23/11/24	23/02/26	Compatibilité java 17 - 20	<p>La fonction permettant d'embarquer un serveur d'application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs).</p> <p>Nécessite également de monter un certain nombre de versions de frameworks en dépendance (Elasticsearch client 8.7, SLF4J 2.0 ... par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route en 2024.</p>

											par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route en 2024.
											Attention support étendu disponible uniquement sur souscription d'une offre commerciale.
											Compatibilité java 17 - 20
Framework de développement	Spring Boot	VMWare	3.3	R	R	R	R	R	23/05/25	23/08/26	La fonction permettant d'embarquer un serveur d'application ne doit pas être utilisée (hors des environnements de développement ou en hébergement en orchestration de conteneurs).
											Nécessite également de monter un certain nombre de versions de frameworks en dépendance (Elasticsearch client 8.7, SLF4J 2.0 ... par exemple). Il est donc recommandé aux projets utilisant cette technologie de planifier une montée de version majeure dans leur feuille de route en 2024.
											Attention support étendu disponible uniquement sur souscription d'une offre commerciale.
											Compatibilité java 17 - 20

Framework de développement	Symfony	Symfony SAS	5.4	R	R	R	R		29/11/24	29/11/25	Privilégier la version LTS 6.4 pour tout nouveau développement.	
Framework de développement	Symfony	Symfony SAS	6.3	I	I	I	I		30/01/24			
Framework de développement	Symfony	Symfony SAS	6.4	R	R	R	R		29/11/26	29/11/27		
Framework de développement	Symfony	Symfony SAS	7.x	I	I	I	I					
Framework de développement	Vue.js	Evan You	2	I	I	I	I		30/12/23			
Framework de développement	Vue.js	Evan You	3	R	R	R	R					
GED	Alfresco Community edition	Hyland	7.0	I	N	I	N	I	N	28/02/23	29/02/24	
GED	Alfresco Community edition	Hyland	7.1	D	O	D	O	D	O	30/09/23	30/09/24	
GED	Alfresco Community edition	Hyland	7.2	D	O	D	O	D	O	29/02/24	28/02/25	
GED	Alfresco Community edition	Hyland	7.3	R	S	A	S	A	S	31/10/24	31/10/25	
GED	Alfresco Community edition	Hyland	7.4	R	S	A	S	A	S	30/04/25	30/04/26	
Génération image	Packer	Hashicorp	1.9.4	R	E							
Gestion de clusters	Rancher	CNCF/SUSE	2.7	D	N	D	N	D	N	14/05/24	17/11/24	Permet de piloter des ensembles de clusters et de gérer les ressources Kubernetes déployées. Retenu pour les offres de conteneurisation cloud C1 du Ministère.

Gestionnaire de backup	Velero	CNCF/SUSE	1.11	A N A N A N						Solution de sauvegarde et restauration de clusters Kubernetes Choisir la version en fonction du support de la version Kubernetes (cf documentation Velero)
Hypervision / Virtualisation	Hyper-V	Microsoft	2012R2	D O D O D O	I	N				Assujetti : uniquement dans les configurations projetables (théâtre et bâtiments tous intranet et sites de proximité STC-IA V02) Le type 1 (bare metal) est à privilégier.
Hypervision / Virtualisation	Hyper-V	Microsoft	2016	A S A S A S				10/01/22	11/01/27	Dans le cadre du projet Mishuco, en OME Le type 1 (bare metal) est à privilégier.
Hypervision / Virtualisation	Hyper-V	Microsoft	2019	A S A S A S				08/01/24	08/01/29	Dans le cadre du projet Mishuco, en OME Le type 1 (bare metal) est à privilégier.
IA/ Big Data	Flink	Apache Software Foundation	1.16.x	E N						
IA/ Big Data	Flink	Apache Software Foundation	1.17.x	E N						1.17.1 actuellement la dernière
IA/ Big Data	NiFi	Apache Software Foundation	1.17	I N I N I N I N	05/10/22					

IA/ Big Data	NiFi	Apache Software Foundation	1.23	E N E N E N									
IA/ Big Data	Spark	Apache Software Foundation	3.2.X	D N D N D N I N							12/10/24		Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.
IA/ Big Data	Spark	Apache Software Foundation	3.3.X	D N D N D N I N							20/02/25		Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.
IA/ Big Data	Spark	Apache Software Foundation	3.4.X	A N A N A N							22/12/25		Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.
IA/ Big Data	Spark	Apache Software Foundation	3.5.X	A N A N A N							12/03/26		Cette solution peut être envisagée pour la recherche, l'extraction, le traitement et le chargement de gros volumes ou gros flux de données.
IGC	IGC-G	MinArm		D O D O D O									Infrastructure de gestion de clés ancienne génération - Dépréciée, lui préférer IGC-G NG
IGC	IGC-G NG	MinArm		R S R S R S									Nouvelle infrastructure de gestion de clés - A privilégier
Intégration continue	Jenkins		2	A N A N A N									Bascule en cours vers GitlabCI sur PICSEL
Interface réseau pour conteneurs	Calico	CNCF/Nirmata	3.26	A N A N A N									Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2.

Interface réseau pour conteneurs	Cilium	CNCF/Isovalent	1.14	A N A N A N									Greffon de gestion du réseau sur un cluster Kubernetes reposant sur l'eBPF et permettant la création de politiques réseaux avancées. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère.
Messagerie	Cyrus IMAP	Université Carnegie-Mellon	3.4.x	A S					I N				Apporte la gestion des network policies sur les noms de domaine contrairement à Calico (à vérifier)
Messagerie	NEMO	MinArm	2	R S									Utilisé en serveur SMTP/IMAP d'appoint, assujetti à une dérogation sur le cadre d'emploi - Dernière version mineure 3.4.5 du 27/2/23
Messagerie	NEMO	MinArm	3		R S	R S							Addon outlook
Messagerie	Outlook	Microsoft	2010		D	D				12/10/15	12/10/20		Cf Office 2010
Messagerie	Outlook	Microsoft	2016	R	R	R				12/10/20	13/10/25		Cf Office 2016
Messagerie	OWA	Microsoft		R									Outlook Web Access est une fonctionnalité portée par les serveurs Microsoft Exchange. Cf ce dernier pour les dates de fin de support.
Messagerie	postfix	Postfix.org	3.5	I N I N I N									
Messagerie	postfix	Postfix.org	3.6	A S A S A S				I N					Assujetti a une dérogation sur le cadre d'emploi.
Messagerie	postfix	Postfix.org	3.7	A S A S A S				I N					Assujetti a une dérogation sur le cadre d'emploi.
													Utilisé dans SIE et NEMO (bordure du système)

Messagerie	postfix	Postfix.org	3.8	A S A S A S I N			Assujetti à une dérogation sur le cadre d'emploi.
Messagerie	postfix	Postfix.org	3.9	A S A S A S I N			Assujetti à une dérogation sur le cadre d'emploi. Utilisé dans SIE et NEMO (bordure du système)
Messagerie	SOGO			A			Assujetti au contexte SIE : Webmail pour le SIE (Baltique/Celtique), connectable avec le client Outlook et offrant des fonctions de partage de calendriers et de carnets d'adresses. Application responsive accessible sur SMOBI tablette ou smartphone.
Messagerie	Thunderbird	Mozilla	115 ESR	A			
MessagerieAgenda	Exchange	Microsoft	2010	I N I N I N I N	12/10/20		Même status pour les versions antérieures
MessagerieAgenda	Exchange	Microsoft	2016	R S R S R S I N	13/10/20	13/10/25	
Métrologie	Dynatrace	Dynatrace	1.2.X	R S			
Moniteur de transfert	CFT	Axway		A S			Assujetti à des échanges avec des partenaires hors MinArm
Moteur de conteneurisation	Containerd	CNCF	1.7	A N A N A N			Par extension, tout moteur s'appuyant sur cet exécutable. Inclus dans la distribution RKE2 et retenu pour les offres de conteneurisation cloud C1 du Ministère.
Moteur de recherche	Qwant	Qwant			R		
Moteur de recherche	Sinequa	Sinequa		A S R S R S			Assujetti sur Intradef lorsque Syriam n'est pas utilisable
Moteur de recherche	SYRIARM	MinArm		R S			
Multimédia	VLC	Videolan		R	R		

Navigateur	Edge	Microsoft		R	E	E					
Navigateur	Firefox	Mozilla	102	D	D	D	I		25/07/22	25/09/23	Version ESR
Navigateur	Firefox	Mozilla	115	R	R	R	R		31/07/23	30/09/24	Version ESR
											Pour les postes installés en Windows 7
Navigateur	Firefox	Mozilla	38		D	D			29/06/15	06/06/16	Version ESR
Navigateur	Firefox	Mozilla	68	I	D	D	I		21/09/20		Version ESR
Navigateur	Firefox	Mozilla	91	D					06/09/21	19/09/22	Version ESR
Navigateur	Internet Explorer	Microsoft	11	I	I	I	I		14/06/22		Déconseillé par Microsoft
Orchestrateur	Kubernetes	CNCF	1.27	I	N	I	N	I	N		<p>Orchestrator de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère.</p> <p>Une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.</p>

Orchestrator	Kubernetes	CNCF	1.28	D	N	D	N	D	N	28/10/24	<p>Orchestrator de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère.</p> <p>Une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.</p>
Orchestrator	Kubernetes	CNCF	1.29	D	N	D	N	D	N	28/02/25	<p>Orchestrator de conteneurs de référence, développé initialement par Google et retenu pour les offres de conteneurisation cloud C1 du Ministère.</p> <p>Une nouvelle version de Kubernetes est publiée tous les 4 mois et est soutenue pour environ 1 an. Les directions de projet doivent donc organiser en conséquence pour soutenir ce rythme de mise à jour. La complexité des écosystèmes nécessaires pour faire fonctionner l'ensemble des briques nécessaire à l'orchestration de conteneurs plaide pour le recours à une distribution.</p>

Orchestrator	Kubernetes	CNCF	1.30	A I	N N	A I	N I	A N	N I	A N	N I								
Orchestration	Ansible	Redhat	2.14	I D	N O	I D	N O	I D	N O	I D	N O								
Orchestration	Ansible	Redhat	2.15	D D	O O	D D	O O	D D	O O	D D	O O								
Orchestration	Ansible	Redhat	2.16	D D	O O	D D	O O	D D	O O	D D	O O								
Orchestration	Ansible	Redhat	2.17	R R	S S	R R	S S	R R	S S	R R	S S								

Orchestration	Ansible Automation Platform	Redhat		A	S				A	S	30/12/25		Utilisé dans le cadre et conformément à Ruche. Également soutenu sur PICSEL
Orchestration	Puppet	Puppet Labs	6.x	I							27/02/23		Dans l'attente de rejointe de la cible Ansible. Présent dans SIE, DGA Dernière version : 6.29 (01-2023)
Orchestration	Puppet	Puppet Labs	7.x	A									Sur SIE (version Baltique), pour la distribution des configurations. A titre transitoire, sur environnement S2NA
Orchestration	Puppet	Puppet Labs	8.x	D									Sur SIE (version Baltique), pour la distribution des configurations. A titre transitoire, sur environnement S2NA
Pare feux	Palo Alto	Palo Alto		R	S	R	S	R	S	R	S		
Partage de données geospatial	Geoserver			A	N	A	N	A	N				
PEM API	PEM Internet	MinArm								E	E		Passerelle d'échange mutualisée (basée sur la solution WSO2 API MANAGER). Usage obligatoire dans le cadre des échanges inter applicatifs (format API) au sein de l'internet maitrisé mais également dans le cadre des échanges inter applicatifs entre Internet maitrisé et Internet public.
PEM API	PEM Intradef	MinArm		R	S								Passerelle d'échange mutualisée (basée sur la solution WSO2 API MANAGER). Usage obligatoire dans le cadre des échanges inter

														applicatifs (format API) au sein de l'intradef.
PEM API	WSO2 API Manager	WSO2	2.6.0	I	N				I	N	21/10/22			Version obsolète. Privilégier l'emploi de la version 4.1.0. Cas d'usage et utilisation à justifier.
PEM API	WSO2 API Manager	WSO2	4.1.0	A	N						10/04/27			Version recommandée pour tout usage hors instances ministérielles mutualisées. Cas d'usage et utilisation à justifier.
Plugin	Flash player	Adobe	32	I		I		I		I	30/12/20			Interdit pour tout nouveau projet. Désactivé sur tous les navigateurs à partir de début 2021. Même statut pour les versions inférieures.
Plugin	Silverlight	Microsoft	5	I		I		I		I	11/10/21			
Portail d'information	Drupal	Drupal	10.1.x	I	N				I	N	30/11/23			
Portail d'information	Drupal	Drupal	10.2	R	S				R	S				10.3 annoncée pour juin 2024
Portail d'information	Drupal	Drupal	6.x	I	N				I	N	23/02/16			
Portail d'information	Drupal	Drupal	7.x	D	O				I	N	04/01/25			C'est la seule version LTS, mais si elle est encore soutenue, ses dépendances sont obsolètes (symfony, jquery,...) Dernière version : 7.98, du 7 juin 2023
Portail d'information	Drupal	Drupal	8.x	I	N				I	N	01/11/21			Version stable 8.9
Portail d'information	Drupal	Drupal	9.5	I	N				I	N	31/10/23			La version 9 utilise symfony 4 et partage sa fin de vie / fin de support. La 9.5 est la dernière 9.x
Portail d'information	Joomla!	Joomla!	4.3	I	N				I	N	30/10/23			Même status pour les versions antérieures
Portail d'information	Joomla!	Joomla!	4.4	R	S				R	S	16/10/25			

Portail d'information	Joomla!	Joomla!	5.0	R S				R S						
Portail d'information	Wordpress	Wordpress Foundation	6.2	I N	I N	I N	I N	I N	I N	07/08/23				
Portail d'information	Wordpress	Wordpress Foundation	6.3	A E	A E	A E	A E							
Portail personnalisable	Liferay Portal	Liferay	7.4.x	R S	R S	R S	R S	R S	R S					
Portail personnalisable	Sharepoint	Microsoft	2010	I N	I N	I N	I N	I N	I N	08/10/23				
Portail personnalisable	Sharepoint	Microsoft	2013	I N	I N	I N	I N	I N	I N	09/04/18	10/04/23			
Portail personnalisable	Sharepoint	Microsoft	2016	R S	R S	R S	R S	I N	I N	12/07/21	13/07/26			
Provisionnement	Terraform	Hashicorp	1.4.x		I N	I N	I N			03/10/23				
Provisionnement	Terraform	Hashicorp	1.5.x		R E	R E	R E							
Provisionnement	Terraform	Hashicorp	1.6.x		R E	R E	R E							Dernière versions supportée 1.6.2 du 18/10/23
Qualimétrie	SonarQube		8.9	I N						06/02/23				Sonar dédié en zone projet PICSEL intégré à la CI/CD

					R	S											Statut : Soutenu sur PICSEL
Qualimétrie	SonarQube		9.9		R	S											
Qualité des données	InfoSphere Information Server	IBM	11.7	A	E												Dernière version à date de rédaction : 11.7.1.4
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	1.9	I	N	I	N	I	N	I	N		30/07/20				Même statut pour les versions impaires
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.2	R	S	R	S	R	S	R	S		06/07/25				
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.4	R	S	R	S	R	S	R	S		13/05/26				
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.6	R	S	R	S	R	S	R	S		30/05/27				
Reverse proxy / Répartiteur de charge	HAProxy	Communauté HAProxy	2.8	R	S	R	S	R	S	R	S		30/05/28				
RPA	OpenRPA	OPEN IAP	1.4.x	A	S												Alternative open source à UiPath
RPA	UiPath	UiPath	2022.10	A	S									26/10/24	26/10/25		Cette technologie devant être considérée comme un moyen temporaire d'amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d'une rejoints vers un environnement non dérogatoire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n'exonère pas du respect des règles de l'Intradef et de facto, n'autorise pas son emploi au travers d'ISPT.

RPA	UiPath	UiPath	2022.4	A	S					08/05/24	08/05/25	Cette technologie devant être considérée comme un moyen temporaire d'amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d'une rejoiante vers un environnement non dérogatoire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n'exonère pas du respect des règles de l'Intradef et de facto, n'autorise pas son emploi au travers d'ISPT.
RPA	UiPath	UiPath	2023.4	A	S					26/04/25	26/04/26	Cette technologie devant être considérée comme un moyen temporaire d'amélioration du fonctionnement de dispositifs anciens, son usage est assujetti à une demande de dérogation justifiant d'une rejoiante vers un environnement non dérogatoire. Deux modes de fonctionnement sont possibles, le mode managé (fonctionnement sur serveur) et non managé (déclenchement sur le poste). Son emploi n'exonere pas du respect des règles de l'Intradef et de facto, n'autorise pas son emploi au travers d'ISPT
Sauvegarde	MIRIA (ADA)	Atempo	3.15	D	O					23/02/24		
Sauvegarde	MIRIA (ADA)	Atempo	4.0.x	R	S							

Sauvegarde	Time Navigator (TINA)	Atempo	4.6.9	I N									Pour les données structurées avec sauvegarde bande / Par défaut en offre VPS Alias TINA 2021 R1
Sauvegarde	Time Navigator (TINA)	Atempo	4.7.1	D O								30/11/24	Pour les données structurées avec sauvegarde bande / Par défaut en offre VPS
Sauvegarde	Time Navigator (TINA)	Atempo	4.8.x	R S									Pour les données structurées avec sauvegarde bande / Par défaut en offre VPS
Sauvegarde	Veeam Backup & Replication	Veeam	11	I N I N I N							31/01/23	31/01/24	
Sauvegarde	Veeam Backup & Replication	Veeam	12	R S R S R S								31/01/26	
Sécurité	Zed!	Prim'X	2022.4	A									Assujetti en l'absence de ACID aux échanges interministériels au niveau max DR.
Serveur d'application	Tomcat	Apache Software Foundation	10.0.X	I N I N I N I N							30/10/22		Version obsolète
Serveur d'application	Tomcat	Apache Software Foundation	10.1.X	R S R S R S R S									implémente les spécifications Java EE 10 : Servlet 6.0, JSP 3.1, EL 5.0 et WebSocket 2.1 Compatible java 11 et +
Serveur d'application	Tomcat	Apache Software Foundation	8.0.x	I N I N I N I N							29/06/18		Version obsolète
Serveur d'application	Tomcat	Apache Software Foundation	8.5.X	I N I N I N I N							30/03/24		implémente les spécifications Java EE 7 : Servlet 3.1, JSP 2.3, EL 3.0 et WebSocket 1.0 Compatible java 7 et +

Serveur d'application	Tomcat	Apache Software Foundation	9.X	R S R S R S R S		03/10/27	implémente les spécifications Java EE 8 (JASPI 1.1) : Servlet 4.0, JSP 2.3, EL 3.0 et WebSocket 1.1 Compatible java 8 et +
Serveur HTTP / Proxy HTTP / Cache HTTP	HTTP Server	Apache Software Foundation	2.2.x	I N I N I N I N			
Serveur HTTP / Proxy HTTP / Cache HTTP	HTTP Server	Apache Software Foundation	2.4.x	R S R S R S R S			
Serveur HTTP / Proxy HTTP / Cache HTTP	IIS	Microsoft	10*	A S A S A S A S		11/01/27	* : Version pour Windows Server 2016 Assujetti au déploiement de solutions adhérentes à l'écosystème Microsoft
Serveur HTTP / Proxy HTTP / Cache HTTP	IIS	Microsoft	10*	A S A S A S A S		08/01/29	* : Version pour Windows Server 2019 Assujetti au déploiement de solutions adhérentes à l'écosystème Microsoft
Serveur HTTP / Proxy HTTP / Cache HTTP	IIS	Microsoft	8.5	I N I N I N I N		09/10/23	Version pour Windows Server 2012 R2
Serveur HTTP / Proxy HTTP / Cache HTTP	Nginx	Nginx	1.24.X	I N I N I N I N			Largement utilisé sur l'Internet . NGINX a justifier par rapport à Httpd Apache.
Serveur HTTP / Proxy HTTP / Cache HTTP	Nginx	Nginx	1.26.X	R S R S R S R S			Largement utilisé sur l'Internet . NGINX a justifier par rapport à Httpd Apache.
Serveur HTTP / Proxy HTTP / Cache HTTP	Nginx	Nginx	1.27.x	I N I N I N I N			Même statut pour les versions mineures impaires.

Serveurs d'application Java	Jetty	Eclipse	11	I	N			I	N	31/12/23		Assujetti à des cas d'usage de micro-services implémente les spécifications Java EE 9 : Servlet 5.0. Nécessite un openJDK en version 11 ou +.
Serveurs d'application Java	Jetty	Eclipse	12	A	N							Assujetti à des cas d'usage de micro-services implémente les spécifications Java EE 8, 9 et 10. Nécessite un openJDK en version 17 ou +.
Serveurs d'application Java et d'EJB	Glassfish	Oracle	6	D	O				I	N		Privilégier Payara / Wildfly À partir de la version 6.1, implémente JakartaEE 9.1. Nécessite openJDK 11 ou 17.
Serveurs d'application Java et d'EJB	Glassfish	Oracle	7	D	O				I	N		Privilégier Payara / Wildfly Implémente JakartaEE 10. Nécessite openJDK 11 ou 17 ; le 17 est nécessaire à l'utilisation de MicroProfile.
Serveurs d'application Java et d'EJB	Jboss EAP	Redhat	6	I	N			I	N	29/06/19	29/06/22	Assujetti à une exigence de support.
Serveurs d'application Java et d'EJB	Jboss EAP	Redhat	7	A	S			A	S	29/06/25	29/11/26	Assujetti à l'usage de JakartaEE et à une exigence de support.
Serveurs d'application Java et d'EJB	Payara Server	Payara Services Ltd	5	I	N			I	N	29/11/22		Implémente JakartaEE 8. Nécessite un OpenJDK en version 8, 11 ou 17.
Serveurs d'application Java et d'EJB	Payara Server	Payara Services Ltd	6.x	D	O			I	N	31/12/27	31/12/32	Implémente JakartaEE 10. Nécessite un OpenJDK en version 11 ou 17.
Serveurs d'application Java et d'EJB	TomEE	Apache Software Foundation	8	I	N			I	N	30/12/23		Tomcat reconfiguré pour supporter aisément les EJB

Serveurs d'application Java et d'EJB	TomEE	Apache Software Foundation	9		A	S				A	S				Assujetti à l'usage de JarkartaEE.
Serveurs d'application Java et d'EJB	Wildfly	Redhat	33	I	N	I	N	I	N	I	N	26/09/24			Attention : évolution de version fréquente, MCS régulier à prévoir. Date de fin de support approximative.
Serveurs d'application Java et d'EJB	Wildfly	Redhat	34	D	O	D	O	D	O	I	N	12/12/24			Attention : évolution de version fréquente, MCS régulier à prévoir. Date de fin de support approximative.
SGBDR	Galera Cluster	Codership		R	S					R	S				Versions : celles embarquées dans les versions recommandées de MariaDB.
SGBDR	MariaDB	MariaDB Foundation	10.10	I	N	I	N	I	N	I	N	16/11/23			Même status pour les versions antérieures, sauf mention contraire.
SGBDR	MariaDB	MariaDB Foundation	10.11	R	S	R	S	R	S	R	S	15/02/28			Version disposant d'un support de long terme (LTS).
SGBDR	MariaDB	MariaDB Foundation	10.6	R	S	R	S	R	S	R	S	05/07/26			Version disposant d'un support de long terme (LTS).
SGBDR	MariaDB	MariaDB Foundation	11.1	I	N	I	N	I	N	I	N	20/08/24			Version non LTS - déconseillée
SGBDR	MySQL	Oracle	5.7	I	N	I	N	I	N	I	N	30/10/23			Cette version a été la dernière version soutenue par le Ministère jusqu'à sa fin de support (opter pour mariaDB ou PostgreSQL)
SGBDR	MySQL	Oracle	8.0	D	N	D	N	D	N	I	N	31/03/25	31/03/26		
SGBDR	MySQL	Oracle	8.1	I	N	I	N	I	N	I	N				Même status pour les versions supérieures

										Dernière version : 12.2.0.1 La fin du support étendue est valable avec ES/ULA. Sans, le support étendu prend fin le 30 avril 2026. Emploi à dûment justifier pour les nouveaux projets, migration à envisager pour les anciens. (*) Soutien uniquement sur structures mutualisées (Exadata)
SGBDR	Oracle Database	Oracle	12.2	I	N			I	N	30/07/18 30/03/22
SGBDR	Oracle Database	Oracle	19c	A	S			I	N	29/04/24 29/04/27
SGBDR	PostGIS	PostGIS	2.5	I	N			I	N	11/11/22
SGBDR	PostGIS	PostGIS	3.0	A	S			A	S	12/11/25
SGBDR	PostGIS	PostGIS	3.1	A	S			A	S	11/11/26
SGBDR	PostGIS	PostGIS	3.2	A	S			A	S	10/11/27
SGBDR	PostGIS	PostGIS	3.3	A	S			A	S	08/11/28
SGBDR	PostGIS	PostGIS	3.4	A	S			A	S	08/11/28

SGBDR	PostgreSQL	PostgreSQL Global Development Group	11.x	I N I N I N I N	08/11/23		
SGBDR	PostgreSQL	PostgreSQL Global Development Group	12.x	D O D O D O D O	13/11/24		
SGBDR	PostgreSQL	PostgreSQL Global Development Group	13.x	R S R S R S R S	12/11/25		Version : 13 dans Ruche Sur HELISING : version portée par Redhat 7 et Redhat 8
SGBDR	PostgreSQL	PostgreSQL Global Development Group	14.x	R S R S R S R S	29/09/26		version cible 14.7
SGBDR	PostgreSQL	PostgreSQL Global Development Group	15.X	R S R S R S R S	10/11/27		version cible 15.2
							Un changement de version ou une sortie doit être envisagée. Il est possible de payer pour un support de sécurité jusqu'en juillet 2025.
SGBDR	SQL Server	Microsoft	2012	I N I N I N I N	10/07/17	11/07/22	Dernier service pack : SP4
SGBDR	SQL Server	Microsoft	2014	I N I N	08/07/19	08/07/24	Dernier service pack : SP3
SGBDR	SQL Server	Microsoft	2016	A S A S A S I N	12/07/21	13/07/26	Dernier service pack : SP3
SGBDR	SQL Server	Microsoft	2017	A N A N A N	10/10/22	11/10/27	
SGBDR	SQL Server	Microsoft	2019	A S	27/02/25	07/01/30	La DIRISI envisage le soutien de cette version comme successeur de SQL Server 2016
SGBDR	SQL Server	Microsoft	2022	E E E E	10/01/28	10/01/33	

SGBDR	SQLite	SQLite		A	N																			
SSO	FranceConnect Particulier	DINUM												R										Pour un besoin générique sans nécessité de savoir que l'utilisateur est un agent ou un ayant droit du ministère. Est soutenu par la DINUM.
SSO	Kerberos	Microsoft		A	S	R	S	R	S	I	N												Option qui va être proposée par MindefConnect courant 2024	
SSO	Keycloak	Redhat	23.x	A	S					I	N												Assujetti pour tout autre usage que MindefConnect sur intradef	
SSO	MindefConnect Internet	MinArm								R	S												Basé sur RedHatSSO	
SSO	MindefConnect Intradef	MinArm		R	S																		Basé sur RedHatSSO	
SSO	Red Hat Single Sign-On	Redhat	7.x	A	S												29/06/22	29/06/25				Assujetti pour tout autre usage que MindefConnect si besoin de support		
SSO	Sign&Go	Ilex	5.1			A	S	A	S														Assujetti aux cas d'utilisation en cours.	
SSO/Authentification mutualisée	Web services Annudef	MinArm		D	O																		Permet de monter des disques vSphere sur les nœuds d'un cluster Kubernetes afin de créer des volumes persistants.	
Stockage	CSI vSphere	VMWare	3.0	D	N	D	N	D	N	D	N	D	N	D	N	31/03/25							Infra hors cloud C1, requis quand sous-jacent VMWare notamment pour Kasten et Velero.	
																							Compatible kubernetes 1.24-1.27	

Stockage	CSI vSphere	VMWare	3.1	A	N	A	N	A	N	A	N	30/09/25		Permet de monter des disques vSphere sur les nœuds d'un cluster Kubernetes afin de créer des volumes persistants. Infra hors cloud C1, requis quand sous-jacent VMWare notamment pour Kasten et Velero. Compatible kubernetes 1.26-1.28
Stockage	CSI vSphere	VMWare	3.2	A	N	A	N	A	N	A	N	31/03/26		Permet de monter des disques vSphere sur les nœuds d'un cluster Kubernetes afin de créer des volumes persistants. Infra hors cloud C1, requis quand sous-jacent VMWare notamment pour Kasten et Velero. Compatible kubernetes 1.27-1.29
Stockage	IRIS	MinArm		R	S	E	E							Stockage objet de fichiers et métadonnées au travers du protocole S3 et de données froides (archivage, sauvegarde). En cours d'intégration sur le SIA.
Stockage	Portworx	Pure Storage	3.0.x	A	N	A	N	A	N			10/01/24		Solution de gestion de stockage sur baies Pure Storage.
Stockage	Scality Ring			A	S	E	E							Pour IRIS.
Supervision	Shinken	Shinken Solutions	2.4.3	R	S	R	S	R	S					Sur les intranets classifiés, inclus dans GSYS
Synchronisation horaire	NTP	Meinberg	4.2.8	A	N	A	N	A	N					
Système d'exploitation	Android	Google	10	A								05/03/23		Assujetti aux SMOBI

															Nom alternatif de la version : Queen Cake
Système d'exploitation	Android	Google	11	E											Assujetti aux SMOBI Nom alternatif de la version : Red Velvet Cake
Système d'exploitation	Android	Google	12	E											Assujetti aux SMOBI Nom alternatif de la version : Snow Cone
Système d'exploitation	Android	Google	8	D										30/10/21	Nom alternatif de la version : Oreo
Système d'exploitation	Android	Google	9	D										30/01/22	Nom alternatif de la version : Pie
Système d'exploitation	RedHat Enterprise Linux	Redhat	7.9	I N I N I N I N										29/06/24	
Système d'exploitation	RedHat Enterprise Linux	Redhat	8.X	A S						R S				30/05/29	Version courante 8.6 La dernière de la branche 8 (8.10) est prévue pour mi 2029.
Système d'exploitation	Ubuntu	Communauté Ubuntu	22.04							A S				31/03/27 31/03/32	Uniquement pour les postes surf ASTEL-I Nom alternatif de la version : Jammy Jellyfish
Système d'exploitation	Windows	Microsoft	10	R	R	R									Pour les intranets classifiés, sauf exception dûment justifiée, c'est la branche SAC qui est préconisée
Système d'exploitation	Windows	Microsoft	11	E										13/10/25	Le déploiement débutera en 2024 pour les postes clients compatibles et se poursuivra en 2025 pour les postes renouvelés au PRB. Cible de fin de déploiement octobre 2025.
Système d'exploitation	Windows	Microsoft	7	I A A I										12/01/15 13/01/20	Assujetti à un emploi sur le segment Secret et FrOps. Migration vers

													windows 10 en cours. Windows 7 sera interdit à l'issue
Système d'exploitation	Windows	Microsoft	8	I	I	I	I	I	I	I	I	I	11/01/16
Système d'exploitation	Windows	Microsoft	8.1	I	I	I	I	I	I	I	I	I	08/01/18 09/01/23
Système d'exploitation poste client	Windows	Microsoft	xp	I	I	I	I	I	I	I	I	I	13/04/09 07/04/14
Système d'exploitation serveur	AlmaLinux	Almalinux OS	8.x	R	S	E	E	E	E	R	S	30/05/29	Dernière version mineure : 8.8 Les templates d'OS durci des versions 8.6 puis 8.8 sont disponibles pour PICSEL, Intradef et Internet et seront maintenus à jour au fur et à mesure.
Système d'exploitation serveur	AlmaLinux	Almalinux OS	9	E	E	E	E	E	E	E	E	30/05/32	Dernière version : 9.2
Système d'exploitation serveur	CentOS	Communauté CentOS	7.x	D	O	D	O	D	O	D	O	29/06/24	Cette version sera la dernière version CentOS soutenue. Elle sera remplacée par une version 8 de la distribution Alma Linux. Dernière version : 7.9 (12/11/2020) Sur le SIA et dans l'attente de la validation du kit OS durci CentOS 7.9, la version 7.8 pourra être autorisée sur dérogation mais impliquera des travaux de migration dès disponibilité de ce dernier.
Système d'exploitation serveur	CentOS	Communauté CentOS	8.x	I	N	I	N	I	N	I	N		Le support de CentOS est abandonné par RedHat/IBM à partir de décembre 2021. L'usage de

Système d'exploitation serveur	Windows Server	Microsoft	2016	A S	A S	A S	A S	A S	10/01/22	11/01/27	Assujetti au déploiement de solutions adhérentes à l'écosystème Microsoft
Système d'exploitation serveur	Windows Server	Microsoft	2019	A S	A S	A S	A S	A S	08/01/24	08/01/29	Assujetti au déploiement de solutions adhérentes à l'écosystème Microsoft
Système d'exploitation serveur	Windows Server	Microsoft	2022	A S					12/10/26	13/10/31	Assujetti aux briques du socle adhérentes à l'écosystème Microsoft.
Tableau Blanc	Lync Live Meeting	Microsoft		I N	D	D	I N				
Traduction	CRISTAL	MinArm			E	E	E				
Traduction	REVERSO	Reverso			D	D					
Transfert de données volumineuses	Defense Drive	OODrive		R S							
Transfert de données volumineuses	France Transfert	DINUM					R S				Sur internet, soutenu par la DINUM
Transfert de données volumineuses	Merlin	Cryptobox		I N							Arrêt du service au 1er mars 2024 (Décision DGNUM)
Transfert de données volumineuses	Pydio Cells	Pydio	4.x				R S				dernier bugfix 4.3.0 du 10/10/23
Wiki	MediaWiki	Wikimedia Foundation	1.39	A N					29/11/25		Assujetti à l'usage de wikidefense ou de TULEAP

8.2.2 Modules pour CMS Drupal, Joomla ! et Wordpress

Les sites d'informations (CMS) peuvent recourir à des modules complémentaires pour étendre les fonctionnalités offertes. Ceci concerne notamment les CMS Drupal, Joomla ! et Wordpress.

La liste retenue au titre du CCT correspond à un ensemble de modules permettant de réaliser la majeure partie des fonctions liées à un CMS. Les modules retenus répondent à une analyse au regard des critères d'éligibilité.

Le besoin de nouveaux modules devra être soumis à la gouvernance technique, après pré-instruction par la direction d'application de la recevabilité des modules au regard des critères d'éligibilité et du non – recouvrement fonctionnel avec les modules déjà acceptés.

Voir l'annexe 8.6.3 *Critères d'éligibilité pour des modules de CMS* pour les critères d'éligibilité des modules.

8.3 Piles logicielles du développement

8.3.1 Pile PICSEL

À date, les principaux composants sont les suivants :

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Gestionnaire de version	Gitlab	Gitlab	Version entreprise	S	PICSEL
Intégration Continue	Gitlab	Gitlab	Gitlab-CI utilisé par des runners en zone projet PICSEL Version entreprise	S	PICSEL
Qualimétrie	SonarQube	SonarSource	Sonar dédié en zone projet PICSEL, intégré au Jenkins	S	PICSEL
Messagerie instantanée	Mattermost	Mattermost	Messagerie instantanée en usage interne au profit des utilisateurs de PICSEL	S	PICSEL
Orchestration	Ansible Automation Platform	Red Hat		S	PICSEL
	Vault Enterprise 1.12.6	Hashicorp	Version entreprise	S	PICSEL
	SI Conformité	Tanium		S	PICSEL
	Elastic	AWS, Elastic		S	PICSEL
	MEDUSA	MinArm	Dépôts de binaires contrôlés (Artifactory 7.55.10 et XRay 7.55.10)	S	PICSEL

8.4 Règles de nommage

8.4.1 Nommage des fichiers

Document	Date	Origine	Type doc	Portée
Directive DGNUM N°31, édition n°2 portant sur le nommage des fichiers numériques au MINARM <i>Commentaire : règles relatives au nommage des fichiers émis en interne ou externe au ministère, archivés ou publiés. Exception : règles de nommage des fichiers relatifs à la procédure des marchés publics destinés à transiter par la place Chorus et qui sont régis par les règles du service des achats de l'État (SAE).</i>	30 octobre 2023	DGNUM	Directive	MinArm

8.4.2 Annuaire - Identifiant unique - Adresse messagerie

Document	Date	Origine	Type doc	Portée
Directive de nommage des annuaires cf. 3.3.4.1 Annuaires / référentiels	12 juin 2012	EMA	Note	MinArm
<i>Commentaire : mise en forme des informations d'annuaire et des adresses de messagerie électronique.</i>				
Schéma d'annuaire des Intranets de la Défense cf. 3.3.4.1 Annuaires / référentiels	26 nov. 2012	SC ² A	Référentiel	MinArm

8.4.3 Nommage DNS

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.016 « nommage DNS » Version 1.0	01/09/2022	DIRISI	Guide	MinArm

8.4.4 Nommage des serveurs

Document	Date	Origine	Type doc	Portée
EMO.GUI.R4.019 « nommage des serveurs » Version 2.0	01/10/2022	DIRISI	Guide	MinArm
<i>Commentaire : Cette directive donne des règles homogènes de nommage des serveurs, physiques et virtuels, du ministère des armées, de façon à en garantir l'unicité du nom. Elle concerne tous les nouveaux serveurs sur tous les intranets, ceux déjà en production ne sont pas concernés sauf dans un cadre d'uniformisation ou d'amélioration de l'exploitation. Dans le cadre du STC-IA, le nommage physique est reproduit comme nom de la ressource dans Active Directory. Trigrammes de SI : le nommage recourt à un trigramme définissant le système d'information concerné, la gestion des trigrammes de SI relève de cette directive (la gestion des trigrammes de sites relève de la directive DIRISI n°67).</i>				
Directive n°149 « nommage des configurations STC-IA v0.5 » Version 0.8	01/03/2015	DIRISI	Directive	SIA
<i>Commentaire : Afin d'identifier tous les sites logiques métropoles SIA du Ministère qui accueillent le socle technique commun SIA S-SF, ce document définit une procédure d'identification basée sur une clé primaire codée sur trois caractères, nommée trigramme de configuration SIA, en complément du trigramme de site physique d'hébergement. Ce trigramme de configuration SIA répond à un besoin de mise en place de règles particulières de nommage complémentaire au profit du Socle Technique Technique Commun InterArmée v0.5 (STC-IA v0.5), devenu depuis SIA S-SF dans une stratégie de déploiement de plusieurs configurations SIA sur un même site géographique d'hébergement.</i>				
EMO.GUI.R4.024 « nommage des serveurs projetables du SIA » Version 1.0	01/07/2023	DIRISI	Guide	SIA

Document	Date	Origine	Type doc	Portée
<i>Commentaire : Le nommage de serveurs des configurations projetables du SIA est réalisé sur la base d'un trigramme de site établi conformément au guide EMO.GUI.R4.019. Ce guide a pour objectif de définir le nommage des serveurs des configurations projetables du SIA et fixe l'emploi unique du trigramme [SCZ] comme identifiant des serveurs du socle (hors serveurs SI métiers).</i>				

8.4.5 Nommage composants d'infrastructure de télécommunication

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°73 d'installation et de nommage des composants d'infrastructure de télécommunication version 4.1	01/09/2018	DIRISI	Directive	Intradef Intraced
<i>Commentaire : Cette directive bien qu'établie pour la durée de vie d'OGIT reste la référence pour le Ministère. Elle donne des règles homogènes de nommage de tous les équipements sous la responsabilité de la DIRISI (métropole, outremer et étranger) : zone technique, répartiteurs, baies, câblage, équipements actifs, terminaux, ... Cette directive précise aussi des règles de câblage des installations.</i>				

CARLA : La description des réseaux physiques locaux de niveau NP et DR (éléments de réseau, éléments de distribution, infrastructure bâtie...) est réalisée au travers de CARLA (CArtographie des Réseaux LocAux). Le système d'information CARLA permet d'avoir une gestion précise et rigoureuse de l'architecture filaire et optique d'un site (infrastructure de câblage courant faible, desserte des locaux) et de donner aux techniciens réseaux les moyens de répondre aux sollicitations multiples des utilisateurs dans des délais très courts, surtout en cas de panne d'une liaison.

Solution	Produit	Fournisseur	Utilisation/Restriction	Statut	Portée
Référentiel	CARLA	DIRISI R3WEB	Gestion des données relatives aux infrastructures de télécommunication, réseaux locaux NP et DR.	R	Intradef

8.4.6 Nommage VLAN

Document	Date	Origine	Type doc	Portée
Guide EMO.GUI.R4.005 « Format des VLAN » Version 1.0	01/03/2022	DIRISI	Guide	MinArm
<i>Commentaire : à pour objet de définir et de permettre de contrôler l'utilisation des VLAN opérés par la DIRISI et mis en oeuvre pour les réseaux de desserte des sites du ministère des Armées (tous niveaux de classification en métropole, outremer, à l'étranger, en OPEX et sur les bâtiments de la Marine nationale) et de définir de manière normée la définition :</i>				
<ul style="list-style-type: none"> - du périmètre d'utilisation des VLAN ; - du standard de nommage des VLAN ; - des principes d'attribution des ID VLAN ; - des principes de mise en relation de l'adressage réseau entre le 3ème octet d'adressage avec l'utilisation des VLAN ; - du processus des demandes de création de VLAN. <i>Le nouveau système GARD (Gestion Automatisée des Réseaux des Datacenter) gère de façon automatisée les VLAN des Datacenters. Ce document ne s'applique donc pas aux Datacenters où GARD est mis en oeuvre.</i>				

8.4.7 Adressage IP

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°129 portant sur l'adressage IPV4 du ministère de la défense : version 2.1 diffusée par note n°922077/DEF/DIRISI/SCOE/EXP/NP du 7 mai 2014	7 mai 2014	DIRISI	Directive	MinArm
Directive DIRISI n°109 portant la politique de routage des flux IP sur l'IP DEFENSE : version 3.0	26 mai 2018	DIRISI	Directive	MinArm
<i>Commentaire sur ces directives : Ces directives présentent le plan d'adressage IPV4 global du ministère des armées ainsi que l'adressage et le routage VPN 2010. Elles s'appliquent à l'ensemble des organismes du ministère des armées.</i>				
<i>Ces directives réfèrent par ailleurs les principales références concernant les plans d'adressage IP relative aux divers réseaux et sous-réseaux du ministère des armées.</i>				
Directive DIRISI n°134 relative à l'adressage IPV4 des réseaux protégés : version 2.1 du 25 juin 2014	25 juin 2014	DIRISI	Directive	MinArm Réseaux Classifiés de défense
<i>Commentaire : Cette directive précise les éléments relatifs à l'adressage des équipements cautionnés (Chip, Netasq, Arkoon ...) et des équipements relevant du classifié de défense (Echinops, TCE621, ...) en métropole, OME, etc. Mais elle ne traite pas des topologies (contextes et associations), et ne concerne ni les CHIP du RCDG (SOCRATE, RTRAN) ni RIFAN 2.</i>				

8.4.8 Marquage de la sensibilité des informations numériques

Document	Date	Origine	Type doc	Portée
Guide Marquage de la sensibilité des informations numériques diffusée par la note N°365ARM/DGNUM/DG du 3/10/2022	3/10/2022	DGNUM	guide	MinArm
<i>Commentaire : Le guide a pour objet de fournir à l'ensemble des utilisateurs et les directions applications du Ministère une sensibilisation avancée sur le marquage de la sensibilité des informations numériques des données. Le marquage de la sensibilité consiste en l'apposition d'un marqueur visuel compréhensible par une personne, sur une information ou un ensemble de données, structurées (notamment dans les bases de données) ou non (fichiers, le guide présente les différents niveaux de protection, et expose les principes à mettre en œuvre pour le marquage numérique de la sensibilité des données informations numériques au ministère des Armées, courriels, etc.)</i>				

8.5 Référentiels / Nomenclatures

8.5.1 Cartographie des services

Le Cadre Commun d'Urbanisation de l'État (CCU) élaboré par la DINUM propose une structuration de la couche infrastructure applicative (NRA : Nomenclature de Référence Applicative) et matérielle (NRI : Nomenclature de Référence Infrastructure).

Document	Date	Origine	Type doc	Portée
Cadre Commun d'Urbanisation de l'État V1.0 diffusé par lettre n°2012-SU-132 du 16 novembre 2012 Nomenclature de Référence Applicative [NRA] Nomenclature de Référence Infrastructure [NRI]	26 octobre 2012	SGMAP DINSIC	Référentiel	MinArm
<i>Commentaire :</i>				

Le ministère des armées s'est doté d'une cartographie des services communs des intranets plus détaillée.

Document	Date	Origine	Type doc	Portée
Cartographie des services communs des intranets de la défense diffusée par note n°489/DEF/DGSIC/SDAU/NPO du 22 septembre 2015 et D-15-005981/DEF/EMA/CPI/NP du 22 septembre 2015	22 sept. 2015	DGSIC - EMA/CPI	Référentiel	MinArm
<i>Commentaire : cette cartographie permet de classer et détailler les services des intranets.</i>				

8.5.2 Catalogue des OID

Information non fournie.

8.5.3 Trigrammes de sites géographiques

Document	Date	Origine	Type doc	Portée
Directive DIRISI n° 67 « gestion des trigrammes » version 1.3 diffusée par note n°406097/DEF/DIRISI/SCOE/EXP du 3 juillet 2015	16 juin 2015	DIRISI	Directive	MinArm
<i>Commentaire : La directive décrit les modalités de gestion des trigrammes de sites géographiques utilisés accueillant des sites d'information et de communication (routeur, data center, équipements de commutation, système d'information...) voir les sites interconnectés avec ceux du ministère des armées. Cette version introduit les trigrammes pour les unités mobiles pour mieux les intégrer dans les projets SIC des armées. Point de contact : le POLE OPS RTD gère la liste et les demandes de nouveaux trigrammes.</i>				
Référentiel des trigrammes de sites	-	DIRISI	Référentiel	MinArm

8.5.4 Mots clés d'attribution (MCA)

Document	Date	Origine	Type doc	Portée
Directive DIRISI n°121 relative à la gestion de la liste unique des mots clés d'attribution (MCA) version 3.0 du 21 mars 2014	21 mars 2014	DIRISI	Directive	MinArm

8.6 Critères d'éligibilité des produits et solutions

8.6.1 Objectifs et contraintes

Le cadre de cohérence technique du ministère a pour objet d'établir et de maintenir dans la durée l'équilibre entre plusieurs besoins et contraintes qui s'opposent par nature. Citons par exemple :

- évolutions et innovations technologiques pouvant offrir un avantage opérationnel ou un gain de ressources ;
- souveraineté en matière de système d'information ;
- interopérabilité ;
- sécurité des systèmes d'information ;
- maîtrise du système d'information ;
- exploitabilité, passage à l'échelle ;
- rationalisation des choix technologiques du ministère.

Si une nouvelle technologie semble présenter des opportunités susceptibles d'apporter un avantage opérationnel ou un gain en ressources pour le Ministère, il est indispensable de s'assurer qu'elle offre un certain nombre de garanties avant de pouvoir l'adopter.

Le domaine de l'informatique évolue à un rythme extrêmement rapide qu'un organisme tel que le Ministère des armées, du fait de la taille de son système d'information et de ses ressources humaines ne peut suivre aveuglément.

Par exemple :

- est-elle pérenne ? L'histoire de l'informatique regorge d'exemples de technologies qui se sont avérées de fausses bonnes idées ou ont été rapidement supplantées par d'autres technologies répondant plus efficacement au besoin (applets Java, technologie Flash, WAP ...) ;
- garantit-elle la maîtrise du système d'information ? une technologie propriétaire ou exclusivement maintenue par un seul acteur est susceptible de mettre le ministère dans une situation de dépendance inacceptable (en terme de souveraineté, de sécurité ou de coût financier à assumer par la suite) ;
- est-elle mature ? Le monde de l'informatique évolue extrêmement rapidement et même si une innovation semble devoir s'imposer durablement, elle peut mettre un peu de temps avant de se stabiliser et de trouver une implémentation durable. Adopter trop vite une technologie peut donc présenter le risque de retenir une implémentation mort-née ;
- est-elle structurellement solide ? des solutions fonctionnellement intéressantes peuvent s'avérer fragiles: défaut de conception, code de mauvaise qualité provoquant des dysfonctionnements, des problèmes de performance, des failles de sécurité ou rendant très difficile ou coûteuse la montée de version ;
- est-elle maîtrisable par le ministère ? Le ministère doit mettre en œuvre et exploiter les technologies à l'aide des ressources, notamment humaines, dont il dispose. Son personnel doit pouvoir les maîtriser, ce qui implique des formations à programmer et un niveau de complexité adapté. En conséquence, il n'est pas envisageable de multiplier les technologies pour répondre à un même besoin. Ceci peut aussi conduire à estimer la réversibilité des solutions retenues et la capacité du Ministère à les reprendre à son compte.

8.6.2 Critères généraux d'appréciation

En déclinaison des orientations précitées, les demandes d'intégration de nouveaux produits ou solutions dans le CCT ou de dérogation sont appréciées au travers de critères dont les principaux sont donnés ci-après :

- **privilégier à iso-fonctionnalités** les produits et solutions sous licence libre, possiblement sans coût de licence associé ; dans tous les cas, il conviendra que le code source puisse être accessible à des fins d'audit ou faire l'objet d'une analyse de sécurité ;
- **fonctionnalités :**
 - pas de doublon fonctionnel avec un autre logiciel ou solution déjà présente au CCT (au-delà du besoin de maintenir des options alternatives quand cela est jugé nécessaire) ;
 - pas de doublon avec des services du réseau support (authentification, supervision applicative, statistiques de fréquentation, etc.) ;
 - pas de produit ou de solution offrant des fonctions de développement, d'exploitation ou d'exécution de code arbitraire à un utilisateur standard ;
- **support :**
 - gestion par une organisation ou un groupe de contributeurs actifs dont l'appartenance à une organisation ou l'éventail de profils offre des garanties suffisantes (sécurité, absence de monopole, politique suggérant la possibilité d'une mise en dépendance technologique et/ou financière voire un abandon, ...) ;
 - vitalité suffisante : l'activité est évaluée par exemple au nombre de livraisons de corrections et évolutions, à la date des dernières livraisons de code ou de sortie des dernières versions, à la rapidité de traitement des bugs et problèmes ;
 - adoption par un nombre suffisant d'acteurs permettant d'assurer une pérennité acceptable de l'écosystème ;
 - versions à durée de vie longue (par exemple versions dites LTS ou long term support) ;
ou, à défaut, disposant d'une durée de support annoncée compatible avec les contraintes du ministère et les durées des projets de systèmes d'information ;
 - version stable : les versions Release Candidate (RC), beta ou alpha ne sont pas autorisées (ainsi que celle ayant recours à un composant en dépendance lui-même en version RC, beta ou alpha) ;
- **sécurité :**
 - nombre de vulnérabilités signalées, vitesse de traitement ;
 - fréquence des signalements ;
 - pas d'échange de données avec l'extérieur (vers des serveurs externes au Ministère, à des fins de statistiques ou de gestion des licences ou pour récupérer des ressources de type scripts javascript, polices de caractères, feuilles de style, images par exemple) ;
 - pas d'exécution de code à la volée ;
 - pas de fonctionnement en mode "boîte noire" (installation en image de VM, en conteneur ou en « fat jar » par exemple) ;
 - existence d'audits ou de certification ;
- **qualité :**
 - présence d'une documentation, si possible en français ;
 - qualité du code (évaluée via SonarQube ou CAST par le CASID par exemple) ;
- **capacité d'intégration** dans le système d'information du Ministère :
 - adéquation avec les orientations du Ministère (technologie web en client léger, présence d'API RESTful, authentification OpenID Connect voire Kerberos pour les réseaux autres

- que NP et DR, « API first », « secure by design » ...);
- o compétences internes disponibles ou pouvant être acquises par le personnel concerné dans des délais adaptés ;
- o compatibilité avec les infrastructures du Ministère (capacités d'hébergement, des infrastructures réseaux, des équipements de sécurité, des services du socle ...);
- o interopérabilité et réversibilité ;
- o capacité à communiquer avec les autres briques du système d'information ;
- o possibilité pour le ministère de reprendre ou de faire reprendre le MCO et le MCS (mise à disponibilité du code source immédiate ou possible, notamment) ;
- o nombre de dépendances : les dépendances doivent également être inscrites au CCT et en nombre raisonnable (ce critère adresse également des préoccupations de support et de sécurité, voire de qualité).

8.6.3 Critères d'éligibilité pour des modules de CMS

Concernant les solutions de CMS (Content Management System), pour être éligible, un module doit vérifier, outre les exigences communes à tous les produits ou solutions (cf. ci-dessus § 8.6.2), les exigences spécifiques suivantes :

- Pas de module dont l'apport fonctionnel est suffisamment minime pour ne pas justifier le recours à un module (si le module fait 3 lignes de code, la fonctionnalité peut être directement implémentée dans le site sans qu'il soit besoin d'un module) ;
- **Support :**
 - o gestion par une organisation (pour DRUPAL, elles sont désignées comme Drupal services provider) ou un groupe de contributeurs actifs dont l'appartenance à une organisation ou l'éventail de profils offre des garanties suffisantes ;
 - o non référencé en tant qu'[Abandonware](#) pour Joomla ;
- **Sécurité :**
 - o Nombre de vulnérabilités signalées, vitesse de traitement, fréquence des signalements
 - <https://www.drupal.org/security>
 - <https://extensions.joomla.org/vulnerable-extensions/about/>
 - o pour DRUPAL, couverture par la [security advisory policy](#).
 - o Pour wordpress :
 - <https://www.easyhoster.com/aide/choisir-plugin-wordpress>
 - <https://make.wordpress.org/plugins/>
 - <https://wpmarmite.com/installer-plugin-wordpress/>
- **Qualité :**
 - o Pas d'adhérence au noyau du CMS (i.e. pas de modification du noyau mais utilisation des API proposées par le framework du CMS)

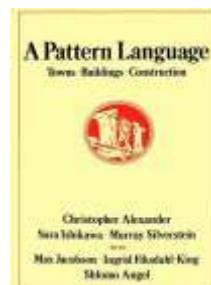
8.7 Modèles d'architecture

8.7.1 Introduction aux modèles d'architecture

8.7.1.1 Qu'est-ce qu'un modèle d'architecture ?

Un modèle ou « pattern » est un modèle dont le but est de décrire une « bonne pratique » afin d'assurer la capitalisation et la diffusion des connaissances dans un domaine métier donné.

La description de « patterns » permettant de réutiliser des « bonnes pratiques » de conception pour réaliser un nouveau projet (dans le domaine du BTP) a été popularisé avec le livre « *A Pattern Language* » paru en 1977⁶⁴.



C'est le livre « Design Patterns » en 1994 qui a généralisé son usage en informatique avec des centaines de livres qui en proposent depuis cette date⁶⁵.



Un modèle d'architecture (terme utilisé dans cette annexe pour traduire « design pattern ») peut être décrit :

⁶⁴ A pattern language: towns, buildings, construction de Christopher Alexander, Sara Ishikawa, Murray Silverstein, 1977 (0-19-501919-9)

⁶⁵ Design Patterns, Elements of Reusable Object-Oriented Software, Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides

- **sous diverses formes** (par exemple sous forme de schéma, de texte descriptif, de spécification, de code spécifique, ...) ;
- **à différents niveaux de granularité** (par exemple le schéma général d'un système complexe, un couplage faible entre 2 SI, l'implémentation d'un proxy en Java, ...) ;
- **mais le but d'un modèle d'architecture, c'est d'avoir un modèle qui décrit la résolution d'un problème récurrent par une communauté d'experts, mis à disposition des non experts.**

Un modèle d'architecture pour le CCT ne décrit pas tous les détails des technologies du MinArm, mais des éléments clefs de conception qu'il faut connaître pour faire un bon usage du CCT.

Cette annexe traite des modèles d'Architecture Applicative et introduit les technologies ayant un statut « Recommandé » au CCT. Les nombreuses technologies ayant un statut « assujetti », « déconseillé », « interdit » ou « émergent » signalées dans le présent CCT ne figurent donc pas dans ces modèles d'architecture.

Le public visé : les RCP et architectes projets (juniors, nouveaux arrivants ou externes).

Pour approfondir le sujet des modèles d'architecture applicative et logicielle, parmi les nombreux livres qui traitent de cette question, la lecture des 5 tomes de « Pattern-oriented software architecture » aux éditions Wiley peut être recommandée :



8.7.2 Modélisation des SI avec Archimate

8.7.2.1 Qu'est-ce que archimate ?

Archimate est un standard de l'Open Group qui est défini par une spécification (actuellement en version 3.2). Cette spécification décrit un langage et une notation graphique permettant de modéliser des systèmes d'information.

Ce langage introduit des concepts et des relations entre ces concepts dont la sémantique est précisée par un meta-modèle. Son utilisation pour modéliser un système donné utilise une notation graphique propre à Archimate.

Archimate permet de décrire un SI selon divers points de vue, de sa finalité stratégique à son implémentation. Dans les modèles d'architecture applicative, le focus est fait sur la couche « Application » et les technologies « recommandées » dans le CCT.

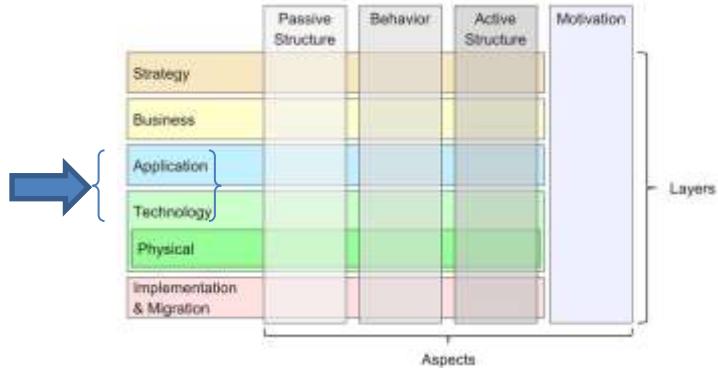


Figure 4 : Description d'un SI dans ARCHIMATE

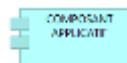
8.7.2.2 Les concepts Archimate utilisés pour les modèles d'architecture CCT

Archimate est un standard de description d'architecture essentiellement à destination des architectes. Or, le meta-modèle décrivant le point de vue applicatif dans Archimate introduit divers concepts qui ne sont pas tous indispensables pour décrire les modèles d'architecture d'intérêt pour le Ministère.

Ainsi, le choix a été fait de réduire le nombre de notations Archimate, dans le but d'en faciliter la compréhension par un responsable de conduite de projet (RCP).

Par simplification, ne seront utilisés que les 4 concepts et notations suivants dans les modèles d'architecture.

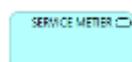
Le composant applicatif :



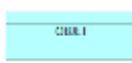
L'interface de composant applicatif pour illustrer le principe de « boîte noire » (nommée en architecture *principe de « couplage faible »* ; ou en programmation *principe « d'encapsulation »*) qui indique que si un composant A appelle un composant B, il le fera via une interface du composant B. La réalisation (que l'on nomme « implémentation ») du composant B restant non visible du composant A (d'où l'appellation de « boîte noire ») :



Le service qui est une interface « publique » (c'est-à-dire visible de l'extérieur du SI) et qui permet à un composant B d'être appelé depuis un composant A qui est dans un autre SI :



Les objets qui vont permettre la persistance des données du SI :



Pour introduire dans les modèles d'architecture les technologies ayant le statut de « recommandé » dans le CCT, également des concepts Archimate du point de vue technologique sont également utilisés.

A nouveau par souci de simplification, cette couche n'est pas reprise dans les modèles d'architecture applicatifs mais les services technologiques apparaissent en vert dans les schémas avec les notations du modèle applicatif (utilisation d'un composant pour un Framework plutôt que d'introduire une notation supplémentaire spécifique aux services technologiques). A titre d'illustration, le framework Vue.js qui est une technologie facilitant le développement d'application en Javascript sera représenté comme suit :

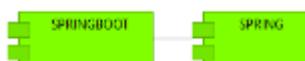
8.7.2.3 Les relations Archimate utilisées pour les modèles d'architecture CCT

Archimate définit 11 types de relation ; toujours par souci de simplification, seules 4 d'entre elles seront utilisées dans les modèles d'architecture.

La **réalisation** qui fait le lien entre un concept du modèle logique et sa réalisation par des technologies recommandées au CCT. Par exemple, est figuré ici que les composants qui s'exécutent sur un poste de travail sont *réalisés* avec les technologies HTML5, CSS3 et Javascript. Cet ensemble constitue ce qui est nommé une « interface client » :



L'**association** est un lien structurel. Par exemple, est signifié ci-après que le framework Spring Boot s'utilise en association avec le framework Spring :



Le **lien de service** montre les dépendances entre le code applicatif et les frameworks dont il dépend. Par exemple, pour réaliser le code d'une interface client, il est représenté ici qu'il est possible d'utiliser les frameworks javascript Vue.js ou React :



Le **lien dynamique** permet de montrer des flux de données lors de l'exécution de l'application et donc la logique de fonctionnement de l'architecture. Par exemple, à l'exécution, un composant applicatif B appelle une fonction d'un composant A via l'interface applicative associée :



8.7.3 Modèles d'architectures logiques de référence

8.7.3.1 Définition et intérêt d'une architecture logique

Une architecture logique décrit une architecture applicative dont les éléments correspondent à une logique d'usage sans qu'il soit fait mention des technologies qui seront utilisées pour les implémenter, ce qui permet de décrire une logique commune pour toute architecture SI quelles que soient les technologies mises en œuvre pour un SI particulier. Ainsi, un SI réalisé en Java, PHP ou Javascript peut s'inscrire dans un modèle standard ayant une logique commune.

8.7.3.2 Modèle de référence

Ce modèle décrit un SI et son interopérabilité au travers de services de médiation conformément au principe de couplage faible dans une architecture orientée services (SOA). Au ministère des Armées, ce service de médiation est apporté par un composant « socle », la PEM (Plateforme d'Exposition et de Médiation). Le couplage faible induit permet de faire évoluer les composants associés à un service, indépendamment des clients de ce service, tant que l'interface de service reste inchangée, facilitant la maintenance et favorisant l'évolutivité globale.

Une architecture applicative se décrit précisément à l'aide de 5 couches. A des fins de simplification, seules les 3 suivantes seront utilisées pour les modèles d'architecture du CCT :

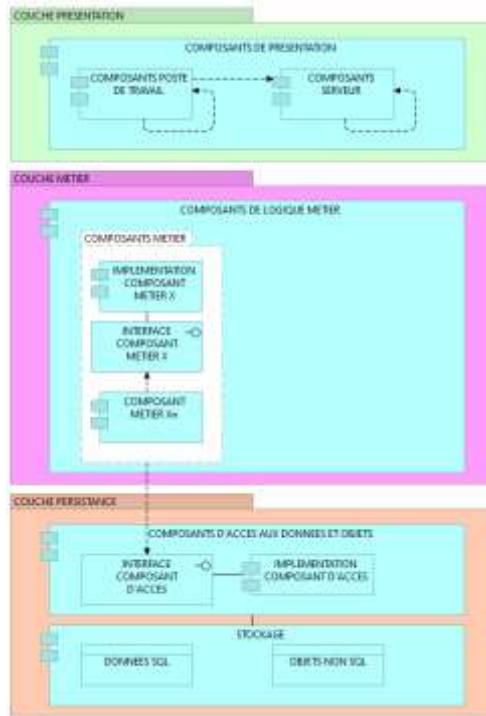


Figure 5 : Architecture applicative

La « **couche de présentation** » représente la partie du SI qui gère les interfaces (généralement des écrans) avec lesquelles interagissent directement les utilisateurs (le terme « IHM » qui signifie « interfaces homme-machine » est également utilisé) ainsi que le contrôle de la cinématique d'enchaînement de ces écrans. Ce schéma logique permet à la fois une approche « client lourd » ou « client léger » ou les 2 à la fois dans le cas d'un « client léger » permettant un mode déconnecté. Dans une architecture « client lourd » (non recommandée), tous les composants nécessaires s'exécutent sur le poste de travail (« Composants poste de travail »). Dans une architecture « client léger », il s'établit un dialogue entre les composants qui s'exécutent sur le poste de travail (dans un navigateur) et des composants hébergés sur serveur (« Composants serveur »). Les composants serveur contrôlent la bonne logique d'enchaînement des pages, leur constitution et leur diffusion à destination du poste de travail pour affichage. Les flèches en pointillés sur le schéma représentent, de façon simplifiée, ces flux d'information entre composants. La flèche entre composant client et composant serveur illustre ce dialogue client-serveur. Une fois celui-ci instauré, le serveur transmet à son tour des flux à destination du poste de travail (qui ne figurent pas ici pour simplifier et souligner qui a l'initiative de ce dialogue).

La « **couche métier** » contient la logique métier du SI, traite les flux provenant de la « couche de présentation » et assure l'accès à la « couche de persistance » qui gère les données du SI. La couche métier

illustre des aspects fondamentaux de l'architecture applicative : une architecture est un assemblage de composants, tout composant applicatif (« Implémentation composant métier X » sur le schéma) dispose d'une interface d'accès (interne au SI, donc privée et donc ni exposable, ni utilisable par un SI tiers) qui permet à un autre composant de ce même SI de l'invoquer (il est possible de gérer des niveaux plus fins à l'intérieur du SI pour préciser quels composants peuvent utiliser cet accès, mais ce niveau de précision n'est pas nécessaire pour les patterns présentés dans le CCT). Les technologies pour implémenter l'interface et le protocole d'appel à utiliser pour l'invoquer seront généralement spécifiques au langage choisi, mais la logique reste la même. Une application métier qui veut exposer des services (« Public API Service ») doit le faire avec un standard indépendant des langages de programmation. Le MinArm a choisi le standard « OpenAPI » qui requiert l'usage d'API selon le pattern REST. Chaque API doit être décrite dans un fichier « OpenAPI » que l'on nomme aussi fichier « swagger » (en respectant les règles de conception du MinArm et soumis à validation préalable du SAND), puis est publiée sur le service de médiation (PEM) pour pouvoir être invoquée par un autre SI. Ce service sert d'interface publique pour masquer l'appel du ou des composants métiers qui réalisent le service. C'est ce que montre le modèle complété ci-dessous.

Ce schéma montre également qu'un composant de la couche de présentation peut appeler un composant de la couche métier via son interface et que le bon usage d'un service de médiation ne concerne que le dialogue entre couches métiers de SI différents. Il est courant que les composants des couches de présentation et métier utilisent le même langage et dans ce cas le protocole d'appel est généralement lié au langage employé. Ceci implique que ces composants sont tous des composants « serveur ». Lorsque ce n'est pas le cas (par exemple dans le cas où la couche « présentation » est développée avec le framework Vue.js en javascript et s'exécute donc côté « client » dans un navigateur web et où la couche « métier » a été développée avec le framework Spring Boot en langage Java et s'exécute côté « serveur »), on utilise alors en général un protocole agnostique au langage tel que « https ». C'est aussi bien sur le cas entre composants exécutés sur le poste de travail et composants hébergés sur serveur de présentation. Le schéma montre également qu'un composant sur le poste de travail ne doit pas échanger directement avec un composant métier côté « serveur » afin que le dialogue reste toujours sous la supervision du contrôleur de l'application qui fait partie de la couche de présentation.

La « **couche de persistance** » contient les composants qui gèrent l'accès aux données (SQL et NO-SQL) avec les solutions qui en assurent le stockage telles que des systèmes de gestion des bases de données (ou **d'objets**). Un composant d'accès aux données est dit « de base » s'il ne contient que des fonctions d'accès de base aux données (fonctions appelées également « CRUD » pour « create », « read », « update » et « delete », termes qui se traduisent respectivement par « création », « lecture », « mise à jour » et « suppression ») sans l'ajout de contrôles ou règles métier. À des fins de découplage, un composant d'accès va recourir à un intermédiaire (ou « proxy ») pour interagir avec la solution de stockage. Par exemple, un pilote de bases de données ou un framework assurant la correspondance (nommé « mapping ») entre les données stockées au format relationnel dans la « base de données » et les objets manipulés par l'application (ces frameworks s'appellent des ORM).

Les interfaces des composants d'accès dans la couche de persistance peuvent également être implémentées par des API REST. C'est notamment le cas le plus usuel dans une architecture Javascript. Pour autant ces API REST, comme indiqué dans le schéma, ne doivent pas être exposées dans la PEM. Ce sont des API privées d'une application. La raison à cela étant que l'intégrité des données et des objets stockés en base de données requiert l'application de règles métier qui ne sont pas dans des composants « de base » mais dans des composants métier (qui eux, comme vu précédemment, sont potentiellement exposables dans la PEM en tant que services via des API REST).

Par conséquent, la création, la consultation, la mise-à-jour et la suppression de données ne peuvent être réalisées que par une seule application (plus précisément, par un composant métier unique appelé « service

métier » dès lors qu'il est exposé via une interface publique), composant métier qui est généralement composé de plusieurs autres composants métiers de l'application et qui communiquent avec un ou plusieurs composants d'accès aux données.

La cohérence métier des données (appelée également « intégrité des données ») étant sous la responsabilité d'un service applicatif dédié, il est dès lors aisé de passer à un déploiement en mini ou micro-services (uniquement lorsque c'est pertinent de le faire, raison pour laquelle ces architectures restent « assujetties ») : en effet, la couche métier de l'application peut se découper selon ses services métier (chacun contenant ses composants métier et de persistance et étant responsables des données ou objets qu'ils gèrent) et chaque service peut être hébergé sur des serveurs virtuels ou containers différents selon les technologies d'hébergement adoptées.

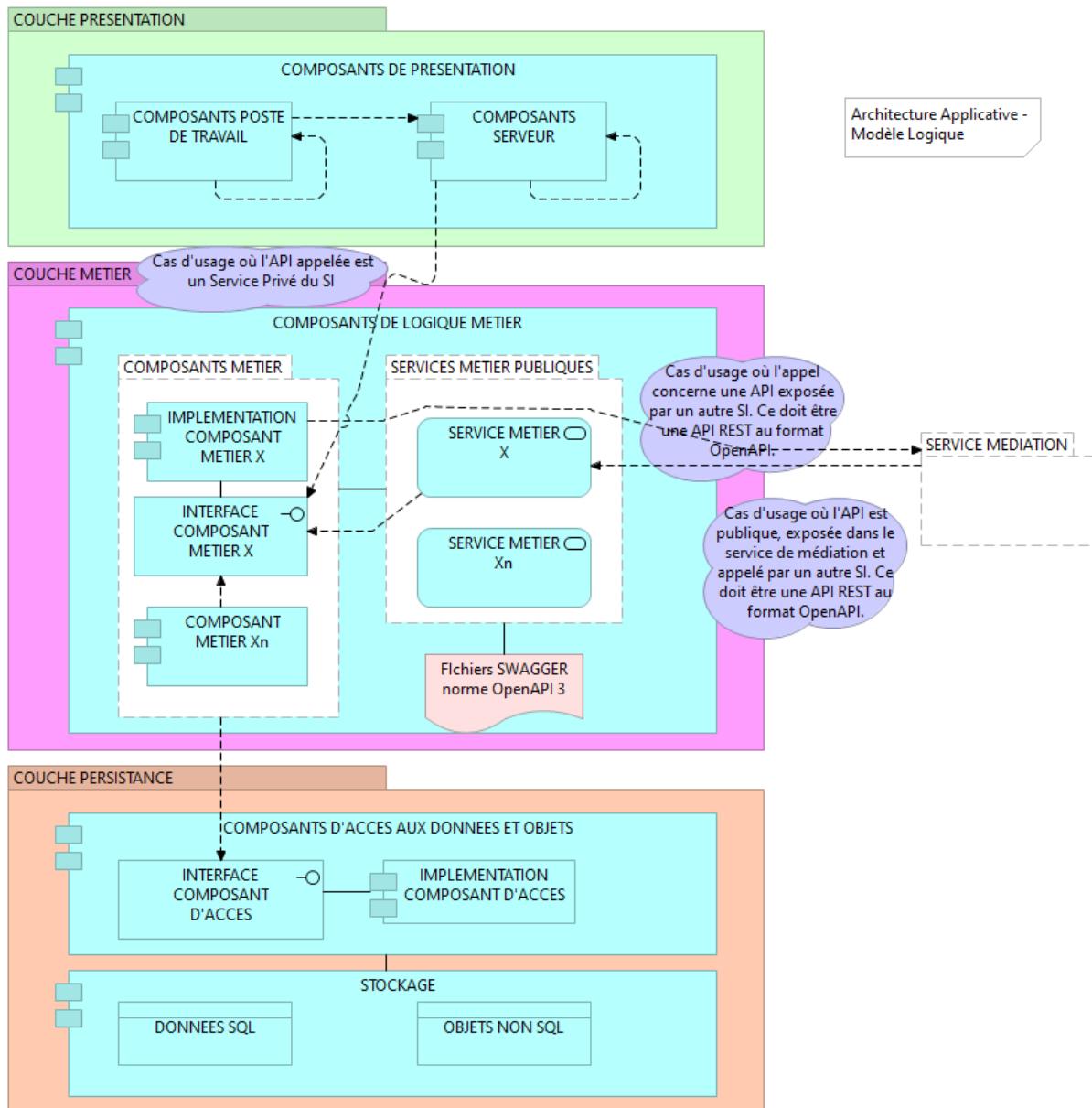


Figure 6 : Architecture applicative (modèle logique)

À noter que sont également utilisés les termes « frontend » pour la partie de l'architecture qui fait référence à la couche de présentation et « backend » pour la partie qui contient la couche métier et la couche de persistance.

8.7.4 Catalogue des modèles d'architecture applicatives

Les schémas suivants ont pour objet de montrer comment l'architecture applicative d'un SI peut être réalisée avec des langages de programmation spécifiques (Javascript ou PHP par exemple) en « client-léger » et comment réaliser un mode déconnecté. Les composants du schéma logique sont implémentés en utilisant des technologies recommandées décrites dans le CCT.

Les architectures présentées mettent en œuvre soit des solutions du marché, soit du code source pouvant provenir pour partie de frameworks logiciels. Le code couleur permet de les différencier :

- en blanc, les composants développés spécifiquement pour l'application ;
- en vert, le code réutilisé provenant d'un framework logiciel ou une solution logicielle ayant le statut « recommandé » au CCT.

Dans le schéma, les composants logiciels qui constituent l'application (codes sources plus les codes issus de frameworks) sont regroupés dans des rectangles blancs afin de les différencier des solutions logicielles qui offrent des « services techniques sur étagère » tels qu'un serveur d'application ou un système de gestion de bases de données.

8.7.4.1 Le modèle d'architecture PHP

Le modèle d'architecture pour des architectures développées en PHP met en évidence pour la couche de présentation que le code réalisé et exécuté sur le poste de travail (dans le navigateur) est développé en Javascript tandis que l'interface de présentation est décrite en HTML5/CSS3.

Côté serveur de présentation, le code est écrit en PHP avec, au choix, le framework Symfony, Laravel ou Drupal (idem pour le code de la couche métier).

L'accès aux données peut s'appuyer sur un ORM pour les framework Laravel et Symfony.

Les solutions de stockage relationnel recommandées et donc représentées ici sont PostgreSQL et MariaDB. Pour cette dernière, un cluster Galera est utilisable si besoin.

Le stockage non relationnel pour une mise en cache en mémoire peut être réalisé avec Memcached (stockage clef/valeur) ; celui recommandé pour stocker, indexer et rechercher de grandes quantités de données de manière rapide est Elasticsearch.

Il n'y a pas d'autres solutions recommandées pour le stockage non relationnel. Le CCT décrit plusieurs solutions utilisables mais qui sont assujetties à certains cas d'usage spécifiques.

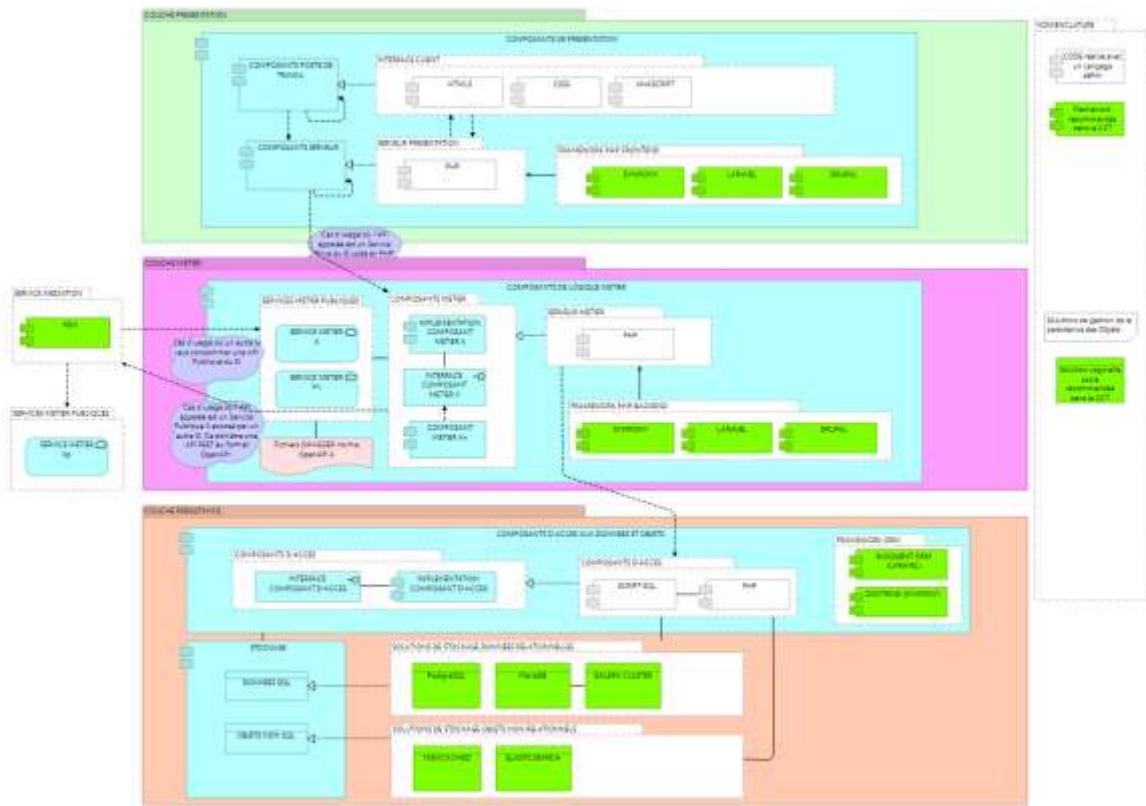


Figure 7 : Modèle d'architecture PHP

8.7.4.2 Le modèle d'architecture Javascript

Le modèle d'architecture pour des architectures développées en Javascript met en évidence pour la couche de présentation, que le code réalisé et exécuté sur le poste de travail (dans le navigateur) est développé en Javascript tandis que l'interface de présentation est décrite en HTML5/CSS3. Le code est réalisé avec le framework Vue.js ou React.

Par défaut, Vue.js comme React sont des framework Javascript qui s'exécutent côté client, c'est-à-dire dans le navigateur web de l'utilisateur. Il n'est donc pas nécessaire d'utiliser Node.js ou Express.js pour les mettre en œuvre côté client, il suffit simplement d'inclure les fichiers Javascript de Vue.js ou de React dans les pages HTML et les exécuter dans le navigateur.

Cependant, du code doit être présent sur le serveur dès lors que qu'il est nécessaire de bénéficier de services qu'il doit exécuter pour effectuer le rendu des pages (SSR), pratique recommandée, ou plus systématiquement pour la gestion de l'authentification et des autorisations. Sur le serveur, le code est écrit en Javascript avec au choix, le framework Vue.js ou React. Le code utilise Node.js comme environnement d'exécution ainsi que le framework Express.

Il n'y a pas d'ORM recommandé pour l'accès aux données.

Les solutions de stockage sont les mêmes que celles utilisées pour PHP (cf. modèle d'architecture PHP ci-dessus).

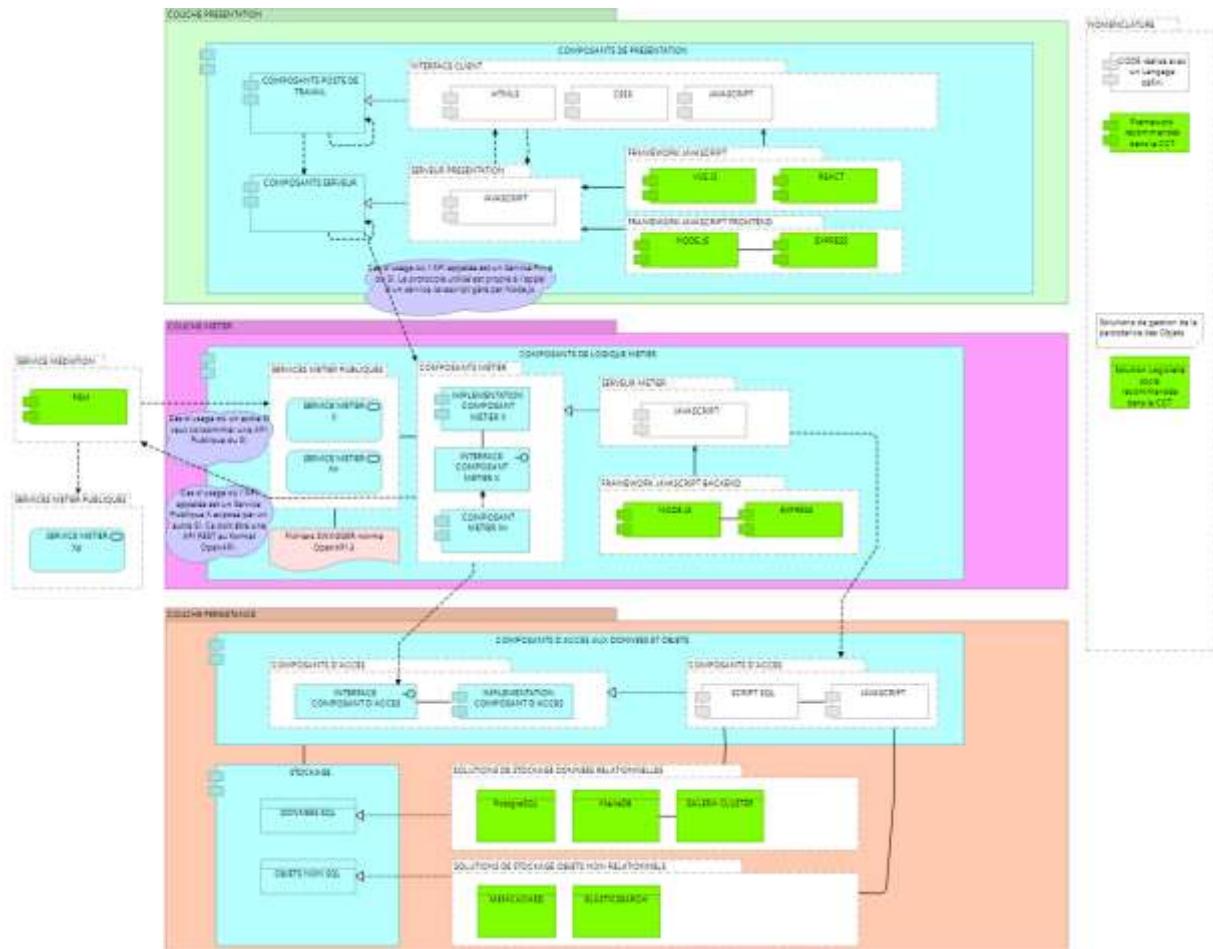


Figure 8 : Modèle d'architecture Javascript

8.7.4.3 Le modèle d'architecture Java

Le modèle d'architecture pour la couche de présentation des architectures développées en Java est similaire à celui du modèle d'architecture Javascript.

Le code de la couche métier utilise Spring Boot et les librairies du Framework Spring. Le principal composant utilisé ici est Spring IoC qui fournit un conteneur responsable de la gestion des objets et de leurs cycles de vie. Il prend en charge l'injection de dépendances, la configuration des beans et la gestion des transactions.

L'accès aux données est également réalisé avec Spring Boot en utilisant le composant Spring Data qui offre un nombre important de possibilités pour des accès SQL et NoSQL. Spring Data offre de surcroît des accès pour Memcached et Elasticsearch. Les accès aux bases de données relationnelles peuvent recourir à Spring Data JDBC ou Spring Data JPA. Les solutions de stockage sont les mêmes que celles présentées pour PHP (cf. modèle d'architecture PHP ci-dessus).

A noter que cette architecture basée principalement sur Spring IoC et Spring Data n'a pas besoin d'un serveur d'application Jakarta EE, un simple Tomcat étant largement suffisant. Ceci a pour avantage de simplifier l'administration, l'exploitation et le MCS du SI en production. Tomcat et la machine virtuelle Java (OpenJRE) sont indiqués dans le schéma en dehors des regroupements « composants de logique métier » et « composants d'accès aux données et objets » car ils ne font pas partie de l'application elle-même.

même. Ce sont des composants externes nécessaires à l'exécution du code Java.

L'architecture résultante est orientée API (la couche métier fournit des services à la couche de présentation en mode API REST) avec un frontend en Javascript et un backend en Java.

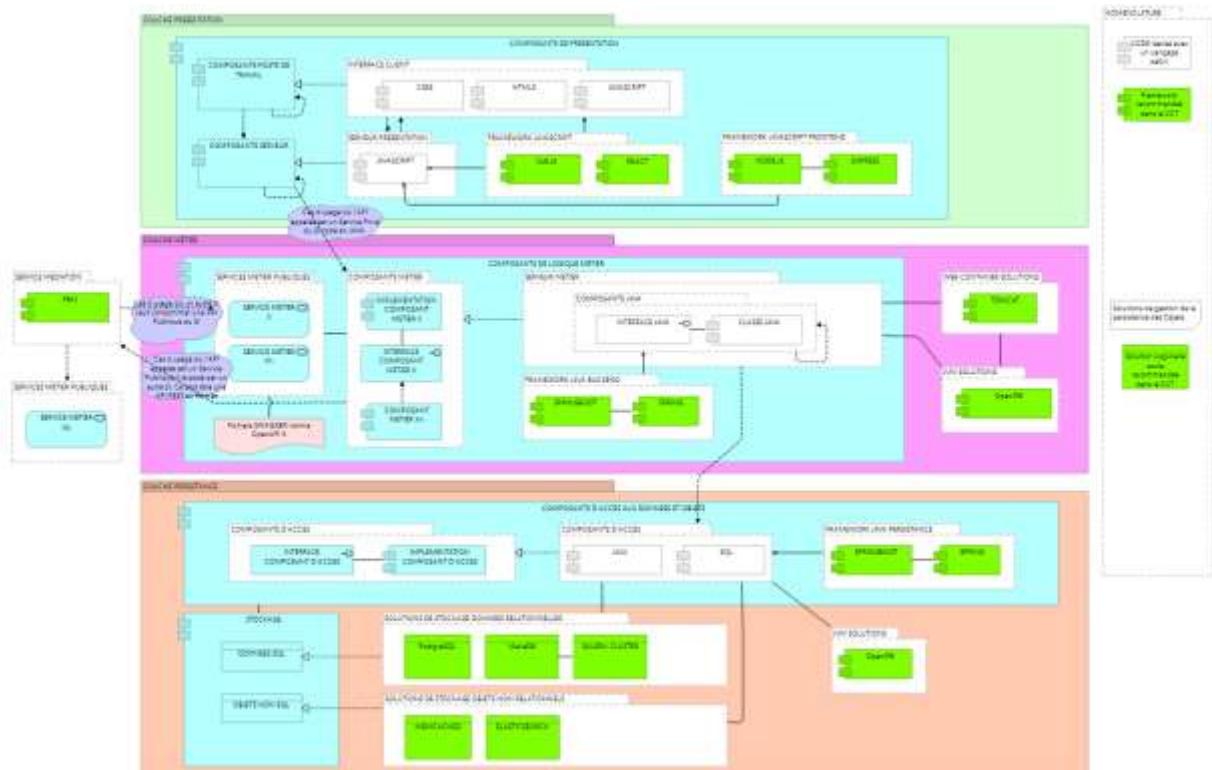


Figure 9 : Modèle d'architecture applicative Javascript sur le Frontend et Java en Backend

Une architecture alternative pourrait consister à n'avoir que du code Java sur le serveur de présentation en utilisant les librairies JSP ou JSF de Jakarta EE mais ce type d'architecture n'est plus recommandé. C'est néanmoins l'architecture de nombreux SI « historiques » du Ministère. Se pose alors la question de la façon de moderniser progressivement le frontend d'un tel SI pour le remettre en conformité.

8.7.4.4 Le modèle d'architecture de modernisation progressive d'un SI « historique » Java

Spring MVC peut servir dans une stratégie de modernisation progressive d'un système d'information « historique » réalisé en JSP ou JSF. La première étape consiste à réaliser une migration technique vers Spring MVC (le principe général est « les vues sont conservées, le contrôleur est modernisé ») puis la couche de présentation est réécrite progressivement avec un Framework Javascript (tel que Vue.js) en faisant cohabiter les nouvelles pages avec les anciennes réalisées en Java, Spring Boot assurant la configuration de l'ensemble. Le framework Javascript assure le routage côté client et Spring MVC gère le routage côté serveur (plus précisément, Spring MVC assure la configuration des routes Vue.js ou React et un contrôleur Spring MVC gère les requêtes pour ces routes). Quand tout le frontend aura été réécrit, le code Java de la couche de présentation pourra être retiré et dès lors le système d'information sera devenu conforme au modèle d'architecture Java recommandé.

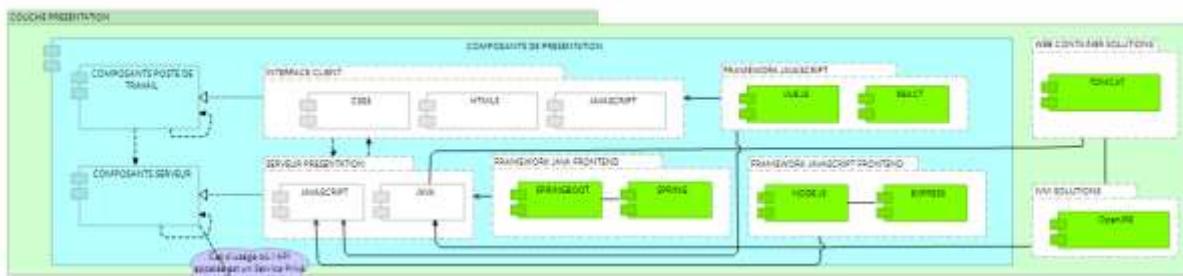


Figure 10 : Modèle d'architecture applicative de transition permettant d'assurer la modernisation progressive d'un SI « historique » Java

8.7.4.5 Le modèle d'architecture « Client-léger » permettant un mode déconnecté

Pour disposer d'un mode déconnecté, l'architecture PWA⁶⁶ est recommandée. Ceci est réalisé en exploitant les fonctionnalités d'un navigateur internet supportant ce mode. Le modèle d'architecture ci-dessous décrit les éléments clefs de cette architecture. Les seules technologies recommandées dans le CCT pour la couche de présentation des applications en client-léger sont Javascript et PHP. Ces technologies permettent ce type d'architecture.

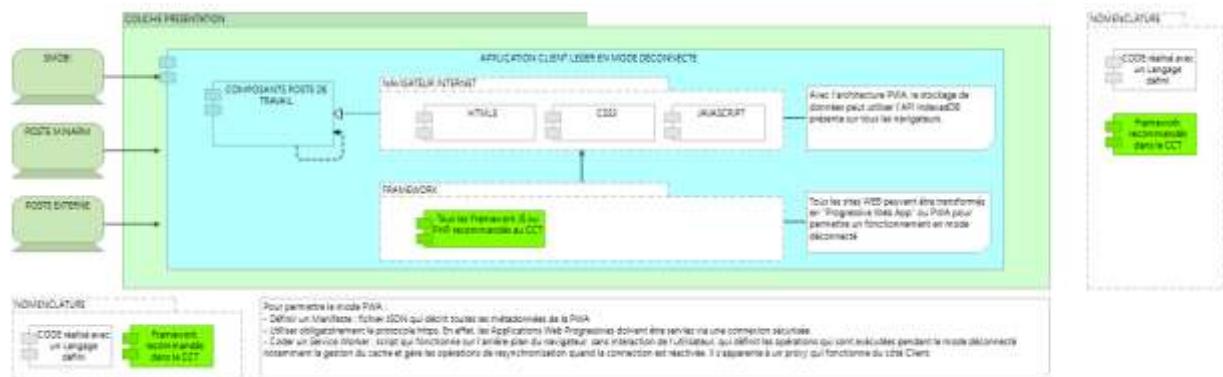


Figure 11 : Modèle d'architecture « client-léger » permettant un mode déconnecté

⁶⁶ Une **progressive web app (PWA, application web progressive en français)** est une application web constituée de pages ou de sites web et qui peuvent se présenter à l'utilisateur de la même manière que les applications natives ou les applications mobiles. Ce type d'application tente de combiner les fonctionnalités offertes par la plupart des navigateurs modernes avec les avantages de l'expérience utilisateur offerte par les appareils mobiles.