

PROJET PAGE ETABLISSEMENT : Version adaptée du portail PAGE UniHA pour les GHT et établissements

- Expression du Besoin

Introduction

Contexte du projet

Présentation de la solution PAGE UniHA existante

PAGE (Portail Adhérents Gestion Établissements) est une solution développée sur mesure par le GCS UniHA depuis 2018 pour gérer ses référentiels et ses processus. Cette plateforme est devenue le portail de référence du groupement, tant sur la partie adhérents que sur la partie métier.

Le projet PAGE ETABLISSEMENT vise à adapter la solution PAGE (développée via les outils PCSOFT en WEBDEV 28) pour créer une version autonome mise à disposition des établissements hospitaliers publics français. Cette adaptation permettra aux structures hospitalières de disposer d'un outil de gestion interne performant, respectant les contraintes réglementaires strictes du secteur de la santé publique.

L'objectif est de transformer une solution mutualisée multi-adhérents (administrée par UniHA) en une solution dédiée mono-établissement ou mono-GHT (administrée par l'hôpital), avec une simplification des modules, une modernisation de l'interface graphique, et l'ajout de fonctionnalités de personnalisation et d'administration autonome.

Périmètre actuel de PAGE UniHA :

- 1800 fournisseurs référencés
- 1400 établissements adhérents
- 12000 comptes utilisateurs actifs
- 4000 procédures d'achat actives
- 15000 produits catalogués
- 300000 documents (pièces de marchés)

La solution PAGE se compose de deux espaces distincts :

- **Backoffice** : destiné aux collaborateurs UniHA avec authentification renforcée (login + mot de passe + token email)
- **Front office** : destiné aux établissements adhérents avec authentification via O365 et API Graph Microsoft



GROUPEMENT D'ACHAT DES HÔPITAUX PUBLICS

L'architecture de PAGE repose sur un système de droits granulaires permettant de gérer finement les accès aux différents modules selon le profil utilisateur et l'établissement de rattachement.

Problématique et opportunité

Les établissements hospitaliers et GHT expriment un besoin croissant d'autonomie dans la gestion de leurs outils numériques tout en bénéficiant de solutions éprouvées. Le retour d'expérience de PAGE UniHA, qui gère avec succès des volumes importants de données et d'utilisateurs depuis plusieurs années, constitue une base solide pour développer une version adaptée aux besoins spécifiques d'un établissement ou d'un GHT unique.

Cette adaptation répond à plusieurs enjeux stratégiques :

- **Simplification opérationnelle** : Fluidité des échanges et facilité d'usage de la solution.
- **Organisation** : Mise en place de process simple optimisant cout et réactivité
- **Maîtrise et sécurisation des données** : maîtrise totale des données de l'établissement sur infrastructure dédiée ou on premise
- **Conformité réglementaire** : Tracabilité des recensements de besoin, des ruptures

Objectifs du projet

Objectif principal

Développer une version simplifiée et personnalisable de la solution PAGE, adaptée aux besoins d'un GHT ou d'un établissement hospitalier autonome, respectant le cadre réglementaire applicable au secteur de la santé publique.

Objectifs spécifiques

1. Simplifier l'architecture en ne conservant que les 5 modules essentiels à la gestion interne
2. Moderniser et simplifier la charte graphique avec un système bicolore personnalisable
3. Permettre la personnalisation visuelle (couleurs, logo) via fichier de configuration
4. Développer un système de gestion des centres d'intérêt pour les notifications
5. Créer une interface d'administration autonome des comptes utilisateurs backoffice
6. Garantir un niveau de sécurité conforme aux exigences hospitalières

Périmètre du projet

Modules conservés (5 modules essentiels)

Module	Description et fonctionnalités
ETABLISSEMENTS	Gestion des établissements du GHT ou de l'établissement unique utilisant la solution. Référentiel géographique et organisationnel.
CONTACTS	Gestion des contacts avec leurs droits, comptes utilisateurs et rattachements aux établissements. Annuaire centralisé.
ESPACE DOCUMENTAIRE	Gestion de l'ensemble des fichiers et documents relatifs aux marchés du GHT ou de l'établissement. Stockage, partage sécurisé.

HERMES	Système de messagerie pour les communications de rupture d'approvisionnement de produits (notamment médicaments) et les messages liés aux marchés. Notifications ciblées et forum d'échanges.
QUANTUM	Outil de recensement et quantification des besoins internes avant publication d'appels d'offres. Gestion des campagnes de recueil de besoin, points de livraison et résultats.

Table 1: Modules conservés dans PAGE ETABLISSEMENT

Modules supprimés

Les modules suivants de la solution PAGE UniHA ne seront pas intégrés dans PAGE ETABLISSEMENT :

- Liste complète des GHT nationaux (hors périmètre établissement)
- Annuaire national des établissements hospitaliers français (hors périmètre)
- Gestion des adhésions aux marchés UniHA (non applicable)
- Centrale d'achat (outil spécifique UniHA)
- Pilot (outil métier UniHA)
- Catalogue fournisseurs national (non nécessaire)
- Modules de gestion des procédures d'achat centralisées

Nouvelles fonctionnalités à développer

Quatre nouvelles fonctionnalités majeures seront développées spécifiquement pour PAGE ETABLISSEMENT :

1. **Modernisation de la charte graphique** : refonte complète de l'interface avec un système bicolore moderne et épuré
2. **Personnalisation visuelle configurable** : possibilité de définir deux couleurs primaires et le logo de l'établissement via fichier de configuration
3. **Gestion avancée des centres d'intérêt** : développement d'une interface dédiée permettant de définir des centres d'intérêt personnalisés pour la réception des messages
4. **Administration des comptes backoffice** : création d'une interface de gestion permettant d'attribuer des droits backoffice aux contacts utilisateurs

Description détaillée des besoins

Besoins fonctionnels

BF01 - Adaptation des modules existants

Module ETABLISSEMENTS

Adaptation pour gérer exclusivement le périmètre du GHT ou de l'établissement utilisateur :

- Référentiel limité aux établissements du GHT ou au seul établissement utilisateur
- Gestion des sites géographiques et points de livraison
- Structuration organisationnelle interne

- Export des données établissements

Module CONTACTS

Conservation de l'ensemble des fonctionnalités avec ajouts spécifiques :

- Gestion complète des contacts (création, modification, suppression)
- Rattachement aux établissements du périmètre
- Gestion des droits front office (par module et par fonctionnalité)
- **NOUVEAU** : Interface d'attribution des droits backoffice (voir BF05)
- Import/export de contacts
- Synchronisation avec annuaire Active Directory (optionnel)

Module ESPACE DOCUMENTAIRE

Conservation de l'ensemble des fonctionnalités :

- Arborescence personnalisable par filière d'achat et segment d'achat
- Upload de documents
- Gestion des droits d'accès par document
- Moteur de recherche avancé
- Génération de ZIP pour téléchargement multiple
- Statistiques de consultation

Module HERMES

Conservation de l'ensemble des fonctionnalités avec ajouts spécifiques :

- Système de messages ciblés par établissement
- Gestion des ruptures d'approvisionnement
- Forum d'échanges par message
- **NOUVEAU** : Gestion des centres d'intérêt personnalisés (voir BF04)
- **NOUVEAU** : API de remontée des ruptures vers UniHA (voir BF06)
- Notifications paramétrables (fréquence, canaux)
- Archivage automatique et manuel
- Export des messages

Module QUANTUM

Conservation de l'ensemble des fonctionnalités :

- Gestion des campagnes de recensement de besoins
- Saisie des quantités par établissement et par point de livraison
- Validation hiérarchique (établissement partie/support)
- Export des résultats

- Import/export Excel
- Tableau de bord de suivi des campagnes

BF02 - Modernisation de la charte graphique

Objectif : Refonte complète de l'interface utilisateur pour adopter un design moderne, épuré et cohérent avec les standards actuels d'ergonomie web.

Principes de design :

- **Simplicité visuelle** : réduction du nombre de couleurs à un système bicolore
 - Couleur primaire : actions principales, boutons CTA, liens importants
 - Couleur secondaire : éléments d'interface, bordures, états hover
- **Hiérarchie visuelle claire** : utilisation de la typographie, des espacements et des contrastes pour guider l'utilisateur
- **Cohérence** : application systématique des mêmes conventions d'interface sur tous les modules
- **Accessibilité** : Conformité d'accès aux personnes ayant un handicap

Éléments à refondre :

- Navigation principale et secondaire
- Boutons et contrôles de formulaire
- Tableaux de données
- Cartes et conteneurs
- Icônes (uniformisation avec bibliothèque moderne type Lucide ou Heroicons)
- États interactifs (hover, focus, active, disabled)
- Messages de feedback (succès, erreur, avertissement, information)
- Modales et overlays

Livrables attendus en phase 1 du projet :

- Maquettes des écrans principaux validées avant développement
- Guide de style (style guide) documentant tous les composants
- Bibliothèque de composants réutilisables

BF03 - Personnalisation visuelle via configuration

Objectif : Permettre à chaque établissement de personnaliser l'identité visuelle de son portail PAGE sans intervention technique.

Mécanisme de configuration :

Création d'un fichier de configuration `customization.json` ou section dédiée dans le fichier de configuration principal contenant :

```
{
  "branding": {
```



GROUPEMENT D'ACHAT DES HÔPITAUX PUBLICS

```
"organizationName": "CHU Example",  
"primaryColor": "#2E7D32",  
"secondaryColor": "#66BB6A",  
"logoPath": "/assets/logo-custom.png",  
"faviconPath": "/assets/favicon-custom.ico"  
}  
}
```

Fonctionnalités :

1. **Définition des couleurs primaire et secondaire**
 - Format hexadécimal RGB (#RRGGBB)
 - Validation automatique du contraste pour accessibilité
 - Application automatique sur tous les composants d'interface
2. **Personnalisation du logo**
 - Upload via interface backoffice ou dépôt fichier
 - Formats acceptés : PNG, SVG (recommandé), JPG
 - Dimensions recommandées : 200x60px (adaptabilité responsive)
 - Affichage : en-tête de navigation, emails, exports PDF et XLSX
3. **Personnalisation du favicon**
 - Format ICO ou PNG 32x32px minimum
4. **Application des modifications**
 - Rechargement automatique de la configuration sans redémarrage applicatif (hot reload)
 - Historique des configurations précédentes

Interface d'administration :

Développement d'un écran d'administration dédié dans le backoffice permettant :

- Modification des couleurs avec color picker
- Upload des fichiers logo et favicon
- Validation et application
- Réinitialisation aux valeurs par défaut

BF04 - Gestion des centres d'intérêt personnalisés

Objectif : Permettre aux administrateurs de l'établissement de définir des centres d'intérêt spécifiques adaptés à leur organisation, au-delà des catégories prédéfinies dans PAGE UniHA.

Contexte :

Dans PAGE UniHA, les centres d'intérêt correspondent aux 17 filières UniHA (Médicaments, Dispositifs médicaux, Biologie, etc.)[2]. PAGE ETABLISSEMENT doit permettre de définir des centres d'intérêt adaptés à l'organisation interne de l'établissement.

Fonctionnalités attendues :

Retrouvez UniHA sur www.uniha.org - contact@uniha.org
UniHA 83 Boulevard Vivier Merge 69003 Lyon SIRET 130 002 223 00043 - Page 6 sur 23

1. **Interface de gestion des centres d'intérêt**

Développement d'une boîte de dialogue/écran d'administration permettant :

- Création de nouveaux centres d'intérêt (libellé, description, code)
- Modification de centres d'intérêt existants
- Suppression (avec gestion des dépendances utilisateurs)
- Activation/désactivation sans suppression
- Organisation hiérarchique (catégorie parent/enfant si pertinent)
- Définition de couleurs associées pour identification visuelle

2. **Affectation aux utilisateurs**

- Lors de la création/modification par un contact de sa fiche contact, possibilité de sélectionner les centres d'intérêt
- Sélection multiple avec interface intuitive (checkboxes, tags)

Données et structure :

Droits d'accès :

Seul l'utilisateur, via sa fiche contact peut gérer ses centres d'intérêt.

BF06 - API de remontée des ruptures vers UniHA

Objectif : Permettre au GCS UniHA d'enrichir son HERMES central avec les ruptures d'approvisionnement déclarées localement dans les instances HERMES des établissements équipés de PAGE ETABLISSEMENT, tout en conservant un contrôle qualité via une interface de validation côté UniHA.

Contexte :

La gestion des ruptures d'approvisionnement constitue un enjeu majeur pour le secteur hospitalier public. Le GCS UniHA, en tant que groupement d'achat national, a besoin de disposer d'une vision consolidée des ruptures déclarées par l'ensemble des établissements pour pouvoir alerter rapidement tous les adhérents concernés et mettre en place des actions correctives (recherche d'alternatives, négociations fournisseurs).

Actuellement, dans PAGE UniHA, les ruptures sont déclarées directement dans HERMES UniHA par les filières de la centrale d'achat. Avec le déploiement de PAGE ETABLISSEMENT, les établissements et GHT disposeront de leur propre instance HERMES pour gérer leurs ruptures locales. Il est donc nécessaire de mettre en place un mécanisme permettant de remonter automatiquement ces informations vers UniHA, tout en garantissant leur fiabilité et leur pertinence.

Seul est attendu la demi interface coté HERMES. UniHA mettra à disposition l'autre demi interface coté UniHA et délivrera les tokens aux adhérents/Etablissements utilisateurs.

Principes de fonctionnement :

1. **Flux de données unidirectionnel :** PAGE ETABLISSEMENT → PAGE UniHA (jamais l'inverse)



GROUPEMENT D'ACHAT DES HÔPITAUX PUBLICS

2. **Remontée sélective** : seules les ruptures marquées comme "à remonter" sont transmises.
3. **Validation côté UniHA** : interface dédiée permettant de valider/rejeter avant intégration
4. **Traçabilité complète** : historique de toutes les remontées et validations
5. **Mise à jour bidirectionnelle** : statut de validation renvoyé à l'établissement

Fonctionnalités côté PAGE ETABLISSEMENT :

1. Marquage des ruptures à remonter

Dans l'interface HERMES Rupture, ajout d'une fonctionnalité permettant :

- Case à cocher "Remonter à UniHA" sur chaque fiche rupture
- Indication visuelle du statut de remontée :
 - Non remontée (pas cochée)
 - En attente de validation UniHA (transmise)
 - Validée par UniHA (intégrée dans HERMES UniHA)
 - Rejetée par UniHA (avec motif)
- Possibilité de modifier/compléter les informations avant remontée

2. Données transmises

Pour chaque rupture, les informations suivantes sont envoyées à l'API UniHA :

- Identifiant établissement (code FINESS)
- Nom établissement et GHT de rattachement
- Référence produit (code EAN, code ACL, ou description détaillée)
- Libellé produit
- Laboratoire/Fournisseur concerné
- Date début rupture (constatée)
- Date fin rupture prévisionnelle (si connue)
- Type de rupture (totale, partielle, contingentement)
- Criticité (impact sur les soins)
- Commentaires et alternatives identifiées localement
- Contact référent établissement
- Date de création de la fiche rupture
- Historique des mises à jour

3. Transmission automatisée

- Envoi automatique lorsque case "Remonter à UniHA" cochée et fiche validée
- Possibilité de transmission manuelle différée (brouillon)
- Mise à jour automatique si modification de la fiche rupture après transmission
- Réception du statut de validation depuis UniHA (webhook ou polling)

Fonctionnalités côté PAGE UniHA :

1. Interface de réception et validation

Développement d'une interface backoffice UniHA dédiée permettant :

- Visualisation de toutes les ruptures remontées par les établissements
- Filtres : par établissement, par GHT, par produit, par date, par statut
- Affichage détaillé de chaque rupture avec toutes les données transmises
- Possibilité de rattachement de la rupture à un marché UniHA
- Actions possibles :
 - Valider : intégration automatique dans HERMES UniHA
 - Rejeter : avec saisie obligatoire du motif de rejet
 - Mettre en attente : demande de complément d'information
 - Fusionner : avec une rupture existante dans HERMES UniHA
- Notification de l'établissement émetteur du statut de validation

2. Intégration dans HERMES UniHA

Lors de la validation :

- Création automatique d'une fiche rupture dans HERMES UniHA
- Enrichissement possible par les filières UniHA (alternatives, offres fournisseurs)
- Lien conservé avec la rupture source de l'établissement
- Diffusion automatique aux adhérents concernés selon leurs centres d'intérêt

3. Tableau de bord statistiques sur HERMES ETABLISSEMENT ET HERMES UNIHA

- Nombre de ruptures remontées par établissement/GHT
- Délai moyen de validation
- Taux de validation/rejet
- Typologie des ruptures (produits, laboratoires)
- Cartographie des ruptures par zone géographique

Spécifications techniques de l'API :

1. Architecture API REST

- Protocole : HTTPS (TLS 1.3 minimum)
- Format : JSON
- Authentification : OAuth 2.0 (Client Credentials Flow)
- Rate limiting : 100 requêtes/minute par établissement

2. Endpoints principaux

POST /api/v1/ruptures/submit

- Soumission d'une nouvelle rupture par un établissement

- Authentification : Token Bearer OAuth 2.0
- Payload : JSON contenant toutes les données rupture
- Réponse : 201 Created avec identifiant unique rupture et statut

PUT /api/v1/ruptures/{id}/update

- Mise à jour d'une rupture existante
- Conditions : rupture non encore validée ou rejetée par UniHA
- Réponse : 200 OK ou 403 Forbidden si déjà traitée

GET /api/v1/ruptures/{id}/status

- Consultation du statut de validation d'une rupture
- Réponse : statut (pending, validated, rejected, merged) + détails

POST /api/v1/ruptures/{id}/validate (côté UniHA uniquement)

- Validation d'une rupture par un utilisateur backoffice UniHA
- Déclenche création dans HERMES UniHA et notification établissement

POST /api/v1/ruptures/{id}/reject (côté UniHA uniquement)

- Rejet d'une rupture avec motif obligatoire
- Notification établissement avec raisons du rejet

3. Authentification et sécurité

- Chaque instance PAGE ETABLISSEMENT reçoit des credentials OAuth 2.0 uniques
- Token d'accès avec expiration (1 heure), refresh token pour renouvellement
- Chiffrement TLS 1.3 sur tous les échanges
- Signature des payloads JSON (HMAC-SHA256) pour garantir intégrité
- Validation côté serveur de l'identité établissement (code FINESS)
- Logs détaillés de tous les appels API (qui, quand, quoi)

4. Gestion des erreurs

Codes HTTP standards :

- 200 OK : succès
- 201 Created : rupture créée
- 400 Bad Request : données invalides (avec détails erreurs)
- 401 Unauthorized : authentification échouée
- 403 Forbidden : opération non autorisée
- 404 Not Found : rupture inexistante
- 429 Too Many Requests : rate limit dépassé
- 500 Internal Server Error : erreur serveur UniHA
- 503 Service Unavailable : maintenance en cours

5. Chaque erreur retourne un JSON structuré :

- Code erreur spécifique
 - Message d'erreur explicite en français
 - Timestamp
 - Identifiant de corrélation pour debug
6. **Webhook de notification (optionnel)**
- PAGE ETABLISSEMENT peut exposer un endpoint pour recevoir notifications
 - UniHA notifie automatiquement changement statut (validation/rejet)
 - Évite polling fréquent de l'API pour vérifier statut
 - Sécurisé par signature HMAC des payloads

Workflow complet :

1. Établissement déclare rupture dans HERMES local
2. Responsable coche "Remonter à UniHA" et valide
3. PAGE ETABLISSEMENT envoie données via API POST /ruptures/submit
4. UniHA reçoit, enregistre avec statut "pending"
5. Notification apparaît dans interface validation UniHA
6. Coordinateur/filière UniHA examine la rupture :
 - Si conforme et pertinente → Validation
 - Si doublon/non pertinente → Rejet avec motif
 - Si incomplète → Demande complément
7. Statut mis à jour côté UniHA
8. Notification renvoyée à PAGE ETABLISSEMENT (webhook ou polling)
9. Si validée : création fiche rupture HERMES UniHA + diffusion adhérents + possibilité de modification
10. Si rejetée : affichage motif dans PAGE ETABLISSEMENT

Contraintes et règles métier :

- Une rupture ne peut être remontée qu'une seule fois (pas de doublons)
- Modifications ultérieures mettent à jour la rupture existante
- Délai de validation cible : 4 heures ouvrées maximum
- Conservation historique : 5 ans minimum
- Anonymisation partielle : contacts établissement non diffusés aux adhérents
- Possibilité pour établissement de révoquer une remontée avant validation

Droits d'accès :

- **Côté établissement :** utilisateurs backoffice HERMES peuvent marquer ruptures à remonter
- **Côté UniHA :** coordinateurs filières et administrateurs système peuvent valider/rejeter

- **Logs audit** : toutes actions tracées avec identité utilisateur

Tests et recette :

- Environnement de test API dédié (sandbox)
- Jeux de données de test fournis
- Tests de charge : 1000 ruptures simultanées
- Tests de sécurité : authentification, autorisation, injection
- Tests de résilience : indisponibilité temporaire API, timeout
- Validation processus complet avec établissement pilote

BF05 - Administration des comptes utilisateurs backoffice

Objectif : Permettre aux administrateurs de l'établissement de gérer de manière autonome les droits d'accès backoffice sans intervention du support technique.

Contexte :

Actuellement dans PAGE UniHA, les droits backoffice sont réservés aux collaborateurs UniHA et gérés de manière centralisée. PAGE ETABLISSEMENT doit permettre à l'établissement d'administrer lui-même les droits backoffice de ses utilisateurs.

Actuellement une interface de gestion des droits existe déjà, accessible seulement aux ADMINISTRATEURS.

La gestion des comptes Backoffice est faite dans une table dédiée, contenant l'ID contact, l'ID utilisateur backoffice, son niveau d'accréditation (USER, ADMINISTRATEUR, SUPER ADMINISTRATEUR), et ses droits. Seul le niveau d'accréditation SUPER ADMINISTRATEUR permet de gérer les droits Backoffice.

Fonctionnalités attendues :

1. **Interface de gestion des droits backoffice**

Développement d'une boîte de dialogue dédiée accessible depuis la fiche contact permettant :

- Visualisation du statut actuel (front office / backoffice)
- Activation/désactivation de l'accès backoffice
- Sélection des modules backoffice accessibles (granularité par module) en se basant sur une chaîne de 41 bit (41 droits) stockée en BD.

2. **Gestion de l'authentification backoffice**

- Conservation du système d'authentification renforcée (login + mot de passe + token)
- Possibilité d'activer l'authentification à deux facteurs (2FA) via application mobile
- Politique de mots de passe configurable (complexité, expiration)
- Gestion des tentatives de connexion échouées et blocage temporaire

3. **Tableau de bord d'administration**

- Vue d'ensemble des utilisateurs backoffice actifs
- Filtres par module, niveau de droits, établissement

- Export de la liste des utilisateurs et droits
- Indicateurs : nombre d'utilisateurs backoffice, dernières connexions, droits à renouveler

Sécurité et contrôles :

- Un utilisateur ne peut pas modifier ses propres droits backoffice ou front office.
- Au moins un administrateur système doit toujours être présent (protection)
- Suppression d'un utilisateur backoffice nécessite confirmation
- Logs détaillés de toutes les modifications de droits (qui, quand, quoi)
- Notification automatique aux administrateurs lors de changements importants

Besoins non fonctionnels

BNF01 - Exigences de sécurité

Le projet PAGE ETABLISSEMENT doit respecter les normes de sécurité les plus strictes applicables aux établissements de santé publics.

Sécurité applicative :

1. **Authentification et contrôle d'accès**
 - Authentification forte pour accès backoffice (multi-facteurs)
 - Support de l'authentification SSO via O365 pour front office
 - Gestion des sessions sécurisées (timeout, renouvellement)
 - Politique de mots de passe robuste (longueur, complexité, historique)
 - Principe du moindre privilège pour attribution des droits
2. **Protection des données**
 - Chiffrement des communications (TLS 1.3 minimum)
 - Chiffrement des données au repos sur les espaces de stockage
 - Pseudonymisation des données dans les logs et exports
 - Mécanismes de sauvegarde chiffrée
3. **Sécurité du code**
 - Protection contre les injections SQL (requêtes paramétrées, ORM)
 - Protection contre les attaques XSS (échappement, CSP)
 - Protection contre les CSRF (tokens anti-CSRF)
 - Validation et sanitisation de toutes les entrées utilisateur
 - Gestion sécurisée des fichiers uploadés (scan antivirus, validation type MIME)
4. **Traçabilité et audit**
 - Logs détaillés de toutes les actions sensibles (connexions, modifications droits, accès données)
 - Conservation des logs conformément aux exigences HDS (minimum 6 mois)

- Impossibilité de modification des logs (intégrité)
- Alertes automatiques sur événements de sécurité critiques

Audit de sécurité obligatoire :

Avant mise en production, l'application devra faire l'objet d'un audit de sécurité par un organisme indépendant spécialisé comprenant :

- Tests d'intrusion (pentest) sur l'ensemble des modules
- Revue de code source (code review) focalisée sécurité
- Analyse des vulnérabilités (scan automatisé + analyse manuelle)
- Vérification de la conformité au référentiel OWASP Top 10
- Rapport d'audit détaillé avec classification des risques

Important : L'audit de sécurité et la correction des vulnérabilités identifiées ne font pas partie du présent périmètre d'expression du besoin mais devront être intégrés au planning global du projet.

BNF02 - Compatibilité et accessibilité

Compatibilité navigateurs :

Support des versions récentes (N et N-1) de :

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari (macOS et iOS)

Compatibilité devices :

- **Desktop** : résolutions de 1366x768 minimum à 4K
- **Tablette** : iPad, tablettes Android (responsive)

Accessibilité :

Conformité RGAA 4.1 (Référentiel Général d'Amélioration de l'Accessibilité) niveau à définir :

- Structuration sémantique HTML5
- Navigation au clavier complète
- Contrastes suffisants (ratio 4.5:1 minimum)
- Alternatives textuelles pour contenus non textuels
- Formulaire étiquetés et messages d'erreur explicites

BNF03 - Maintenabilité et évolutivité

Architecture logicielle :

- Architecture modulaire facilitant l'évolution indépendante des modules

- Séparation claire des couches (présentation, logique métier, données)
- Code commenté et documenté (documentation technique complète)
- Respect des standards de développement PCSOFT
- Tests unitaires sur fonctions critiques (couverture 70% minimum)

Base de code :

- Gestion de versions Git avec historique complet
- Stratégie de branches (develop, staging, production)
- Documentation des dépendances et procédures de déploiement
- Scripts d'installation et migration de données

Transfert de compétences :

Le prestataire devra prévoir :

- Documentation technique complète (architecture, schémas BDD, APIs)
- Documentation fonctionnelle (guides administrateur, guides utilisateur)
- Sessions de formation pour l'équipe technique de l'établissement
- Support pendant période de garantie (durée à définir contractuellement)

Besoins techniques

Architecture technique

Stack technologique attendue :

En cohérence avec l'existant PAGE UniHA et les contraintes de souveraineté :

- **Backend / Frontend:**
 - PC SOFT WEBDEV 28 minimum
 - Base de données : SQL Server 2019
 - Serveur web : IIS (environnement Windows) ou Nginx/Apache
- **Authentification :**
 - Support OAuth 2.0 / OpenID Connect pour SSO O365
 - API Microsoft Graph pour authentification front office
 - Système de tokens JWT pour gestion des sessions
- **Stockage fichiers :**
 - Système de fichiers Windows (espaces réseau)

Commenté [EB1]: Reformuler ce qui est attendu « les exigences relatives à la maîtrise des données, à leur localisation et à la sécurité des systèmes d'information »

Commenté [EB2]: On ne peut pas imposer une technologie !

Environnement d'exécution :

- Serveurs Windows Server 2019+ ou Linux (selon préférence établissement)
- Conteneurisation possible (Docker) pour faciliter déploiements



GROUPEMENT D'ACHAT DES HÔPITAUX PUBLICS

- Scripts de déploiement automatisé (CI/CD)

Intégrations et APIs

Demi APIs à développer :

1. API RESTful pour accès aux données (JSON)
 - Authentification par tokens Bearer
 - Documentation OpenAPI 3.0 (Swagger)
 - Endpoints pour chaque module (CRUD)
 - Pagination, filtres, tri sur collections

Intégrations externes :

- **Microsoft 365** : authentification SSO via Azure AD / Microsoft Graph API
- **Antivirus** : scan automatique fichiers uploadés sur Mon Espace Doc (API ClamAV ou équivalent)
- **API UniHA** : remontée ruptures HERMES vers centrale UniHA (voir BF06)

Configuration et paramétrage

Fichiers de configuration :

L'ensemble des paramètres sont externalisés dans des fichiers de configuration pour chaque module (pas de hardcoding) :

- Connexion base de données (host, port, credentials)
- Chemins espaces de stockage fichiers
- Configuration serveur SMTP (host, port, authentification)
- Timeouts (sessions, connexions, uploads)
- Paramètres métier :
 - Délais d'archivage automatique messages/ruptures
 - Tailles maximales fichiers uploadés
 - Nombre de résultats par page
 - URLs externes (support, FAQ)
- Personnalisation visuelle (couleurs, logos) - voir BF03

Format : JSON ou YAML privilégiés pour lisibilité et facilité de maintenance.

Sécurité : Les credentials sensibles devront être chiffrées dans les fichiers de configuration ou gérées via variables d'environnement.

Organisation du projet

Gouvernance et pilotage

Comité de pilotage

Retrouvez UniHA sur www.uniha.org - contact@uniha.org
UniHA 83 Boulevard Vivier Merge 69003 Lyon SIRET 130 002 223 00043 - Page 16 sur 23



GROUPEMENT D'ACHAT DES HÔPITAUX PUBLICS

Composition :

- DSI UniHA
- Product Owner UniHA + Etablissements
- Direction du pôle AR UniHA
- Responsable Projets et Outils numériques UniHA
- Représentants métiers (Achats, Pharmacie, Logistique)
- Chef de projet prestataire
- Architecte technique

Rôle :

- Validation des livrables majeurs (spécifications, maquettes, recettes)
- Arbitrage sur orientations fonctionnelles et techniques
- Suivi du planning et du budget
- Gestion des risques et des changements de périmètre

Fréquence : réunion mensuelle minimum, exceptionnelle si besoin

Équipe projet

Côté maîtrise d'ouvrage (UniHA+Etablissements demandeurs) :

- **Chef de projet MOA** : coordination générale, interface prestataire, suivi planning/budget
- **Product Owner des établissements adhérents**
- **Référent fonctionnel module ETABLISSEMENTS/CONTACTS** : expression des besoins, validation
- **Référent fonctionnel module ESPACE DOCUMENTAIRE** : expression des besoins, validation
- **Référent fonctionnel module HERMES** : expression des besoins, validation
- **Référent fonctionnel module QUANTUM** : expression des besoins, validation
- **Administrateur système** : préparation infrastructure, exploitation future

Côté prestataire (MOE) :

- **Chef de projet MOE** : coordination équipe, interface MOA, planning détaillé, qualité livrables
- **Architecte technique** : conception architecture, choix technologiques, documentation technique
- **Développeurs backend** : développement modules serveur, APIs, base de données (2-3 personnes)
- **Développeurs frontend** : refonte interface, composants UI, responsive (2 personnes)
- **Expert sécurité** : implémentation mesures sécurité, préparation audit
- **Testeur QA** : tests fonctionnels, non-régressifs, performance

- **Rédacteur technique** : documentation technique et fonctionnelle

Méthodologie et phases (à titre indicatif)

Approche méthodologique : Méthodologie Agile adaptée avec cycles itératifs et validation progressive.

Phases du projet :

Phase 1 : Cadrage et conception (environ 3 mois, à titre indicatif)

Objectifs :

- Validation détaillée des spécifications fonctionnelles
- Conception de l'architecture technique
- Validation des maquettes et de la charte graphique
- Préparation environnements de développement
- Plan de tests

Livrables :

- Spécifications fonctionnelles détaillées validées
- Dossier d'Architecture Technique (DAT)
- Maquettes écrans (wireframes et mockups haute-fidélité)
- Guide de style (design system)
- Plan d'Assurance Qualité (PAQ)
- Planning détaillé phases suivantes

Jalons :

- J+15 : Atelier de cadrage et présentation méthodologie
- J+30 : Validation spécifications fonctionnelles
- J+45 : Validation maquettes et charte graphique
- J+60 : Validation DAT et lancement développement

Phase 2 : Développement itératif (environ 3 mois, à titre indicatif)

Organisation : 3 sprints par exemple

Sprint 1 : Modules de base et nouvelle charte

Périmètre :

- Refonte complète de la charte graphique
- Module ETABLISSEMENTS adapté
- Module CONTACTS adapté (hors gestion droits backoffice)
- Infrastructure d'authentification (SSO O365)
- BF03 : Système de personnalisation visuelle configurable

Livrable : Version beta 1 déployée sur environnement de recette

Sprint 2 : Modules métiers

Périmètre :

- Module ESPACE DOCUMENTAIRE complet
- Module HERMES adapté (hors centres d'intérêt personnalisés et API)
- Module QUANTUM adapté
- BF04 : Gestion des centres d'intérêt personnalisés

Livrable : Version beta 2 déployée sur environnement de recette

Sprint 3 : Fonctionnalités avancées et finalisation

Périmètre :

- BF05 : Administration des comptes backoffice
- BF06 : API de remontée des ruptures vers UniHA
- APIs et exports
- Optimisations performance
- Corrections anomalies identifiées

Livrable : Version Release Candidate

Rituels Agile :

- Réunion de lancement de sprint (Sprint Planning)
- Démo de fin de sprint avec MOA (Sprint Review)
- Rétrospective d'amélioration continue
- Points hebdomadaires de suivi (stand-up)

Phase 3 : Recette et sécurisation (2 mois environ à titre indicatif)

Recette fonctionnelle

- Exécution des scénarios de tests par équipe MOA
- Tests d'acceptation utilisateurs (UAT) avec panel utilisateurs réels
- Tests de charge et performance
- Tests de compatibilité navigateurs/devices
- Tests d'accessibilité RGAA
- Correction des anomalies bloquantes et majeures

Audit de sécurité et corrections

- Audit de sécurité par organisme indépendant (pentest, revue code)
- Analyse des vulnérabilités identifiées

- Corrections des failles de sécurité
- Nouvel audit de contrôle (si nécessaire)
- Obtention du rapport d'audit favorable

Livrables :

- PV de recette fonctionnelle
- Rapport d'audit de sécurité
- Version finale validée pour production
- Documentation complète (technique, fonctionnelle, exploitation)

Phase 4 : Déploiement et accompagnement (1 mois environ à titre indicatif)

Mise en production

- Préparation infrastructure production (serveurs, BDD, stockage)
- Migration des données initiales (établissements, contacts)
- Déploiement application sur environnement production
- Tests de bon fonctionnement production (smoke tests)
- Formations administrateurs et utilisateurs
- Communication et accompagnement au changement
- Mise en service progressive (pilote puis généralisation)

Support post-déploiement :

- Accompagnement renforcé pendant 1 mois (support réactif)
- Correction des anomalies résiduelles
- Ajustements mineurs selon retours utilisateurs
- Transfert de compétences équipe technique établissement

Livrables :

- Application déployée en production
- Documentation d'exploitation
- Guides utilisateurs finaux
- PV de mise en service
- Bilan de projet

Planning prévisionnel global à titre indicatif

Durée totale estimée : 11 mois

Phase	Durée	Période
Phase 1 : Cadrage et conception	2 mois	M1-M2
Phase 2 : Développement itératif	3 mois	M3-M8

Phase 3 : Recette et sécurisation	2 mois	M9-M10
Phase 4 : Déploiement et accompagnement	1 mois	M11

Table 2: Planning prévisionnel du projet PAGE ETABLISSEMENT

Jalons majeurs :

- M2 : Go/No-Go développement
- M4 : Livraison Beta 1 (charte + modules de base)
- M6 : Livraison Beta 2 (modules métiers)
- M8 : Livraison Release Candidate
- M9 : PV de recette fonctionnelle
- M10 : Rapport d'audit de sécurité favorable
- M11 : Mise en production

Gestion des risques

Principaux risques identifiés :

Risque	Impact	Mitigation
Disponibilité des référents MOA	Retards validation, specs incomplètes	Engagement formel disponibilité, backup pour chaque rôle
Complexité technique sous-estimée	Dépassements délais/budget	Phase de cadrage approfondie, validation DAT, sprints courts
Échec audit de sécurité	Retard mise en production, retravail important	Expert sécurité intégré dès phase 1, pre-audit mi-projet
Évolution réglementaire	Refontes techniques	Veille réglementaire continue, architecture modulaire
Résistance au changement utilisateurs	Faible adoption outil	Implication utilisateurs dès conception, formations, communication
Indisponibilité infrastructure	Blocage développement/recette	Environnements préparés en amont, PRA/PCA définis

Table 3: Matrice des risques projet

Livrables attendus

Livrables conception :

- Spécifications fonctionnelles détaillées
- Dossier d'Architecture Technique (DAT)
- Maquettes et guide de style
- Plan d'Assurance Qualité

Livrables développement :

- Code source complet avec gestion de versions
- Scripts de déploiement et migration
- Version applicative déployable

Livrables documentation :

- Documentation technique complète (architecture, BDD, APIs)
- Documentation d'exploitation (installation, configuration, supervision)
- Documentation administrateur (gestion droits, centres d'intérêt, personnalisation)

Livrables recette et sécurité :

- Cahier de tests et PV de recette
- Rapport d'audit de sécurité avec plan de remédiation
- Rapport de tests de performance

Livrables déploiement :

- Procédures de déploiement production
- Plan de formation et supports
- PV de mise en service
- Bilan de projet

Critères d'acceptation

Critères fonctionnels

Le projet sera considéré comme accepté si :

1. Les 5 modules (ETABLISSEMENTS, CONTACTS, ESPACE DOCUMENTAIRE, HERMES, QUANTUM) sont opérationnels et conformes aux spécifications validées
2. La nouvelle charte graphique bicolore est appliquée de manière cohérente sur l'ensemble des écrans
3. La personnalisation visuelle (2 couleurs + logo) est fonctionnelle via fichier de configuration et interface d'administration
4. La gestion des centres d'intérêt personnalisés est opérationnelle avec interface dédiée
5. L'administration des comptes backoffice est fonctionnelle avec interface de gestion des droits
6. L'API de remontée des ruptures vers UniHA est opérationnelle avec interface de validation côté UniHA
7. Tous les scénarios de tests de recette sont validés (taux de succès 100% sur scénarios critiques, 95% sur scénarios nominaux)
8. L'outil est utilisable sur les navigateurs et devices définis (compatibilité validée)
9. L'accessibilité correspond aux niveaux de spécifications demandées

Critères non-fonctionnels

1. Les objectifs de performance sont atteints (temps de réponse \leq 2s pour 95% des requêtes)
2. L'audit de sécurité est favorable (aucune vulnérabilité critique ou haute non corrigée)
3. La documentation est complète et de qualité suffisante pour exploitation autonome
4. Les formations ont été dispensées et validées par les participants

Conditions d'Admission

L'admission du projet se déroulera dans les conditions définies au chapitre 6 du CCAG TIC avec les précisions suivantes :

- La vérification d'aptitude (recette fonctionnelle)
- Audit de sécurité
- Vérification de service régulier d'une durée de trois mois.

A l'issue de ces vérifications, UniHA prendra une décision dans les conditions de l'article 33 du CCAG TIC.

Annexes

Glossaire

- **GHT** : Groupement Hospitalier de Territoire - regroupement d'établissements publics de santé d'un même territoire
- **UniHA** : Union des Hôpitaux pour les Achats - groupement de coopération sanitaire (GCS) spécialisé dans les achats hospitaliers
- **RGPD** : Règlement Général sur la Protection des Données - réglementation européenne sur la protection des données personnelles
- **SSO** : Single Sign-On - mécanisme d'authentification unique
- **API** : Application Programming Interface - interface de programmation
- **RGAA** : Référentiel Général d'Amélioration de l'Accessibilité - norme française d'accessibilité numérique
- **PGSSI-S** : Politique Générale de Sécurité des Systèmes d'Information de Santé