YOUR CAR YOUR WAY

COMPLIANCE ASSESSMENT

Évaluation de conformité architecturale

Version	2.0
Date	01 février 2026
Auteur	Arnaud DERISBOURG
Statut	Version révisée

Historique des versions

Version	Date	Modifications
1.0	30/01/2026	Version initiale
2.0	01/02/2026	Contrôles quantifiables, métriques, seuils, traçabilité ADD/BR

Sommaire

Objet du document

Ce document évalue la conformité de l'implémentation de l'application Your Car Your Way par rapport aux spécifications définies dans le Business Requirements (BR) et l'Architecture Definition Document (ADD).

Chaque contrôle est défini avec une métrique mesurable, un seuil d'acceptation quantifié, une méthode de vérification reproductible et une référence directe vers la section de l'ADD ou du BR correspondante. Cette approche garantit que chaque contrôle est objectivement vérifiable.

Périmètre : les contrôles portent principalement sur le périmètre du PoC (authentification + support client temps réel + chatbot). Les éléments hors PoC sont signalés.

Description générale de l'architecture

L'application Your Car Your Way repose sur une architecture client-serveur en couches (cf. ADD §3 et §6) :

- Frontend : Angular 19 (SPA avec standalone components) communiquant via REST et WebSocket
- Backend : Spring Boot 4.0.0 (Java 21) organisé en couches Controller → Service → Repository
- Base de données : PostgreSQL 15, conformité 3NF démontrée (cf. ADD §5.1)
- Temps réel : WebSocket avec protocole STOMP pour le tchat (cf. ADD §6.5)
- Sécurité : JWT stateless + BCrypt + CORS (cf. ADD §6.4)
- Infrastructure : Docker Compose pour la conteneurisation de la BDD (cf. ADD §7)

Listes de contrôle

Chaque contrôle est identifié par un code unique (CC-xxx) et évalué selon les critères suivants :

Champ	Description
Métrique	Indicateur mesurable permettant d'évaluer le critère
Seuil	Valeur minimale ou maximale à respecter pour la conformité
Méthode	Procédure concrète pour vérifier le contrôle (test, revue, inspection)
Réf. ADD/BR	Section précise du document ADD ou du BR que le contrôle vérifie
Statut	✓ Conforme, ⚠ Partiel (justifié), ✗ Non conforme

Composants logiciels

N°	Critère de contrôle	Métrique / Indicateur	Seuil d'acceptation	Méthode de vérification	Réf. ADD / BR	Statut
CC-01	API REST documentée (Swagger)	Nombre d'endpoints documentés / total	100 % des endpoints PoC	Accéder à /swagger-ui et vérifier la couverture	ADD §6.1 (SpringDoc), BR — Exig. API	✓
CC-02	Séparation Controller / Service / Repository	Nombre de classes violant le pattern	0 violation	Revue de code : vérifier qu'aucun Controller n'accède directement au Repository	ADD §6.3 (Architecture en couches)	✓

CC-03	Mapping DTO / Entity systématique	Nombre d'entités exposées directement dans l'API	0 entité exposée	Revue de code : vérifier que chaque endpoint retourne un DTO, jamais une Entity	ADD §6.3 (Mapper)	✓
CC-04	Gestion centralisée des erreurs	Nombre d'exceptions non interceptées en production	0 exception non gérée	Test : envoyer des requêtes invalides, vérifier le format de réponse erreur {code, message}	ADD §6.3 (Exception)	✓
CC-05	Frontend modulaire (lazy loading)	Nombre de routes avec chargement paresseux	100 % des routes protégées	Inspecter app.routes.ts : vérifier loadComponent sur chaque route	ADD §6.1 (Angular)	✓
CC-06	WebSocket STOMP configuré	Présence de @EnableWebSocketMessageBroker	Configuration présente et active	Vérifier WebSocketConfig.java et la connexion ws:// depuis le navigateur	ADD §6.5 (WebSocket)	✓

Sécurité

N°	Critère de contrôle	Métrique / Indicateur	Seuil d'acceptation	Méthode de vérification	Réf. ADD / BR	Statut
CC-07	Authentification JWT fonctionnelle	Taux de réussite login avec identifiants valides	100 %	Test : POST /api/auth/login avec identifiants valides → token JWT reçu	ADD §6.4, BR-AUTH-02	✓
CC-08	Rejet des identifiants invalides	Taux de rejet des identifiants incorrects	100 %	Test : POST /api/auth/login avec mauvais MDP → 401 Unauthorized	ADD §6.4, BR-AUTH-02	✓
CC-09	Mots de passe hashés BCrypt	Nombre de mots de passe en clair en base	0	Requête SQL : SELECT password FROM users → vérifier préfixe $2a$	ADD §5.3 (users), RM-05	✓
CC-10	Protection CORS configurée	Présence de CorsConfigurationSource	Configuration active	Revue de SecurityConfig.java : vérifier origins, methods, headers autorisés	ADD §6.3 (Security)	✓
CC-11	Endpoints publics limités	Nombre d'endpoints sans authentification	≤ 5 (auth/*, chat, swagger)	Revue de SecurityConfig : lister les endpoints dans la whitelist	ADD §6.3 (Security)	✓
CC-12	Contrôle d'accès par rôle	Requêtes non autorisées bloquées	100 % bloquées	Test : accès endpoint employé avec token USER → 403 Forbidden	ADD §6.3, BR-AUTH-02	✓
CC-13	Validation comptes employés par admin	Connexion d'un employé non validé	Refusée	Test : login avec un compte EMPLOYEE au statut PENDING → rejet	ADD §4.1, BR-AUTH-01	✓

CC-14	Token JWT avec expiration	Durée de validité du token	≤ 24 h	Décoder un token JWT : vérifier le claim exp	ADD §6.4	✓

Tchat temps réel (PoC)

N°	Critère de contrôle	Métrique / Indicateur	Seuil d'acceptation	Méthode de vérification	Réf. ADD / BR	Statut
CC-15	Connexion WebSocket fonctionnelle	Taux de connexion réussie	100 % (réseau stable)	Test : ouvrir la console navigateur, vérifier le handshake ws://	ADD §6.5, BR-SUP-02	✓
CC-16	Messages reçus sans rechargement	Nombre de rechargements nécessaires	0 rechargement	Test : envoyer un message depuis client A, vérifier affichage chez client B sans F5	ADD §6.5, BR-SUP-02	✓
CC-17	Latence d'affichage des messages	Temps entre envoi et affichage chez le destinataire	< 2 secondes	Test chronométré : envoyer un message et mesurer le délai d'apparition	ADD §6.5, BR-SUP-02	✓
CC-18	Messages persistés en base	Nombre de messages perdus après fermeture de session	0 message perdu	Test : envoyer des messages, fermer le navigateur, rouvrir → messages présents	ADD §6.5, BR-SUP-01	✓
CC-19	Souscription par conversation	Isolation des topics entre conversations	100 % isolés	Test : ouvrir 2 conversations distinctes, vérifier qu'un message n'apparaît que dans la bonne	ADD §6.5	✓
CC-20	Authentification WebSocket par JWT	Connexion ws:// sans token	Refusée	Test : tenter une connexion WebSocket sans header Authorization → rejet	ADD §6.5, §6.4	✓

Gestion des données

N°	Critère de contrôle	Métrique / Indicateur	Seuil d'acceptation	Méthode de vérification	Réf. ADD / BR	Statut
CC-21	Conformité 3NF du schéma	Nombre de violations 3NF	0 violation	Revue du MPD (ADD §5.1) : vérifier 1NF, 2NF, 3NF pour chaque table	ADD §5.1 (3NF)	✓

CC-22	Intégrité référentielle (FK)	Nombre de FK définies vs attendues	100 % des relations couvertes	Requête SQL : \d+ rentals → vérifier les FOREIGN KEY constraints	ADD §5.2 (Relations)	✓
CC-23	Pas de données sensibles en clair	Nombre de champs sensibles non chiffrés	0	Revue BDD : vérifier password (BCrypt), tokens (hashés), pas de CB stockée	ADD §5.3, RM-05	✓
CC-24	Persistance Docker volumes	Données conservées après redémarrage conteneur	100 %	Test : docker-compose down puis up → vérifier que les données sont intactes	ADD §7.2 (Volumes)	✓
CC-25	Scripts SQL de création fournis	Présence de scripts DDL (CREATE TABLE)	Tous les scripts présents	Vérifier le dossier /sql ou le README : scripts de création + données initiales	ADD §5, BR — Exig. reproductibilité	✓

Infrastructure

N°	Critère de contrôle	Métrique / Indicateur	Seuil d'acceptation	Méthode de vérification	Réf. ADD / BR	Statut
CC-26	Docker Compose fonctionnel	Lancement en une commande	docker-compose up sans erreur	Test : cloner le repo, exécuter docker-compose up, vérifier les logs	ADD §7.2	✓
CC-27	Conteneur PostgreSQL accessible	Connexion au port 5432	Connexion réussie	Test : psql -h localhost -p 5432 -U postgres → connecté	ADD §7.2	✓
CC-28	Redémarrage automatique	Politique restart	restart: always	Revue docker-compose.yml : vérifier la directive restart pour chaque service	ADD §7.2	✓
CC-29	Configuration externalisée	Nombre de secrets en dur dans le code	0 secret en dur	Revue : vérifier application.yaml → ${ENV_VAR} pour JWT_SECRET, DB_PASSWORD, API keys	ADD §7.2	✓
CC-30	README d'exécution du PoC	Présence d'un README avec étapes de lancement	README complet et à jour	Vérifier : prérequis listés, commandes de lancement, ports utilisés, exemples	ADD §7	✓

Services et composants tiers

Ce tableau recense les services tiers utilisés et vérifie leur conformité en termes de licence et d'intégration.

Réf.	Service	Licence	Périmètre	Réf. ADD	Statut
CC-31	PostgreSQL 15	PostgreSQL License (libre)	PoC	ADD §5, §7.2	✓
CC-32	OpenAI API	Commercial (pay-per-use)	PoC	ADD §6.1	✓
CC-33	Spring Boot 4	Apache 2.0 (libre)	PoC	ADD §6.1	✓
CC-34	Stripe API	Commercial	Hors PoC	ADD §6.1, §8	✓
CC-35	OpenPDF	LGPL/MPL (libre)	Hors PoC	ADD §6.1	✓
CC-36	Spring Mail (SMTP)	Apache 2.0 (libre)	PoC	ADD §6.1	✓

Couverture fonctionnelle des exigences BR

Ce tableau vérifie que chaque exigence du Business Requirements est couverte par au moins un élément d'architecture dans l'ADD et un contrôle dans ce Compliance Assessment.

Réf. BR	Fonctionnalité	Couverture ADD	Contrôle(s) CC	Statut
BR-AUTH-01	Inscription	ADD §6.3 (AuthController), §6.4 (Security)	CC-09, CC-13	✓
BR-AUTH-02	Connexion JWT	ADD §6.4 (Flux JWT)	CC-07, CC-08, CC-14	✓
BR-AUTH-03	Déconnexion	ADD §6.4 (JWT stateless)	CC-07	✓
BR-SUP-01	Messagerie asynchrone	ADD §6.3 (ConversationCtrl), §5 (messages)	CC-01, CC-18	✓
BR-SUP-02	Tchat temps réel	ADD §6.5 (WebSocket STOMP)	CC-06, CC-15 à CC-20	✓
BR-SUP-03	Visioconférence	ADD §6.6 (WebRTC — V2)	—	⚠ V2
BR-SUP-04	Chatbot IA	ADD §6.1 (OpenAI API)	CC-32	✓
BR-PROF-01/02/03	Gestion du profil	ADD §4 (Acteurs), §5 (users)	—	Hors PoC
BR-LOC-01 à 07	Locations, paiement	ADD §5 (rentals, agencys), §6.1 (Stripe)	CC-34	Hors PoC
RM-01 à 07	Règles métier	ADD §3 (Principes), §8 (Traçabilité)	CC-02, CC-09	✓
BR — Exig. API	API REST documentée	ADD §6.1 (SpringDoc)	CC-01	✓

Synthèse de conformité

Le tableau ci-dessous récapitule le taux de conformité par catégorie de contrôle.

Catégorie	Conformes	Total	Taux
Composants logiciels (CC-01 à CC-06)	6	6	✓ 100 %
Sécurité (CC-07 à CC-14)	8	8	✓ 100 %
Tchat temps réel (CC-15 à CC-20)	6	6	✓ 100 %
Gestion des données (CC-21 à CC-25)	5	5	✓ 100 %
Infrastructure (CC-26 à CC-30)	5	5	✓ 100 %
Services tiers (CC-31 à CC-36)	6	6	✓ 100 %
CONFORMITÉ GLOBALE (PoC)	**36**	**36**	**✓ 100 %**

Note concernant BR-SUP-03 (Visioconférence) : cette exigence est documentée dans le BR et l'ADD (architecture WebRTC prévue) mais n'est pas implémentée dans le périmètre du PoC. Elle est planifiée pour la version 2 de l'application. Ce choix de périmètre est explicitement justifié dans le BR §3.2 (Périmètre du PoC).

Conclusion

L'ensemble des 36 contrôles définis dans ce document est conforme aux spécifications du Business Requirements et de l'Architecture Definition Document. Chaque contrôle dispose d'une métrique mesurable, d'un seuil d'acceptation quantifié et d'une méthode de vérification reproductible, permettant une évaluation objective de la conformité.

La traçabilité est assurée de bout en bout : chaque exigence du BR est couverte par au moins un élément d'architecture de l'ADD et un contrôle de ce Compliance Assessment. Les éléments hors périmètre du PoC sont clairement identifiés et justifiés.