BIG MFA V4

CONTRE-AUDIT FINAL — RAPPORT D'AUDIT SÉCURITÉ ET CONTRE-VALIDATION DE RELEASE

CANDIDATE FINALE VALIDÉE

Date du rapport :	13 août 2026	**Extension :**	Chrome Manifest V3 (v4.0.0)
Périmètre :	Artefact de production final REL/DATA-01	**Statut :**	VALIDÉE (avec dette Sonar documentée)
Package vérifié :	big-mfa-v4-production.zip (75 fichiers)	**SHA-256 :**	c1d1465c63b5387fd0169b3598c3df6fa3c53335c6812e39baadba43e4fed05a

Document de synthèse fondé sur les contrôles indépendants exécutés sur le bundle d'audit et sur l'artefact final de production.

1. Synthèse exécutive

Conclusion générale. Le contre-audit final de Big MFA v4 n'a mis en évidence aucune vulnérabilité exploitable confirmée dans le périmètre analysé. Les tests fonctionnels et de sécurité automatisés sont tous passés, les scanners SAST principaux n'ont remonté aucun finding de sécurité, et l'artefact publié correspond bit à bit au code de production audité. Le smoke test final sous Chrome est également validé.

Contrôle	Résultat	Statut
Tests automatisés	387/387	PASS
Couverture c8	87,49 % lignes/statements; 75,19% branches	PASS
ESLint	0 diagnostic	PASS
Semgrep auto	217 règles/66 cibles / 0 finding	PASS
Semgrep sécurité	99 règles/66 cibles / 0 finding	PASS
CodeQL security-extended	105 requêtes; 13/13 JS/TS; 0 résultat	PASS
SonarQube sécurité	0 vulnérabilité; 0 hotspot; Security A	PASS
SonarQube fiabilité	0 bug; Reliability A	PASS
Gitleaks	8 findings bruts; 0 secret réel après revue	PASS AVEC DISPOSITION

Contrôle	Résultat	Statut
Intégrité release	75/75 fichiers identiques bit à bit	PASS
Chrome smoke test	Validé	PASS
Quality Gate Sonar	ERROR: 96 new violations de maintenabilité	DETTE ACCEPTÉE

Réserve principale : SonarQube conserve 100 code smells ouverts, dont 96 dans la période de New Code. Ils relèvent de la maintenabilité et du style ; ils ne correspondent pas à 96 vulnérabilités. Le Quality Gate est rouge uniquement parce que la politique actuelle refuse toute nouvelle violation (>0).

2. Objet, périmètre et méthodologie

Le présent rapport retrace l'état initial audité, les anomalies identifiées, les corrections appliquées, le correctif REL/DATA-01, les contre-analyses indépendantes, les dispositions des faux positifs et la décision finale de release.

- **Périmètre de production :** extension Chrome Manifest V3 Big MFA v4, version 4.0.0.
- **Fonctions critiques couvertes :** TOTP/HOTP, coffre local chiffré, sauvegarde/restauration v3, import/export QR, Google Migration, internationalisation et parcours de déverrouillage.
- **Approche :** audit statique + tests automatisés + couverture + revue manuelle des alertes + intégrité d'artefact + smoke test Chrome.
- **Principe de décision :** ne pas confondre résultat scanner, défaut réel et dette de maintenabilité; chaque finding notable est contextualisé avant disposition.

3. État initial audité et corrections de release

Avant REL/DATA-01, le cycle de correction avait déjà traité plusieurs défauts ciblés sans modification des primitives cryptographiques ni du protocole de sauvegarde.

Réf.	Constat	Correction/disposition
`SEC-01`	Génération du batch_id Google Migration	Remplacement par Web Crypto; entier positif 31 bits.
`A11Y-01`	Contraste du bouton guide/PDF	Dégradé assombri; contraste renforcé sans modifier la couleur globale.
`REL-05`	Sélecteur de langue	Ajout d'un aria-label cohérent.
`HTML-01`	HTML invalide	Échappement de & dans le titre RGPD.
`BUG-I18N-01`	Message français codé en dur	Ajout de la clé `err_image_unreadable` dans les 50 langues.
`CATCH-950`	Validation mot de passe	Message spécifique pour mot de passe vide.
`CATCH-1670`	Création de coffre	Erreur inattendue rendue générique; pas d'exposition du message natif.
`CATCH-2830`	Décodeur rapide	Message traduit et générique en cas d'échec.
`CATCH-2956/3300`	QR/changement de mot de passe	

Réf.	Constat	Correction/disposition
		Messages d'échec génériques sans fuite de contenu sensible.
`PERF-CANVAS-01`	Lecture répétée Canvas2D	Ajout de `{ willReadFrequently: true }` ; warning Chrome supprimé.

4. Finding REL/DATA-01 - intégrité et corruption des données du coffre

Classification : Reliability / Data Integrity - sévérité Medium. Ce finding n'a pas été démontré comme une vulnérabilité de confidentialité ou de vol de secrets.

4.1 Comportement pré-correctif

Dans un chemin legacy, un `mfa_accounts` explicitement présent mais contenant un JSON invalide ou une valeur non-tableau pouvait être normalisé silencieusement vers un tableau vide. Cette tolérance pouvait masquer une corruption et créer un risque de perte de données lors d'opérations ultérieures.

4.2 Comportement requis et appliqué

- Un `mfa_accounts` absent reste accepté pour compatibilité historique.
- Un `mfa_accounts` égal à `[]` reste accepté comme coffre vide légitime.
- Un `mfa_accounts` présent mais JSON invalide ou non-tableau entraîne un refus de déverrouillage.
- Les clés de session `sessionKey`, `sessionSalt` et `sessionVaultHmacKey` sont annulées sur ce chemin d'erreur.
- Un message traduit de corruption est présenté; aucune persistance, re-signature ni entrée dans `showApp()` n'est autorisée.
- Le comportement du coffre moderne signé reste inchangé et la logique anti-bruteforce n'est pas affectée.

4.3 Validation automatisée de REL/DATA-01

1. Legacy + JSON invalide: unlock refusé, session nulle, aucune persistance.
2. Legacy + JSON valide non-tableau: même refus.
3. Compte vide `[]` : déverrouillage normal.
4. `mfa_accounts` absent: compatibilité historique préservée.
5. Coffre moderne valide: comportement inchangé.
6. Coffre moderne signé avec `mfa_accounts` corrompu: corruption détectée avant HMAC, sans re-signature.
7. Mauvais mot de passe: anti-bruteforce toujours déclenché.

> **Résultat :** 7/7 tests REL/DATA-01 passent.

5. Tests automatisés, lint et couverture

La suite finale contient 387 tests. Deux exécutions ont confirmé 387 pass, 0 fail, 0 cancelled, 0 skipped, 0 todo. Les messages JSDOM *« navigation not implemented »* proviennent du harness de test et n'ont pas provoqué d'échec.

Fichier	Statements %	Branches %	Functions %	Lines %
Global	**87,49**	**75,19**	**91,46**	**87,49**
`backup-v3.js`	94,06	76,97	100	94,06

Fichier	Statements %	Branches %	Functions %	Lines %
`crypto.js`	99,13	96,00	100	99,13
`guide.js`	97,10	61,11	100	97,10
`i18n.js`	99,73	91,30	100	99,73
`official-links.js`	100	100	100	100
`otpmigration.js`	98,44	79,46	100	98,44
`popup.js`	82,94	69,19	85,71	82,94
`totp.js`	100	85,88	100	100

Lint : ESLint sans diagnostic sur les 11 fichiers JavaScript de production ciblés.

Locales : 50 langues, 424 clés par langue, 0 erreur de validation. Les 506 warnings sont advisory (termes techniques, marques, placeholders ou alertes de longueur) et n'ont pas motivé de correction massive avant release.

6. Résultats des scanners de sécurité

Outil	Périmètre	Résultat brut	Disposition
npm audit	175 packages audités	0 vulnérabilité	PASS
Semgrep auto	217 règles/66 cibles / ~100% parsé	0 finding	PASS
Semgrep sécurité	99 règles/66 cibles/~100 % parsé	0 finding	PASS
CodeQL security-extended	105 requêtes; 13/13 JS/TS	0 résultat SARIF	PASS
SonarQube	32/32 sources JS/TS; TextAndSecrets 33/33	0 bug/0 vulnérabilité / 0 hotspot	PASS sécurité
Gitleaks production	~2,99 MB scannés	1 finding brut, non-secret	PASS après revue
Gitleaks tests	~340 KB scannés	7 findings bruts, vecteurs de test	PASS après revue

7. SonarQube - analyse détaillée et Quality Gate

SonarQube Community Build 26.7.0.124771, SonarScanner CLI 7.0.0.4796. Le scan final est techniquement réussi et le rapport a été traité par le serveur.

Métrique	Valeur	Lecture
Coverage globale	85,1%	OK
New coverage	85,0%	OK (seuil 80%)
Duplication globale	3,0%	Information
New duplication	1,644%	OK (seuil 3%)

Métrique	Valeur	Lecture
Bugs	0	OK
Vulnerabilities	0	OK
Security Hotspots	0	OK
Security rating	A (1,0)	OK
Reliability rating	A (1,0)	OK
Maintainability / sqale	A (1,0)	OK
Code smells ouverts	100	Dette de maintenabilité
New violations	96	**Quality Gate ERROR**

Conclusion Quality Gate : le statut ERROR provient uniquement de la condition `new_violations > 0` (96). La couverture et la duplication nouvelles passent leurs seuils. Aucune condition de sécurité ne fait échouer le gate.

7.1 Disposition des 100 code smells

Règle	Nombre	Nature
`S2486`	34	Catch / exception non traitée explicitement
`S6582`	19	Optional chaining
`S7758`	9	charCodeAt/fromCharCode -> codePointAt/fromCodePoint
`S3776`	8	Complexité cognitive
`S7761`	6	getAttribute -> dataset
`S7776`	6	Array -> Set
`S7786`	3	Error -> TypeError
`S7778`	3	push répétés
`S4138`	2	for -> for-of
Autres règles unitaires	10	Maintenabilité / lisibilité / accessibilité

La revue précédente des 96 violations de New Code avait conclu que 95 ne justifiaient pas de modification pré-release et qu'un seul cas représentait un risque réel de fiabilité/données : REL/DATA-01. Après correction, Sonar affiche 100 issues ouvertes au total, dont 96 nouvelles et 4 historiques. Les quatre issues historiques sont `crypto.js:43` (S7758), `crypto.js:136` (S2486), `crypto.js:206` (S2486) et `qrimport.js:21` (S2486).

Il serait incorrect de déclarer les 100 code smells comme « faux positifs ». La majorité sont des recommandations légitimes de maintenabilité ou de style, mais acceptées comme dette technique afin de ne pas introduire de régression tardive dans des fonctions critiques. Le cas HTML `AvoidCommentedOutCodeCheck` a été jugé non applicable/assimilable à un faux positif architectural.

7.2 Complexité cognitive - S3776

Zone	Fonction	Complexité	Décision
`backup-v3.js:192`	`validateBackupV3Envelope`	32	Validation stricte d'enveloppe cryptographique externe
`backup-v3.js:260`	`validateBackupV3Payload`	38	Validation stricte du payload/comptes
`otpmigration.js:111`	`parseMigrationPayload`	27	Parseur protobuf migration
`popup.js:1744 env.`	`unlockVault`	37 au scan final	Frontière sécurité / déverrouillage
`popup.js:2658 env.`	`refreshCodes`	21	Déchiffrement + TOTP/HOTP + UI
`popup.js:3447 env.`	`import handler`	22	Flux import
`popup.js:3625 env.`	`mergeImport`	22	Fusion import
`popup.js:3724 env.`	`restoreImport`	17	Restauration

Décision : pas de refactorisation opportuniste avant publication uniquement pour faire baisser Sonar; ces fonctions seront de meilleurs candidats à une campagne de dette technique post-release avec tests supplémentaires.

8. Gitleaks - findings bruts et dispositions

8.1 Production

Finding brut : `production/popup.js:1711` , règle `generic-api-key` , valeur `"azertyuiop12"`

Disposition : faux positif / donnée de politique de mot de passe. Cette valeur appartient à la liste de mots de passe faibles interdits. Elle n'est ni une clé API, ni un secret applicatif, ni un credential de production.

8.2 Tests

Sept findings bruts correspondent aux vecteurs OTP synthétiques/publics utilisés par les tests HOTP/TOTP/QR/backup, notamment les chaînes Base32 RFC de type `GEZDGNBV...` et `KRSXG5CTMVRXEZLU` .

Disposition finale Gitleaks : 8 findings bruts, 0 secret réel identifié après revue manuelle.

9. Intégrité, packaging et traçabilité de l'artefact

Archive	`big-mfa-v4-production.zip`
Taille	765 990 octets
SHA-256	`c1d1465c63b5387fd0169b3598c3df6fa3c53335c6812e39baadba43e4fed05a`
Fichiers réels	75
Entrées de dossiers	54
Entrées ZIP totales	129
Manifest	`manifest.json` présent à la racine

Vérification intégrité	75 identiques; 0 manquant; 0 supplémentaire; 0 différent

Preuve de correspondance : le script `verify:production` confirme que `production/` correspond bit à bit au ZIP publié, 75/75 fichiers.

10. Smoke test final Chrome

Le smoke test manuel final sous Chrome a été déclaré OK sur l'artefact candidat. Le warning Canvas2D observé précédemment lors des lectures répétées `getImageData` a disparu après PERF-CANVAS-01. Ce contrôle complète les tests JSDOM par une vérification dans l'environnement navigateur cible.

11. Risques résiduels et recommandations post-release

Sujet	Risque résiduel	Recommandation
Dette Sonar	100 code smells ouverts, dont 96 New Code.	Planifier une campagne dédiée sans pression de release ; conserver les tests comme garde-fous.
Complexité des frontières critiques	8 fonctions au-dessus du seuil cognitif.	Refactoriser progressivement avec tests de caractérisation et revue sécurité.
S2486	34 catches signalés.	Documenter explicitement les exceptions volontairement ignorées; traiter prioritairement celles sur chemins de persistance/import.
Locales	506 warnings advisory.	Faire une revue linguistique progressive, sans changement massif juste avant publication.
Gitleaks	Findings connus sur denylist et vecteurs de tests.	Conserver les dispositions documentées; éviter de masquer globalement les règles.
Quality Gate	Politique zéro nouvelle violation très stricte.	Conserver le gate ou ajuster sa politique de dette de manière gouvernée, sans l'assouplir uniquement pour rendre ce build vert.

12. Verdict final

CANDIDATE FINALE VALIDÉE POUR RELEASE

Aucune vulnérabilité exploitable confirmée dans le périmètre audité. Dette de maintenabilité Sonar documentée et acceptée, sans être requalifiée artificiellement en faux positifs.

Ce verdict repose sur la combinaison des éléments suivants : 387/387 tests, couverture élevée, lint propre, npm audit sans vulnérabilité, Semgrep et CodeQL sans finding, Sonar sans bug/vulnérabilité/hotspot, dispositions Gitleaks documentées, intégrité bit à bit du package et smoke test Chrome final réussi.

Limite de portée : aucun audit ne démontre l'absence absolue de vulnérabilité. Le verdict signifie qu'aucun défaut bloquant ou vulnérabilité exploitable n'a été confirmé par les contrôles effectués sur cette candidate de release.

Annexe A - Chronologie de contre-validation finale

Étape	Résultat
`npm ci`	174 packages ajoutés, 175 audités, 0 vulnérabilité.
Lint + locales	ESLint sans diagnostic; 50 langues x 424 clés ; 0 erreur.
Tests	387/387 pass.
Coverage	87,49 / 75,19 / 91,46 / 87,49.
Semgrep	217 règles auto + 99 règles sécurité; 0 finding.
CodeQL	105 requêtes; 13/13 fichiers JS/TS; SARIF 0 résultat; 103 définitions de règles.
SonarQube	0 bug, 0 vulnérabilité, 0 hotspot; A/A/A; 100 smells; gate ERROR sur 96 new violations.
Gitleaks	1 finding production + 7 tests; 0 secret réel après revue.
`verify:production`	75/75 bit à bit.
Chrome	Smoke test final OK.

Annexe B - Empreintes de release

Archive	SHA-256	Taille (octets)
`big-mfa-v4-production.zip`	`c1d1465c63b5387fd0169b3598c3df6fa3c53335c6812e39baadba43e4fed05a`	765 990
`big-mfa-v4-production-audit.zip`	`acb1be66fd820c18096862ef9e17ab9dd29f408fb3c1ae919eff57f4797cd4fd`	2 075 922
`big-mfa-v4-dev-complet.zip`	`716942930dbaa5dd5e3bf0d72f71cd3a7d0a0a7942c46a59fa6db45f8a528714`	2 054 950

Fin du rapport — Big MFA v4 — 13 août 2026