Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ordonnance sur la durée du travail et du repos des conducteurs professionnels de véhicules légers affectés au transport de personnes et de voitures de tourisme lourdes (OTR 2)

Modification du …

Le Conseil fédéral suisse
arrête :

I

L'ordonnance du 6 mai 1981 sur la durée du travail et du repos des conducteurs professionnels de véhicules légers affectés au transport de personnes et de voitures de tourisme lourdes[1] est modifiée comme suit :

Préambule
vu les art. 25, al. 2bis, 56, 103 et 106 de la loi fédérale du 19 décembre 1958 sur la circulation routière[2]

Art. 14, let. a^{bis}
Pour contrôler si la durée du travail, de la conduite et du repos a été observée (art. 5 à 12), il faut se fonder notamment :

a^{bis}. sur les données enregistrées dans l'application électronique (art. 16*b* à 16*g*) ;

Art. 16b Application électronique
L'application électronique permet de saisir, traiter, visualiser et transmettre des informations sur la durée du travail, de la conduite et du repos de conducteurs professionnels (données) au moyen d'un logiciel installé sur un terminal de données ou utilisé via un réseau de données.

RS .....
1 RS **822.222**
2 RS **741.01**

Art. 16c Exigences requises pour l'application électronique

[1] L'application électronique doit satisfaire aux exigences suivantes :

a. les données visées aux art. 16*g* et 18, al. 5 et 6, doivent pouvoir être saisies et validées électroniquement ;

b. le moment de la saisie des données doit être visible ;

c. toute modification de données saisies doit être visible et pouvoir être aisément retracée et vérifiée ;

d. les données doivent être automatiquement et immédiatement saisies et mémorisées après chaque entrée ;

e. les données saisies doivent être visibles immédiatement et consultables sans restriction et dans leur intégralité pendant 28 jours au moins ; passé ce délai, elles peuvent être supprimées ou écrasées ;

f. les données saisies doivent être accessibles aux autorités de contrôle :

1. sous la forme présentée à l'annexe 1, avec la possibilité pour lesdites autorités de sauvegarder les données sur place par des moyens standardisés,

2. en ligne via une URL unique, par exemple sous la forme d'un code QR ;

g. les données et leur transmission doivent être protégées contre les manipulations et contre tout accès non autorisé ;

h. l'application électronique doit être pourvue d'un numéro séquentiel permettant d'identifier clairement la copie installée pour le conducteur concerné ainsi que de l'élément d'identification du certificat.

[2] L'application électronique peut comporter des fonctions supplémentaires liées à la course, pour autant que le respect des exigences visées à l'al. 1 ne s'en trouve pas compromis.

Art. 16d Certification de l'application électronique

[1] L'application électronique doit être soumise pour examen et certification à un organisme de certification au sens de l'art. 16*e*. L'examen est effectué conformément à un schéma de certification basé sur les directives figurant à l'annexe 2, ch. 2. Si l'application remplit les exigences visées à l'art. 16*c*, son détenteur obtient un certificat (titulaire du certificat). Le certificat est délivré pour une durée maximale de cinq ans.

[2] Le titulaire du certificat doit :

a. soumettre à l'organisme de certification toute modification majeure des fonctions de l'application pour vérification et approbation ;

b. signaler chaque année à l'organisme de certification les évènements indiquant de possibles dysfonctionnements.

[3] À la demande du titulaire du certificat, ce dernier peut être prolongé à chaque fois de cinq années supplémentaires au maximum, pour autant que les exigences visées à l'art. 16*c* soient toujours remplies. L'organisme de certification réalise un audit à cet

effet. La demande de prolongation doit être déposée avant l'expiration de la validité du certificat.

4 Le tribunal civil statue en cas de litiges contractuels entre l'organisme de certification et le requérant ou le titulaire du certificat.

Art. 16e *Exigences relatives à l'organisme de certification*

L'application électronique ne peut être certifiée que par des organismes qui :

a. sont accrédités pour les domaines ci-après selon la norme ISO/CEI 17065, 2013, Évaluation de la conformité – Exigences pour les organismes certifiant les produits, les procédés et les services :
   1. cryptographie et communication sûre,
   2. protection des données,
   3. sécurité de l'application mobile, et
b. satisfont aux exigences visées à l'annexe 2.

Art. 16f Conditions d'utilisation de l'application électronique

1 Il est permis d'utiliser l'application électronique pour des véhicules dont le permis de circulation comporte une inscription au sens de l'art. 80, al. 2, de l'ordonnance du 27 octobre 1976 réglant l'admission à la circulation routière (OAC)[3] et qui ne sont pas équipés d'un tachygraphe.

2 Avant d'utiliser l'application électronique, le conducteur du véhicule doit communiquer à l'OFROU le numéro d'identification visé à l'art. 16*c*, al. 1, let. h. Un conducteur peut utiliser au maximum deux applications.

3 Le conducteur doit veiller à ce que le terminal de données :

a. soit toujours doté d'une protection à jour contre les manipulations et contre tout accès non autorisé ;
b. soit protégé efficacement contre toute charge mécanique et toujours suffisamment alimenté en énergie.

4 Sur demande, il aide les autorités de contrôle à accéder aux données.

Art. 16g Saisie de la durée du travail, de la conduite et du repos dans l'application électronique

1 Le conducteur doit saisir les données selon l'art. 18, al. 5 et 6, et vérifier les éventuelles entrées automatiques. Il doit fournir les indications de manière suivie. Celles-ci ne doivent pas nécessairement être graphiques.

2 Si le conducteur professionnel effectue une course privée avec le véhicule, il doit indiquer celle-ci comme telle dans l'application électronique avant le départ. Il doit saisir le début, la fin et le kilométrage de la course privée.

3 RS **741.51**

3 Si des tiers effectuent une course privée avec le véhicule, le conducteur professionnel doit saisir, avant sa prochaine course professionnelle, la différence de kilométrage qui en a résulté et ajouter la mention « autre conducteur » dans l'application électronique.

4 Le conducteur doit mettre à la disposition de son employeur les données de l'application électronique relatives à la durée du travail, de la conduite et du repos au plus tard le premier jour de travail de la semaine suivante.

Art. 19, al. 7

7 Il est possible de renoncer à remplir le livret de travail lorsque la durée du travail, de la conduite et du repos est saisie au moyen d'une application électronique.

Art. 21, al. 1, phrase introductive, et 2

1 À l'aide des moyens disponibles, tels que les disques et les jeux de disques hebdomadaires du tachygraphe, les données enregistrées dans l'application électronique, les feuilles hebdomadaires et quotidiennes du livret de travail et, s'il y a lieu, les rapports journaliers à l'usage de l'entreprise ou les cartes de contrôle (art. 19, al. 1, et 25, al. 4), l'employeur s'assurera de manière constante que les dispositions sur la durée du travail, de la conduite et du repos (art. 5 à 12) sont observées. À cet effet, il inscrira, pour chaque conducteur, les indications suivantes dans un registre :

2 Pour les salariés dont la durée quotidienne de la conduite est manifestement inférieure à 7 heures d'après un contrôle sommaire des moyens de contrôle visés à l'art. 14, let. a et a^{bis}, il n'est pas nécessaire d'inscrire dans le registre la durée de la conduite ; il suffit d'inclure celle-ci dans la durée totale du travail quotidien (al. 1, let. b).

Art. 22, al. 3 à 5

3 Il doit mettre à la disposition du conducteur le livret de travail ainsi que les clefs et disques nécessaires à l'utilisation du tachygraphe ou l'application électronique. Le cas échéant, le conducteur doit annoncer le plus vite possible à son employeur toute défectuosité du tachygraphe ou de l'application électronique.

4 L'employeur doit établir une liste comprenant les noms des conducteurs, leur adresse et leur année de naissance ainsi que les numéros de leurs livrets de travail.

5 Il doit veiller à ce que les données personnelles des conducteurs qu'il traite dans le cadre de l'exécution de la présente ordonnance soient utilisées uniquement aux fins de celle-ci et protégées contre tout accès non autorisé.

Art. 23, al. 3, phrase introductive et let. b^{bis}

3 Ils conserveront pendant deux ans, au siège de l'entreprise :

b^{bis}. les données enregistrées dans l'application électronique (art. 16*f* et 16*g*) ;

Art. 28, al. 2, let. d, e et f

2 Sera puni de l'amende quiconque enfreint les dispositions sur le contrôle (art. 15 à 23), notamment quiconque :

d. ne saisit pas ou ne saisit pas correctement, dans l'application électronique, les données prescrites ;

e. manipule le système global (application électronique, terminal de données et données mémorisées de façon centralisée) de telle sorte que celui-ci fournisse des données erronées ;

f. utilise des applications électroniques non certifiées.

Art. 32, al. 1bis

1bis Il actualise les annexes.

II

La présente ordonnance est complétée par les annexes 1 et 2 ci-jointes.

III

La présente ordonnance entre en vigueur le …

… Au nom du Conseil fédéral suisse :

La présidente de la Confédération, Karin Keller-Sutter
Le chancelier de la Confédération, Viktor Rossi

Annexe 1
(art. 16*c*, al. 1, let. e)

Formulaires pour la saisie de la durée du travail, de la conduite et du repos

1. Généralités

Les formulaires ci-après (1.1 à 1.4), qui comportent les indications requises selon l'art. 18, al. 5 et 6, sont obligatoires.

1.1 Feuille quotidienne pour salariés

Champ	**Inscription**
Prénom, nom	
Début du travail	
Date	
Numéro de la plaque de contrôle	
Kilométrage (initial)	
Durée du repos précédant l'entrée en service	
Déroulement chronologique/Activités (début et fin du travail) (Durées du travail, de la conduite, pauses, courses privées)	

Fin du travail	
Kilométrage (final)	
Nombre de kilomètres parcourus durant la journée	
Nombre de kilomètres parcourus dans le cadre de courses privées	
Kilométrage total (courses privées incluses)	
Durée totale par activité	Durée de la conduite :
	Durée du travail :
	Pause :
Remarques	
Signature	

(Annexe 1.2)

1.2 Feuille hebdomadaire pour salariés

Prénom, nom								
Semaine								
Dernier jour de repos hebdomadaire								
Jour de la semaine	**LU**	**MA**	**ME**	**JE**	**VE**	**SA**	**DI**	**Total hebdomadaire**
Plaque de contrôle								
Durée du repos précédant le début en h et min.								
Début du travail								
Fin du travail								
Durée de la conduite en h et min.	.							
Durée du travail en h et min.		.						
Pauses en h et min.								
Somme de la durée du travail et de la durée de la conduite en h et min.								
Jour de repos hebdomadaire								
Demi-jour de congé hebdomadaire								
Remarques								

(Annexe 1.3)

1.3 Feuille quotidienne pour conducteurs indépendants

Champ	Inscription
Prénom, nom	
Date	
Numéro de la plaque de contrôle	
Kilométrage (initial)	
Durée du repos précédant l'entrée en service en h et min.	
Déroulement chronologique/Activités (début et fin de la conduite)	
Kilométrage (final)	
Nombre de kilomètres parcourus durant la journée	
Durée totale de la conduite en h et min.	
Remarques	
Signature	

(Annexe 1.4)

1.4 Feuille hebdomadaire pour conducteurs indépendants

Prénom, nom								
Semaine								
Dernier jour de repos hebdomadaire								
Jour de la semaine	**LU**	**MA**	**ME**	**JE**	**VE**	**SA**	**DI**	**Total hebdomadaire**
Plaque de contrôle							-	
Durée du repos précédant le début en h et min.								
Début de l'activité professionnelle							-	
Fin de l'activité professionnelle							-	
Durée de la conduite en h et min.								
Jour de repos hebdomadaire								
Demi-jour de congé hebdomadaire								
Remarques								

Annexe 2
(Art. 16*d,* al. 1 et 16*e*)

Exigences relatives aux organismes de certification

1. Généralités

1.1 Organisme de certification

Tout organisme de certification est tenu :

- de travailler en toute impartialité et d'éviter les conflits d'intérêts ;
- de garantir la confidentialité des informations propriétaires, du code source et de la documentation de sécurité ;
- d'appliquer le schéma de certification de façon cohérente ;
- de consigner les évaluations et décisions.

1.2 Schéma de certification

Pour examiner la conformité des applications électroniques avec les exigences visées à l'art. 16*c*, al. 1 et 2, l'organisme de certification élabore un schéma de certification en tenant compte des directives formulées au ch. 2.

Il veille à cet égard à garantir la conformité avec les exigences de la présente ordonnance et avec les normes internationales pertinentes (par ex. SN EN ISO/CEI 15408, 2023, Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information [*Common Criteria*] ; SN EN ISO/CEI 62443-4-1, 2018, et 62443-4-2, 2019, Sécurité des systèmes d'automatisation et de commande industriels ; SN EN ISO/CEI 27034, 2023, *Information technology – Security techniques – Application security* ; NF EN ETSI 303645, 2024, CYBER – Cybersécurité pour l'Internet des objets grand public : exigences de base[4] ; *Mobile Application Security Verification Standard* [MASVS] de l'*Open Worldwide Application Security Project* [OWASP])[5].

Il gère et actualise le schéma de certification au besoin.

2. Directives concernant le schéma de certification

2.1 Champ d'application et principes des directives

Le schéma de certification vaut pour les applications mobiles et leurs services connexes qui sont utilisés pour vérifier le respect des exigences prescrites par la présente ordonnance.

[4] Les normes peuvent être consultées gratuitement et achetées auprès de l'Association Suisse de Normalisation (SNV), Sulzerallee 70, 8404 Winterthour ; www.snv.ch (en partie en anglais seulement).
[5] Consultable à l'adresse suivante : https://mas.owasp.org > MASVS (version 2.1.0).

Les exigences techniques découlent des objectifs et exigences des *Common Criteria*, des exigences de la présente ordonnance et du MASVS (OWASP).

2.2 Planification des activités

Les différentes phases doivent être planifiées et convenues par l'organisme de certification en accord avec le requérant.

2.3 Examen des artefacts de sécurité pertinents

Tous les artefacts de sécurité déployés par l'application (par ex. procédures, modèles, instruments et rapports de test utilisés durant le développement de l'application) doivent être soumis à un examen théorique.

Le tableau 1 « Exigences de sécurité » dresse la liste des principaux artefacts de sécurité à examiner, sur la base de prescriptions et standards actuels pour les applications mobiles. Quatre niveaux d'évaluation sont définis.

Abréviation	Description
BE	Examen de base. L'élément est contrôlé par simple lecture. L'objectif est de saisir le texte dans les grandes lignes et de le comprendre. Questions que devrait se poser l'examinateur : que dit le texte ? Quelles informations puis-je tirer de ce dernier ?
CE	Examen critique. L'élément est contrôlé moyennant une lecture critique. L'objectif est d'apprécier le fonctionnement du texte et d'analyser, interpréter et évaluer ce dernier. Questions que devrait se poser l'examinateur : comment fonctionne le texte ? Comment l'argumentation est-elle construite ? Sur quelles hypothèses le texte repose-t-il ? Que signifie-il ?
SE	Examen par échantillonnage. L'élément est composé de plusieurs documents ou paragraphes, dont certains sont contrôlés à l'aide d'une procédure d'échantillonnage systématique. L'étendue de la vérification pour les éléments sélectionnés correspond à celle de l'examen critique. Les critères de sélection reposent sur le principe suivant : la priorité est donnée aux documents ayant une incidence majeure sur la sécurité.
NE	Aucun examen. L'élément n'est pas contrôlé.

Tableau 1 : Exigences de sécurité

Le tableau 2 « Objectifs de sécurité » définit les objectifs et contrôles de sécurité obligatoires pour les applications mobiles selon le MASVS (OWASP) et les *Common Criteria*. Lesdits objectifs servent de base pour les audits et doivent être examinés dans leur intégralité.

Domaine	Exigence principale	PP[6]	MASVS (OWASP)

6 *Protection Profile for Application Software :* profil de protection pour application de la NIAP (*National Information Assurance Partnership*)

Cryptographie	Cryptage, gestion des clés, protocoles sûrs	FCS[7]	CRYPTO
Protection des données	Cryptage de données au repos, contrôle des accès, communication	FDP[8]	STORAGE, NETWORK
Configuration et gestion	Configuration sûre, gestion des fonctions critiques	FMT[9]	PLATFORM, ARCH
Anti-exploitation	ASLR, DEP, canaries de pile (*stack canaries*), numéro d'identification du logiciel (*software ID*), mises à jour	FPT[10]	RESILIENCE, ARCH
Canaux fiables	Protection des données pendant la transmission	FTP[11]	NETWORK
Protection des données	Consentement de l'utilisateur pour la transmission de PII	FPR[12]	PRIVACY
Détection du débridage (*rooting/jailbreaking*)	Reconnaissance par l'application d'un environnement compromis	N/A[13]	RESILIENCE-1, -2

Tableau 2 : Objectifs de sécurité

Les *Common Criteria* ou le MASVS de l'OWASP peuvent servir de base pour des exigences d'examen et de test spécifiques.

2.4 Examen des processus de soutien – Niveau 1

Les artefacts doivent être reproductibles. À cet effet, des processus de soutien doivent être définis dans le système de gestion du requérant, lesquels doivent faire l'objet d'un examen théorique visant à en contrôler l'exhaustivité et l'exactitude.

Document à examiner	Première vérification / Surveillance de modifications majeures	Surveillance de modifications mineures
Manuel sur la gestion de la cybersécurité	CE	BE
	BE si ISO27001	BE
Manuel sur la gestion des comptes	CE	BE
		BE
Rapport sur l'architecture	CE	BE

7 *Functional Class Cryptographic Support* : prise en charge cryptographique
8 *Functional Class User Data Protection* : protection des données d'utilisateur
9 *Functional Class Security Management* : gestion de la sécurité
10 *Functional Class Protection of the TSF (TOE Security Functions)* : protection des fonctions de sécurité de l'objet à tester
11 *Functional Class Trusted Path/Channels* : chemin/canaux sécurisés
12 *Functional Class Privacy* : protection des données / sphère privée
13 *Not applicable* : sans objet

Rapport sur les audits de sécurité	SE	BE
Manuel sur la gestion des configurations	CE	BE
Manuel sur la gestion des évènements	SE	BE
Manuel sur les processus d'intervention en cas d'incident	SE	BE
Manuel sur la maintenance et la gestion des correctifs	SE	BE
Rapport sur la protection contre les logiciels malveillants	SE	BE
Rapport sur l'accès à distance	CE	BE
Manuel sur la sécurisation dès la conception	CE	BE
Manuel sur la sécurité de l'implémentation	CE	BE
Manuel sur les processus des tests de sécurité	CE	BE
Manuel sur les mises à jour de sécurité	CE	BE
Rapport sur la cybersécurité SIS[14]	CE	BE
Analyse de la communication sans fil	SE	BE

Tableau 3 : Vérification des processus

2.5 Tests – Niveau 2

L'organisme de certification peut choisir entre trois approches :

- réalisation de ses propres tests ;
- utilisation d'un rapport de test externe ;
- observation de tests.

La dernière approche peut être combinée avec la deuxième si la réputation du prestataire de test externe ne peut être garantie.

2.5.1 Observation de tests

En l'absence d'exigences claires concernant les tests dans les standards disponibles, il faut suivre l'approche définie dans le présent schéma, laquelle couvre des fonctions de sécurité techniques. Les tests effectués dans les laboratoires ad hoc du requérant doivent être observés selon les statuts décrits ci-dessous. Pour ces tests, il est possible de tenir compte des résultats de l'examen des artefacts de sécurité pertinents.

Les tests ci-après peuvent être réalisés :

a. les tests P (*Performed by the customer and witness based on sampling*), qui sont effectués par le requérant ; l'organisme de certification en observe une partie par échantillonnage ;

[14] *Secure Internet Service* : service Internet sécurisé

b. les tests PW (*Performed and fully Witness*), qui sont validés par une observation.

Tests	Première vérification / Surveillance de modifications majeures	Surveillance de modifications mineures
Tests d'authentification (connexion, séances, …)	PW	P
Tests d'autorisation (droits d'accès, éléments non fiables, …)	PW	P
Tests de journalisation (notifications, alarme, enregistrement des évènements)	PW	PW
Tests de la robustesse de la communication (intégrité, conformité avec les protocoles)	PW	PW
Tests d'interface (injection de données, test à données aléatoires, validation des entrées)	PW	P
Tests de disponibilité (tests de résistance)	PW	P
Tests d'intrusion	PW	P

Tableau 4 : Stratégie d'observation des tests

2.5.2 Examen des spécifications et instruments de test

Avant toute observation de tests, le plan des tests, les spécifications et des informations caractéristiques concernant les instruments et processus de test du requérant doivent être présentés au responsable de l'audit. Sont évalués :

a. la couverture de test ;
b. l'efficacité des tests ;
c. la qualité de la documentation des tests ;
d. l'adéquation des instruments de test ;
e. les preuves de validation des instruments de test ;
f. la compétence du personnel ;
g. les processus d'entreprise.

2.5.3 Durant l'observation de tests

Le responsable de l'audit doit :

a. observer la session de tests et la perturber le moins possible, ayant demandé tous les renseignements et clarifications nécessaires avant le début des tests ;
b. vérifier si les tests sont effectués conformément aux procédures convenues, au plan ad hoc et aux spécifications de test ;
c. contrôler que les tests sont réalisés par les examinateurs désignés dans le plan ;

d. prendre note des instruments utilisés et de leurs versions, et les comparer avec ceux définis dans les spécifications.

Le responsable de l'audit a l'interdiction :

a. de participer activement aux activités de test ou d'assumer un rôle ou une fonction qui devrait incomber au personnel du requérant ;

b. de formuler des avis ou des propositions et de répondre à des questions ;

c. d'influencer de quelque manière que ce soit le processus de test, le laboratoire ou les résultats.

Le responsable de l'audit peut interrompre le test à tout moment si une grave non-conformité qui invaliderait les résultats du test est constatée. Dans ce cas, il en informe immédiatement le requérant.

2.5.4 Résultats de l'observation de tests

Le responsable de l'audit doit établir un rapport comportant au minimum les indications suivantes :

a. date, heure, lieu ;

b. personnel impliqué et rôles de celui-ci ;

c. objectif et contexte des tests ;

d. version des scénarios de test appliqués ;

e. écarts entre les résultats attendus et les résultats obtenus ;

f. évaluation des résultats par des tiers.

2.6 Audit – Niveau 3

Il est nécessaire d'évaluer l'efficacité et la pertinence des artefacts et des processus, et de confirmer l'appréciation des partenaires concernés. À cet effet, un audit formel, ciblé sur les éléments ci-après, est réalisé après l'examen préliminaire des artefacts de sécurité et des processus y relatifs :

- examen des fonctions de sécurité de l'objet examiné ;
- évaluation du niveau d'implémentation et de maturité des processus de soutien.

L'audit peut porter notamment sur les thèmes suivants :

- organisation de la sécurité et compétences ;
- processus d'amélioration continu ;
- audits internes de cybersécurité ;
- cycle de vie ;
- système de la gestion de la qualité ;
- gestion des configurations ;
- gestion des modifications ;

- analyse d'impact ;
- examen et vérification ;
- structure de la documentation et modèles ;
- gestion des fournisseurs ;
- processus de développement ultérieur (par ex. surveillance des produits, gestion des vulnérabilités).

2.7 Examen – Recommandation de certification

Sur la base des résultats des étapes 2.3 à 2.6, le responsable de l'audit vérifie si toutes les exigences requises pour une certification sont remplies.

2.8 Décision de certification

En se fondant sur l'examen fait par le responsable de l'audit, un comité indépendant doit examiner la recommandation de certification. Il statue ensuite sur la délivrance du certificat.

2.9 Attestation, licence

L'organisme de certification octroie au requérant le droit d'utiliser une marque de certification. Il peut réutiliser une marque existante à cet effet.

2.10. Surveillance

Les audits de cybersécurité doivent être garantis. À cet effet, l'application certifiée pour des applications mobiles doit être constamment actualisée et l'organisme de certification doit mener des activités de surveillance tous les 12 mois au moins à compter de la décision de certification. Les activités de surveillance doivent comprendre au minimum les éléments suivants :

- surveillance des incidents : preuve que le requérant surveille son application et traite les incidents de manière adaptée ;
- gestion des modifications : modalités d'exécution des mises à jour et manière de garantir la sécurité de ces dernières ;

  audit : entretiens avec les partenaires concernés au sujet de la gestion des modifications et de l'amélioration continue.

Toutes les modifications apportées au produit ou aux processus de soutien doivent être systématiquement catégorisées sur la base de leur incidence sur les objectifs de sécurité et le niveau de confiance. Les modifications sont réputées mineures ou majeures :

- modifications mineures : modifications qui n'influent pas sur la fonctionnalité centrale, le modèle de menaces ou la conformité (par ex. mises à jour superficielles, optimisations de performance, améliorations de la documentation) ; en général, elles nécessitent seulement des mises à jour de la documentation ou une vérification limitée ;

- modifications majeures : modifications qui concernent les fonctions de sécurité, l'architecture ou le profil de risque (par ex. nouvelles fonctions, mises à jour importantes de mécanismes cryptographiques, modifications de la menace) ; elles nécessitent une évaluation approfondie et éventuellement une nouvelle certification (partielle).

L'organisme de certification est responsable de la classification de toutes les modifications et de l'adoption du niveau d'évaluation adéquat.

2.11 Suspension

La validité d'un certificat peut être suspendue temporairement, en particulier dans les cas suivants :

- la surveillance révèle une non-conformité qui ne nécessite pas de retrait immédiat ;
- l'utilisation inadéquate du certificat ou de la marque n'a pas été corrigée par des mesures adaptées ;
- d'autres infractions au schéma de certification ou aux procédures de l'organisme de certification ont été commises.

La suspension est communiquée au requérant par écrit. Durant celle-ci, l'application peut rester enregistrée.

2.12 Retrait

Le certificat est retiré dans les cas suivants :

- la surveillance révèle une grave non-conformité ;
- une violation de la convention passée entre le requérant et l'organisme de certification a été commise ;
- aucune mesure adaptée n'a été prise après une suspension ;
- le requérant ne souhaite pas prolonger le certificat ;
- le requérant ne peut ou ne veut pas satisfaire aux nouvelles exigences découlant de l'évolution de standards ou règles ;
- le produit n'est plus fabriqué ou le requérant cesse son activité.

Le retrait est communiqué par écrit. Le titulaire du certificat doit en informer tous les clients dans un délai de dix jours au maximum à compter de la notification, et leur signaler qu'ils ne sont plus autorisés à utiliser l'application.

3. Modification des exigences relatives aux produits

En cas de modification des exigences relatives aux produits, l'organisme de certification doit informer sans délai le requérant par écrit de leur entrée en vigueur ainsi que de l'éventuelle nécessité d'un examen complémentaire.