**Présentation du protocole**

**Gestion des malfaçons**

**et des règles de gestion**

**Version 1.0**

|  |  |  |  |
| --- | --- | --- | --- |
| SUIVI DES VERSIONS | | | |
| Version | Date | Nom du rédacteur | Nature de la modification |
| 0.1 | 20/04/2022 | C. Gerard | Création |
| 0.2 | 05/07/2022 | C. Gerard | Enrichissement des règles de gestion |
| 0.3 | 14/09/2022 | Atelier ad-hoc | Relecture du document – clarification des cas d’usage |
| 0.4 | 20/09/2022 | Orange | Rajout de la description d’une API TMF |

Table des matières

[**1.** Introduction 4](#_Toc113986289)

[1.1. Objet du document 4](#_Toc113986290)

[1.2. Lexique 4](#_Toc113986291)

[1.3. Document de référence applicable 5](#_Toc113986292)

[1.4. Contexte 5](#_Toc113986293)

[1.5. Processus 5](#_Toc113986294)

[**2.** Généralités sur la solution technique 6](#_Toc113986295)

[2.1. Proposition globale 6](#_Toc113986296)

[2.2. Détails API 6](#_Toc113986297)

[2.3. Architecture 6](#_Toc113986298)

[2.4. Protocoles et sécurité 7](#_Toc113986299)

[**3.** Règles de gestion 8](#_Toc113986300)

[3.1. API Malfaçon 8](#_Toc113986301)

[3.2. API Ticketing 8](#_Toc113986302)

[3.2.1. Criticité 8](#_Toc113986303)

[3.2.2. Cycle de vie des tickets 8](#_Toc113986304)

[3.2.3. Codes erreurs 9](#_Toc113986305)

[3.2.4. Cas de gestion 10](#_Toc113986306)

[3.2.5. Dépôt 11](#_Toc113986307)

Introduction

## Objet du document

Ce document est le descriptif de la version 1.0 de l’outil normalisé défini par le Groupe Interop’fibre pour la déclaration d’une malfaçon par l’opérateur d’infrastructure à l’opérateur commercial.

## Lexique

| **Sigle ou concept** | **Signification** |
| --- | --- |
| OI | Opérateur d’immeuble : Toute personne chargée de l’établissement ou de la gestion d’une ou plusieurs lignes dans un immeuble bâti, notamment dans le cadre d’une convention d’installation, d’entretien, de remplacement ou de gestion des lignes signée avec le propriétaire ou le syndicat de copropriétaires, en application de l’article L. 33-6 du code des postes et des communications électroniques ; l’opérateur d’immeuble n’est pas nécessairement un opérateur au sens de l’article L. 33-1 du même code |
| OC | Opérateur commercial : Opérateur choisi par le client final pour la fourniture d'un service de télécommunications ou par un fournisseur d’accès au service pour la fourniture d’un service de télécommunications à son propre client final |
| Malfaçon | Une malfaçon est une non-conformité issue de travaux menés dans le cadre d'une prestation de production ou de SAV sur un accès (PM/PBO/PTO), confiée à un intervenant selon un cahier des charges (STAS et règles de l'art) |

## Documents de référence applicables

| **Nom du Document** | **Description** |
| --- | --- |
| Documentation GitHub | <https://github.com/before-interop/malfacon> |
| Document de cadrage (Atelier A4) |  |

## Contexte

Cet outil permet la déclaration et le traitement d’une malfaçon grâce à des flux normalisés.

## Processus

Les travaux inter-opérateurs ont permis de définir des typologies de malfaçons sur le périmètre suivant :

1. La signalisation de malfaçons peut être faite par un OI vers OC comme par un OC vers un OI
2. Certaines malfaçons sont détectables aussi bien par un OI que par un OC, d’autres sont vues comme détectables uniquement par un OI ou uniquement par un OC
3. La signalisation de malfaçon par un OI vers un OC est une notification appelant action de la part de l’OC destinataire ou informant ce dernier d’une malfaçon n’appelant pas action de sa part.

Cette notification suppose que l’OC pourra intervenir pour traiter la malfaçon : si les conditions font que c’est impossible et plus particulièrement sur un PM devenu inexploitable, alors l’OI doit procéder par une Remise En Conformité (REC)

Si l’OC constate lors de son intervention que l’état du PM ne lui permet pas de traiter la malfaçon, alors il aura la possibilité de le signaler en retour à l’OI.

1. La signalisation de malfaçon par un OC vers un OI est une remontée d’information qui n’implique pas d’engagement de l’OC sur son niveau de précision : cette signalisation constitue une information complémentaire pour l’OI dans le cadre de l’exploitation de son réseau.
2. De par sa définition, la Malfaçon se distingue de la notion de « Dysfonctionnement » dont est ici rappelée la définition Interop’Fibre :

« *Un dysfonctionnement est une problématique qui rend impossible l’adduction du réseau d’un OC au PM mis à disposition par un OI* »

1. A noter que les notions de « Dommages », qui peuvent apparaître dans les contrats des OI, ne sont pas normalisées. Dans tous les cas, il est important que ces définitions contractuelles ne viennent pas recouvrir le périmètre de la **Malfaçon**.

Généralités sur la solution technique

## Proposition globale

La proposition comprend trois API :

* **Malfaçon** qui permet de :
  + typer les malfaçons selon un zonage à savoir que chaque malfaçon se définit par rapport à une « localisation » et un « détail de localisation »
  + différencier les objets envoyés par l'OC (POST), de ceux pouvant être récupérés par l'API (GET)
* **Attachment** : qui permet l'upload/download simple de fichiers et le référencement de ces fichiers dans d'autres APIs
* **Ticketing** : inspiré du TMF (pruning et adaptation avec ajout de champs notamment), qui décrit comment déposer un ticket, ainsi que son cycle de vie.
* **API TMF**:



## Détails API

Les séquences d’appels et les modèles de données des API sont indiquées via le lien [https://github.com/before-interop/malfacon](https://github.com/before-interop/malfacons)

## Architecture

Le tableau suivant montre les couches techniques intervenant dans l’interface des services FTTH :

|  |  |
| --- | --- |
|  | **SERVEUR** |
|  | API REST format d’échange JSON |
|  | http |
|  | SSL |
|  | TCP/IP |

Le SWAGGER de l’API est conforme à l’Interop et téléchargeable depuis GitHub dont le lien sera indiqué sur le site Interop fibre.

## Protocoles et sécurité

Les différentes API sont des webservices de type API utilisant « REST » et HTTPS (HTTP et SSL) comme protocoles applicatifs.

Le traitement de la sécurité des échanges est défini par les échanges bilatéraux entre l’OC et l’OI.

# Règles de gestion

## API Malfaçon

L’API Malfaçon contient les données de référence nécessaires pour créer une malfaçon.

Process liant les données de l’API Malfaçon et l’API Ticketing :

1. Création de la malfaçon chez l’OI (id, hrefMF)
2. Création d’un TT OI qui va faire référence à la malfaçon créée (relatedEntity malfaçon)
3. Création TT OC de type malfaçon
4. Corrélation entre TT OI et TT OC
5. Pour avoir le détail de la malfaçon, une interrogation de l’API Malfaçons est nécessaire

## API Ticketing

### Criticité



### Cycle de vie des tickets

Revue du cycle de vie des tickets

* **acknowledged** : Syntaxe validée et prise en compte du ticket par l’OI

Un délai indicatif sera donné à l’OC à l’état acknowledged qui pourra augmenter ou réduire à l’état inProgress.

* **rejected :** ticket rejeté : Le passage de acknowledged à rejected se fera suite à un contrôle machine.
* **inProgress** : Qualification du ticket par OI

Afin de permettre à l’OC de relancer l’OI (ex : si le client final vient d’emménager dans son logement, délai dépassé, …), une note sera rajoutée dans l’état inProgress. Un changement de sévérité par l’OC sera également possible à l’état inProgress.

* **pending** (gel du ticket) : Demande de pièces complémentaires à l’OC. A noter que l’OI aura la possibilité d’annuler le ticket s’il reste trop longtemps dans l’état pending sous un délai à discrétion de chaque OI.
* **held** pour permettre à l’OI d’afficher une information à l’OC avec un gel interne OI
* **resolved :** ticket résolu
* **cancelled :** ticket annulé par l’OC
* **closed :** ticket clôturé

Utilisation de l’attribut statutChangeReason pour décrire la raison d’un KO et/ou d’un changement d’état

Possibilité pour l’OC de modifier le statut du ticket sur les cas :

* pending -> InProgress
* InProgress -> rejected : demande de rejet du ticket faite par l’OC (motif à indiquer)
* pending -> rejected : demande de rejet du ticket faite par l’OC (motif à indiquer)
* resolved -> InProgress permet à l’OI de refuser la résolution.

A l’état « resolved », une clôture automatique du ticket pourra être faite par l’OC (si l’OI n’a pas accepté ou refusé la résolution) après avoir laissé un délai raisonnable de prise en charge du ticket par l’OI.

### Codes erreurs

* Codes erreurs génériques :

|  |  |  |
| --- | --- | --- |
|  | **CODE** | **LIBELLE** |
| **SYNTAXE (code http 400)** |  | INFORMATIONS MANQUANTES (champs obligatoires non renseignés)  ERREUR SYNTAXIQUE |
| **TRAITEMENT (code http 422)** | 101 | ANNULATION OI |
| 102 | ANNULATION OC |
| 103 | ANNULATION TIERS |
| 104 | ANNULATION INTERDITE |

* Codes erreurs spécifiques – Malfaçon :

Motifs REJECTED (OC > OI) : refus de la part de l'OC de reprendre la malfaçon

|  |  |  |
| --- | --- | --- |
|  | CODE | LIBELLE |
| **TRAITEMENT** |  | PM critique |
|  |  | Tiers erroné / non concerné |
|  |  | Manque d’information |
|  |  | Commande mise en service depuis plus d’un an (OI reprend directement la malfaçon sans actionner l’OC) |

Motifs WAITING (OC > OI) OK pour reprise par l’OC, mais manque d'infos à fournir par l’OI

|  |  |  |
| --- | --- | --- |
|  | CODE | LIBELLE |
| **TRAITEMENT** |  | Photo non exploitable (flou mal cadré) |
|  | Photo qui n'illustre pas le problème (ex : photo de poignée au lieu d'une jarretière) |
|  | Confusion entre identification du PM et PM déclaré |
|  | Mauvaise géolocalisation du site |
|  | Demande non conforme aux STAS |
|  | Reprise impossible en l’état (Intervention préalable de l’OI nécessaire) + commentaire obligatoire : (possibilité de découper selon les cas génériques rencontrés : sécurité/sanitaire/environnement/accès/autres…) |

### Cas de gestion

Les cas de gestion identifiés sont les suivants :

* cas nominal : déclaration d'une malfaçon par l'OI à l'OC concerné et reprise par l'OC selon les dispositions contractuelles. Quand la reprise est effectuée, l'OC passe le ticket en résolu avec en PJ n photos (à discrétion de l’OC) de la reprise pour permettre à l'OI de valider la résolution.
* cas d'une malfaçon critique avec reprise par OI : quand la reprise est effectuée, l'OI clôt le ticket avec en PJ une photo de la reprise critique pour information de l'OC
* cas d'une malfaçon critique avec reprise par OC : process cas nominal
* cas d'une malfaçon imputable avec reprise par OI suite au dépassement du délai contractuel : quand le délai contractuel est dépassé, le changement de responsabilité du ticket est fait par l'OI. Quand la reprise est effectuée, l'OI clôt le ticket avec en PJ une photo de la reprise critique pour information de l'OC.

Précision : L’OI peut redéclencher l’OC (passage du ticket à InProgress) sur une même malfaçon en cas de contrôle de résolution KO tant que le délai de reprise contractuel n’est pas dépassé. En cas de dépassement de ce délai contractuel, c'est l'OI qui reprend la malfaçon avec un transfert de responsabilité du ticket.

* cas d'une malfaçon non imputable : 1 ticket est envoyé à chaque OC présent sur l’infrastructure concernée puis process malfaçon critique avec reprise par OI
* cas du rejet par l’OI de la reprise de la malfaçon faite par l’OC
* cas de demande d’information complémentaire à l’OC pour permettre à l’OI de valider la résolution
* cas de demande d’information complémentaire à l’OI à la réception du ticket malfaçon

Les diagrammes de séquence associés sont publiés sur GitHub.

Précisions :

* Si une coupure est nécessaire pour la reprise de la malfaçon, un TP sera ouvert par l’OI.
* Pendant le temps de traitement sur un élément réseau, l’OI n’enverra pas de nouveau ticket sur une malfaçon donnée pour un OC donné.

### Dépôt

* Création unitaire des TT pour une typologie de malfaçon : 1 ticket = 1 typologie de malfaçon
* si besoin, solution de regroupement asynchrone des différents tickets concernés via "TroubleTicketRelationship"