

Spécifications relatives aux destinataires finaux

Directives pour la norme en matière de prestations (KLE)

Swissdec, 6002 Lucerne

www.swissdec.ch

Directives pour la norme en matière de prestations
Spécifications relatives aux destinataires finaux

Les Directives relatives aux destinataires finaux pour la transmission de données dans la norme en matière de prestations (KLE) ont été élaborées en collaboration par:

- la Suva,
- l'Association suisse d'assurances.

Éditeur

Swissdec
Fluhmattstrasse 1
Case postale 4358
6002 Lucerne
www.swissdec.ch

Table des matières

1	Introduction	6
1.1	Tests	6
1.2	Abréviations	6
1.3	Processus de transmission des données d'événement	7
2	Aperçu des cas d'utilisation.....	8
2.1	Explications des cas d'utilisation.....	10
2.2	Cas d'utilisation et opérations y relatives	10
2.3	Résumé des cas d'utilisation.....	10
2.3.1	UC001 Recevoir une déclaration d'événement.....	10
2.3.2	UC002 Recevoir une synchronisation d'événement.....	10
2.3.3	UC003 Vérifier la joignabilité.....	10
2.3.4	UC004 Appliquer la sécurité	10
2.3.5	UC005 Appliquer une fenêtre de maintenance	11
2.3.6	UC006 Données de test reçues	11
2.3.7	UC007 Traiter les duplicatas.....	11
2.3.8	UC008 Régler les flux de données	11
2.3.9	UC009 Traiter une demande de support.....	11
3	Description des cas d'utilisation	12
3.1	UC001 Recevoir une déclaration d'événement.....	12
3.2	UC002 Recevoir la synchronisation d'événement.....	14
3.3	UC003 Vérifier la joignabilité.....	16
3.4	UC004 Appliquer la sécurité	16
3.5	UC005 Activer une fenêtre de maintenance	17
3.6	UC006 Données de test reçues	17
3.7	UC007 Traiter des duplicatas.....	18
3.7.1	Déclarer des duplicatas.....	18
3.7.2	Déclarer un duplicata sans détection par le distributeur.....	18
3.7.3	Synchroniser des duplicatas	18
3.7.4	Synchronisation d'un historique identique.....	18
3.7.5	Synchronise StoryID non unique à l'intérieur de l'IncidentContext.....	18
3.8	UC008 Régler les flux de données	20
3.9	UC009 Traiter une demande de support.....	21
4	Exigences supplémentaires	22
4.1	Version de la norme suisse en matières de prestations.....	22
4.2	Normes de communication	22
4.3	Compression en option	22
4.4	Disponibilité.....	22
4.4.1	Périodes définies.....	23
4.4.2	Plages de valeurs définies	23
4.5	Extensibilité.....	23
4.6	Modifications à l'interface.....	24
4.7	Support et temps de réaction	24
4.8	Performance / Débit utile.....	25
4.9	Sécurité et protection des données.....	26
4.10	Adressage et filtrage	26
5	Annexe	27
5.1	Documents de spécifications également applicables	27

Liste des illustrations

<i>Figure 1: Declare et Synchronize dans la norme en matière de prestations, diagramme BPMN Diagramm et interfaces.....</i>	<i>7</i>
<i>Figure 2: Cas d'utilisation – Aperçu de la déclaration d'événement</i>	<i>8</i>
<i>Figure 3: Cas d'utilisation - Aperçu de la synchronisation d'événement.....</i>	<i>8</i>
<i>Figure 4: Cas d'utilisation - Aperçu de la configuration et du support.....</i>	<i>9</i>
<i>Figure 5: Document d'instance pour destinataire final et indications des temps</i>	<i>25</i>

Aperçu des modifications

Directives pour la transmission de données d'événement - Spécifications relatives aux destinataires finaux, version ID-CH 1.0, édition todo 2017mmjj du jj.mm.aaaa.

Chapitre	Modification
----------	--------------

Première version de la norme suisse en matière de prestations	
---	--

Conventions utilisées dans ce document

Les graphies suivantes sont utilisées dans ce document:

Texte	Documentation
Texte	Code
<Texte>	Élément XML
[TEXTE]	Référence à un autre document

L'aspect contraignant des spécifications est défini comme suit:

Aspect contraignant	Mot
Obligation	<i>doit obligatoirement</i>
Souhait	<i>devrait</i>
Intention	<i>sera</i>
Proposition	<i>peut</i>

Tableau 1: Aspect contraignant des spécifications

Attention:

Des schémas relativement anciens suffisent souvent pour la compréhension des concepts, mais **seuls les fichiers XML officiels¹ sont contraignants.**

Les expressions spéciales sont expliquées dans le glossaire du document (RL-IDCH, 2017).

¹ www.swissdec.ch

1 Introduction

Le présent document contient les spécifications fonctionnelles et autres pour les destinataires finaux qui sont utilisés dans le cadre de la norme suisse en matière de prestations. Il traite les aspects techniques de la norme en matière de prestations et non pas les aspects logiques spécifiques à la branche (aspects métier). Un destinataire final est utilisé pour recevoir les annonces d'événement qui ont été envoyées par voie électronique à partir du système ERP d'une entreprise.

Une vue d'ensemble de la procédure normalisée est utile pour la compréhension des spécifications ci-après. Pour acquérir cette vue d'ensemble, nous renvoyons le lecteur au document «IncidentStandardOverview.pdf» (OV-IDCH, 2018).

Les dispositions des documents figurant en annexe doivent également être observées. Des aspects essentiels pour le destinataire final sont déjà décrits notamment dans les chapitres traitant des domaines de numérisation et des aspects techniques de la norme dans les directives spécifiques (RL-IDCH, 2017).

1.1 Tests

Les tests de la réception se rapportent aux cas d'utilisation et aux spécifications supplémentaires. Ils peuvent être téléchargés sur le site de Swissdec (RCTS-IDCH, 2018). Associés aux spécifications, ils contribuent à la compréhension générale du système à réaliser. Ils seront de préférence pris en compte déjà pendant le développement par le fabricant.

1.2 Abréviations

Les abréviations suivantes sont utilisées pour les opérations WSDL:

- **Declare:**
DeclareIncident
DeclareIncidentConsumer
- **Synchronize:**
SynchronizeIncident
SynchronizeIncidentConsumer

1.3 Processus de transmission des données d'événement

La transmission des données d'événement s'effectue de manière séparée dans la déclaration et dans la synchronisation périodique.

1. Déclaration de l'événement avec données initiales (Declare) et référence à l'InsuranceCaseID
2. Complément de l'événement déclaré par des données sous la forme d'«historiques» et réception simultanée de résultats, d'un statut modifié, etc. (Synchronize).

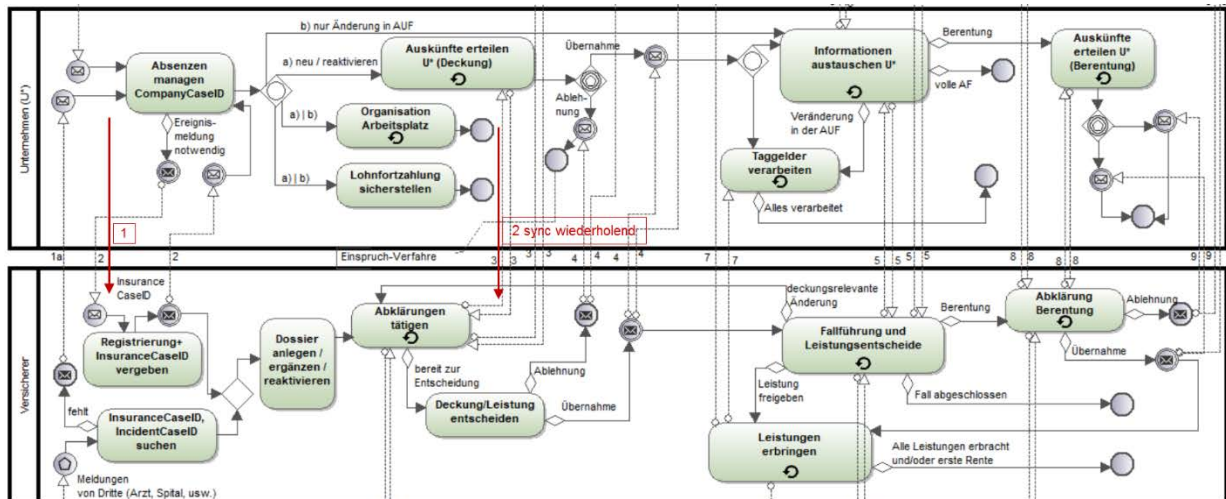


Figure 1: Declare et Synchronize dans la norme en matière de prestations, diagramme BPMN et interfaces

2 Aperçu des cas d'utilisation

Dans les cas d'utilisation ci-après sont décrites les spécifications techniques essentielles pour le destinataire final. Ils doivent être lus avec les documents (RL-IDCH, 2017), (ACKNSwissdec, 2018), (DIAL-IDCH, 2018), (WSDL-IDCH, 2018) et (SEC-ERSwissdec, 2018) ainsi que vérifiés par les tests mentionnés dans (RCTS-IDCH, 2018).

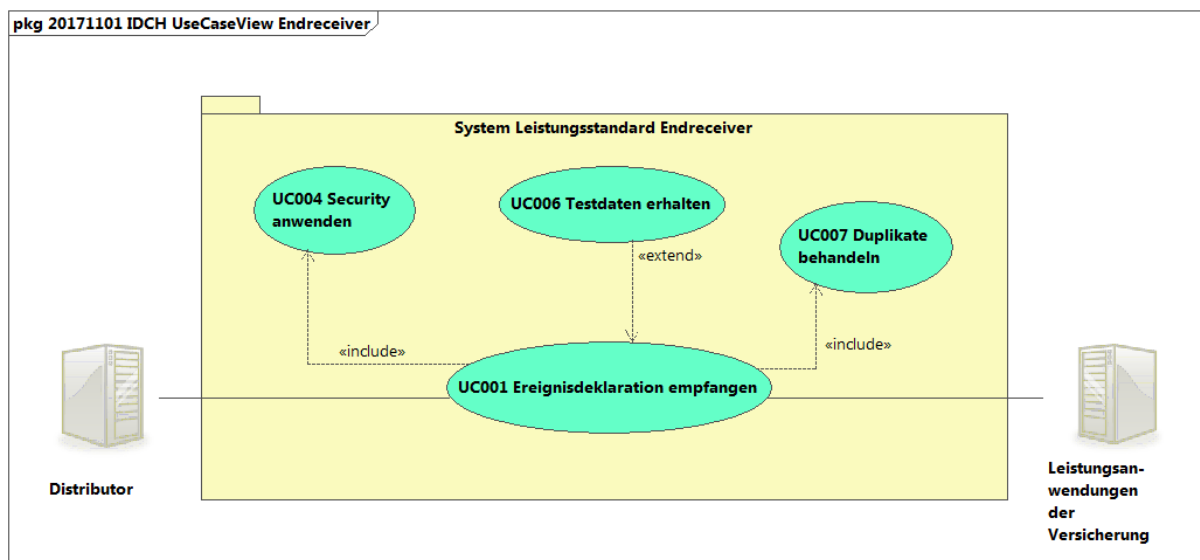


Figure 2: Cas d'utilisation – Aperçu de la déclaration d'événement

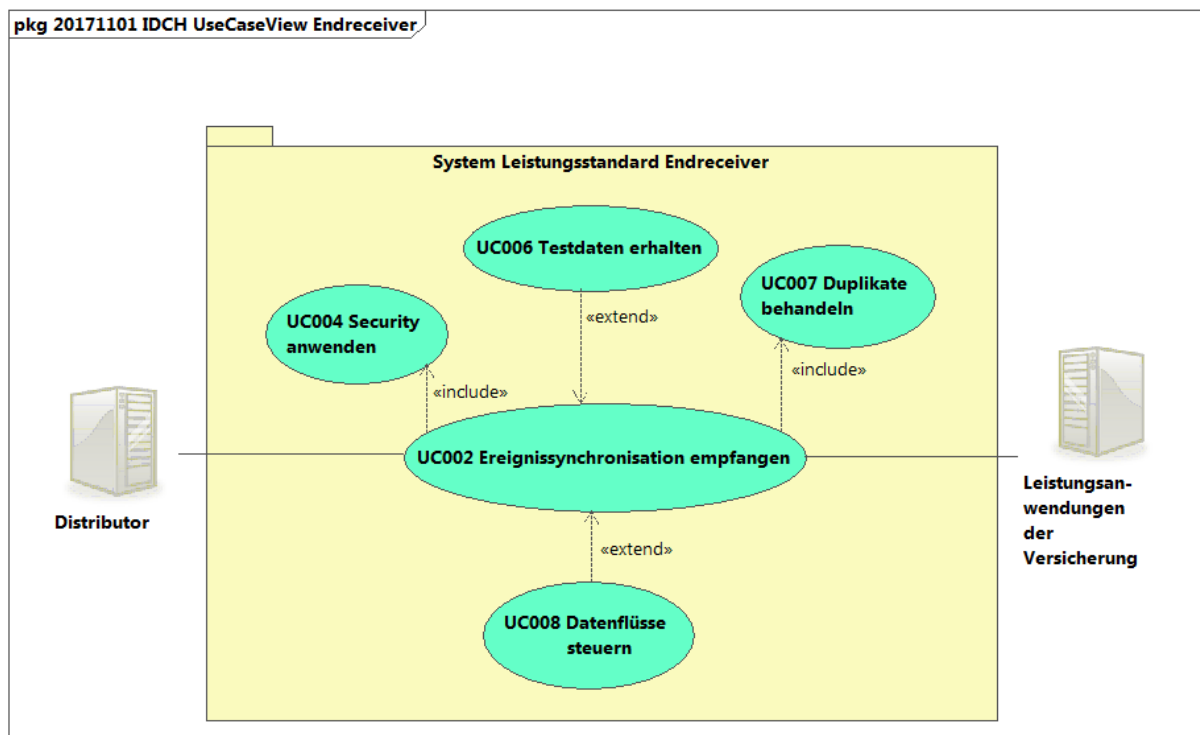


Figure 3: Cas d'utilisation - Aperçu de la synchronisation d'événement

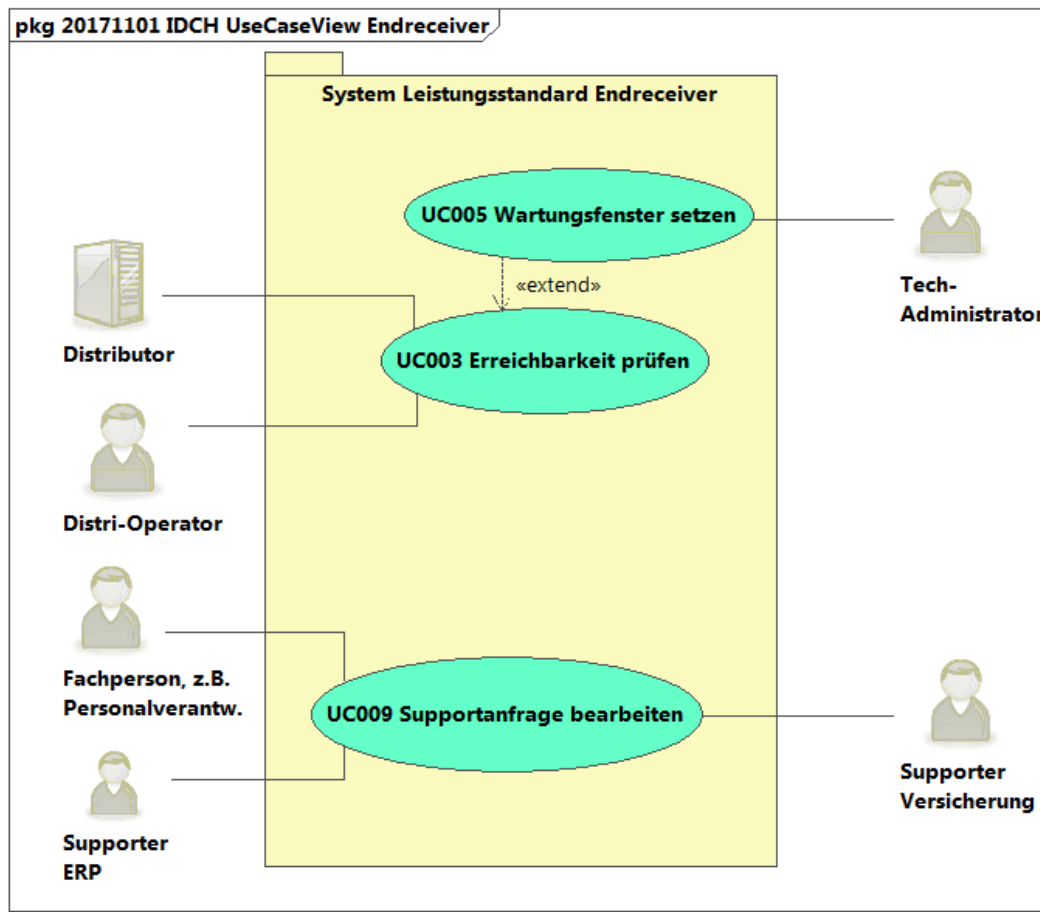


Figure 4: Cas d'utilisation - Aperçu de la configuration et du support

Les acteurs peuvent être subdivisés en trois groupes:

- Opérateur, administrateur [groupe technique]
- Spécialistes, responsables du personnel, y c. fiduciaire [groupe spécialisé]
- Collaborateurs du support [mélange du groupe technique et du groupe spécialisé]

La provenance des acteurs peut être décrite de la manière suivante:

- Opérateur de distribution: technicien au niveau du distributeur
- Spécialiste: utilisateur final dans l'entreprise
- Collaborateur du support: au choix collaborateur du support de l'entreprise ou du fabricant du système ERP, spécialiste du service du support chez le destinataire final
- Administrateur technique: technicien au niveau du destinataire final

2.1 Explications des cas d'utilisation

Les spécifications représentées sous la forme de cas d'utilisation se réfèrent à la partie technique d'un système de traitement des prestations qui reçoit des données d'événement, quittance les annonces, communique avec le système d'une entreprise et pilote le traitement des événements.

Les exigences métier, qui se rapportent au traitement des données après leur transmission, etc. ne font pas partie des présentes spécifications.

Un système de traitement des prestations avec récepteur **doit obligatoirement**, pour la réception à l'intérieur d'un domaine de numérisation (RL-IDCH, 2017), toujours remplir toutes les exigences système envers ce domaine. Concernant les cas d'utilisation non pris en charge, pour d'autres domaines de numérisation, un message d'erreur spécifié dans le document (ACKNSwissdec, 2018) est renvoyé.

2.2 Cas d'utilisation et opérations y relatives

Le modèle sous-jacent est un système client-serveur, avec le destinataire final comme serveur et le distributeur comme client. Sont utilisées les normes XML WSDL et schéma XML. Les opérations et les éléments mentionnés ci-après se trouvent dans le fichier WSDL (WSDL-IDCH, 2018) y relatif ainsi que dans les schémas correspondants. La procédure et le protocole sont expliqués dans le document (OV-IDCH, 2018).

Tous les appels du transmetteur en direction du distributeur puis du destinataire final sont synchrones. Pour traiter de grands volumes de données, le nombre des historiques à transmettre (RL-IDCH, 2017) au sein d'une requête peut être réglé (UC008 «Régler les flux de données»).

Cas d'utilisation	Opération / Élément
UC001 Recevoir une déclaration d'événement	<ul style="list-style-type: none">▪ DeclareIncidentConsumer▪ DeclareIncidentConsumerResponse▪ IncidentDeclarationConsumerFault
UC002 Recevoir le résultat d'une synchronisation d'événement	<ul style="list-style-type: none">▪ SynchronizeIncidentConsumer▪ SynchronizeIncidentConsumerResponse▪ IncidentDeclarationConsumerFault
UC003 Vérifier la joignabilité	<ul style="list-style-type: none">▪ PingConsumer▪ PingConsumerResponse

Tableau 2 Cas d'utilisation et opérations

2.3 Résumé des cas d'utilisation

2.3.1 UC001 Recevoir une déclaration d'événement

Une déclaration d'événement est envoyée du distributeur à un destinataire final, puis est vérifiée et traitée par celui-ci. La réponse du destinataire final contient les données nécessaires pour la suite du traitement de l'événement dans le processus de prestations.

2.3.2 UC002 Recevoir une synchronisation d'événement

Une synchronisation d'événement est envoyée par le distributeur à un destinataire final. Ce dernier traite les historiques et les quittances reçus du transmetteur. Ce faisant, il procède à un contrôle des transactions. Si nécessaire, il règle activement le flux des données.

2.3.3 UC003 Vérifier la joignabilité

Il s'agit là d'un message déclenché cycliquement, qui vérifie, à intervalles réguliers, la disponibilité du destinataire final et, le cas échéant, les fenêtres de maintenance activées.

2.3.4 UC004 Appliquer la sécurité

Le destinataire final vérifie les certificats reçus et décrypte le message. En direction du distributeur, il signe et crypte la réponse. La sécurité est décrite dans le document (SEC-ERSwissdec, 2018).

2.3.5 UC005 Appliquer une fenêtre de maintenance

En complément à UC003 «Vérifier la joignabilité», une fenêtre de maintenance doit pouvoir être inscrite dans la réponse au distributeur.

2.3.6 UC006 Données de test reçues

Un message de test correspond à un message comme pour UC001 ou UC002, mais certains événements y sont marqués comme résultats de test. Ces résultats ne doivent pas être traités productivement. Dans la réponse, les résultats de test doivent eux aussi être marqués comme cas de test.

2.3.7 UC007 Traiter les duplicatas

Des duplicatas d'une requête complète sont caractérisés par le distributeur. Si les informations contenues dans le duplicata n'ont pas encore été traitées et sont encore sans réponse, cela doit être rattrapé. D'autres duplicatas doivent pouvoir être reconnus et traités tant lors de la fonction Declare que lors de la fonction Synchronize.

2.3.8 UC008 Régler les flux de données

Le volume de données des réponses au distributeur est réduit par la répartition en plusieurs cycles requête-réponse. La taille maximale d'une requête est définie d'après les «meilleures pratiques actuelles» (RL-IDCH, 2017) 11.2.

2.3.9 UC009 Traiter une demande de support

Afin de pouvoir traiter une demande de support, la personne compétente chez l'assureur doit avoir la possibilité d'accéder à l'annonce d'événement correspondante ainsi qu'aux fichiers journaux qui y sont associés.

3 Description des cas d'utilisation

3.1 UC001 Recevoir une déclaration d'événement

Description succincte	Le distributeur envoie la déclaration d'événement de l'entreprise au destinataire final. La déclaration d'événement contient peu de détails sur l'événement lui-même (WSDL-IDCH, 2018). Elle est vérifiée et traitée par le destinataire final. La réponse de celui-ci contient, entre autres, l'InsuranceCaseID attribuée par l'assurance pour cet événement, l'IncidentCaseID octroyée par le distributeur et la CompanyCaseID donnée par l'entreprise, cf. (RL-IDCH, 2017) «Système d'identification».
Acteurs	Distributeur
Déclencheur	Le distributeur a reçu une déclaration d'événement d'un transmetteur.
Conditions préalables	Le distributeur a validé la déclaration d'événement et l'a plausibilisée selon le document (ACKNSwissdec, 2018).
Conditions ultérieures	Le destinataire final a sauvegardé les données de déclaration et les a renvoyées au distributeur, InsuranceCaseID comprise.
Cas d'utilisation inclus	UC004 Appliquer la sécurité, UC007 Traiter les duplicatas
Déroulement standard	<ol style="list-style-type: none"> 1. Les données de la déclaration d'événement sont reçues. 2. Les données de transport du distributeur doivent être vérifiées conformément au couplage de celui-ci. La sécurité est contrôlée, UC004. Les doublons² sont détectés, UC007. Les anomalies dans la déclaration d'événement peuvent être contrôlées. 3. La déclaration d'événement est vérifiée conformément à la norme suisse en matière de prestations (acceptation). 4. Toutes les données requises de la déclaration d'événement sont sauvegardées conformément aux principes de la protection des données. 5. Une InsuranceCaseID est attribuée pour l'événement. 6. La réponse au distributeur ou à l'entreprise est construite conformément à la norme suisse en matière de prestations / (ACKNSwissdec, 2018), message déjà établi par le distributeur inclus <ProducerResponseNotifications> (ACKNSwissdec, 2018). Dès la présence d'au moins un avertissement, un code acceptedWithWarning <i>doit obligatoirement</i> être renvoyé (.. /ResponseState/Code). La réponse <i>doit obligatoirement</i> contenir l'indication du domaine de numérisation du destinataire, voir (RL-IDCH, 2017), chapitre sur les domaines de numérisation.
Déroulements alternatifs	<p>{ Étape 4: les données de test sont marquées en tant que telles d'après UC006 et ne sont pas traitées productivement}</p> <p>{ Étape 1: fenêtre de maintenance / service non disponible}</p> <p>L'information relative à la fenêtre de maintenance (de-à) a déjà été transmise par UC003 «Vérifier la joignabilité» au distributeur. Pendant ce temps, les messages de réponse contenant cette information sous interruption sont renvoyés directement du distributeur au système ERP demandeur.</p> <p>{ Étape 1: interruption non planifiée / service non disponible}</p> <p>Pendant ce temps, les messages d'erreur du distributeur sont renvoyés directement au système ERP demandeur, voir le document (ACKNSwissdec, 2018).</p> <p>{ Étape 2: un doublon a été détecté, procédure selon UC007 «Traiter des duplicatas»}</p>

² Toutes les données sont transmises aussi pour les doublons

	<p>{ Étape 2: sécurité non valable, rejet du message}</p> <p>{ Étape 3: un événement est déclaré et une InsuranceCaseID a déjà été octroyée}</p> <p>Nous avons ici un cas spécial (LAA, LAAC, IJM). Implémentation selon (RL-IDCH, 2017), chapitre 3 sur les explications concernant le processus nominal.</p>
Liste des erreurs	<p>Erreur:</p> <ul style="list-style-type: none">▪ le message n'est pas valide d'après (WSDL-IDCH, 2018)▪ le message ne peut pas être décrypté▪ etc. <p>voir (ACKNSwissdec, 2018)</p>

3.2 UC002 Recevoir la synchronisation d'événement

Description succincte	<p>Des historiques (RL-IDCH, 2017) et des quittances sont reçus du distributeur; dans la réponse, des historiques, des quittances et des états sont renvoyés au distributeur.</p> <p>Un contrôle de transaction est exécuté.</p> <p>Le cas échéant, le flux des données est réglé activement.</p>
Acteurs	Distributeur
Déclencheur	Le transmetteur a envoyé une synchronisation d'événement au distributeur. Cela peut avoir diverses raisons spécifiques, telles que la livraison d'historiques manquants dans le processus de prestations ou une demande si de nouvelles données sont disponibles.
Conditions préalables	<p>Le distributeur a validé la synchronisation d'événement et l'a plausibilisé selon le document (ACKNSwissdec, 2018).</p> <p>Déroulement standard: une déclaration d'événement a été transmise et quittancée préalablement.</p>
Conditions ultérieures	<p>Les historiques reçus du transmetteur sont sauvegardés conformément aux principes de la protection des données.</p> <p>Une synchronisation sans IncidentStories est enregistrée p. ex. dans un Access Log, avec CustomerIdentity.</p> <p>Les historiques du destinataire final déjà livrés et auxquels appartiennent les quittances reçues sont marqués comme quittancés.</p> <p>Le statut actuel du processus et le statut actuel de reprise de l'événement ont été renvoyés dans la réponse, voir (RL-IDCH, 2017), chapitre 7.</p> <p>Le cas échéant, des quittances pour les historiques de transmetteur transmis sont livrées dans la réponse à l'entreprise.</p> <p>Le cas échéant, les historiques de transmetteur encore manquants sont demandés dans la réponse.</p> <p>Le cas échéant, les historiques de destinataire final déjà mis à disposition pour la prise en charge sont livrés dans la réponse à l'entreprise (RL-IDCH, 2017) «Comportement SynchronizeIncident Request et Response».</p> <p>Le cas échéant, d'autres historiques de destinataire final déjà prêts à la prise en charge sont listés dans la réponse à l'entreprise.</p> <p>Le cas échéant, les éléments <Error>, <Warning> ou <Info> contenus dans certains historiques reçus sont sauvegardés.</p>
Cas d'utilisation inclus	UC004 Appliquer la sécurité, UC007 Traiter des duplicatas
Déroulement standard	<ol style="list-style-type: none"> 1. Les données de la synchronisation d'événement sont reçues. 2. Les données de transport du distributeur supplémentaires sont vérifiées conformément au couplage du distributeur (SEC-ERSwissdec, 2018). La sécurité est vérifiée, UC004. Les doublons³ sont détectés, UC007. 3. La synchronisation d'événement est vérifiée conformément à la norme suisse en matière de prestations (acceptation). 4. Toutes les données nécessaires de la synchronisation d'événement, notamment les nouveaux historiques, sont sauvegardées conformément aux principes de la protection des données. 5. Le contrôle de transaction est effectué (RL-IDCH, 2017), chapitre 11. Les historiques de transmetteur reçus sont quittancés dans la réponse. Pour les quit-

³ Toutes les données sont transmises pour les doublons également

	<p>tances reçues, les historiques du destinataire final correspondants sont recherchés et marqués comme quittancés. Les historiques de transmetteur manquants sont demandés. Les historiques du destinataire final, les quittances et les annonces d'état non encore envoyés sont intégrés dans la réponse (RL-IDCH, 2017) «Comportement SynchronizeIncident Request et Response».</p> <p>6. Si nécessaire, le flux des données est réglé activement - UC008 «Régler les flux de données».</p> <p>7. (La réponse au distributeur ou à l'entreprise est construite conformément à la norme suisse en matière de prestations / (ACKNSwissdec, 2018) message déjà établi par le distributeur inclus <ProducerResponseNotifications> (ACKNSwissdec, 2018). Dès la présence d'au moins un avertissement, un code <code>acceptedWithWarning</code> doit <i>obligatoirement</i> être renvoyé (.. /ResponseState/Code). La réponse <i>doit obligatoirement</i> contenir l'indication du domaine de numérisation du destinataire, voir (RL-IDCH, 2017), chapitre sur les domaines de numérisation.)</p>
Déroulements alternatifs	<p>{ Étape 4: les données de test sont marquées en tant que telles d'après UC006 et ne sont pas traitées productivement}</p> <p>{ Étape 3: l'événement ne peut pas être identifié à l'aide des données reçues, car aucune InsuranceCaseID n'a été envoyée. Simultanément, un élément «StoriesWithoutDeclaration» existe dans la requête}</p> <p>Cela est un cas spécial d'«annonce d'événement manquante» (RL-IDCH, 2017), chapitre sur les cas spéciaux. Le destinataire final doit pouvoir réagir d'après la procédure décrite à cet endroit.</p> <p>{Étape 6: l'historique relatif à une quittance reçue n'est pas présent} Si un historique n'est pas trouvé pour une quittance reçue, cette dernière peut être ignorée.</p>
Liste des erreurs	<p>Erreur:</p> <ul style="list-style-type: none"> ▪ Le message n'est pas valide selon (WSDL-IDCH, 2018). ▪ Le message ne peut pas être décrypté. ▪ Le message contient des historiques qui ne peuvent pas être traités avec le domaine de numérisation implémenté du destinataire final. ▪ Aucune InsuranceCaseID ni élément StoriesWithoutDeclaration: la requête est rejetée (ACKNSwissdec, 2018) ▪ etc. ▪ voir (ACKNSwissdec, 2018)

La plupart des cas spéciaux mentionnés dans (RL-IDCH, 2017), chapitre «Cas spéciaux» sont de nature spécifique et ne sont pas décrits de nouveau dans les présentes spécifications du destinataire final afin d'éviter les redondances.

3.3 UC003 Vérifier la joignabilité

Le cas d'utilisation Vérifier la joignabilité présuppose le cryptage SSL dans les deux sens. La requête et la réponse sont signées et les données XML sont cryptées.

Description succincte	La joignabilité du destinataire final doit être vérifiée par le distributeur. À cet effet, une simple demande PingConsumerRequest selon (WSDL-IDCH, 2018) est envoyée au destinataire final, qui de son côté confirme sa joignabilité en envoyant une PingConsumerResponse.
Acteurs	Distributeur, opérateur du distributeur
Déclencheur	Vérification cyclique par le distributeur ou l'opérateur en cas de dérangement
Conditions préalables	Aucune
Conditions ultérieures	Aucune
Cas d'utilisation inclus	UC004 Appliquer la sécurité
Déroulement standard	<ol style="list-style-type: none"> 1. La demande est envoyée au destinataire final par le distributeur. L'intervalle du polling est en outre communiqué. Intervalle: actuellement 30 minutes (également pendant une fenêtre de maintenance; ainsi, l'intervalle est dynamique) 2. La sécurité est vérifiée, UC004. 3. Le destinataire final répond avec son horodatage actuel, voir <PingConsumerResponse> (WSDL-IDCH, 2018).
Déroulements alternatifs	{Étape 3: en option, une fenêtre de maintenance planifiée (non-disponibilité de x à y) peut être communiquée au distributeur au moyen d'UC005 «Activer une fenêtre de maintenance». Ce cas d'utilisation <i>doit obligatoirement</i> être mis en œuvre.}
Liste des erreurs	Erreurs techniques: <ul style="list-style-type: none"> ▪ le message n'est pas valide (WSDL-IDCH, 2018) ▪ le message ne peut pas être décrypté

3.4 UC004 Appliquer la sécurité

Le destinataire final vérifie les certificats reçus et décrypte le message comme décrit dans (SEC-ERSwissdec, 2018). À la différence de la norme suisse de transmission des données salariales, le destinataire final reçoit, en plus de la double signature, le certificat électronique, contenant l'IDE-OFS, de l'entreprise émettrice. Ainsi, une information relative à l'entreprise émettrice (l'entreprise elle-même ou sa fiduciaire) est communiquée et permet de vérifier si celle-ci est autorisée à annoncer l'événement.

3.5 UC005 Activer une fenêtre de maintenance

Description succincte	Extension d'UC003 «Vérifier la joignabilité». Le destinataire final <i>doit obligatoirement</i> implémenter une fonctionnalité permettant d'inscrire des données pour une fenêtre de maintenance et de la communiquer au distributeur dans la réponse d'UC003 «Vérifier la joignabilité».
Acteurs	Administrateur technique du destinataire final
Déclencheur	Vérification cyclique du distributeur, ou de l'opérateur en cas de dérangement
Conditions préalables	Aucune
Conditions ultérieures	Aucune
Cas d'utilisation inclus	Aucun
Déroulement standard	<ol style="list-style-type: none"> 1. L'administrateur technique du destinataire final inscrit les données de la fenêtre de maintenance. 2. La réponse du destinataire final (PingConsumerResponse) au distributeur contient les données inscrites pour la fenêtre de maintenance.
Déroulements alternatifs	Aucun
Liste des erreurs	Erreur technique: <ul style="list-style-type: none"> ▪ le message n'est pas valide (WSDL-IDCH, 2018)

3.6 UC006 Données de test reçues

L'UC006 «Données de test reçues» ne se différencie que dans son but de l'UC001 «Déclaration d'événement reçue» ou d'UC002 «Synchronisation d'événement reçue».

Certains événements sont caractérisés au moyen d'un élément <TestCase>. Ils ne peuvent pas être traités productivement. Dans la réponse, ces événements doivent également être marqués comme cas de test à l'aide de l'élément <TestCase>.

Objectifs de l'UC006:

- Permettre à l'utilisateur final de se familiariser avec la transmission électronique des données d'événement.
- Permettre des tests lors de l'installation.
- Permettre des tests en cas de problèmes au niveau de la production.

Si l'événement est marqué comme cas de test dans le Declare, la suite du processus de prestations pour cet événement doit toujours se dérouler en mode de test. Lors de la synchronisation, cet événement *doit obligatoirement* être marqué aussi au moyen de l'élément <TestCase> du côté du transmetteur et de celui du destinataire final.

Si la déclaration de test est «mélangée» par inadvertance avec une synchronisation productive, les historiques du destinataire final qui, par erreur, n'ont pas été marqués comme cas de test doivent être refusés au moyen de l'élément «IncidentStories/Error/RequestStoryID» et de la notification que prévoit le document (ACKNSwissdec, 2018) dans l'élément «IncidentStories/Error/Notification».

Ce cas d'utilisation ne doit être utilisé qu'exceptionnellement. Il ne **peut pas** être utilisé comme système de démonstration ou de développement. Une application de référence est disponible à ces fins.

Ce cas d'utilisation sert à la **localisation** de problèmes dans la **chaîne productive de transmission**. Des annonces d'événement de l'entreprise doivent alors être envoyées à travers toute la chaîne d'automatisation des systèmes concernés (ERP, transmetteur, distributeur, destinataire final) et de leurs composants sans déclencher un cas commercial réel. **Aucun événement productif ni aucune InsuranceCaseID** productive ne doit être généré.

D'une manière générale, seuls des déclarations d'événement et des synchronisations de test **correctes et complètes** doivent alors être envoyées.

3.7 UC007 Traiter des duplicatas

On distingue ici entre les deux fonctions Declare et Synchronize (déclarer et synchroniser).

3.7.1 Déclarer des duplicatas

Des duplicatas d'une DeclareIncidentConsumerRequest complète sont détectés techniquement (égalité des bits) par le distributeur et caractérisés au moyen d'un élément «Duplicate» dans le DistributorRequestContext.

Si les informations contenues dans le duplicata n'ont pas encore été traitées et sont encore sans réponse, cela doit être rattrapé.

Si la requête originale a déjà reçu une réponse, une réponse doit être envoyée pour le duplicata avec le même contenu que la réponse envoyée suite à la requête originale (comportement idempotent).

3.7.2 Déclarer un duplicata sans détection par le distributeur

Une DeclareIncidentConsumerRequest modifiée et renvoyée pour un ou plusieurs événements identiques ne peut pas être détectée comme duplicata par le distributeur.

Pour le destinataire final, cela signifie qu'en cas de DeclareIncidentConsumerRequest, des contrôles supplémentaires *doivent obligatoirement* (vérification spécifique) être exécutés par déclaration d'événement (p. ex. «DeclareIncidentConsumer/IncidentDeclaration/Company/Staff/Person/UVG-LAA-Registration») en présence d'un duplicata.

Si des duplicatas de déclarations d'événement sont contenus dans une DeclareIncidentConsumerRequest et que cela n'a pas été détecté par le distributeur, celui-ci a généré une nouvelle IncidentCaseID. Un tel duplicata d'une déclaration d'événement *doit obligatoirement* être détecté quand même par le destinataire final. Il incombe à l'assureur de décider sur la base de quelles données cela se produit. Il *ne peut pas* enregistrer un nouvel événement et il *ne peut pas* générer une nouvelle InsuranceCaseID. L'IncidentCaseID et l'InsuranceCaseID avec lesquelles l'événement a déjà été enregistré *doivent obligatoirement* être utilisées dans la réponse du destinataire final au distributeur. La réponse par déclaration d'événement *doit obligatoirement* correspondre à celle de la déclaration d'événement déjà effectuée et *doit obligatoirement* aussi contenir un avertissement de duplicata d'après le document (ACKNSwissdec, 2018).

3.7.3 Synchroniser des duplicatas

Pour un SynchronizeIncidentConsumer, il n'existe aucune détection de duplicata du côté du distributeur. Cette détection *doit obligatoirement* être effectuée par le destinataire final, qui *doit obligatoirement* reconnaître les duplicatas.

3.7.4 Synchronisation d'un historique identique

En cas de synchronisation, il peut arriver qu'un historique identique soit reçu. Un historique identique se caractérise par la même «StoryID», le même «IncidentContext» (CompanyCaseID, IncidentCaseID, InsuranceCaseID), la même «CreationDate» et le même nom d'historique. Il n'est pas nécessaire de vérifier le reste du contenu de l'historique.

Si un historique identique est détecté d'après les métadonnées décrites ci-dessus, il ne peut pas être enregistré une nouvelle fois. La réponse au distributeur doit correspondre à celle déjà donnée auparavant à cet historique. En outre, un avertissement de duplicata *doit obligatoirement* être renvoyé dans l'élément «IncidentStories/Warning» avec la «RequestStoryID» et la «Notification» correspondante, conformément au document (ACKNSwissdec, 2018).

3.7.5 Synchronize StoryID non unique à l'intérieur de l'IncidentContext

Les StoryID doivent être uniques pour un incident pendant tout le processus. Le système ERP doit donc, par exemple, attribuer une nouvelle StoryID en cas de correction d'un historique.

Si lors de la synchronisation d'un incident des historiques sont reçus avec la même StoryID et le même «IncidentContext» (CompanyCaseID, IncidentCaseID, InsuranceCaseID), mais avec un autre nom de l'élément d'historique ou une autre «CreationDate» qui sont contenus dans une requête précédente ou dans la même requête, ils doivent être rejetés comme duplicatas StoryID non valables. Cela s'effectue au moyen de l'élément «IncidentStories/Error», avec la «RequestStoryID» concernée et la «Notification» correspondante conformément au document (ACKNSwissdec, 2018).

3.8 UC008 Régler les flux de données

UC008 «Régler les flux de données» est un sous-cas d'utilisation d'UC002 «Recevoir la synchronisation d'événement».

Les flux de données *doivent obligatoirement* pouvoir être contrôlés et réglés tant par le destinataire final que par le transmetteur. La raison en est que la taille de réponse de certains cycles Request-Response peut être réduite par répartition en plusieurs cycles (RL-IDCH, 2017), 11.2 «Comportement SynchronizeIncident Request et Response»

Le *destinataire final* peut réduire le volume de données en ne livrant pas toutes les données présentes, mais seulement une partie d'entre elles, au transmetteur. Pour le reste des données encore présentes, les IncidentCaseID sont listées dans l'élément de réponse <Available>.

Le transmetteur exécute ensuite d'autres SynchronizeIncidents pour les IncidentCaseID indiquées dans <Available>.

La taille maximale des requêtes est définie d'après les «meilleures pratiques actuelles» (RL-IDCH, 2017), 11.2.

Description succincte	Le volume de données des réponses au distributeur est réduit par la répartition en plusieurs cycles Request-Response.
Acteurs	Distributeur
Déclencheur	Le volume de données des historiques à livrer à une entreprise serait trop grand.
Conditions préalables	Aucune
Conditions ultérieures	Tous les historiques et quittances ont été livrés au distributeur pour toutes les IncidentCaseID de l'entreprise.
Cas d'utilisation inclus	Aucun
Déroulement standard	<ol style="list-style-type: none"> 1. Un SynchronizeIncident du distributeur est reçu pour un ou plusieurs événements (RL-IDCH, 2017) «Système d'identification». 2. L'entreprise émettrice est identifiée d'après les données fournies «CustomerId» et, le cas échéant, «ContractId». 3. Si une trop grande quantité d'historiques est prête à la livraison pour l'entreprise et les événements demandés, seule une partie d'entre eux seront communiqués dans la réponse. Les IncidentCaseID des historiques restants sont listés dans l'élément <Available> de la réponse. 4. Les étapes 1 à 3 sont répétées jusqu'à ce que tous les historiques des événements demandés pour l'entreprise aient été livrés.
Déroulements alternatifs	Aucun
Liste des erreurs	<ul style="list-style-type: none"> ▪ L'entreprise n'a pas pu être identifiée.

3.9 UC009 Traiter une demande de support

Description succincte	Traiter des exceptions, des dérangements et d'autres problèmes
Acteurs	Spécialistes de l'entreprise, collaborateurs du support du fabricant du système ERP, collaborateurs du support du destinataire final
Déclencheur	Le spécialiste de l'entreprise ou le collaborateur de support du fabricant ERP émet une demande de support par e-mail ou par téléphone.
Conditions préalables	Aucune
Conditions ultérieures	La demande de support a pu être traitée avec succès.
Cas d'utilisation inclus	Aucun
Déroulement standard	<ol style="list-style-type: none">1. Une nouvelle demande de support par un spécialiste de l'entreprise ou un collaborateur de support du fabricant ERP est émise par e-mail ou par téléphone.2. Le problème est analysé par le collaborateur de support du destinataire final, qui y répond.
Déroulements alternatifs	{après l'étape 1} <ol style="list-style-type: none">1. Le problème est remonté et arrive au support de second ou de troisième niveau. {continuer à l'étape 2}
Liste des erreurs	Aucune erreur

Concernant les cas de support, il importe que les informations de support soient communiquées de manière uniforme. Les erreurs, les avertissements et les informations doivent être établis et insérés dans la réponse conformément à (ACKNSwissdec, 2018). Les codes décrits dans (ACKNSwissdec, 2018) sont contraignants.

En cas de demande de support, il *doit obligatoirement* y avoir une possibilité d'accéder aux informations nécessaires pour le traitement du problème, p. ex. sur la base d'un instant de la requête ou de l'InsuranceCaseID, de l'IncidentCaseID, de la CustomerIdentity et de la CompanyCaseID.

4 Exigences supplémentaires

4.1 Version de la norme suisse en matières de prestations

Dans le schéma se trouve l'élément `<RequestContext/UserAgent/StandardVersion>` qui désigne la version utilisée de la norme suisse en matière de prestations. Cela est nécessaire à cause de modifications entre différentes versions qui ne se rapportent pas au schéma, mais exclusivement au contenu des éléments.

4.2 Normes de communication

Le couplage standard *doit obligatoirement* se baser sur le Web Service Technologie (SOAP⁴ version 1.1, WSDL⁵ version 1.1 et WSS⁶ version 1.0). Les données *doivent obligatoirement* être cryptées entre la couche HTTPS⁷ (two-way SSL/TLS) ainsi qu'au niveau SOAP selon WSS (SEC-ERSwissdec, 2018).

4.3 Compression en option

Une compression des requêtes et des réponses est optionnelle. Les données XML peuvent être fortement comprimées car elles contiennent de nombreuses informations redondantes. L'expérience montre que les données cryptées peuvent être comprimées de 50% environ. Pour que le distributeur puisse distribuer de grandes annonces d'événement et afin d'économiser un débit précieux pour toutes les parties concernées, il est possible de compresser selon l'algorithme GZIP les requêtes partant du distributeur. L'utilisation de la compression est décidée lors du couplage.

Les requêtes partant du distributeur comprennent au moins les champs suivants dans l'en-tête http en cas de compression GZIP du corps du message:

- Content-Encoding: gzip
- Accept-Encoding: gzip

Les réponses comprimées des destinataires finaux *doivent obligatoirement*, si la compression est utilisée, contenir le champ suivant:

- Content-Encoding: gzip

D'autres informations figurent à l'adresse <http://www.ietf.org/rfc/rfc1952.txt>.

4.4 Disponibilité

L'unité d'observation comprend le distributeur et tous les destinataires finaux couplés, c'est-à-dire que l'entreprise (source des données d'événement) voit tout le système en tant qu'unité. Si un destinataire final n'est pas exploité dans la qualité requise, il réduit la fiabilité de tout le système. Tous les participants doivent donc se mettre d'accord sur une fiabilité **minimale**.

Exigence de la norme suisse en matière de prestations

- Toutes les transmissions m2m (machine à machine) s'effectuent en **«temps réel» (disponibilité Internet 7 x 24h)**.

Cette exigence a les conséquences suivantes pour le destinataire:

- les institutions/leurs destinataires finaux **doivent obligatoirement** aussi offrir au moins **un service 7x24 h pour la réception des données**;
- **les interruptions planifiées⁸ (p. ex. fenêtre de maintenance)** *doivent obligatoirement* être exécutées aux heures creuses et *doivent obligatoirement* être annoncées au préalable (voir à ce propos le cas d'utilisation UC003 «Vérifier la joignabilité»);
- après **une interruption non planifiée**, les entreprises concernées par un échec de transmission *devraient* être informées dès que le destinataire est de nouveau disponible;
- si des services internes **ne sont pas disponibles** pour la vérification de l'acceptation, on *peut* quand même quittance par une acceptation. Cela *devrait* être communiqué à l'expéditeur dans la quittance au moyen d'une

⁴ SOAP (Simple Object Access Protocol)

⁵ Web Services Description Language (WSDL) définit la spécification XML indépendante de toute plate-forme, langage de programmation et protocole pour la description de services réseau (Web Services) permettant l'échange de messages.

⁶ Web Services Security (WSS) von Organization for the Advancement of Structured Information Standards (OASIS)

⁷ http 1.0 ou 1.1; au moins TLS 1.2 avec longueur minimale de clé de session de 256 bits

⁸ S'applique aux travaux de maintenance normaux, donc à l'exception des hotfix et des patch

Warning/Notification. Si un contrôle ultérieur des données provoque le rejet du message, cela doit être communiqué au client en dehors de cette spécification du système.

Procédure orientée objectif concernant la disponibilité:

Nous avons à cœur d'appliquer l'**orientation clientèle**. Les disponibilités des systèmes doivent être considérées comme des **futures valeurs cibles**. Ainsi, les entreprises seront motivées de transmettre leurs annonces par voie électronique. Aucun contrôle de disponibilité n'est prévu. C'est pourquoi seules les valeurs limites essentielles sont définies ici et les principes y relatifs sont mentionnés en annexe.

4.4.1 Périodes définies

- Horaire d'exploitation de tout le système (distributeur, communication et destinataire final; trajet m2m jusqu'à la quittance-réponse à l'entreprise)
 - 24 heures sur 24, 7 jours par semaine
 - Heures de pointe: de 6 à 20 heures sauf le week-end (les autres heures sont considérées comme des heures creuses)
- Fenêtre de maintenance pour corrections et mises à jour
 - 10 heures par semaine
 - En dehors des heures de pointe, si possible entre 2 h 00 et 5 h 00 du matin
- Heures de service et de support pour les participants au système (distributeur et ses destinataires finaux)
 - Aux heures de bureau usuelles
 - Support pour fenêtre de maintenance sur demande

4.4.2 Plages de valeurs définies

Objectif: solution pragmatique = «lightweight construction» et «best effort»

- Aux **heures de pointe**, la disponibilité des destinataires finaux (m2m) **doit** être au moins de **99,52 %**.
- Aux **heures creuses**, la disponibilité des destinataires finaux (m2m) **doit** être au moins de **93,00 %**.

4.5 Extensibilité

Les systèmes de destinataires finaux devraient pouvoir s'étendre en fonction de la charge à traiter. Il est tout à fait envisageable de commencer avec une solution minimale et d'augmenter la puissance au besoin afin de garantir la disponibilité et la performance requises.

4.6 Modifications à l'interface

- Si des modifications de la norme suisse en matière de prestations doivent être activées aussi chez le destinataire final, tout le couplage (du côté du distributeur et de celui du destinataire final) *doit obligatoirement* être adapté.
- Si les modifications de la norme suisse en matière de prestations ne doivent pas être activées chez le destinataire final, le distributeur *peut* transformer la structure de données existante (mapping) dans la mesure où cela est possible au niveau du contenu («Design-Firewall»).

Le distributeur reçoit toujours des données clairement définies sur le plan spécifique. Actuellement, aucune solution générique n'est prévue.

4.7 Support et temps de réaction

Seuls les aspects techniques du support sont fixés, c'est-à-dire qu'ici sont définies uniquement des structures d'information pour tous les systèmes de la chaîne de processus.

Le support *doit obligatoirement* être fourni en allemand, en français et en italien pour les domaines ou acteurs suivants:

- entreprises et leur fabricant de système ERP;
- institutions destinataires finaux.

Par conséquent, certains messages d'erreur doivent aussi être émis dans les langues correspondantes. Voir dans le message:

.../RequestContext /LanguageCode

Pour déterminer un temps de réaction, les **catégories d'erreurs** suivantes ont été définies:

- Critical = 15 min
- Medium = 4 h
- Uncritical = 1 jour

Ces catégories d'erreurs seront utilisées plus tard dans différents systèmes (applications, fichiers journaux, outil de surveillance, etc.).

En outre, le support du deuxième niveau *doit obligatoirement* être coordonné avec les développeurs d'applications.

4.8 Performance / Débit utile

- Le volume maximal de données doit être déterminé par chaque destinataire final et les systèmes doivent être dimensionnés en conséquence.
- Temps de réponse (pour toutes les opérations): toute la transmission doit se dérouler en «temps réel». Le temps de transmission/de distribution doit être **inférieur à une minute**. Pour le destinataire final, cela signifie que:
 - le temps de traitement dépend du destinataire final, du volume de données et de la capacité de la ligne
 - une réponse *devrait* arriver en moins de 20 secondes
 - en outre, un temps maximal d'attente est défini pour chaque destinataire final par le distributeur (time-out: valeur actuelle par défaut = 60 secondes).
 - Pour la synchronisation, le destinataire final peut réduire, si nécessaire, le temps de traitement à l'aide du cas «UC008 Régler les flux de données».
- Le contrôle et le traitement détaillés proprement dits (p. ex. intégration de services supplémentaires) s'effectueront après la 1^{ère} étape.

Figure 5: Document d'instance pour destinataire final et indications des temps

4.9 Sécurité et protection des données

La sécurité et la protection des données sont des bases conceptuelles importantes pour la communication dans la norme suisse en matière de prestations et doivent être prises en compte pour la construction et l'exploitation du destinataire final.

Dans le domaine de la protection des données, la norme suisse en matière de prestations fournit déjà des solutions

- transparence grâce à la standardisation (norme de prestations swissdec);
- déclaration d'intention au moyen de la balise <Job> dans la déclaration d'événement;
- filtrage à l'aide de transformations sur le distributeur.

Ces solutions doivent être exploitées de manière sûre et fiable.

L'institution destinataire finale *doit obligatoirement* garantir que seuls des systèmes «spécialement sécurisés», équipés des correctifs de sécurité actuels, des voies de communication cryptées et des configurations étudiées pour la sécurité sont utilisés. Elle *doit obligatoirement* protéger l'application contre les attaques DoS et DdoS (Denial of Service / Distributed Denial of Service). En outre, elle doit la protéger contre les hackers et les virus (IDS (intrusion detection system / prevention); antivirus).

- D'une manière générale, les dispositions normales en matière de protection des données de l'institution du destinataire final sont applicables.

4.10 Adressage et filtrage

Une requête mal adressée *doit obligatoirement* être refusée. Elle pourrait aussi être la conséquence d'une attaque sécuritaire.

Recommandations:

- du point de vue de la protection des données, une **pseudonymisation**⁹ devrait être exécutée le plus vite possible.

⁹ Forme plus faible de l'anonymisation; modification de données personnelles par une prescription d'attribution, p. ex. en utilisant deux tableaux séparés (personne et événement), qui sont reliés au moyen d'une clé anonyme.

5 Annexe

5.1 Documents de spécifications également applicables

Les documents suivants s'appliquent également pour le test et la réception.

Renvoi aux documents de spécifications également applicables

ACKNSwissdec, s. (2018, janvier 31). AcknowledgementNotification. (swissdec, Éd.) Berne, Suisse. Récupéré sur <https://tst.itserve.ch/swissdec/infopoint/datapool.xhtml>

DIAL-IDCH, s. (2018, février 27). Spécifications de la représentation des messages de dialogue. (swissdec, Éd.) Berne, Suisse. Récupéré sur <https://www.swissdec.ch/de/releases-und-updates/richtlinien-kee>

OV-IDCH, s. (2018, janvier 15). IncidentDeclarationStandardOverview. Berne, Suisse.

RCTS-IDCH, s. (2018, février 26). Receiver Certification Test Suite IncidentDeclaration. (swissdec, Éd.) Berne, Suisse. Récupéré sur <https://receiver.swissdec.ch>

RL-IDCH, s. (2017, novembre 09). Directives pour la norme suisse en matière de prestations. (swissdec, Éd.) Berne, Suisse. Récupéré sur <https://www.swissdec.ch/de/releases-und-updates/richtlinien-kee>

SEC-ERSwissdec, s. (2018, février 15). SecurityEndreceiver. (swissdec, Éd.) Berne, Suisse. Récupéré sur <https://tst.itserve.ch/swissdec/infopoint/datapool.xhtml>

WSDL-IDCH, s. (2018, janvier 15). IncidentDeclarationConsumerService.wsdl. (swissdec, Éd.) Berne, Suisse. Récupéré sur <https://www.swissdec.ch/de/releases-und-updates/richtlinien-kee>