

---

# **AssurPharma**

## **Integration Specification version 2.3.1**

---

Last modification date 18/11/2025



# 1 Document control

## Document revision history

Version	Date	Author	Comments
0.1	19/08/2013	Accenture	Initial version
0.2	20/08/2013	Accenture	Version for review
0.3	21/08/2013	Accenture	Added clarification on certificates and BVAC event
0.4	29/08/2013	Accenture	Update after feedback insurers
0.5	04/10/2013	Accenture	Final update after clarification SFTP issues <ul style="list-style-type: none"> <li>• Updated doc with info provided by email               <ul style="list-style-type: none"> <li>○ url's</li> <li>○ latest version single message</li> </ul> </li> <li>• SFTP no longer needs x.509 for authentication, but a simple SSH (limitation SFTP setup)</li> <li>• Brought drawing and text in line with wsdl (previous doc contained an old version of the visio)</li> <li>• Added further clarifications across the document</li> </ul>
0.5.1	14/10/2013	Accenture	Added minOccurs="0" to the routingParametersCBFA in the ASSURPHARMATIPSystemServices_protocol-1_0.xsd
0.6	21/10/2013	Accenture	Update with answers to questions received from Assuralia members during integration
0.6.1	08/11/2013	Accenture	Updates following integration with insurers
0.7	12/11/2013	Accenture	Finalised version
1.0	15-09-2014	Marc Buckens	<ul style="list-style-type: none"> <li>- Renamed the project to ASSURPHARMA</li> <li>- Extract the embedded files to a packaging level</li> <li>- Appended information               <ul style="list-style-type: none"> <li>○ General Functioning</li> <li>○ Karakterestieken</li> <li>○ Services, Messages, Data Formats</li> <li>○ Integration guidelines for all stakeholders</li> <li>○ Acceptance Test Approach</li> </ul> </li> </ul>
1.1	17-10-2014	Marc Buckens	<ul style="list-style-type: none"> <li>- Updated UTC</li> <li>- Xchecked xsd and xml</li> </ul>
2.1	20/02/2020	Marc Buckens / Manon Buyl	<ul style="list-style-type: none"> <li>- Update document technical</li> <li>- Flow change to less paper</li> </ul>
2.2	26/03/2020	Kerlijne Van Den Broeck	Minor textual changes
2.3.1	18/11/2025	Marc Buckens	Restore broken links in document

# Contents

<b>1</b>	<b>Document control .....</b>	<b>1</b>
<b>2</b>	<b>Introduction.....</b>	<b>7</b>
2.1	Scope.....	7
2.2	Intended Audience .....	7
2.3	Context.....	7
<b>3</b>	<b>General Functioning .....</b>	<b>8</b>
3.1	Working assumptions/conditions when digitizing the BVAC attestation.....	8
3.2	The patient is informed.....	8
3.3	Overall Data Flow .....	9
3.4	[ISV] Patient-Pharmacist flow aka operations concepts .....	10
3.4.1	The patient identification is specific to the private insurer .....	10
3.4.2	The pharmacist identifies the patient .....	11
3.4.3	The patient requests a BVAC attestation .....	11
3.4.4	The data is encrypted .....	13
3.4.5	The encoded data is sent to a back-office system for further processing .....	13
3.4.6	A proof of receipt is returned to the pharmacy software .....	13
3.4.7	The back-office system will return a receipt to the pharmacist. It serves as an evidence for correct transmission. The printed proof of the BVAC with additional information is given to the patient.....	14
3.4.8	Real-time acknowledge or fall-back to paper BVAC.....	16
3.4.9	Proof-of-activation registration.....	16
3.5	[ISV] Services offered by the multi-business connector extending the SMC with the BVAC flow.....	16
3.5.1	The Multi-business connector for pharmacies.....	16
3.5.2	Connector specificities in view of supporting the BVAC data registration.....	17
3.5.3	The offline component is not used for the BVAC event.....	17
3.5.4	Get Configuration (System Services) .....	17
3.6	[TIP] TIP administrative extension to support the BVAC.....	18
3.6.1	Insurer configuration on basis of their CBFA identification .....	18
3.6.2	Directory localisation.....	19
3.6.3	Batch localisation.....	19
3.7	[INSURER] Insurer data collection .....	20

3.7.1	“Assuralia Table” .....	20
3.7.2	Get BVAC through webservice .....	20
3.7.3	Get BVAC through SFTP .....	21
<b>4</b>	<b>Characteristics.....</b>	<b>23</b>
4.1	Characteristics of the [Case Number] (dossiernummer ,numéro de dossier) .....	23
4.2	Characteristics of the [Affiliation Number].....	23
4.3	Characteristics of the [Document Number] ( documentnummer, numéro de document) .....	24
4.4	Code 128/ <u>QR</u> .....	24
4.5	Period of storage of encrypted data for the receiving insurer.....	24
<b>5</b>	<b>Services, Messages and Data Formats .....</b>	<b>25</b>
5.1	Single Message – the basics .....	25
5.2	BVAC Event Type – vehicle for sending the BVAC data.....	25
5.2.1	Message structure of the SMC supporting the BVAC EventType.....	26
5.2.2	Unique identifiers .....	27
5.2.3	BVAC Event structure – xsd .....	27
5.3	BVAC Document – payload data.....	27
5.3.1	BVAC Document Definition .....	27
5.3.2	BVAC Document – Message Format.....	28
5.4	Webservice “get BVAC” and response Message format .....	29
5.5	Sftp “get BVAC” and response Message format.....	30
<b>6</b>	<b>Integration guidelines for the ISV application .....</b>	<b>32</b>
6.1	The identification of the patient with regards to the private insurer.....	32
6.2	Creation of the BVAC attestation .....	32
<b>7</b>	<b>Integration guidelines for integrating the multi-business connector.....</b>	<b>33</b>
<b>8</b>	<b>TIP configuration guidelines.....</b>	<b>34</b>
8.1	SFTP Server configuration.....	34
8.1.1	Authentication .....	34
8.1.2	Authorization .....	34
8.1.3	Authentication & secure message transfer .....	34
8.1.4	Connection Parameters .....	34
8.1.5	Technical Registration .....	34
<b>9</b>	<b>Integration guidelines for the BVAC retrieval.....</b>	<b>37</b>

9.1	<i>Authentication &amp; encryption – securing the transport</i> .....	37
9.1.1	[Web-Service] Insurer X.509 Certificate for transport .....	37
9.1.2	[SFTP] Insurer SSH key for transport (for SFTP).....	39
9.2	<i>Authentication &amp; encryption – encrypting the payload</i> .....	40
10	<b>FAQ &amp; Code snippets</b> .....	42
10.1	<i>Convention on the Date-Time format</i> .....	42
10.2	<i>.net</i> .....	42
10.2.1	PKCS# padding .....	42
10.2.2	What is the size of IV for the AES encryption? .....	42
10.2.3	How to initialize the vector?.....	42
10.3	<i>Java</i> .....	42
10.3.1	What is the algorithm used to verify the signature? .....	42
10.3.2	How to AES encrypt? .....	43
10.3.3	How to AES decrypt? .....	43
10.3.4	How to do RSA encryption? .....	43
10.3.5	How to do RSA decryption.....	43
11	<b>Test Cases – Validation Approach</b> .....	45
12	<b>Reference data</b> .....	Fout! Bladwijzer niet gedefinieerd.
12.1	<i>Single Message</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.2	<i>Pharmacy SDK</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.3	<i>Application Design</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.4	<i>BVAC Document message formats</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.5	<i>AssurPharma Webservices Specification for insurers</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.6	<i>AssurPharma CBFA Configuration</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.7	<i>Assuralia Identification Insurers</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.8	<i>TIP System Services</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>
12.9	<i>GetBVAC WebService Error Messages</i> .....	<b>Fout! Bladwijzer niet gedefinieerd.</b>



# List of Figures

Figure 1 Multi-business connector for pharmacies.....**Fout! Bladwijzer niet gedefinieerd.**

Figure 2 - Single Message hierarchy overview ..... 25

Figure 3 – Single Message and BVAC Event Type ..... 26

Figure 4 BVAC Document Definition ..... 28

(Figure 5 – WebService Get BVAC messages)..... 29

(Figure 6 - Error response structure)..... 29

Figure 7 – SFTP XML file structure..... 30

Figure 8 - Example encryption in context of delegation ..... 36



# List of Tables

Table 1 - Example technical registration parameters..... 36

## 2 Introduction

### 2.1 Scope

---

This document establishes a set of requirements and constraints for the interface between insurers and the TIP system for retrieval of BVAC messages.

It outlines the interface requirements to support the Assuralia business events in the TIP system solution. It details the integration procedure expected to be implemented by the insurers be able to use the services offered by the TIP System for retrieval of BVAC messages.

### 2.2 Intended Audience

---

This document is intended for use by architects, developers and testers of the applications identified.

### 2.3 Context

---

Next to the national compulsory health insurance (RIZIV-INAMI), a citizen has the possibility to contract complementary coverage for health related out-of-pocket costs with the insurer(s) of his choice.

Contrary to interventions by RIZIV for pharmaceutical products using a third party settlement process, the patient still has to advance the amount and claim reimbursement from his insurer in case of complementary insurance. To this means the pharmacist can issue a BVAC attestation clearly identifying the patient, the product(s) and the price among other things. The patient/insured person submits the BVAC to his insurer by post, handover or other permitted channels to obtain a (partial) reimbursement depending on the specifics of his contract.

As the personal share of medical expenses (portion of the cost not covered by INAMI) is increasing, patients are increasing their complementary coverage. At present an estimated 3 million BVAC attestations are issued yearly.

In the context of the ASSURPHARMA project, we will implement an Assuralia flow in the TIP that will automate the transfer of the information contained within the BVAC attestation from pharmacist to insurer enabling reimbursement to the patient/insured person. This will reduce the administrative load for

- ☐ the patient: no more manual intervention to claim reimbursement
- ☐ the insurer: reduced handling and recoding as structured information is transferred electronically.

This flow can be called by pharmacy software through connector module.

Remark that some use AssurCard as an aggregator to interact with care providers, the TIP will thus transfer the BVAC attestations to AssurCard instead of directly to these respective.

At present only the electronic transfer of the BVAC data from pharmacist to insurer is in scope.

## 3 General Functioning

### 3.1 Working assumptions/conditions when digitizing the BVAC attestation

- ☐ The solution should not provide any additional administrative burden on the pharmacist
- ☐ The solution shall at all times be a free choice of the whether or not to exchange the digitized BVAC data to the private insurer
- ☐ The solution must ensure that clear agreements are enforced in the case of liability. The pharmacist can not be held responsible for whether or not processing or reimbursements will be done by the private insurer
- ☐ The project is only in the context of supplementary insurance

### 3.2 The patient is informed

The following information is given by the by the private insurer to the patient:

1. A general writing by the private insurers to the patient informing that he can request the reimbursement to the private insurer through a service offered by the pharmacists. Data from the BVAC attestation can be send in digitized form and in direct from the pharmacy outlet to the private insurer.
2. On admission to hospital, this information can be handed over again.
3. The patient must submit a "specific identification" to the pharmacist when registering:
  - a. These specific identifier contains at least the identification of the private insurer
  - b. This specific identification may also contain a reference to a specific "dossier" specific to each of the private insurance companies
  - c. Patients with no "specific identification" can fall back on the paper circuit.
4. General information about the data protection will be made public (via website).

Conceptually, the following approach is further developed by insurers:

*Logo van de verzekeraar*

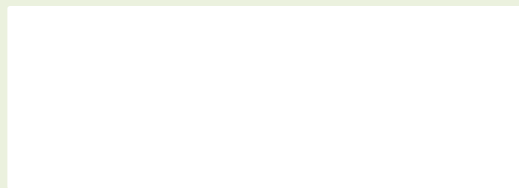
*Identiteitsgegevens van verzekerde*

*Gegevens van verzekeraar*

Indien u naar aanleiding van uw hospitalisatie medicijnen moet gebruiken, gelieve dan aan uw apotheker een BVAC-attest te vragen en deze brief aan uw apotheker te geven wanneer u deze medicijnen aankoopt. Door de afgifte van deze brief aan de apotheker gaat u ermee akkoord dat de apotheker de gegevens vermeld op het gevraagde BVAC-attest elektronisch zal doorsturen naar ons. U zal tevens een bewijs ontvangen dat uw BVAC-attest correct werd verwerkt, u kan dit bewijs best bewaren. Wij zullen op basis van de ontvangen elektronische gegevens de medicijnen terugbetalen volgens de algemene en bijzondere voorwaarden van uw verzekeringsovereenkomst.

Indien u vragen zou hebben over de terugbetaling van de medicijnen, kan u steeds contact op nemen met ... *[de verzekeraar – vermelding contactgegevens]*. Vermeld dan zeker het specifieke nummer dat op het papieren BVAC-attest staat.

### Barcode



## 3.3 Overall Data Flow

The BVAC flow is an extension on the TIP Single Message Concept, enabling:

All services pass through authentication and authorization processing inherent to the secured data collection.

- ☐ **[ISV] Patient-Pharmacist flow:** to be implemented by the ISV
- ☐ **[ISV] Services offered by the connector extending the SMC with the BVAC flow:** A variant of the existing TIP "Register Data" Flow
  - To submit BVAC messages to the TIP,
  - For receiving real-time confirmation of the BVAC message hand-over to the TIP
  - For routing to new endpoints
  - For returning resulting status messages from AssurCard / Insurers.

➔ to be interfaced with by the ISV.

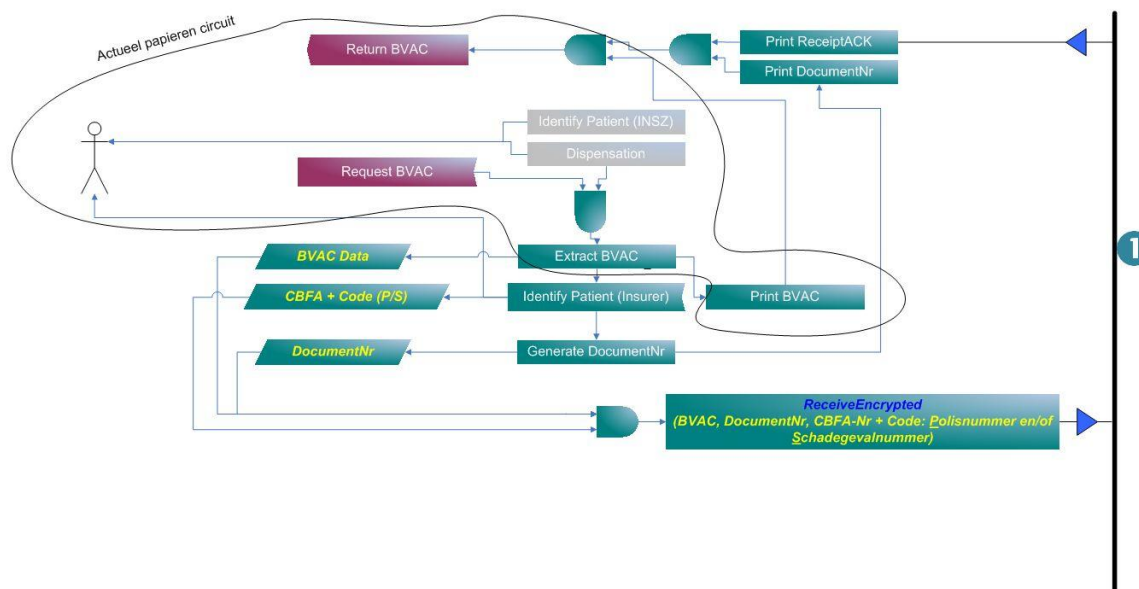
- ☐ **[TIP] TIP administrative extension to support the BVAC:** dedicated configuration for CBFA numbers that can be used by connector module to be implemented by the TIP administration
- ☐ **[INSURER] Insurer data collection:** both web service and SFTP service (both not passing through eHealth) allowing Insurers to pick up BVAC messages from TIP (whether independently or through an aggregator like Assurcard) ➔ to be implemented by the Insurer

### 3.4 [ISV] Patient-Pharmacist flow aka operations concepts

Wednesday, May 22, 2013



#### Flowchart Apotheekomgeving



Fluxx | Service Support Center 095 2000 1000

Page 4

#### 3.4.1 The patient identification is specific to the private insurer

The pharmacist identifies the patient in a uniform manner through its national number [NISS]. The private insurers each use a different identification mechanism. This because the use of the national number is not authorized for the private insurers.

In the context of the digitization of the BVAC information we distinguish the following possible identification mechanisms:

- ☐ Identification based on an awarded [Case Number] (dossiernummer ,numéro de dossier)
- ☐ Identification with no [Case Number] (dossiernummer ,numéro de dossier) is known:
  - o Identification based on a patient-specific account with a private insurer [Affiliation Number] (aansluitingsnummer, numéro d'affiliation)
  - o No identification to a private insurer

*This identification mechanisms are specific to the identification used by the internal administration of the private insurers. Concretely, a patient who walks into a pharmacy will be in possession of either a [Case Number] (dossiernummer ,numéro de dossier) or an [Affiliation Number] (aansluitingsnummer, numéro d'affiliation).*

*Regardless of the type of identification that the patient has at its disposal, the system will work transparent to each of these identification mechanisms. Even if a patient is in possession of a [Case Number] (dossiernummer ,numéro de dossier) and only give the [Affiliation Number] (aansluitingsnummer, numéro d'affiliation), the system will ensure that the BVAC is handled properly. The linking the [Affiliation*



Number] (aansluitingsnummer, numéro d'affiliation) to a specific [Case Number] (dossiernummer, numéro de dossier) belongs to the processing in the back office of the private insurers.

In essence, the solution will be flexible with different identification mechanisms. Even more: this identification mechanism happens before the patient enters the pharmacy

#### ➤ *The identification of a patient based on the [Case Number] (dossiernummer, numéro de dossier)*

On admission to a hospital a [Case Number] (dossiernummer, numéro de dossier) will be granted. This [Case Number] (dossiernummer, numéro de dossier) is also printed on a cover letter in barcode form printed and will be handed over to the patient. Note that in this cover letter will also be used in the pharmacy. On the cover letter, the instructions and responsibilities of the patients will be provided.

*For more details on the format of the [Case Number] (dossiernummer, numéro de dossier), we refer to "Features" on page **Fout! Bladwijzer niet gedefinieerd**. The patient may receive the [Case Number] (dossiernummer, numéro de dossier) in a variety of ways. On admission to the hospital a document can be printed that contains this [Case Number] (dossiernummer, numéro de dossier) - also in barcode form. We also plan to provide a patient portal governed by the private insurers where the patient could consult his [Case Number] (dossiernummer, numéro de dossier).*

#### ➤ *The identification of a patient based on an account number with a private insurer*

A valid identification of account with a private insurer [Affiliation Number] (aansluitingsnummer, numéro d'affiliation) is an unique identifier that can be coded in an automated way.

Preferably, there is also a bar code provided on the card which allows the pharmacist to scan identification.

*The patient can obtain his [Affiliation Number] (aansluitingsnummer, numéro d'affiliation) in different ways. For example, we are envisaging a writing to the patient in which the [Affiliation Number] (aansluitingsnummer, numéro d'affiliation) will also be provided in barcode form.*

*Also planned in the same writing is to have the responsibilities for the pharmacist explained, the implicit consent the patient will give to the pharmacist and the private insurer to exchange the BVAC data when handing over the [Affiliation Number] (aansluitingsnummer, numéro d'affiliation).*

#### ➤ *Identification of the patient when there is no specific identification of the insurer known*

When there is no specific identification known, the BVAC data will not be exchanged digitally.

### 3.4.2 *The pharmacist identifies the patient*

The pharmacist identifies the patient in a uniform manner on the basis of his national number [NISS]. The pharmacist will be responsible for the delivery of the medication and the associated guidance in the context of basic and continuing pharmaceutical care.

*To clarify: there is no link between the NISS and the identification of the patient.*

### 3.4.3 *The patient requests a BVAC attestation*

At the request of the patient, the pharmacist will be responsible for delivering a BVAC attestation. This request triggers the following actions in the pharmacy:

1. The pharmacist 1 asks about the available identification of the patient with respect to the private insurance companies<sup>1</sup>

As described in 'Fout! Verwijzingsbron niet gevonden.' on page Fout! Bladwijzer niet gedefinieerd., we distinguish between two possible identification mechanisms:

- ☐ [Case Number] (dossiernummer ,numéro de dossier)
- ☐ [Affiliation Number] (aansluitingsnummer, numéro d'affiliation)

2. The pharmacist encodes the necessary data.

The billing information and other data are encoded by the pharmacy software.

(refer to 'Fout! Verwijzingsbron niet gevonden.' on page Fout! Bladwijzer niet gedefinieerd.)

3. A unique [Document Number] ( documentnummer, numéro de document) is assigned to this data.

Next to the identification of the patient, we also introduce a unique reference for the BVAC: the [Document Number] ( documentnummer, numéro de document). This [Document Number] ( documentnummer, numéro de document) refers to a specific set of data belonging to a BVAC. It is unique and it is generated by the Multi-Business connector.

4. The encoded data is sent to a back-office system for further processing.

Above all, it is important that the patient - where possible – is informed that the BVAC data is effectively transmitted to his private insurer. On the other hand, it is important for the pharmacist to not be imposed by additional administrative tasks. In concreto, the pharmacist should not have an in-depth knowledge on the specifics of the administrative processing at the private insurers.

The pharmacist just has to send the encrypted data to a back office system for further processing. (Refer also to 'Fout! Verwijzingsbron niet gevonden.' on page Fout! Bladwijzer niet gedefinieerd.)

5. The back-office system provides a receipt confirmation.

The solution will provide a return message that the data is properly handed-over for further processing by the back-office system. In this way the patient and the pharmacist are informed that further handling, correction, dispute should not happen with the pharmacist.

*In a letter sent to the patient it will be explicitly noted that it is not the responsibility of the pharmacist to correctly process the request for reimbursement by the private insurer.*

(refer also to 'Fout! Verwijzingsbron niet gevonden.' on page Fout! Bladwijzer niet gedefinieerd.)

6. The proof of successful transmissopn is printed and given to the patient. This proof contains the [Document Number] (documentnummer, numéro de document) and if available the [Case Number] (dossiernummer ,numéro de dossier) and / or the [Affiliation Number] (aansluitingsnummer, numéro d'affiliation) for purpose traceability.

(refer also to 'Fout! Verwijzingsbron niet gevonden.' on page Fout! Bladwijzer niet gedefinieerd.)

Each of these steps will be explained in more detail.

---

<sup>1</sup> This question is not actively asked by the pharmacist. Enkel op vraag van de patiënt wordt naar zijn beschikbare gegevens rond de bijkomende verzekering gevraagd.

When the BVAC is send electronically, the patient receives the proof of successful transmission. This proof contains the [Document Number] (documentnummer, numéro de document) and if available the [Case Number] (dossiernummer, numéro de dossier) and / or the [Affiliation Number] (aansluitingsnummer, numéro d'affiliation) for purpose traceability. Further processing is done in the back office. Do note that the patient can always request to receive his BVAC attestation in paper (duplicate).

### 3.4.4 The data is encrypted

The pharmacist will be responsible at the request of the patient to deliver (read print-out) a BVAC. This in accordance with the known actions at the pharmacy.

In preparation for printing the BVAC pharmacy software will 'pick' this information from the pharmacy system

These data contain at least the information required in the BVAC

In concreto, we distinguish the following information

- ☐ Invoice data → see **Fout! Verwijzingsbron niet gevonden.**
- ☐ Other data → see **Fout! Verwijzingsbron niet gevonden.**

#### 3.4.4.1.1 Codification of the invoice data

All delivered products will be encrypted and this in accordance with the “bijlage V van het K.B. van 21/01/2009 houdende onderrichtingen voor apotheker”/”annexe V de l’arrête royal du 21/01/2009 pourtant instruction pour les pharmaciens”

#### 3.4.4.1.2 Codification of other data

Next to the invoicing data, the pharmacist can code additional data such as:

- ☐ Data on pharmaceutical care acts
- ☐ data in the context of the ‘derdebetalerssysteem’/’tiers payant’

### 3.4.5 The encoded data is sent to a back-office system for further processing



Meanwhile, the data set consists of the BVAC data, additional data and a unique [Document Number] ( documentnummer, numéro de document).

In the aim of not drawing any liability to the pharmacists regarding the correct processing of the private insurance the encrypted data is provided to the back-office system and the back-office system responds that the data has been received correctly

The attentive reader will understand that there is an 'online' processing where the pharmacist will receive an immediate confirmation that further processing will be handled by the back-office system. The patient can be informed to contact his private insurer for any questions. The patient can in each case refer to the [Document Number] ( documentnummer, numéro de document) whether or not accompanied by his [Affiliation Number] (aansluitingsnummer, numéro d'affiliation) or [Case Number] (dossiernummer, numéro de dossier).

### 3.4.6 A proof of receipt is returned to the pharmacy software

### 3.4.7 *The back-office system will return a receipt to the pharmacist. It serves as an evidence for correct transmission. The printed proof of the BVAC with additional information is given to the patient*

At the end, the pharmacy software will –upon demand of the patient- issue the additional information including:

- Technical data including
  - [Document Number] ( documentnummer, numéro de document) and if present [Affiliation Number] (aansluitingsnummer, numéro d’affiliation)[Case Number] (dossiernummer ,numéro de dossier)
  - Evidence of receipt and specific information about contact name for further processing (cfr. Helpdesk number, document number, ...)
  - Other technical data

In case the [Affiliation Number] (aansluitingsnummer, numéro d’affiliation) and / or [Case Number] (dossiernummer ,numéro de dossier) are known, the encrypted data will be made available for the intended private insurer. It is up to the private insurer to pick them up. The recipient is known by name

#### ➤ *Layout additional information when printed first time*

**The first line and a small part of the third paragraph of this acknowledge text has to be in bold font/characters!**

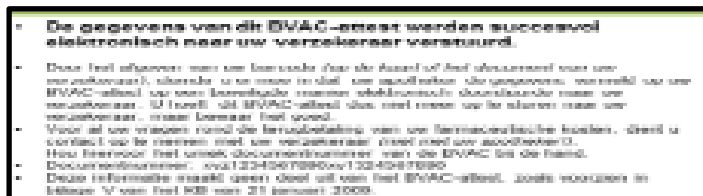
Nederlandstalige tekst van de acknowledge:

- **De gegevens van dit BVAC-attest werden succesvol elektronisch naar uw verzekeraar verstuurd.**
- Door het afgeven van uw barcode (op de kaart of het document van uw verzekeraar), stemde u er mee in dat uw apotheker de gegevens van uw aankoop op een beveiligde manier elektronisch doorstuurde naar uw verzekeraar.
- Voor al uw vragen rond de terugbetaling van uw farmaceutische kosten, dient u contact op te nemen met uw verzekeraar **(niet met uw apotheker!)**.  
Hou hiervoor het uniek documentnummer van de BVAC bij de hand.
- Documentnummer: 0054d2e1-d9c8-e42f-0c05-6fc417617e04 met de bijhorende barcode volgens barcode “code 128 or QR-code (ref. **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**/QR op pagina **Fout! Bladwijzer niet gedefinieerd.**)
- Deze informatie maakt geen deel uit van het BVAC-attest, zoals voorzien in bijlage V van het KB van 21 januari 2009.

Texte en Français de l’acknowledge:

- **Les données de cette attestation BVAC ont été transmises avec succès à votre assureur.**
- Par la remise de votre code-barres (sur la carte ou sur le document de votre assureur), vous avez marqué votre accord pour que votre pharmacien transmette à votre assureur, par voie électronique sécurisée, les données de votre achat.
- Pour toute question concernant le remboursement de vos frais pharmaceutiques, vous devez prendre contact avec votre assureur **(et non avec votre pharmacien !)**.  
Gardez à cet effet à portée de main le numéro de document unique de l'attestation BVAC.

- Numéro de document: 0054d2e1-d9c8-e42f-0c05-6fc417617e04 avec le code a barre correspondant «code 128/QR » (ref. **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**/QR, page **Fout! Bladwijzer niet gedefinieerd.**)
- Ces informations ne font pas partie de l'attestation BVAC telle que prévue à l'annexe V de l'AR du 21 janvier 2009.



- *Layout BVAC with additional information when printed second time like. This is the original layout as when the project started but with on top 'DUPLICATA'*

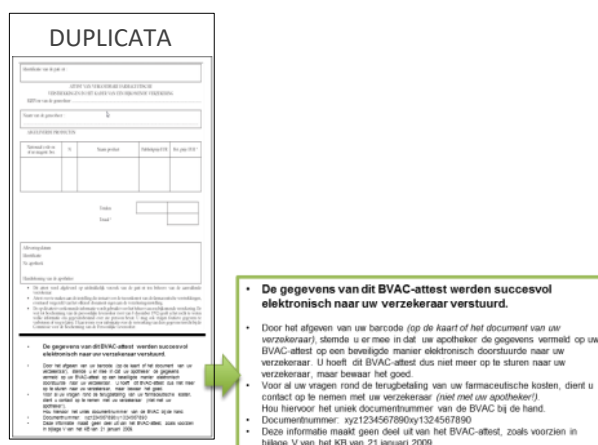
The first line and a small part of the third paragraph of this acknowledge text has to be in bold font/characters!

Nederlandstalige tekst van de acknowledge:

- **De gegevens van dit BVAC-attest werden succesvol elektronisch naar uw verzekeraar verstuurd.**
- Door het afgeven van uw barcode (op de kaart of het document van uw verzekeraar), stemde u er mee in dat uw apotheker de gegevens vermeld op uw BVAC-attest op een beveiligde manier elektronisch doorstuurt naar uw verzekeraar. U hoeft dit BVAC-attest dus niet meer op te sturen naar uw verzekeraar, maar bewaar het goed.
- Voor al uw vragen rond de terugbetaling van uw farmaceutische kosten, dient u contact op te nemen met uw verzekeraar **(niet met uw apotheker!)**.  
Hou hiervoor het uniek documentnummer van de BVAC bij de hand.
- Documentnummer: 0054d2e1-d9c8-e42f-0c05-6fc417617e04 met de bijhorende barcode volgens barcode "code 128/QR" (ref. 4.4 Code 128/QR op pagina 24)
- Deze informatie maakt geen deel uit van het BVAC-attest, zoals voorzien in bijlage V van het KB van 21 januari 2009.

Texte en Français de l'acknowledge:

- **Les données de cette attestation BVAC ont été transmises avec succès à votre assureur.**
- Par la remise de votre code-barres (sur la carte ou le document de votre assureur), vous avez marqué votre accord pour que votre pharmacien transmette à votre assureur, par voie électronique sécurisée, les données mentionnées sur votre attestation BVAC. Vous ne devez donc plus envoyer cette attestation BVAC à votre assureur, mais conservez-la bien.
- Pour toute question concernant le remboursement de vos frais pharmaceutiques, vous devez prendre contact avec votre assureur **(et non avec votre pharmacien !)**.  
Gardez à cet effet à portée de main le numéro de document unique de l'attestation BVAC.
- Numéro de document: 0054d2e1-d9c8-e42f-0c05-6fc417617e04 avec le code a barre correspondant «code 128/QR » (ref. 4.4 Code 128/QR, page 24)
- Ces informations ne font pas partie de l'attestation BVAC telle que prévue à l'annexe V de l'AR du 21 janvier 2009.



### 3.4.8 Real-time acknowledge or fall-back to paper BVAC

The connector module will process all BVAC Registrations in real-time. No off-line queue will be used. Within a default time-out of 10 seconds, an acknowledge will be given to the pharmacy software. In the case no acknowledgement is retrieved in “real-time”, the fall-back to ‘paper BVAC’ shall be used. The patient is informed.

De gegevens van dit BVAC-attest worden succesvol elektronisch naar uw verzekeraar verzonden.



### 3.4.9 Proof-of-activation registration

A specific registration to validate the activation of the solution at the pharmacy outlet will be provided. In essence, this is a registration to a fictive CBFA number for a fictive patient.

## 3.5 [ISV] Services offered by the multi-business connector extending the SMC with the BVAC flow

### 3.5.1 The Multi-business connector for pharmacies

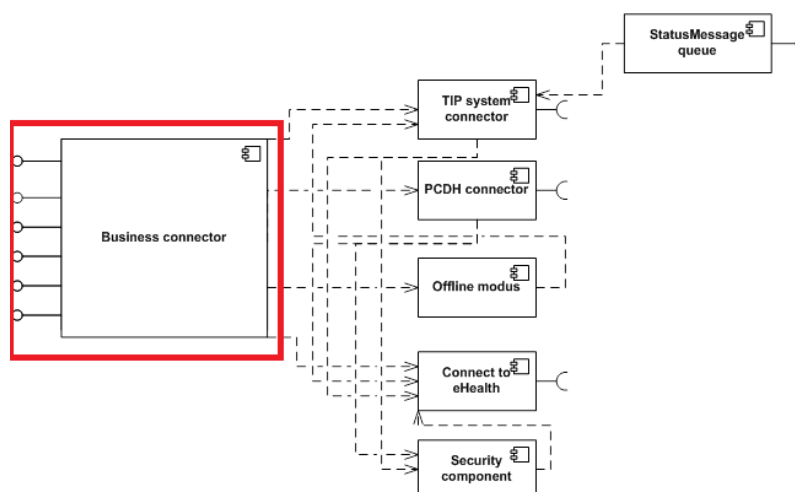


Figure 1 Multi-business connector for pharmacies.

A multi-business connector for pharmacies implements a secured and standardised registration capability also referred to as the single message concept. The registration itself makes use of an intermediate system referred to as the TIP – Trusted Intermediate for Pharmacies. In essence, the TIP offloads adaptive data qualification, routing flexibility, standards transformation and temporisation from the local pharmacy outlet.

### 3.5.2 *Connector specificities in view of supporting the BVAC data registration.*

For the registration of the BVAC related information, the solution extends the existing ‘registerdata’ with a specific registration of the BVAC data. Consequently, the impact on the connector is limited to

1. Support of extended single message (including BVAC event) for register data event. The register data function of the business connector supports validation for the XSD including the BVAC event.
2. Generation of unique BVAC document Id (UUID – 36 characters) to include in SMC BVAC event. This BVAC document id is returned to pharmacy software<sup>2</sup>.
3. Get System Configuration – CBFA number. The Get System Configuration call is extended with a list of the supported CBFA numbers by TIP (cf. Get Configuration for TIP Solution). This list needs to be cached in memory of connector module.<sup>3</sup>
4. Validation on CBFA number. The business connector function “register data” will include validation on CBFA number based on list retrieved in point 2<sup>4</sup>. When the CBFA number is not known in the pharmacy outlet, the pharmacist informs the patient to deliver the BVAC attest manually to the insurer as done nowadays.

### 3.5.3 *The offline component is not used for the BVAC event.*

In case of BVAC event, then the “register data” function in the business connector will directly make a call to TIP without going through the offline component. In case the TIP cannot be reached (for any possible reason), then the message is discarded (with an entry in local log) and the pharmacy software retrieves an error stating TIP not available and BVAC attest cannot be delivered electronically. In the latter case the pharmacist must tell to the patient to deliver the BVAC attest manually to the insurer as done nowadays.

### 3.5.4 *Get Configuration (System Services)*

The connector module will validate the CBFA number in the single message BVAC event provided by the pharmacy software. Only CBFA numbers that are available in the connector configuration will be accepted, otherwise an exception ‘invalid CBFA number’ is thrown to the ISV application.

The CBFA list in the connector module is provided by the TIP system as part of the existing “Get Configuration” service (existing TIP System Services).

The TIP System Services is an XML containing various configurations related to systems to which the connector module can connect. It contains e.g. system IDs, URL of webservices for systems, ..

For Assuralia, we add an optional contract list for a system (here TIP) to provide a list of parties (CBFAs of insurers) that participate to a specific contract (here BVAC). This CBFA list will be used by connector module to validate that TIP supports interaction with insurer for BVAC.

<sup>2</sup> Similar logic is applied as done for Dispensation GUID.

<sup>3</sup> In case a connector module is not yet upgraded to the latest version support new system configuration file, it will not fail but only skip the not yet known configuration fields in the system configuration file.

<sup>4</sup> In case CBFA number is not supported by TIP, an error ‘Insurer not supported, CBFA number unknown’ is thrown to pharmacy software and an entry is made in local log.

For the proper XML format, please refer to paragraph **Fout! Verwijzingsbron niet gevonden.. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd..**

For the connector, the CBFA list is requested to TIP on a daily basis at the start of the day, when the single sign-on session is started. It is part of the same 'full' system configuration message sent by TIP with TIP connection parameters during start-up.

## 3.6 [TIP] TIP administrative extension to support the BVAC.

### 3.6.1 *Insurer configuration on basis of their CBFA identification*

Insurers (or their subcontractors) need to be uniquely identified to the TIP system by means of:

- ☐ Name
- ☐ CBFA
- ☐ **Type of endpoint : ["HTTPS"; "SFTP"]** Please mind that for a transporter this indicates the method he can use to come and get the BVAC's, but that where the BVAC's are put (be it queue or SFTP directory) are decided by the endpoint type of the insurer for which the messages are meant
- ☐ For party doing transport: Transport key
- ☐ For insurer: Encryption key
- ☐ For insurer: Party able to access the (encrypted) messages for this insurer (i.e. the transporter)

The actual configuration upload is done by providing an xml file and placing it in the **/opt/users/weblogic/configuration/ASSURALIA/bvac** directory.

The xml file needs to correspond to xsd as specified in **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd.**<sup>5</sup>.

This configuration should be in line with the Assuralia Identification insurers as specified in **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd..** Any update or need for revision shall be requested to assurpharma@farmaflux.be.

**The configuration file is cached in the TIP during start-up.** The TIP Insurer Configuration is manually uploaded by the TIP configuration manager into the TIP system, and contains the CBFA list.

#### ➤ *Insurer switch from SFTP to Web Service*

Please be aware that an insurer can only start calling the Get BVAC web service when the TIP insurer configuration is adapted in the TIP by APB. As long as APB does not confirm the configuration change, the insurer will need to keep doing SFTP.

When an insurer switches from SFTP to Web Service, it can occur that there are still files present in the SFTP directory of the insurer. In this case it's up to the insurer to retrieve these files before they are deleted by the nightly deletion batch. Once a file has been created, it is no longer possible to retrieve the contained BVAC records by web service.

#### ➤ *Insurer public key localization for transport encryption*

For the connecting party (insurer or delegated company) willing to connect to the TIP system using web service, the connecting party needs to identify and authenticate himself:

<sup>5</sup> Please note the distinction between "end-insurer" and "transporter".

- ☐ For a web service based call an X.509 certificate is used and the public key is to be configured/localized by the TIP System.
- ☐ For the SFTP based call a ssh key (RSA 2048 bits) is used and the public part is to be configured/localized by the TIP system.

/opt/users/weblogic/configuration/certificates/assuralia/

### ➤ *Insurer public key localization for payload encryption*

All insurers willing to receive a BVAC message need to request an X.509 certificate from a valid certificate authority with a linked public /private key pair (2048 bits) and need to provide the public part to Farmaflux for configuration.

/opt/users/weblogic/configuration/certificates/assuralia/

### 3.6.2 *Directory localisation*

There is one output directory for each end-insurer willing to use SFTP, indicated by its CBFA number /<CBFA>/. These subdirectories are found in the same main directory (currently /opt/users/weblogic/configuration/assuraliasftp/). E.g.

BVAC extracts are placed in a specific directory. This directory is configured in the batch properties files (e.g. **batch-prod.properties**)

batch.assuralia.sftp.folder=/opt/users/weblogic/configuration/assuraliasftp/

Within this directory, we create a subdirectory per CBFA with the name of the subdirectory being the CBFA number

/opt/users/weblogic/configuration/assuraliasftp/<CBFA>

These sub directories do not need to be configured separately for the solution to be able to use them. If in the configuration xml an end-insurer with transport method SFTP is found, it looks at the properties file for the general directory and assumes there is a sub-directory with the CBFA as found in the configuration file.

### 3.6.3 *Batch localisation*

In total we have 3 batches foreseen for AssurPharma

- ☐ Extract batch, which extracts the BVAC messages for SFTP
- ☐ 'Sent' batch which checks if the SFTP messages have been retrieved and updates the status accordingly
- ☐ 'Deletion' batch which cleans the tables and potentially also files on filesystem
  - When the messages have been retrieved (web service or SFTP)
  - When a file has been on the file system for a certain period, and not yet picked up
  - When a message has been on new for a certain period, and not yet picked up

When these batches will be run, can be found in the **batch.properties** properties file. We have entries for all three batches.

- ☐ **Extract batch:** batch.AssuraliaSFTPExtractBatch.start and batch.AssuraliaSFTPExtractBatch.interval
- ☐ **Sent batch:** batch.SFTPSentBatch.start and batch.SFTPSentBatch.interval
- ☐ **Deletion batch:** batch.AssuraliaBatches.start and batch.AssuraliaBatches.interval

Note below that the extract is done 4 times per day, and the other ones only once per day. (start = start hour, interval = time between runs)

- batch.AssuraliaSFTPExtractBatch.start=3
- batch.AssuraliaSFTPExtractBatch.interval=6
- batch.SFTPSentBatch.start=3
- batch.SFTPSentBatch.interval=24
- batch.AssuraliaBatches.start=3
- batch.AssuraliaBatches.interval=24

The deletion batch also removes 'old' entries and files. Specifically we have two parameters in the **batch.properties** file which indicates after how many days this deletion can happen

- When a file has been on the file system for a certain period, and not yet picked up:  
batch.AssuraliaBatches.bvac.file.retention
- When a message has been on new for a certain period, and not yet picked up:  
batch.AssuraliaBatches.bvac.message.retention

batch.AssuraliaBatches.bvac.file.retention=141

batch.AssuraliaBatches.bvac.message.retention=141

### 3.7 [INSURER] Insurer data collection

The "Get BVAC DATA" service will allow Insurers to retrieve BVAC messages sent by pharmacies from the TIP system. The TIP will allow 2 mechanisms:

- ☐ Through web service
- ☐ Through sftp

#### 3.7.1 "Assuralia Table"

- The full BVAC Single message is **encrypted with the public certificate of the insurer** corresponding with the given CBFA number. Added to message in clear in XML are Pharmacy ID, CBFA number and Document Id.
- The Assuralia Table provides the following fields
  - **Id** : Oracle sequence
  - **Pharmacy**: pharmacy ID
  - **CBFA**: identifying insurer
  - **DocId**: BVAC document ID
  - **BVACmessage**: **encrypted** message content for insurer
  - **ReceivedDate**: current dateTime
  - **Status**: "New"
  - **StatusDate**: current dateTime
  - **FileName**: name of file in SFTP directory of CBFA

Assuralia	
PK	id
	Pharmacy ID
	CBFA
	DocId
	<b>BVACmessage</b>
	ReceivedDate
	Status
	StatusDate
	FileName

encrypted

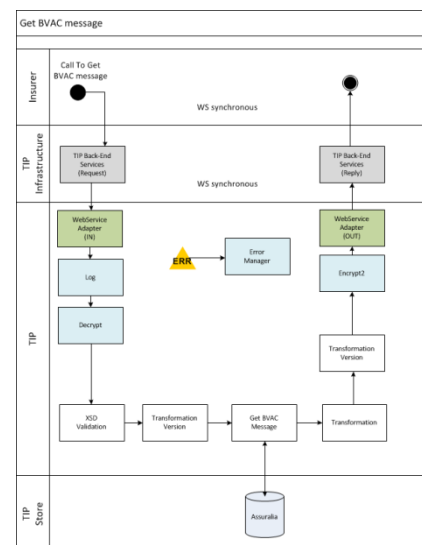


#### 3.7.2 Get BVAC through webservice

The Assuralia table is reachable through HTTPS for all authenticated insurers.

The Assuralia table is reachable through HTTPS for all authenticated insurers:

1. The webservice adapter gets the “get BVAC” message (**Fout! Verwijzingsbron niet gevonden.**)<sup>6</sup>
2. A log entry is made for auditing purposes
3. The request is decrypted for the TIP<sup>7</sup>.
4. The request is validated against an XSD
5. There is only one type of operation ‘getBVACMessage’. The service tag equals the WSDL operation value.<sup>8</sup>
6. An optional transformation to the latest XSD version is executed in case the insurer is not working on the latest XSD version on which the logic of TIP is built.
7. Aggregated messages of all available (‘New’) BVAC messages are retrieved from the Assuralia table based on the CBFA number in the request<sup>9</sup>.
  - The aggregated BVAC messages are formatted
  - The XSL file is optional depending on build.
  - An optional transformation occurs on the response from the latest XSD version to the XSD version of the calling insurer.
8. The FULL response is encrypted for the targeting insurer / AssurCard / ... with the proper public certificate.<sup>10</sup>
9. The response is returned to the insurer. A log entry is made in audit table to indicate that BVAC messages have been sent to CBFA.



### 3.7.3 Get BVAC through SFTP

The TIP system will extract 4 times per day all data from the Assuralia Table for every insurer that is configured with end-point-type = **SFTP** and where the Status of the BVAC Message is ‘New’.

This resulting list of BVAC messages are aggregated into a single file referenced as “BVAC-<CBFA>-<date>.xml” and put on the SFTP directory for the given CBFA: `(/opt/users/weblogic/configuration/assuraliasftp/<CBFA>)`

The file can then be picked up by an insurer through SFTP connection.

The access to the SFTP directories are configured on infrastructure to be only accessible by the authenticated insurer by verifying public key. The SSH public key (2048 bits) of the insurer is stored on TIP. The public/private key pair needs to be renewed every 3 years between TIP and Insurer through manual agreement between APB (Farmaflux) and Insurer (or AssurCard).

<sup>6</sup> Note that the calling party is here already authenticated & authorized to make this call via the TIP proxy.

<sup>7</sup> Note that the Insurer should have the TIP public key on its server to be able to encrypt the message. When the TIP public key is updated, the insurers should receive the updated version (manual intervention).

<sup>8</sup> The signature of the requestor is checked to ensure integrity of the request and validate public key.

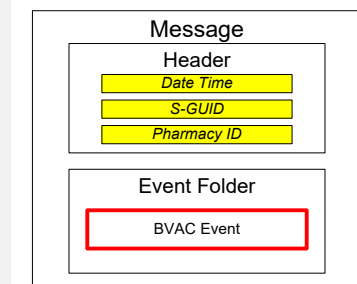
<sup>9</sup> A calling party can only pick up the BVAC messages to which it is authorized. This is checked through the **Fout! Verwijzingsbron niet gevonden.** TIP Insurer configuration and public key (validated in 4). If not an insurer (no CBFA number), the TIP will check if the calling party is available in the party list for the CBFA in the TIP Insurer Configuration, based on public key id, and as such is authorized to pick up the BVAC messages.

<sup>10</sup> Note that the encryption is not using eHealth, but will be a local encryption using the public key of the requestor (AssurCard, Van Breda, Insurer, ..) that is stored on the TIP.

The TIP SFTP setup will associate the user name of the insurer with the public SSH Key, so there is no need to each time enter a password. The data is transferred from TIP to Insurer through a secure channel (SSH-2) with data encryption based on a temporary agreed symmetric session key based on AES-192 algorithm.

The file format is XML and looks like:

```
<bvac-list>
<CBFA>0196</CBFA>
<bvac>
  <bvac-document-id>12345687987654321</bvac-document-id>
  <bvac-document>
    <!--ENCRYPTED (for Insurer corresponding with CBFA) -->
  </bvac-document>
</bvac >
<bvac >
  <bvac-document-id>12345687987654322</bvac-document-id>
  <bvac-document>
    <!-- ENCRYPTED (for Insurer corresponding with CBFA) -->
  </bvac-document>
</bvac >
...
</bvac-list>
```



## 4 Characteristics

### 4.1 Characteristics of the [Case Number] (dossiernummer ,numéro de dossier)

Members insurance companies each have their own format of the [Case Number] (dossiernummer ,numéro de dossier). To ensure correct reading of this [Case Number] (dossiernummer ,numéro de dossier) by the pharmacy software, a standard approach is agreed by all insurers who wish to participate in this project. **They shall use:**

Format: **14N**

- ☐ with the first four positions (4N), the official identification of the insurer (formerly known under the name CBFA number (eg AG-Ins., Ethias). DKV = 0739
- ☐ with the following 10 positions (10N) can be filled in "free" by insurers, with either the file or the extension number.
- ☐ with the last two positions (2N) preferred, but not mandatory, a check digit with a known algorithm (eg 97 -. Modulo 97) contain, in order to avoid incorrect (possibly manual) input a number.

Into the effectiveness of the solution to this [Case Number] (dossiernummer ,numéro de dossier)

- ☐ shall be readable by a bar code reader (read scan) in the pharmacy. Member insurers make the necessary efforts to uniformly (eg. Default location on a standardized type of letter) make available to the patient (eg. upon admission to the hospital) this barcode. Here we assume a linear Code 128 barcode or QR-code (see 4.4 Code 128/QR).
- ☐ The barcode will be accompanied by a character representation of the code. This serves as a fall back for the situations where the file cannot be scanned correctly.

### 4.2 Characteristics of the [Affiliation Number]

Members insurance companies each have their own format of the [Affiliation Number] (aansluitingsnummer, numéro d'affiliation). To ensure correct reading of this [Affiliation Number] (aansluitingsnummer, numéro d'affiliation) by the pharmacy software, a standard approach is agreed by all insurers who wish to participate in this project. **They shall use:**

Format: **14N**

- ☐ with the first four positions (4N), the official identification of the insurer (formerly known under the name CBFA number (eg AG-Ins., Ethias). Eg. DKV = 0739
- ☐ with the following 10 positions (10N) can be filled in "free" by insurers, with either the file or the extension number.
- ☐ with the last two positions (2N) preferred, but not mandatory, a check digit with a known algorithm (eg 97 -. Modulo 97) contain, in order to avoid incorrect (possibly manual) input a number.

Into the effectiveness of the solution to this [Affiliation Number] (aansluitingsnummer, numéro d'affiliation)

- ☐ shall be readable by a bar code reader (read scan) in the pharmacy. Members insurers make the necessary efforts to uniformly (eg. Default location on a standardized type of letter) make available to the patient (eg. upon

admission to the hospital) this barcode. Here we assume a linear Code 128 barcode or QR-code (see 4.4 Code 128/QR).

- ☐ The barcode will be accompanied by a character representation of the code. This serves as a fall back for the situations where the file cannot be scanned correctly.

### 4.3 Characteristics of the [Document Number] ( documentnummer, numéro de document)

---

The [Document Number] ( documentnummer, numéro de document) is a unique number over a period of 30 years, taking into account 2 million BVAC's per year in the early phase, and rising to a maximum of 240 million BVAC's.

The [Document Number] ( documentnummer, numéro de document) should be made available as a barcode under the Code 128/QR specification.

This document number adheres to the specifications of a UUID (more details can be found at wikipedia).

### 4.4 Code 128/QR

---

The Code 128 specification is an international barcode format that is supported by the barcode readers of the pharmacists. The barcode symbology is specified in ISO/IEC 15417:2007. The QR-code is a type of matrix barcode or two-dimensional barcode which is a newer type of barcode that is supported by the barcode readers of the pharmacist. Recommendations:

- ☐ Preferably subset is used
- ☐ Density: 0.250 mm.
- ☐ Hight: (at least) 10 mm
- ☐ Width: 45 mm wide.
- ☐ Both before and after the barcode there is an empty space of at least 2.5 mm.
- ☐ Below the barcode, the code number is displayed in Arabic numerals, the height of the figures being 2 mm and minimum 1 mm empty space is provided between the barcode and the code in numbers.
- ☐ This information is printed in black ink on a white background

### 4.5 Period of storage of encrypted data for the receiving insurer

---

The Segregated Storage serves primarily as a "buffer" or "temporary storage" of the BVAC data. Each insurer will collect these data on a frequent basis.

(Refer configuration at the TIP: **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd.**)

# 5 Services, Messages and Data Formats

## 5.1 Single Message – the basics

The single message format is an XML specification used to communicate/collect information from and to the pharmacy outlet.

The message structure contains a *hierarchy of events and entities in its body*.

- ❑ **Events** embody specific **datasets exchanged with the pharmacy outlet**.
- ❑ **Entities** are the **data objects** manipulated by or associated with events.
  - *These are either part of, or referenced by, events.* The latter is preferred if multiple events reference the same entity.

The following simplified diagram contains *fictional* elements to illustrate the difference between *events* and *entities*. In this case, a revocation is an event that references a dispensation delivery.

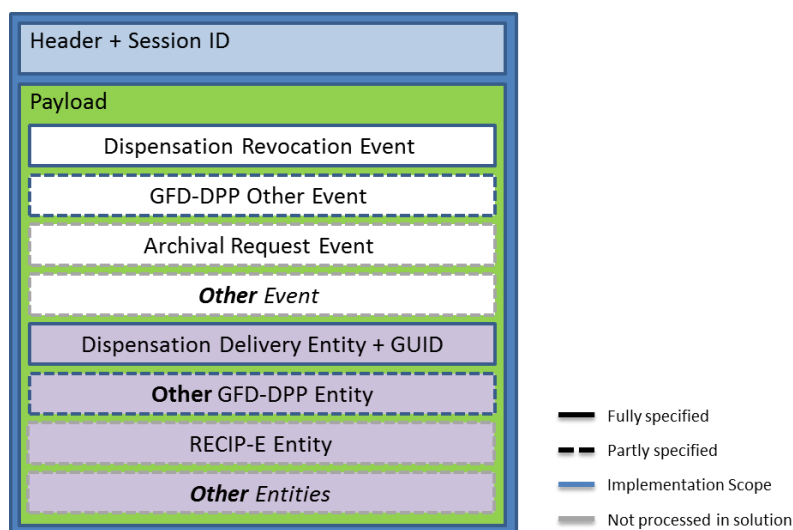


Figure 2 - Single Message hierarchy overview

Details on the SMC and the revisions hereof are maintained at paragraph **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd..**

## 5.2 BVAC Event Type – vehicle for sending the BVAC data

This single message concept [SMC] has incorporated the “BVACEventType” as a vehicle for sending the BVAC data.

### 5.2.1 Message structure of the SMC supporting the BVAC EventType

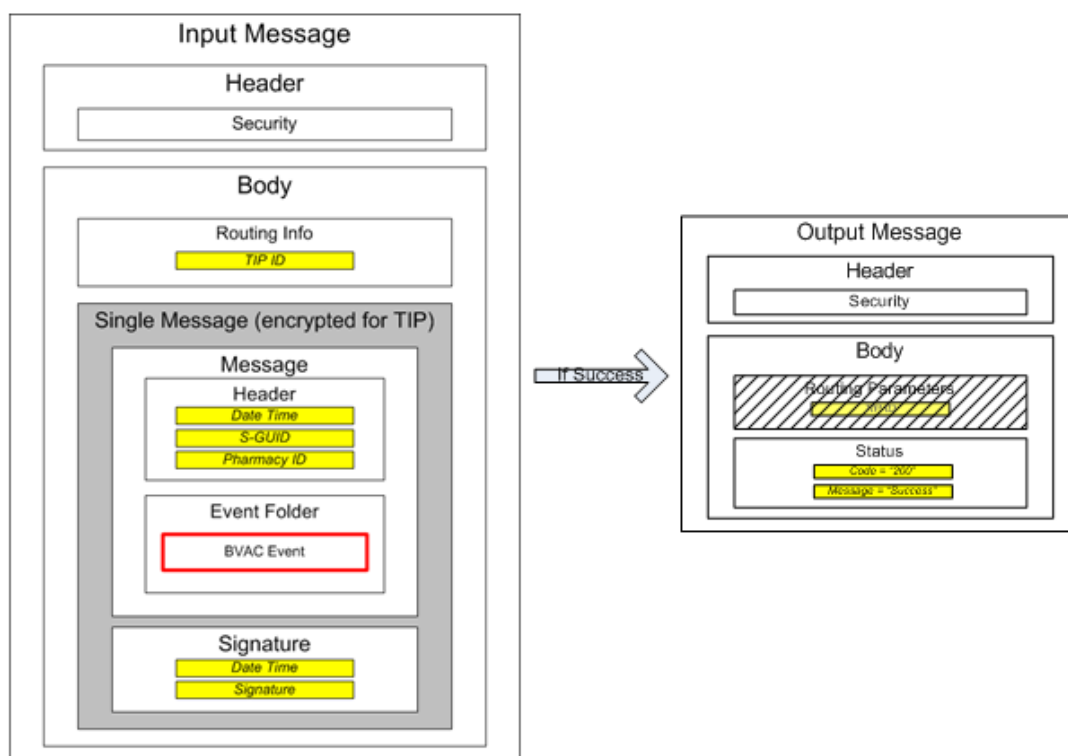


Figure 3 – Single Message and BVAC Event Type

### 5.2.2 Unique identifiers

2 fields of note are the **S-GUID** and the **BVAC Document Id**. Both are auto-generated and unique id's across the pharmacies, TIP System and insurer.

- ❑ **S-GUID**: the S-GUID is used for end-to-end traceability across any type of message passing the TIP system
- ❑ **BVAC Document ID**: the BVAC document Id is particular to the BVAC message flow.

One S-GUID exists per single message and one BVAC document id exists per BVAC message. Since a single message only contains one BVAC document id, there is also a 1 to 1 mapping between both ids, but this cannot be taken as a fixed assumption, since in the future a different setup with more than 1 BVAC message per Single Message could be envisioned.

The insurer is requested to also keep both the S-GUID and BVAC Document ID when processing the BVAC messages.

An additional field is also added on request of the insurers **BvacInternalReference** this is an optional field that can be filled in by the software vendor with an internal referencenumber of every sale.

- ❑ BVAC Internal reference: the BVAC Internal reference shall be the RID in case a dispensation is related to an electronic prescription. In the case the dispensation is not related to an electronic prescription, the internal unique reference number to the sale shall be used.

### 5.2.3 BVAC Event structure – xsd

We distinguish the following event structures

- ❑ Event structures between the pharmacy outlet and the TIP (Refer to **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd.** for all xsd formats. )
- ❑ Event structures between the TIP and the insurer (Refer to **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd.**)

## 5.3 BVAC Document – payload data

---

### 5.3.1 BVAC Document Definition

In the diagrams below, the graphical conventions are:

- ❑ yellow for a data field;
- ❑ white blocks indicate composite elements;
- ❑ striped blocks are optional fields not filled in the shown exchanged message.

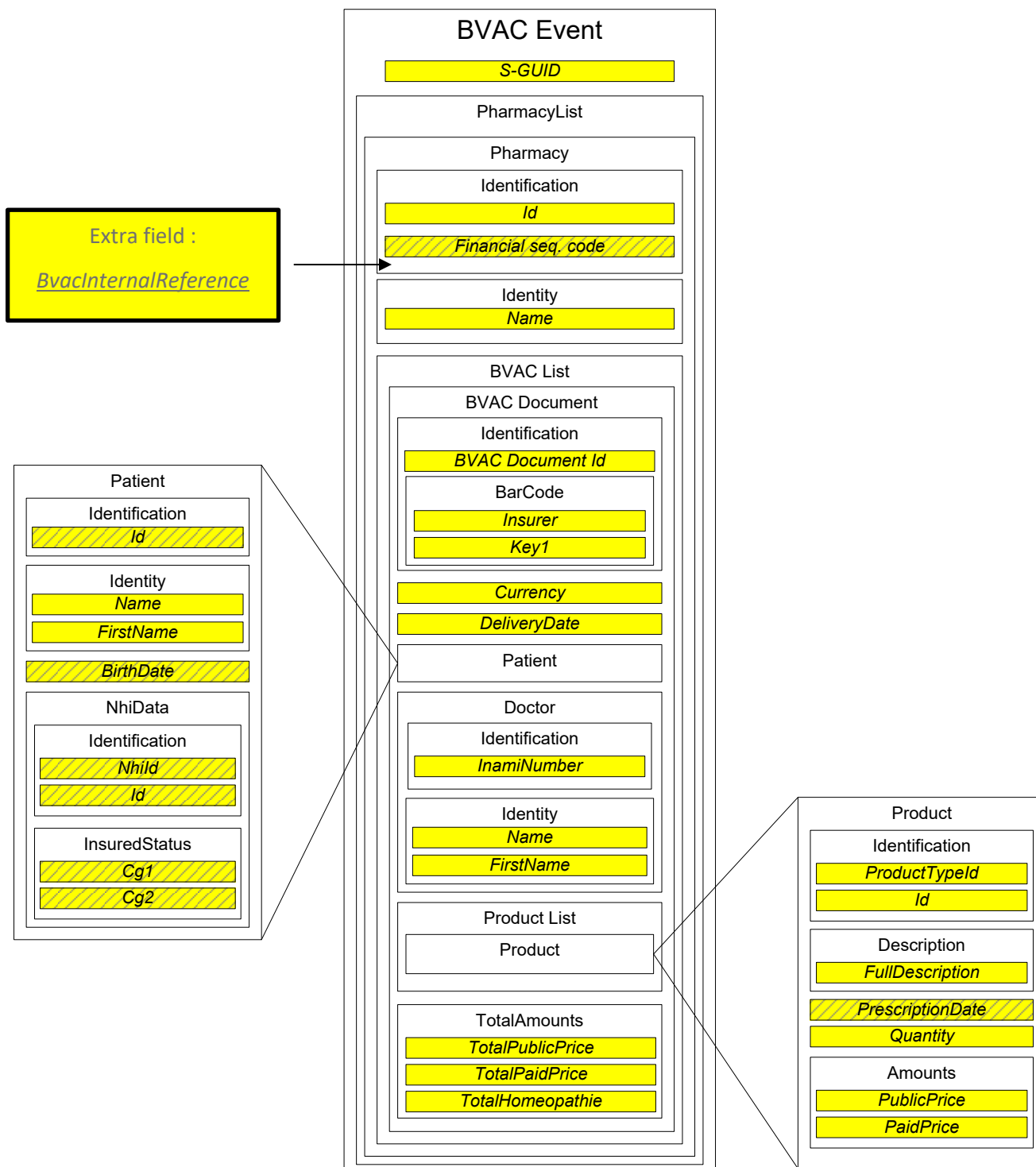


Figure 4 BVAC Document Definition

### 5.3.2 BVAC Document – Message Format

- ❑ **Description:** details on the message format and the revisions hereof are maintained at paragraph **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd..**
- ❑ **Xsd:** structure on the message format and the revisions hereof are also maintained at paragraph **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd..**

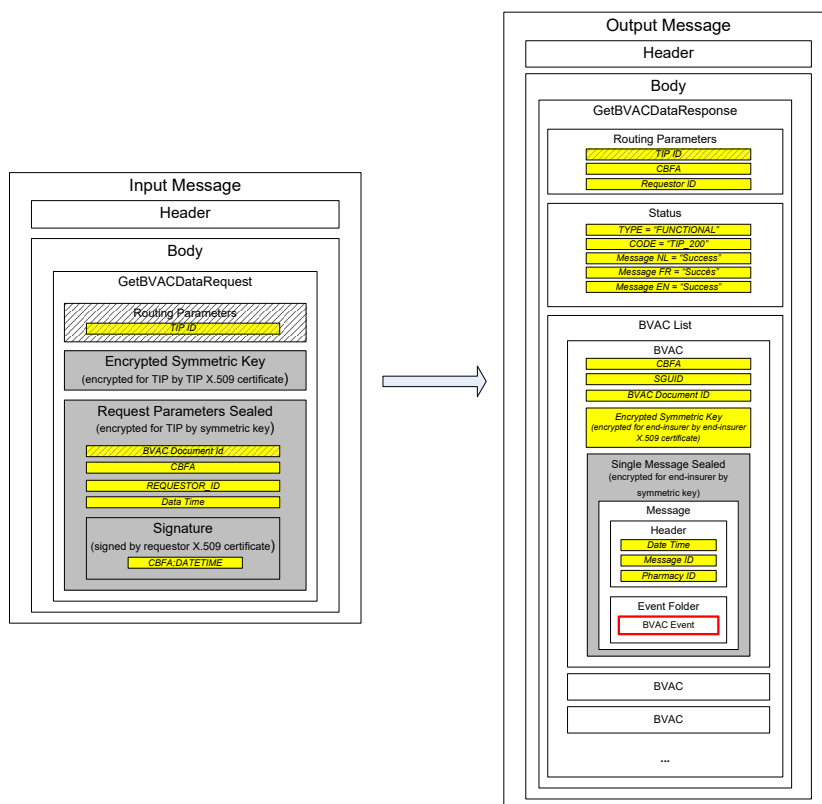
## 5.4 Webservice “get BVAC” and response Message format

(Figure 5 – Webservice Get BVAC messages)

The grey box means that this content is in encrypted format. This means that the request parameters, the symmetric key and the single message only appear in encrypted (sealed) format.

In the input message, the structure ‘routing parameters’ is optional (see the dashed box). It is foreseen for future extension sake. This means that you do not have to provide this structure. However, if you do provide it, it should contain the CBE number to which the TIP system public key belongs (i.e. 0406753266 at the writing of this document).

In the output message, the field TIP ID in the routing info is optional (see the dashed box). It is foreseen for future extension sake. Currently it will not be returned.



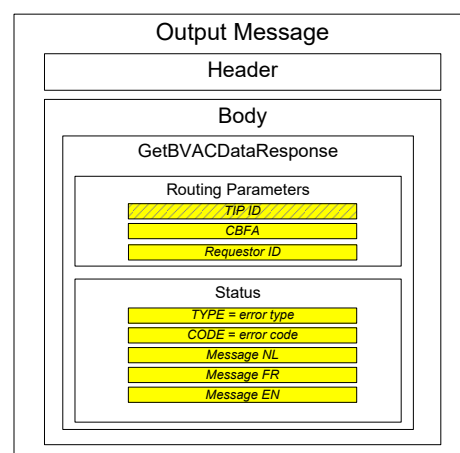
The output message contains a BVAC list, which contains a number of BVAC structures.

Each BVAC structure, contains one single message structure (see 5.1 Single Message), which in its turn contains one BVAC event (see 5.2 BVAC Event), which contains one BVAC document.

The output message always contains a success or error message, together with the error text in Dutch, French and English.

More details can be found in paragraph **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd..**

If error



(Figure 6 - Error response structure)

## 5.5 Sftp “get BVAC” and response Message format

On the TIP system, there is one output directory for each CBFA

The file name of the nightly extracts, is *BVAC-<CBFA>-<datetime>.xml* where <CBFA> is the CBFA number of the insurer and <date> is the datetime of the extract.

E.g. for the party x as in our previous example, you could have following files (assuming the files where not retrieved in the past 2 days).

/3333/BVAC-3333-20130819

233252.xml

/3333/BVAC-3333-20130820 233012.xml

The file format is XML and has following structure:

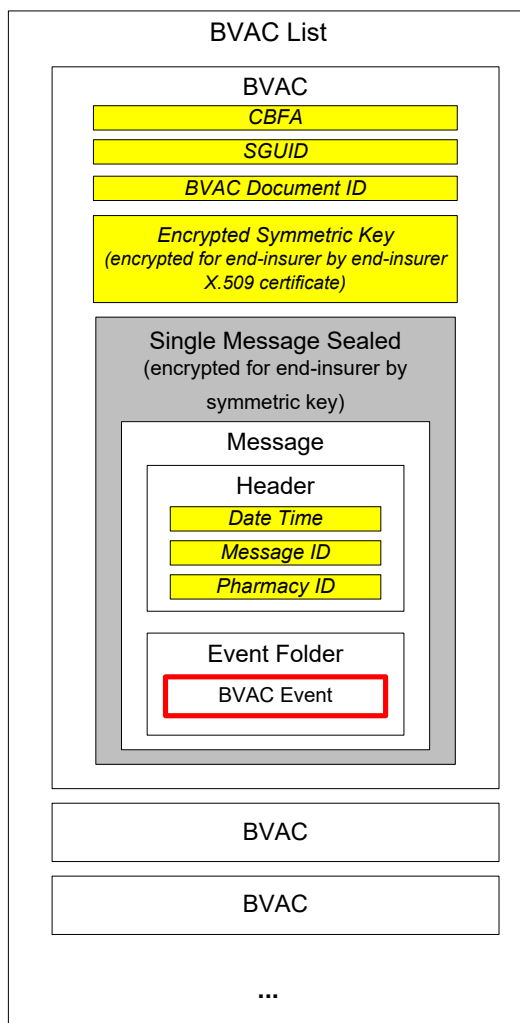


Figure 7 – SFTP XML file structure

An example file would be:

```
<BvacList>
  <Bvac>
    <CBFA>5000</CBFA>
    <SGUID>sguid_1</SGUID>
    <BvacDocumentId>document_1</BvacDocumentId>
    <EncryptedSymmetricKey>VGhpcyBpcyBhbiBlbmNyeXB0aW9uIGtleQ==</EncryptedSymmetricKey>
    <SingleMessageSealed>VGhpcyBpcyBhbiBub3QgZW5jb2RlZCBidmFjIG1lc3NhZ2U=</SingleMessageSealed>
  </Bvac>
  <Bvac>
    <CBFA>5000</CBFA>
    <SGUID>sguid_1</SGUID>
    <BvacDocumentId>document_1</BvacDocumentId>
    <EncryptedSymmetricKey>VGhpcyBpcyBhbiBlbmNyeXB0aW9uIGtleQ==</EncryptedSymmetricKey>
    <SingleMessageSealed>VGhpcyBpcyBhbiBub3QgZW5jb2RlZCBidmFjIG1lc3NhZ2U=</SingleMessageSealed>
  </Bvac>
</BvacList>
```

Please mind that:

- This structure is exactly the same as the inner structure returned via the web service (also see the xsd's provided in the chapter on webservice)
- This file contains multiple 'Single Messages', namely one per BVAC document.
- The S-GUID and Document ID are present in the file for easy reference

# 6 Integration guidelines for the ISV application

## 6.1 The identification of the patient with regards to the private insurer

The use of the NISS number is not authorized for private insurers. Hence the identification of patient with regards to the AssurPharma project is based on the following:

- ☐ Identification based on an assigned [**casenumber**]
- ☐ Identificatie op basis van een aansluiting bij een privé-verzekeraar [Affiliation Number] (aansluitingsnummer, numéro d'affiliation)

If the patient does not possess any of the above numbers, no electronic BVAC will be sent.

The software will be capable of capturing this number (via manual input or through reading of the barcode) and to split it up in the CBFA number (first 4 numbers) and patient ID (last 10 numbers)

**This number will not be stored persistently.**

## 6.2 Creation of the BVAC attestation

On demand of the patient the pharmacist will be responsible for issuing a BVAC attestation.

This question triggers the following actions in the pharmacy:

1. The software collects the necessary data
2. The software processes the encoded data in a Single Message (BVAC-event) and executes a RegisterData using the Multi-Business Connector

Attention: only 1 BVAC document per single message!

3. When the event has successfully been sent to the TIP, a unique document id (UUID) will be generated by the Multi-Business Connector. The software provides a time-out: if no answer is received from the TIP in a predefined time period then the software package will continue handling the BVAC event on paper. If this is the case, the pharmacist will be notified.
4. Only the confirmation of the treatment by the back-end system will be printed out and handed to the patient.
5. If the patient desires a duplicate then, as initially foreseen, a BVAC attestation with the supplementary information is printed out and handed to the patient. This duplicate will clearly mention "DUPLICATA" on top.

# 7 Integration guidelines for integrating the multi-business connector

Assumed as common expertise at the ISV.

# 8 TIP configuration guidelines.

## 8.1 SFTP Server configuration

Besides the general configuration, there is also a specific setup needed to be able to use SFTP.

- Credentials for parties willing to connect to the SFTP server (transporters) need to be configured
- The correct link directory – authenticated party needs to be made

### 8.1.1 Authentication

The party (insurer or other company) willing to connect to the TIP system using SFTP is required to create a ssh certificate (RSA 2048 bits) and needs to provide the public part to the TIP System at configuration. This SSH certificate is used for setting up the SSH session with the file server uses the SSH certificate (so not username/password). The public part of the certificate needs to be provided to the hosting partner (or APB) who will make the necessary configurations in the SFTP server.

### 8.1.2 Authorization

The correct directory needs to be associated to the correct user on the filesystem (see section on authentication). Specifically, each transporter needs to have access (read and write on files in that directory) to the directories of the parties for which he can transport BVAC messages, and cannot have access to any other files or directories. This needs to be configured by the hosting partner (or APB) depending on the setup of the SFTP and filesystem.

### 8.1.3 Authentication & secure message transfer

The access to the SFTP directories are configured on infrastructure to be only accessible by the authenticated insurer by verifying their public key. The TIP SFTP setup will associate the Username of the insurer with the SSH Key. The data is transferred from TIP to Insurer through a secure channel (SSH-2) with data encryption based on a temporary agreed symmetric session key based on AES algorithm.

### 8.1.4 Connection Parameters

The IP addresses to connect to the SFTP for each environment:

- ☐ Acceptance: IP Addresses: 81.247.254.229 - Port: 22
- ☐ Production: IP Addresses: 81.247.254.84 - Port: 22

### 8.1.5 Technical Registration

#### ➤ Insurer information

In order to allow access to the TIP system to retrieve BVAC messages, the insurer or party retrieving messages for an insurer, needs to provide a number of technical configuration parameters:

- Name
- CBFA number (if insurer)
- End-point-type: SFTP or HTTPS (i.e. web service)
- SSH key or X.509 Certificate used for transport (public part)

- X.509 Certificate used for encryption (public part)
- A delegation list of parties that may retrieve BVAC messages for this insurer
- For SFTP: the IP addresses of the servers going to access the SFTP
- 
- Depending on the setup one of both the certificates need to be provided
  - An insurer retrieving its own messages needs to provide both certificates
  - An insurer which has another party retrieving its messages (delegator) only needs to provide the encryption certificate
  - A party retrieving messages for insurers (delegate), only needs to provide the transport certificate
- 
- Please note that it can take 2-3 days to activate a new party, so do not delay in requesting the different certificates from your CA of choice.
- Please note that for the Acceptance and Production environment other certificates have to be used to maximise security.
- 
- Note on switching from SFTP to web service
- An insurer is expected to choose or SFTP or Web service. In the case where an insurer wishes to switch from SFTP to Web service, please mind that
- An insurer can only start calling the Get BVAC web service when the insurer configuration is adapted in the TIP System by Farmaflux. As long as Farmaflux does not confirm the configuration change, the insurer will need to keep doing SFTP.
- Once a file has been created for SFTP, it is no longer possible to retrieve the contained BVAC records by web service so when an insurer switches from SFTP to Web Service, it can occur that there are still files present in the SFTP directory of the insurer. In this case it's up to the insurer to retrieve these files before they are deleted by the nightly deletion batch which deletes files if they are older than a certain number of days (see section 0 Retention period)

#### ➤ *Delegation of retrieval of BVAC messages*

An insurer can delegate the retrieval of its BVAC messages to one or more insurers, or in general other parties having a CBFA number. E.g. Assurcard has a number of Insurers for which it can retrieve BVAC messages.

Both parties (delegator and delegate) need to have passed the technical registration, and for both parties the respective public keys need to be known (for the delegator this is the encryption key, for the delegate this is the transport key).

This list of parties to which it delegates, is communicated by the delegator (i.e. the end-insurer) at the time of technical registration.

Retrieval of the BVAC messages is transparent for a non-delegated party as for a delegated party:

Authentication and authorization of the requestor is done on the basis of the transport public/private key-pair of the requestor.

In the request it is specified for which end-insurer the BVAC messages are meant.

The distinct BVAC messages are encrypted (message by message) by the encryption public key of the end-insurer

Important for this setup is also that it is possible (in theory) that multiple parties are allowed to retrieve BVAC messages for one end-insurer. This retrieval happens on a first-come-first-served basis. If one party with access

to the messages has retrieved them, then a second party which also has access to these messages will no longer find them on the TIP System.

### ➤ *An example to clarify*

Assume we have a party A which retrieves BVAC messages for parties x and y. For completeness sake, we also have insurers S and T retrieving their own messages.

During the technical setup, we will have following information

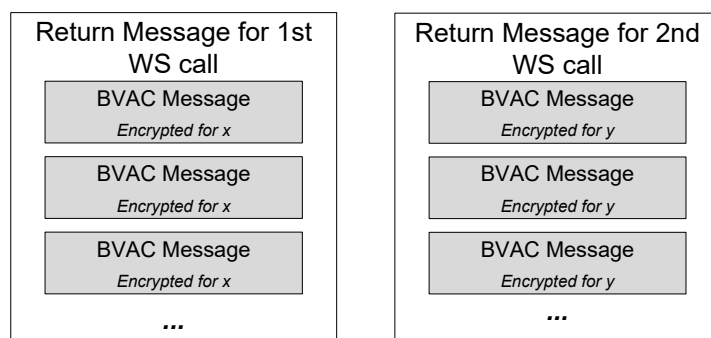
Name	CBFA	End-point-type	Public Key for transport	Public Key for encryption	Accessible by
A	-	HTTPS	@transport key A@	-	-
X	0001	HTTPS	-	@encryption key x@	A
Y	0002	HTTPS	-	@encryption key y@	A
S	0003	HTTPS	@transport key S@	@encryption key S@	S
T	0004	SFTP	@transport key T@	@encryption key T@	T

**Table 1 - Example technical registration parameters**

When party A wants to retrieve the BVAC messages for both x and y, he sets up an HTTPS session with the TIP system checking the connection against the SSL certificate of the TIP system

Sends two requests (i.e. 2 webservice calls), one for CBFA 0001 and one for CBFA 0002. Each request is signed with its private key (@transport key A@)

Two return messages are returned, each containing a number of BVAC messages, with each BVAC message encrypted with the public keys of the end-insurers (@encryption key x@ & @encryption key y@)



**Figure 8 - Example encryption in context of delegation**

# 9 Integration guidelines for the BVAC retrieval

- The “Get BVAC DATA” service will allow to retrieve BVAC messages sent by pharmacies from the TIP system.
- The TIP System allows 2 mechanisms:
  - ❑ **SFTP:** The TIP System provides file access to the BVAC messages by means of SFTP over SSH.
  - ❑ **Webservice:** The TIP System exposes a standard web service that allows access of the BVAC messages for a particular Assuralia member.

Both options imply that some technical processing must be performed on client side (such as encryption/decryption, setting up a SSH connection for SFTP, ...). This technical processing must be implemented by the insurers.

## 9.1 Authentication & encryption – securing the transport

### 9.1.1 [Web-Service] Insurer X.509 Certificate for transport

#### ➤ Context

The party (insurer or delegated company) willing to connect to the TIP system using web service is required to request an X.509 certificate from a valid certificate authority with a linked public / private key pair (2048 bits) and needs to provide the public part to the TIP System for configuration.

The certificate + public/private key pair is expected to be renewed every 3 years between TIP and Insurer through manual agreement between APB (Farmaflux) and Insurer (or AssurCard). Preferably the certificate is organisational.

This Transport X.509 certificate is used by the “*get BVAC data request*”. The message is signed with the X.509 certificate of the requestor, which is checked by the TIP System.

The insurer willing to use the web service, should have the TIP System public key on its server. This is provided by Farmaflux at time of configuration and is valid for a period of 3 years. 3 months before the end of the 3 year period, the insurer will be provided with a new public key.

It is used for the *get bvac data* web service request message which needs to be encrypted with the public key of the TIP System

#### ➤ Usage

A HTTPS session is setup by the insurer using the TIP systems SSL certificate.

Further authentication is done by signing of request messages with the own private key to allow the TIP System to validate the originator of the message.

The BVAC messages are reachable through HTTPS for all authenticated insurers.

1. Calling party sets up a HTTPS connection to the TIP System using the TIP system SSL certificate

2. Calling party creates and sends a request message, containing
    - An AES-256 symmetric key, encrypted with the public key of the TIP system (Algorithm: RSA/ECB/PKCS1Padding)
    - Request parameters encrypted with said symmetric key, and containing
      - ⇒ CBFA number for which the BVAC messages need to be retrieved
      - ⇒ REQUESTOR\_ID of the party doing the transport (i.e. the CBFA number of simply "ASSURCARD" for Assurcard)
      - ⇒ Date-time in format yyyy-MM-ddTHH:mm:ss.fffz (UTC TimeZone)
      - ⇒ Signature: concatenation of the CBFA number ";" and the date-time (in format ddMMyyyyHHmmss. UTC (E.g. 17102013110341) ), signed with the private key of the calling party (e.g. 5000;17102013110341)
  3. TIP System checks the request message
    - Decrypts the symmetric key with the private key of the TIP system (Algorithm: RSA/ECB/PKCS1Padding)
    - Decrypts the request parameters with said symmetric AES key
    - Checks the signature against the transport public key of the calling party
    - Checks if the calling party has access to the BVAC messages of the CBFA indicated in the request message (using the parameters provided during technical registration)
  4. TIP System creates a return message
    - Retrieves the BVAC messages for the CBFA indicated. These are each in its turn already encrypted with the encryption public key of the insurer to which the CBFA number belongs
    - Puts these BVAC messages (single message format) together in an aggregated BVAC List
    - Encrypts the BVAC list with a generated AES-256 symmetric key
    - Encrypts the symmetric key with the transport public key of the calling party and adds it to the BVAC
    - Returns the BVAC list
  5. Calling party treats the return message. Depending on the setup:
    - ⇒ In the case where the decryption private key of the delegator is kept at the delegate: Decrypts the individual BVAC messages with the decryption private key linked to the insurer for which the messages were requested
    - ⇒ In the case where the decryption private key of the delegator is not kept at the delegate: Passes along the BVAC messages to the delegator for which it retrieved the message. This delegator party is then responsible for decrypting the individual BVAC messages with its decryption private key.
- Refer to paragraph 5.4 Webservice "get BVAC" and response Message on page 29 for details on the message itself.

#### ➤ WSDL and XSD

Format of WSDL and corresponding XSD's for the get bvac data web service:

- ❑ WSDL of the get bvac data web service can be found at:  
<https://acc-tip.gfd-dpp.be/be-apb-gfddpp-services-TIPSystem/ASSURPHARMATIPSystemServices?wsdl> Do refer to paragraph **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd.** for the applicable revisions.
- ❑ Xsd of the webservice ([..\ASSURPHARMA - xsd\PanoramixTIPSystemServices\\_protocol-1\\_0.xsd](#))

- ❑ Xsd of the encrypted part of the request parameters. ([..\ASSURPHARMA - xsd\assuralia-request-parameters-v20130916.xsd](#))

### ➤ *Sample input and output message*

The input message contains request parameter, which are sealed with a symmetric key, after which the symmetric key is also sealed on its turn by the public key of the TIP System. Some samples are provided:

- ❑ A sample xml of the request parameters before sealing with the symmetric key ([..\ASSURPHARMA - xsd\GetBvacData-request-not-encrypted-parameters-example.xml](#))
- ❑ A sample xml of the total input message, after sealing the request parameters. We also included the optional routing parameters. ([..\ASSURPHARMA - xsd\GetBvacData-request-example.xml](#))
- ❑ A sample xml of the output message ([..\ASSURPHARMA - xsd\GetBvacData-response-example.xml](#))

## 9.1.2 *[SFTP] Insurer SSH key for transport (for SFTP)*

### ➤ *Context*

The party (insurer or other company) willing to connect to the TIP system using SFTP is required to create a ssh key (RSA 2048 bits) and needs to provide the public part to Farmaflux for configuration.

This SSH key is used setting up the SSH session with the file server combined with the Username Farmaflux will provide. The username is referenced in **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** on page **Fout! Bladwijzer niet gedefinieerd.**

The insurer willing to use the web service, should have the TIP System SSL certificate installed on its server. This is provided by Farmaflux at time of configuration and is valid for a period of 1 year. Between a period of 3 to 1 month before the end of the year, the insurer will be provided with a new public key.

This SSL certificate is used to setup the HTTPS session.

Besides the general configuration, there is also a specific setup needed to be able to use SFTP.

- Credentials for parties willing to connect to the SFTP server (transporters) need to be configured
- The correct link directory – authenticated party needs to be made

**Authentication:** The party (insurer or other company) willing to connect to the TIP system using SFTP is required to create a ssh certificate (RSA 2048 bits) and needs to provide the public part to the TIP System at configuration. This SSH certificate is used for setting up the SSH session with the file server uses the SSH certificate (so not username/password). The public part of the certificate needs to be provided to the hosting partner (or APB) who will make the necessary configurations in the SFTP server.

**Authorization:** The correct directory needs to be associated to the correct user on the filesystem (see section on authentication). Specifically, each transporter needs to have access (read and write on files in that directory) to the directories of the parties for which he can transport BVAC messages, and cannot have access to any other files or directories. This needs to be configured by the hosting partner (or APB) depending on the setup of the SFTP and filesystem.

**Authentication & secure message transfer** The access to the SFTP directories are configured on infrastructure to be only accessible by the authenticated insurer by verifying their public key. The TIP SFTP setup will associate the Username of the insurer with the SSH Key. The data is transferred from TIP to Insurer through a secure channel (SSH-2) with data encryption based on a temporary agreed symmetric session key based on AES algorithm.

**Retention period** The messages are kept on the queue / on the file server for a configurable period which is currently set at 14 calendar days. If a message is still on the queue or on the file server after 14 calendar days have passed, they will be deleted by a deletion batch at night.

### ➤ Usage

The TIP system will have a 4-daily “BVAC extract” batch that will extract all BVAC messages for every insurer that is configured with end-point-type = SFTP. The distinct BVAC messages are encrypted with the encryption public key of the target insurer and grouped into an aggregate file per CBFA

The retrieving party sets up an SFTP connection to the TIP System file server using its SSH key and the Username provided by Farmaflux

The TIP System file server only allows access to the directories belonging to the insurers for which the retrieving party has access (using the parameters provided during technical registration)

The file can then be picked up by the retrieving party through SFTP connection

After successful retrieval of the file, the retrieving party is expected to delete the file. This indicates to the TIP System that the retrieval was a success.

1. Depending on the setup, the calling party
  - a. In the case where the decryption private key of the delegator is kept at the delegate:
    - i. Decrypts the symmetric key (AES-256) with the decryption private key linked to the insurer for which the messages were requested
    - ii. Decrypts the individual BVAC messages using the provided the symmetric key
  - b. In the case where the decryption private key of the delegator is not kept at the delegate:
    - i. Passes along the BVAC messages to the delegator for which it retrieved the message. This delegator party is then responsible for decryption



- Please mind that since we do not know which party will be retrieving the file, we cannot encrypt the aggregate message. Only the individual messages out of which the aggregate message is made up, are encrypted.



### ➤ Connection Parameters

The IP addresses to connect to the SFTP for each environment: (NSLOOKUP tip.gfd-dpp.be )

- ☐ Acceptance: IP Addresses: 213.181.53.27
- ☐ Production: IP Addresses: 213.181.53.28



## 9.2 Authentication & encryption – encrypting the payload

On top of the public/private key pair used for transport, there is an additional public/private key pair for encrypting the message for the insurer.

All insurers willing to receive a BVAC message need to request an X.509 certificate from a valid certificate authority with a linked public /private key pair (2048 bits) and need to provide the public part to Farmaflux for configuration.

The certificate + public/private key pair is expected to be renewed every 3 years between TIP system and Insurer through manual agreement between Farmaflux and Insurer (or AssurCard). Preferably the certificate is organizational.

- This X.509 certificate is used differently depending on the chosen transport approach:
  - ❑ For SFTP based BVAC Request, the content of the file found, is encrypted with the public key of the end-insurer and needs to be decrypted by its private key
  - ❑ For Web service based BVAC request, the web service return messages are encrypted with the public key of the end-insurer and need to be decrypted by its private
- 
- For an insurer that retrieves its own BVAC messages, the transport and encryption certificates can in fact be the same certificate. It is up to the insurers to decide if they are willing to use the same certificate.

# 10 FAQ & Code snippets

## 10.1 Convention on the Date-Time format

When creating the signature it's important to have the correct date structure.

- Date-time in format yyyy-MM-ddTHH:mm:ss.fffzzz (UTC TimeZone) (e.g. 2013-11-08T12:14:47.495Z)
- Signature: concatenation of the CBFA number “;” and the date-time (in format ddMMyyyyHHmmss. UTC(E.g. 17102013110341)), signed with the private key of the calling party (e.g. 5000;17102013110341)

## 10.2 .net

### 10.2.1 PKCS# padding

For the RSA encryption/decryption it's important to force PKCS# padding. Snippet below:

```
RSACryptoServiceProvider rsaPublicKeyEncryptor = ((RSACryptoServiceProvider)publicKeyCert.PublicKey.Key
byte[] encryptMessage = rsaPublicKeyEncryptor.Encrypt(Encoding.UTF8.GetBytes("Hello world"), false);
```

### 10.2.2 What is the size of IV for the AES encryption?

16 Bytes (256bits). Because the IV vector is needed some extra steps are needed for the encryption. The first 16Bytes of the sealed message are reserved for the IV.

### 10.2.3 How to initialize the vector?

```
byte[] ivArr = { 1, 2, 3, 4, 5, 6, 6, 5, 4, 3, 2, 1, 7, 7, 7, 7 };
byte[] IVBytes16Value = new byte[16];
Array.Copy(ivArr, IVBytes16Value, 16);
var keyBytes = new byte[32];
var secretKeyBytes = Encoding.UTF8.GetBytes(secretKey);
Array.Copy(secretKeyBytes, keyBytes, Math.Min(keyBytes.Length, secretKeyBytes.Length));
return new RijndaelManaged {
    Mode = CipherMode.CBC,
    Padding = PaddingMode.PKCS7,
    KeySize = 256,
    BlockSize = 128, //256,
    Key = keyBytes,
    IV = IVBytes16Value
};
```

## 10.3 Java

### 10.3.1 What is the algorithm used to verify the signature?

```
Signature signature = Signature.getInstance("SHA1withRSA");
```

### 10.3.2 How to AES encrypt?

```
public byte[] encryptAes(byte[] dataToEncrypt, SecretKeySpec aesKey) {
    byte[] encryptedData = null; byte iv[] = new byte[16];
    SecureRandom random = new SecureRandom();
    random.nextBytes(iv);
    IvParameterSpec ivspec = new IvParameterSpec(iv);
    Cipher aesCipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    aesCipher.init(Cipher.ENCRYPT_MODE, aesKey, ivspec);
    encryptedData = aesCipher.doFinal(dataToEncrypt);
    byte[] combined = new byte[iv.length + encryptedData.length];
    System.arraycopy(iv, 0, combined, 0, iv.length);
    System.arraycopy(encryptedData, 0, combined, iv.length, encryptedData.length);
    return Base64.encodeBase64(combined);
}
```

### 10.3.3 How to AES decrypt?

```
public byte[] decryptAes(byte[] encryptedData, byte[] key) {
    byte[] decryptedData = null;
    byte[] iv = new byte[16];
    System.arraycopy(encryptedData, 0, iv, 0, iv.length);
    SecretKeySpec secretKeySpecy = new SecretKeySpec(key, "AES");
    Cipher aescipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    aescipher.init(Cipher.DECRYPT_MODE, secretKeySpecy, new IvParameterSpec(iv));
    byte[] encryptedDataWithOffset = new byte[encryptedData.length - 16];
    System.arraycopy(encryptedData, 16, encryptedDataWithOffset, 0, encryptedDataWithOffset.length);
    decryptedData = aescipher.doFinal(encryptedDataWithOffset);
    String SealedMessageDecrypted = new String(decryptedData, "UTF-8");
    return decryptedData;
}
```

### 10.3.4 How to do RSA encryption?

```
private byte[] encryptRsa(PublicKey publicKey, byte[] clearData) {
    Cipher rsa = Cipher.getInstance(ENCRYPTION_ALGORITHM);
    rsa.init(Cipher.ENCRYPT_MODE, publicKey);
    ByteArrayOutputStream byteOutputStream = new ByteArrayOutputStream();
    CipherOutputStream os = new CipherOutputStream(byteOutputStream, rsa);
    os.write(clearData);
    os.flush();
    os.close();
    return Base64.encodeBase64(byteOutputStream.toByteArray());
}
```

### 10.3.5 How to do RSA decryption

```
private byte[] decryptRsa(PrivateKey privateKey, byte[] data) {
    Cipher rsa = Cipher.getInstance(ENCRYPTION_ALGORITHM);
    rsa.init(Cipher.DECRYPT_MODE, privateKey);
    ByteArrayOutputStream byteOutputStream = new ByteArrayOutputStream();
    CipherOutputStream os = new CipherOutputStream(byteOutputStream, rsa);
    os.write(data);
    os.flush();
    os.close();
}
```

```
return byteOutputStream.toByteArray();  
}
```

# 11 Test Cases – Validation Approach

- ☐ Validate the BVAC registration for each insurer based on effective scanning of the patient his identification means
- ☐ Validate the BVAC registration based on the scanning of the reference documents provided by the insurer to the patient
- ☐ Validate the BVAC registration for the proof of pharmacy activation
- ☐ Validate the BVAC registration failure for pharmacies not having a Assurpharma service activated
- ☐ Validate the BVAC registration for erroneous CBFA number
- ☐ Validate the BVAC registration for erroneous patient identification
- ☐ Validate the BVAC registration for invalid UUID
- ☐ Validate the BVAC registration full dataset
- ☐ ...