European Medicines Verification Organisation: Requirements for the European Medicines Verification System – URS Lite

Table of Contents

1 Introduction

The purpose of this document is to provide an overview of the basic principles and main elements of the systems that are governed and / or operated by the European Medicines Verification Organisation (EMVO) and the National Medicines Verification Organisations (NMVO's). This concerns particularly the European Hub and the National Blueprint Systems[1]. As such it is part of the foundation documents of the EMVO.

This document is limited to a level of detail that suffices all relevant stakeholders to understand and agree upon aspects of the technical system that are related to their respective material interests. A detailed and comprehensive description of the systems' functions is given by the corresponding User Requirement Specification for the European Medicines Verification System (EMVS), parts I to VI.

The document is organised as follows: In chapter 2**Error! Reference source not found.** the overall architecture of the European Medicines Verification landscape and the scope of the EMVS are explained briefly. A summary of the major functionalities of the system parts is given. Chapter 3 illustrates the major principles which govern the design and the operation of the EMVS. The use cases supported by EMVS are listed and explained in chapter 4. The so-called non-functional requirements as described in chapter 0 complete the description of the EMVS by general aspects which are not related to a dedicated use case.

2 System Overview

EMVS enables the operation of the Point-of-Dispense (PoD) Verification concept. The concept covers the basic legal requirements according to Commission Delegated Regulation (EU) 2016/161 of 9th February 2016 which supplements Directive 2001/83/EC of the marking of each medicine pack with a unique code at the point of manufacture and the verification of this safety feature prior to the dispense of the pack to the patient (e. g. at the pharmacy or the hospital). In addition to the mandatory manufacturer and pharmacist processes, the concept includes the risk-based verification of the medicine packs by wholesalers as well as the verification of returns from other wholesalers, pharmacies and other persons authorised to supply medicines to the public.

This chapter introduces the overall system landscape and the major functionality of the two EMVS components (European Hub and National Blueprint System) which are planned to be operated by the

[1] The National Blueprint System refers to a system developed in the context of the Advanced National Blueprint System strategy.

EMVO and the NMVO's. The components operated by other organizations than EMVO are not within the scope of this chapter, though the rules on governance and data protection apply also to such other organizations. While a congruent infrastructure between EMVO and National Systems is highly desirable, these National Systems therefore might differ from the EMVO infrastructure in certain details.

2.1 System Landscape

The European Medicines Verification landscape is designed as depicted in Figure 1 for the purpose of implementing the PoD Verification concept.

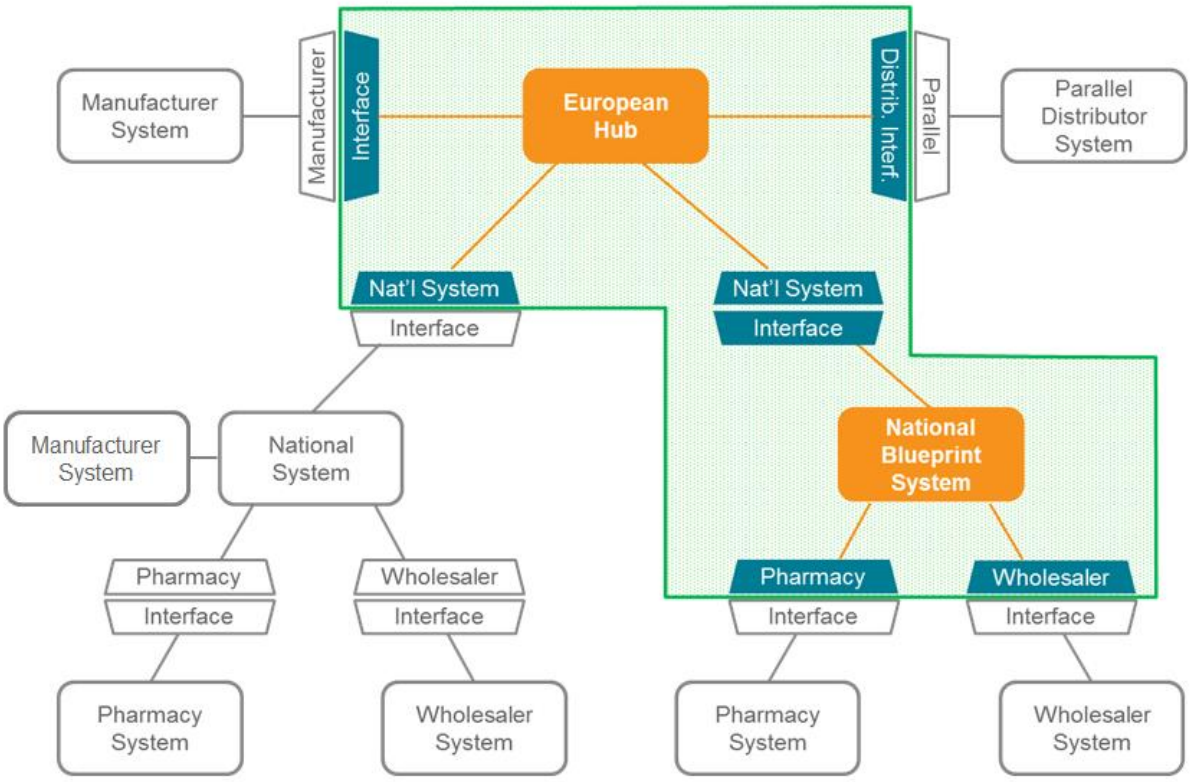

Figure 1: European Medicines Verification, scope of EMVS within EMVO responsibility (Green Area)

The different systems within the illustrated system landscape are represented by rounded boxes. The communication of systems runs via different interfaces illustrated by angled boxes; each interface is built out of two parts related to the corresponding systems. The green area defines the EMVS operated by EMVO and the NMVO's; white coloured areas are governed and operated by other parties. The

national data upload indicated above covers only the case where products and packs for the local market are exchanged. Multi-market packs may not be uploaded to one local system for all markets. The additional costs to the EMVS for national upload shall be borne by the national stakeholders requiring national upload.

2.2 European Hub

The main purpose of the European Hub is to serve as the principle place for storage of master data and as a gateway for the transmission of manufacturer data to the national and national Blueprint systems. Furthermore, data reconciliation on repackaging activities, i.e. maintaining a link between original and repackaged product batches, is exclusively performed on the European Hub.

The European Hub is a core component of the EMVS that has a number of key tasks to perform. These can be summarised as:

- It provides a single entity into which each manufacturing organisation (parallel distributors included) will transmit product serialisation data.
- It provides a single entity from which national systems can obtain revised/new product serialisation data.
- It provides a centralised location for the storage of manufacturing master data and master data regarding the connected national systems.
- It provides a means by which multi-market packs can be systematically marked as 'decommissioned' in all affected markets once a pack has been sold in one market.
- It provides a means to decommission packs by manufacturers and parallel distributors.
- It provides a verification gateway for parallel distributors to access the repositories of the source markets for verification of authenticity.
- It provides a central point from where information concerning product recalls can be transmitted in addition to the established recall procedures.
- It provides a mechanism by which exported and imported products can be reconciled at a dose level as they are used by parallel distributors in repackaging / relabelling.
- It provides a central point from which alerts, that cannot be handled solely at the national level e.g. issues in different countries with multi-market packs, can be managed. This includes providing response e.g. to the appropriate manufacturer / regulatory authority etc.

The European Hub comprises two types of interfaces to ensure connectivity and interoperability for national systems: first, to manufacturer systems (only blue side of interfaces with respect to illustration at Figure 1); second interfaces to National systems. In the document on hand the term "manufacturer" is used as a reference for both manufacturers and parallel distributors. These manufacturer systems enable the execution of transaction such as transmission of product data or the verification of pack data. The European Hub interfaces National systems for the distribution of product master data and product pack data to the relevant markets. A complete listing of use cases supported by the EMVS using the European Hub and its interfaces to connected systems is given in chapter 4.

2.3 National System

The main purpose of the National Systems is to serve as the verification platforms that pharmacies or other registered parties such as wholesalers, self-dispensing doctors or hospital pharmacies can use to check a product's 'authenticity'. All data necessary to perform this and other relevant transactions are stored in the respective National Systems.

The National Blueprint Systems serve as a cost-effective off-the-shelf verification platform that is offered to national stakeholder organisations. The National System uses the interface to the hub and serves the functionality as described in the National Blueprint System.

The key tasks of the National System are:

- Containing the relevant product serialisation data.
- Receiving revised/new product serialisation data from the European Hub.
- Serving as the verification platform for pharmacies or other registered parties such as wholesalers to check for a product's authenticity.
- Serving as the platform for pharmacies and wholesalers in the case of member states application of Art 23, to mark a product pack as decommissioned prior to handing it over to the patient.
- Serving as the platform for registered parties such as pharmacies, wholesalers, manufacturers, and parallel distributors to mark a product pack as 'decommissioned' e.g. 'exported out of EU'.

The National Systems offer interfaces to pharmacy and wholesaler systems (only blue side at Figure 1.) ensuring at least the verification of product packs. A complete listing of use cases supported by the EMVS using the National System and its interfaces to connected systems is given in chapter 4.

2.4 Operational Responsibility

For the operation of the European hub and the National Blueprint Systems the following levels of responsibility are considered:

- Governance: the decision making level of European or national stakeholders, e.g. the board of the system management organisation
- System management: a not-for-profit organisation under the direction of the governance level
- System operation: a contracted IT (Information Technology) company that builds and runs the system

The roles for the EMVS are as shown in Table 1.

Table 1: Responsibilities for EMVS operation.

Operational Level	European Hub	National Blueprint System
Governance	EMVO board	National Medicines Verification Organisation board
System management	EMVO	National Medicines Verification Organisation or EMVO (on behalf)
System operation	IT provider	IT provider

3 Governing Principles

Certain high level principles for the EMVS have been defined by the stakeholders that are strictly adhered to when setting up the verification system. These are summarised in the following sections.

3.1 Overarching Principles

A.1 The original pack unique identifier must be cancelled in the database by the parallel distributor and a new number provided. The new unique identifier must be linked to the original product number at the batch level in the European Hub to enable the product to be identified in case of recalls or other safety issues.

A.2 All national database systems must be able to work together through the European Hub in order to allow in any Member State a check on whether the pack has been decommissioned before, irrespective of its country of origin. The European Hub provides this functioning of interoperability between the national systems.

A.3 Without this interoperability, counterfeiters would be able to exploit gaps between national systems to insert falsified medicines into the legitimate supply chain.

In the case when NMVO should outsource under a service agreement system management tasks to EMVO, the NMVO assigns to EMVO all the database rights[2] relating to all Data. In return, EMVO grants to NMVO a non-exclusive, non-transferable and royalty free licence to extract, reuse, reproduce, and share all or a substantial portion of the contents of the Data for the purposes of this Service Agreement.

A.4 There should be sufficient flexibility to implement national solutions within the European Medicines Verification landscape. EMVO has assessed that the blueprint concept and all its aspects is expected to be the most cost efficient model. The cost allocation model as described in Appendix A is a core element of the blueprint concept.

A.5 National database systems should meet appropriate quality assurance requirements.

A.6 The unique serial number can only provide protection against falsification if it is routinely or systematically checked out and the status changed on the database to "decommissioned" before the product is handed to the patient or when it is processed in repackaging/ relabelling (as examples only).

A.7 Systems should be configured so that pharmacists can undertake checks when medicines enter pharmacy stock as well as at point of dispensing.

A.8 The process of verification in the pharmacy should be virtually instantaneous. The process of verification at all levels (i.e. pharmacies, wholesalers, manufacturers, and parallel distributors) should allow products to be checked without changing the status on the database.

A.9 Verification systems are for preventing falsifications, not for accessing individual stakeholder data.

A.10 Manufacturers do not seek, and will not have access to, individual patient/prescribing profile information.

A.11 As a principle, the data contained in the EMVS system belongs to the user who generates this data when interacting with the EMVS ('whoever creates the data, owns the data'). The European Medicines Verification System (EMVS) repositories system shall hold the following data components:

- Static data (i.e., the information listed under Article 33(2) of Commission Delegated Regulation (EU) No 161/2016);
- Dynamic data i.e.,:
    - the status of the unique identifier, i.e., active or de-commissioned. In case of 'de-commissioned' also the detail, e.g. dispensed, recalled, stolen, etc.;

[2] including sui generis database rights other than copyright resulting from Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

- changes to the audit trail as referred to in Article 35(1), g) of Commission Delegated Regulation (EU) No 161/2016, which contains a record of all operations concerning a unique identifier, of the users performing those operations and the nature of the operations.

As per the principle outlined above, dynamic data and static data contained in the EMVS system belong to the operator who generates the data when interacting with the system. This information must not be accessible for any other party, with exception of the static data and the information on the status of a unique identifier for the sole purpose of verification (Article 38(1) of Commission Delegated Regulation (EU) No 161/2016) and without prejudice to the right of access by national competent authorities as provided for under Article 39 of Commission Delegated Regulation (EU) No 161/2016.

Data generated by an end user's own IT system (e.g., sales or transactional data, stock movements, pricing information, etc.) by electronic or manual means, or captured with the same, is exclusively owned and may be freely used without any restriction whatsoever by the concerned end user. For the avoidance of doubt, this means that pharmacists own the data generated by their own IT system, that wholesalers own the data generated by their own IT system, and that manufacturing and/or marketing authorisation holders own the data generated by their own IT system.

A.12 Without any restriction whatsoever to the use of the data generated by an end user's own IT system as mentioned above, access to and/or use of any data (static or dynamic) extracted from, copied from or downloaded from the EMVS for purposes outside of the scope of the Falsified Medicines Directive and its Delegated Regulation needs to be agreed by all the stakeholders owning that data on a case-by-case basis in compliance with relevant legislation.

A.13 Any additional use of transactional data would need to be agreed by all stakeholders owning the data on a case-by-case basis in light of national circumstances and in compliance with relevant legislation.

A.14 The product verification solution proposed should meet the criteria of being practical, affordable and accessible.

A.15 Only the manufacturer can enter serial numbers into the system (in the case of parallel distributed products, the relabelling/repackaging entity will inevitably be a manufacturer).

A.16 There will be a requirement for an "undo" capability within the system where, for example, a serial number has accidently been "checked out" or a patient no longer requires the medicine.

A.17 The code to be affixed to each pack should include the data elements required by the Commission Delegated Regulation (EU) 2016/161 i.e. product identification code

(including national code where relevant), the expiry date, the batch number, and a serial number.

A.18 It is necessary to make a link at the level of the originator's batch between (a) the number of newly commissioned packages (and their dose count) and (b) the originator's batch as well as the list of decommissioned and newly commissioned serial numbers. The number of decommissioned packages (and dose count) will enable the system, in a timely manner, to reconcile parallel distributed products by verifying that the number of doses "decommissioned" does not exceed the number of doses subsequently checked in or "commissioned" into the system (see also A.1 above). This link needs to be maintained over the lifespan of a batch.

A.19 Deleted as it duplicated A.8.

A.20 Intentionally left blank

A.21 The system should be highly secured and permit access to data only under strict and defined conditions.

A.22 In very simple terms, a serialisation system holds the information in accordance with Commission Delegated Regulation (EU) 2016/161 Article 33(2).

A.23 Negative verification results are reported according to the defined escalation procedures, e.g. "The data elements that are scanned do not match the database information – e.g. the batch number or the expiry date."

A.24 In a product recall scenario, relevant stakeholders would require access to the status of all impacted serial numbers, including details of which impacted serial numbers have been decommissioned (e.g. dispensed or repacked). For that purpose, the European Hub will provide information in aggregated form (directly or via the national system).

A.25 Without prejudice to principles A11 and A12, data in the system shall not be used for quantitative analysis of flow of goods in the supply chain. Should Member States decide to use the information contained in the repositories system, for the purposes of reimbursement, pharmacovigilance or pharmacoepidemiology, the system shall provide them with the necessary access/reports.

A.26 The governing principles described in this document will be reflected in the contractual arrangements between EMVO and the National Medication Verification Organizations.

3.2 System Design and Implementation

In addition to the overarching principles stated in section 3.1, the following principles are valid. They cover principles with regard to both the ways of working and the system:

3.2.1 General Principles

B.1 The European Medicines Verification Model is based on the idea of a mandatory verification step on exit of a product pack from the market (e.g. in the pharmacies) plus optional verification steps where deemed necessary.

B.2 The model intentionally excludes any functionality that would, as a standard feature, allow the determination of current and/or the past locations of each product pack (so-called “track & trace” functionality).

B.3 Each pack is uniquely identified by the product code and the serial number i.e. for a given product code, each serial number will be unique across all batch numbers for the data retention period required by GxP rules (see also B.12) and at least one year after the product expiry date of that pack or five years after the product has been released for sales/distribution whichever is the longer.

B.4 The end-user systems calling a verification transaction (e.g. pharmacy systems, wholesaler systems) are required to have built-in a functionality that detects the scanning of non-serialised codes for products that should bear a serialised pack identifier.

B.5 The randomisation of the serial numbers is a key success factor of the medicines verification concept. Therefore, the following quality criteria on randomisation apply:

- The probability that a valid serial number can be “guessed” should be in accordance with Commission Delegated Regulation (EU) 2016/161 Article 4(1)(c)

Given a sufficiently large set of (randomised) serial numbers for a product, the serial numbers have to fulfil the following randomisation criteria:

- They must be equally distributed.
- They must be independent.
- They must not be built using an algorithm that is easy to find out when knowing the given set of serials or a subset thereof.

B.6 Each manufacturer will be required to use the hub for all transactions that result in product being placed into a country for sale.

B.7 It will be each manufacturer’s responsibility to upload product pack data to the European Hub. This task cannot be transferred to another party, e.g. a contract manufacturer (CMO).

B.8 In refinement of principle A.2 concerning the interoperability of all national database systems, the following design principles apply:

- For packs with one dedicated target country, any actions such as verification and dispense will only be handled by the national system of that target country and not elsewhere.

- For packs with multiple target countries (so-called multi-market packs), any pack-related action can be handled by each of the relevant national systems and information e.g. regarding the pack status is exchanged between these national systems via the European Hub.
- Parallel import / distribution of products requires a repackaging step that includes both the decommissioning of the original product packs in the export country system and the information distribution about the newly created packs to the import country system. This is exclusively done through the European Hub.

B.9 The system needs to be capable to handle different coding schemes in accordance with standards set out in Commission Delegated Regulation (EU) 2016/161., e.g. GS1 and PPN coding schemes.

B.10 In refinement of principle A.1, the following pack statuses have been defined: active and decommissioned and the following series of pack indications then equate to a decommissioning operation, exported from EU*, recalled, checked-out*, withdrawn, expired, free sample, sample (NCA), stolen*, intended for destruction*, locked*, supplied*.[3]

B.11 A pack is “decommissioned” by the party that physically takes a pack out of the supply chain. In other words, when e.g. a pharmacist sends a product back to the wholesaler who himself sends it back to the manufacturer for e.g. destruction, it would be the manufacturer as the last party in the reverse logistics process who sets the pack as “decommissioned” by setting an appropriate pack indication. Article 23 of Commission Delegated Regulation (EU) 2016/161 also permits the decommissioning of product by parties supplying to (in general) healthcare institutions on behalf of the healthcare institution. The system shall also support compliance with this requirement.

It should also be possible to undo the decommission operation of a pack within the 10 days after the pack was previously decommissioned. Following should be considered before performing Undo decommissioning:

- Undo Decommissioning must be performed from the same authorisations level and from the same premises where decommissioning was performed.
- The pack of medicinal product has not expired.
- The pack of medicinal product has not been registered in the repositories system as recalled, withdrawn, intend for destruction or stolen and the person performing the reverting option doesn’t have knowledge that the pack is stolen.
- The medicinal product has not been supplied to the public.

[3] ‘*’ = Within the same market and in another market

In case any of the above mentioned validation steps fail, the medicinal product must not be returned to sellable stock.

B.12 Applicable legislation and regulatory requirements such as e.g. GxP rules need to be considered.

B.13 Existing competition laws (EU and local) need to be considered in case of enhanced data access.

B.14 The system will provide functionality to transmit information concerning product recalls in addition to the established recall procedures. For that purpose, the European Hub will propagate the recall information to the concerned national systems. There, the status of the affect batch (or for those packs that have an "Active" status) is set to "recalled" – the status of all other packs remains unaffected.

B.15 The national systems will offer standard interfaces (including software development kits, (SDK) for pharmacy and wholesaler software providers to connect to the national systems. The exposed interfaces including the relevant documentation are considered to be part of the national systems. Unless otherwise agreed by the national stakeholders, any software developed and used by the connecting partners falls into their responsibilities.

B.16 Bulk verification as outlined under the use case 4.2.4.1 can only be performed by stakeholders in respect of products under their physical control in the frame of their obligations as outlined by the FMD and its DR.

3.2.2 Design Principles Related to Data Storage and Access

B.17 Data must be stored in such a way that data confidentiality (per stakeholder) is ensured.

B.18 The European Hub will store the minimum set of data necessary for its proper functioning and to comply with applicable legislations and regulatory requirements.

B.19 The European Hub will comprise a non-volatile repository of product master data sets that include e.g. product code, NHRN, product name, target market(s) etc. A full description of the contents of the product master data sets is provided in section 4.2.1.

B.20 The European Hub will comprise a non-volatile, dynamically growing repository to retain knowledge of which batch data was transmitted to what national system location to assist with recall activities and with multi-market pack distribution.

B.21 The European Hub will comprise a non-volatile repository containing access credentials and configuration information e.g. the electronic locations of the various national systems and of authorized manufacturers.

B.22 Pack-related data necessary to respond to transaction requests by persons authorised or entitled to supply medicinal products to the public and wholesalers will only be held

permanently in the national systems. This data can be temporarily stored in the European Hub system during the phase of transmission from the manufacturer to the destination system(s). Once successfully transmitted to the applicable national system(s), this data will be deleted from the European Hub. This statement is equally valid for both single- and multi-market packs.

B.23 Each system will maintain an event log where the transaction history is stored. Event log entries will include the pack identifier, the type of transaction, the actor, and a time stamp.

B.24 Data needed to check consistency of cross-border trade will be kept at the European Hub. Unless there is an alert flagged by the system's automatic checking procedures this data will be accessible only by the parallel distributor who has generated the data.

B.25 Data storage requirements will be reviewed in the light of applicable legislation and regulatory requirements.

B.26 Only the stakeholder triggering a pack status change transaction will receive a notification assuming the transaction doesn't lead to an exception event (alert). This is equally valid for both multi and single-country packs.

B.27 In the case of an alert, the same principles apply for both multi- and single-country packs.

B.28 Authorities will be granted the data access necessary to fulfil their regulatory action. For that purpose, the data will be retrieved from the system by appropriately trained and authorised personnel or via an agreed set of reports accessed via a GUI.

3.2.3 Design Principles Related to Exception Events

Exception events are (1) an indication of a suspicion that a given product may be falsified or the system may be attacked or (2) another problem that prevents normal (or uninterrupted) use of the system. Exception events can be classified into system exceptions and functional exceptions:

A system exception is:

- Any mal-operation of the system such as e.g. a system component that is not available, a network connection that could not be established, a scanner malfunction, a division by zero, or a system crash, and
- Any security exception such as a system attack e.g. a Distributed Denial of Service (DDoS) attack, or a hacking attempt.

A functional exception is any deviation from the "To Be" process as described in the use cases, e.g. a Data Matrix code that is unreadable and therefore causes an error message, or a manufacturer transmitting product pack data for a non-existent product code.

With this proviso, the following principles apply:

B.29 Escalations upon occurrence of an exceptional event will reflect the classification and the level of severity of that exception.

B.30 In order to be able to reflect the severity of an exception, different escalation levels will be defined e.g.

- Level 1: The system can handle the exception on its own.
- Level 2: The initiator of a transaction / the user is informed about the exception.
- Level 3: The system administrator (European or national) is informed about the exception.
- Level 4: More than one system administrator is informed about the exception.
- Level 5: In addition to the initiator of a transaction / the user and system administrators, disclosure of information to other stakeholders is required including NCA's.
- Each exception will be assigned an escalation level. This assignment may depend on the frequency of occurrence[4].

B.31 Higher escalation levels may include lower ones[5].

3.2.4 Design Principles Related to Technical Aspects

B.32 The European Hub will provide interfaces for the exchange of information with local systems manufacturers, and other parties if required.

B.33 It will be the responsibility of the European Hub management to ensure that these interfaces are well documented, evolve (if required) in a backward compatible manner and are provided with relevant support and test environments.

B.34 Per Pharmaceutical Corporation and per parallel distributor respectively, there will be a maximum of two communication channels available for data exchange with the European Hub. The restriction is to limit the overhead imposed on EMVO for each additional channel on-boarded.

B.35 Manufacturers will only transmit data to the European Hub for those packs that are brought into the commercial market (e.g. that data for reference sample packs will not be transmitted).

B.36 Bulk data transmission from the manufacturer systems and the parallel distributor systems, respectively, to the European Hub will be performed according to a push principle.

[4] Example: Upon failure to establish a network connection, the system could at first retry to establish the connection for a defined number of attempts (level 1) before informing a system administrator (level 3).
[5] Example: In case of a network failure preventing an operator to verify a product pack, both the operator (level 2) and a system administrator (level 3) could be informed about this problem.

B.37 Bulk data transfer from the European Hub to the national systems will be performed according to a push principle.

B.38 The response time for a verification or decommission transaction requests related to one pack (or a few packs) where the pack data is held within the local national system should be less than 300 milliseconds (excluding the internet time) in at least 95% of queries per validation system. Such requests will be managed by the national / national Blueprint systems and the European Hub.

B.39 Bulk type verification requests (i.e. involving a “large” number of serial numbers) are only envisaged for well-defined cases and will therefore be allowed only under these conditions. For that purpose, access to batch type verification requests might be limited to accounts with extended access rights and/or considering the actor type. Example: a manufacturer recalls a batch or a parallel distributor repackages parts of a batch.

B.40 The end-user systems should be able to identify and differentiate by scanning, those products that are required to be serialised and those that are not required to be serialized.

4 Use Cases

The EMVS supports a collection of use cases which will be run by the different system users in order to operate a medicinal product pack verification system in accordance with Commission Delegated Regulation (EU) 2016/161 of 9th February 2016 which supplements Directive 2001/83/EC. With each use case one step of the concept is implemented. The core idea of the PoD Verification concept can be fulfilled by the following sequence of use cases: a) provide serialised product pack data to the system, b) verify serial numbers and related batch data within supply chain, c) mark product packs as decommissioned when dispensing pack to the patient. A number of additional use cases are available in order to manage more complex processes.

This chapter provides an overview of the use cases supported by EMVS and the different occurrences are explained (section 4.1). Each use case is described briefly including particular functions (sections 0 and 0); the detailed specification of use cases is provided by the User Requirement Specification of the EMVS. Furthermore, some fundamental information about exception handling is given in section 0.

4.1 Overview of Use Cases

The EMVS supports the following use cases in order to implement the PoD Verification concept:

- Upload product master data: transmission of product master data from the original product manufacturers or parallel distributors to the European Hub and succeeding distribution from the European Hub to the relevant national systems
- Upload product pack data: transmission of product pack data from the original product manufacturers or parallel distributors to the European Hub and succeeding distribution from the European Hub to the relevant national systems
- Recall batch: transmission of recall information for a complete batch by the original product manufacturers or parallel distributors
- Verify pack: verification of product pack data (product code, serial number, batch data) against data from national systems
- Decommission pack: decommissioning a pack prevents it being further used within the market. In order to decommission a pack, the status of “decommissioned” will contain a further attribute/indication equal to one of the following:
    - Stolen: stolen product packs to be reported
    - Checked-Out (*proxy for Repacked*)
    - Free Sample: Provided as free samples
    - Sample (NCA): Provided as samples to the National competent authorities
    - Intended for destruction: Product packs to be destroyed
    - Locked: A product pack is locked temporarily for investigation purposes

- Supplied (*proxy for Dispensed*).
- Export pack from EU: setting the indication of product packs to “exported from EU” following an export from the EU

Batches may also be decommissioned by means of setting the batch level status attribute to ‘recalled’.

Products may be completely removed from the market by setting the product level status attribute to ‘withdrawn’. If a product is withdrawn from a market all the batches for that specific product will be decommissioned

- Request report: report metrics on system usage and performance or create stakeholder specific reports

For the above mentioned use cases variant occurrences are available for different scenarios of application. This variation is with respect to the following reasons:

- Initiator: actors belonging to different stakeholder groups can use the same type of use case
- Multi-market: for multi-market product packs more than one national systems is taken into account
- Undo / change: in case of incorrect transactions a cancelation or a modification is enabled
- Bulk of packs: mass-data transaction is possible for a bulk of product packs

Each single product pack which is known by the national systems has a dedicated status/indication which controls the allowed usage of this pack (see corresponding principles in chapter 3). An additional characteristic of the use cases mentioned above is the specific interaction with this product pack status. On the one hand application the use of certain use cases is restricted to packs having a specific pack status; if the required pack status is not given an exception is created. On the other hand some use cases also change the status of a pack.

Table 2 lists the use cases supported by EMVS. Each occurrence of a valid use case / initiator combination as well as possible variant is marked with a cross.

Table 2: Use Cases Supported by EMVS and their Occurrences

Use Case	Initiator					Variation			Changes pack status
	Manufacturer	*Par. Distributor*	*Pharmacist*	*Wholesaler*	*Administrator*	*Multi-market*	*Undo / change*	*Bulk of packs*	
Upload product master data	X	X				X	X		
Upload product pack data	X	X				X	X	X	X
Recall batch	X	X				X		X	X
Verify pack	X	X	X	X		X		X	
Dispense pack	X	X	X	X		X	X	X	X
Decommission pack	X	X				X	X	X	X
Export pack from EU	X			X		X	X	X	X
Request report	X	X	X	X	X	X		X	
Withdraw Product	X	X				X			X
Mark pack as Stolen	X	X		X		X		X	X
Mark pack as Intended for Destruction	X	X		X		X		X	X
Mark pack as free sample	X	X				X	X		X
Mark pack as sample (NCA)	X	X	X	X		X	X		X
Mark pack as Locked	X	X		X		X	X	X	X

For each use case several supporting functions are implemented. For example, after transmission of data (from the European Hub to the national system), there will be confirmation messages sent to the source system. In this chapter each of the above mentioned use cases are described briefly. The

purpose of the use cases and the different occurrences for specific scenarios are explained in the following sections 0 and 0. Management of exceptional cases is provided as well (section 0).

4.2 Use Cases: Connection to European Hub

This section deals with those uses cases which are triggered by users or their systems connected to the European hub. Primarily this is valid for manufacturers and parallel distributors. Some use cases support scenarios for other initiators as well (see Table 2); appropriate comments are given in the description of the use cases.

4.2.1 Use Case: Upload Product Master Data

4.2.1.1 Use Case Execution Sequence

Master Data are considered as the set of data elements associated with a specific product record and contain the elements of information about the product that do not belong to a specific batch (see list of data elements below). The Upload Master Data use case essentially consists of two major steps: (1) the transmission of product master data from the manufacturers to the product catalogue of the European Hub, and (2) the distribution from the European Hub to each national system relevant for the product. The transmission of product master data is done at the appropriate time, but in any case in advance of the first transmission of product pack data / serial numbers.

4.2.1.2 Product Versions

The use case can be used for the initial transmission and a subsequent data maintenance transaction because a product code version attribute is available in order to handle both cases as follows: when data for a new product code is submitted, the new product code is created in the European Hub Product Catalogue as version 01, whereas when new data for an existing product code is submitted, a new product code version (previous version number +1) is created. When the European Hub Product Catalogue is interrogated, it is normally the latest version of the product code that is presented, though it will be possible to select previous versions (depending on the effective date provided as part of the master data).

4.2.1.3 Content of Product Master Data

The product master data include the following attributes in accordance with Commission Delegated Regulation (EU) 2016/161 Article 33(2) noting that this is the data content expected to be used by the verification system and not that all parts should store all of this data where it is possible to link to or with other qualified/standard data sources:

- Unique product code
- Product code version (internally held attribute only)
- Coding Scheme
- Product name

- Common Name
- Pack type (which carries the serial number e. g. bottle, carton)
- Pack Size
- Pharmaceutical Form (e. g. tablet, capsules, solution)
- Strength of the formulated drug (e. g. 20mg, 1mg/ml)
- Number of doses per pack (e. g. 10 tablets, 100 ml)
- Wholesalers who are designated by the marketing authorisation holder, by means of a written contract, to store and distribute the products covered by his marketing authorisation on his behalf (Wholesaler ID, Name and Address)
- Product code status (shows whether the product code has been distributed to the national systems, whether it is marked as inactive etc.)
- Product Market Data
    - Market of Intended sale
    - Article 57 code or PCID (to be determined later as IDMP advances)
    - MAH ID, Name and Address
    - National Code
    - Coding Scheme
    - Serialisation Flag (indicates if a particular product is subject to point of dispense verification in a particular market)

Where practical the element names will be normalised with those used by ISO IDMP.

4.2.1.4 Supported Product Coding Schemes

The EMVS is capable to handle two different product coding schemes provided by

GS1, i.e. “Global Trade Item Number” (GTIN) or “National Trade Item Number (NTIN) for markets in which a National Registration Number is required, and

IFA (Institut für Arzneimittelspezialitaeten, Frankfurt), i.e.“Pharmacy Product Number” (PPN).

The European Hub checks data validity by tests such as:

- Is product code formally valid (digit check)?
- The maximum length has not been exceeded
- The expiry date has not passed
- The batch code length has not been exceeded
- The serial number and batch code character set content is valid
- The serial number provided has sufficiently random distribution

- Is the manufacturer (known from submitting manufacturer system) the owner of the product code and therefore entitled to submit this information?
- If new data: are all attribute values valid / within the range of possible values?
- If product code already exists: is there a change of values for attributes which must not be changed; for example number of doses (new product code is required instead)?

4.2.1.5 Upload Product Master Data from National System to the Hub

National upload might be supported by a non-blueprint National system for single-market products only and in this case the hub provides an option to upload data from National system to the hub instead from the manufacturer system to the hub. Only data intended for the connected local market may be uploaded – multi-market data is excluded.

The Upload Master Data from National system to Hub use case essentially consists of two major step: (1) the transmission of product master data from the manufacturers to the product catalogue of the National System, and (2) the distribution from the National System to the European Hub. The transmission of product master data is done at the appropriate time, but in any case in advance of the first transmission of product pack data / serial numbers.

The national upload defined above as Step (1) is not supported by EMVS (blueprint system) and is not defined in this document.

4.2.2 Use Case: Upload Product Pack Data

4.2.2.1 Content of Product Pack Data

In contrast to the product master data, transactional data is associated with specific batches of products. Transactional data is made up from two parts:

- Pack Data: This is the data that essentially describes the serial numbers of each pack and the batch to which the packs belong. The data is removed from the European Hub once propagation to the national systems is complete.
- Batch Data: This is the data that provides the link between the Pack Data and the Product Master Data. This data is retained at the European Hub. Nevertheless batch data is transferred to the European Hub in combination with the pack data; no separate use case for transferring batch data is available. The product batch data include the following attributes:
    - Batch Number
    - Expiry Date

- Manufacturer ID, name and address
- Batch Status

The assumption for the coding of a product pack is that packs will be serialised using a two-dimensional Data Matrix code containing a minimum of four elements: product code, batch number, expiry date, serial number; (and national codes in case of using a National Healthcare Reimbursement Number (NHRN)).

4.2.2.2 Use Case Execution Sequence

This use case essentially consists of two major steps: (1) the transmission of product master data from the original product manufacturers or parallel distributors to the European Hub, and (2) the distribution from the European Hub to the appropriate national system. In case of multi-market packs, the data needs to be distributed to multiple national systems.

Manufacturer data must be transmitted prior to the shipment of the products and is expected to take place at any time of the day. During these data transmission sessions, the process step on hand will be started once per batch produced.

4.2.2.3 Upload by Manufacturer

The manufacturer produces new product packs and marks them with both a Data Matrix code and the information in human-readable form. Prior to shipping (parts of) the batch to the commercial market the manufacturer has to transmit the product packs details to the European Hub; typically from an own production system.

4.2.2.4 Upload by Parallel Distributor

The upload of product pack data by a parallel distributor is related to the repackaging process as described in section 4.2.5.4.1.

4.2.2.5 Modification of Product Pack Data

The situation might occur that a manufacturer has marked the product packs with the correct information but uploaded the wrong information to the European Hub; corrective actions are necessary. Changes to the product code or to the serial number in a product pack record are not possible. If such situation occurs, the manufacturer has to decommission the affected packs in the system. In contrast wrong batch numbers or expiry dates can be modified via this use case.

4.2.2.6 Check of Product Pack Data

On transmission of pack data some checks will be executed by the European Hub prior to the distribution to the national systems:

- Expiry date not exceeded
- Transmitted information with regard to Dose per Pack matches related information in product master data
- Sufficient quality of randomization of serials for the serials provided in the given upload.

After distribution by the European Hub the national systems check the quality of randomisation of serials for the full set and uniqueness of serial numbers per product code in order to avoid duplications.

If all applicable national systems have confirmed successful receipt and modification of data receipted, the manufacturer system will be notified and the product pack data (serial number, pack status etc.) will be removed from the European Hub buffer; in contrast batch data (batch number, expiry date etc.) remain at the hub.

4.2.2.7 Upload Batch data from National System to Hub

In the use case where only for single market product, the product pack data is uploaded to the National system by the manufacturer, it is still possible for the manufacturer to also upload the product pack data to the EU Hub directly. The batch related attributes of the uploaded product pack data when uploaded locally, must be transferred from the National system to the EU Hub. The uploading of the product data directly to a National blueprint system is not supported.

4.2.3 Use Case: Recall Batch

4.2.3.1 Purpose and Use Case Execution *Sequence*

This use case describes the transmission of recall information for a complete batch by a manufacturer or a parallel distributor in case of a batch recall due to any reason in one or several countries. In parallel to issuing the batch recall via the existing way (e.g. paper-based information to all pharmacies in a market), the manufacturer or parallel distributor will inform also the European Hub by transmitting the affected batch data (product code, batch number) and affected markets. The European Hub then looks up which markets could be affected at the maximum and sends a corresponding list to the manufacturer system. In addition to the markets that were notified by the manufacturer or parallel distributor this list contains the markets that the European Hub has transmitted the batch information to; even if that are not affected by the recall (example: recall due to a leaflet having a misprint only in the language of the affected market).

The national system then executes the batch level status change to “recalled” such that all affected product packs are decommissioned: The individual status of packs that have a status other than “Active” remain unaffected. After execution of the necessary status change(s), the national system

sends back the confirmation to the European Hub. The confirmation does not include any serial numbers of related packs; it is just informing that the change(s) were successfully executed.

4.2.3.2 Notification of Parallel Distributors

In addition to informing the affected national systems, the European Hub needs to notify the parallel distributors. Upon receipt of the confirmation messages of all possibly affected parallel distributors, the European Hub sends a confirmation message to the recall-issuing manufacturer. This message does neither contain the number nor the names of the parallel distributors but is just the confirmation that the recall notification has been successfully delivered to each possibly affected parallel distributor.

4.2.3.3 Withdraw Product

In case a product is withdrawn from the market, EMVS provides the functionality for manufacturers and parallel distributors to mark all the batches related to that product as “Withdrawn”. All packs and batches relating to the withdrawn product code will then be decommissioned. The “Withdrawn” status indication will be made at product code level.

Once a product is identified to be withdrawn by manufacturer or a parallel distributor the withdrawn product must be reported to the European hub. European hub must send the updated product status to the respective National systems. National systems will update the status of the product code to withdrawn. After execution of the necessary status changes, the national system sends back a confirmation to the European Hub.

Withdrawal of a product will impact repacked products in the same way as it occurs for the recall of a batch.

4.2.4 Use Case: Verify Pack

4.2.4.1 Use Case Execution *Sequence: Bulk Verification by Manufacturer*

The use case supports the verification of a bulk of packs for a user who connects to the European hub. Rules regarding bulk verifications have been defined in B.16. It is a scenario that is designed to be used by both pharmaceutical manufacturers and parallel distributors. The verification request is sent to the European Hub first. Afterwards the European Hub selects the national system where to forward the verification request. A single verification is done for each pack within the national system. A report of the verification results is then sent to the manufacturer system via the hub.

4.2.5 Use Case: Decommission Pack

4.2.5.1 Purpose

Within normal operational processes, product packs will be decommissioned for various reasons such as stolen, repack, free-sample etc. This use case provides the functionality required to remove packs from the European supply chain.

The scenarios describing the decommissioning of a single pack or a bulk of packs by a user who connects to a national system are described in section 4.3.2.

4.2.5.2 Use Case Execution *Sequence: Bulk Decommissioning by Manufacturer*

This section describes the decommissioning of a bulk of packs by a user who connects to the European hub rather than directly to a national system. It is a use case that is designed to be used by both pharmaceutical manufacturers and parallel distributors who need to decommission packs when they are e.g. damaged or stolen.

Furthermore, it will be used by parallel distributors to set the pack status to “Checked-Out” for those product packs that are intended to be used in a repackaging activity.

It is assumed that the manufacturer system will not send one decommission request per pack to the European hub but transmits within one transaction the product code plus batch and the entire set of serial numbers to be decommissioned. This information then needs to be routed by the European hub to the applicable national system. The use case is essentially of the same nature as the previous “Verify Packs (European hub case)” use case.

Once the decommissioning of all product packs is completed, the national systems transmit the set of decommissioning results together with the corresponding serial numbers back to the European Hub for relay to the instigating client.

4.2.5.3 Decommissioning by Parallel Distributor

The decommissioning of product packs by a parallel distributor is related to the repackaging process as described in section 4.2.5.4.1

4.2.5.4 States for Decommissioning

The following sections describe the different occurrences of the decommissioning use case

4.2.5.4.1 Repack by Parallel Distributor

Technically the repackaging use case by a parallel distributor is covered by the above mentioned use cases “decommission pack” and “upload product pack data”. This section describes how both use cases are used in order to support the repackaging process.

The parallel distributor unpacks the original product packs (supported by decommission pack use case), produces repacked product packs and marks them with a Data Matrix code. The information about the original product code and batch used for repackaging and the new product code and batch for the repacked product packs is then transmitted from the parallel distributor system to the European Hub (supported by upload product pack data use case).

For a pair of product code and batch ID, a “For Repack” Buffer contains the quantity information about how many doses of this product / batch have been decommissioned for repackaging by the parallel distributor. This quantity information is reduced by the number of doses that has been transmitted as repacked product to the European Hub. The conversion from number of packs to number of doses is done based on the information contained in the applicable product master data set.

Note that a link between the original product batch information and the parallel distributor undertaking the repackaging activity is needed in the Recall Batch use case (section 4.2.3) in order to figure out those parallel distributors that might be affected by a recall of an original manufacturer batch. The list of serial numbers decommissioned and new serial numbers created for a given repack operation is also maintained within the given buffer (ref Art 34(4) of Commission Delegated Regulation (EU) 2016/161 of 9th February 2016.

Once the decommissioning of all product packs is completed, the national system transmits the set of repack results together with the corresponding serial numbers to the European Hub that receives it. The European hub stores the batch number and the information about the quantity of doses whose status has been set to “Checked-Out” in a “For Repack” buffer. This enables the European hub to maintain accurate figures about the original product quantities that will be used in a repackaging activity – for later reconciliation with the quantity of repacked product.

4.2.5.4.2 Mark as Stolen

In case a product pack is identified as stolen, this use case provides the manufacturer and/or Parallel distributors the ability to mark the product pack(s) as stolen. The occurrence of the “Mark as Stolen” use case includes single product pack or multiple product packs. Once a product pack has been

identified as stolen the pack must be reported as such to the European Hub which will transfer the new product pack status to the National System(s). At National system the stolen pack gets decommissioned and obtains a new indication “Stolen”.

4.2.5.4.3 Pack Supplied as a Sample

If a manufacturer intends to provide a product pack(s) bearing the safety features as free sample(s), the product pack must be reported to the European hub as having a pack status “Free Sample”.

Once the product pack is reported to the European hub as a free sample the European hub will transfer the new product pack status to the National System(s). The product pack will be decommissioned and obtains the new indication “Free Sample”. Alternatively, if the manufacturer also holds a wholesaler license and is required to provide a sample for an NCA, the product pack will be decommissioned and obtains the new indication “Sample (NCA)”

4.2.5.4.4 Locked

The pack status “Locked” is used to place a pack(s) into a state where they cannot be removed from the market but if scanned, will not cause the generation of alerts/exceptions. The “Locked” status is used where the pack(s) maybe subject to an irreversible state change operation however the full investigation has not yet concluded. “Locked” is therefore used to prevent continued use of a product until the investigation has concluded. The use case starts with identifying the single product pack or bulk of product packs as subject to further investigation which can be conducted by the manufacturer; in this case the product pack must be reported as “Locked” to the European hub.

Once the product pack is reported to the European hub as locked, the European hub will transfer the new product pack status to the National System(s). The product pack gets decommissioned and obtains the new indication “Locked”.

This is a temporary state. Once the investigation is completed the pack or bulk of packs can be either set again to its previous indication or will be marked as being decommissioned with another indication, e.g. “Stolen”.

4.2.5.4.5 Intended for Destruction

The manufacturer can mark a product pack as intended for destruction where the pack(s) are to be permanently removed from supply. Once the product pack is reported to the European hub as intended for destruction, the European hub will transfer the new product pack status to the National System(s). The product pack gets decommissioned and obtains a new indication “Intended for Destruction”.

4.2.5.5 Undo Decommissioning

Where packs have been decommissioned only with the state of “Supplied”, “Exported from EU”, “Checked-out”, “Free Sample”, “Sample (NCA)” and “Locked” it is possible for them to be re-introduced into the EU supply chain, e.g. when an error was made at decommissioning. Note that in the repack case, the ‘For Repack’ buffer needs to be reduced accordingly. Rules regarding the reversal of the decommissioned state are defined in B.11.

4.2.6 Use Case: Request Report

This use case enables both physical users and systems (e. g. the manufacturer's system) to request reports and metrics from the European Hub and the national systems for different purposes. In addition to the above mentioned users of the EMVS, physical users are also system administrators or staff members of the system-governing stakeholder organisations.

To allow requesting physical users to fulfil their tasks, both European Hub and national systems need to provide a user-friendly interface including standard functions such as user and rights management, filtering options, and file export.

A variety of queries support the users of the EMVS at gaining benefit from the data available in the European Hub and the national systems. The audit trail data (see chapter 0) of EMVS is used as a major information source. The execution of queries is strictly restricted to the designated operators within the relevant stakeholder organisations in order to control access to data according to the agreed principles.

Reports for following example purposes are submitted:

- Confirm correct execution of exception events for post event 'forensic style' analysis
- Monitor general system operation and performance including statistical process control
- Monitor system access by users including unusual access attempts
- Follow the lifecycle of a product pack
- Monitor pack verification attempts including reporting on suspicious activities

In general no reports will be offered that violate the rules for access to and ownership of data.

4.3 Use Cases: Connected to National System

This section deals with those uses cases which were triggered by users or their systems connected to the National system. Primarily this is valid for pharmacists and wholesalers. Some use cases support scenarios for other initiators as well (see Table 2); appropriate comments are given in the description of the use cases.

4.3.1 Use Case: Verify Pack

4.3.1.1 Purpose

This use case processes a verification of a single pack or a bulk of product packs and will only be performed by a stakeholder in the frame of their obligations as outlined by the FMD and its DR. The use case is applicable to a large number of different scenarios and actors (see also section 4.2.4 for verification via the European hub). In general, for a given pack at hand, the opportunity exists within the supply chain for a simple verification process (without changing pack status) to be undertaken. The verification process will allow the operator to gain knowledge about the present status of a product pack; for example the pack can be confirmed by the system as “Active” prior to dispensing to the patient.

4.3.1.2 Use Case Execution Sequence: Single Verification

A standard occurrence of the use case describes the verification of a single pack by a pharmacist (or wholesaler) who connects to a national system. The pack at hand is scanned and the data scanned is interpreted within the local environment to confirm if the pack code should contain serialised data. If the pack should be serialised but the code scanned is not a serialised code, no alert is generated but a local error message is returned to the operator.

If the pack data is serialised, the data from the scan process is sent to the national system where the product code and serial ID pair are used to look-up the pack record. When the pack has been located the batch code and expiry date scanned from the code data are compared to the data held on the database for each of these fields. Only if the product code, serial number, batch, and expiry match, the pack record is considered to be found.

4.3.1.3 Use Case Execution Sequence: Bulk Verification

Another verification scenario is the bulk verification request to the national system. This scenario envisaged to be used by wholesalers. Different to the single pack verification, it is assumed that the wholesaler system will not send one verification request per pack to the national system but transmits within one transaction the product code and the entire set of serial numbers to be verified.

For bulk verification by pharmaceutical manufacturers and parallel distributors connected to the European hub see section 4.2.4.

4.3.1.4 Use Case Execution Sequence: Multiple Verification

This use case describes the verification of a set of packs by a pharmacist who connects to a national system. Multiple verification requests means that each pack is scanned and pack data is stored in the client system. Once the scanning is completed the client system sends a single verification request to the national system for these packs that do not necessarily have the same product codes to the national system. Limits may be set at national level (in terms of frequency, times or number of packs).

4.3.1.5 Use Case Execution Sequence: Inter Market Verification

This use case describes the functionality that occurs when a pack is scanned in a market that was not its originally intended market for sale. This can occur when packs are consumed in markets such as Luxembourg but can also occur when packs are dispensed by internet pharmacy or are part of a compassionate use program etc. In these (and other related) scenarios, the Delegated Regulation is clear that the scanned pack shall not be immediately reported to the user as 'unknown' by the connected National repository but instead a query will be sent to the European Hub and the Hub will then send a directed query to the market originally intended for the sale of the pack scanned. The response will then be routed, via the Hub to the originating National System and from there back to the user. The Delegated Regulation and supporting Q&A allow each queried repository to take a maximum of 300mS for each passage of the query making Inter-Market queries have a longer response time than the more usual 'within own market' queries. It is acknowledged that this extended capability will now mean that the response to a genuine unknown pack will now take longer than originally specified (because the system cannot initially differentiate in all cases between a genuinely unknown pack and one that requires an inter-market query)

This functionality is not restricted as packs may be verified or decommissioned in the same manner as 'own market' packs.

4.3.2 Use Case: Decommission Pack

4.3.2.1 Use Case Execution Sequence: Single Pack Decommissioning

This section describes the decommissioning of packs from the supply chain by a user connected to a national system rather than to the European hub (see also the definitions in section 4.2.5).

One occurrence of this use case describes the decommissioning of a single pack; it is a case that is envisaged to be used by pharmacists & wholesalers. The operator will scan the pack and the data from

the pack will be sent to the national system for processing. The national system will perform a pack verification to check that the pack in hand is available for decommission. If the pack is "Active", the pack status will be changed to one of those defined by principle B.10.

If the Decommission process is successful and the pack is a multi-market pack, the pack details will be sent to the European hub so that the decommission event can be propagated to all other legitimate markets where the pack could be sold (status is set to the same status with an extension "in another market"). Once a positive acknowledgment has been received from all applicable markets, the data used to undertake the propagation will be removed from the European Hub.

4.3.2.2 Use Case Execution Sequence: Bulk Decommissioning

Additionally the use case supports the decommissioning of a bulk of packs by a user who connects to a national system. It is a use case that is envisaged to be used by wholesalers. Different to the single pack case, it is assumed that the wholesaler system will not send one decommissioning request per pack to the national system but transmits within one transaction the product code and the entire set of serial numbers to be decommissioned.

4.3.2.3 States for Decommissioning

The following sections describe the different occurrences of the decommissioning use case

4.3.2.3.1 Pack Supplied as Sample (NCA)

The wholesaler intends to provide the product pack(s) bearing the safety features as sample(s) to a National Competent Authority. Once the product pack(s) is reported to the National System as a sample (NCA), the product pack(s) will be decommissioned and obtain the new state "Sample (NCA)" and this information will be forwarded to the other National systems via the European hub.

4.3.2.3.2 Export Pack from EU

Within normal operational wholesale processes, the opportunity exists for product packs to be exported from the EU market. In this situation, this use case provides the functionality required to fully update the pack records such that they reflect the new pack status. This use case provides the functionality to permit the removal of packs from the European supply chain following an export from the EU market. It is a subtype of the corresponding wholesaler triggered scenario of the "decommission pack" use case (including undo option) except that this is one occurrence of the various reasons of decommissioning.

4.3.2.3.3 Dispense

This use case describes the process of dispensing a product; for example within a retail pharmacy environment or supplied within a wholesaler process.

4.3.2.3.3.1 Single Pack Dispense

The use case starts with the verification of a single pack within the national system (see "Verify Pack" use case above). Subsequently the status for the pack found is checked to determine if it has already been decommissioned or has any of the other reasons of decommissioning. Assuming that the pack has not already been decommissioned or has none of the reasons for decommissioning, the pack is checked to confirm if it is available (status "Active") and if it is, the pack status is set to "Decommissioned", and obtains a new indication "Supplied" within the national system.

If the pack has already been decommissioned, a further check is undertaken to determine if the original dispense operation was undertaken within the same client location. For the same client a number of 'double decommission' operations within the agreed national limits is accepted.

If the pack is a multi-market pack, the pack data is sent to the European Hub where it is received as being supplied within the known market. The European Hub will then propagate the "decommissioned/supplied" status for the pack to all the other national systems of relevant markets. Once the propagation process is successfully completed the information on pack status is deleted from the Hub's data base.

4.3.2.3.3.2 Manual Pack Entry

A variation of use case offers the opportunity to manually enter the pack data in the event that the pack cannot be scanned (e.g. scanner malfunction). In order to minimise the risk of typing errors, only the product code and the serial ID have to be entered; no entry of batch ID and expiry date is required. If the pack is "unknown" to the system the assumption is that the operator has mistyped some information within the allowed limits of attempts for the client location.

4.3.2.3.3.3 Bulk Dispense

In case of a temporary disconnection between the pharmacy or wholesaler system and the National System an offline buffer capability is required to ensure on-going dispensing to patients. After connectivity restoration a performant automatic system synchronisation recovers a consistent state of all related product packs. For the provision of the synchronisation procedure a "Dispense Bulk of Packs" use case is foreseen (not described in this document).

4.3.2.3.3.4 Point of Entry to the Pharmacy Verification

The "Dispense Pack" use case reflects the understanding that packs will be checked at the point of dispensing. However, if in accordance with legal requirements at national level, the medicine may be checked and its status changed at the point of entry to the pharmacy, a relevant use case for this situation will be developed resulting in the status being changed to 'Decommissioned' and obtaining a new indication "Supplied".

4.3.2.3.4 Mark as Stolen

In case a product pack is identified as stolen, this use case provides wholesalers with the ability to mark the product pack(s) as stolen. The occurrence of the "Mark as Stolen" use case includes single product pack or multiple product packs. Once a product pack has been identified as stolen, if the pack is multi-market the change must be reported as such to the European Hub which will transfer the new product pack status to other affected National System(s). At National system the stolen pack gets decommissioned and obtains a new indication "Stolen".

4.3.2.3.5 Locked

The pack status "Locked" is used to place a pack(s) into a state where they cannot be removed from the market but if scanned, will not cause the generation of alerts/exceptions. The "Locked" status is used where the pack(s) maybe subject to an irreversible state change operation however the full investigation has not yet concluded. "Locked" is therefore used to prevent continued use of a product until the investigation has concluded. The use case starts with identifying the single product pack or bulk of product packs as subject to further investigation which can be conducted by a wholesaler; in this case the product pack must be reported as "Locked" to the National System.

Once the product pack is reported to the National System as "locked", the National System will check if the product is a multi-market type and if so, will transfer the new product pack status to the European Hub for National System(s) synchronisation. The product pack gets decommissioned and obtains the new indication "Locked".

This is a temporary state. Once the investigation is completed the pack or bulk of packs can be either set again to its previous indication or will be marked as being decommissioned with another indication, e.g. "Stolen".

4.3.2.3.6 Intended for Destruction

A wholesaler can mark a product pack as intended for destruction where the pack(s) are to be permanently removed from supply. Once the product pack is reported to the National System as "intended for destruction", the National System will check if the product is a multi-market type and if so, will transfer the new product pack status to the European Hub for National System(s) synchronisation. The product pack gets decommissioned and obtains the new indication "Intended for Destruction".

4.3.2.4 Undo Decommissioning

EMVS allows the re-introduction of a previously "Decommissioned/Supplied" / "locked" / "Free Sample" / "sample (NCA)"/ "exported from EU" pack back into stock. In addition to requirements for a series of local physical process steps that need to be followed, the system relevant process is the

following: the operator will scan the pack and the data from the pack will be sent to the national system for processing. The national system will check that the pack was originally processed by the same client location and is being returned within 10 days. If the same location is confirmed and the pack is being returned within time, the pack status will be changed to make the pack “Active” (only if no other impediment exists to prevent this, e.g. product is expired or status is “recalled”, “stolen”, “withdrawn” or “Intended for destruction”).

If the undo process is successful and the pack is a multi-market pack, the pack details will be sent to the European Hub so that the re-introduction event can be propagated to all other legitimate markets where the pack could be sold.

4.3.3 Use Case: Request Report

A general description of the use case valid for both users connected to the European hub and the national system is given in section 0.

4.4 Exception Handling

The use cases of the EMVS support management of exceptional cases. An exceptional case is a deviation from the "to be" process. For instance, an exception occurs if the prerequisites for use case execution are not fulfilled or if errors occur during technical execution, e. g. during data transmission from one system to another. Each occurrence of an exception triggers certain actions by the system and the using organisations such as: rejecting the requested data change, sending notifications, investigating on root causes, or correcting input data.

A large number of various exceptions can occur in the context of the EMVS use cases. Most exceptions lead to a low level of escalation, e. g. a notification to the originator of the corresponding transaction.

This section provides a summary of those kinds of exceptions only which lead to an additional notification to a 3rd party - when someone who has not triggered the use case gets informed about the exception. In addition to the notifications mentioned below in those cases a notification is sent to the administrator of the European Hub and / or the administrator of the involved national system.

In general three types can be distinguished when looking at potential exceptions. These are briefly summarized in the following sections.

4.4.1 Process Exception Related to a Potential Counterfeit/Falsification

For a process exception related to a potential falsification, an alert is created for a certain serial number and sent to the EMVO, the manufacturer, the parallel distributor and / or the national organization. The following occurrences are managed by the system:

- One of the following reasons occurs at pack verification: unknown / duplicate serial number, incorrect batch, or incorrect expiry date.
- An inappropriate pack status is given before starting a decommissioning use case (including "undo" scenario) e.g. "supplied" or "export from EU". This exception occurs for example if a pharmacist tries to dispense a pack which has the current status "decommissioned".

4.4.2 Process Exception Not Related to a Potential Counterfeit/Falsification

A process exception occurs if the system is used in an inappropriate way. The following exceptions are relevant:

- Exceptions due to prerequisites for data are not fulfilled:
    - The manufacturer tries to upload product pack data with an insufficient quality (e. g. incorrect dose, exceeded expiry date, or insufficient randomization).
    - Master data has not been successfully transferred before when manufacturer's product pack data is distributed to a national system.

  - Same pack identifier (product code, serial number) is used for more than one pack when uploading product pack data.
  - No initial upload of batch data has occurred when the manufacturer tries to modify batch related product pack data (expiry date, batch number) or recall a batch.
  - The pack status is not “Active” when a manufacturer tries to modify product pack data.
  - The repacked doses exceed the original doses when a parallel distributor uploads data for repacked products.
  - A batch recall by a manufacturer fails because the batch is not known by the national system or the status change fails.
  - A product code is not known at pack verification.
  - The Hub or a related national system (market) does not know the product code of a pack which is intended to be dispensed, decommissioned or exported (multi-market functionality).
- Exceptions due to authorisation is not given:
  - The manufacturer uploads data for a product code which is not assigned to him. This exception is related to the upload of product master and product pack data and a batch recall.
  - A requested report fails because no authorization is given.
  - A pharmacist starts a multiple verification request beyond the limits set at national level (in terms of frequency, times or number of packs).

A few exceptions raised for technical reasons lead to a notification to stakeholders other than the originator of the transaction and the system. These are the following:

- The transfer of data to the hub or the national system fails for technical reasons (e. g. incorrect format). This exception is related to the upload of product master and product pack data triggered by the manufacturer.
- An expected confirmation or acknowledgement is not sent by the national system to the hub. This exception is related to the use cases upload of product master data, recall batch, verify batch, withdraw product and export pack from EU.
- A requested report fails because the report is not available, or no response is provided by the national system.

5 Non-Functional Requirements

Chapter 4 summarizes the use cases supported by the EMVS which serve to the functional needs of the system users. These are designed in order to fulfil the specific business needs, i.e. the operation of the PoD concept. In addition this chapter presents non-functional requirements. These are typically of more general interest; most of them are valid for a majority of IT systems (with differing characteristics).

5.1 Graphical User Interface

5.1.1 Graphical User Interface related to the National Authority

In order to provide the National Authorities functionality to supervise the functioning of the repositories, investigate potential incidents of falsification and provide access for reimbursement and pharmacovigilance or pharmacoepidemiology, it is required to provide a Graphical User Interface to the National Authorities. The graphical user interface should provide functionality to the National authorities to access a series of yet to be defined reports and to obtain alert information.

5.1.2 Graphical User Interface related to the Wholesaler and Pharmacy

It is required to provide a Graphical User Interface for the wholesalers and pharmacies providing the functionality to perform the verification of the product pack and perform the decommissioning operations in case of failure of their own software. In this case the graphical user interface will send the user entered verification or decommissioning request to the National system and receive the response which will be shown to the user. The graphical user interface is expected to be a manual data entry system and not driven by a code reader/scanner.

5.2 Access Management

Two different categories are given with respect to system access: system users (computer systems connected) and non-systems users (persons using the system). Both types of access to EMVS need to be managed in a way which prevents unauthorized access to data. The following requirements are valid:

- The system shall allow only authorised users to access and operate the system.
- The system shall be designed such that there is a zero tolerance for data leaks to unauthorised parties.
- The system shall be designed to ensure that all data is segregated in such a way that guarantees independence and prevention of access to non-authorised parties.
- The system shall encrypt all or part of the data such that unauthorised access to the data would result in data that was unusable.

- Common functions and principles are available for the administration of users and passwords.
- The system shall incorporate the principle and capability to assign access rights by group. Individual access rights may be assigned to users only by reference to a pre-defined group.
- The system shall allocate system user credentials to specific client locations and shall not allow access to the host using valid, but incorrectly matched system user credentials.
- The system shall ensure that user credentials refer back to a unique and permanent ID that remains constant for the specific user.
- The system shall authenticate each connection to confirm client validity, location, and equipment.
- The system shall not use hardware “dongles” or external hardware “key” devices without a full discussion on the merits of use and prior agreement by EMVO.
- The system shall ensure that client system access to the host (European Hub or national system) is limited to the specified minimal functionality.
- The system shall ensure that clients only have access to read, write or amend their own data unless resulting from the use of a valid use case scenario.
- The system shall provide an offline capability for the pharmacy and wholesaler client use cases with performant automatic system synchronisation on connection restoration.
- The pharmacy client interface shall be capable of operating different dispense terminals that belong to the same pharmacy.
- Access to the GUI’s will ensure that the location of service provision is fixed (i.e. not user based) to ensure that the GUI cannot be used from any location other than that which was intended or approved.

5.3 Business Continuity Management

The following requirements are specified in order to ensure an appropriate system reliability and availability:

- The system shall be designed so that replication technologies being used will check for the existence of false records and cause an exception alert if any are found.
- The system shall incorporate multiple means of providing communication links in the event of catastrophic communication failure.
- The system shall be designed to provide failover capability at all critical points.
- The system shall be designed as such that all maintenance activity is conducted overnight and in such a manner as to ensure that the system does not go completely off-line. Specifically, it is expected that the European Hub and the national Blueprint systems have a scheduled uptime of 7 x 24 hours with the exception of planned downtimes for hardware and/or

software maintenance. It is the goal to limit unplanned downtime to less than 0.1 % of scheduled uptime. The exact service level for unplanned downtime will be specified in contracts with the relevant service providers on the basis of reasonable commercial conditions.

- The system shall provide a secure means of provision for authorised external, remote system access that can be used by EMVO / Stakeholder delegates.

5.4 System Performance

In order to ensure a high system usability and thus sufficient support of business processes, an appropriate system performance is essential. Therefore the following requirements are specified:

- For national system clients, the response time of the repository, not considering the speed of the internet connection, shall be lower than 300 milliseconds in at least 95% of queries.
- The system shall ensure an end-to-end response time of less than 1 minute for bulk transactions by manufacturers such as a bulk decommissioning of 200 packs of the same product code.
- The system shall ensure that responses to pack data upload transactions are provided to the originating manufacturer within 2 minutes of the initial upload completing for a batch size of 10,000 packs.
- Transaction requests to both the European Hub and the National Systems should be processed directly rather than in scheduled batch mode.
- The system provider shall ensure that manufacturing data can be uploaded at any time.

5.5 System Monitoring

The monitoring of the system is used for various purposes such as performance evaluation and intrusion prevention. In general system monitoring is based on the collection of appropriate data (via logging / audit trail, see section 5.6) and the tailored reporting of this data for specific purposes (see also section 4.3.3 for the reporting use case). The following requirements are valid for system monitoring:

- The system shall implement transaction level monitoring and logging.
- The system shall be able to maintain lists of web services and email addresses that must be notified in case of error, for each interface flow.
- The system shall actively refuse connection attempts from sources, even if apparently legitimate, where the connection pattern is uncharacteristic or excessive.
- The system shall be designed such that activity and access attempt records can be used to support forensic examination and be used as evidence with potential legal proceedings.

- The system provider shall implement the use of heuristic and rule based monitoring to detect and trap anomalous system activity and interrogations.
- The system provider shall ensure that full auditable system logging is maintained.
- The system provider shall monitor network activity at all times.
- The system shall provide an audit trail of changes to operational parameters and operator actions.

5.6 Audit Trail

The European Hub and national Blueprint systems include the capability to accumulate a secure, non-modifiable, time-stamped, electronic audit trail which can be used to ensure system performance and to review system activity (if necessary for, e.g., the analysis of exceptional events) under the strict control of the system stakeholder organisation (EMVO or National Stakeholder Organisation as appropriate). The audit trail must include the data and time of the change/record, an identification of the person/system making the change, the value prior to the change being made, and the reason for the change (where practical). The audit trail delivers various data collections such as:

- Data transmission from and to the system
- Data associated with one individual product pack across the entire 'life' of the pack
- Data associated with user or users' system interaction such as login attempts, transactions etc.
- Data associated with all exceptions recorded by the systems
- Full error logging
- Administrator activities

5.7 System Development

In order to deliver high system quality over the whole lifecycle of EMVS the following requirements need to be fulfilled by the system supplier:

- The supplier shall have a documented Quality Management System in place, certified to a recognised standard.
- The system should be validated according to a written procedure for Computerized System Validation.
- The life cycle should be structured into phases and activities and be aligned to GAMP 5 (Good Automated Manufacturing Practice). The validation process should be performed for new developed systems and is expected to have taken place for existing operational systems.
- Tests should be executed on a qualified test environment.

- The interface documentation shall be sufficient to enable manufacturer / wholesaler / pharmacy software providers to implement their part of the client interface.
- The supplier shall define a standard on-boarding package for the suppliers of manufacturer systems, wholesaler systems, and pharmacy software. The package should describe among others quality, security, and testing requirements.

5.8 System Operation

In addition to the quality management at system development the supplier needs to establish a variety of processes and systems providing a reliable operation of the systems on a high level of quality. These are as follows:

- IT service management such as ITIL (Information Technology Infrastructure Library)
- Information security management system certified by an independent auditor and corresponding processes guaranteeing the confidentiality, integrity, and availability of information
- Service Level Agreements (SLA) including monitoring of SLA by corresponding KPI
- IT service continuity management ensuring the fulfilment of the agreed minimum service levels even in the event of an IT services disruption
- System backup and data restore
- Change management
- Configuration management
- Deployment management ensuring the protection of the live environment
- Incident and service request management
- Problem management including a corrective and preventive action process (CAPA)
- Periodic review confirming the required support and maintenance
- Training of persons who act under the supplier's responsibility (e.g. development, maintenance, administration)
- Regular audits

The specific characteristics of services delivered by the supplier to the user of EMVS are part of the corresponding SLA (response times etc.). In addition there are some general services required (valid for the European Hub and the national Blueprint systems if not stated differently):

- System availability across Europe
- Hosting in EEA countries
- Support (help desk etc.) to each national Blueprint system in the local language as well as in English

- Service desk as the single point of contact for the users (via phone, email, and web)
- Provision of 1st, 2nd, and 3rd level support
- Application support with respect to installation of security patches, update of operating system etc.
- Integration support for the suppliers of manufacturer systems, wholesaler systems, and pharmacy software systems who develop interfaces to the European Hub and the national Blueprint systems, respectively
- Access management
- End and key user training
- Annual review of service level KPI including major release changes and corrective and preventive actions
- Update of the security risk assessment (e.g. in case of possible new security risks) including proposals how to prevent the risk
- Initiation of system security audits
- Retention of data in the European Hub for a period of batch expiry date + 1 year or 5 years whichever is the longest
- Retention of data in the national Blueprint system for a period that is configurable and applicable to the region being serviced
- Backup of all audit trail and usage data for a minimum term that is configurable and agreed upon with the customer
- Archiving and retrieval of data to ensure long-term accessibility
- Central application of patches and updates in a secure manner
- Application of patches and updates not automatically but according to a defined SOP including risk assessment, testing etc.
- Appendix A: Concept Paper for a cost allocation model application of patches and updates in a secure manner
- Application of patches and updates not automatically but according to a defined SOP including risk assessment, testing etc.

6 Appendix A: Concept Paper for a cost allocation model

6.1 Executive summary

To comply with the requirements of the Falsified Medicines Directive and the Delegated Regulation (collectively referred to as the FMD) on the establishment of a European-wide medicines verification system, five stakeholder associations have incorporated a non-profit association, EMVO (European Medicines Verification Organisation), [6] to interconnect national verification systems in all EU and EEA countries.

The FMD provides that the costs of the repositories system shall be borne by Manufacturing Authorisation Holders and that the system shall be operational as of 9 February 2019. To finance the system, the stakeholders representing the manufacturers, namely EFPIA, EAEPC and Medicines for Europe, have agreed upon a model that will charge annual upfront usage fees based on a single flat fee per Marketing Authorisation Holder or parallel distributor.

Where the Marketing Authorisation Holder for any given product is not the same legal entity as the Manufacturing Authorisation Holder, both parties shall be required to contractually agree how to attribute the usage fees between them in compliance with the FMD.

EMVO hereby notifies all Manufacturing Authorisation Holders and Marketing Authorisation Holders of the practical implications of the agreed cost allocation model and encourages them to have the necessary contractual agreements in place so that fees are paid in a timely manner to ensure that the repositories system is fully effective from the outset.

6.2 Background

The FMD aims to improve patient safety by mandating stakeholders to put in place a system to prevent falsified medicines from entering the legal supply chain. This system should allow the verification of the authenticity of medicines. The founding members of EMVO, recognizing that patient health and safety is essential across the entire supply chain, have been closely collaborating under the auspices of the European Medicines Verification Organisation (EMVO)

[6] The founding members of EMVO are: EFPIA representing the research pharmaceutical industry, Medicines for Europe (or formerly EGA) representing the generic and biosimilar medicines industry, and the EAEPC representing the parallel trade pharmaceutical industry, together with PGEU representing pharmacists and GIRP representing wholesalers.

since February 2015 to establish the repositories system, referred to as the European Medicines Verifications System (EMVS).

The EMVS is designed to function as a secure, interoperable and cost effective system across Europe. It comprises a European hub interacting with national verification systems. Stakeholders at national level can opt for a standalone national system or can avail of efficiencies by using the "Blueprint Approach" that builds on the legal and IT architecture employed by EMVO. The EMVS comprises the European hub and the national (or supra-national blueprint) repository systems.

6.2.1 Transitional Phase - Establishment of National Repositories

EMVO currently bears the hub development costs and the costs for the related legal and technical support provided to the national stakeholders incorporated in the so-called blueprint approach.

EMVO is financed through membership fees of approximately 400.000 EUR p.a., which is about 10% of the annual costs since the bulk are technical development costs over the period 2016-2019. The stakeholders have agreed that part of these costs will be financed by loans provided by member companies of the three manufacturer associations (EFPIA, EAEPC and Medicines for Europe). These loans are interest bearing and will be repaid 3 years after the EMVS is fully operational and generates its own revenue. In this way, the ramp-up costs can be financed and later recovered.

6.2.2 Operational Phase - Launch on 9 February 2016

This revenue stream will begin to flow only after the date of mandatory application of the rules on safety features, i.e. after 9 February 2019. At this stage of full operations the stakeholders representing manufacturers have agreed on a flat fee financing model to cover the significant costs involved in establishing and managing the EMVS. The flat fee model is designed to be transparent, non-discriminatory and proportionate in relation to the services rendered.

6.3 The mechanics of the flat fee model

The legal entity responsible for placing the product on the market where it is verified shall enter into an agreement with the entity(ies) managing the repositories system in a given market and shall be liable for the upfront payment of the service fees on an annual basis to the entity in charge of this repository. Any Marketing Authorisation Holder or parallel distributor that fails to pay the flat fee will not have its medicines verified.

The cost allocation model calculates a single fixed fee based on the number of users of the national/supra-national repositories (i.e. all Marketing Authorisation Holders and parallel distributors requiring the verification services of any given repository). The fee payable is equal

for all users. The single flat fee model has significant advantages in terms of ease of administration in the invoicing process, as well as offering users predictability and transparency.

Larger manufacturing companies that contract with multiple Marketing Authorisation Holders per market will pay a multiple in fees compared to small companies with fewer marketing authorisations. The level of the fees payable in any given market is estimated at between € 4,000 and € 21,000 depending on the market size and the number of active Marketing Authorisation Holders (and parallel distributors) active in that market. This fee level is comparable to the maintenance fee of some DCP Marketing Authorisations and is regarded as proportionate and non-discriminatory.

By virtue of Article 54a (2)e, the costs of the repositories system shall be borne by the Manufacturing Authorisation Holders. The term "Manufacturing Authorisation Holder" covers pharmaceutical manufacturers as well as parallel distributors who repackage and for that purpose require a manufacturing license, or equivalent GMP authorisation. However, as a rule, Manufacturing Authorisation Holders do not operate directly on the markets that their products serve unless they are also the marketing authorisation holder. In all national markets that are part of the EMVS, it is the Marketing Authorisation Holders or parallel distribution license holders that have the legal right to place products on each national market.

For these reasons, the EMVS access principles foresee that only those entities holding marketing authorisations (or parallel distribution licenses) can establish a legitimate connection to the EU Hub for the uploading of product data. This is expressly intended to protect the system against unauthorized and uncontrollable data upload, and to impose clear responsibility on the Marketing Authorisation Holders for the proper implementation of the EMVS. This is fully in line with the *acquis communautaire*.[7]

[7] The obligation to affix safety features onto medicines packages, as in Article 54(o) of the Directive 2001/83 as amended, is addressed to marketing authorisation holders, and it is an obligation of the QP of the manufacturing authorisation holder to ensure that these features are indeed affixed in accordance to the marketing authorisation of the product concerned (Article 51/1/a). The Human Medicines Directive holds the Marketing Authorisation Holder legally responsible for a medicinal product on a given market and all related obligations, such as pharmacovigilance (see Article 6, paragraph 1a, of Directive 2001/83). These obligations are also imposed on parallel distributors, even if the EU legislation does not recognise them as Marketing Authorisation Holders in the formal sense. In case a Marketing Authorisation Holder delegates certain GMP related functions to a holder of the Manufacturing Authorisation, the scope and responsibilities of such delegation are set out in a GMP compliant Technical Agreement, but the responsibility for the compliance of the medicinal product with its marketing authorisation remains with the holder of said authorisation.

This means that in the event that the Manufacturing Authorisation Holder and the Marketing Authorisation Holder are not one and the same legal entity, these parties should agree that fees payable for use of the EMVS shall be made by the Marketing Authorisation Holders and the terms on which those costs may be passed on to the relevant Manufacturing Authorisation Holders.

It is incumbent upon Marketing Authorisation Holders (and parallel distributors) to ensure their readiness to pay the fee for verification services by the EMVS including through their contractual relations put in place with Manufacturing Authorisation Holders where appropriate.

7 Appendix B - Balance in representation.

Within EMVO there are three associations of manufacturers and marketing authorisation holders (EAEPC, EFPIA and EGA), one association of wholesalers (GIRP) and one association of community pharmacists (PGEU), which each also represent a constituency.

In many countries the exact same constellation of national trade associations may not exist. However, it is recommended that national stakeholders aim for a fair and balanced division in the voting rights between associations (or constituencies where applicable) of manufacturers and marketing authorisation holders and associations (or constituencies where applicable) of wholesalers and pharmacies.

Since they all participate in the governance of the entity and financially contribute to its costs, associations of manufacturers, marketing authorisation holders, wholesalers and pharmacists should actively take in part in all decisions. Decisions should be taken on a consensus basis. Decisions based upon or according to majority of voting rights should be avoided by principle