European Medicines Verification System:

White Paper on EMVS Data Upload

Contents

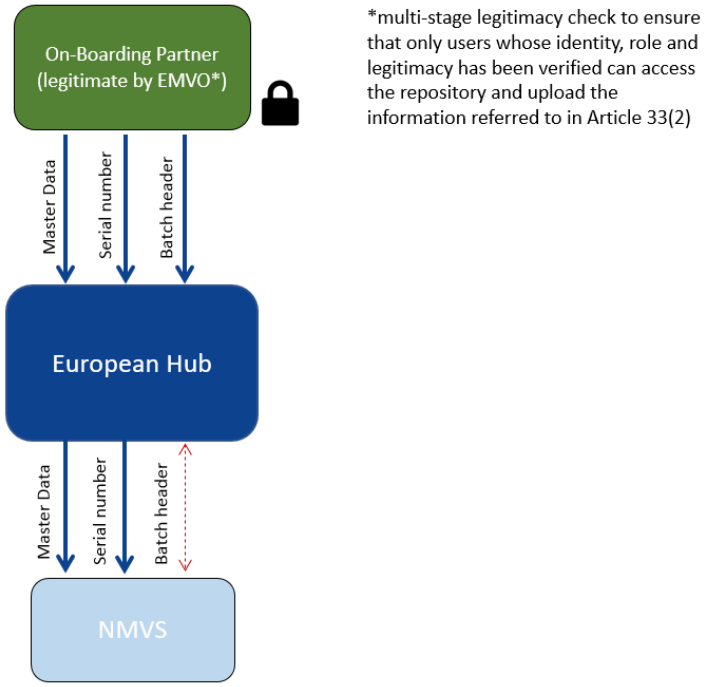
1 Introduction

When the original European Medicines Verification System (EMVS) was scoped and specified security was, and remains, the highest priority for system design and robustness. The original system was designed to have a single entry point for all inbound data to funnel the uploaded data as a trusted 3rd party out to the various member state satellite systems. The primary rationale for designing the system in this way from a security point of view was simple. If we ensured that all connecting parties who 'inject' data to the system come in through one single point and have a robust system to verify their need to connect, the entire European system can be robustly secured by building a strong security wall around the single connection point, the European Hub (EU Hub).

As with any system, integrity and security are only as strong as the weakest point and thus, if the security and verification process for connecting parties was delegated to one or more National Medicines Verification Systems (NMVS), those systems would have to adopt similarly secure and thorough processes to avoid the risk that one or more were weaker in this regard and would thus open the entire EMVS landscape up to the risk fake data injection via the weakest connection point.

The EMVS User Requirement Specification (URS) currently considers that all master data should be injected into the system via the EU Hub by parties who have successfully passed a multi-stage legitimacy check. The URS also allows for batch and pack data to be injected into the system either by use of the same EU Hub interface (used for the master data injection) or to a national injection point where the batch header information is subsequently shared with the EU Hub (note, not the serial ID's).

Pictorially the system is described by the EMVS URS as follows.



The support for national injection of batch data adds considerable system cost and ideally would not be supported, however this scheme is secure a position since it ensures system integrity whilst still offering some increased flexibility to those marketing authorisation holders (MAH) who are prepared to fund the extra functionality provided.

1.1 Delegated Regulation

When the Delegated Regulation (DR) was published in February 2016, it allowed for the possibility to upload data via the NMVS. Article 33 (3) deals with this directly stating that "The information referred to in paragraph 2 shall be uploaded to the repositories system [the EMVS] either through the hub or through a national or supranational repository [the NMVS]" which imposes the requirement to provide at least one of these options, the EMVS provides the one via the EU Hub. The same paragraph goes on to state that "Where the upload is performed through a national or supranational repository [the NMVS], that repository shall immediately transfer to the hub a copy of the information referred to in paragraph 2(a) to (d), with the exception of the serial number, using the data format and data exchange specifications defined by the hub." This last part puts restrictions on the system design and places the responsibility for this interface design clearly upon the EU Hub, thus European Medicines Verification Organisation (EMVO).

Article 34(4) also states that "When it receives the information referred to in Article 35(4), the hub shall ensure the electronic linking of the batch numbers before and after the repackaging or re-labelling operations with the set of unique identifiers decommissioned and with the set of equivalent unique identifiers placed.

Article 39(a) describes the access and supervision requirements for National Competent Authorities (NCA's). Uploading data via the EU Hub does not in any way restrict any future access or supervision by NCA's and is fully compliant with the requirements as defined by Article 39(a).

Article 31(1) describes that the repositories system shall be set up and managed by stakeholders. Therefore, the cost increasing decision to implement a national upload interface can only be made by stakeholders.

Article 31(5) states that manufacturers (marketing authorisation holders) have to bear the costs of the repositories system. Stakeholders on national level should take into account that the implementation of a national upload interface jeopardises the cost-effectiveness of the pan-European medicines verification system and increases the cost for of their repository tremendously for the following reasons:

1. Extra functionality within the NMVS.
2. Extra functionality within the EU Hub.
3. Operation of a national upload interface (including technical support for MAH).
4. Execution of an additional multi-stage MAH legitimacy check at national level.

Manufacturers/MAHs must be aware that they have to pay a higher flat fee if a National Medicines Verification Organisation (NMVO) introduce a national upload interface since all extra costs that are

caused by the selection of national data upload (on a national and European level as described above in point 1 - 4) will be borne by the relevant national industry.

Article 37(b) describes the requirement for each connecting party to be subject to a process that confirms their identity and legitimacy. "…put in place security procedures ensuring that only users whose identity, role and legitimacy has been verified can access the repository or upload the information referred to in Article 33(2)". To this end, having a single entry point where each and every connecting party has been subject to a thorough and rigorous legitimacy checking process maximises the security of the system overall. This is further discussed in section 2.2.

1.1.1 Pack Data

The DR defines the requirements for the data flow of the pack Unique Identifiers, otherwise referred to more generally as 'the serial numbers': These are expressly forbidden by the DR for transmission from a national repository to the EU Hub. This is stated in Article 33(3) "…the information referred to in paragraph 2(a) to (d), with the exception of the serial number…". As such, serial numbers/pack data uploaded locally to a national system will not be sent to the EU Hub and can therefore not be distributed by the EU Hub to other markets in case the master data indicates that the product code is multi-market. This Article therefore obliges an MAH to upload multi-market pack data to each market in turn if a national upload option were adopted.

What the article does not prevent, and what the EU Hub will fully support, is the exchange of the batch header information (batch number, expiry date and batch status). This information has to be transferred to the EU Hub to allow the EU Hub to correctly respond to multi-market pack decommissioning operations and also recall/withdrawal operations when invoked centrally. The information is also critical to the function of parallel distribution and thus must be supported by all parties for all packs (i.e. not just multi-market packs).

When batch header data is transferred from the national system to the EU Hub, the data sent must carry an identification of the data owner that is recognised by the EU Hub to ensure the data is correctly attributed to an On-boarding Partner (OBP) account. This means therefore that every MAH – even if they opt for national data upload – must register directly as an OPB or indirectly (represented by an OBP) with the EU Hub.

1.1.2 Master Data

Master data is critical to the operation of the system. For master data to be loaded, many attributes have to be in place prior to the upload. The OBP has to have a valid and active account with the EU Hub, the data has to be validated by the EU Hub to ensure that the product code does not belong to another party. The identity of the MAH declared within the market data segment is pre-known by the EU Hub as belonging to the OBP organisational structure as well as checking other attributes for data content and dimension.

To undertake all of this in a secure manner, it is vital that the OBP has already been subject to a successful verification process (as described above). Only then will an OBP account be created and only then EMVO can be sure that this OBP has a valid need to use the EMVS and is able to upload data. To ensure that this process is fully discharged and to ensure that security/integrity of each OBP

account and the associated data is maintained, the specification for the interface between the EU Hub and the national repositories only supports the transfer of master data in one direction, EU Hub → national repository. As a result, master data can only be uploaded to the EMVS via the EU Hub.

1.1.3 Parallel Distribution

As a result of Article 34 (4) and in order to prevent the transfer of serial numbers from the national repository to the EU Hub when uploading data, parallel distributors have only the option of interfacing with the EU Hub as to do otherwise would prevent them from discharging their duties under the DR with respect to the issues raised in Article 34.

2 System Security

The following is a brief outline of some aspects regarding data and connection security that build to provide an understanding of the rationale behind the statements made above.

2.1 European Hub External Security

There are multiple aspects to securing the components of any IT infrastructure. Clearly the system has physical security mechanisms around it and it supports a highly robust and secure means of authenticating users and also detecting connection hijack/hack attempts. However, a robust IT security system is worth nothing if the processes and procedures to grant initial access to the system are not similarly robust and thorough. As such, each connecting party, who are referred to as OBP's, including a complete verification process to determine the identity of their organisation, the key nominated personnel, the MAH structure and the sales of medicinal product. Only once this thorough process has been completed with a positive outcome, is the OBP permitted to even start the connection process.

2.2 European Hub Internal Security

This paper is not the place to describe the internal construction of the EU Hub in detail, which is confidential in nature; instead the key considerations are briefly described.

One of the primary considerations when designing a system that is used by multiple stakeholders who each have a desire to retain the privacy of their own data - is to ensure that any data taken into the system is attributed to its owner and then subsequently ensure that only the data owner can access the data (accepting the occasions where more general access may be permitted). To achieve this, each data owner is allocated to a user account post the verification process previously described and all data uploaded on their behalf is attributed to their account. This ensures that other accounts cannot access data that is not managed by them and ensures that all data in the system is attributed to a valid, verified owner.

Keeping this in mind, it should be clear that the only means by which data entries for any given OBP can be created in the EU Hub, is via the primary OBP interface with the EU Hub. It should also be clear that each OBP, regardless of where they might like to upload data, has to have a valid ID within the EU Hub.

2.3 National Repository Security

Each NMVS will require a user verification process that broadly follows the same ideals and functions used by EMVO for OBP's. However, any such process is outside of the verification process applied by EMVO and therefore cannot act as a proxy for the process adopted by EMVO. EMVO has responsibilities for the action of granting access to the system. This cannot be delegated to an NMVO without the potential for delegating risk and liability. Therefore, no such delegation of security and account verification is foreseen.

When the EU Hub distributes master data it will also distribute the identity of the OBP by means of the product code and MAH designation. It is the absolute responsibility of each NMVS/NMVO to securely maintain this information and ensure that in the event a national data upload capability is implemented that the ID of each OBP is correctly attributed to the batch header data passed over the interface. Failure to undertake this responsibility reliably could result in batch data being assigned to the incorrect OBP resulting in pack synchronisation issues, parallel distribution activity failures and data leakage. None of these are acceptable.

3 System Efficiency

The overall purpose of the EMVS is well documented with the primary goal being to provide a common means by which medicinal packs can be systematically verified and decommissioned in the interests of increased patient safety resulting from the prevention of dispensation of falsified medicines. In addition, the bulk of the system has to be funded by the pharmaceutical industry and as such, it is important that the purpose of the system is executed in an efficient and cost effective manner.

4 European Hub as a Benefit.

The European hub could be viewed, at a superficial level, as an extra complication and an extra cost burden however it is vital to understand more completely some of the reasons why the EU Hub represents an overall benefit over time. These reasons include:

1. Improved system interoperability.
2. Overall cost effectiveness.
3. Ability to fully support cross-border trade in a standardised manner.

The use of the European Hub does not impact or restrict the use of the system by MAHs who 'only' produce for a local market. The local market product argument is a complex one however it's important to realise that an MAH has little control over the distribution of their product when the product is open for cross-border trade/repacking. As such, it is vital that the product is 'known' beyond

the boundaries of the originally intended marketplace. The centralised data injection point in no way provides a disadvantage to these 'local' MAHs, indeed the European Hub and the centralised approach provides an advantage – at worst no disadvantage over a more local approach. The centralised upload of data to the European Hub is not an anti-competitive approach (as confirmed by legal consultation) and offers a more organised, efficient and cost-effective solution for all parties.

4.1.1 System Interoperability

If one were to imagine a scenario where the European Hub did not exist we would be left with the situation where all 32 countries (EU + EEA + Switzerland) would have their own national system (or supra-national systems) and all would be faced with the dilemma of "how do we now make our system communicate with all the relevant MAHs and how do we make our system communicate with all of the other (31) national systems".

It is clear that it would be theoretically possible to define communication standards to permit each national system to communicate with each other in the same manner. It is also clear that it would be theoretically possible to define a common set of standards by which all MAHs would communicate with all national systems. However, to achieve this would be politically challenging and the more likely outcome is a scenario where each of the national systems implements a similar but subtly different interface standard for MAHs. The inter-connectivity between national systems would result in a multiplicity of different connection standards between systems. Even if the time were available to resolve all these issues, without a common central connection point (the European Hub), MAHs would have to maintain and connect to multiple national systems potentially using different connection mechanisms and every national systems would, worst case, have to support the 31 different connections to other national systems and implement these complexities to handle cross border trade, inter-market queries, standardised product withdrawal and standardised batch recall. The practicalities of this are extreme and could take years to overcome, resulting in a delayed implementation and a potentially vastly increased cost. By implementing the European Hub, the MAH interfaces are standardised by default and the inter-connectivity between national systems is standardised by default.

The only other approach that would provide similar inter-operability advantages would be to have one single central European system to which all end users (MAHs, Wholesalers and Pharmacies etc.) connected to across the whole of Europe. This was considered, from a political point of view, very unlikely to be acceptable and provided an increased challenge as a vast single point of failure.

4.1.2 Overall Cost Effectiveness

Much of this has been eluded to in the previous section. By enforcing the communications and interface standards between national systems and MAHs, the European Hub minimised the number of connections each has to develop and subsequently support. The European Hub also handles the complexities of distributing MAH data (Article 33(2)) to the specific national systems that require it. Over time the cost profile of the system will be significantly reduced as a result of the European Hub.

4.1.3 Cross Border Trade

Without the European Hub each cross-border trade movement would have to be targeted by the Parallel Distributor in terms of where the goods came from and where they were sent to. There would be no single authoritative system to manage and reconcile the trade movements. As a result, none of the aspects contained within the DR pertaining the cross-border trade could be effectively or practically realised. In addition, inter-market queries to support compassionate use products or products that are legitimately used in a market but originates from another would be more complex than a solution that is provided centrally by one single entity.