Falsified Medicines Directive

User Implementation Belgium and GD Luxembourg

End User software development

Purpose of this document

The purpose of this document is to have a high level overview of the different work packages that are part of the end user development for the implementation of the verification activity and the connection to the verification database (BMVS). Detailed and more extended information is available in the NMVS Implementation Guidelines on the Arvato development portal.

Further, this document is listing the activities the end users must apply to be compliant with the FMD regulation.

The objective of this document is not to give a detailed specifications for each work package or the way the different activities for the end users are implemented in his processes.
More details on the technical and development aspects can be sourced from the extended documentation and specification on the development portal of Arvato.
The way the processes will need to be executed b the end users is dependent on the specific configuration of the different user systems, the processes and procedures that are currently being used by the use and the type of user and the FMD actions that are proper to his situation.

However, this overview should contain the main parts that need to be implemented for the end user to be FMD compliant.

Content of this document

A_ Work packages: elements to consider for implementing FMD in the end user system

B_ End User FMD activity: FMD processes that the end user must perform

- Wholesalers
- Pharmacies

A. Work packages

This chapter lists a set of work packages that need to be looked at by the software department or vendor when designing the implementation of FMD at the level of the end users.

1. Scanner configuration & settings

The 2D scanner of the user must be configured to read the 2D matrix on BE packs but also on packs from countries where the 2D content deviates from the Belgian standard. Dependent on the hardware of the user, the settings might be different.
Also, the signal from the 2D scanner to the user's hardware needs to be set correctly (eg keyboard dependent). An idea might be to provide the user with a sample 2D matrix (eg containing a code like ABC123klm098) allowing the user to test the scanner when this would be needed.

2. Interpretation of scanned information

The scanned information must be decomposed to be processed in the user system. The GS1 standards are to be applied for Belgian products where the GTin is used. For packs from a country using an NTin the same rules apply, but can be different for packs from countries using a PPN. Therefore through the scanning and the interpretation of the scanned information the type of code GTin/Ntin or PPN must be identified and stored. There need also to be a process allowing the user to enter the product information and pack codes manually in case the scanner is not working.

3. GTIN-CNK conversion

Process and functionality to import the reference file containing the bridge from GTIN to CNK. Business rules for importing the conversion table and handling of errors at import of the conversion table. Business rules in the Client system to handle errors in the use of the conversion table, eg. "Gtin not found". Similar a business rule must be implemented in case a PPN is being identified in the 2D. Further, a business rule can be implemented to use the back-up solution, ie where the CNK is being returned in the response to the web service query.

Through the web services, when submitting a verification or a transaction query, the response from the verification repository will also include the national number entered by the MAH when loading the product and pack data (see Arvato implementation guidelines and technical documentation). For Belgian products, the CNK will be included. This information can be used if the GTIN cannot be found in the conversion table.
To note for Luxembourg users that for products registered in Luxembourg as from German origin the PZN will be returned and for products registered as from French origin, the CIP13 will be returned.

4. Handling pack information

Process to store the data from the 2D matrix scan in the Client system for further use. Use of the data can be linked to FMD, but can also be linked to other functionality that is present or to be developed in the Client system. Expiry date can be used for stock management. Batch number can be used in case of a recall of batch. GTIN and UI have to be used for transmission to OT/TD.

5. Pre-filtering for generating the web service

The web service needs only to be generated and send to the system for those packs that are in scope for FMD. Para-pharmaceuticals, medical devices, veterinary products… can also have a 2D matrix code, but for these products the web service should not be started because a negative result will be returned.

For that reason a pre-filtering needs to be built in the user system to submit only queries for products in scope.

6. Create the 'data packs' for the different web services

The data packs for the different web services need to contain specific information elements in a documented XML format. Some of these data elements are not coming from the 2D scan, but need to be retrieved from the Client system (User identification, SW system and version, unique transaction ID, …).

The type of data packs needs also to be triggered from the user system. Is the web service called for verification only, for decommissioning as delivery, as pack for export, as pack for destroyed, …

Besides the type of transaction, the user needs also to identify if it is a single pack transaction or a bulk transaction (homogeneous or heterogeneous).

Besides the 'transactional' web services, there are also admin services that can be called from the users system, such as, download master data, change password, … These need to be included as a functionality in the user's system.

7. Transmission approach

Client system processes to implement for the different ways of submitting verification requests (including decommission, …) to the BMVS.
The different approaches are:

- Single pack synchronous transaction
    - Execute web service on each scan immediately with immediate response.
- Single pack buffered synchronous transaction
    - Buffer scans and execute web services in back ground while the user is scanning other packs; responses can also be buffered and released later or immediate at reception; display all responses or global response (eg 'all OK') to the user.
    - Buffer scans and execute web services when user closing transaction with his client; transmit all scans in single mode; receive immediate response and construct answer/message (global or by pack) for the user.
- Asynchronous Bulk transmission
    - Bulk transmission after transaction closure with response request in background; run in back ground response request web service until response received; construct answer/message for user.

Related to this also the processes for:

- Synchronous Undo transaction

8. Connection type for web services

Connect each workstation from the user separately to BMVS or connect through an internal server (ie accumulation connection) where all end users are at the same location.

In case the different end users of the same organization are at different locations (eg wholesaler with several warehouses), the different end users can be connected directly to the NMVS system or also through a central server where the different end users (at different locations) are identified by a sub-user ID.

9. Client to BMVS connection

This concerns the management of the user credentials, needed to connect the user to the BMVS using login, password and certificate according the documented procedure.
The management of the user credentials should best be automated in the user's system in such way the update process is running in background and transparent for the user. This can be done by storing the date when the password/certificate was last updated and schedule the update task xx days before the next update is required. Automatic update can then be done using the available webservices for these actions. (In a future release, the MVS system will also send a message to the user's system when the update is required).
Be aware that the user will also need his login & password to access the Web GUI. You might implement a function to display the password information to the user.

Further, implement the processes around the acceptance of the Terms&Conditions (T&C) and the Data Privacy Policy (DPP). This process is required when the user is connecting for the first time to the verification system, but the end user system must also be able to process future updates of the T&C and DPP, with alerts during the grace period reminding the end user to confirm the updated T&C and DPP. This process needs to be managed in the user's system based on the messages received through web services from the verification system.

10. Web service response – Return code and message handling

Process and business rules for receiving, reading, translating and handling of the responses from BMVS to Client system and display on the client system screen. Impact on business rules in the Client system.

Process for handling return and message codes received from BMVS.

- Admin related codes (eg wrong password, …)
- Data related codes (eg product unknown, already dispensed, …)

Certain return codes will require action from the user.
In case of admin related codes, this can be eg the fact the user needs to update his password, or that the user needs to accept a new version of the T&C.
Data related return codes can indicate a potential alert. In such case, the user needs to perform a number of actions (verify the scanned versus the printed codes on the pack, verify the settings of his scanner, provide information for further investigation, …). The user should be guided in his system through these actions.

11. Implement admin web services

- Information services
    - Download product master
- Connection services
    - Password change
    - Download certificate
    - Renew certificate

Process for generating and processing the result of these services in the Client system.

12. GUI interface

Integrate process for connecting to BMVS using the GUI interface in the web browser. Install the certificate in the browser to allow access to the GUI. The GUI is needed for manual input of limited transactions (eg when the scanner does not work or the 2D matrix is damaged).

13. Transition phase

The transition phase between now and February 2019 is requiring specific functions to allow the user to cope with the mixed situation of 'older' and 'newer' packs, situations where packs are on the market but codes not yet loaded by the MAH, … It is advised that all messages coming as response to the web services are displayed in a 'low profile' way.

But also after 9/2/2019 there will be a mix of 'older' and 'newer' packs on the market. In case packs containing both the 2D matric with a UI and a linear barcode with a serial number, the user should only be able to scan and store one of both.
In case of a reimbursable pack with a 2D and UI, but still also containing a linear but without srial number, the user must be alerted in case he scans the linear (without the serial number).

14. End user instructions

The user will need to receive the necessary information and documentation on how to use the system and how to handle specific processes such as changing password, renew certificate, … The way these are implemented in the system will differ from SW to SW.

The clearer the procedures are explained and documented for the user, the less support will be needed.

All technical information regarding the web services, the GUI, the overall elements related to the user on boarding, … can be found on the development portal of Arvato:

https://www.sws-nmvs.eu

This portal gives also the access to the software integration platform containing test scripts that can be used for testing the developments.

After development and certification by Arvato, the user can be connected to the live Production environment of the verification repository.

The connection to the Production environment will be available as from February 2018.

At that moment starts also the Pilot period. During this period, the BeMVO will closely observe all activity from the users and feed back where necessary to the development teams where optimization possibilities are identified.
The Pilot period with additional support from BeMVO for the development implementation will run until April 2018.

In parallel the roll out to the different users should start aiming to be finished by August 2018.

B. End User FMD activity

As from 9 FEB 2019 the execution of the rules defined for the end users in the Delegated Regulation become mandatory. The cases where the end user needs to verify the code on a pack or where the user needs to change the status of the pack are different depending on the type of user.

Wholesalers

The general principle for wholesalers is a risk based verification. This means that the wholesaler needs to verify the pack code where a falsification risk can be assumed.
More specifically this is the case when he receives a pack

- returned to him from the pharmacy or hospital (or other client)
- from another wholesaler who is not the manufacturer/MAH or a wholesaler acting on behalf of the manufacturer/MAH

The wholesaler also needs to decommission the pack when

- the pack is exported outside the EU
- the pack is returned to him (by pharmacy, …) and he cannot take the pack back into the saleable stock
- the pack is intended for destruction
- the pack is provided to the authorities as a sample
- the pack is sold to persons or institutions which are outside the traditional supply chain (see list in chapter C.)

If the result of the verification indicates that the pack has no longer the status “active”, the wholesaler must evaluate if the pack is a potential falsification.
See the document with the “Falsified pack” alert procedure.

Pharmacies

The pharmacy must verify the pack at the moment when the pack is supplied to the public. The pharmacy can also scan and verify the pack earlier, eg at reception, but anyhow a verification and especially the decommissioning of the pack must be done at the moment of delivery.

An exception exists for the hospital pharmacy.
The hospital pharmacy can verify and decommission the pack at any moment when the pack is in his possession, so also when receiving the pack, provided that after the decommissioning the pack is supplied within the hospital.

The pharmacy also needs to verify and decommission the pack when

- the pack cannot be returned to the wholesaler or manufacturer
- the pack is provided to the authorities as a sample
- the pack is subsequently used as authorized investigational medicinal product or as authorized auxiliary medicinal product [EU Regulation 536/2014, 2(2),(9) and (10)]

The pharmacy is exempted from the verification and decommissioning if the product is provided to him as a free sample. But the pharmacy has to verify the anti-tampering device of the sample.
A hospital pharmacy can also be exempted if the decommissioning was done by a wholesaler who

belongs to the same legal entity as the hospital, there was no sale between the wholesaler and the hospital and the product is supplied within the hospital.

In case the pharmacy is only supplying part of the pack, the verification and decommissioning must be done at the moment when the pack is opened for the first time.

If the pharmacy has a technical problem and cannot connect directly with his system to the verification database, then the pharmacy has 2 options

- he can use the web interface in his web browser and enter the codes manually for verification and decommissioning
- if not, he must store the codes in his system and submit the codes for verification and decommissioning as soon as his system is again connected to the verification database

If the result of the verification indicates that the pack has no longer the status “active”, the wholesaler must evaluate if the pack is a potential falsification.
See the document with the “Falsified pack” alert procedure.