Requirements to an end-user software with integration to NoMVS – direct or indirect

Nomvec and the software suppliers (SWS) providing software for end users who is obliged to comply to FMD, must strive for a unified implementation of the Falsified Medicines Directive (2011/62/EU), and subsequently {{Delegated Regulation (EU) 2016/161. Considering this joint responsibility, it is important that end-users can rely on correct, fully interpreted and timely processed information. All processes related to scanning, sending and receiving transactions to NoMVS must be processed correctly and consistently within the end-user software information systems.

To ensure this, requirements that lay down the minimum functional and technical requirements that SWSs must meet have been drawn up. These requirements provide a common quality framework that supports developers in the correct implementation, data processing and communication between the NoMVS and the end-user software.

Nomvec will invite the SWS to a start-up meeting for all new SWSs to have a walk-through of Nomvecs requirements and the NMVS SWS-portal, where all relevant technical documentation regarding development and integration to a Medicines Verification System is located.

Requirements for an integration with NoMVS

To ensure that the NoMVS integration is of good quality and that the information presented to the end-user is correct, Nomvec has the following requirements in relation to the development of end user software:

Scans:

- The software must be able to read a 2D matrix code in full, and interpret the GS1 Application Identifiers:
    - (01) Global Trade Item Number (GTIN)

Nomvec AS
Essendropsgate 3
0368 Oslo
Norge

Organisasjonsnummer 818 142 382
post@nomvec.no
Prodspoc@nomvec.no
mahsupport@nomvec.no

- (10) Batch or lot number
- (17) Expiration Date (YYMMDD)
- (21) Serial number

Note: Some manufacturers of human medicinal products encodes a fifth element into their 2D-matrix code, and it will be of benefit that the end user software is able to read and ignore a potential fifth element without causing a system error if present.

- The data contained in the 2D-matrix code and read by the software by means of scan or manual entry must be transmitted to the NoMVS in full and without any modification.
- The response from the NoMVS to a transaction from the end user system must be received and presented to the end-user in full and unchanged via the end-user software. It must be visible to the end-user in real time, without delay.
- If NoMVS does not recognize the data sent from the end user software, or the end user is attempting an action that is not allowed, an exception is received from the NoMVS. The exception is given as a return code and a return code message. Both must be presented to the end user as received from the NoMVS, unchanged and unmodified.
- Repeated exceptions on one pack shall not be filtered out. Any re must be passed on immediately, completely and unaltered to the end-user.

Quality assurance:

- The SWS is required to provide a technical and functional description of the end-user software integration with NoMVS to Nomvec.
- If areas for improvement are found, Nomvec consults with the SWS. In the absence of agreement on an improvement plan, Nomvec is mandated by Norway's competent authority to issue instructions to arrive at a situation where the end user system complies with the applicable laws and regulations, agreements and this protocol.

- Confidential information exchanged in the context of quality assurance activities will be treated as such by Nomvec and will not be shared with third parties, unless this is required by law.

Receiving and sending transactions

Exceptions and Return codes

Every transaction (request) to the NoMVS is answered with a response containing information such as the return code and a description. If the transaction has been managed successfully by the NoMVS the return code is NMVS_SUCCESS and the return code description is Successfully processed.

If NoMVS does not recognize the data sent from the end user software, or the end user is attempting an action that is not allowed, an exception is received from the NoMVS. The response from NoMVS is either an L1 to L4 exception or an L5 exception, which also contains a unique alert ID. L1 exceptions are managed by the NoMVS itself, and never reaches the end user.

L2 exceptions are a warning from the system that may indicate issues related to connectivity or the end-user's account.

L4 exceptions are exceptions indicating that a transaction attempt is not allowed due to different reasons, such as the pack has expired or the undo transactions is performed too late (after 10 days).

L5 exception contains a unique alertID and indicates that the pack data is not recognized or that the transaction attempted is not allowed (for other reasons than the one returning L4-exceptions).

In all cases of exceptions, the following information is included in the response from NoMVS. This information must be presented to the end-user immediately and unaltered:

- Pack state (e.g active/inactive/unknown)

- Pack State Reason
- Return Code
- Return Code Description
- Sub Code
- Sub Code Description
- Alert ID

L5 exception

The following return codes with description are classified as L5 exception (with an alertID):

Return Code	Return Code Description
NMVS_FE_LOT_03	Failed to find a batch for the given data.
NMVS_FE_LOT_12	Expiry date does not match the date held in the NMVS.
NMVS_FE_LOT_13	The batch ID does not match the serial number in the NMVS
NMVS_NC_PC_02	Unknown serial number.
NMVS_NC_PCK_06	Actual pack status doesn't match the undo transaction
NMVS_NC_PCK_19	Property already set on pack
NMVS_NC_PCK_22	Pack is already inactive
NMVS_NC_PCK_27	Status change could not be performed

L3-4 Exception

Norwegian authorities have required NO end users to act upon several exceptions of level 3 or 4. It is therefore important that these exceptions are visible to the end user immediately:

Return Code	Return Code Description
NMVS_NC_PC_01	Unknown product code.

Return Code	Return Code Description
NMVS_NC_PC_15	This product or batch is not in scope of FMD regulations.
NMVS_NC_PCK_20	Defined timeframe between setting this property and the undo was exceeded.
NMVS_NC_PCK_21	Undo can only be executed by the same user who previously set the attribute
NMVS_NC_PCK_23	Re-setting of the property via double scan is registered. NMVS_NC_PCK_28 – Property is already set on pack (no alert). NMVS_NC_PCK_30 – Pack is already inactive (no alert).
NMVS_TE_REQ_01	System unavailable.
NMVS_TE_REQ_03	The connection attempt from the NMVS to the HUB failed. NMVS_TE_REQ_04 – Connection to the HUB was successful, but the HUB does not respond within the agreed timeframe.

**This list is not exhaustive*

L2 Exception

Nomvec advises displaying the response with L2 exceptions, so that the end-user can contact Nomvec or the SWS if problems occur. Below is a list of the most common L2 exceptions:

Return Code	Return Code Description
NMVS_FE_AU_01	The entered user or password does not match.
NMVS_FE_AU_02	The user is locked, login is not possible.
NMVS_FE_AU_10	Entered password does not match the stored current password.
NMVS_FE_AU_11	The entered password is either expired or an initial password. Please renew your password.
NMVS_FE_TX_02	Transaction ID unknown or the processing result is not yet available.

**This list is not exhaustive*

L2 Warnings (Information message)

Due to issues with scanners switching upper case to lower case if CapsLock is enabled, and re-setting of keyboard language of scanners from QWERTY to QWERTZ, a functionality is developed in NoMVS to check for these causes in cases where the packs Unique Identifier (UI) is not recognized. If the UI is then found, the packs are processed as normal, and NoMVS returns a warning to the end user. These warnings must be presented to the end user, alongside that the pack has been verified or decommissioned successfully.

Return Code	Return Code Description
NMVS_WARN_SCAN_01	Processed with warnings. Check uppercase-lowercase configuration of the scanner to rule out potential counterfeit.
NMVS_WARN_SCAN_02	Processed with warnings. Check regional configuration of the scanner to rule out potential counterfeit

Nomvec is responsible for translation of the most common exceptions to Norwegian. A SWS must show it to the end-user, without any editing. Changes to return codes are possible, about which the Nomvec will communicate in a timely manner.

Manual entry

The NoMVS has two separate transactions for Verify Single Pack and Dispense Single Pack to distinguish between data that comes in from a scan has and those where the data has been manually entered (typed) by means of a keyboard. Scanned entries requires all four parameters (GTIN, batch, serial number and expiry date). Manually typed entries requires only two parameters (GTIN and SN).

For the risk analysis of alerts, it is important to know whether the data in the transaction was entered manually or provided by a scan. One example of when an end-user is in need of manually entering the UIs is when the 2D Metrics code is not possible to scan.

For transactions where the data fields are fed by a scan, the following transactions must be used:

- G110 Verify single pack (Pharmacy & Wholesaler)
- G120 Dispense single pack (Pharmacy & Wholesaler)

For transactions where the fields are fed via manual input with a keyboard with only the two parameters GTIN and SN, the following transactions must be used:

- G112 Manual verify single pack (Pharmacy & Wholesaler)
- G122 Manual dispense single pack (Pharmacy & Wholesaler)

Per design the manual transaction types G112 and G122 are not propagated from NoMVS to the EU Hub, as the EU Hub does not know the batch, and thus cannot send the transaction to the right NMVS for handling there.

In order to manually verify and decommission packs not uploaded to NoMVS (unlicensed medicines etc), it is highly recommended by Nomvec that the end user in these cases are able to enter all four parameters manually, and that such transactions

are sent to NoMVS as either G110 (Verify Single Pack) or G120 (Dispence Single Pack). (This in addition to the possibility to only use two parameters for manual verify and dispence for NO packs, which is easier and provides less typing related exceptions.)

Data integrity

With some exceptions, as provided in Annex I of the Delegated Regulation (EU) 2016/161, all medicinal products subject to presecription only in the EU- or EEA countries to which they are marketed, are provided with a 2D-matix code with information of the packs UI are encoded (product code/GTIN, serial number, batch number and expiry date).

The information in the 2D-matrix code is uploaded by the manufacturer to the NoMVS and shall correspond 1 to 1 with the data on the medicinal pack.

Nomvec manages the Norwegian translations of the return codes in NoMVS. These translations might change if the functionality in the NoMVS change, or if Nomvec recognises the need to specify the NO translation better. To enable the end users to see the complete and correct information in the response from NoMVS mentioned in chapter 5.2.1 this must be presented to the end-user in the GUI. Nomvec will not instruct the SWS how to implement this in their software since this is a matter of GUI design. The requirement from Nomvec is that the information mentioned in chapter 5.2.1 must, when available, must be presented in a complete manner e.g. as dialogue boxes or in the GUI directly.

The only source for data sent to NoMVS shall be the UI as printed on the pack. The NoMVS shall be the only source consulted by the end-user's software for FMD control. It is therefore not allowed to use other sources to send data to the NoMVS, and it is not allowed to modify the response from NoMVS or internally map the response to any internal translations etc. If such happen, no correct FMD control takes place.

If Nomvec discovers that another source is being used, the SWS will be contacted.

Certificate and passwords

A user-ID, certificate and password are required to connect to the NoMVS. A NoMVS UserID is created by Nomvec and the NoMVS issues the NoMVS user certificate after Nomvec has approved the end user's legitimacy and checked that their chosen end-user software has an approved FMD integration.

The NoMVS credentials are confidential and unique to each user. The responsibility for the correct management of the certificate and password is the end-user's responsibility.

Download and install certificate

The certificate can only be used by the user to whom the certificate is linked. This makes the certificate unique to that end-user. For security reasons the certificate must be renewed every two years. This process is automatically initiated by NoMVS, and the new certificate is issued 60 days prior expiry date and sent the end user via an email from NoMVS, together with a TAN that is required for downloading the certificate. From 30 days prior expiry date, a reminder email is sent from NoMVS to the email address that is registered on the NoMVS user profile in NoMVS Core.

Without timely renewal, the user will lose their connection to NoMVS in their respective end-user software. It is therefore important that an end-user is given the opportunity to renew the certificate in a timely manner. If this functionality does not exist in the end-user software and the user is dependent on the SWS to arrange the download and installation, the SWS must take care of this for the user. In case the old certificate has expired, the SWS must take care of the installation of the new one as soon as possible, to enable the end user to be compliant to the FMD regulations.

Change password

Every end-user software must have the function changing the password of the NoMVS user. Nomvec has set the frequency for password change to every 365 days, which will be notified by email to the registered email address for the end user.

There are no limitations for a more frequent password change, if this is required by the SWS's or end user's policies.

NMVS Software Supplier Portal

The NoMVS is still under development and may therefore change. In order not to let the communication from Nomvec fail, it is therefore important to keep the contact details of the SWS up-to-date.

The NMVS Software Supplier Portal (SWS-portal) is a web portal operated by Arvato Systems for SWSs and internal IT teams that need to connect their systems to a country's National Medicines Verification System (NMVS) under the EU Falsified Medicines Directive (FMD).

The portal provides everything required for developing against and integrating with Arvato-operated NMVS, including:

- Registration and approval workflow
- Technical documentation and API/WSDL specifications
- Integration and testing environments
- Baseline test packs
- News, updates, and FAQs
- Rollout guidance for production deployment

Baseline Testing – The NMVS Software Supplier Portal

All end user systems must pass a baseline test before access to the PROD environment can be granted by Nomvec. The NMVS SWS Portal provides test packs, test documentation and test report templates.

The results of the baseline tests shall be documented by the means of screenshots and uploaded to the SWS portal.

Nomvec will review and ensure that all required tests have been performed and passed. This must be in place before Nomvec can approve the end-user software for NoMVS integrational purposes.

Changing Pharmacy Interface version

To ensure and develop proper functioning of the NoMVS, enhance security or to implement new return codes, new versions of the NoMVS Pharmacy Interface may be created. SWSs are obliged to implement these new versions. In most cases, this time frame will be sufficient for the SWS to make the necessary changes.

The SWSs must perform a new baseline test when updating the interface version to ensure the correct implementation of the new functionality on the new interface version, before the new version of the NoMVS Pharmacy interface is taken into use. Arvato Systems will inform when new interface versions are available via the SWS portal. The new Pharmacy Interface Versions are the link between the end user software and the NoMVS and are separate from the functional releases of the NoMVS and might change every 2 to 3 years.

SWSs must perform testing activities exclusively in a specific test environment (NMVS Sandbox).

Changes to contact details

The NoMVS is continuously being developed, and functionality, interfaces, return codes or other parts may therefore change. In order be able to receive and act on communication from Nomvec regarding important changes, it is important to keep the contact details of the SWS up to date.

Nomvec keeps records of all SWSs that have performed a baseline test for the NoMVS. To guarantee communication, it is important that SWSs report changes in company details and contact persons to Nomvec. The contact details are also used to communicate software problems, Therefore, Nomvec needs the following information:

- Company name
- Company Address
- General telephone number
- General email address
- Name of the end-user software that has an integration to the NoMVS
- First and last name of the contact person
- Position of the contact person
- Contact email address
- Contact phone number

Processing end-user software name and company name in transactions

In the transactions that are sent to the NoMVS, the name of the software the transactions is performed through and the company that provides the software is mentioned. This information is required for proper investigation of alerts by Nomvec.

Examples

Processed transactions

A processed transaction means that the end-user software receives a response from NoMVS. The response may indicate that the requested operation was completed successfully, or that an exception occurred.

There are five main response variants, that may need to be presented to the end user:

- Operation completed successfully, with no exception or information message.
- Operation completed successfully, with no exception but with an information message.
- Response containing an exception without an Alert ID.
- Response containing an exception with an Alert ID.
- Response containing an exception with an Alert ID and a warning (e.g WARN_SCAN_01).

These five variants are also listed in the chapter Responses and Requests to and from the NoMVS.

Where included in the response, the end-user software should present the relevant information returned by NoMVS, including:

- Pack state and pack-state reason
- Return code and return-code description
- Subcode and subcode description
- Alert ID
- Information or notification message

As mentioned above, the NoMVS return code descriptions must not be replaced or reinterpreted through a local mapping table in the end-user software, but they must be presented as received from NoMVS.

Transactions that could not be processed

In rare situations, NoMVS may be unavailable, or the end user may have one or more invalid credentials, such as invalid password or certificate. In such situations NoMVS will either return error response or the end user system returns connection errors. These responses must be presented clearly to the end user so that they can contact their IT-support.

If NoMVS is temporarily unavailable, Nomvec strongly recommends that the end user system's work flow is not interrupted due to not receiving response from NoMVS. In such cases the transaction should be placed in a queue for controlled automatic resubmission when NoMVS becomes available again, and the workflow should be able to continue as normal.

If automatic resubmission is not supported, the end user must be given a clear way to handle or resubmit the transaction manually.