

Slovenian Medicines Verification System (SiMVS)

Response and alert management procedures

TABLE OF CONTENTS

TABLE OF CONTENTS	1
1. THE PURPOSE	2
2. THE SCOPE	2
3. DEFINITIONS	2
4. Response Management.....	3
4.1. SiMVS Responses	3
4.2. System design.....	3
4.2.1. Expected system responses.....	4
4.2.2. Suspected product falsification	4
4.3. Response classification.....	5
4.3.1. System non-responsiveness.....	5
4.3.2. Responses of type "YES the medicine can be dispensed"	5
4.3.3. Responses of type "The medicine cannot be dispensed, additional verification required"	5
4.3.4. Responses of type "NO the medicine cannot be dispensed" - Alerts	5
4.4. Management of responses.....	6
5. Control lists	6
5.1. Control list for the USERS.....	6
5.2. Control list for the MAHs	7
5.3. Control list for ZAPAZ	7
6. Annexes:	8
6.1. Annex 2 List of return codes and messages with a description of actions required	9
6.2. Annex 2 Response management procedure	14
6.3. Annex 3 List of other possible responses in additional processes, not used in pharmacies.....	15

1. THE PURPOSE

The purpose of this document is to provide the system users and software suppliers with additional information and recommendations regarding the management of responses and alerts about potential falsification in the end-user systems.

This document is based on the current system design. It may be upgraded with further development of the system and practical user experience.

The document was prepared by the Agency for Medicinal Products and Medical Devices of the Republic of Slovenia (JAZMP) and Medicines Verification Institute Slovenia (ZAPAZ) in association with Slovene Chamber of Pharmacies.

2. THE SCOPE

The document addresses the responses generated by the SiMVS verification system after the receipt of a request from the end-user. The focus is on return codes and messages generated by the system.

The messages displayed in the graphical interface are similar to web service messages; they are not dealt with specifically herein.

The document does not address the existing obligations and procedures by individuals and commercial entities involved in the marketing of a medicinal product, regarding the notification of JAZMP of unsuitable quality of medicines or suspected falsification of medicines in cases where the suspicion does not arise from the SiMVS response.

3. DEFINITIONS

ATD	Anti-tampering device for medicinal products
JAZMP	Agency for Medicinal Products and Medical Devices of the Republic of Slovenia
ZAPAZ	Medicines Verification Institute of Slovenia
SiMVS/NMVS	The Slovenian Medicines Verification System
EMVS	The European Medicines Verification System, the European Hub and all the connected National Medicines Verification Systems
GUI	Graphical user interface (user-accessible via web browser)
NCA	The national competent authority (JAZMP)
SWS	Software suppliers and the users' internal IT departments
User	The end user
Alert ID	The unique identification number of an individual alert (e.g. SI-0VJ-MBM-2Y5-W6A)
PC	Product code
LOT	Batch/lot number
EXP	Expiry date
SN	Serial number

4. Response Management

4.1. SiMVS Responses

When the SiMVS system receives a request, its response includes a **return code** along with the **corresponding message**.

- The expected positive system response means an “**Information**” type message which means the request can be processed in line with the expectations.
- The SiMVS system can also respond with a different message, indicating that something went wrong. In such a case, a “**Warning**” type message is given. Such messages are for example: “incorrect user login data”, “system technical difficulties”. Certain messages of this type can indicate a potentially falsified medicinal product. These are “**Alert**” type messages which include an “**Alert ID**”.

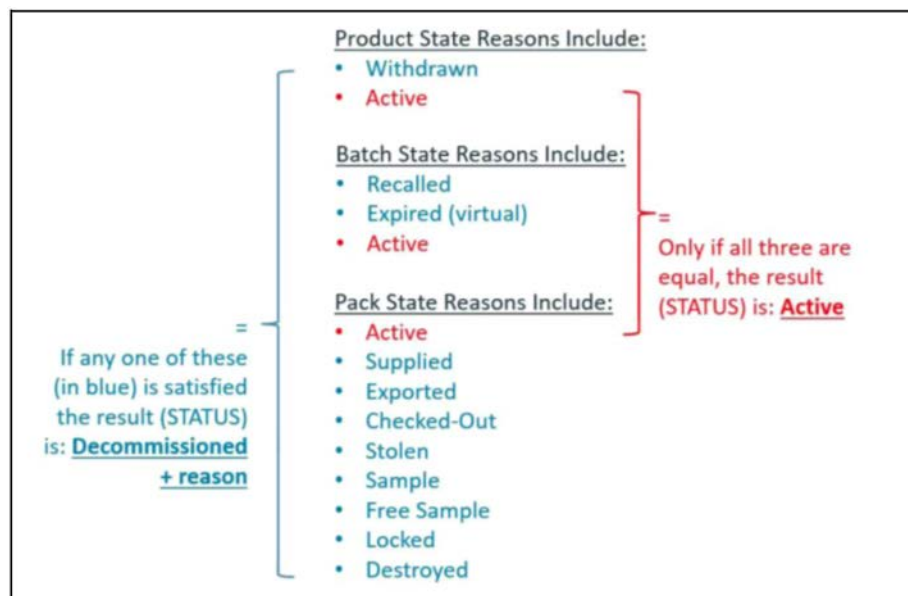
The ZAPAZ recommendation for pharmacy software developers is that, in addition to providing a return code and accompanying message, the information is shown and presented in a way that is completely comprehensible to the user and facilitates fast decision-making regarding further action.

4.2. System design

Conceptually, the data within the verification system are organised into 3 levels: the product level, the batch level, and the individual pack level.

Each of these levels has its own status and only when the status of all three levels is “active”, the pack in question can be dispensed and the system does not respond with an “**Error**” message.

Schematic overview:



Based on the above, the following responses are available when a verification request is received:

Product level: GTIN return status/product code (PC)

- Active
- Withdrawn
- PC not found

Batch level: batch number (LOT) and expiry date (EXP) return status

- Active
- Batch recalled
- Batch code not found (for the concerned PC)
- Expiry date (EXP) expired
- Expiry date in the system different from code in the query for the PC/batch concerned

Pack level: serial number (SN) return status of an individual pack

- Active
- Decommissioned (for any reason) or Locked = Not Active
- SN not found

System verifications are performed in a specific order. If PC is not found, the system cannot progress to verifying LOT, EXP or SN. If the batch number (LOT) is not found, the system cannot verify EXP and SN, etc.

4.2.1. *Expected system responses*

The following examples show the expected system responses and do not require a further description of the process:

PC	LOT	EXP	SN	Action
Active	Active	Correct	Active	Medicine can be dispensed
Active	Active	Expired	/	Batch expired, please follow the valid procedure
Active	Decommissioned	/	/	Batch decommissioned, please follow the valid procedure
Withdrawn	/	/	/	Product decommissioned, please follow the valid procedure

4.2.2. *Suspected product falsification*

Cases where falsification is suspected and further verification is required are:

PC	LOT	EXP	SN	Example
Not found	/	/	/	Product code not found in the whole EMVS - no alert
Active	Not found	/	/	Batch number not found
Active	Active	Different	/	The query EXP different from EXP in the NMVS
Active	Active	Correct	Not active	Serial number not set as active
Active	Active	Correct	Not found	Serial number not found

4.3. Response classification

4.3.1. System non-responsiveness

In the case of system non-responsiveness, the system may, due to various causes (e.g. broken internet connection), not respond at all or respond with a type of return codes and messages that indicate that the SiMVS and/or the pharmacy system is not working correctly.

In addition to return codes and messages that the SiMVS and/or the pharmacy system is not working correctly, the user may also see messages referring to difficulties with user login data (incorrect or invalid username or password) or that the user is attempting to conduct a transaction outside the scope of their role (e.g. user in the role of pharmacy trying to execute an “Export outside of the EU” transaction).

If the system is non-responsive due to technical difficulties, verification and deactivation are not possible.

4.3.2. Responses of type “YES the medicine can be dispensed”

Such a response means that the request has been processed successfully and that the data in the repository matches the data in the product package unique identifier. The medication is thus verified and the user may dispense it (“green response”). Some pharmacy systems do not display this message to the users; however it is important that the pack status information (e.g. active, dispensed, decommissioned) is shown to the user during the verification process.

4.3.3. Responses of type “The medicine cannot be dispensed, additional verification required”

After scanning the unique identifier, the user may receive an error message which may require further action by the user, its SWS or ZAPAZ. The **medicine cannot be dispensed** (“yellow response”). IT service providers (SWSs) are advised to present the explanation of the cause of error in the user interface, in a way that is sensible to the user.

This group of responses/return codes contains the following types of messages:

- Messages warning the end user that a **medication has been decommissioned or withdrawn or that its expiry date has expired**.
- Messages indicating **end user software issues or scanner issues**. This type of messages can also mean that the user has scanned a code which does not contain a unique identifier (an OTC medicine or other product) or that the code data are incorrectly encoded. This group also contains responses meaning that the user is close to exceeding the number of allowed deactivation attempts (three attempts of deactivating the same box with a scanner are permitted) and that the next attempt will trigger an alert.
- Messages indicating **suspected falsification** where the SiMVS has not perceived this as an alarm for various reasons which cannot be removed through measures by IT providers or ZAPAZ.

4.3.4. Responses of type “NO the medicine cannot be dispensed” – Alerts

The user may not dispense the medicine. The reasons are presented on the secondary level. Return codes and messages about possible falsification indicate that the pack cannot be distributed further or dispensed because there is a suspicion that the pack is falsified.

With this type of messages (“red response”), the user receives an alert that is also sent to ZAPAZ and the MAH concerned.

The information about alerts is stored in the ZAPAZ records system, complete with information about the users and MAHs involved, all information about the product/pack, results of investigations, decisions by JAZMP, actions, and further procedures.

4.4. Management of responses

A list of return codes and messages with a description of actions required can be found in Annex 1.

The response management procedure can be found in Annex 2.

5. Control lists

5.1. Control list for the End Uses

In case of an alert, system non-responsiveness or response of the type “The medicine cannot be dispensed, additional verification required”, the End User should check the following:

- **Does the product need to be equipped with protective elements?**

This must be integrated into the pharmacy system. The user’s product database must be updated with serialization data, based on external sources (CBZ). Otherwise the user may receive many alerts when scanning medicines for which protective elements are not required; however the medicines are serialized according to the same standards for a particular reason. If this information is not correctly integrated into the pharmacy system, the user must check it on their own.

- **Has a wrong code been scanned?**

It must be checked whether the scanned code is in fact the code intended for the identification and verification of medicinal products or perhaps some other code, coming from e.g. the Indian medicines verification system, or any other code that is not a GTIN code from the SiMVS system.

- **Is the user’s scanner working correctly? Is the user’s system working as expected?**

Is the data sent to the user’s system from the scanner correct? The user may check this by comparing the scanned and the printed data. They can also check by scanning another product and checking if an alert is received and if the data matches the printed code. Checking by scanning a different product may also help identify possible other issues with the user’s system that could trigger an alert. The user should also check whether “Caps Lock” on their keyboard is on; in this mode, the scanner converts upper-case letters into lower-case letters and this can cause an alert.

- **Has there been a typing error during manual entry?**

The user should check the code entered. They may re-enter the code to see if the alert persists. In order to avoid cases arising from incorrect entry of codes (including scanning errors), the pharmacy system can always verify the control number that is part of every GTIN code. In case of manual entry it is not recommended to enter the batch number and expiry date.

- **Has the user performed an invalid transaction?**

This can occur when the user scans and deactivates the same pack several times (the first three (3) attempts of “double scanning” do not trigger an alert). In such a case, the message will also show whether the user has previously deactivated the pack. If the user deactivated the pack, an alert will not be triggered. (If a package was deactivated less than 10 days before and the reason for the deactivation was not destruction of theft, the user may revoke the deactivation).

In order to facilitate verification for the users, we recommend that IT providers of pharmacy systems include an additional window into the user’s system, containing a list of possible causes that the user needs to check.

- **Has the medicine been decommissioned, withdrawn or has it expired?**

In the case of such messages, the user should follow the valid procedures for returning the medicine to the wholesaler/supplier or for the destruction of the medicine.

5.2. Control list for the MAHs

Upon receiving the alert and information from the user and ZAPAZ, the MAH must immediately begin an investigation on its side.

Depending on the alert type, the responsible MAH must investigate the following possible causes of alert:

- Check if the product code for Slovenia has been uploaded.
- Check if there were any error messages upon the upload and whether they have been duly addressed.
- Have the data on products in the database been updated and what is the current version number of the product in the system.
- Check whether the batch has been uploaded and whether it has been uploaded with the correct batch number.
- Has the expiry date been uploaded with the batch? Does the expiry date in the system match the information on the packaging?
- Were any error messages upon uploading the batch data and have they been duly addressed?
- Is the first version of batch data still present in the system, has data been uploaded at a later point? Has the changed data been uploaded successfully?
- Has all the data about the pack been uploaded?
- Were there error messages, were any codes rejected (double codes, rejected records e.g. due to the use of special characters), and have the notifications been addressed correctly?
- Check the physical pack and compare the printed and 2D data against the data in the system.
- Check whether similar alerts for this product have been recorded in any other countries.

The MAH must communicate its findings to ZAPAZ via e-mail and it will participate in further investigations.

5.3. Control list for ZAPAZ

Along with the investigations carried out by the user and the MAH, ZAPAZ must also check whether the alert could be caused by difficulties within the SiMVS.

Depending on the alert type, ZAPAZ must investigate the following possible causes of alert:

- Check whether the system also returned alerts for the same case with any other users.
- Check whether an unusual number of alerts have been triggered with the user in question.
- Check the total status of alerts triggered in comparison to historical data.
- Check the history of data about the product, batch and pack.
- Check whether there are any other error messages recorded in the system (rejected entries, files...) for different entries in connection with the source of the alert.
- Check for potential technical difficulties in the system (the functioning of the system, etc.).

ZAPAZ shall reconcile the investigation results with the user and the MAH concerned and determine whether a technical error or an error at the level of user, MAH or ZAPAZ can be ruled out. In such an event, the case must be submitted to JAZMP, which shall treat the case as a confirmed suspicion of falsification.

6. Annexes:

Annex 1 List of return codes and messages with a description of actions required

Annex 2 Response management procedure

Annex 3 List of other possible responses in additional processes, not used in pharmacies

6.1. Annex 2 List of return codes and messages with a description of actions required

No.	Response code	Alert code	Return message	Note	Action
System non-responsive or a response about the system not functioning; verification not possible due to technical difficulties (Section 4.3.1)					
1	70020000 70010000	/	The national medicines verification system is overloaded. Please try again later.	SiMVS not functioning correctly.	1
2	B1020000	/	Unknown product code (PC). Error in communication with the European Hub. Please try again later.	SiMVS not functioning correctly.	1
3	44020001 64120000 62120002 62120004 62120005 61020002 61020009 61020010 61020012 61020013 61020014	/	Error in entering request. Please contact the technical support.	The pharmacy system is not working correctly.	1
4	44020003	/	The scheme of product code is not supported: {0}.	The pharmacy system is not working correctly.	1
5	62120007	/	The requested status is invalid.	The pharmacy system is not working correctly.	1
6	61020005	/	The scheme of product code (coding) is not supported ({0}).	The pharmacy system is not working correctly.	1
7	401	/	401 Unauthorized	This message will be received by the user if their token for performing transactions is not valid. In this case there could be an error in system credentials or the user's IT system (e.g. not requesting or correctly refreshing the token).	1
8	30020000	/	The client does not have the authorisation to perform this operation.	E.g. a pharmacy attempting to perform an operation as a wholesaler.	1
Responses of type "YES the medicine can be dispensed" (Section 4.3.2)					
9	11110100	/	The box is active.	/	0
10	11110200 11210200	/	The box has been dispensed.	/	0
11	11410100	/	The box has been reactivated.	/	0
Responses of type "The medicine cannot be dispensed, additional verification required" - Responses preventing immediate dispense of medicine however SiMVS does not return an alert (Section 4.3.3)					

12	51421000	/	The box cannot be reactivated. The batch has expired.	/	1
13	51421100	/	The box cannot be reactivated. The batch has been decommissioned.	/	1
14	51421200	/	The box cannot be reactivated. The medicine has been withdrawn from the market.	/	1
15	51321000	/	The box cannot be deactivated. The batch has expired.	/	1
16	51321100	/	The box cannot be deactivated. The batch has been decommissioned.	/	1
17	51321200	/	The box cannot be deactivated. The medicine has been withdrawn from the market.	/	1
18	51221000	/	The box cannot be dispensed. The batch has expired.	/	1
19	51221100	/	The box cannot be dispensed. The batch has been decommissioned.	/	1
20	51221200	/	The box cannot be dispensed. The medicine has been withdrawn from the market.	/	1
21	51320000	/	The box cannot be deactivated.	In the case or manual entry error.	1
22	44020000 41020000	/	Unknown product code (PC).	E.g. Indian medicine, OTC or other product. Data has not been uploaded into the system.	2
23	44020002 61020001	/	Missing product code (PC).	Error in SW; code not scanned because it is not present.	2
24	44020004 61020008	/	Invalid product code.	The scanned code is not GTIN or PC or is incorrectly encoded.	2
25	11420100 51420100	/	The box cannot be reactivated because it is already active.	Check and re-scan to dispense.	0
26	51420000 51420300 51420400	/	The box cannot be reactivated.	In the case or manual entry error.	2
27	51420002 51420200 51420501 51420601 51420801	/	The box cannot be reactivated. Time limit has expired.	More than 10 days from deactivation for the purpose of dispense, free sample, sample or export have passed. Return or use in accordance with Article 25 (2) of the DU - applies to hospitals.	2
28	61020007	/	Invalid expiry date.	Incorrect encoding.	2
29	11220200	/	The box has already been dispensed at this location.	"Double dispense" - attempts 1 and 2.	1
30	11220201	/	The box has already been dispensed at this location. The next attempt will be rejected.	"Double dispense" - attempt 3.	1
31	51220000	/	The box cannot be dispensed.		2
32	41020002	/	Unknown serial number (SN).		2

33	41020004	/	The batch number (LOT) does not match the batch number in the system.	In the case of manual entry error.	2
34	41020006	/	The expiry date does not match the expiry date in the system.	In the case of manual entry error.	2
35	61020000	/	Missing batch number (LOT).	Incorrectly encoded LOT.	2
36	61020003	/	Serialization number (SN) missing.	Code not scanned because it is not present.	2
37	61020004	/	Expiry date (EXP) missing.	Incorrectly encoded EXP.	2
38	51420201	/	The box cannot be reactivated. It has been issued at another location.	Reactivation is not possible.	2
39	51420001 51420500 51420600 51420700 51420800	/	The box cannot be reactivated. It has been deactivated at another location.	A box that has been deactivated in another pharmacy (e.g. as a sample, free sample, exported, locked) cannot be reactivated.	2
40	51320200 51320300 51320400 51320500 51320600 51320700 51320800 51320900 51020200	A24	The box cannot be deactivated. The competent body will be notified.	The box is already in one of the states preventing deactivation, e.g. dispensed at another location, stolen, destroyed, given as a (free) sample, locked, exported, repackaged.	3
41	52120000	A16	Doubled serialization number. The competent body will be notified.	/	3
42	51420900	A24	The box cannot be reactivated. The competent body will be notified.	The box is in a "checked-out" state due to repackaging by parallel importer, thus the previous unique identifier cannot be reactivated.	3
43	41020001	A3	Unknown serialization number (SN). The competent body will be notified.	/	3
44	41020003	A2 A68	The batch number (LOT) does not match the batch number in the system. The competent body will be notified.	/	3
45	41020005	A52	The expiry date does not match the expiry date in the system. The competent body will be notified.	/	3
46	51220200 51220300 51220400 51220500 51220600 51220700 51220800 51220900	A24	The box cannot be dispensed. The competent body will be notified.	The box is already in one of the states preventing deactivation, e.g. dispensed at another location, stolen, destroyed, given as a (free) sample, locked, exported, repackaged.	3
47	51220201	A7	The box has already been dispensed at this location. Too many repeated attempts. The competent body will be notified.	The box has already been dispensed; too many repeated attempts, or a 4 th "double dispense" attempt.	3

Medicine verification without deactivation					
48	11110300	/	The box is marked as stolen.		3
49	11110400	/	The box is marked as destroyed.		3
50	11110500	/	The box is marked as a sample.		3
51	11110600	/	The box is marked as a free sample.		3
52	11110700	/	The box is marked as locked.		3
53	11110800	/	The box is marked as exported from the EU.		3
54	11110900	/	The box has been repackaged.		3
55	11111000	/	The batch has expired.		1
56	11111100	/	The batch has been decommissioned.		1
57	11111200	/	The medicine has been withdrawn from the market.		1
58	70020000	/	Too many requests; 40 requests per minute maximum.		1
Medicine deactivation with determination of status: "sample, destroyed, stolen, free sample, locked, exported from the EU"					
59	11310500		The box has been marked as a sample.	In the pharmacy.	/
60	11310400		The box has been marked as destroyed.	In the pharmacy.	/
61	11310300		The box has been marked as stolen.	At the wholesaler.	/
62	11310600		The box has been marked as a free sample.	At the wholesaler.	/
63	11310700		The box has been marked as locked.	At the wholesaler.	/
64	11310800		The box has been marked as exported from the EU.	At the wholesaler.	/

Description of measures / actions by the end-user:

- 0 The request has been processed successfully. The medicine has been verified and the user can (deactivate and) dispense it or return it to sales stock in case of reactivation.
- 1 First, the user must check possible causes using the control list. They should correct any scanning errors, deactivate the medicine again and dispense it. If the user is unable to remedy the error on their own, they should contact the software supplier, the internal IT department or ZAPAZ. If the error cannot be remedied, the user must follow the same procedure as for management of alerts, described under Item 3. The user notifies ZAPAZ via the e-mail address published on the ZAPAZ website (www.zapaz.si) or via an equivalent communication channel with guaranteed traceability. The pack in question shall be stored in quarantine where it shall be kept for 24 hour or, in case of bank holidays, until the end of the next workday.¹ In the case of a message informing the user that the medicine is decommissioned, withdrawn or expired, the user must follow the valid procedures for returning the medicine to the wholesaler/supplier or for destroying the medicine.
- 2 The user must treat such a case as suspected falsification and follow the same procedure as for management of alerts, described under Item 3. In such a case, the user must notify ZAPAZ via the e-mail address published on the ZAPAZ website (www.zapaz.si) or via an equivalent communication channel with guaranteed traceability. The pack in question must be kept in quarantine for 24 hour or, in case of bank holidays, until the end of the next workday.² If the cause of response preventing dispense is not determined within 24 hours or, in case of bank holidays, until the end of the next workday, and if the medicine may be returned to sales stock if suspected falsification is not confirmed, the user shall return the medicine to the wholesaler in accordance with the valid return procedure, unless JAZMP decides otherwise.
- 3 Upon each alert, the user receives a case number which facilitates traceability and communication throughout the investigation. The user shall record the case number and, in a suitable way, mark the medicine pack that triggered the alert. The pack in question must be kept in quarantine for 24 hour or, in case of bank holidays, until the end of the next workday. Using the control list, the user checks other possible causes to confirm whether the alert was in fact triggered by the pack. If the cause of alert was a technical or procedural error and the user can remedy it alone or with the assistance of its SWS, the user must again check and deactivate the medicine, dispense it and notify ZAPAZ. If the cause of alert is not determined within 24 hours or, in case of bank holidays, until the end of the next workday, and if the medicine may be returned to sales stock if suspected falsification is not confirmed, the user shall return the medicine to the wholesaler in accordance with the valid return procedure, unless JAZMP decides otherwise.

ZAPAZ must receive the alert number of the suspected falsification case from the user and it shall request additional information if necessary. It must check whether the verification system is functioning correctly and if other similar alerts have been received. ZAPAZ may add this information to the notification of the MAH. If the cause of alert was a technical or procedural error, it shall remedy it and inform the MAH and the user who will again deactivate and dispense the medicine.

When the MAH is informed of the alert, it must check whether the data has been correctly uploaded into the EMVS/NMVS. The MAH may request additional information regarding the pack from ZAPAZ. If the cause of alert was a technical or procedural error, it shall remedy it and inform ZAPAZ which shall in turn inform the user to again deactivate and dispense the medicine.

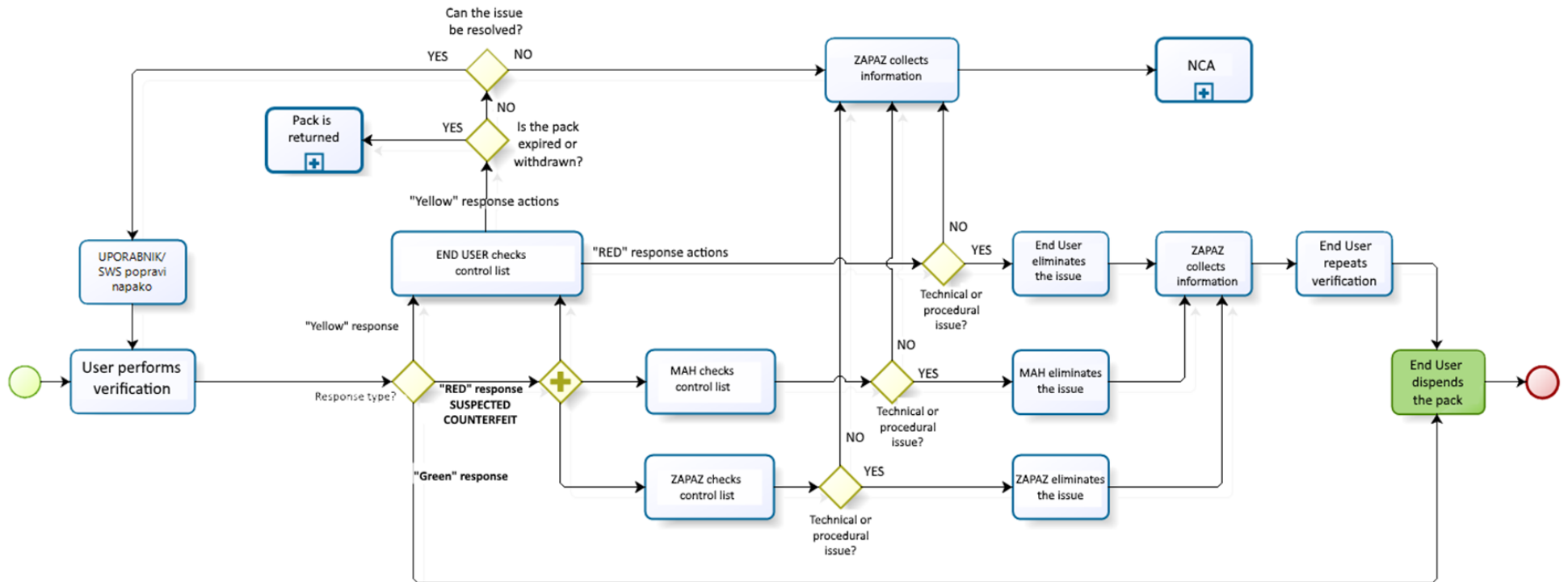
ZAPAZ shall notify JAZMP that the technical error which caused the alert has been remedied.

If the cause cannot be determined at the level of the user or the MAH, they shall notify ZAPAZ via e-mail address published on the ZAPAZ website (www.zapaz.si) or via an equivalent communication channel with guaranteed traceability. All the information received from the user and the results of investigations by the MAH and ZAPAZ must be communicated by ZAPAZ, together with the case number, to JAZMP via e-mail to quality-defects@jazmp.si. JAZMP shall treat the notification as a **confirmed suspicion of falsification** and proceed in line with the valid procedures. After the finished investigation, JAZMP shall communicate the decision of measures taken and their results to the subjects affected by this decision.

¹ Because ZAPAZ is not automatically informed of the issue in the case of such a response, the quarantine period begins with the time of ZAPAZ being notified.

² Because ZAPAZ is not automatically informed of the issue in the case of such a response, the quarantine period begins with the time of ZAPAZ being notified.

6.2. Annex 2 Response management procedure



"GREEN" response: Attempted action was successful - pack can be dispensed
"YELLOW" response: Pack cannot be dispensed immediately - further inspection is required
"RED" response: Alarm - suspected counterfeit

Key:

Green response = Request processed successfully, the medicine can be dispensed.

Yellow response = The medicine cannot be dispensed immediately, additional verification is required.

Red alert = alert, suspected falsification

6.3. Annex 3 List of other possible responses in additional processes, not used in pharmacies

HTTP code	Process	Response type	Response code	Return message
409	Post Bulk-of-Product Code	Warning	54120000	Duplicate product codes provided.
422	Post Bulk-of-Product Code	Warning	64120001	Too many product codes in request. A maximum of {0} product codes will be accepted.
200	Post Bulk-of-Product Code	No information provided	14100000	
200	Single Product Code	No information provided	14000000	
200	Delete a Report	Information	15610000	Report Deleted
403	Delete a Report	Warning	35620000	Not authorised to access requested report
404	Delete a Report	Warning	45620000	Report not found
403	Retrieve a Report	Warning	35420000	Not authorised to access requested report
404	Retrieve a Report	Warning	45420000	Report not found
409	Retrieve a Report	Warning	55420000	Report not ready
500	Retrieve a Report	Warning	A5420000	Error Creating Report
200	Get Report Job Status	No information provided	15100000	
200	Request Report Metadata	No information provided	15800000	
403	Request Report Metadata	Warning	35820000	Not authorised to access requested report type
404	Request Report Metadata	Warning	45820000	Unknown report type
200	Request Report Types	No information provided	15700000	
202	Request a Report	Information	25010000	
403	Request a Report	Warning	35020000	Not authorised to access requested report
422	Request a Report	Warning	65020000	Unknown report type
422	Request a Report	Warning	65020001	Invalid Report Parameters
200	Get Bulk-of-Pack Results	No information provided	12200000	
404	Get Bulk-of-Pack Results	Warning	42220000	No results found. The results may have expired.
409	Get Bulk-of-Pack Results	Information	52210000	The request is still being processed.
202	Post Bulk-of-Pack	No information provided	22100000	
422	Post Bulk-of-Pack	Warning	62120001	The actual number of packs does not match the stated number.
422	Post Bulk-of-Pack	Warning	62120003	Too many packs in bulk request. A maximum of {0} packs will be accepted.
422	Post Bulk-of-Pack	Warning	62120006	Manually entered bulk of pack requests are not supported.
405	Post Bulk-of-Pack	Information	92110000	Recovery APIs are currently unimplemented.