

# ALERTS MANAGEMENT USING API

## User Manual

**ver. 1.1**

---

## Table of Contents

1. Introduction.....	3
2. Description of System Expansion.....	4
2.1. Areas of expansion .....	4
2.2. Use of API.....	6
2.3. Technical Solution.....	7
3. Description of Expansion for Individual Areas .....	7
3.1. Alert status and change .....	7
3.2. Information exchange.....	8
3.3. Data archiving (closed alerts).....	9
3.4. Web interface .....	10
4. Integration of API with MAHs' or End Users' Software .....	14
4.1. Assumptions .....	14
4.2. Integration procedure .....	14
ATTACHMENT.....	14

## Terms glossary

Term/Abbreviation	Description
NMVS	National Medicines Verification System (application)
EU-HUB	Data interface
MAH/OBP	Marketing authorization holder for the given country, or an on-boarding partner authorized to upload data in the verification system.
SIDC	State Institute for Drug Control
FMD	Falsified Medicines Directive
csv	File format
SSR	Solidsoft Reply. The supplier of the medicines verification system for the Czech Republic and other EU Member States.
ALERT	An incident in the NMVS or in EU-HUB – level 3 and higher
API	Application programming interface
REST	Application interface standard

## 1. Introduction

Based on the EU's Falsified Medicines Directive, the individual Member States created their own national verification systems and connected them to the European system.

All distributors and pharmacies join the national system. The national system of the Czech Republic (NMVS) is based on Solidsoft Reply's solution that all obliged entities join.

**Národní organizace pro ověřování léčiv, z.s. (NOOL)** was founded to create, operate and connect individual entities.

NOOL is responsible, among other things, for investigating alerts (i.e. system incidents of level 3 and higher) generated in the NMVS. For these purposes, NOOL has developed an alert management application and set up a call-center that supports alert investigations. MAHs or OBPs are notified about generated alerts by notification e-mails and can respond to these alerts via these e-mails or request help from the call-center.

This, however, requires a lot of manual work and this is why, NOOL has expanded the alert management system for API that makes it possible to connect to end users' and MAHs' software and to largely automate the process. The API solution also includes a web portal that makes the API functionality available even to users without their own alert management software. However, the scope of automation through the web portal is limited.

**This document describes how API is used, i.e. describes its web interface and use for alert investigations.**

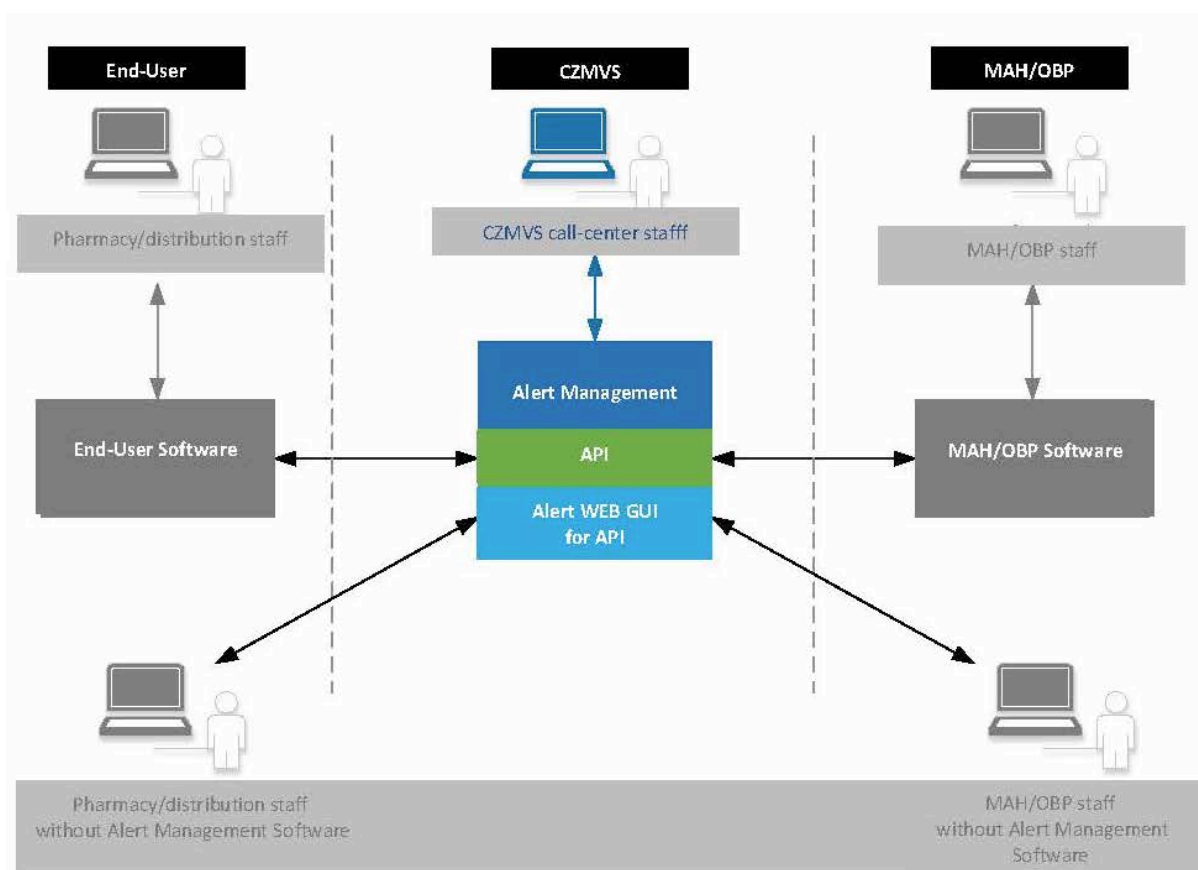
## 2. Description of System Expansion

### 2.1. Areas of expansion

The goal of the expansion is to **provide for automated information processing**, i.e. to automatically identify and change the status of alerts and thus to provide for an integration with MAHs and end users' current applications.

Once the processing is fully automated, it shall be possible to (optionally) totally eliminate the sending of notification e-mails and to switch to full electronic processing without the need to contact NOOL's call-center at all or only sometimes.

Figure 1 – Alert management



The expansion thus interlinks NOOL's alert management system with end users' and MAHs'/OBPs' alert management systems. End customers' and MAHs' alert management systems are connected to NOOL's API alert management. The interlink of software through API will make it possible to automate alert investigation operations.

Figure 1 also shows the possibility to use the web interface to API for users who do not have their own alert management software; however, automation is rather limited in this case. All MAHs/OBPs or end users need is a web browser.

Available functions differ, depending on the type of authentication:

- **Simplified authentication** is intended for end users, i.e. pharmacies and distributors, only. The reason is to reduce the work with distribution and maintenance of access details for the largest group of users. An access detail comprises of *the alert code UPRC* and *the location (workplace) code*.
- **Full authentication** allows access to all available functions and is primarily intended for MAHs and OBPs because it is not possible to change the alert status without full authentication. End users can also use this type of access and expanded sets of functions but cannot change the alert status. Users must contact NOOL to obtain access details and must use these details use for every API call.

#### 2.1.1. Functions available for simplified authentication (only for pharmacies and distributors)

- To see the alert status and the presence of messages/files for the given alert.
- To attach or receive messages/files for the given alert.

#### 2.1.2. Functions available for full authentication (primarily for MAHs but also for end users)

- To see the list and status of one or several alerts, based on entered criteria (time span, alert status, etc.).
- To change the status of one or several alerts based on UPRC.
- To change the status of a group of alerts that has already been re-defined (alert grouping for the purposes of notification).
- To attach or receive messages/files for the given alert.

**Note:** The reason for attaching/receiving a message or a file is to allow a direct **anonymous communication between end users and MAHs during alert investigations** without the need to communicate with NOOL's call-center employees. It also makes it possible to send messages with a pre-defined content. The purpose of these messages is to overcome a potential language barrier in communication between MAHs and end users. Only the message number is sent, which makes it possible to translate the message in the MAH's or the end user's software into the local language. However, automated message sending requires support by both parties, i.e. the end user and the MAH. In the case that there is no response to the message within the time-limit set by the system parameter, NOOL's call-center shall be notified and shall contact the parties. This shall cover both the situation where the end user does not communicate through API and the situation where both parties use such communication, but the end user does not respond within the set time-limit.

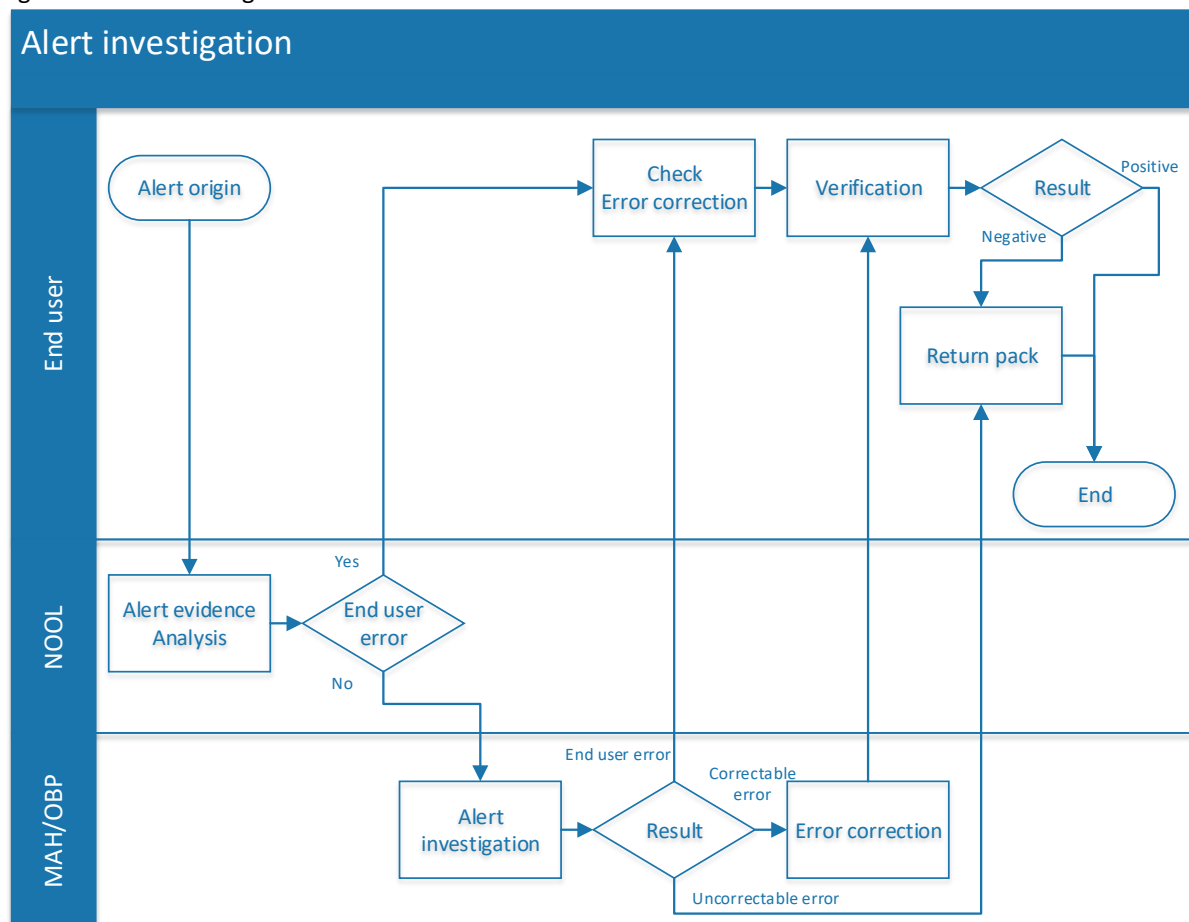
**Attention:**

The expansion **does not inform** end users **about whether or not they can dispense the given medicinal product. This is in full competency of the authorized person of the given business premises.**

## 2.2. Use of API

The use of API depends on the progress of an alert investigation (see Figure 2).

Figure 2 – Alert investigation



The process is simplified, some steps may in fact repeat, etc. But it shows the activities that API can speed up and make more effective.

The end user's software regularly checks, through API functions, the status of alerts that the end user generated. Thanks to API, the end user is able to detect a change in the alert status. According to the result of the MAH's investigation, the end user shall perform verification, based on which the end user shall dispense the medicinal product or shall return it to the distributor. In the case that the investigation discovers an error on the part of the end user (typically an incorrectly setup scanner, Caps Lock turned on by mistake, etc.), the end user shall correct it and shall verify the medicinal product again.

As part of alert status identification, the end user shall also be informed about whether a message or a file, typically the MAH's request for additional information, is attached to the given alert. If so, the end user can attach the requested information to the alert, using the API function.

MAHs'/OBPs' software can also regularly detect the list and status of alerts assigned to them. The alert status also includes information about messages or files. In the case that MAHs/OBPs need end users' cooperation, they can add to the alert, through API, a message (a request for additional information). As part of alert investigation, they shall check whether or not end users provided requested additional information or responded to their message. If so, they shall receive such information and use it in their investigation. Once the reason for the alert or a group of alerts is investigated, they shall set up the investigation result through API.

### 2.3. Technical Solution

To ensure the required functions, API is used as the best communication tool with a maximum level of automated data communication, reliability and security.

Authentication is required to access information. There are two types of authentication, depending on the type of access. Simplified authentication (the alert code UPRC and the location code are used as access details) is intended for end users and full authentication (the name and password is issued by NOOL upon request) is intended for MAHs/OBPs and potentially also for end users (typically rather distributors and large pharmacy chains).

#### **Attention:**

Since there are currently several ways to update the alert status (to respond to a notification e-mail, a manual response of the call-center to written requests of MAHs/OBPs), MAHs/OBPs must have internal processes for setting up rules for working with alerts in order to avoid parallel updates of the alert status through different channels.

## 3. Description of Expansion for Individual Areas

### 3.1. Alert status and change

It describes functions that allow to detect and change the alert status. The function availability and authentication need differ, depending on the type of entity – MAH, end user (pharmacy or distributor).

- **Detection of the alert status and presence of messages/files (simplified authentication)**  
The current alert status is provided based on the sent unique alert identifier UPRC and identifier of the location (workplace) where the alert was generated. In addition to the alert status, information about whether a message or a file is attached to the given alert is returned.

- 
- **Detection of the alert status and presence of messages/files (full authentication)**  
The function shall return a list of alerts assigned to the given MAH based on entered criteria. Filtering by time, alert status or audit trail request is available. It also includes information about whether a message or file is attached to the given alert.
  - **A change in the alert status (full authentication, for MAHs only)**  
The function shall change the alert status based on the entered UPRC to one of the potential statuses from the status list.
  - **A change in the status of group of alerts that has already been predefined – grouping used in notifications (full authentication, for MAHs only)**  
The function shall change the status of all alerts in the group based on the entered group identifier.
  - **Uploading the list of all alert groups (full authentication, for MAHs only)**  
The function allows to upload the list of groups and their identifiers assigned to the given MAH/OBP. It is then possible to work with group identifiers in the functions “*Uploading the List of Alert Identifiers*” and “*Change in the Status of the Alert Group.*”
  - **Uploading the list of alert identifiers (UPRC) in the given group**  
The function shall return the list of all alert identifiers in the given group.
  - **Adding the list of Exceptions**  
The function allows to record a list of medicines that have an exception under § 11 r) of the Act on Pharmaceuticals or medicines that were released from production before 9th February 2019.

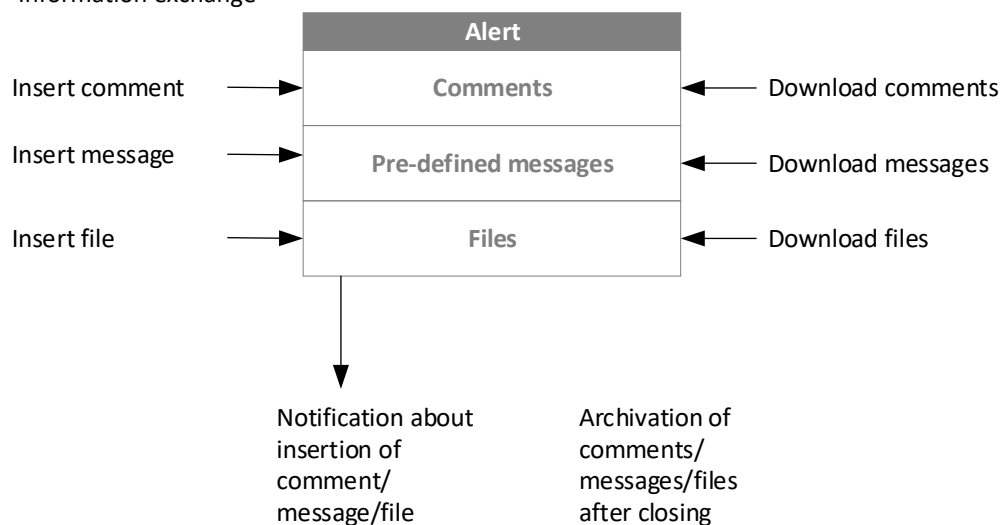
Note: the function will be available in API version 2.0 (late November 2019).

## 3.2. Information exchange

The system allows to attach additional data, comments or files to the given alert ID. The system should obtain the majority of such additional information automatically from data sources of MAHs’/OBPs’/end users’ software (see Figure 3).



Figure 3 – Information exchange



The system allows a direct anonymous exchange of information between MAHs and end users (business premises, location where the alert was generated).

The objective is to maintain **end users' anonymity** as much as possible – i.e. where possible, MAHs shall not automatically receive information about specific end users.

Once additional information is entered, the system shall send notification to the contact e-mail of the given MAH and end user. Once the alert is closed, data shall be moved to an archive after the set time-limit expires.

### 3.2.1. Types of message

The system allows to transfer the following three types of message:

- Classical text field where it is possible to write.
- Pre-defined message based on the code list – only the message code is sent. This type of communication helps to overcome a language barrier in the case that the end user and the MAH are from different EU States. The most common types of message (communication) have codes with an assigned meaning that can be automatically translated in the end user's/MAH's software.
- File in a supported format (txt, csv, jpg, png, tiff).

Since the use of the alert management system is up to each end user, it is not guaranteed that the end user shall respond to a request for additional information. Therefore, in the case that no response is obtained within the set time-limit, NOOL's call-center shall be informed about it by e-mail and shall contact the relevant parties and transmit the message or, in some justified cases, shall connect the MAH with the end user.

### 3.3. Data archiving (closed alerts)

Once an alert is closed, data are inactivated (they are visible but can no longer be modified) after the set time-limit (currently 90 days) expires. However, even after that it shall be

possible to inquire about the status of the given alert ID. Later on (after 12 months), they shall be moved to the archival database but shall still be available for reports in the case of audits performed by supervising authorities. After that (after 6 years), they shall be stored on an archival external medium and deleted from the archival database.


### 3.4. Web interface

Users who do not have their own alert management software can use a web interface that provides an equivalent functionality. However, the automation of the entire process of alert handling is rather limited as compared to access through API.

After the login to the web interface, a screen with a list of functions shall appear. Each function is selected using the tabs in the upper part of the screen.

#### 3.4.1. Upload data

The function allows to obtain a list of alerts that can be filtered by entered criteria, such as alert generation date, alert status or time since the last change.

 **Národní organizace**  
pro ověřování  
pravosti léčiv

CZ EN  
NOOL

[Login as another user](#)

HOMEPAGE	DOCUMENTATIONS	PRODUCT FILTERING	ALERTS
----------	----------------	-------------------	--------

## Alerts

Get dataInsert dataEdit dataDelete data

Get alert states, messages, file and enums

**Result as**

**Show** 

- ✓ Alert state
- Messages
- File
- Alert states enum

**Filter**

**Latest**

**UPRC**

**Alert creation time** from:  :  hod., to:  :  hod.

**Change alert state** from:  :  hod.

**State ID**

**Audit required**

**Page**   
Size od page: 500 items

CancelGenerate JSON query for APIDo request

10/ 14

Národní organizace pro ověřování pravosti léčiv, z.s., IBC Pobřežní 620/3, Karlín, 186 00 Praha 8  
IČ: 05851742, www.czmvo.cz

### 3.4.2. Enter data

The function allows to add a message or a file to the given alert.

HOME PAGE	DOCUMENTATIONS	PRODUCT FILTERING	ALERTS	
-----------	----------------	-------------------	--------	--

## Alerts

Get data **Insert data** Edit data Delete data

Insert messages and files

**UPRC**

**Intended for**

**Answer to**   
Message ID

**Subject**   
Subject of message


**Message**

**File**    
Filetype should be txt, pdf, csv, jpg, tiff, png

**Name of the file**   
Name of the attachment (with extension)

### 3.4.3. Change data

The function allows to change the alert status or to respond to a message by entering another text. To select an operation, it is necessary to click on Change Data.

 **Národní organizace**  
pro ověřování  
pravosti léčiv

[CZ](#) [EN](#)

NOOL

[Login as another user](#)

---

<a href="#">HOMEPAGE</a>	<a href="#">DOCUMENTATIONS</a>	<a href="#">PRODUCT FILTERING</a>	<a href="#">ALERTS</a>
--------------------------	--------------------------------	-----------------------------------	------------------------

## Alerts

[Get data](#) [Insert data](#) [Edit data](#) [Delete data](#)

Edit messages




**Message ID**

**Intended for**

**Subject**   
Subject of message

**Message**

[Cancel](#) [Generate JSON query for API](#) [Do request](#)

© Copyright 2019 Národní organizace pro ověřování pravosti léčiv, z.s. [Neofema, s.r.o.](#)

### 3.4.4. Delete data

The function allows to delete the attached message.

HOME PAGE DOCUMENTATIONS PRODUCT FILTERING ALERTS

## Alerts

Get data Insert data Edit data **Delete data**

Delete of message

Message ID

Cancel Generate JSON query for API Do request

---

## 4. Integration of API with MAHs' or End Users' Software

The basic points of integration to API are the same for MAHs and end users. The difference is in the method of authentication and the actual use.

### 4.1. Assumptions

MAHs or end users has alert management software that can be adapted to use REST API of NOOL's system.

### 4.2. Integration procedure

- First, it is necessary to modify the MAH's/end customer's software so that it would cooperate with API based on the specification.  
There is an **API testing environment** with a full-fledged data set. We recommend debugging software first and testing it in a testing environment.
- We recommend setting up appropriate alert-solving procedures and processes (in connection to other policies and processes of the organization).

Once software is debugged, it can be connected to the production system. MAHs must obtain access details for authentication that NOOL shall provide upon request.

**Note:**

End users (pharmacies, distributors) can also obtain access to expanded functions but must first ask NOOL for access details just like MAHs.

## ATTACHMENT

API správa alertů\_dokumentace\_ver\_5.1.2.pdf – Technical documentation for developers