oneIDentity+ User Manual

Detailed description of the 1D+ Automated Code Upload Tool

Author	Bittrich, Mirja
Version	1.0 ACU
Datum	07.06.2018
Status	Final

oneIDentity+ GmbH
Steinheilstraße 10
85737 Ismaning
Germany
Tel: +49 (0)89 321216 – 0

1 Introduction

Product piracy, digitalization and Industry 4.0 are global challenges affecting all manufacturers and markets.

1.1 oneIDentity+ is more

With the oneIDentity+ solution manufacturers, suppliers and dealers can do more than to protect their products against counterfeiting. The oneIDentity+ solution is a cross-sectoral service platform supporting role-specific, digital and mobile processes, by serialized and therefore clearly marked products.

This marking is carried out by a data matrix code according to GS1 and ISO standards (ECC 200 – see ISO/IEC 16022:2006): the so-called MAPP code. MAPP stands for "**M**anufacturers **a**gainst **P**roduct **P**iracy" and is a cross-company initiative, whereby leading component manufacturers have organized themselves so as to work together in the fight against product piracy.

Based on the code validation – and depending on the role of the user (in the following also "code checker") – additional product details and vehicle repair and maintenance information can be displayed and/or linked to mobile marketing activities.

This allows users – using just one system – to retrieve customized information from various manufacturers via a mobile device.

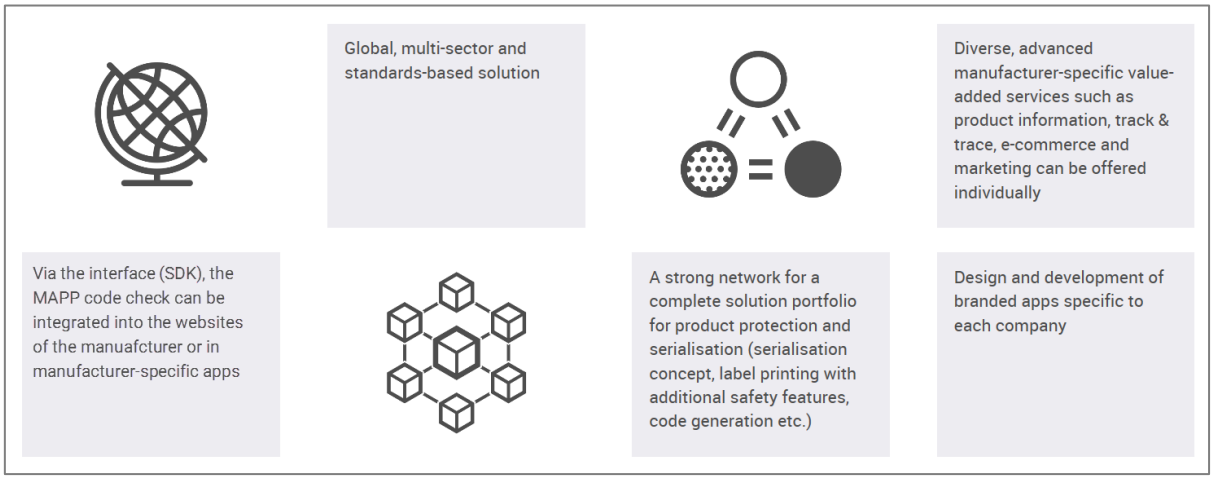


Figure 1 - The benefits for part manufacturers using oneIDentity+

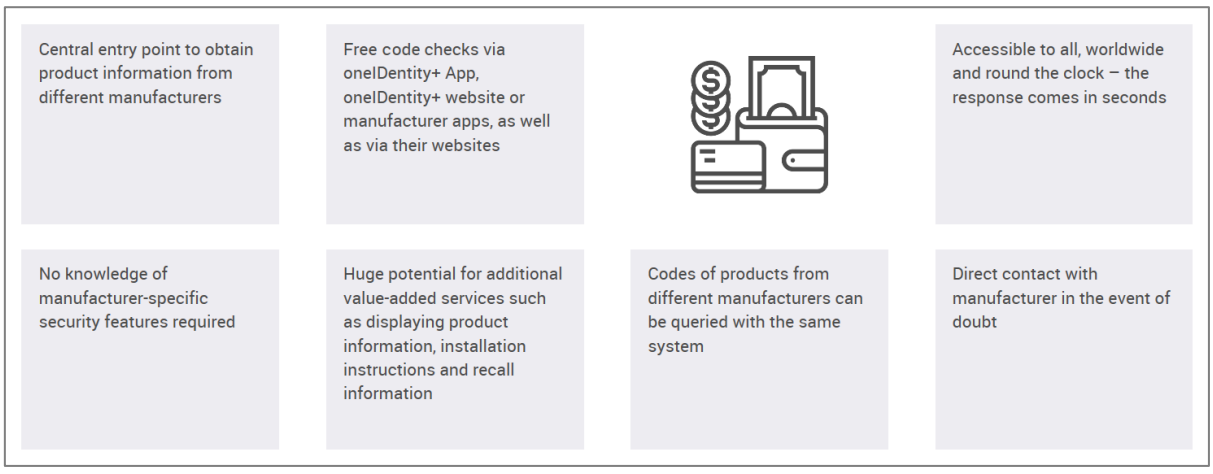


Figure 2 - The benefits for service employees, workshops, customs officers or internet buyers using oneIDentity+

1.2 How does the oneIDentity+ service work?

The oneIDentity+ solution is a service platform to **check the authenticity of product codes*** based on the unique MAPP code (in the following “product codes” or “Mapp codes”). In addition, it gives manufacturers the option to provide additional Value Added Services to specific users. This can be done irrespective of the mobile device used, be it an iPhone, iPad, Android phone or tablet.

Using this solution, anyone who wants to inspect an article (i.e. customs, garage, wholesaler, manufacturer or end customer) has a simple way to check whether the code on the product is valid or not. By using a PC and its keyboard or a mobile phone with a camera, the MAPP code can be captured and sent off to the Authentication Platform (internet connection required). There the code will be checked and the result (in form of a text messages combined with a green/yellow/red traffic light) will be sent back right away This will provide the user with an indication whether the respective part is genuine or not. If the result is not positive the user can send a counterfeit report to the manufacturer who can then take further steps.

In addition, the manufacturers using the oneIDentity+ solution for their products have the option to grant authorized users access to additional Value Added Services. These can be product information (e.g. article details, fitting instructions) as well as marketing and sales related services (e.g. the connection to customer loyalty systems or the sending of an order request). This depends on the manufacturer’s needs and requires a special implementation based on standard function components oneIDentity+ offers.

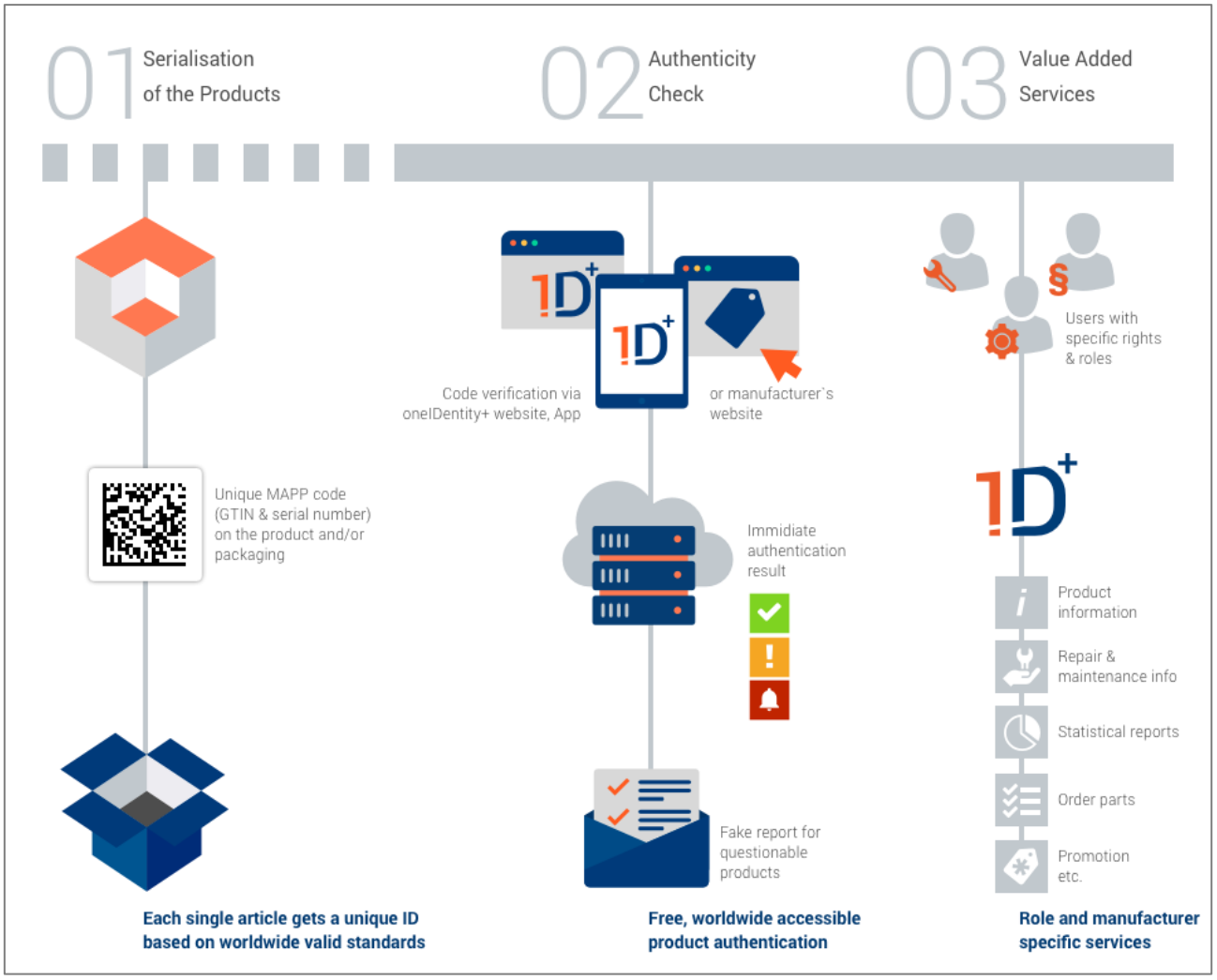


Figure 3 - Operating principle of oneIDentity+

***Important note:** oneIDentity+ checks if a code on a product/package is registered (= in the oneIDentity+ database) and was not checked too many times already. This gives an **indication** about a products genuineness, but is no proof. Only in conjunction with other visible and sometimes hidden product properties, facts about sales cycles etc. the product's genuineness can be confirmed.

1.3 The MAPP code

The principle behind the oneIDentity+ solution is as follows: Each product is labelled with an **identification number, unique in the world**, in the form of a **MAPP code** (data matrix code). This code can be checked with a scanner, mobile phone camera or via manual entry. With the oneIDentity+ solution the code can be identified, verified and further product-related information can be retrieved – all this within seconds, worldwide, 24 hours a day.

The MAPP code is a standard for technical industries like the independent automotive aftermarket, machine and plant building, rail etc. It is based on GS1 and ISO standards.

Note: MAPP stands for **M**anufacturers **a**gainst **p**roduct **p**iracy. For more details about this initiative see **www.mapp-code.com**

The MAPP code is a two-dimensional data matrix code following the globally established GS1 standards (for more information see www.gs1.org). A 2D code does not consist of lines like a one-dimensional code but of groups of squares or lines on a rectangular or square surface. Because of the second dimension, 2D codes can encode substantially more information in the smallest space. In addition, errors when reading MAPP codes are very limited. The code is readable even if it has been partially damaged (for more information with respect to GS1 DataMatrix see https://www.gs1.org/docs/barcodes/GS1_DataMatrix_Guideline.pdf).

Figure 4 - EAN Barcode (1D Code)

QR code (Link to websites etc.)

MAPP code (2D DataMatrix)

Just like a fingerprint can be assigned to just one person, a MAPP code can be assigned to exactly one product or package. With this unique product code identification, a tool is now available to fight against product counterfeiting; it can be used by all market participants.

Figure 5 - The principle behind oneIDentity+ and the MAPP code

The MAPP code consists of a Global Trade Item Number (formally known as EAN – European Article Number – based on the Global Company Prefix (GCP) which is assigned to companies by GS1 member organisations – see application identifier (01) in figure 6) in combination with a serial component (see application identifier (21) in figure 6). This so-called serialized GTIN is a globally valid standard used across many industries.

Figure 6 – Examples for the usage of the MAPP code (GS1 data matrix) in different industries

There are different ways to apply the MAPP code to a product. It can be placed on the package using prefabricated labels, optionally with an additional security feature like a hologram, or be printed directly on the label by the manufacturer himself. Another option is to directly mark the product e.g. by laser engraving.

Figure 7 - Ways to mark a product

Note: In certain use cases it might be required to use other/additional data carrier or code types than the 2D DataMatrix. Therefore special implementation projects within oneIDentity+ are required.

2 Overview of oneIDentity+ Components

oneIDentity+ is a comprehensive cloud platform with different components. The following graphic provides an overview:

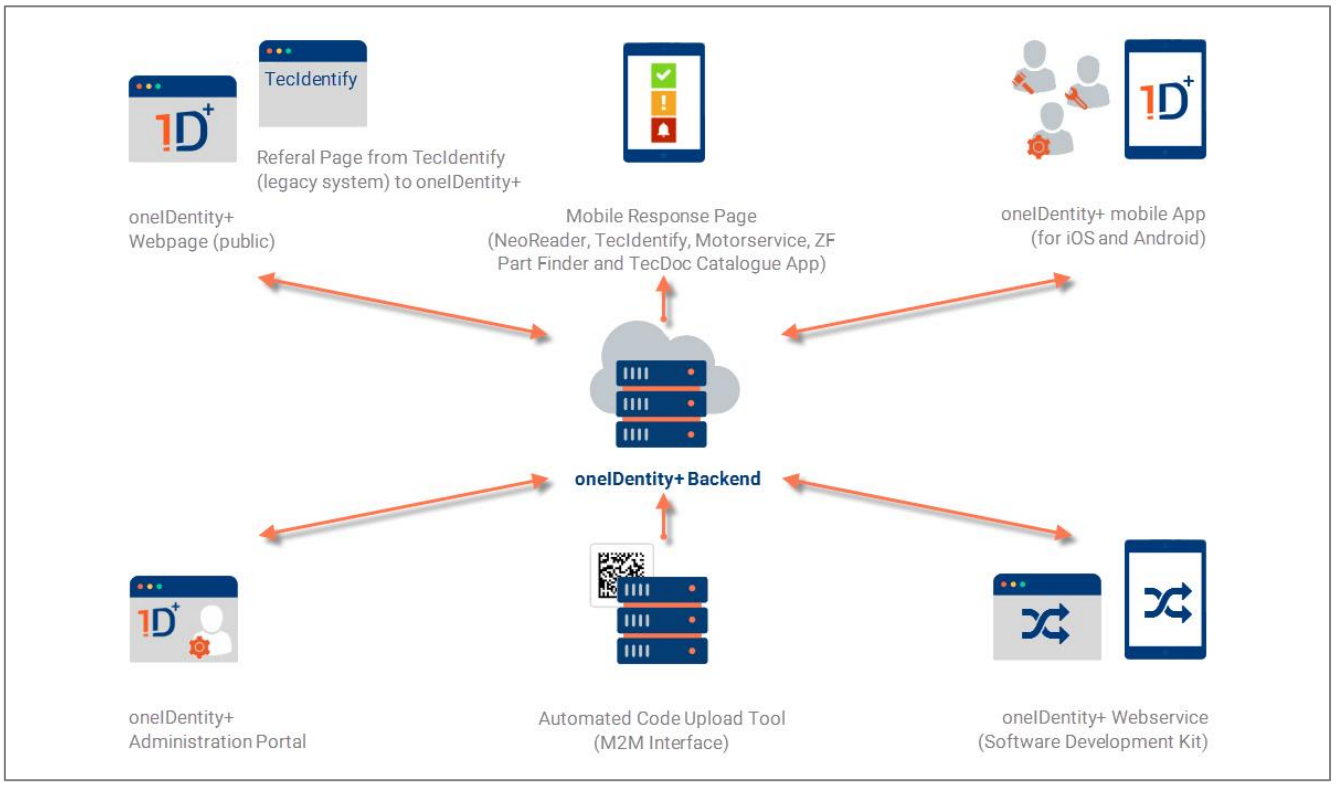


Figure 8 - oneIDentity+ components

2.1 Processes, users and components within oneIDentity+

In the following the processes carried out by the different users using the various oneIDentity+ components are described:

1. The first step in the oneIDentity+ processes is the **creation of the MAPP codes** which will then be used to uniquely mark a product. This can be done by the **manufacturer's** infrastructure (optional with the **oneIDentity+ Serialization Engine** to create the serials) or by an **external service provider** for labels.
2. Then follows the application of **the MAPP codes on the product and/or package**. This will be done by the **manufacturers** in their production line or during commission or shipping processes.
3. In addition an **upload of the MAPP codes** to the **oneIDentity+ Database** by the **manufacturer** or the **external service provider** for the labels is required. This can be done via the **oneIDentity+ Administration Portal** or by the **oneIDentity+ Automated Code Upload Tool**.
4. After each Code Upload the **manufacturer** receives a **Code Upload Confirmation** and once a month a **Code Upload Overview** via email from the **oneIDentity+ Platform** (backend).
5. To allow the code upload for each manufacturer, the **creation of the organisation** with its settings, users, GCPs etc. by the **oneIDentity+ Super Admin** in the **oneIDentity+ Administration Portal** is required.

6. By logging into the **oneIDentity+ Administration Portal** the Organization Admin of the **manufacturer** can further **administer the organisation's settings and users** – he can define thresholds, authentication response texts, GTINs (Global Trade Item Numbers) to allow the code upload, users and their roles, available Value Added Services for each role etc.
7. The **Product Authentication via MAPP code check** is available for everyone (e.g. **service employees, dealers, garages, authorities, end customers**) free of charge, 24 hours a day, worldwide. It can be done by different endpoints:
   - by scanning or manual input of the code with the **oneIDentity+ Mobile App**
   - by entering the code manually on the **oneIDentity+ Website** www.one-identity-plus.com
   - by scanning or manual input of the code with the NeoReader/TecIdentify App or one of the Catalogue Apps (e.g. ZF Part Finder, Motorservice App) developed by TecAlliance GmbH which all call the **oneIDentity+ Mobile Response page** with the Authentication Result
   - by scanning or manual input of the code with a specific manufacturer's webpage or mobile app (prerequisite: implementation by the manufacturer) which uses the **oneIDentity+ Webservice (Software Development Kit)** to show the authentication result
8. After input/scan of the code at one of these endpoints the request is automatically transferred to the **oneIDentity+ Platform** and the **MAPP code validation** is carried out.
9. As **Authentication Result** a colour code (similar to a traffic light) in combination with a manufacturer/GTIN specific authentication response text (all languages possible) plus optional promotional information (image, text, links) is displayed. The possible authenticity check results are:

Green: The MAPP code is valid and in the oneIDentity+ database.
Depending on the scanned product and the role of the logged in user additional **Value Added Services** are shown within the oneIDentity+ Mobile App.

Yellow: The MAPP code is in the oneIDentity+ database but has been checked many times already. (Which means that the threshold of allowed scans defined by the manufacturer was exceeded.) In case of doubt about the genuineness of the product the manufacturer can be informed by filling out a **Counterfeit Report**. Nevertheless additional Value Added Services are shown within the oneIDentity+ Mobile App with respect to the role of the logged in user.

Red: The code is not known by oneIDentity+. This is a potential fake. The **code checker** can contact the manufacturer by filling out a **Counterfeit Report**. No Value Added Services are shown.

10. This **Counterfeit Report** is sent to the **oneIDentity+ Platform** and forwarded from there to the email addresses defined by the manufacturer for this purpose. The **manufacturer** is now in charge to take further steps and get in contact with the code checker.
11. In addition, authorized users of the **manufacturer** can use the **oneIDentity+ Administration Portal** to **view and download statistical reports** of all checks carried out for products of their organisation.

    When using **oneIDentity+ Mobile App** authorized (registered) **code checkers** can have access to additional **Value Added Services** defined by the manufacturer. These services can be manifold – reaching from product and marketing information up to very complex services and processes. This depends on the manufacturer's requirements, which are based on a special implementation and are not part of this document.

manufacturer or external service provider for labels	**Creation of the unique MAPP codes** 	1D+ Serialization Engine [Manufacturer's infrastructure]
manufacturer	**Apply MAPP codes on products/packages** 	[Manufacturer's production, packaging or commission processes]
1D+ Super Admin	**Creation of manufacturer's 1D+ Organization** 	1D+ Administration Portal
manufacturer	**Administer organization's settings and users** 	1D+ Administration Portal
manufacturer or external service provider for labels	**Upload Codes into 1D+ database** 	1D+ Administration Portal 1D+ Automated Code Upload Tool
1D+ Backend	**Code Upload Confirmation/Monthly Report** 	1D+ Backend
end customers, service employees, garages, dealers, authorities	**MAPP code check & Authentication result** 	1D+ Mobile App 1D+ Mobile Response Page 1D+ Webpage, 1D+ Web service
end customers, service employees, garages, dealers, authorities	**Counterfeit Report for suspicious articles** 	1D+ Mobile App 1D+ Mobile Response Page 1D+ Webpage
end customers, service employees, garages, dealers, authorities	**Value Added Services** 	1D+ Mobile App
manufacturer	**Statistical Reports** 	1D+ Administration Portal

Figure 9 – Processes (orange), users/roles (black) and components (blue) of oneIDentity+

2.2 oneIDentity+ Mobile App

The **oneIDentity+ Mobile App** allows anonymous and logged in users to check if a product code is in the oneIDentity+ database and from there draw conclusions about the genuineness of the respective product. In case of doubt about the genuineness of the product (e.g. A yellow or red traffic light, if the product code is not in the database or has already been checked too often) the App user can fill out a counterfeit report to inform the manufacturer.

Logged in users have – depending on their rights – also access to additional product and marketing information and other manufacturer specific **Value Added Services**. (Note that this functionality is only available for products of manufacturers with the Premium package and that the manufacturer is in charge of providing the login to his employees, authorized partners and prime customers.)

The oneIDentity mobile App is available worldwide for iOS and Android via the Apple App Store, Google Play and local Chinese Android stores.

2.3 oneIDentity+ Webpage

The oneIDentity+ Webpage **https://www.one-identity-plus.com** is a public webpage providing information about the oneIDentity+ service and the oneIDentity+ GmbH as a company.

It also offers the possibility to check the Authenticity of product codes by entering a MAPP code manually. After each check the **authentication result** (traffic light and authentication result text) plus optional **promotional information** (image, text and link) is displayed. In case of doubt about the genuineness of the product code (yellow or red traffic light) the webpage user can fill out a **counterfeit report** to inform the manufacturer.

Value Added Services and the user login are not available on the oneIDentity+ Webpage.

Code checkers who previously used the legacy system TecIdentify including the TecIdentify Webpage www.tecidentfy.com (to check codes) are now guided from there to one of the following **referral pages:**

- https://www.one-identity-plus.com/tecidentify-jetzt-ersetzt-durch-one-identity-plus/ (German page)
- https://www.one-identity-plus.com/en/tecidentify-now-replaced-by-one-identity-plus/ (English page)
- https://www.one-identity-plus.com/zh-hans/%E7%8E%B0%E5%9C%A8%E5%8D%87%E7%BA%A7%E4%B8%BAoneidentity/ (Chinese page)

These pages provide the same code check functionality as the oneIDentity+ Webpage.

2.4 oneIDentity+ Mobile Response Page

The Authenticity of Products Codes can also be checked by scanning a MAPP code with the NeoReader App, the TecIdentify App, the Motorservice App, the TecDoc Catalogue Mobile and the ZF Part Finder App.

To display the authentication result the so called oneIDentity+ Mobile Response Page is used. It shows the **authentication result** (traffic light and authentication result text) and also allows the display of **promotional information** (image, text and link). In case of doubt about the genuineness of the product code (yellow or red traffic light) the user can fill out a **counterfeit report** to inform the manufacturer.

Value Added Services and the user login are not available within the Mobile Response Page.

2.5 oneIDentity+ Administration Portal

The oneIDentity+ Administration Portal is a web interface especially created for manufacturers' administrators and members of the supplier's brand protection team. It allows authorized users to manage their organization's users, settings and Value Added Services, view and download statistical reports, upload codes into the oneIDentity+ database etc. To access the oneIDentity+ Administration Portal standard internet browsers in the current versions can be used.

2.6 oneIDentity+ Webservice (SDK)

The oneIDentity+ Webservice (Software Development Kit) provides manufacturers with a tool to integrate the oneIDentity+ authenticity check into their own webpages or mobile Apps using their own company specific design.

2.7 oneIDentity+ Automated Code Upload Tool

Before the Authenticity of Product Codes can be checked the corresponding MAPP codes have to be uploaded into the oneIDentity+ database. This can be done by the manufacturer's administrator via the oneIDentity+ Administration Portal by manually uploading *.CSV files or by using the **oneIDentity+ Automated Code Upload Tool**.

The latter is an application which allows to automatically upload codes saved in *.CSV files from the manufacturer's machine (Windows Operating System) to the oneIDentity+ database without any manual interaction.

- fic light: the **Report Counterfeit** button
- the promotional campaign information in form of an image, a text and a link (if this exists for the checked GTIN)

For this call the oneIDentity+ platform stores the following information which is further used in the check statistic:

- the checked MAPP code
- the manufacturer (oneIDentity+ Org) to which this code belongs
- the date and time of the check
- "Mobile Response Page (manual input)" or "Mobile Response Page (scan)" as origin of the check
- the authenticity check result (green/yellow/red)
- Geo information data (Country, longitude, latitude etc.) of the check (only if the user allows this)
- Language of the check response

2.8 Report Counterfeit functionality

For codes which display a red or yellow traffic light the button **Report Counterfeit** appears on the Authenticity Check result page. This allows the user to fill out a counterfeit report for suspicious products and send it automatically to the manufacturer via email.

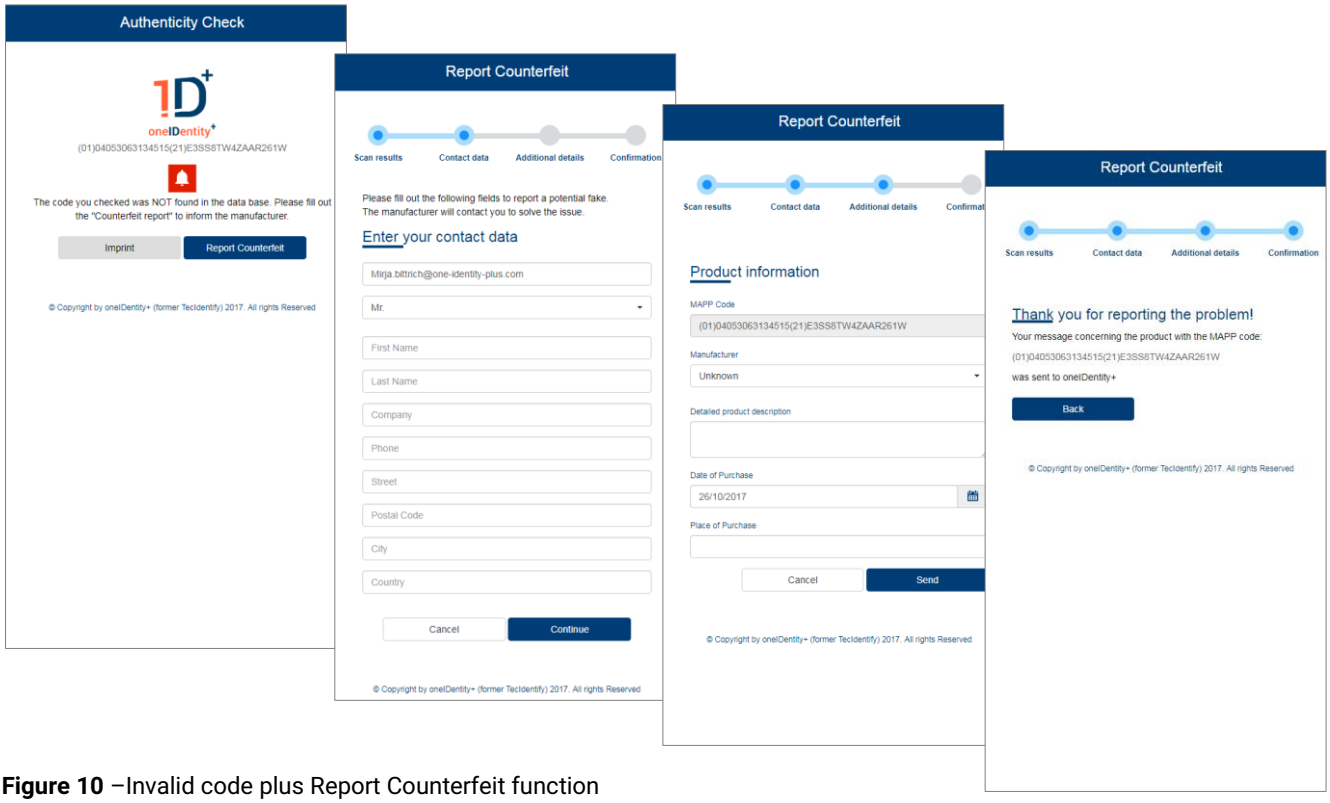


Figure 10 –Invalid code plus Report Counterfeit function

3 oneIDentity+ Automated Code Upload Tool

3.1 Overview

Before the authenticity of products can be checked the corresponding MAPP codes have to be uploaded into the oneIDentity+ database. This can be done by the manufacturer's admin (portal role Organization admin) via the oneIDentity+ Administration Portal by manually uploading *.CSV files or by using the **oneIDentity+ Automated Code Upload Tool**.

The latter is an application which allows to automatically upload codes saved in *.CSV files from the manufacturer's machine (Windows Operating System) to the oneIDentity+ database without any manual interaction.

The workflow is as follows:

1. The oneIDentity+ Automated Code Upload Tool (Java application which runs as windows service in the background) needs to be installed on the manufacturer's code creation machine (Windows Operating System).
2. All codes to be uploaded must be saved in *.CSV files following a certain oneIDentity+ specific schema (for details about the required structure see Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.) and placed in the **Import folder**.
3. A **Properties file** defines were this Import Folder, the Error and Archive folders are on the machine, which credentials should be used etc.
4. The Automated Code Upload Tool checks periodically if there are any *.CSV files in the CSV folder.
5. If this is the case it fetches the *.CSV files, processes and sends them to the oneIDentity+ cloud with **EPCIS events.**
6. In case there are erroneous files that cannot be imported into the oneIDentity+ database (or erroneous codes within the file) the *.CSV file is placed in the **Error folder** on the machine where the Automated Upload Tool is installed.
7. The *.CSV files successfully imported into the oneIDentity+ database are moved from the Import folder into the **Uploaded folder** on the machine.
8. The Automated Upload Tool automatically creates **Log** files with the upload results and information about the import process.
9. To carry out the code upload the Automated Upload Tool needs to authenticate at the oneIDentity+ platform. Only authorized users can upload codes for their organization. In addition, it is important that the GTIN of the codes to be uploaded has been assigned already to the organization by the Organization Admin of the manufacturer via the oneIDentity+ Administration portal.

Note: In case there are one or more invalid codes within a *.CSV file, the following happens: The valid codes are uploaded into the oneIDentity+ database. But since there is at least one invalid code in the file the entire file is moved to the Error folder. In the log file it is visible, which codes in the file are erroneous and what kind of error appeared. Please correct the error and place the corrected *.CSV in the input folder again.

Important: For uploads done via the oneIDentity+ Automated Code Upload Tool you do **also** receive an **Immediate Code Upload Confirmation** via email. In addition, the uploads done via the oneIDentity+ Automated Code Upload Tool are included in the **Monthly Code Upload Report.**

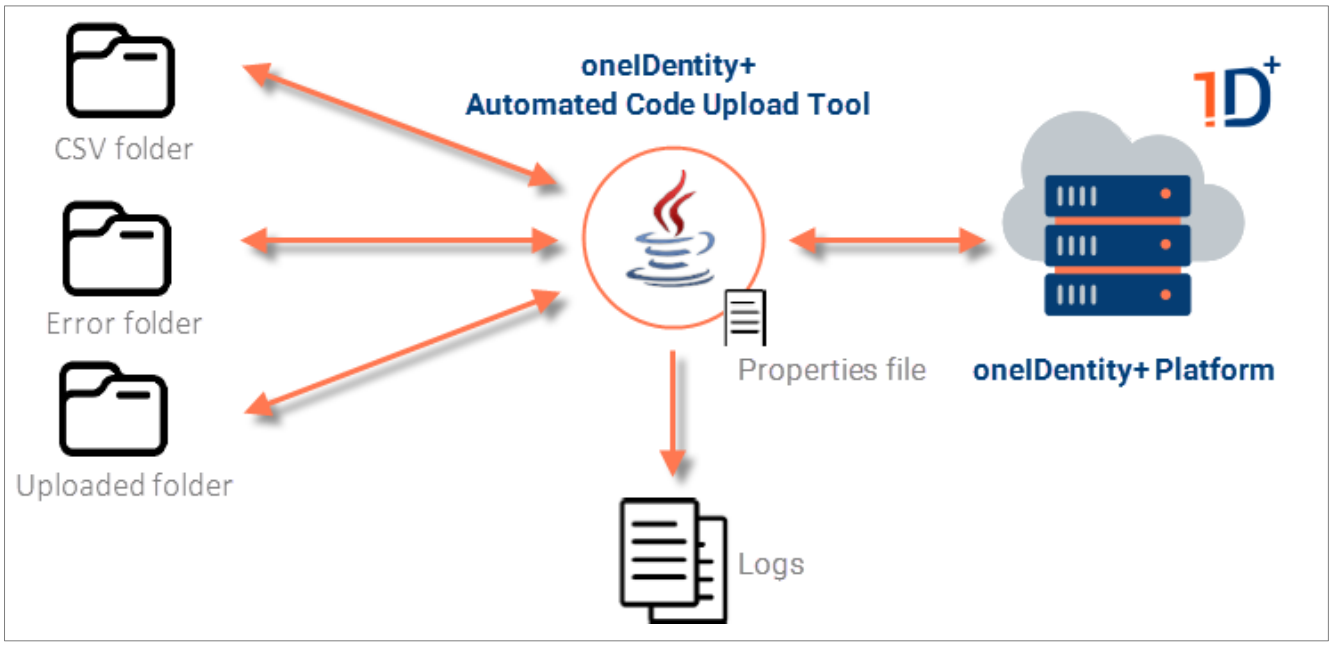


Figure 11 – Workflow of the Automated Code Upload Tool for oneIDentity+

3.2 System Requirements

To use the Automated Code Upload Tool the following is required:

- Operative System: **Windows XP or Higher**
- Access to the **Windows Scheduler Task**
- **Java SE Runtime Environment 8** installed in your computer. This can be downloaded here: http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html

3.3 Installation and Configuration

3.3.1 Step 1: Extract ZIP file

The Automated Code Upload Tool is provided in a zip file.

You need to extract it. After decompressing, you should find the following files and folders:

- **csvFolder:** The CSV files that should be uploaded must be placed in this folder.
- **errorFolder:** If the upload of one or more codes in the CSV file failed, the entire file is moved to this folder.
- **uploadedFolder:** If the upload of all codes in the CSV file was successful, the file is moved to this folder.
- **acu.properties:** This file contains the configuration (password, users, urls…) to be used by the tool.
- **automatic-code-upload.jar:** This file contains the tool.

- **run.cmd:** This file is used to execute the tool.

Very important: These folders and files must not be renamed!

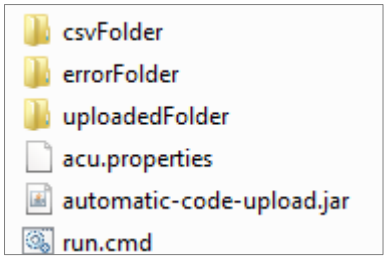


Figure 12 – Folder structure of the Automated Code Upload Tool

3.3.2 Step 2: Configuration of the Properties file

The **acu.properties** file contains the main configuration of the tool. This configuration is customizable and needs to be modified as described in this section. To edit this file and add the custom configuration carry out the following steps:

1. Open the **acu.properties** file with a text editor like Notepad.
2. Change the values of the keys according to your needs:
   - **csv.folder:** Define here the path of the csvFolder. In this folder the CSV files to be uploaded must be placed.
   - **error.folder:** Define here the path of the errorFolder. The oneIDentity+ Code Upload Tool will move the CSV files, which cannot be completely uploaded, to this folder.
   - **uploaded.folder:** Define here the path of the uploadedFolder. The oneIDentity+ Code Upload Tool will move the CSV files, which were successfully uploaded, to this folder.
   - **system.useProxy:** Some systems work under a proxy to call other systems via WebService. In case of the use of a proxy is necessary, add "Y" value for "Yes" to this key, if not, add "N" value for "No".
   - **system.proxyProtocol:** Proxy protocol contains the value of the connection protocol. Is mandatory for the proxy connection and the available values are "**http**" or "**https**"
   - **system.proxyHost:** If required, define here the proxy Host value.
   - **system.proxyPort:** If required, define here the proxy Port value.
   - **system.proxyUser:** If required, define here the proxy User value.
   - **system.proxyPassword:** If required, define here the proxy Password value.
   - **oneidentityplus.url:** Define here the URL of the Movilizer cloud. For the Demo system this is https://demo.movilizer.com/mds/m2m and for productive system https://www.one-identity-plus.com/mds/m2m
   - **oneidentityplus.deviceAddres:** Define here the device address provided by the oneIDentity+ Super Admin.
   - **oneidentityplus.password:** Enter here the password of the device address provided by the oneIDentity+ Super Admin.

- **oneidentityplus.epcis:** Enter here the URL of the cloud to send the WebServices with the code information. For the Demo system this is http://demo.movilizer.com/MovilizerDistributionService/epcis/capture and http://www.one-identity-plus.com/MovilizerDistributionService/epcis/capture for the Productive system.
- **user.email:** Enter here the user email registered in the oneIDentity+ Administration Portal. Be aware that this user needs the portal rights **Organization admin** to upload codes.
- **user.password:** Enter here the encrypted password of the user defined above. **Important:** For security reasons you must not enter the password as plain text but encrypted. How to transfer your plain text password into an encrypted one see chapter **3.5 Password encryption for the usage in the Automated Code Upload Tool**
- The key **pwd.SYSTEMID** needs to contain the SYSTEMID of your organization. The value of this key is the password of the SYSTEMID. Both will be provided by the oneIDentity+ Super Admin.

  Example:
  If the user has an organization called “Example Organization” in the platform and the SystemID of this organization in the platform is “00001” with the password “00001PWD”, the configuration of this key is the following: **pwd.00001=00001PWD**

  Important: If the same user can upload codes for different organizations, the user can add more values with the same format in the properties file. This might be the case for big companies using for each brand a different oneIDentity+ organization.

3. **Save** the **acu.properties** file and close it.
4. **Note:** You must not rename the properties file!

```
//UPLOADER CONFIG
csv.folder=C:\\Users\\H217452\\Desktop\\AutomaticCodeUpload\\csvFolder
error.folder=C:\\Users\\H217452\\Desktop\\AutomaticCodeUpload\\errorFolder
uploaded.folder=C:\\Users\\H217452\\Desktop\\AutomaticCodeUpload\\uploadedFolder

//PROXY CONFIGURATION
//If you don't want use proxy, add N value to system.useProxy property
//If you want to use proxy, add Y value to system.useProxy property and add a value to system.proxyProtocol system.proxyHost and system.proxyPort
//If the proxy needs user and password, add a value to the properties system.proxyUser and system.proxyPassword
system.useProxy = N
//Available values for proxyProtocol are "http" or "https"
system.proxyProtocol = http
//URL of proxyHost must be "http://myurl" or "https://myurl" without port
system.proxyHost =
//ProxyPort must only contains the port number
system.proxyPort =
system.proxyUser =
system.proxyPassword =

//CONNECTION ONEIDENTITYPLUS PROPERTIES
oneidentityplus.url = https://www.one-identity-plus.com/mds/m2m
oneidentityplus.deviceAddres = @authentication@movilizer.com
oneidentityplus.password = EYlKJlE8Ek+xIhLpSPDY0g==
oneidentityplus.epcis = http://www.one-identity-plus.com/MovilizerDistributionService/epcis/capture
user.email = test_user@oneid.com
user.password = EYlKJlE8Ek+xIhLpSPDY0g==
pwd.18270006 = 123456
```

Figure 13 – Example of the acu.properties file

3.3.3 Step 3: Configuration of the Run.cmd

The **run.cmd** file is used by the computer to execute the tool. This file contains the path where the tool is installed.

To configure this path, do a right click on the file and select **Edit**.

In the Edit screen, you can modify the path in the third line and add the correct path to the tool folder.

Example:

If the path of the Automated Upload Tool is E:\Temp\AutomaticCodeUpload than the **run.cmd** file should look as follows:

```
@echo off
REM Eventually change directory to the program directory
cd E:\Temp\AutomaticCodeUpload
REM run the program
java -jar automatic-code-upload2.jar
```

Figure 14 – Example of the run.cmd file

3.3.4 Step 4: Add Task in the Task Scheduler

To start the installation of the automatic task in Windows, we need to configure a Scheduler Task. The way to open the Task Scheduler depends on the Windows version you use.

To open the Scheduler Task in Windows XP carry out the following steps:

1. Click **Start** button
2. Click **All Programs**
3. Point to **Accessories**
4. Point to **System Tools**
5. Click on **Scheduled Tasks**

To open the Scheduler Task in Windows 7 or Windows Vista carry out the following steps:

1. Click the **Start** button
2. Click **Control Panel**
3. Click **System and Maintenance**
4. Click **Administrative Tools**
5. Double-click **Task Scheduler**

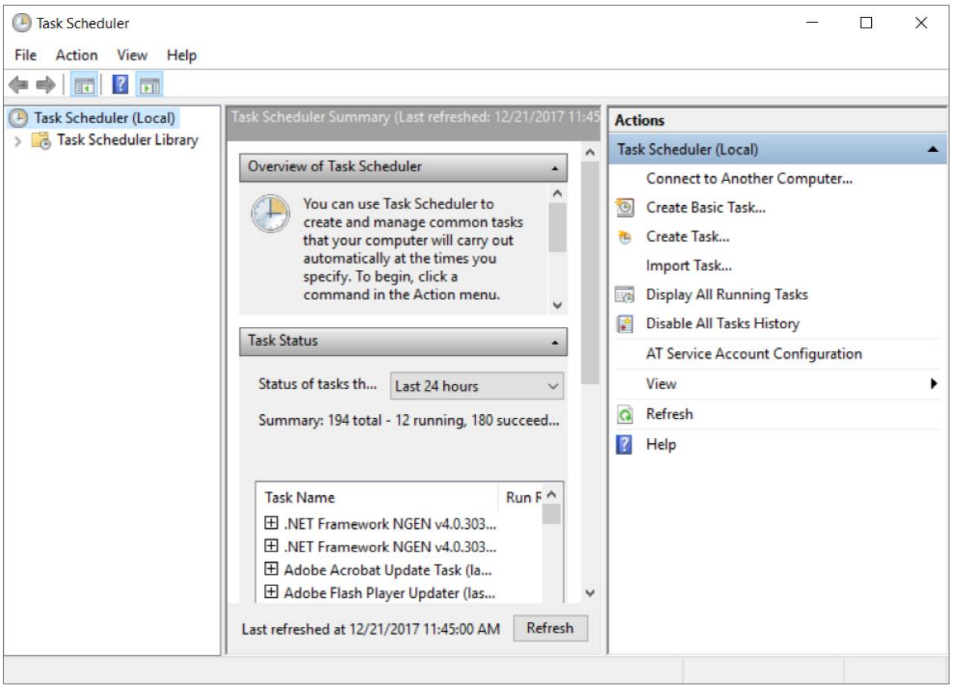
Note: To find the Task Scheduler on a machine with a German Windows 7 Professional simply click the Start button and type “Aufgabenplanung”.

To open the Scheduler Task in Windows 8 or Windows 10 carry out the following steps:

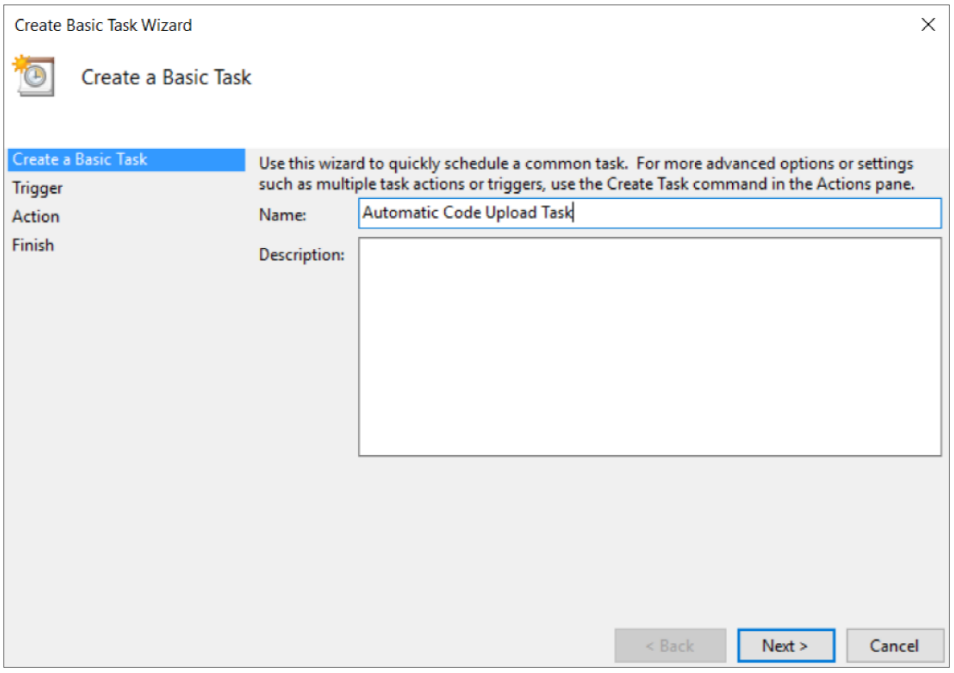
1. Tap the **Search** button on the taskbar
2. Type “**schedule**” in the **blank box**
3. Click **Task Scheduler**

After the Task Scheduler is open, you can start the Task configuration:

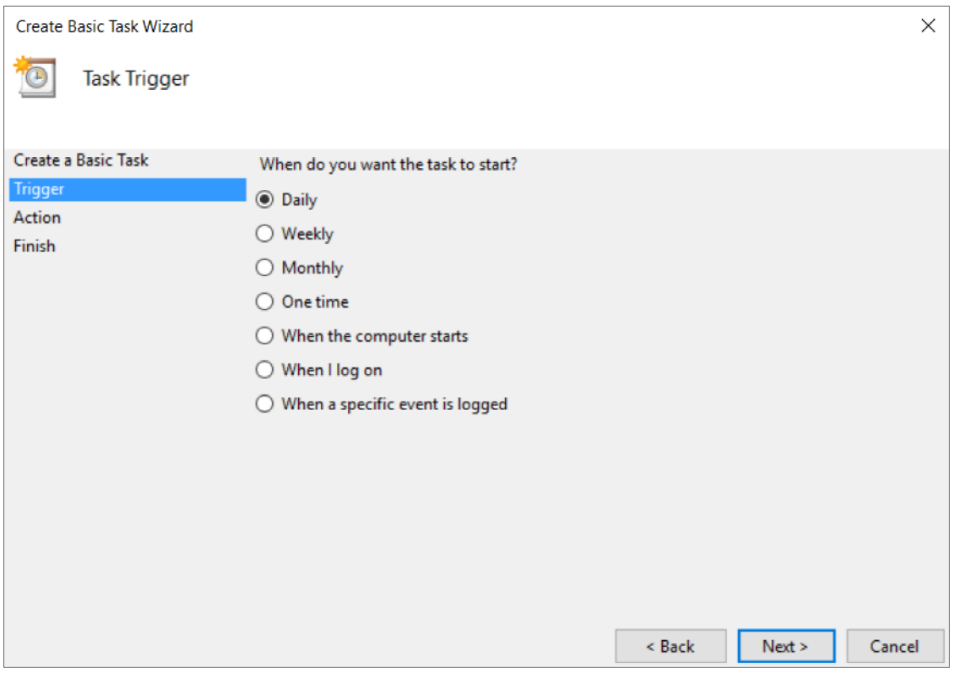
1. In the right panel of the Task Scheduler screen, right click on **Create basic task…** below **Task Scheduler (Local)** and click on



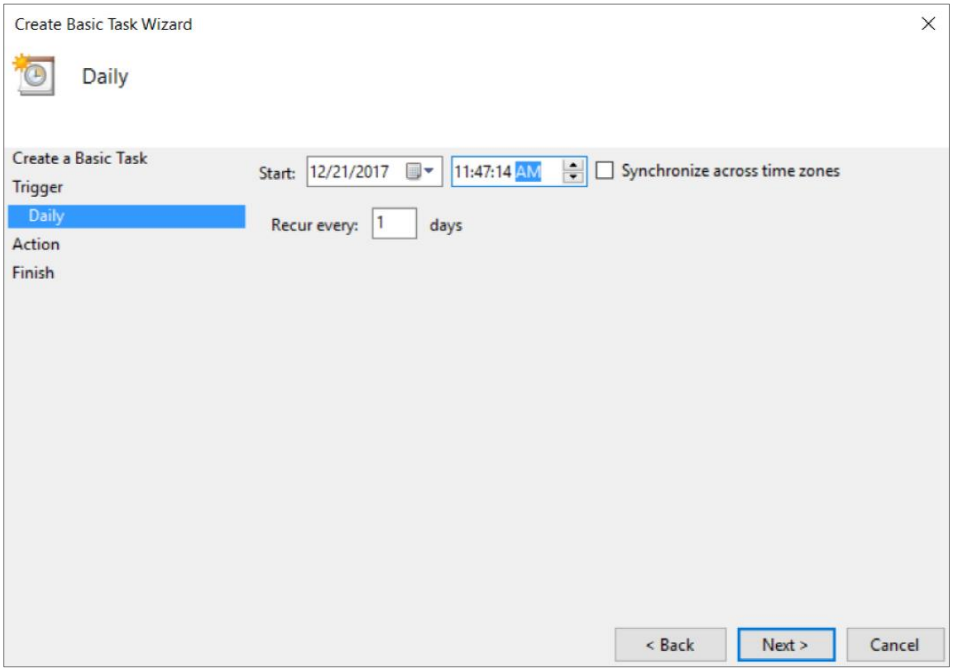
2. Add the task name in the blank field (in our case "**Automatic Code Upload Task**") and press **Next**.



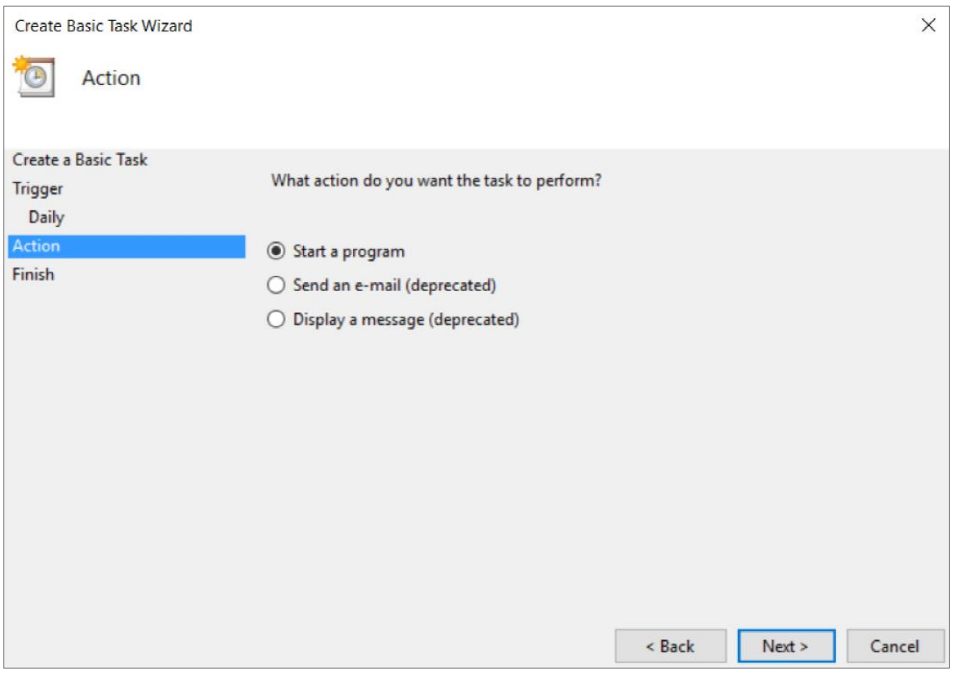
3. Select the **Trigger time** (in this case **Daily**) and press **Next** button.



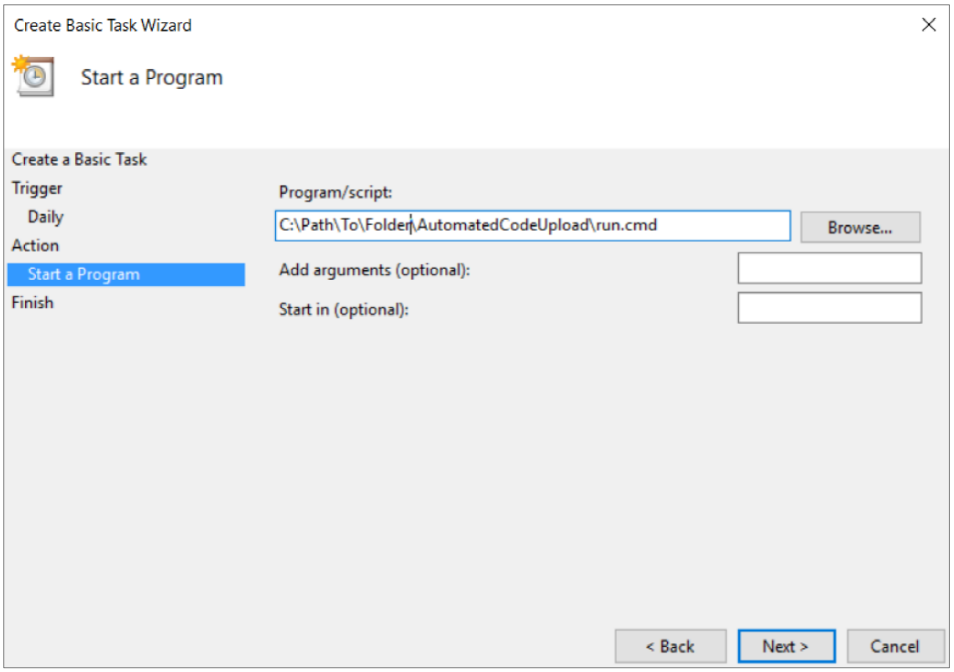
4. Define the **time** when you want to start the upload and press **Next**.



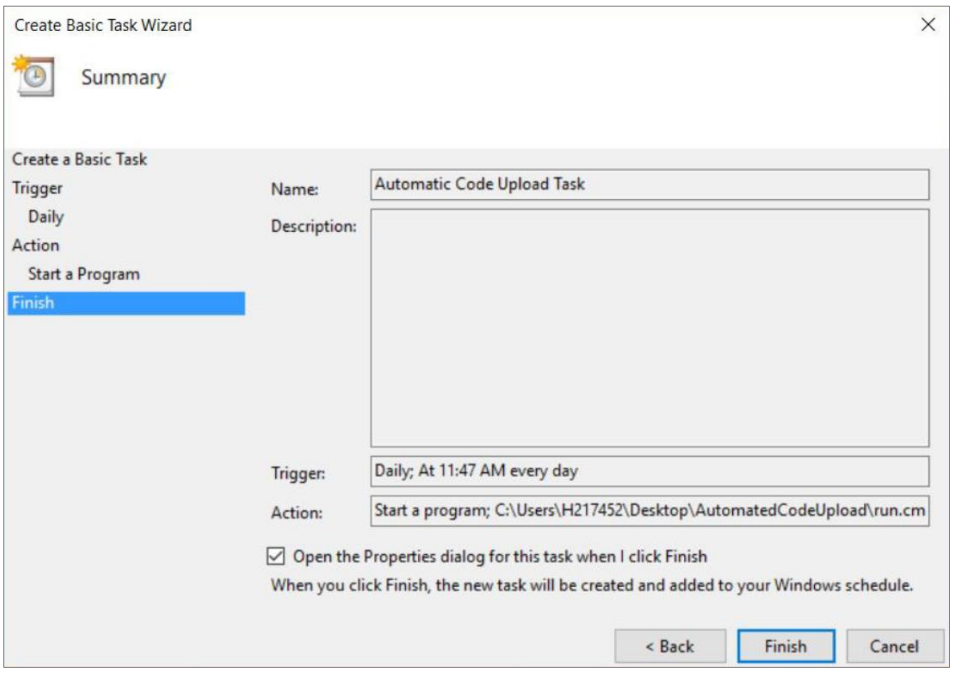
5. In the Action selection screen select **Start a program** and press **Next**.



6. In the next screen click on **Browse...** and select the file **run.cmd** program of the Automatic Code Upload folder. After that, press **Next** button.

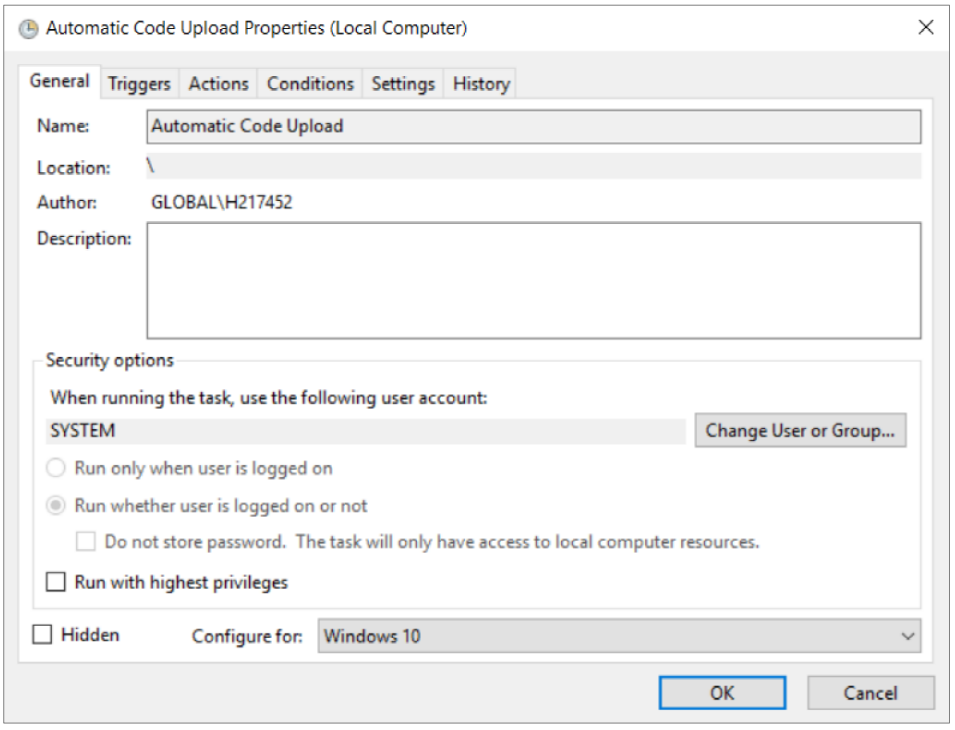


7. In the last screen, we can find a Summary of our configuration, check the **Open the Properties dialog for this task when I click Finish** checkbox and click **Finish** button.

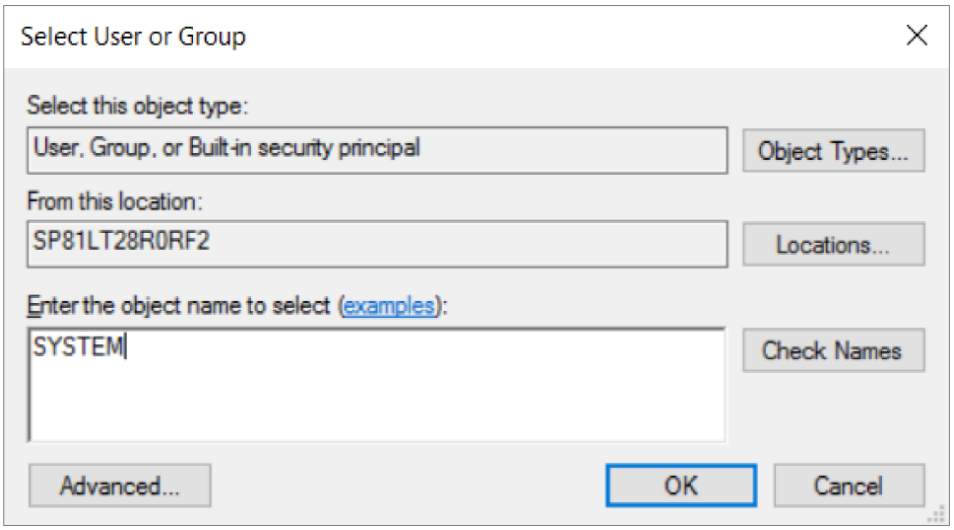


8. In the next installation steps, we are going to change the user to the **SYSTEM** user, this is necessary when the tool needs to be launched on a computer without login user (like a server) and to execute the tool without interruptions for the logged in user. To add an invisible task, click on **Change user or Group…** button.

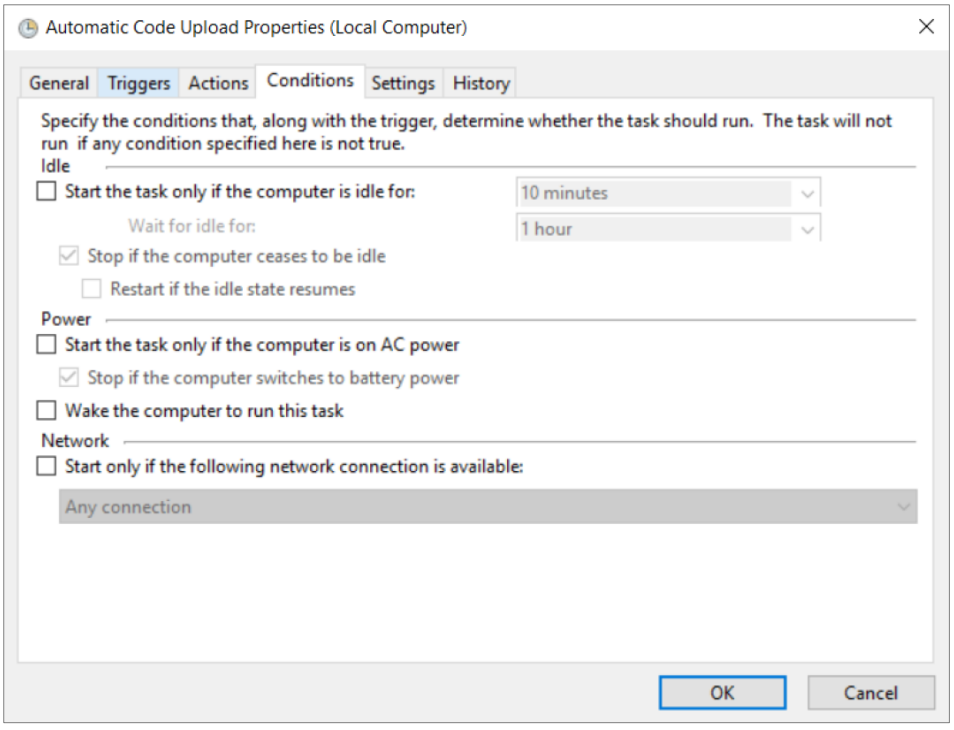
   NOTE: If you want to see the task screen when the execution starts, don't follow these steps. You can still launch the tool on a computer without login user (like a server). Therefore you need to add the option to run the task when the user is logged off by selecting the radio button **"Run whether user is logged on or not"** in the screen below (and leave the user as it is):



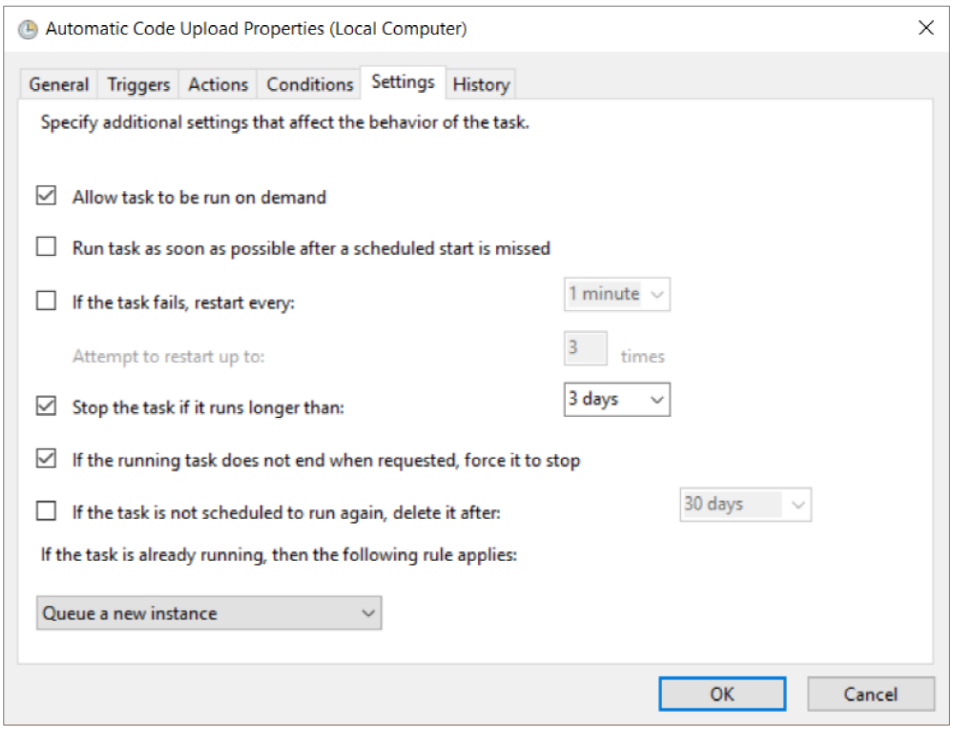
9. In the field **Enter the object name to select**, add **SYSTEM** and press **Check Names**. After that, press **OK** button.



10. In the **Conditions** tab, you can configure the conditions to start the task, we are going to uncheck **Start the task only if the computer is on AC power**. This way the task starts even if the system is a laptop and is in battery mode.



11. To finish the installation, in the **Settings** tab, select in the last drop -down list the **Queue a new instance** value. This means that, if one task spends too much time and a new task is launched to upload new codes, the new task will wait for the first one to finish.



12. After that you can click on **OK** button.

Your task is now configured and the code upload should run automatically in the background at the defined times.

This was the last step of the installation and configuration process!

3.4 Logging and error handling of the code upload

3.4.1 Log file

For each CSV file uploaded with the oneIDentity+ Automated Code Upload Tool an log file is created.

This log file is named **CodeUploadLog_[YearMonthDay_Time].log** and placed in the AutomatedCodeUpload folder. It contains the following information:

- Start and end date and time of the Upload
- Name of the uploaded CSV file
- Total number of codes in the file
- Number of correctly uploaded codes
- Number of malformed (and therefore not uploaded) codes
- Number of codes with wrong GTN (therefore not uploaded)
- invalid code(s)in human readable format in case there were/was any
- Information if the file was moved to the error or uploaded files folder

If there are one or more invalid codes within the *.CSV file, the valid codes are uploaded but the entire file is moved to the error folder. In this case you have to correct the wrong codes and upload them again by placing the corrected file once more in the input folder.

If the log file shows that the number of **Codes uploaded correctly** equals the **Total codes in file** you can be sure that all your codes were uploaded correctly, since the information about the correctly uploaded codes is only written in the log file after the **1D+ Automated Code Upload Tool** received the response from the 1D+ database in the cloud.

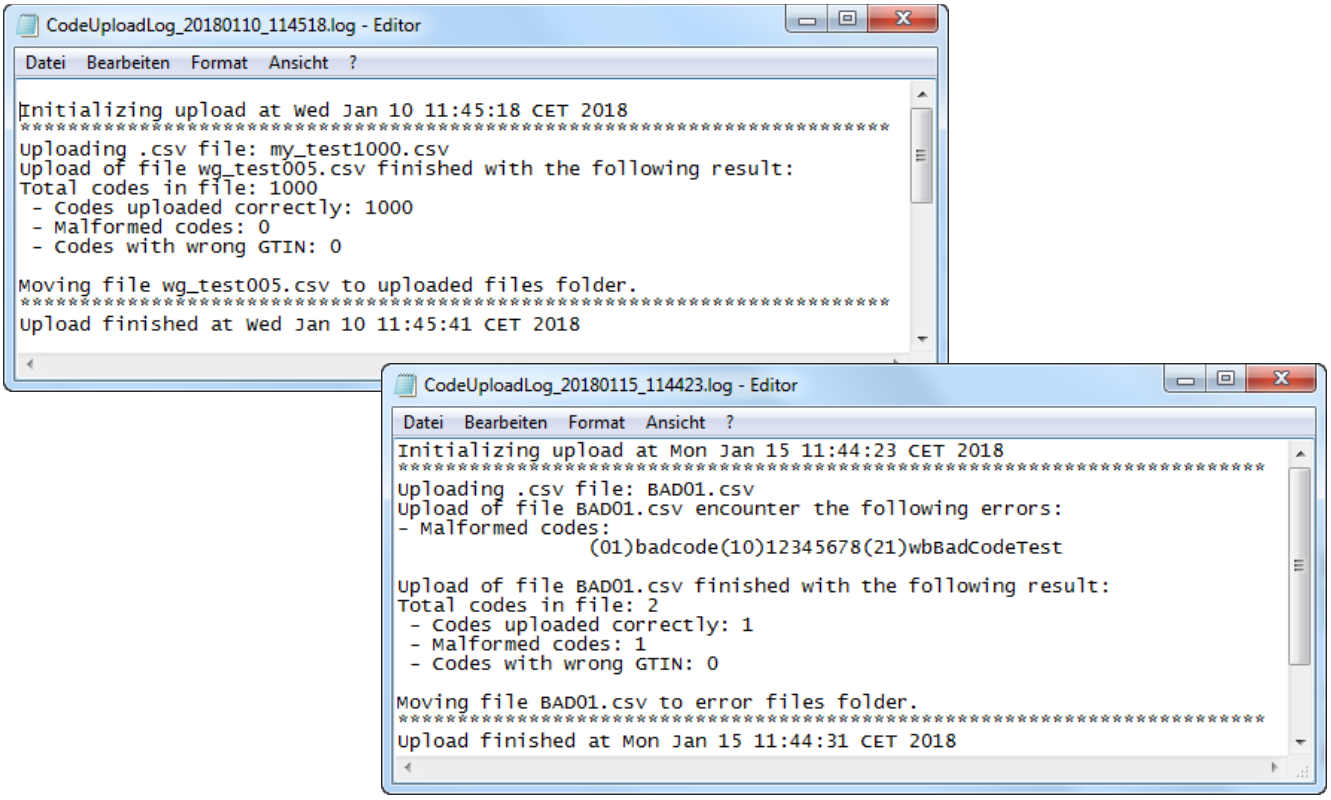


Figure 15 – Example of Log files with correct codes (above) and an invalid code (below)

3.4.2 Email Confirmations

For uploads done via the oneIDentity+ Automated Code Upload Tool you do **also** receive an **Immediate Code Upload Confirmation** via email. In addition, the uploads done via the oneIDentity+ Automated Code Upload Tool are included in the **Monthly Code Upload Report.**

Note: The **Immediate Code Upload Confirmation** will be received by all users of your organization assigned within the oneIDentity+ Administration Portal under **Code Upload** in the subtab Organization on tab Organizations, whereas the **Monthly Code Upload Report** will be send to all users defined under **Reports**.

For more details about the email confirmations see chapter Fehler! Verweisquelle konnte nicht gefunden werden.

3.5 Password encryption for the usage in the Automated Code Upload Tool

In the **acu.porperties file** of the **oneIDentity+ Automated Code Upload Tool** you need to enter user credentials (e-mail and password). For security reasons you must not enter the password as plain text but encrypted.

To transfer your plain text password into an encrypted one carry out the following steps:

1. Go to the oneIDentity+ webpage **https://www.one-identity-plus.com**
2. Open the fly-out menu below **Login** (German: **Anmelden**) on the right and select **1D+ Code Upload Tool**
3. The pop-up **Request the encrypted password for the 1D+ Automated Code Upload Tool** appears.
4. Enter the **username (e-mail)** and the **plain text password** of the Automated Code Upload Tool or SDK user and click on **SUBMIT**.
5. After a successful validation of your credentials the encrypted password is displayed.
6. Copy this to the clipboard and insert it into the **acu.porperties file**.

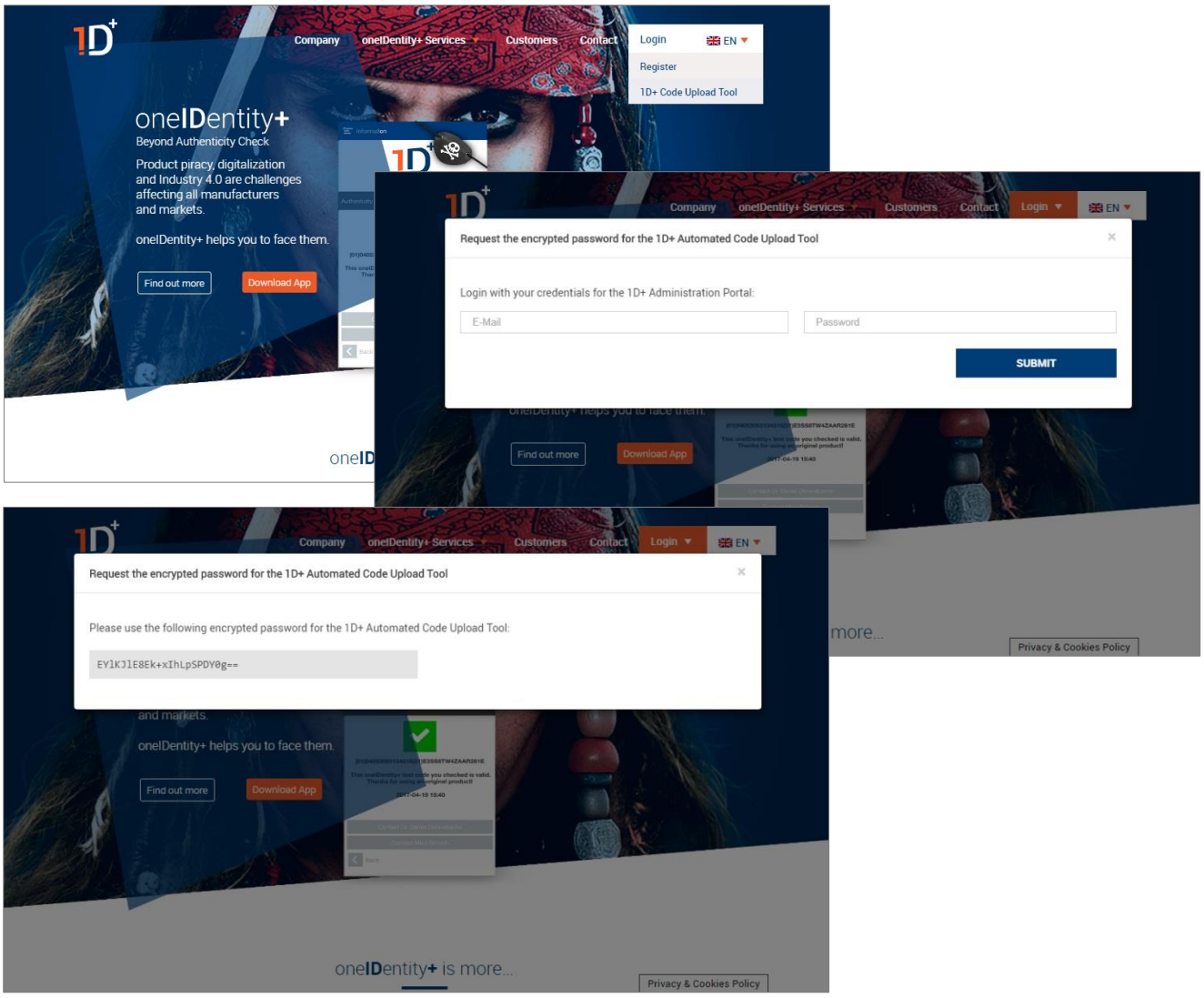


Figure 16 – Password encryption via oneIDentity+ website

4 Glossary

Term	Explanation
1D+	oneIDentity+
Super Admin	Special role within the oneIDentity+ Administration Portal for an authorized employee of the oneIDentity+ GmbH - committed to secrecy - who has access to all Organisations and all settings.
Authenticity Check	Check/validation carried out by oneIDentity+ if a code on a product/package is registered (= in the oneIDentity+ database) and was not checked too many times already. This gives an **indication** about a products genuineness, but is no proof. Only in combination with many other visible and sometimes hidden product properties, facts about sales cycles etc. the product's genuineness can be confirmed.
Authenticity of Product Codes	Indication, but no legal proof about a products authenticity by checking a MAPP code on a product/package against the oneIDentity+ database. See also Authenticity Check.
Authentication Platform	oneIDentity+ Platform which carries out a check if a code on a product/package is valid (= in the oneIDentity+ database) and was not checked too many times already. This gives an **indication** about a products genuineness, but is no proof. Only in conjunction with many other visible and sometimes hidden product properties, facts about sales cycles etc. the product's genuineness can be confirmed.
Authentication Result	Result of the Authenticity Check (see above) carried out by oneIDentity+
EPCIS	= Electronic Product Code Information Services This is a global GS1 Standard for creating and sharing visibility event data, both within and across enterprises, to enable users to gain a shared view of physical or digital objects within a relevant business context.
GCP (GS1 Company Prefix)	= Global Company Prefix according to GS1 standards A unique string of four to twelve digits used to issue GS1 identification keys. The first digits are a valid GS1 Prefix and the length must be at least one digit longer than the length of the GS1 Prefix. The GS1 Company Prefix is issued by a GS1 Member Organisation. As the GS1 Company Prefix varies in length, the issuance of a GS1 Company Prefix excludes all longer strings that start with the same digits from being issued as GS1 Company Prefixes.
GLN	= Global Location Number according to GS1 standards This GS1 Identification Key is used to identify physical locations or legal entities. The key comprises of a GS1 Company Prefix, Location Reference, and Check Digit. This identifier is compliant with norm ISO/IEC 6523.
GS1	A not-for-profit organisation that develops and maintains global standards for business communication (e.g. the barcode based on the GTIN [former EAN] from which the product type can be concluded and which is scanned electronically at counters etc.)
GTIN	= Global trade item number

	This GS1 identification key used to identify trade items. The key comprises of a GS1 Company Prefix, an item reference and check digit and is the first part of the MAPP code.
MAPP	= Manufacturers against Product Piracy Initiative of different manufacturers mainly within the Independent Automotive Aftermarket to fight together against counterfeiters (see www.mapp-code.com)
MAPP code	2D data matrix code according to GS1 standards used by members of the MAPP initiative to genuinely mark their products
Organization Admin	Special role within the oneIDentity+ Administration Portal for the administrator of the manufacturer using oneIDentity+. Administrators can view and download statistics about their organizations code checks, administer settings and users of their company and upload product codes into the oneIDentity+ database.
Product Code Authentication	See Authenticity Check
VAS	Value Added Service within oneIDentity+