Trust.med

Developer API Documentation

Last Updated: 09/2023

Document Details

Document Status	Approved ▾
Document Owner	John Winkler
Reviewers	Dan Kraciun Tom Cooper Eric Moore
Distribution	External

Introduction

Welcome to the Trust.med API documentation, your gateway to seamless integration with Trust.med's utilities for secure and efficient healthcare supply chain communication. Trust.med empowers partners with a suite of powerful communication utilities to enhance transparency, streamline operations, and ensure the highest standards of product quality and patient safety.

Our API enables you to perform the following actions:

1. **Submit EPCIS Data (DataX):** Seamlessly exchange Electronic Product Code Information Services (EPCIS) data with your trading partners. Whether you prefer direct file transfers or transmitting EPCIS data as an XML string body, Trust.med provides you with the flexibility you need. Your XML data should encompass an EPCIS Header, complete with a Standard Business Document Header, and an EPCIS Body housing an Event List.

2. **Verification Requests:** Utilize the GS1 Verification Lightweight Messaging Standard (VLMS) to initiate verification requests. By providing the requisite information, you can submit verification requests to a Verification Router Service (VRS) partner. Alternatively, for quick and convenient product verification, you can submit a scanned string from a 2D Data-Matrix.

   Note: Please refer to the dedicated "Verification API" section for detailed information and usage guidelines.

3. **Recall Notifications:** Access Recall Notifications sent to downstream partners, gather acknowledgment status for recalls initiated within the Trust.med system. If you are a downstream partner, you can get access to and acknowledge recall notifications sent to your locations. This feature ensures timely awareness and response to recalls, bolstering the integrity of your supply chain systems.

Table of Contents

Authentication

The Trust.med API utilizes two methods for Authentication:

1. mTLS Certificate based authentication
2. JWT Token based authentication
    a. Backed by Basic Authentication: Username and Password

Certificate Authentication

In order to authenticate via certificate, you must complete the following:

1. Generate a self-signing CA Certificate (or use an accepted signed like Verisign)
2. Trade Public keys of CA or CA bundles with Trust.med.
3. Generate and sign your client certificate using the CA.
4. Provide your signed client certificate with all requests.

After Step 3, Trust.med support will need to associate the CN value from your certificate with an account in the system. If your CN value changes at any time, Trust.med will need to verify the new CN value and update this within our platform.

JWT Token Authentication

Authentication Type: Username/Password Basic Authentication

TEST Domain: https://demo.api.trust.med/v1.0

PROD Domain: https://api.trust.med/v1.0

POST /token/

API endpoints contained in this document that require the use of an access token passed within the header of the request in order to facilitate authentication.

Example Header:

```
"Authorization: Bearer 123abc...987zyx"
```

In order to generate the access token, follow these steps:

1. Gather your username and password.
2. Send a request to the Access Token Generation endpoint.

3. You will send the username, password, scope, grant_type and client_id as Post Body elements.
4. Gather the access token from the response that comes back.

Example

Request Body

Data	Format	Description
username	string	The Username for your API account
password	string	The Password for your API account
client_id	Exact	dotmed
scope	Exact	openid

```
{
       "username": "your-username",
       "password": "your-password",
       "client_id": "dotmed",
       "scope": "openid"
}
```

Response

When successful, the API will return a HTTP 200_OK response with the following body:

```
{
  "access_token": "abc123...987zyx",
  "expires_in": 2592000,
  "token_type": "Bearer"
}
```

DataX API

Authentication Type: mTLS Certificate Based Authentication

TEST Domain: https://staging.partner.trust.med/v1

PROD Domain: https://partner.trust.med/v1

Submit an EPCIS File / Data

POST: /client/storage/

By submitting a file as an “application/xml” or “text/xml” content type, Trust.med will capture, consume, and route the appropriate EPCIS information to your, and the downstream partner’s, data repositories.

If the downstream partner has been configured with a service provider integration, we will also deliver the information to the partner via that service provider method configured.

It is important that the Sender GLN and the Receiver GLN be provided within the Standard Business Document Header for identification and routing purposes for all **Standard/Direct Ship** data communications. **Drop Ship** data communications will use a slightly different approach please contact Trust.med for more information regarding the Drop Ship method of data transfer.

Example

Request Body

```
<?xml version="1.0" encoding="utf-8"?>
<EPCISDocument xmlns:cbvmda="urn:epcglobal:cbv:mda" xmlns:gs1ushc="http://epcis.gs1us.org/hc/ns"
schemaVersion="1.2" xmlns="urn:epcglobal:epcis:xsd:1">
  <EPCISHeader>
    <StandardBusinessDocumentHeader
xmlns="http://www.unece.org/cefact/namespaces/StandardBusinessDocumentHeader">
      …
    </StandardBusinessDocumentHeader>
  </EPCISHeader>
  <EPCISBody>
    <EventList>
      …
    </EventList>
  </EPCISBody>
</EPCISDocument>
```

Response

When successful, the API will return a HTTP 200_OK response with the following body:

```
{
    "id": UUID4 ID,
    "created_at": Datetime
}
```

Verification API

Authentication Type: JWT Authentication

TEST Domain:

- https://staging.api.trust.med/v1.0

PROD Domain:

- https://api.trust.med/v1.0

The Verification API uses the Trust.med Registry system with our API system to bring the power of Verification to each and every configured property within the ecosystem. The Verification API endpoint provides a uniquely tailored URL. Appending the appropriate Verification details to the unique uniquely generated URL submits a product verification request. If the GTIN or NDC provided within the request has not been configured an HTTP 404 response will be returned.

Gather the Verification URL

GET /verify/{type}/{value}

Request Path Parameters

Data	Format	Description
type	a-zA-Z0-9-	String or Number Application Identifier EX: “gtin” or “01”
value	N{14}	The GTIN or dash included NDC value

Responses

Code	Response	Description
200	URL as string	The identifier was found and verification configured
204	None	The identifier was found but verification not configured
404	None	The identifier was not found

Submit Verification with Text

GET /verify/gtin/{gtin}/lot/{lot}/ser/{serial}/?exp={YYMMDD}
GET /gtin/{gtin}/lot/{lot}/ser/{serial}/?exp={YYMMDD}

Special Header Information

The following pieces of information can be passed in the header. Information passed in the header will be attached to the verification request through to the verification responder.

Data	Format	Description
ATP-Authorization	Verifiable Presentation	An ATP presentation
GS1US-Version	N.N.N (Ex: 1.3.1)	The GS1 Implementation Guideline Version

Request Path Parameters

Data	Format	Description
gtin	N{14}	14-digit GTIN value (even for NDC domains)
lot	a-zA-Z0-9-	The lot in question
serial	a-zA-Z0-9-	The serial number in question

Query String Parameters

Name	Format	Required	Description / Value
exp	YYMMDD	Yes	Expiration date of the product being verified
linkType	Exact	Yes	verificationService
context	Exact	Yes	dscsaSaleableReturn
reqGLN	N{13}	Yes	The GLN of the requesting party
corrUUID	A{8-4-4-4-12}	Yes	The v4 UUID used to identify the request
ctrlPossessAtt	Boolean	Yes	Is the drug in your possession
email	String	Yes **	The contact email for the requestor
telephone	N{30}	Yes **	The contact phone number for the requestor

** At least 1 of an email address OR telephone number must be provided.

Examples

Response

When successful, the API will return a HTTP 200 response with the following body:

```
{
    "verificationTimestamp": Datetime,
    "responderGLN": 13-digit String,
    "data": {
        "verified": Boolean
    },
    "corrUUID": UUID4,
    "contactPoint": {
        "email": String
        "telephone": String
    }
}
```

Submit Verification with Scan String

POST /verify/

Special Header Information

The following pieces of information can be passed in the header. Information passed in the header will be attached to the verification request through to the verification responder.

Data	Format	Description
ATP-Authorization	Verifiable Presentation	An ATP presentation
GS1US-Version	N.N.N (Ex: 1.3.1)	The GS1 Implementation Guideline Version

Query String Parameters

Name	Format	Required	Description / Value
scan_str	Hex String	Variable *	Scanned string representation of the 2d Data Matrix
linkType	Exact	Yes	verificationService
context	String	Yes	dscsaSaleableReturn
reqGLN	N{13}	Yes	The GLN of the requesting party
corrUUID	A{8-4-4-4-12}	Yes	The v4 UUID used to identify the request
ctrlPossessAtt	Boolean	Yes	Is the drug in your possesion
email	String	Yes **	The contact email for the requestor
telephone	N{30}	Yes **	The contact phone number for the requestor

* The scan_str MUST contain the GTIN, Lot, Serial and Expiration, hex encoded, provided in the query string or post body.
** At least 1 of an email address OR telephone number must be provided.

Post Body Parameters

Name	Format	Required	Description / Value
scan_str	Hex String	Variable *	Scanned string representation of the 2d Data Matrix
format	Exact	No	hri - Will read string as if it has ( ) included around AI's
seperator	Character	No	The separator character for scan if the default FNC1 is not used

Examples

cURL

```
curl --request POST\
--url
'.../verify?linkType=verificationService&context=dscsaSaleableReturn&reqGLN=1200109
076893&ctrlPossessAtt=true&email=tester@example.med&corrUUID=0545a13c-f14c-4437-b8d
f-fbb8bcf91ce0&scanstr=303130393532313131313233343536323137333031323331313054455354
4c4f54313233341d323154455354534552313233 34' \
--header 'Authorization: Bearer abc123…xyz'
```

Note: The hex conversion for the FNC1 character is 1d, which you can see underlined and bolded towards the end of the scan_str in the above example.

Response

When successful, the API will return a HTTP 200 response with the following body:

```
{
    "verificationTimestamp": Datetime,
    "responderGLN": 13-digit String,
    "data": {
        "verified": Boolean
    },
    "corrUUID": UUID4,
    "contactPoint": {
        "email": String
        "telephone": String
    }
}
```

Recall API

Authentication Type: JWT Authentication

TEST Domain:

- https://staging.api.trust.med/v1.0 (Token)
- https://demo.dashboard.trust.med/v1.0 (Recall)

PROD Domain:

- https://api.trust.med/v1.0 (Token)
- https://dashboard.trust.med/v1.0 (Recall)

Manufacturer - List Recalls

GET /recall/

Response

When successful, the API will return a HTTP 200 response with the following body:

```
[
  {
    "id": 12345,
    "identifier": "…",
    ...
    "products": [{
        "id": 123,
        ...
        "ndc_list": [{
          "Id":4523,
          "Inner_label": "12345-123-01",
          ...
         },...
        ]
    },...]
  },
...
]
```

Manufacturer - List Notifications for a Recall

GET /recall/{id}/notifications

Request Path Parameters

Data	Format	Description
id	Number	The numerical ID for the recall

Response

When successful, the API will return a HTTP 200 response with the following body:

```
[
  {
    "id": 12345,
    "Acknowledge": true,
    ...
    "company": {...},
    "location": {...},
    "recall": {...},
  },
...
]
```

Downstream Partner - Gathering New Recall Notifications

GET /recall-notifications/

This endpoint will be utilized to gather all new Recall Notifications tied to the locations that the user manages. While this is like the above, it doesn't require an ID and is used by downstream partners to gather only the "new" notifications tied to their specific locations.

Note: If you are a data service provider gathering the list of notifications for your clients, they will automatically be marked as "Acknowledged" to the manufacturers view with the expectation that your software will deliver the notification and required information to the downstream partner. You are accepting liability for distributing the information to the partner on behalf of Trust.med and the upstream partner.

Response

When successful, the API will return a HTTP 200 response with the following body:

```
[
  {
    "id": 12345,
    "identifier": "…",
    ...
    "products": [{
        "id": 123,
        ...
        "ndc_list": [{
          "Id":4523,
          "Inner_label": "12345-123-01",
          ...
         },...
        ]
    },...]
  },
...
]
```

Contact Details

If you require assistance please contact Trust.med at:

Email: support@trust.med
Phone: 855-630-0633