Government of India
Ministry of Commerce and Industry
Department of Commerce
Directorate General of Foreign Trade
*****

Vanijya Bhawan, New Delhi
Dated: September 07, 2026

Trade Notice No. 25/2026-27

To,

1. All Exporters / Members of Trade & Industry
2. All Designated CoO Issuing Agencies
3. All Export Promotion Councils / Trade and Industry Associations
4. All DGFT Regional Authorities

Subject: Introduction of Open API Integration for Certificate of Origin (CoO) through Trade Connect e-Platform – regarding.

The Directorate General of Foreign Trade (DGFT) has been undertaking various initiatives for digitalisation and ease of doing business. In this regard, an Open API facility for issuance of Certificates of Origin (CoOs) has been introduced on the Trade Connect e-Platform and is now being released and made available for use by eligible exporters/systems as per the prescribed process and technical requirements.

2. The objective of the Open API facility is to enable exporters to integrate their Enterprise Resource Planning (ERP), accounting or other software systems with the DGFT's Certificate of Origin system for electronic submission and exchange of CoO-related information, thereby reducing manual data entry and facilitating a more efficient application process.

3. **Access and Onboarding:** The complete process for registration, API access, authentication, technical integration and use of the Open API facility is available on the Trade Connect e-Platform at:

"https://www.trade.gov.in/pages/certificate-of-origin → API Management for Exporters"

3.1. The Help Manual containing the step-by-step procedure for accessing and using the facility is provided at Annexure-I.

UNCOMPLYCATE Simplifying compliance

4. **Support Channels:** Exporters and stakeholders are encouraged to reach out to the DGFT Helpdesk with respect to any queries, suggestions, or feedback related to the eCoO module. Support is available through the following channels:

- **Toll-Free Assistance:** You may contact the DGFT Helpdesk through our toll-free numbers for support.
- **Email Inquiries:** For clarifications or further assistance, please e-mail DGFT.

6. All concerned stakeholders are encouraged to undertake the necessary technical integration and make use of the Open API facility in accordance with the process and technical specifications prescribed by DGFT.

This is issued with the approval of the competent authority.

(Prakash Kamble)
Deputy DGFT

(Issued from File No. 01/02/60/AM-25/EG&TF)

UNCOMPLYGATE
Simplifying Compliance

Annexure – I

Help Manual for accessing API facility on Trade Connect ePlatform

1. Introduction

The Certificate of Origin (CoO) Open API framework enables secure integration between user systems and the CoO Trade Connect ePlatform for the submission, processing, issuance, and verification of Certificates of Origin. The objective is to establish a standardized digital ecosystem that reduces manual intervention, eliminates duplicate data entry, improves data accuracy, and facilitates seamless information exchange among exporters, certifying agencies, and regulatory authorities.

The platform supports:

1.1. Preferential Certificate of Origin

Issued under Free Trade Agreements (FTAs), Regional Trade Agreements (RTAs), and Preferential Trade Agreements (PTAs), enabling exporters to obtain tariff concessions in importing countries.

1.2. Non-Preferential Certificate of Origin

Issued for compliance, customs clearance, trade remedy implementation, and other trade-related purposes without providing any preferential tariff benefits.

2. API Process Flow

2.1. Prerequisites

Before proceeding with API integration, agencies are required to:

- Obtain onboarding credentials from the API Management section of the CoO Portal.
- Add the relevant public IP address(es) to the IP Whitelist in the API Management section of the CoO Portal.
- Ensure that the user system has a document signer configured for digitally signing the payload before transmission to the CoO system.

2.2. Workflow

1. Obtain API credentials, including User ID, Password, API Key, and Public Key, from the API Management section of the CoO Portal.
2. Encrypt the password using PBKDF2 with a dynamic salt.
3. Call the Authentication API to generate an access token.
4. The system validates the credentials and, upon successful validation, returns

an access token.

5. The access token remains valid for 60 minutes.
6. Submit CoO applications using the CoO File API.
7. Issued certificates can be validated using the Certificate Verification API.

2.3. Process Workflow

1. The user will be provided with the X-API-Key, unique User ID, Password, and CoO Public Key through the API Management section of the CoO Portal.
2. The user shall provide the public IP address(es) from which the API calls will be made. Only API calls originating from the whitelisted public IP addresses will be permitted by the CoO system.
3. The user shall append a 32-byte dynamic salt to the password before hashing it using PBKDF2, with an iteration count of 65,536 and a key length of 256 bits. The string representation of the dynamic salt bytes appended to the encrypted hash bytes shall be passed as the password.
4. The user system shall generate an access token by passing the X-API-Key, User ID, and PBKDF2 dynamic-salted password generated in Step 3 to the generateAuthToken API. The CoO system shall validate the User ID, password, and IP address. Upon successful validation, the system shall return the access token.
5. The access token generated in Step 4 shall remain valid for 60 minutes. The user may cache and reuse the token during its validity period.
6. CoO File API: The user shall submit the data in the prescribed standard format and, in response, receive the certificate and associated data.
7. CoO Verify API: The API shall be used to verify the authenticity of a Certificate of Origin issued through the CoO system.

3. API Credentials & Ledger Management Guide

3.1. API Credentials

Please refer to the API Credentials screen for details regarding API credentials, IP whitelisting, and public certificates.

The user may regenerate the password and secret key using the respective buttons provided on the screen. The password, X-API Key, and secret key can be viewed after successful validation of the OTP received on the registered mobile number and email address.

Call the Auth Token API to obtain an access token. The access token remains valid for 60 minutes and may be reused during its validity period.

3.2. Ledger Management

1. A ledger shall be maintained for each API transaction. The applicable ledger statuses are:

- Draft
- In Process
- Approved
- Certificate Issued
- Rejected

2. Upon successful processing, the CoO system shall return the following details:

- Acknowledgement ID
- File Number
- File Date
- Certificate Number
- Response Code
- Remarks

These details shall be recorded in the exporter's ledger.

3.3. API Help

Please refer to the API Help tab under the API Management section for detailed API specification information.

Note:

All requests and responses shall be digitally signed using:

- SHA-256 RSA Digital Signature
- 2048-bit X.509 Certificates

This ensures:

- Data integrity
- Sender authentication
- Non-repudiation

4. Certificate of Origin Auth Token API

Please refer to the API Credentials screen for details regarding API credentials, IP whitelisting, and public certificates.

Call the Authentication Token API to obtain an access token.

The access token remains valid for 60 minutes and may be reused during its validity period.

UNCOMPLYCATE Simplifying Compliance

The request contains the following parameters in JSON format:

- User ID
- Password
- Header
- Content-Type: application/json
- X-API-Key

5. Certificate of Origin File API

The CoO File API is the primary transaction API used for application submission.

5.1. Applicant Information

The applicant section captures:

- IEC Number
- Firm Name
- Branch Details
- GSTIN
- Address Information
- State and District
- Declaration Status
- Postal Delivery Requirement

5.2. Certificate Information

The certificate section includes:

- Certificate Type
- Trade Agreement
- Request Type
- Issuing User
- Regional Office
- Issuing Office
- Exhibition Declaration
- Cumulation Information
- Producer/Exporter Details

5.3. Importer Information

Key details include:

- Importer Name
- Country
- Address

UNCOMPLYCATE
Simplifying Compliance

- Email Information

5.4. Producer Information

Where applicable, the following details may be provided:

- Producer Name
- Address
- Country
- Producer Identifier
- Telephone Number
- Email Address

5.5. Invoice Information

The invoice section includes:

- Invoice Number
- Invoice Date
- Currency
- Exchange Rates
- Third Country Invoicing Information

5.6. Export Product Information

The export product section captures:

- ITC HS Codes
- Product Description
- Quantity
- Unit of Measurement
- Invoice Value
- FOB Value
- Packaging Details
- Preference Criteria

5.7. Shipment Information

The shipment section includes:

- Mode of Transport
- Shipment Documents
- Port of Shipment
- Port of Discharge
- Route Information

UNCOMPLYCATE
Simplifying Compliance

- Vessel Details
- Departure Date
- Exporter Remarks

5.8. Supporting Documents

The supporting document section stores:

- Attachment Type
- Upload URL
- Remarks
- Attestation Requirements

5.9. Declaration Information

Mandatory declaration information includes:

- Place
- Date
- Applicant Name
- Designation
- Contact Information
- Compliance Declaration Acceptance

Note:

Trade Agreements Supported

The framework supports the following trade agreements and certification schemes.

Key Agreements:

- India-Japan CEPA (IJCEPA)
- India-Korea CEPA (IKCEPA)
- SAFTA
- SAPTA
- ASEAN-India FTA
- India-Singapore CECA
- India-Malaysia CECA
- India-Chile PTA
- India-Mercosur PTA
- India-UAE CEPA
- India-Australia ECTA
- India-Oman CEPA
- India-EFTA TEPA

UNCOMPLYCATE Simplifying Compliance

- India-UK CETA
- Generalized System of Preferences (GSP)
- Non-Preferential CoO Scheme

Dynamic Validation

Each agreement contains specific:

- Mandatory fields
- Optional fields
- Business validations
- Product origin criteria
- Shipment requirements
- Producer and exporter declarations

The API dynamically validates applications according to the selected agreement.

6. Certificate Verification API

Verification can be performed using:

- File Number
- File Date
- Certificate Number
- Certificate Date

The CoO system returns:

- Validity Status
- Certificate PDF URL
- Verification Remarks

UNCOMPLYGATE
Simplifying Compliance