



TAMIL NADU POLLUTION CONTROL BOARD

The Open API (Application Programmable Interface) with Client Side requirement for other Software developers to develop client side requirement and establish connectivity with the Central software of Knowledge Lens at Care Air Centre. The interested developers after development shall contact Care Air Centre, TNPCB for demo for approval of Technical committee.



GLens Central Server Software Open API

July 3, 2015

GLens Open API Version No 2.1 dated 3rd July 2015

Overview

GLens provides an Open API for integrating multi-software clients to GLens server. All communication between GLens Central Server and acquisition clients (at Industry site) are all managed through HTTP-based REST API. All the API are authenticated. Any approved software client complying with the specified open API can upload the data to the Central GLens Server.

Supported Operations in Version 2.1

The following are the operations supported in Version 2.1 of the GLens Open API. All clients should support full integration with all these operations.

- Real Time Data Upload
- Delayed Data Upload
- Remote Analyser Configuration
- Remote Analyser Calibration
- Analyser Diagnostic Fetch

Key Concepts

The following are the key concepts to be followed while working with the GLens Open API

- Site ID: Unique Site ID identifying the specific industry
- Monitoring ID: Each Site has multiple monitoring stations. Each monitoring station will be assigned a unique monitoring ID relative to the Site
- Analyser ID: Each analyser make and model will be assigned a unique Analyser ID
- Parameter ID: Each monitored parameter will have a common unified ID across all industries

Client Side Software Requirement

Each client software implementing the API should also comply with “Client Side Software Requirement published by TNPCB”

Key API Requirements

- Each site client software has to collect the data from the analyser based on the poll frequency defined. Ideal frequency for data sampling from analyser is 10 second. Data



GLens Central Server Software Open API

July 3, 2015

transmission to the Central Server should be at 1 minute frequency. The raw data and linearized data should be transmitted to the server along with the data quality code and captured timestamp.

- The captured data should be transmitted to the Server immediately after encrypting the data with the digital private key. This digital private key should be kept safe and shouldn't be tampered with or disclosed to others. The Client Software should provide a mechanism for generating industry specific digital signature to establish the data connectivity with Central Server Software. Industry should procure the Digital Signature as soon as possible, provide the details of the Digital Signature and use that for data encryption to ensure authentic tamper proof data transmission.
- The transmitted data should be encrypted zipped data in ISO-7168. All API request data transfer should be using a REST Service over HTTP protocol.
- The client site software should wait for successful upload and also read subsequent instructions (Remote calibration, Configuration update, Diagnostics information etc.) from the Central Server Software
- On receiving instructions on Remote calibrations or Configuration update, the site client software should invoke the Remote Calibration or Configuration update services to download the corresponding configurations.
- In-case of any communication failure or any delayed data transmitted beyond a period 2 minutes, site software should store the data the locally and upload to the Delayed Data Upload URL and not to the Real Time upload URL. This is to ensure that the delayed data is captured separately at the Central Server and can be tracked for any integrity issues.
- All client should transmit data captured directly from the analyser from the site location. Any data transmission from different location will be rejected by the server.
- All the requests from the client to the server should be authenticated requests only. Any unauthenticated requests will be discarded or not processed.

Basic Organization of API

<http://<ipaddress:port>/GLensServer>

Resource	Description	Route	Request type
Data upload	This is for uploading data to the central server from the client. Any authenticated client with proper credentials can upload data to the server using this api. Only real time data (delay of max 2 min) will be accepted through /realtimeupload URL and any delayed data should be uploaded using /delayedUpload URL	/realtimeUpload /delayedUpload	POST
Configuration Download	This is for downloading the configuration from the server. Any approved client software can	/getConfig	POST



GLens Central Server Software Open API

July 3, 2015

	download the configuration from the server using this API		
Fetch Client Configuration	When the ConfigurationUpdateFlag is set to "True" in the response of the Realtime Upload or Delayed Upload, client needs to provide the current configurations set at the Analyser.	/uploadConfig	POST
Acknowledge Configuration Download	When the ConfigurationDownloadFlag flag is set to "True" in the response of the Realtime Upload or Delayed Upload, the client software should use the /getConfig URL to download the configuration from the Central Server. Once the configuration is updated in the Analyser, the client should update the Central Server with the status of the configuration update. Till the status is updated to success, client will be asked continuously to update the configuration by setting the ConfigurationDownload flag to "True".	/completedConfig	POST
Calibration download service	When the RemoteCalibrationUpdateFlag is set to "True", the client software should use this URL for downloading the configuration required for calibration. The remote calibration data and sequence should be updated to the Calibrator locally	/getcalibrationconfig	POST
Calibration Update Acknowledgement	After successful download of the Remote Calibration Configuration and updating the local calibrator or analyser who will be performing the calibration, the client software should acknowledge the status of calibration status using this URL	/updatecalibrationconfig	POST
Diagnostic Upload service	When the DiagnosticUpdateFlag is set to "True", the client software should use this URL for uploading the diagnostic information including any internal state of the analyser as per the analyser make and model.	/uploadDiagnosticInfo	POST



Authentication Mechanism for the API

Each API request header should have the following information

- A. Timestamp
- B. Authorization → Encrypted data from the site which has the authentication digest. Each request should send authentication digest with the following encrypted data
 - site_key → Unique Site Key provided by the Tamil Nadu Pollution Board for each site for authentication
 - software_version_id → Software version set by the Central Server for the industry
 - time_stamp_data → Timestamp when the data was encrypted

The authentication digest is decrypted using the Site Private Key. The timestamp is ensured to be not more than 15 minutes (configurable) from the current timestamp. The software version is verified against the registered software version with the Central Server Software. This ensures the data is encrypted just before transmission and the client program have access to Site Private Key and the current registered software version. The registered software version will be updated from Central Server Software time to time and hence is not depend on client software version.

Data Upload

The standard response format is described below. Any approved client software with proper credentials can send data to the central server using this API.

Data Upload Format

The GLens API supports 2 different types of data format for data upload. The data upload follows an ISO-7168 format zip file or a simplified delimited or fixed width file format.

The zip file upload to the server will be multipart/form-data format. The data should be sent in zip format. The uploaded zip file will have two files, namely 1. Data File, 2. Metadata File. The Data file should be encrypted using the Site Private Key. The zip file should be uploaded to the server with proper authentication using the key. Else the response with HTTP 401 with "Authentication Failure" will be returned.

The metadata file will specify the file formats (ISO-7168, CSV, FixedWidth) etc. and the data file should comply with the same. This gives flexibility to support different file formats based on the analyser or client software capability.

However, all files has to follow the basic guidelines

1. Data should encrypted
2. File should zipped
3. Metadata file should provide the file specification and format
4. Header should have the encryption digest for decryption of the data

Request Details

Upload data to Central Server



GLens Central Server Software Open API

July 3, 2015

This method uploads data to the server. The requests will be authenticated and hence should have the authentication header as described in section [“Authentication Mechanism for the API”](#)

<http://ipaddress:port/GLensServer/realtimeUpload> OR

<http://ipaddress:port/GLensServer/delayedUpload>

Path: **realtimeUpload or delayedUpload**

Method: **POST**

Parameters: The file to be uploaded should be send as the parameter.

Returns: Response JSON which contains the status as either **success** or **failure**

Note: realtimeUpload URL will take only data that is captured from the analyser during the last poll frequency defined by regulator. Anything delayed should be uploaded to delayedUpload URL

If the upload is success, the following response will be obtained.

```
{
  "status": "Success",
  "serverConfigLastUpdatedTime": "<time>",
  "ConfigurationDownloadFlag": "<Flag>",
  "ConfigurationUpdateFlag": "<Flag>",
  "RemoteCalibrationUpdateFlag ": "<Flag>",
  "DiagnosticUpdateFlag": "<Flag>",
  "statusMessage": "file uploaded successfully."
}
```

Where the **<time>** is the last updated time of server configurations and **<Flag>** is a Boolean value depending upon whether the site configuration is updated or not.

Flag can have values “True” or “False”

Eg:

```
{
  "status": "Success",
  "serverConfigLastUpdatedTime": "2015-02-24T13:21:19Z",
  "ConfigurationDownloadFlag": "True",
  "ConfigurationUpdateFlag": "False",
```



GLens Central Server Software Open API

July 3, 2015

```
"RemoteCalibrationUpdateFlag ": "True",  
"DiagnosticUpdateFlag": "False",  
"statusMessage": "file uploaded successfully. "  
}
```

If the upload is a failure the following response will be obtained.

```
{  
  "status": "Failed",  
  "statusMessage": "No files were uploaded."  
}
```

Configuration Download from server

The configuration download request helps the client software understand the format and parameters which should be transferred to the server. This request enables the client software to download the entire configuration for the monitoring station. This configuration should be synchronized with the analyser.

This method download the configuration from the server.

<http://ipaddress:port/GLensServer/getConfig>

Path: **getConfig**

Method: **POST**

Parameters: The site id will be passed as the parameter.

Returns: The response json contains, the configuration in case of success or failure message in case of failure.

Request body:

```
{  
  "siteId": <site-id>,  
  "monitoringid": <monitor-id>  
}
```

If the configuration download request is success, the following response will come. Any approved client software with proper credentials can download the configurations from the central server using this api. Software with improper credentials will be blocked. The request should have the valid authenticated headers.



GLens Central Server Software Open API

July 3, 2015

Request Format

The request for site configuration update will be in the following format.

```
{
  "siteId": "site_108",
  "monitoringid": "ETP_PLANT"
}
```

Response Format

```
{
  "status": "Success",
  "serverConfigLastUpdatedTime": <ServerConfigUpdatedLastTime>,
  "SiteDetails": {
    "siteName": <SiteName>,
    "siteLabel": <SiteLabel>,
    "siteConfigLastUpdatedTime": <SiteConfigUpdatedLastTime>,
    "siteId": <site id>,
    "customparameters" :{}
  },
  "CollectorDetails":[ {
    "CollectorType": <>,
    "CollectorName": <>,
    "ConfiguredChannels": <>,
    "PollingStep": <polling step>,
    "ChecksumStatusBit": <checksum bit>,
    "Address": <address>,
    "HeartBeat": <heartbeat>,
    "DataFormatBits": "00",
    "Port": <port>,
    "CommunicationTimeOut": <communication bit>
    "customparameters" :{}
  }],
  "configJson": {
    "monitoringType": {
      "required": "True",
      "padding": "-",
      "start_pos": 55,
      "end_pos": 64,
      "type": "string",
      "alignment": "left"
    },
    "monitoringId": {
      "required": "True",
      "padding": "-",
      "start_pos": 65,
      "end_pos": 84,
      "type": "string",
      "alignment": "left"
    },
    "QualityCode": {
      "required": "True",
```



GLens Central Server Software Open API

July 3, 2015

```
"padding": "*",
"start_pos": 42,
"end_pos": 43,
"type": "string",
"alignment": "left"
},
"SensorTime": {
  "required": "True",
  "padding": "-",
  "start_pos": 44,
  "end_pos": 54,
  "type": "string",
  "alignment": "left"
},
"parameterId": {
  "required": "True",
  "padding": "-",
  "start_pos": 85,
  "end_pos": 100,
  "type": "string",
  "alignment": "left"
},
"parameterName": {
  "required": "True",
  "padding": "*",
  "start_pos": 11,
  "end_pos": 25,
  "type": "string",
  "alignment": "left"
},
"Reading": {
  "required": "True",
  "padding": "*",
  "start_pos": 26,
  "end_pos": 41,
  "type": "string",
  "alignment": "left"
},
"id": {
  "required": "True",
  "padding": "-",
  "start_pos": 1,
  "end_pos": 8,
  "type": "string",
  "alignment": "left"
},
"sensorChannel": {
  "required": "True",
  "padding": "-",
  "start_pos": 9,
  "end_pos": 10,
  "type": "string",
  "alignment": "left"
},
"analyzerId": {
  "required": "True",
```



GLens Central Server Software Open API

July 3, 2015

```
        "padding": "-",
        "start_pos": 101,
        "end_pos": 115,
        "type": "string",
        "alignment": "left"
    }
},
"AcquisitionSystemDetails": {
    "AcquisitionVersion": <Version Number>,
    "AcquisitionSystem": <Acquisition System Name>
},
"SensorA": {
    "collectorType": <Monitoring Type>,
    "monitoringType": <Monitoring Type>,
    "monitoringId": <Monitoring Id>,
    "ChannelNo": "0",
    "GaugeMinimum": "",
    "CoefficientA": "",
    "parameterId": <parameter id>,
    "GaugeMaximum": "",
    "MeasurementUnit": <measurement unit>,
    "compPort": "",
    "parameterName": <parameter name>,
    "CoefficientB": "",
    "analyzerId": <analyzer id>
    "customparameters" :{}
},
.
.
.

"SensorN": {
    "monitoringType": <Monitoring Type>,
    "monitoringId": <Monitoring Id>,
    "ChannelNo": "0",
    "GaugeMinimum": "",
    "CoefficientA": "1",
    "parameterId": <parameter id>,
    "GaugeMaximum": "",
    "MeasurementUnit": <measurement unit>,
    "compPort": "",
    "parameterName": <parameter name>,
    "CoefficientB": "0",
    "analyzerId": <analyzer id>,
    "customparameters" :{}
}
}
```

If the configuration request status is failed, the response will be

```
{
    "status": "Failed"
}
```



Fetch Configuration From Client

This method will be invoked by the client to upload the current configuration in the analyser to the Central Server Software when the ConfigurationUpdateFlag is set to "True"

<http://ipaddress:port/GLensServer/uploadConfig>

Path: uploadConfig

Method: POST

Parameter: The configuration of the Site in the json format

Returns: The response json contains, success in case of success or failure message in case of failure.

Request body:

```
{
  "Command": "ConfigFetch",
  "serverConfigLastUpdatedTime": <ServerConfigUpdatedLastTime>,
  "SiteDetails": {
    "siteName": <SiteName>,
    "siteLabel": <SiteLabel>,
    "siteConfigLastUpdatedTime": <SiteConfigUpdatedLastTime>,
    "siteId": <site id>,
    "monitoringId": <monitoring id>,
    "customparameters" :{}
  },
  "CollectorDetails":[ {
    "CollectorType": <>,
    "CollectorName": <>,
    "ConfiguredChannels": <>,
    "PollingStep": <polling step>,
    "ChecksumStatusBit": <checksum bit>,
    "Address": <address>,
    "HeartBeat": <heartbeat>,
    "DataFormatBits": "00",
    "Port": <port>,
    "CommunicationTimeOut": <communication bit>
    "customparameters" :{}
  }
],
  "configJson": {
    "monitoringType": {
      "required": "True",
      "padding": "-",
      "start_pos": 55,
      "end_pos": 64,
```



GLens Central Server Software Open API

July 3, 2015

```
    "type": "string",
    "alignment": "left"
  },
  "monitoringId": {
    "required": "True",
    "padding": "-",
    "start_pos": 65,
    "end_pos": 84,
    "type": "string",
    "alignment": "left"
  },
  "QualityCode": {
    "required": "True",
    "padding": "*",
    "start_pos": 42,
    "end_pos": 43,
    "type": "string",
    "alignment": "left"
  },
  "SensorTime": {
    "required": "True",
    "padding": "-",
    "start_pos": 44,
    "end_pos": 54,
    "type": "string",
    "alignment": "left"
  },
  "parameterId": {
    "required": "True",
    "padding": "-",
    "start_pos": 85,
    "end_pos": 100,
    "type": "string",
    "alignment": "left"
  },
  "parameterName": {
    "required": "True",
    "padding": "*",
    "start_pos": 11,
    "end_pos": 25,
    "type": "string",
    "alignment": "left"
  },
  "Reading": {
    "required": "True",
    "padding": "*",
    "start_pos": 26,
    "end_pos": 41,
    "type": "string",
    "alignment": "left"
  },
  "id": {
    "required": "True",
    "padding": "-",
    "start_pos": 1,
    "end_pos": 8,
```



GLens Central Server Software Open API

July 3, 2015

```
    "type": "string",
    "alignment": "left"
  },
  "sensorChannel": {
    "required": "True",
    "padding": "-",
    "start_pos": 9,
    "end_pos": 10,
    "type": "string",
    "alignment": "left"
  },
  "analyzerId": {
    "required": "True",
    "padding": "-",
    "start_pos": 101,
    "end_pos": 115,
    "type": "string",
    "alignment": "left"
  }
},
"AcquisitionSystemDetails": {
  "AcquisitionVersion": <Version Number>,
  "AcquisitionSystem": <Acquisition System Name>
},
"SensorA": {
  "collectorType": <Monitoring Type>,
  "monitoringType": <Monitoring Type>,
  "monitoringId": <Monitoring Id>,
  "ChannelNo": "0",
  "GaugeMinimum": "",
  "CoefficientA": "",
  "parameterId": <parameter id>,
  "GaugeMaximum": "",
  "MeasurementUnit": <measurement unit>,
  "compPort": "",
  "parameterName": <parameter name>,
  "CoefficientB": "",
  "analyzerId": <analyzer id>
  "customparameters" :{}
},
.
.
.

"SensorN": {
  "monitoringType": <Monitoring Type>,
  "monitoringId": <Monitoring Id>,
  "ChannelNo": "0",
  "GaugeMinimum": "",
  "CoefficientA": "1",
  "parameterId": <parameter id>,
  "GaugeMaximum": "",
  "MeasurementUnit": <measurement unit>,
  "compPort": "",
  "parameterName": <parameter name>,
```



GLens Central Server Software Open API

July 3, 2015

```
"CoefficientB": "0",  
"analyzerId": <analyzer id>,  
"customparameters" :{}  
}  
}
```

Response for the Request will be

Success status

```
{  
  "status": "Success",  
  "configUpdateStatus": "Received Site configuration successfully"  
}
```

Failure status

```
{  
  "status": "Failed",  
  "configUpdateStatus": "Failed to receive Site Configuration. Please  
retry"  
}
```

Configuration Update Acknowledgement

Whenever the site client software has received the configuration from the Central Server Software and successfully update the site configuration, the client software should provide acknowledgement to the Central Server to ensure that server doesn't request for configuration update again.

This method gives the status of calibration.

<http://ipaddress:port/GLensServer/completedConfig>

Path: completedConfig

Method: POST

Parameter: The site id and monitoring id will be passed as the parameter.

Returns: The response json contains, success in case of success or failure message in case of failure.

Request body:

```
{
```



GLens Central Server Software Open API

July 3, 2015

```
"siteId": <site-id>,  
"monitoringid": <monitor-id>,  
"ConfigUpdated": "True"  
}
```

Response to Configuration acknowledgement received by client software

Success Response

```
{  
  "status": "Success",  
  "calibrationUpdateStatus": "Server and Site Configuration Synchronized"  
}
```

Failure response

```
{  
  "status": "Failed",  
  "calibrationUpdateStatus": "Failed to update Configuration status"  
}
```

Remote Calibration Service

This method download the configuration required for calibration.

<http://ipaddress:port/GLensServer/getCalibrationConfig>

Path: **getCalibrationConfig**

Method: **POST**

Parameter: The site id, monitoring id, CalibrationType will be passed as the parameter. CalibrationType will be "scheduled" when a schedule is submitted to client or "immediate" if an immediate request for calibration is required.

Returns: The response json contains the configuration required for calibration

Request body:

```
{  
  "siteId": <site-id>,  
  "monitoringid": <monitor-id>,  
  "CalibrationType": "Scheduled" or "Immediate"  
}
```

Response provided by the Server will have the following fields. If any analyser maker needs any additional fields for performing, remote calibration, this can be discussed with glens team at glens@knowledgelens.com and can use "customparameters" tag in the json



GLens Central Server Software Open API

July 3, 2015

The configuration details has the sequence for calibrations, the required parameters for calibrations and the schedule for the calibrations.

RESPONSE

```
{
  "status": "Success",
  "calibration": {
    "calibratorName": <calibrator-name>,
    "sequence": [
      {
        "function": <function name>,
        "duration_secs": <duration in seconds>,
        "gas": <gas>,
        "value": "0",
        "delay": <delay in minutes>,
        "sequenceName": <sequence name>,
        "duration": <duration in minute>,
        "type": <type of calibration>,
        "unit": <unit of gas>
      } .....
    ],
    "siteName": <site name>,
    "monitoringType": <monitoring type>,
    "frequency": <frequency>,
    "analyzerId": <analyser id>,
    "parameterId": <parameter id>,
    "remoteCalibrationId": <remote calibration id>,
    "parameterName": "SO2",
    "cycleUnit": "1",
    "total_duration": <total duration>,
    "frequencyDay": <day>,
    "siteId": <site id>,
    "startTime": {
      "date": <date>,
      "time": <time>
    },
    "executeImmediate": "True",
    "day": <day>,
    "cycle": <cycle>,
    "frequencyTime": <frequency time>,
    "calibratorId": <calibration id>,
    "monitoringUnit": <monitoring unit>,
    "value": "",
    "channelNumber": <channel number>,
    "analyzerType": <analyser type>,
    "endTime": {
      "date": <date>,
      "time": <time>
    },
    "remoteCalibrationName": <remote calibration name>,
    "analyzerName": <analyser name>
  },
}
```



GLens Central Server Software Open API

July 3, 2015

```
"serverCalibrationLastUpdatedTime": <serverCalibrationLastUpdatedTime>,
"siteCalibrationLastUpdatedTime": <siteCalibrationLastUpdatedTime>,
"lastCalibratedOn": <lastCalibratedOn>,
"siteId": <siteid>
}
```

Failure

```
{
  "status": "Failed. Calibration configuration not available"
}
```

Calibration Update Acknowledgement

Whenever the site client software has received the calibration sequence and has scheduled the calibration on the analyser, the calibration acknowledgement has to be provided to Glens server to ensure that server doesn't request for calibration configuration again.

This method gives the status of calibration.

<http://ipaddress:port/GLensServer/updateCalibrationConfig>

Path: **updateCalibrationConfig**

Method: **POST**

Parameter: The site id and monitoring id will be passed as the parameter.

Returns: The response json contains, success in case of success or failure message in case of failure.

Request body:

```
{
  "siteId": <site-id>,
  "monitoringid": <monitor-id>,
  "CalibrationType": "Scheduled" or "Immediate"
}
```

Response to Calibration Update Received by Client Software

Success Response

```
{
  "status": "Success",
  "calibrationUpdateStatus": "Server and Site Calibration Synchronized"
```



```
}
```

Failure response

```
{
  "status": "Failed",
  "calibrationUpdateStatus": "Failed to update calibration configuration
status"
}
```

Fetch Diagnostic Information From Client

This method will be invoked by the client to upload the current diagnostic information in the analyser to the Central Server Software when the DiagnosticUpdateFlag is set to "True"

<http://ipaddress:port/GLensServer/uploadDiagnosticsInfo>

Path: uploadDiagnosticInfo

Method: POST

Parameter: The diagnostic information of the Site in the json format

Returns: The response json contains, success in case of success or failure message in case of failure. The diagnostics json will be an array of key value pair with the corresponding category associated to the key.

Request body:

```
{
  "Command": "DiagnosticFetch",
  "SiteDetails": {
    "siteName": <SiteName>,
    "siteLabel": <SiteLabel>,
    "siteConfigLastUpdatedTime": <SiteConfigUpdatedLastTime>,
    "siteId": <site id>,
    "monitoringId": <monitoring id>,
    "customparameters" :{}
  },
  "CollectorDetails": [ {
    "CollectorType": <>,
    "CollectorName": <>,
    "ConfiguredChannels": <>,
    "PollingStep": <polling step>,
    "ChecksumStatusBit": <checksum bit>,
    "Address": <address>,
    "HeartBeat": <heartbeat>,
    "DataFormatBits": "00",
    "Port": <port>,
    "CommunicationTimeOut": <communication bit>
  }
}
```



Glens Central Server Software Open API

July 3, 2015

```
    "customparameters" :{}  
  }],  
  "diagnosticJson": [{"analyserId":<analyser-id>,"parameterName":"","  
diagnostics":[{"key":<key>, "value":<value>,"category":<category>}]}]  
}
```

Response for the Request will be

Success status

```
{  
  "status": "Success",  
  "diagnosticUpdateStatus": "Received Site diagnostics successfully"  
}
```

Failure status

```
{  
  "status": "Failed",  
  "diagnosticUpdateStatus": "Failed to receive Site diagnostics. Please  
retry"  
}
```

Contacts

Glens provides clients for various analysers which meets these requirements. Glens software team can assist any industry or analyser supplier to enable them to comply with this common format. For any queries please send the request to glens@knowledgelens.com or call at +91 9916025302

Client Side Software Requirement

1. The data collection and transmission module should directly connect to the installed analyser and fetch the data directly from the analyser **without any intermediary software or conversions**. The software should have no editing provision for altering/correcting the data at the industry side.
2. No data shall be accepted as an output from OPC of Server or DCS or any other intermediate software at Industry side.
3. The data collection and transmission module should encrypt the data with unique client specific encryption key to ensure authentic data transfer from the industry to the central server. Only encrypted and authenticated data shall be received by the Central Server Module.
4. During internet connectivity failure or a communication issue with the central server, the data collection and transmission module should store the encrypted data locally and retransmit when the transmission can be restored. Any such delayed transmission should be identifiable at the regulator side using data quality codes.
5. The data collection and transmission module should wait for acknowledgement from the server and should retransmit the data if no acknowledgement is received within the timeout period.
6. The data collection and transmission module should support remote analyser configuration. The data collection and transmission module should accept remote analyser configuration commands and update the analyser configurations with the set value.
7. Each measurement should be associated with the data quality code inferred while data collection and the data quality code should be

transmitted along with the data. The data quality code should indicate analyser failures, analyser communication failures etc. The data format should comply to ISO-7168 format.

8. Software should support reading analyser configuration and report the configuration changes to the central server. Any configuration changes done at the site should have audit trail and reported to the regulator for approval in the form of workflow.
9. The data collection and transmission module should accept commands for calibration (auto and manual) and able to perform calibration of the analyser locally.
10. The data collection and transmission module should be able to collect the data directly from the analyser with a minimum scan interval of 10 seconds.
11. Data collection and transmission shall be minimum 15 min or other mean average period selectable by user.
12. The data collection and acquisition software should be able to collect and encrypt the data locally on the industry site. The data should archive the data locally on the client machine for a period of 1 year.
13. The data collection and transmission module should communicate the status periodically to the central server even when no analyser is connected or when analyser is faulty with appropriate data quality code.
14. The data collection and transmission module should auto-restart on failure or machine reboots.
15. The data collection and transmission module should be able to transmit the data over Broadband/LAN/wifi/gprs/gsm etc.

16. The data collection and transmission module should support any analyser, make and model based on the configuration and protocol specific extensions. (**analyser suppliers should be open enough to share their analyser output protocol for easy data transmission digitally**)
17. The data collection and transmission module should be customizable to support any specific protocol required.