TRUSTGATE
SECURE TRANSACTION. TRUSTED BUSINESS

Interface Control Document

Project Name:	Andas PKI		
Date:	19-Jan-2026	**Release:**	~~Draft~~/Final
Author/Prepared by:	Fadzil bin Mohd Raihan 19/01/26		
Reviewed and Approved by:	Amir Faiz Husin 19/01/26		
Client:	Andas Capital Sdn. Bhd.		
Document Number:	1.0		

Note: This document is only valid on final version.

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
19-01-2026	N/A	Final version release	1.0

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version
Dr. Ivan Chew	Andas Capital Sdn. Bhd	19-01-2026	1.0
Amir Faiz Husin	Project Manager, MSC Trustgate	19-01-2026	1.0

Table of Contents

1. Introduction

1.1. Purpose

This Interface Control Document (ICD) is to describe the requirements and interface between the client software/system and MyTrustSigner API via MyTrustSigner Agent (web services).

1.2. Scope

This document becomes applicable in the development and integration phase of MyTrustSigner API with the client software/system. The API's scope is to interact with client systems which will utilize Trustgate's PKI system, via a roaming infrastructure.

1.3. MyTrustSigner API Overview

The following diagram depicts the MyTrustSigner API components and integration with Project's Business Application.

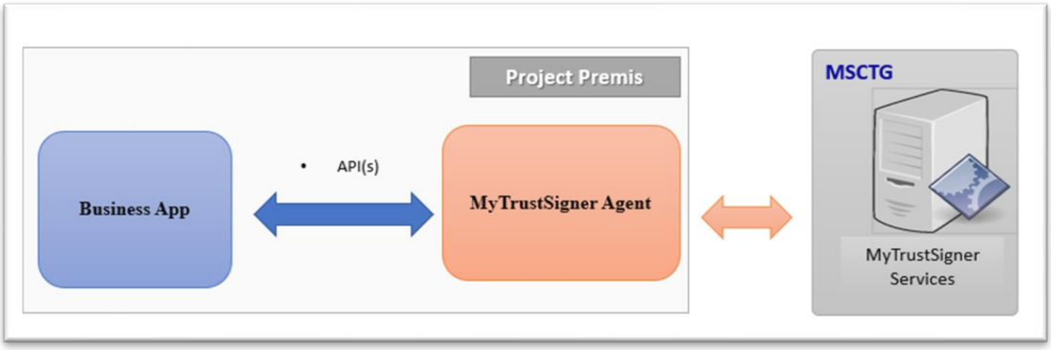


Figure 1: MyTrustSigner API Overview

1.4. Requirements

In order to utilize the MyTrustSigner API, the following requirements are required:

i. Users with valid Malaysian citizenship identification card (MyKad) or valid Passport

ii. MyTrustSigner Agent has been successfully deployed and configured

iii. The MyTrustSigner Agent is using SOAP technology, therefore, client software shall call the MyTrustSigner Agent API via SOAP web service client

iv. Each web service call shall have the following header information:
   - Username
   - Password

v. MyTrustSigner Agent has been successfully deployed and configured

vi. For internal users, it is MANDATORY to submit a user list with the following details:

   1. Full Name (as per MyKad/Passport)
   2. MyKad No. / Passport No.
   3. Email Address
   4. Phone Number

   This list be used during request certificate process. It is also required to restrict and control the number of officers to authorized and approve the application.

2. Interface Definitions

This section describes the following API function(s) :

- Via MyTrustSigner Agent (webservice API):
    1. RequestCertificate
    2. GetCertInfo
    3. SignPDF
    4. VerifyPDFSignature
    5. RequestRevokeCert
    6. UpdateEmailAddress
    7. RequestEmailOTP
    8. VerifyCertPin
    9. ResetCertificatePin

2.1. RequestCertificate

This API function is used when a client software request to enrol a roaming digital certificate via MyTrustSigner Agent.

Function/Method Name:	RequestCertificate
Description	To request for a roaming digital certificate
URL:	*Please refer to Section 3.1 MyTrustSigner API*
Supported Request Formats:	Application/xml

Input Parameters:

Field Name	Type (Length)	M/O	Remarks
UserID	String(12)	M	12 digit Malaysian NRIC (without dash symbol) or Passport Number *Example: 770908012232*
FullName	String(100)	M	User's full name as per MyKad or Passport
EmailAddress	String (50)	M	User's email address
MobileNo	String(15)	M	User's mobile phone number
Nationality	String(2)	M	User's nationality - Two letter country code. Default is "MY"
UserType	String(1)	M	User type **Valid value:** 1 - for External users, example: Borrower 2 - for Internal users, example: Authorised Signatory or Attestator
AuthFactor	String(6) for Email/SMS OTP String(8) for PIN	M	Authentication method set as the following: For UserType 1 (External) : Email OTP For UserType 2 (Internal) : PIN
IDType	String(1)	M	User identity type **Valid value:** N - for Malaysian NRIC P - for Passport
NRICFront	String	M/O	Mandatory if IDType=N MyKad front coloured image (format jpeg or png) file in base64 string format
NRICBack	String	M/O	Mandatory if IDType=N MyKad back coloured image (format jpeg or png) file in base64 string format
PassportImage	String	M/O	Mandatory if IDType=P

			Passport coloured image (format jpeg or png) file in base64 string format
SelfieImage	String	M	Selfie image file in base64 string format
OrganisationInfo	Object	M/O	Object containing details of user's organisation For UserType 1: Optional For UserType 2: Mandatory
VerificationData	Object	M/O	Object containing details of Verification Data For UserType 1 (External) : Optional For UserType 2 (Internal) : Mandatory

Note: M/O: Mandatory/Optional

VerificationData object:

Please refer to Section 5.0 Verification Data Information

Field Name	Type(Length)	Remarks
verifyStatus	String(100)	The outcome or result of a verification process, confirming and establishing a linkage between the claimed identity and the real-life existence of the applicant presenting the government-issued photo ID as evidence.
verifyDatetime	String	Date and time when applicant's identity is verified during the certificate application process. **Valid format:** yyyy-MM-dd HH:mm:ss *Example: 2024-05-19 11:01:12*
verifyVerifier	String(100)	The individual, entity, or machine responsible for conducting the verification process
verifyMethod	String(100)	Refer to the method used by the AP to confirm the identity of the applicant. It can be, and is not limited one of the following: a. Manual face-to-face verification b. Manual face-to-face verification with biometric c. Secure automated self-service verification with biometric d. e-KYC (face recognition with liveness detection) as per Bank Negara Malaysia (BNM) Electronic Know-Your-Customer (e-KYC)

OrganisationDetails:

Field Name	Type	M/O	Remarks
orgName	String	M	Name of the organisation
orgUserDesignation	String	M	User's designation in the organisation. May contain the following information: • User's organizational role/title in the organisation, example: Director • User's a regulated professional designation, example: Doctor
orgUserRegistrationNo	String	M	May contain the following information: • User's registration number of a regulated professional organization • User's organizational staff/employee ID • User's ID number
orgUserRegistrationType	String	M	Mandatory if ***orgUserRegistrationNo*** is specified. Valid value: • PAS - For an identifier based on a passport number. • IDC - For an identifier based on a national identity card (MyKad).
orgAddress	String	M	Organisation's address
orgAddressCity	String	M	Organisation address's city
orgAddressState	String	M	Organisation address's state
orgAddressPostcode	String	M	Organisation address's postcode
orgAddressCountry	String	M	Two letter country code Default is "MY"
orgRegistationNo	String	M	Organisation's registration or identifier number
orgRegistationType	String	M	Organisation's identifier on registration number, valid value: • NTRMY – for an identifier allocated by a national or state trade register in Malaysia • IRB - for an identifier allocated by the national tax authorities (Inland Revenue Board) • RMC - for an identifier allocated by the Royal Malaysia Customs

			• CIDB - for an identifier allocated by the Construction Industry Development Board (CIDB) • BAM - for an identifier allocated by the Board of Architects Malaysia • GOV - for the Government Entities • GOVSUB - for the Government subdivision entities (state or province) level • INT - for International Organization Entities • LEI - for LEI Registration Scheme
orgPhoneNo	String	M	Organisation’s telephone number
orgFaxNo	String	O	Organisation’s fax number

Output/Return Values:

Field Name	Type	Remarks
statusCode	String	Status code of the request
statusMsg	String	Message containing information on the request status
certX509	String	Certificate in X509 format **
certValidTo	String	Certificate end date **
certValidFrom	String	Certificate start date **
certSerialNo	String	Certificate serial number **
certRequestID	String	Request ID **
certRequestStatus	String	Request status **
userID	String	User’s ID Number (MyKad or Passport)

Note:

** If request is unsuccessful: Null (Empty)

Status Code

Please refer to Section 3.2 Status Code Definitions

Request Payload (XML)

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mtsa="http://mtsa.msctg.com/">
   <soapenv:Header/>
   <soapenv:Body>
      <mtsa:RequestCertificate>
         <UserID></UserID>
         <FullName></FullName>
         <EmailAddress></EmailAddress>
         <MobileNo></MobileNo>
         <Nationality></Nationality>
         <UserType></UserType>
         <IDType></IDType>
         <AuthFactor></AuthFactor>
         <NRICFront></NRICFront>
         <NRICBack></NRICBack>
         <SelfieImage></SelfieImage>
         <PassportImage></PassportImage>
         <OrganisationInfo>
            <orgAddress></orgAddress>
            <orgAddressCity></orgAddressCity>
```

```
        <orgAddressCountry></orgAddressCountry>
        <orgAddressPostcode></orgAddressPostcode>
        <orgAddressState></orgAddressState>
        <orgFaxNo></orgFaxNo>
        <orgName></orgName>
        <orgPhoneNo></orgPhoneNo>
        <orgRegistationNo></orgRegistationNo>
        <orgRegistationType></orgRegistationType>
        <orgUserDesignation></orgUserDesignation>
        <orgUserRegistrationNo></orgUserRegistrationNo>
        <orgUserRegistrationType></orgUserRegistrationType>
      </OrganisationInfo>
      <VerificationData>
        <verifyDatetime></verifyDatetime>
        <verifyMethod></verifyMethod>
        <verifyStatus></verifyStatus>
        <verifyVerifier></verifyVerifier>
      </VerificationData>
    </mtsa:RequestCertificate>
  </soapenv:Body>
</soapenv:Envelope>
```

2.2. GetCertInfo

This API function is used when a client software request to check digital certificate information via MyTrustSigner Agent.

<table>
<tr><td>Function/Method Name:</td><td>GetCertInfo</td></tr>
<tr><td>Description</td><td>Request to get details of a digital certificate</td></tr>
<tr><td>URL:</td><td><i>Please refer to Section 3.1 MyTrustSigner API</i></td></tr>
<tr><td>Supported Request Formats:</td><td>Application/xml</td></tr>
<tr><td>Input Parameters:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>M/O</th><th>Remarks</th></tr>
<tr><td>UserID</td><td>String</td><td>M</td><td>Malaysian NRIC or Passport Number
Example: 770908012232</td></tr>
</table>
Note: M/O: Mandatory/Optional
</td></tr>
</table>

<table>
<tr><td>Output/Return Values:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>Remarks</th></tr>
<tr><td>certStatus</td><td>String</td><td>Status of the certificates
Example: Expired, Revoked, Valid</td></tr>
<tr><td>certValidTo</td><td>String</td><td>Certificate end date
Example: 2020-08-29 07:59:59</td></tr>
<tr><td>certValidFrom</td><td>String</td><td>Certificate start date
Example: 2020-07-01 08:00:00</td></tr>
<tr><td>statusCode</td><td>String</td><td>Status code of the request</td></tr>
<tr><td>statusMsg</td><td>String</td><td>Status message of the request</td></tr>
<tr><td>certX509</td><td>String</td><td>Certificate in base64 String format</td></tr>
<tr><td>certIssuer</td><td>String</td><td>Certificate issuer info</td></tr>
<tr><td>certSubjectDN</td><td>String</td><td>Certificate subject info</td></tr>
<tr><td>certSerialNo</td><td>String</td><td>Certificate serial number</td></tr>
</table>
</td></tr>
<tr><td>Status Code</td><td><i>Please refer to Section 3.2 Status Code Definitions</i></td></tr>
</table>

Request Payload (XML)	*<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:mtsa="http://mtsa.msctg.com/">* *<soapenv:Header/>* *<soapenv:Body>* *<mtsa:GetCertInfo>* *<UserID></UserID>* *</mtsa:GetCertInfo>* *</soapenv:Body>* *</soapenv:Envelope>*

2.3. SignPDF

This API function is used when a client software request to Sign a PDF file via MyTrustSigner Agent. If specified, the request will fill in data into specified PDF form field(s).

Function/Method Name:	SignPDF
Description	To sign a PDF file
URL:	*Please refer to Section 3.1 MyTrustSigner API*
Supported Request Formats:	Application/xml
Input Parameters:	

Field Name	Type(length)	M/O	Remarks
UserID	String(12)	M	Malaysian NRIC or Passport Number *Example: 770908012232*
FullName	String(100)	M	Full name as per MyKad or Passport *Example:* *Mohd Hariz bin Marzuki*
FieldListToUpdate	List<PdfFieldNameValue>	M	List of object containing details of pdf form fields and value to be updated during digital signing.
SignatureInfo	SignatureDetails	M	Object containing details of a signature
AuthFactor	String(6) for Email OTP String(8) for PIN	M	Authentication method set as the following: UserType 1: Email OTP UserType 2: PIN

SignatureDetails object:

Field Nme	Type	M/O	Remarks
visibility	Boolean	M	Visibility of the signature in pdf Valid value: • true • false
x1	Integer	M/O	Location of signature in pdf – Mandatory if Visibility is true *Please refer to Section 3.4 Signature Location*
y1	Integer	M/O	Location of signature in pdf – Mandatory if Visibility is true *Please refer to Section 3.4 Signature Location*
x2	Integer	M/O	Location of signature in pdf – Mandatory if Visibility is true *Please refer to Section 3.4 Signature Location*
y2	Integer	M/O	Location of signature in pdf – Mandatory if Visibility is true *Please refer to Section 3.4 Signature Location*
pageNo	Integer	M/O	Page of the signature will be located in pdf – Mandatory if Visibility is true
pdfInBase64	String	M	PDF document (in Base64)
sigImageInBase64	String	O	Signature image to represent the digital signature
additionalInfo1	String	O	Additional information #1 to be displayed in the Digital Signature text *Example: IP Address or User Designation*
additionalInfo2	String	O	Additional information #2 to be displayed in the Digital Signature text *Example: Department Name*

PdfFieldNameValue object:

<table>
<tr><th>Field Name</th><th>Type</th><th>M/O</th><th>Remarks</th></tr>
<tr><td>PdfFieldName</td><td>String</td><td>M</td><td>PDF form field name</td></tr>
<tr><td>FieldValue</td><td>String</td><td>M</td><td>Any value for the form field

Note: The following template can be used to auto fill the form field:

<ul><li>CURR_DATE,F=<FORMAT>,D=<DELIMITER&gt;</li></ul>
Auto fill with current date in specified <FORMAT> and <DELIMITER>
Valid <FORMAT>
<ul><li>DDMMMMMYYYY</li><li>DDMMMYYYY</li><li>DDMMYYYY</li><li>YYYYMMMMMDD</li><li>YYYYMMMDD</li><li>YYYYMMDD</li></ul>
Valid <DELIMITER>
<ul><li>SPACE</li><li>FSLASH</li><li>DASH</li></ul>
Examples: Date 12/03/2021
<table>
<tr><th>FIELD VALUE TEMPLATE with FORMAT & DELIMITER</th><th>EXAMPLE OUTPUT</th></tr>
<tr><td>CURR_DATE,F=DDMMMMMYYYY,D=SPACE</td><td>21 MARCH 2021</td></tr>
<tr><td>CURR_DATE,F=DDMMMYYYY,D=FLASH</td><td>21/MAR/2021</td></tr>
<tr><td>CURR_DATE,F=DDMMYY,D=DASH</td><td>21-03-2021</td></tr>
<tr><td>CURR_DATE,F=YYYYMMMMMDD,D=SPACE</td><td>2021 MARCH 21</td></tr>
<tr><td>CURR_DATE,F=YYYYMMMDD,D=DASH</td><td>2021-MAR-21</td></tr>
<tr><td>CURR_DATE,F=YYYYMMDD,D=FLASH</td><td>2021/03/21</td></tr>
</table>
<ul><li>SIGNER_FULLNAME
Auto fill with signer’s full name</li><li>SIGNER_ID
Auto fill with signer’s User ID (NRIC or Passport No)</li></ul>
</td></tr>
</table>

Note: M/O : Mandatory/Optional

Output/Return Values:

Field Name	Type	Remarks
statusCode	String	Status code of the request
statusMsg	String	Message containing information on the request status
signedPdfInBase64	String	Signed pdf in Base64 string
userCert	String	Signer’s certificate in X509 format

Status Code	*Please refer to Section 3.2 Status Code Definitions*

Request Payload (XML)

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mtsa="http://mtsa.msctg.com/">
  <soapenv:Header/>
  <soapenv:Body>
    <mtsa:SignPDF>
      <UserID></UserID>
      <FullName></FullName>
      <AuthFactor></AuthFactor>
      <SignatureInfo>
        <pageNo></pageNo>
        <pdfInBase64></pdfInBase64>
        <sigImageInBase64></sigImageInBase64>
        <visibility></visibility>
        <visibleOnEveryPages></visibleOnEveryPages>
        <x1></x1>
        <x2></x2>
        <y1></y1>
        <y2></y2>
        <additionalInfo1></additionalInfo1>
        <additionalInfo2></additionalInfo2>
      </SignatureInfo>
      <!--Zero or more repetitions:-->
      <FieldListToUpdate>
        <pdfFieldName></pdfFieldName>
        <pdfFieldValue></pdfFieldValue>
      </FieldListToUpdate>
    </mtsa:SignPDF>
  </soapenv:Body>
</soapenv:Envelope>
```

2.4. VerifyPDFSignature

This API function is used when a client software request to verify digital signature in a signed PDF document via MyTrustSigner Agent.

Function/Method Name:	VerifyPDFSignature
Description	To verify digital signature in a signed PDF document
URL:	*Please refer to Section 3.1 MyTrustSigner API*
Supported Request Formats:	Application/xml
Input Parameters:	

Field Name	Type	M/O	Remarks
SignedPdfInBase64	String	M	Digitally signed PDF document (in Base64)

Note: M/O: Mandatory/Optional

Output/Return Values:

Field Name	Type	Remarks
statusCode	String	Status code of the request
statusMsg	String	Message containing information on the request status
totalSignatureInPdf	Integer	Total number of digital signature exists in a signed PDF document
pdfSignatureList	List <PdfSignatureData>	Object containing details of digital signature validity

PdfSignatureData object:

Field Name	Type	Remarks
sigCoverWholeDocument	Boolean	Status if digital signature covers the whole document
sigName	String	Digital signature's name in PDF
sigRevisionNo	String	Digital signature's revision info
sigSignerCert	String	Signer's certificate in X509 format
sigSignerCertIssuer	String	Signer's certificate issuer info
sigSignerCertStatus	String	Signer's certificate status
sigSignerCertSubject	String	Signer's certificate subject info

<table>
<tr><td></td><td><table>
<tr><td>sigStatusValid</td><td>Boolean</td><td>Digital signature’s validity status.
Value: true or false</td></tr>
<tr><td>sigTimeStamp</td><td>String</td><td>Digital signature’s timestamp info
Example:
2020-06-22 15:39:37.00</td></tr>
</table></td></tr>
<tr><td>Status Code</td><td><i>Please refer to Section 3.2 Status Code Definitions</i></td></tr>
<tr><td>Request Payload (XML)</td><td><i><soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:mtsa="http://mtsa.msctg.com/">
  <soapenv:Header/>
  <soapenv:Body>
    <mtsa:VerifyPDFSignature>
      <SignedPdfInBase64></SignedPdfInBase64>
    </mtsa:VerifyPDFSignature>
  </soapenv:Body>
</soapenv:Envelope></i></td></tr>
</table>

2.5. RequestRevokeCert

This API function is used when a client software request to revoke a digital certificate via MyTrustSigner Agent.

Function/Method Name:	RequestRevokeCert
Description	Request to revoke a digital certificate
URL:	*Please refer to Section 3.1 MyTrustSigner API*
Supported Request Formats:	Application/xml
Input Parameters:	

Field Name	Type(length)	M/O	Remarks
UserID	String(12)	M	Malaysian NRIC or Passport Number Example: 770908012232
CertSerialNo	String(50)	M	Certificate serial number
RevokeReason	String(100)	M	Reason for certificate revocation. **Valid values:** • keyCompromise • CACompromise • affiliationChanged • superseded • cessationOfOperation *Please refer to Section 3.9 Revocation Definitions*
RevokeBy	String	M	Revocation requested by either admin or user: **Valid values:** Admin – Admin request for revocation Self – User request for revocation
AuthFactor	String(6) for SMS/EMAIL OTP String(8) for PIN	M	Authentication method set as the following: UserType 1: EMAIL OTP UserType 2: PIN
IDType	String(1)	M	User identity type **Valid value:** N - for Malaysian NRIC P - for Passport
NRICFront	String	M/O	Mandatory if IDType=N MyKad front coloured image (format jpeg or png) file in base64 string format

NRICBack	String	M/O	Mandatory if IDType=N MyKad back coloured image (format jpeg or png) file in base64 string format
PassportImage	String	M/O	Mandatory if IDType=P Passport coloured image (format jpeg or png) file in base64 string format
VerificationData	Object	M	Object containing details of Verification Data

Note: M/O: Mandatory/Optional

VerificationData object:

Please refer to Section 5.0 Verification Data Information

Field Name	Type	Remarks
verifyStatus	String(100)	The outcome or result of a verification process, confirming and establishing a linkage between the claimed identity and the real-life existence of the applicant presenting the government-issued photo ID as evidence.
verifyDatetime	String	Date and time when applicant's identity is verified during the certificate application process. **Valid format:** yyyy-MM-dd HH:mm:ss *Example: 2024-05-19 11:01:12*
verifyVerifier	String(100)	The individual, entity, or machine responsible for conducting the verification process
verifyMethod	String(100)	Refer to the method used by the AP to confirm the identity of the applicant. It can be, and is not limited one of the following: a. Manual face-to-face verification b. Manual face-to-face verification with biometric c. Secure automated self-service verification with biometric d. e-KYC (face recognition with liveness detection) as per Bank Negara Malaysia (BNM) Electronic Know-Your-Customer (e-KYC)

<table>
<tr><td>Output/Return Values:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>Remarks</th></tr>
<tr><td>statusCode</td><td>String</td><td>Status code of the request</td></tr>
<tr><td>statusMsg</td><td>String</td><td>Status message of the request</td></tr>
</table>
</td></tr>
<tr><td>Status Code</td><td><em>Please refer to Section 3.2 Status Code Definitions</em></td></tr>
<tr><td>Request Payload (XML)</td><td><pre>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mtsa="http://mtsa.msctg.com/">
  <soapenv:Header/>
  <soapenv:Body>
    <mtsa:RequestRevokeCert>
      <UserID></UserID>
      <CertSerialNo></CertSerialNo>
      <RevokeReason></RevokeReason>
      <RevokeBy></RevokeBy>
      <IDType></IDType>
      <AuthFactor></AuthFactor>
      <NRICFront></NRICFront>
      <NRICBack></NRICBack>
      <PassportImage></PassportImage>
      <VerificationData>
        <verifyDatetime></verifyDatetime>
        <verifyMethod></verifyMethod>
        <verifyStatus></verifyStatus>
        <verifyVerifier></verifyVerifier>
      </VerificationData>
    </mtsa:RequestRevokeCert>
  </soapenv:Body>
</soapenv:Envelope>
</pre></td></tr>
</table>

2.6. RequestEmailOTP

This API function is used when a client software request to generate One Time Password (Email OTP) via MyTrustSigner Agent.

<table>
<tr><td>Function/Method Name:</td><td>RequestEmailOTP</td></tr>
<tr><td>Description</td><td>Request to generate One Time Password (Email OTP)</td></tr>
<tr><td>URL:</td><td><i>Please refer to Section 3.1 Web Services URL</i></td></tr>
<tr><td>Supported Request Formats:</td><td>Application/xml</td></tr>
<tr><td>Input Parameters:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>M/O</th><th>Remarks</th></tr>
<tr><td>UserID</td><td>String</td><td>M</td><td>Malaysian NRIC Number
Example: 770908012232</td></tr>
<tr><td>OTPUsage</td><td>String</td><td>M</td><td>Usage of the EMAIL OTP
<b><u>Valid value:</u></b>
DS – for digital signing
NU – for the following functions:
• RequestCertificate
• UpdateEmailAddress
• RequestRevokeCert</td></tr>
<tr><td>EmailAddress</td><td>String</td><td>M/O</td><td>User’s email address
Mandatory if Email OTP is requested for Enrolment and Email Address Update process</td></tr>
</table>
Note: M/O : Mandatory/Optional
</td></tr>
</table>

<table>
<tr><td>Output/Return Values:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>Remarks</th></tr>
<tr><td>statusCode</td><td>String</td><td>Status code of the request</td></tr>
<tr><td>statusMsg</td><td>String</td><td>Message containing information on the request status</td></tr>
</table>
</td></tr>
<tr><td>Status Code</td><td><i>Please refer to Section 3.2 Status Code Definitions</i></td></tr>
</table>

Request Payload (XML)	*<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:mtsa="http://mtsa.msctg.com/">* *<soapenv:Header/>* *<soapenv:Body>* *<mtsa:RequestEmailOTP>* *<UserID></UserID>* *<EmailAddress></EmailAddress>* *<OTPUsage></OTPUsage>* *</mtsa:RequestEmailOTP>* *</soapenv:Body>* *</soapenv:Envelope>*

2.7. UpdateEmailAddress

This API function is used when a client software request to update user’s email address via MyTrustSigner Agent.

<table>
<tr><td>Function/Method Name:</td><td>UpdateEmailAddress</td></tr>
<tr><td>Description</td><td>Request to update user’s email address</td></tr>
<tr><td>URL:</td><td><i>Please refer to Section 3.1 Web Services URL</i></td></tr>
<tr><td>Supported Request Formats:</td><td>Application/xml</td></tr>
<tr><td>Input Parameters:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>M/O</th><th>Remarks</th></tr>
<tr><td>UserID</td><td>String</td><td>M</td><td>Malaysian NRIC Number
Example: 770908012232</td></tr>
<tr><td>NewEmailAddress</td><td>String</td><td>M</td><td>New email address</td></tr>
<tr><td>EmailOTP</td><td>String</td><td>M</td><td>Email OTP received by user</td></tr>
</table>
Note: M/O : Mandatory/Optional
</td></tr>
</table>

<table>
<tr><td>Output/Return Values:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>Remarks</th></tr>
<tr><td>statusCode</td><td>String</td><td>Status code of the request</td></tr>
<tr><td>statusMsg</td><td>String</td><td>Message containing information on the request status</td></tr>
</table>
</td></tr>
<tr><td>Status Code</td><td><i>Please refer to Section 3.2 Status Code Definitions</i></td></tr>
<tr><td>Request Payload (XML)</td><td><i>&lt;soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:mtsa="http://mtsa.msctg.com/">
<soapenv:Header/>
<soapenv:Body>
<mtsa:UpdateEmailAddress>
<UserID></UserID>
<NewEmailAddress></NewEmailAddress&gt;</i></td></tr>
</table>

	<EmailOTP></EmailOTP> *</mtsa:UpdateEmailAddress>* *</soapenv:Body>* *</soapenv:Envelope>*

2.8. VerifyCertPin

This API function is used when a client software request to verify a digital certificate's PIN via MyTrustSigner Agent.

Function/Method Name:	VerifyCertPin
Description	Request to verify a digital certificate's PIN
URL:	*Please refer to Section 3.1 MyTrustSigner API*
Supported Request Formats:	Application/xml
Input Parameters:	

Field Name	Type (Length)	M/O	Remarks
UserID	String(12)	M	Malaysian NRIC or Passport Number Example: 770908012232
CertSerialNo	String(50)	M	Certificate Serial No
CertPin	String (8)	M	Certificate PIN

Note: M/O: Mandatory/Optional

Output/Return Values:	

Field Name	Type	Remarks
statusCode	String	Status code of the request
statusMsg	String	Status message of the request
certStatus	String	Certificate status: Valid or Invalid
certPinStatus	String	Certificate PIN status: Valid or Invalid

Status Code	*Please refer to Section 3.3 Status Code Definitions*
Request Payload (XML)	

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:mtsa="http://mtsa.msctg.com/">
  <soapenv:Header/>
  <soapenv:Body>
    <mtsa:VerifyCertPin>
      <UserID></UserID>
      <CertPin></CertPin>
```

	<CertSerialNo></CertSerialNo> </mtsa:VerifyCertPin> </soapenv:Body> </soapenv:Envelope>

2.9. ResetCertificatePin

This API function is used when a client software request to reset a digital certificate’s pin via MyTrustSigner Agent.

<table>
<tr><td>Function/Method Name:</td><td>ResetCertificatePin</td></tr>
<tr><td>Description</td><td>Request to reset a digital certificate’s pin</td></tr>
<tr><td>URL:</td><td><i>Please refer to Section 3.1 MyTrustSigner API</i></td></tr>
<tr><td>Supported Request Formats:</td><td>Application/xml</td></tr>
<tr><td>Input Parameters:</td><td>
<table>
<tr><th>Field Name</th><th>Type (Length)</th><th>M/O</th><th>Remarks</th></tr>
<tr><td>UserID</td><td>String(12)</td><td>M</td><td>Malaysian NRIC or Passport Number
Example: 770908012232</td></tr>
<tr><td>CertSerialNo</td><td>String(50)</td><td>M</td><td>Certificate Serial No</td></tr>
<tr><td>NewPin</td><td>String (8)</td><td>M</td><td>New certificate PIN</td></tr>
</table>
Note: M/O: Mandatory/Optional
</td></tr>
</table>

<table>
<tr><td>Output/Return Values:</td><td>
<table>
<tr><th>Field Name</th><th>Type</th><th>Remarks</th></tr>
<tr><td>statusCode</td><td>String</td><td>Status code of the request</td></tr>
<tr><td>statusMsg</td><td>String</td><td>Status message of the request</td></tr>
</table>
</td></tr>
<tr><td>Status Code</td><td><i>Please refer to Section 3.3 Status Code Definitions</i></td></tr>
<tr><td>Request Payload (XML)</td><td>
<pre>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:mtsa="http://mtsa.msctg.com/">
  <soapenv:Header/>
  <soapenv:Body>
    <mtsa:ResetCertificatePin>
      <UserID></UserID>
      <CertSerialNo></CertSerialNo>
      <NewPin></NewPin>
    </mtsa:ResetCertificatePin>
  </soapenv:Body>
</soapenv:Envelope>
</pre>
</td></tr>
</table>

3. Additional Information

3.1. MyTrustSigner API

The following is MyTrustSigner API URL for Pilot and Production environment.

Note:

i. Pilot API to be used in client system development and integration.

ii. Production API to be used in UAT Phase

3.1.1. Environment URL

Environment	API URL
Pilot	<DOMAIN_PROD:PORT>/MTSAPilot/MyTrustSignerAgentWSAPv2?wsdl
Production	<DOMAIN_PROD:PORT>/MTSA/MyTrustSignerAgentWSAPv2?wsdl

3.1.2. MyTrustSigner API Credentials

Web service request shall have the following information:

Header	Value for pilot	Value for production
Username	andas_capital_pilot	andas_capital
Password	YcuLxvMMcXWPLRaW	yYmrL57aKW7ege2h

3.2. Status Code Definitions

The following describes all status code and messages returned by MyTrustSigner Agent API functions:

API	Status Code	Status Message
Common for all MyTrustSigner Agent API	WS100	Failed to initiate API
	WS101	Read config failed
	WS102	Invalid API credential
	WS103	Credential file not found
	WS104	Missing required parameters
	WS105	Failed to get Project Profile
	WS106	Failed to auto renew cert
	WS110	Username value is missing from Web Service Header
	WS111	Username is missing from Web Service Header
	WS112	Password value is missing from Web Service Header
	WS113	Password is missing from Web Service Header
	WS114	Error in processing Web Service Header
	WS115	MyTrustSigner Service returns error: <Error message>
	WS116	No permission to execute this API function
	WS117	Error in initiating API execution: <Error message>

API	Status Code	Status Message
SignPDF	000	Success
	DS002	Failed to call signPDF function
	DS100	Failed to read digital signing config
	DS101	Missing required parameter for digital signing
	DS102	Failed to read user cert
	DS103	Cert has expired
	DS104	Cert has been revoked
	DS105	Cert not found
	DS106	Failed to auto renew expired cert
	DS107	Invalid PDF form field name
	DS110	Failed to prepare hash
	DS111	Failed to process hash
	DS120	Failed to embed signature into pdf

	DS121	Failed to generate signed pdf file
	DS122	Failed create Base64 String from signed pdf file
	DS130	Failed to read cert from X509
	DS131	Failed to create external signature
	DS132	Failed to embed signature into pdf
	DS133	Certificate type is not supported
	DS134	Cannot define certificate type
	DS135	Error on getting info from Timestamping Authority Service

API	Status Code	Status Message
VerifyPDFSignature	VS100	Missing pdf path
	VS101	Invalid pdf file path
	VS102	IOException Error: <Error message>
	VS103	GeneralSecurityException Error: <Error message>
	VS104	Exceptions Error: <Error message>
	VS110	Date parse error
	VS111	No signature found in document

API	Status Code	Status Message
GetCertInfo	000	Success
	GC100	Cert not found
	GC101	Failed to read user's digital certificate
	GC102	Error while reading user's digital certificate: <Error message>
	GC103	Error while processing user's digital certificate info
	GC104	Cert has been revoked
	GC200	Get Cert detail failed

API	Status Code	Status Message
RequestCertificate	000	Success
	AP100	Certificate auto-enrolment failed
	AP101	Missing required parameter: <Parameter Name>
	AP102	Invalid parameter length: <Parameter Name>
	AP103	Invalid value for UserType. Either 1 (for External Users) or 2 (for Internal Users such as Authorised Signatory or Attestator) is valid
	AP104	Error in parameter validation: <Parameter Name>

	AP105	Invalid value for Nationality. Either MY (for Malaysian) or ZZ (for Non-Malaysian) is valid
	AP106	Invalid validator value: <Parameter Name>
	AP107	Invalid parameter format: <Parameter Name>
	AP108	Invalid image file: <Parameter Name>
	AP109	Invalid base 64 string: < Parameter Name >
	AP110	Invalid value for IDType. Either P (for Passport) or N (for Malaysian NRIC) is valid
	AP111	User already has a certificate
	AP112	Invalid AuthFactor
	AP113	AuthFactor has expired
	AP114	AuthFactor validation failed
	AP115	EKYC Error: <Error Message>
	AP120	MyTrustID Service returns error: <Error Message>
	AP121	User already has an active certificate request
	AP122	Document size is bigger than the limit
	AP123	No document to upload

API	Status Code	Status Message
RequestRevokeCert	000	Success
	RV100	Certificate auto-revocation failed
	RV101	Missing required parameter: <Parameter Name>
	RV102	Invalid parameter length: <Parameter Name>
	RV103	Invalid value for RevokeBy. Either Admin (for Admin request) or Self (for User request) is valid
	RV104	Error in parameter validation: <Parameter Name>
	RV105	Manual approval is required
	RV106	Invalid validator value: <Parameter Name>
	RV107	Invalid parameter format: <Parameter Name>
	RV108	Invalid image file: <Parameter Name>
	RV109	Invalid base 64 string: < Parameter Name >
	RV110	Invalid value for IDType. Either P (for Passport) or N (for Malaysian NRIC) is valid
	RV111	Invalid certificate status: <Certificate Status>
	RV112	Invalid AuthFactor
	RV113	AuthFactor has expired
	RV114	AuthFactor validation failed
	RV115	Failed to retrieve certificate request record

	RV116	User has no completed certificate request record
	RV117	MyTrustID Service returns error: <Error Message>
	RV118	Document size is bigger than the limit
	RV119	No document to upload
	RV120	Failed to revoke: <Error Message>

API	Status Code	Status Message
RequestEmailOTP	000	Success
	OT100	Failed to generate OTP: <Error message>

API	Status Code	Status Message
UpdateEmailAddress	000	Success
	UI100	Failed to update: <Error message>

API	Status Code	Status Message
VerifyCertPin	000	Success
	VP100	Failed to verify PIN: <Error Message>
	VP101	User has no valid certificate
	VP102	The certificate has not yet been activated
	VP103	Failed to read user's digital certificate
	VP104	Certificate PIN is invalid
	VP105	Invalid certificate serial number

API	Status Code	Status Message
ResetCertificatePin	000	Success
	RP101	MyTrustSigner Reset Pin Service returns error: <Error Message>
	RP102	Error in reset certificate pin - Cert has been revoked
	RP103	Mininum 8
	RP104	Failed to reset PIN: <Error Message>

3.3. Signature Location

The following depicts PDF Signature location (X-Y coordinate):

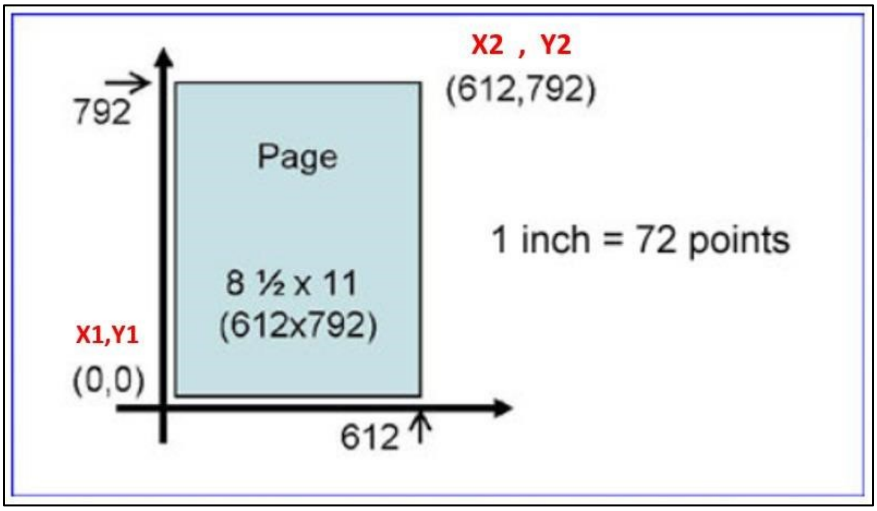
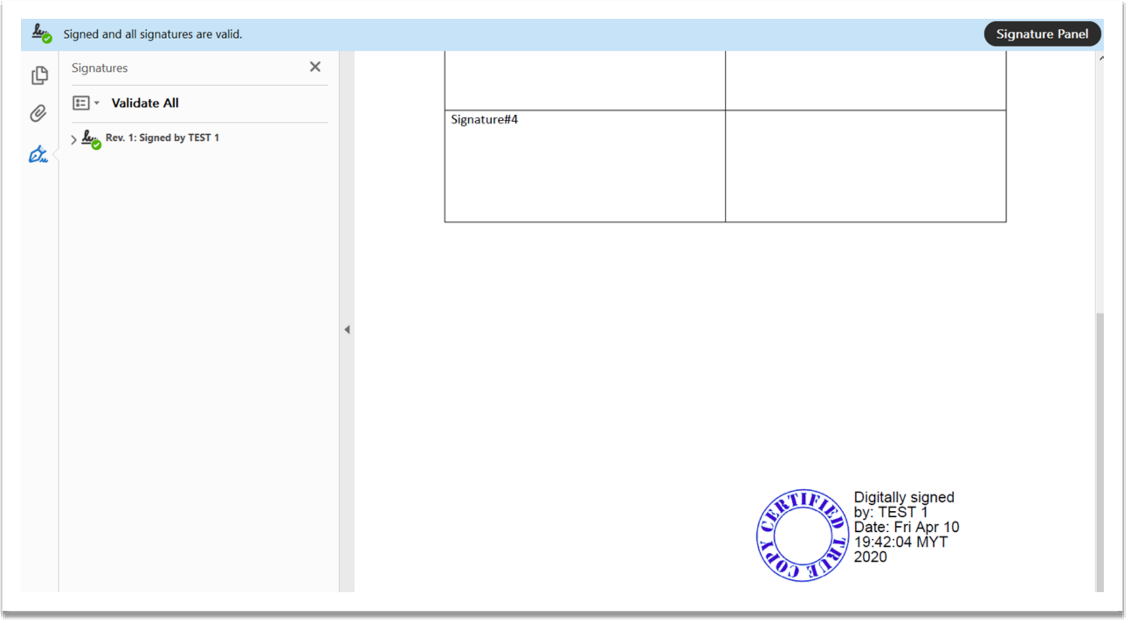


Figure 2: Signature coordinates (XY)

3.4. Digital Signature Samples

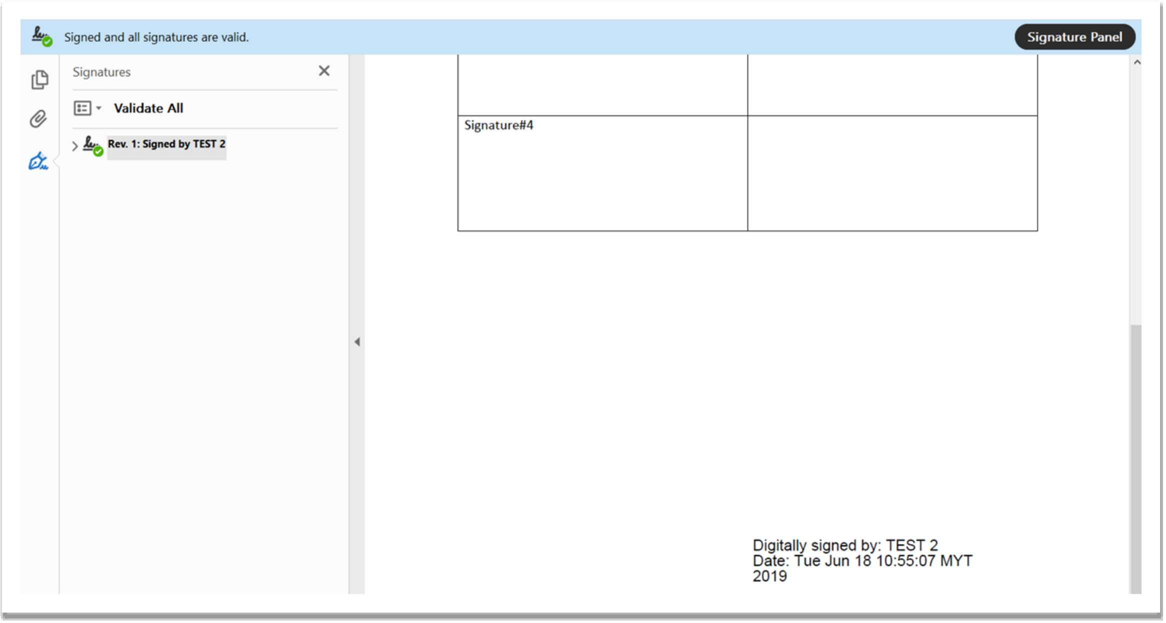
3.4.1. Signature With Image



Digitally signed by: TEST 1
Date: Fri Apr 10 19:42:04 MYT 2020

Figure 3: Signature with image

3.4.2. Signature Without image



Digitally signed by: TEST 2
Date: Tue Jun 18 10:55:07 MYT 2019

Figure 4: Signature without image

3.4.3. Invisible Signature

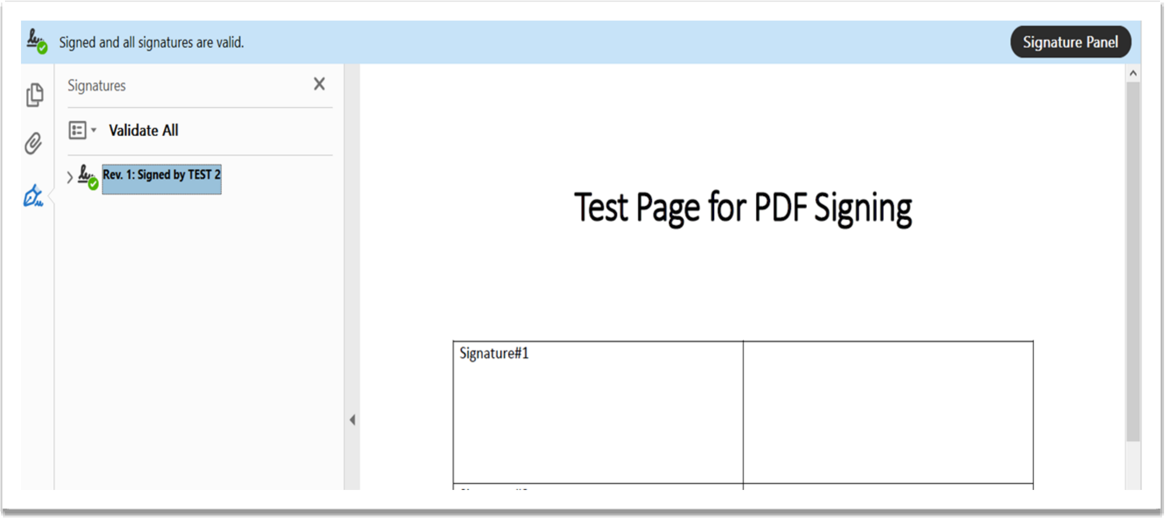


Figure 5: Invisible Signature

4. Other Requirements

4.1. Software Requirements

Operating System

MyTrust Agent can be deployed in Linux or Windows OS platform.

- Microsoft Windows 7 x64, 10 x64; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64 or;
- CentOS Linux, Red Hat Enterprise Linux AS/ES 6 x64, 6 x86, 7 x64

-Recommended is Linux based-

Software requirements:

- JDK 17 (the latest JDK 17 latest version)
- Tomcat version 9 (the tomcat 9 latest version)

4.2. Hardware Requirements

Minimum hardware requirements:

- RAM: 16GB
- HDD: 20GB
- CPU: 64-bit
- Cores: Single (Single Core 3GHz or higher, Dual Core 2GHz or higher recommended)

4.3. Network Requirements

Network Access

MyTrustAgent located at client premises shall have access to the following web based services:-

- MSCTG CRL/OCSP service
- MSCTG Timestamping service
- MSCTG CA system

SSL Certificate

If the MyTrustSigner API is designed to face public access, connected server/transaction server or host must has SSL client authentication digital certificate and keypairs to be implemented as identification for the access and permission rights. The SSL certificate can be purchased from MSC Trustgate.

5. Verification Data Information

This section briefly defines the **Authorized Personnel** definition.

The AP is required to pass the following data to MSC Trustgate for further validation and certificate issuance process, ensuring compliance with the Digital Signature Act 1997 and Digital Signature Regulations 1998 (DSA 1997 and DSR 1998):

i. **Personally Identifiable Information (PII)**: This refers to any data that can be used to identify a specific individual. Examples of PII include a person's name, address, phone number, email address, Mykad number, passport number, and any other information that can be linked directly or indirectly to a particular person.

ii. **Verification status**: Refers to the outcome or result of a verification process, confirming and establishing a linkage between the claimed identity and the real-life existence of the applicant presenting the government-issued photo ID as evidence.

iii. **Date time of verification**: To indicate date and time when applicant’s identity is verified during the certificate application process.

iv. **Verifier**: Refers to identifying the individual, entity, or machine responsible for conducting the verification process.

v. **Verification Method**: Refer to the method used by the AP to confirm the identity of the applicant. It can be, and is not limited one of the following:

   a. Manual face-to-face verification
   b. Manual face-to-face verification with biometric
   c. Secure automated self-service verification with biometric
   d. e-KYC (face recognition with liveness detection) as per Bank Negara Malaysia (BNM) Electronic Know-Your-Customer (e-KYC)

vi. **Evidence**: Refers to the supporting documents used to confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the government-issued photo ID. Additionally, the Authorized Personnel (AP) may provide additional documents such as a letter of authorization (LoA) or a membership document to associate the applicant with an organization if this information is required to be included in the digital certificate s

6. Revocation Definitons

As mentioned the MSC Trustgate's CPS, https://www.msctrustgate.com/tgcps, section 7.2 CRL profile, MSC Trustgate.com specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

1. keyCompromise
2. cACompromise
3. affiliationChanged
4. superseded
5. cessationOfOperation

As defined in the earlier section, below is further definitions of the revocation reasons:

keyCompromise	The token or disk location where the private key associated with the certificate has been compromised and is in the possession of an unauthorized individual. This can include the case where a laptop is stolen, or a smart card is lost.
CACompromise	The token or disk location where the CA's private key is stored has been compromised and is in the possession of an unauthorized individual. When a CA's private key is revoked, this results in all certificates issued by the CA that are signed using the private key associated with the revoked certificate being considered revoked.
affiliationChanged	The user has terminated his or her relationship with the organization indicated in the Distinguished Name attribute of the certificate. This revocation code is typically used when an individual is terminated or has resigned from an organization. You do not have to revoke a certificate when a user changes departments, unless your security policy requires different certificate be issued by a departmental CA.
superseded	A replacement certificate has been issued to a user, and the reason does not fall under the previous reasons. This revocation reason is typically used when a smart card fails, the password for a token is forgotten by a user, or the user has changed their legal name.

cessationOfOperation	If a CA is decommissioned, no longer to be used, the CA's certificate should be revoked with this reason code. Do not revoke the CA's certificate if the CA no longer issues new certificates, yet still publishes CRLs for the currently issued certificates.