User Requirements Specifications

Project Name:	OPG Capital PKI		
Date:	06 August 2025	**Release:**	~~Draft~~ / Final
Author:	Rosliza binti Abdul Ghani		
Owner:	Amir Faiz Husin		
Client:	OPG Capital Holdings 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
06 Aug 2025	-	Initial first-cut	No

Approvals

This document is prepared by MSC Trustgate.com Sdn. Bhd., in fulfilment of the requirements of the OPG CAPITAL PKI projects deliverables. Preparation of this document is under the authority of MSC Trustgate.com Sdn. Bhd. Project Manager and all relevant parties within MSC Trustgate.com Sdn. Bhd. Before being effective this document shall be checked and approved by OPG Capital Holdings Sdn Bhd.

This document requires the following approvals. A signed copy should be placed in the project files. All items outlined in this document shall be deemed agreed upon in the absence of any feedback within seven (7) working days from the date of submission.

Name	Signature	Title	Date of Issue	Version
Dr. Ivan Chew		OPG Capital Holdings Sdn Bhd.	06 Aug 2025	1.0
Amir Faiz Husin		Project Manager, MSC Trustgate	06 Aug 2025	1.0

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version
Dr. Ivan Chew	OPG Capital Holdings Sdn Bhd.	06 Aug 2025	1.0
	OPG Capital Holdings Sdn Bhd.	06 Aug 2025	1.0
	OPG Capital Holdings Sdn Bhd.	06 Aug 2025	1.0
Ruzita Ahmad	Account Manager	06 Aug 2025	1.0
Fadzil Mohd Raihan	Head of Product Development	06 Aug 2025	1.0
Amir Faiz Husin	Project Manager	06 Aug 2025	1.0
Zulkifle Muhammad	Developer	06 Aug 2025	1.0

Overview

This document is to finalise on the Analysis/Software Requirements of the planned timeline.

A process flow is created based on the initial agreed discussions on the requirements. It is placed in this document and require a signed approval before it goes into the execution phase of the User Requirement Specifications (URS).

The terms and abbreviations used in this document and their definitions that are needed in this document.

Contents

Introduction

MSC Trustgate is to deliver a public key infrastructure (PKI) solution, digital certificates, and digital signature component to the OPG CAPITAL PKI project. MSC Trustgate will be known as “Trustgate” throughout the rest of this document.

The company, OPG Capital Holdings Sdn Bhd. which hereinafter will be referred to as **“OPG CAPITAL”**. The project name shall be known as OPG CAPITAL Public Key Infrastructure project which hereinafter will be referred to as **“OPG CAPITAL PKI”** project.

Purpose

The purpose of this Users Requirements and Specifications (URS) document is to define prerogative agreeable stated requirements, scope, and act as the baseline deliverables to the development phase of system analysis and design for the OPG CAPITAL PKI project.

This URS will also be used as the reference point for the System Integration Test (SIT) and User Acceptance Test (UAT) phases and its signoff’s.

Project Background

Current Mode of Operations (CMO) is not seen as OPG CAPITAL seeks an integration of a PKI solution to its application.

This project was initiated by OPG CAPITAL to improve the efficiency of the e-Lending process within the OPG Capital application. Generally, OPG Capital provides loan facilities to clients who apply through the platform, with the entire process from application submission to loan agreement signing carried out digitally. Once a loan application is approved, the client will proceed to sign the Loan Agreement electronically within the OPG Capital app.

Objective and Outcome

The Future Mode of Operations (FMO) for OPG CAPITAL to achieve the PKI part, OPG CAPITAL PKI will need 2 (two) main parts from Trustgate which consist of:

i. Certificate Enrollment

ii. Digital Signing

Project Product Description and Composition

Objective

The objective is to describe the OPG CAPITAL PKI product and its composition. Authenticate and verify OPG CAPITAL user's identification and utilize their own digital certificate to create OPG CAPITAL user's digital signatures on Loan Agreement.

There are two types of users involved in the digital signing process which is internal and external. Internal users refer to officers or personnel within the organization who are responsible for approving and attesting the lending application, while external users are the borrowers applying for the loan.

For internal users, OPG Capital is required to submit a **Letter of Authorization (LoA)** to MSC Trustgate, confirming the list of authorized personnel who will be responsible for approving and attesting the lending applications. The LoA must be signed by a **company director** or an authorized signatory.

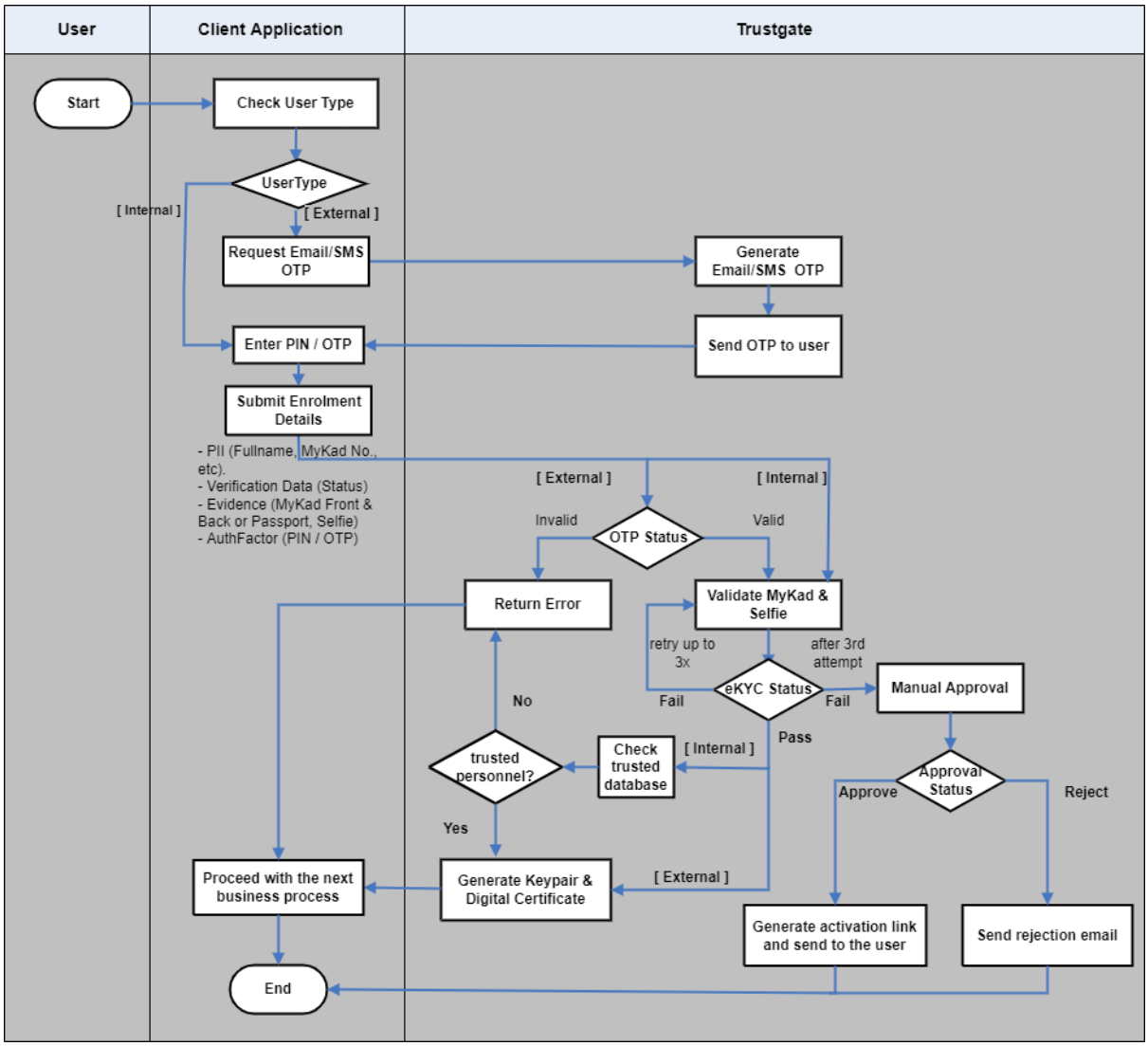
The list of authorized personnel should include the following details:

1. Full Name
2. NRIC/MyKad No. or Passport No.
3. Email Address
4. Organization Name
5. SSM No.

Once the list of names has been received, it will be stored in a trusted database, which will serve as the source for validating their legitimacy.

The high-level process flow are as follows: -

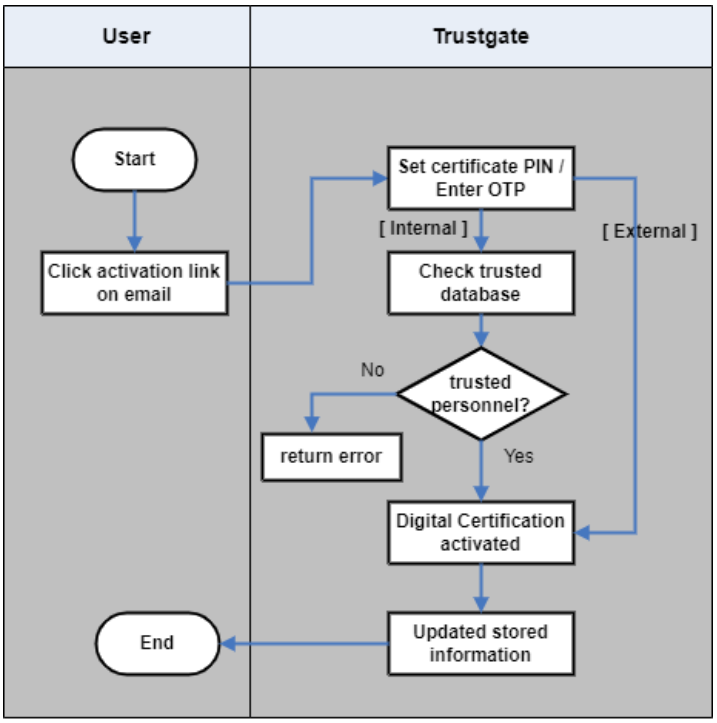
Certificate Enrollment High Level Process Flow



1. The client application starts the registration process by checking whether the user is an internal or external user.
2. If the user is external, the client application requests an email/ SMS OTP from Trustgate, which then generates and sends the OTP to the user. Internal users will enter PIN number to serve as security code for preserve their digital certificate.
3. After OTP validation, the client application collects the required enrollment details:
    - Personal Identifiable Information (PII)
    - Verification status
    - Identification evidence (MyKad/ Passport front and back, selfie)
    - Authentication factor (PIN / OTP)
4. These details are submitted to Trustgate's API for validation and digital certificate issuance.
5. Trustgate validates the OTP status for external users.
6. Then, Trustgate validates MyKad and selfie for both internal and external users.

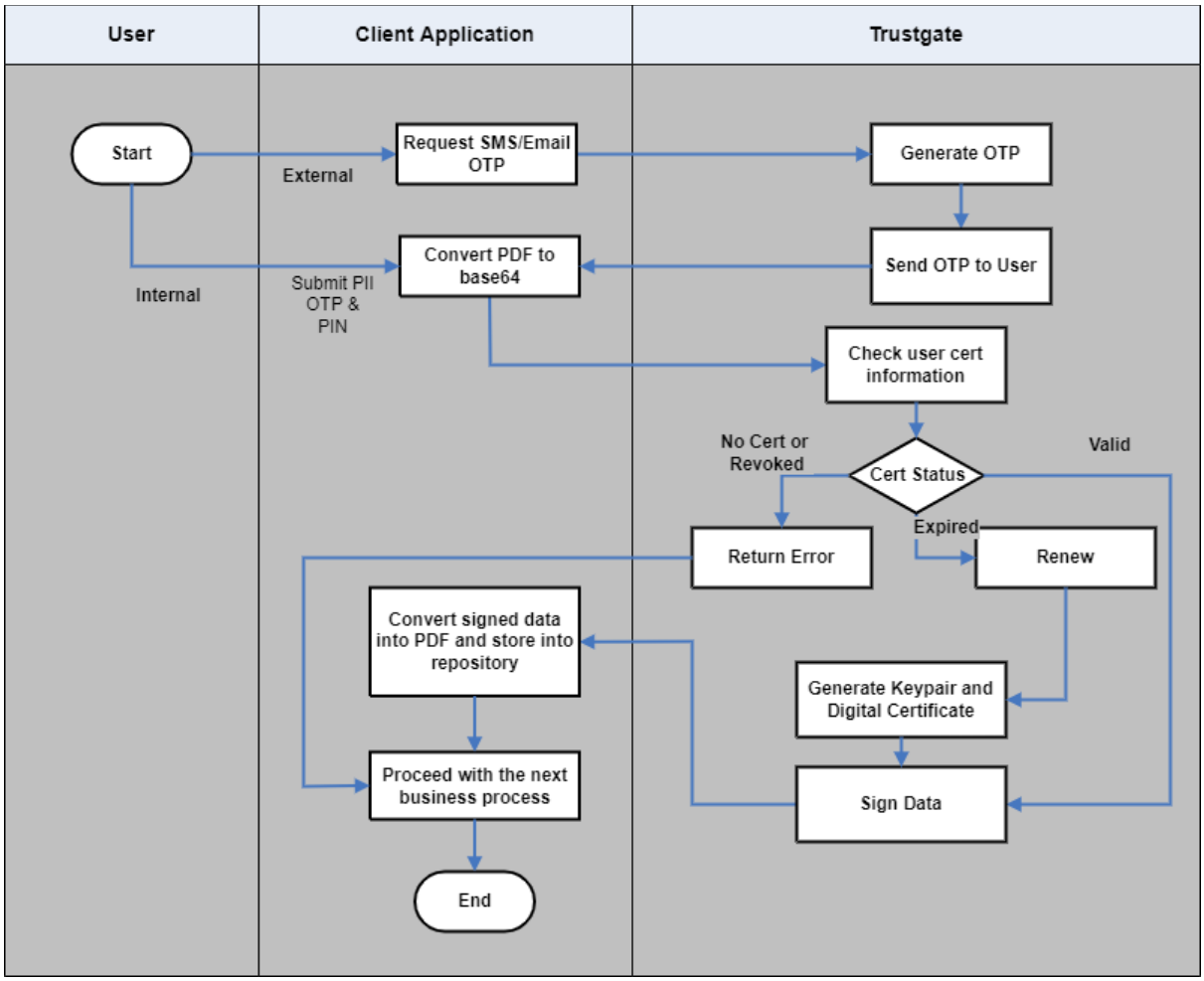
7. Using the submitted data, the Trustgate API will perform the eKYC process to verify the accuracy and authenticity of the information and documents in accordance with compliance requirements.
8. Upon completion, the API will return a result indicating whether the verification passed or failed. If successful, the digital certificate will be issued immediately, and the application will receive the certificate details in the API response. If unsuccessful, an error message will be returned, allowing the user to resubmit the request up to three (3) times.
9. If the process fails after the third attempt, a manual verification process will be triggered. Trustgate will manually review the submitted data and documents before approving or rejecting requests and this process will take at least three to five business days.

Certificate Activation High Level Process Flow



1. Users who undergo manual verification will receive an email notification confirming the outcome of their digital-certificate request.
2. For those who succeed, the notification email will contain an activation link to allow users to perform an activation for their digital certificate.
3. Once they click on the activation link, they will be redirected to an activation page which requires them to key-in their certificate PIN / OTP.
4. Once completed, the digital certificate is activated, and the information is securely stored by Trustgate.

Digital Signing High Level Process Flow



1. The client application handles document preparation. For external users, an OTP request is initiated and Trustgate generates and sends the OTP via SMS/ email. For internal users, client applications should submit PIN numbers to initiate digital signing.
2. Once the PDF document is ready, the client application converts it into a Base64 string format. This step is applicable to both internal and external users.
3. The client application will then initiate a call to Trustgate API, sending the Base64-encoded PDF along with the user's data (PII) and authentication factor such as PIN or OTP.
4. Trustgate API will verify the validity of the user's digital certificate before proceeding with the digital signing process.
5. Once the document is successfully signed, the signed data will be returned to the client application, which will then either proceed with the next signer or continue with the subsequent business process.

High Level Project Timeline

No	Key Milestones	Target Date
1.	Kick-Off	5 Aug 2025
2.	URS Finalized and Sign Off	6 – 15 Aug 2025
3.	Pilot Preparation & Deployment	18 – 27 Aug 2025
3.1.	Integration with Business Apps (OPG Capital Staging/Pilot/Dev)	28 Aug – 12 Sept 2025
4.	SIT Completed and Sign-Off	17 – 19 Sept 2025
5.	Prod Release & Deployment	22 -24 Sept 2025
5.1.	Integration with Business Apps (OPG Capital Prod)	25 Sept – 3 Oct 2025
6.	UAT Completed and Sign-Off	6 – 8 Oct 2025
7.	Go-Live	9 Oct 2025

Scope

A. Trustgate to provide 8 API to OPG CAPITAL which are as below: -

1. EnrollCertificateWithEKYC
2. GetCertInfo
3. SignPDF
4. VerifyPDFSignature
5. RevokeCert
6. RequestEmailOTP
7. RequestSMSOTP
8. ResetCertificatePin

B. OPG CAPITAL to provide the following servers as per below environments; -

1. Pilot/Test Environment
2. Production Environment

C. Trustgate to install necessary software needed for its modules onto the environments mention on item (B) above. The software needed are as below; -

1. JDK 17.02 (or latest variant)
2. Apache Tomcat 9.0.62 (or latest variant)

Project Exclusions

1. To provide any hardware, maintenance, installation, and warranties.
2. To accommodate any software/hardware license, unless stated otherwise.
3. Server/Operating System hardening.
4. Performance and Security Issues.
5. Liabilities are imposed on performance and security issues that are caused by hardware or network.
6. Training will NOT be provided, as the integration is between API to Web Services.
7. Validation of MyKad data against Jabatan Pendaftaran Negara (JPN)

Project Approach

The project is using the Agile Methodology, where product, features and deliverables of OPG CAPITAL PKI project are released in a staggered approach.

Project Communications

Communications on the project will be via

1. Email – As per distribution list
2. WhatsApp Group

Acceptance Criteria

1. Below outlines the Entry Criteria to signify the project is good to enter UAT phase:

   - All test cases have been reviewed and accepted by OPG Capital.
   - System Integration Testing has been completed and accepted by OPG Capital.
   - All development on the features for a release of OPG Capital PKI part to be completed.

2. Below outlines the Acceptance Criteria to signify the successful completion of UAT:

   - All test cases are executed successfully by OPG Capital.
   - All defects and severity have been triaged and agreed upon.
   - All Severity **Critical** defects are resolved and closed.
   - All Severity **Major** defects are resolved and closed or with a work-around agreed by OPG Capital.

Project Tolerances

5% - 10% deviation from the plan.

Acceptance Method

Project goes through phases of SIT and UAT before actual implementation or Go Live. The project shall meet the exit criteria as stated in the Acceptance Criteria in order for the project Team to recommend on the exit of each phase.

Acceptance Responsibilities

All testers are required to sign-off for the acceptance. Thereafter, the Project Team to recommend on the exit of each phase.

Terminology

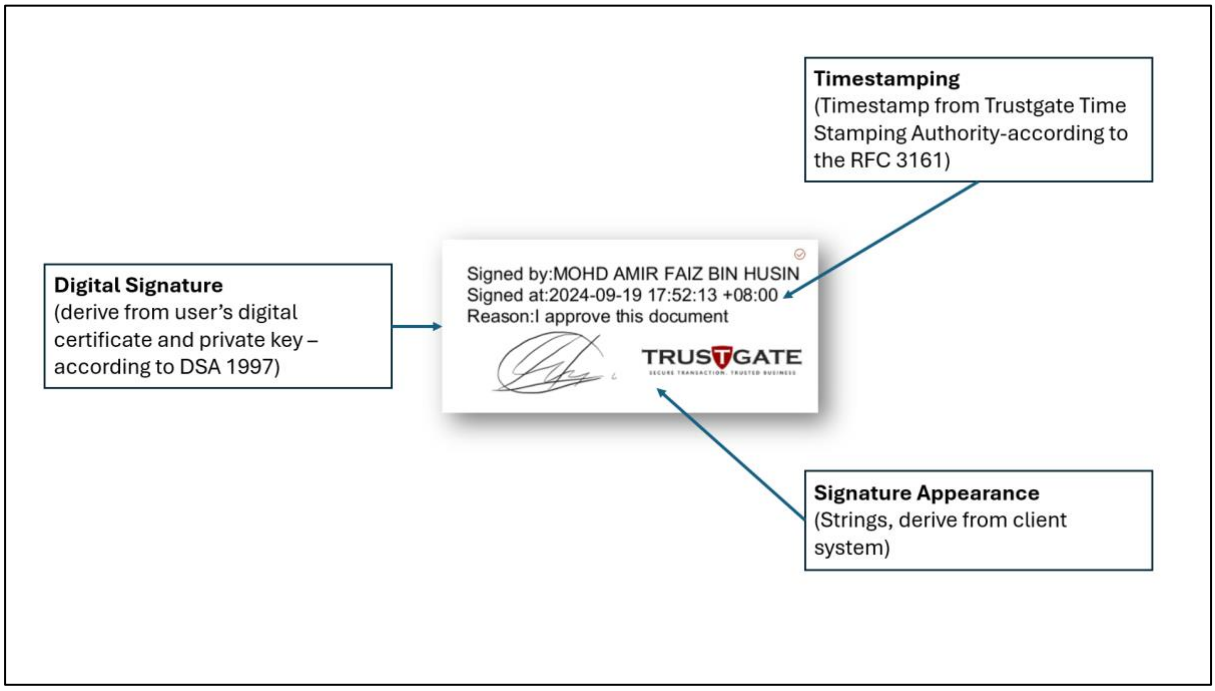
The terms and abbreviations used in this document and their definitions that are needed in this document are shown as below.

Abbreviations	Definition
API	Application Programming Interface
App	Application
CMO	Current Mode of Operations
FMO	Future Mode of Operations
ICD	Interface Control Document (API Technical Specifications Document)
eKYC	Electronic Know Your Customer
JPN	Jabatan Pendaftaran Negara
MyKad	Malaysian National Registration Identity Card
PIN	Personal Identification Number
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PRD	Production Environment
OPG CAPITAL	OPG Capital Holdings Sdn Bhd
OPG CAPITAL PKI	OPG Capital Public Key Infrastructure
SIT	System Integration Testing
Trustgate	MSC Trustgate.com Sdn. Bhd.
UAT	User Acceptance Test
URS	User Requirement Specifications

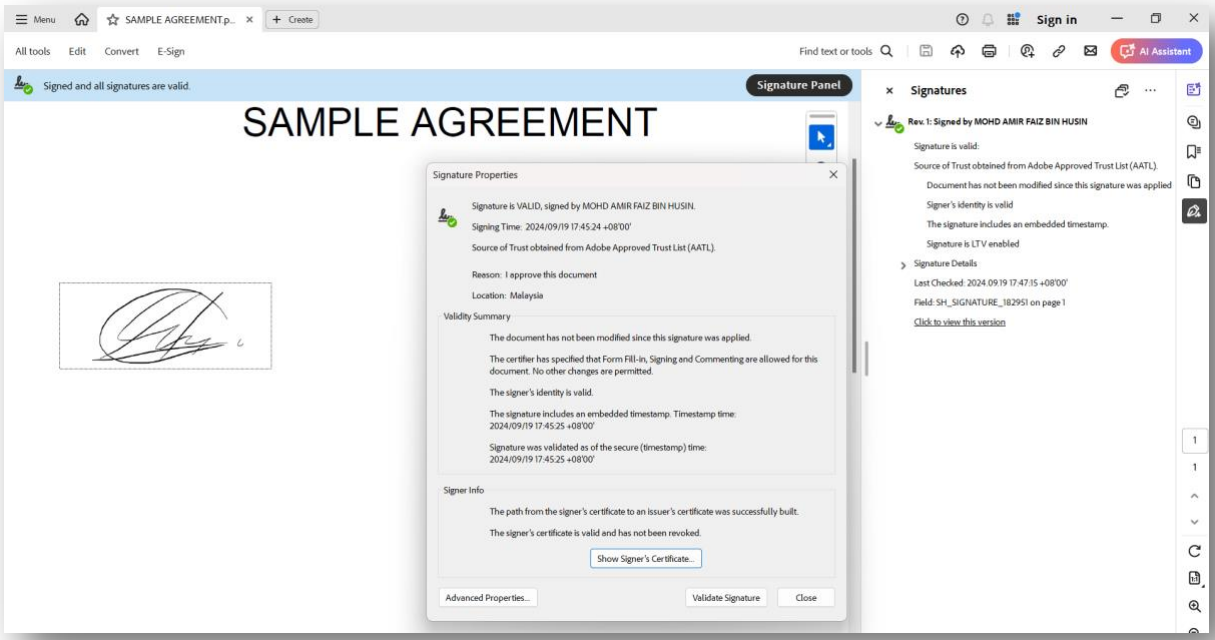
Appendix 1

Sample of Digital Signature

Digital Signature with the display appearance purposes, as a visible signature on a glance. The customizable digital signatures appearance contains several details so that the signatures are visibly verifiable.



Digital signature output in accordance with the Digital Signature Act 1997 (Act 562), RFC 3126 and RFC 3647.Timestamp is according to the RFC 3161 and Malaysia Communications and Multimedia Commission (MCMC) Guidelines for Recognised Date/Time Stamp Service. Our NTP is align with the Malaysia local time or officially named as the Malaysia Standard Time (MST) is decided by the Time and Frequency Laboratory of the National Metrology Institute of Malaysia (NMIM), the appointed national timekeeper (refer to Cabinet Note H 226/92), from the caesium atomic clocks that it maintained.



Long Term Validation (LTV) means that both a timestamp and the signer's certificate status information (OCSP or CRLs) is embedded inside the signature.