PT DIGITAL TANDA TANGAN ASLI

PANDUAN VERIFIKASI TANDA TANGAN ELEKTRONIK TERSERTIFIKASI DAN VERIFIKASI SERTIFIKAT ELEKTRONIK

No Dokumen : IT-SOP-56-00

No Revision : 00

4 April 2022

Administrator CP Front-End

Digitally Signed By
Bilal Abudan

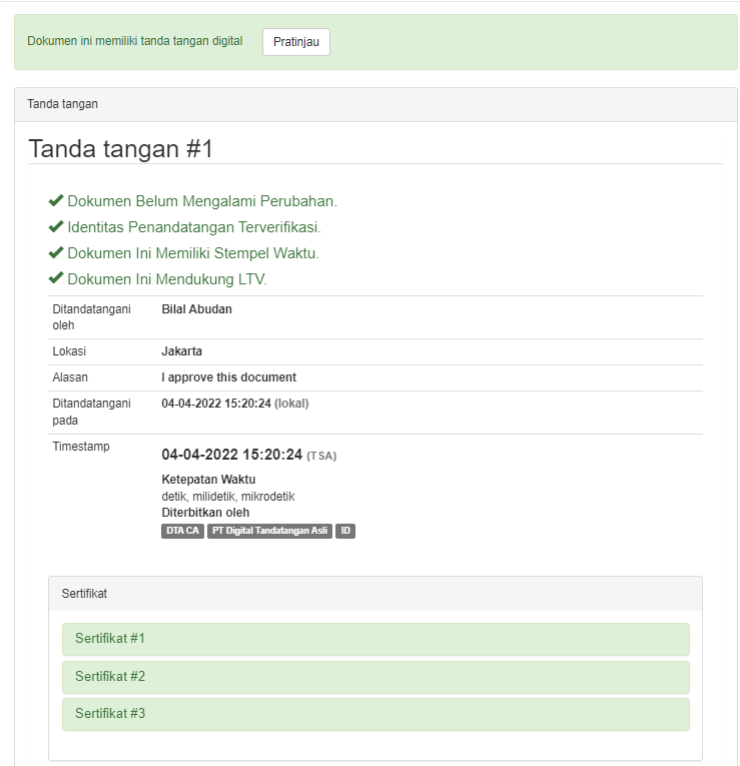
Bilal Abudan

Daftar Isi

Verifikasi melalui web

A. Buka situs https://tte.kominfo.go.id/verifyPDF , kemudian seret berkas pdf ke kotak bergaris putus-putus atau klik untuk memilih file di explorer, kemudian klik “Unggah”

B. Jika berkas memiliki tanda tangan elektronik tersertifikasi maka setelah pengunggahan selesai akan muncul tampilan seperti pada gambar berikut.
   - Verifikasi Tanda Tangan Elektronik



   - **Dokumen Belum Mengalami Perubahan** artinya isi dokumen tersebut belum pernah diubah sejak dokumen tersebut ditandatangani (Integritas dokumen).

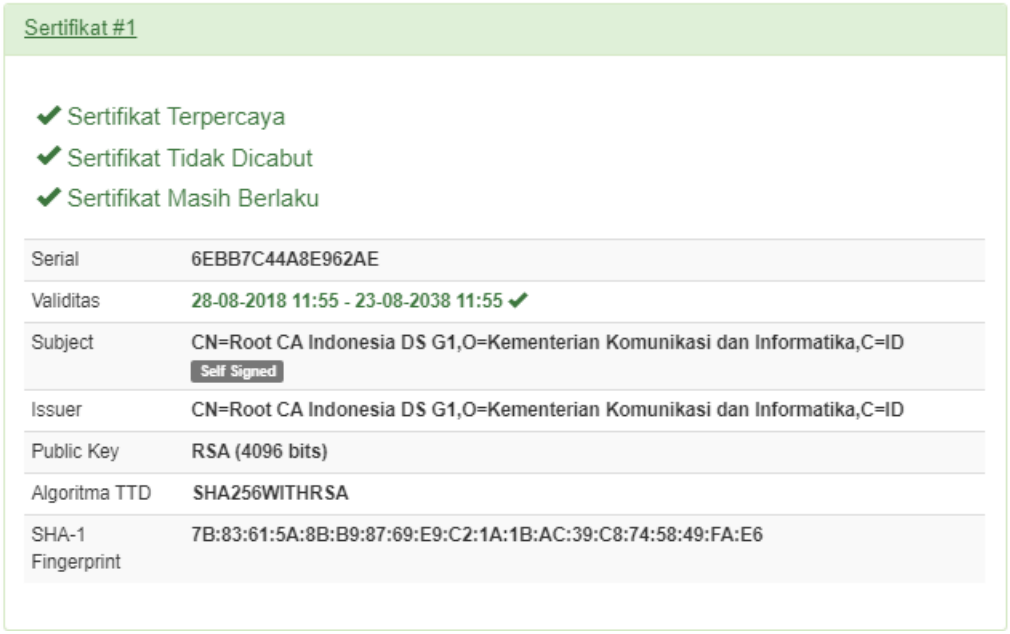
- **Identitas Penanda Tangan Terverifikasi** artinya sertifikat elektronik yang berisi identitas Penanda Tangan yang sudah diverifikasi oleh DTA dan sertifikat elektroniknya belum kadaluarsa dan tidak pernah dicabut.

- **Dokumen Ini Memiliki Stempel Waktu** artinya waktu penandatanganan mengacu pada Timestamp server yang disepakati, bukan terhadap waktu komputer lokal.

- **Dokumen Ini Mendukung LTV** artinya sertifikat elektronik yang digunakan untuk membuat tanda tangan elektronik tersebut menggunakan fitur Long-Term Validation (LTV), dengan tujuan agar tanda tangan elektronik tetap dapat diverifikasi meskipun masa berlaku sertifikat elektroniknya sudah habis.

- Verifikasi Sertifikat

  - Sertifikat RootCA



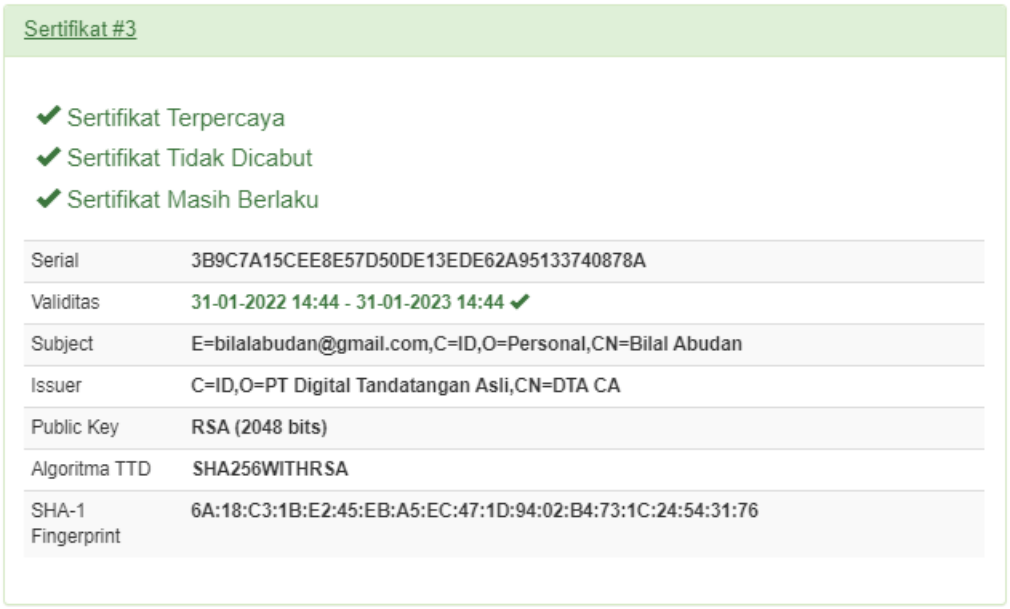
- Sertifikat IntermediaryCA


Sertifikat #2

✔ Sertifikat Terpercaya
✔ Sertifikat Tidak Dicabut
✔ Sertifikat Masih Berlaku

Serial	0888A72F7AE3604B
Validitas	22-12-2021 09:54 - 20-12-2031 09:54 ✔
Subject	C=ID,O=PT Digital Tandatangan Asli,CN=DTA CA
Issuer	CN=Root CA Indonesia DS G1,O=Kementerian Komunikasi dan Informatika,C=ID
Public Key	RSA (4096 bits)
Algoritma TTD	SHA256WITHRSA
SHA-1 Fingerprint	60:53:60:79:AF:E8:E1:1B:55:31:34:B0:41:CD:7A:5B:4B:0B:F1:23

- Sertifikat Entity


Sertifikat #3

✔ Sertifikat Terpercaya
✔ Sertifikat Tidak Dicabut
✔ Sertifikat Masih Berlaku

Serial	3B9C7A15CEE8E57D50DE13EDE62A95133740878A
Validitas	31-01-2022 14:44 - 31-01-2023 14:44 ✔
Subject	E=bilalabudan@gmail.com,C=ID,O=Personal,CN=Bilal Abudan
Issuer	C=ID,O=PT Digital Tandatangan Asli,CN=DTA CA
Public Key	RSA (2048 bits)
Algoritma TTD	SHA256WITHRSA
SHA-1 Fingerprint	6A:18:C3:1B:E2:45:EB:A5:EC:47:1D:94:02:B4:73:1C:24:54:31:76

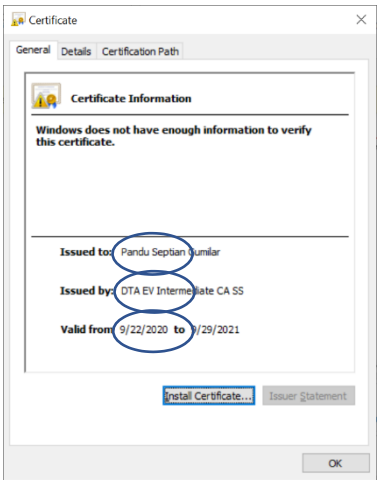
Keterangan rinci sertifikat:

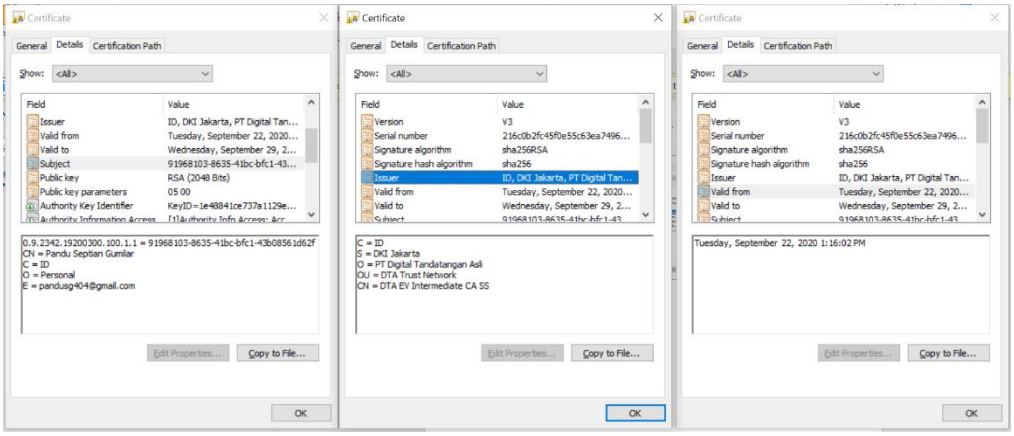
- **Sertifikat Terpercaya** maksudnya adalah sertifikat elektronik diterbitkan oleh DTA
- **Sertifikat Tidak Dicabut** maksudnya adalah sertifikat elektronik yang digunakan untuk menandatangani tidak pernah dicabut (revoke).
- **Sertifikat Masih Berlaku** adalah sertifikat elektronik yang belum kadaluwarsa saat digunakan untuk menandatangani dokumen.
    - Keterangan rinci sertifikat:
        - Serial: nomor serial unik sertifikat a elektronik

- Validitas: masa berlaku sertifikat elektronik
- Subject :
  - E : Alamat email pemilik sertifikat elektronik
  - O : Organization. Organisasi pemilik sertifikat elektronik.
  - C : Country. Negara dari pemilik sertifikat elektronik.
  - CN : Common Name. Nama pemilik sertifikat elektronik
- Issuer :
  - CN : Common Name. Nama pemilik sertifikat elektronik
  - OU : Organization Unit. Berisi unit organisasi pemilik sertifikat
  - O : Organization. Organisasi pemilik sertifikat elektronik.
  - C : Country. Negara dari pemilik sertifikat elektronik.
- Public Key: Algoritma yang digunakan untuk pembuatan pasangan kunci
- Signature Algorithm: Algoritma yang digunakan untuk melakukan hashing terhadap Dokumen Elektronik dan Tanda Tangan Elektronik
- SHA-1 Fingerprint: Nilai hash dari sertifikat elektronik

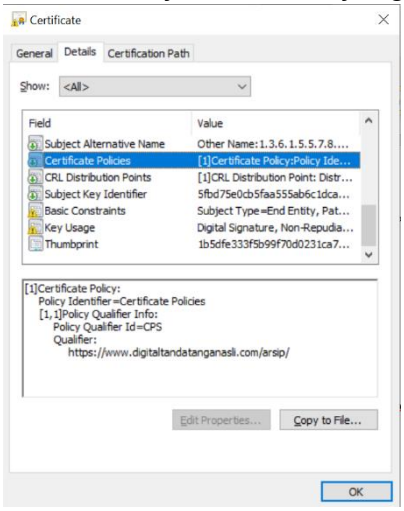
Verifikasi tanpa web

- Unduh sertifikat dari detail sertifikat yang ada di dokumen yang sudah ditandatangan
- Buka sertifikat dengan double click
- Attribute pada sertifikat sebagai berikut :
  a) Issued to / Subject, adalah pemilik dari sertifikat, contoh : Pandu Septian Gumilar.
  b) Issued by, adalah CA yang mengeluarkan sertifikat, contoh : DTA Intermediate CA SS
  c) Valid From - To -, adalah Masa berlaku sertifikat.

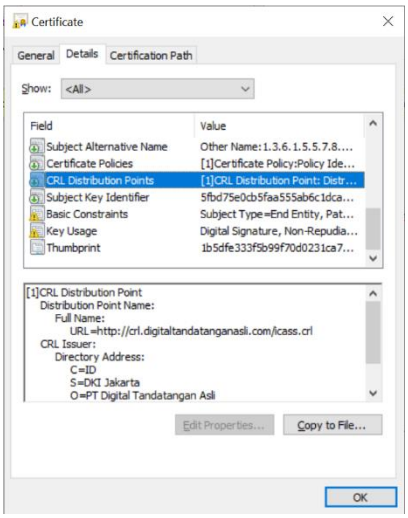




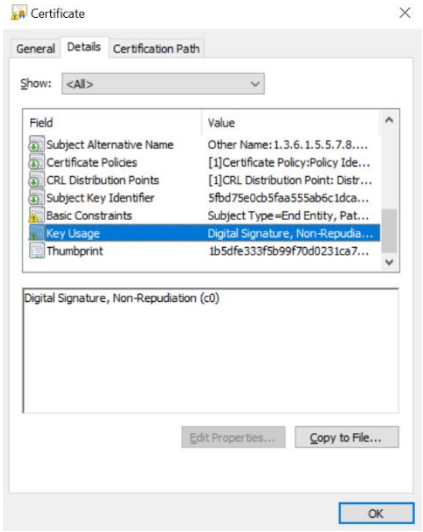
- Sertifikat Policy, berisi CPS yang dipublikasikan oleh CA.



- CRL Distribution Point, Sertifikat Revoke List dimana daftar sertifikat yang sudah dicabut.



- Key Usage, adalah peruntukan dari Sertifikat yang dikeluarkan, contoh nya untuk Digital Signature / Document Signing.



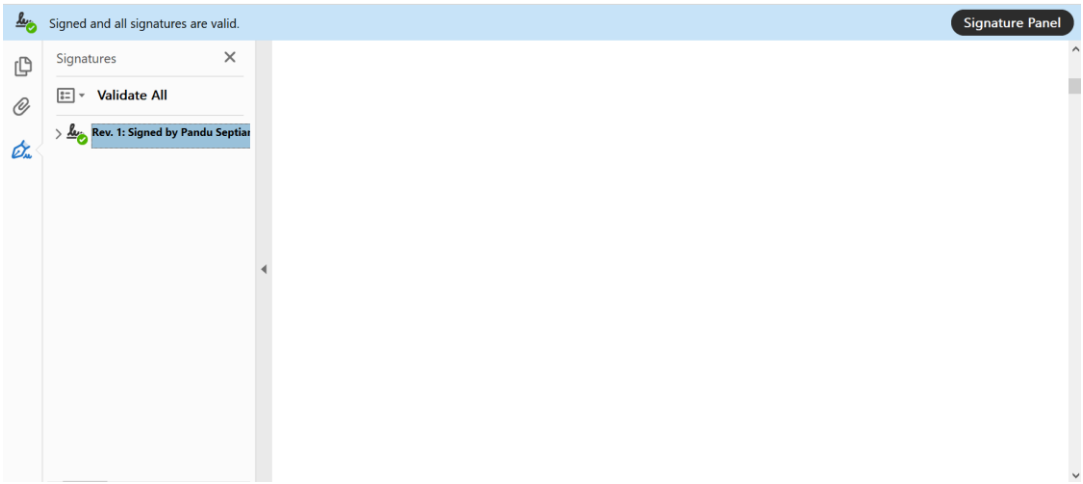
Catatan:

Setiap sertifikat dapat dilihat detailnya menggunakan pdf Adobe Reader atau membuka file.crt pada Windows. Informasi yang perlu diperiksa di antaranya :

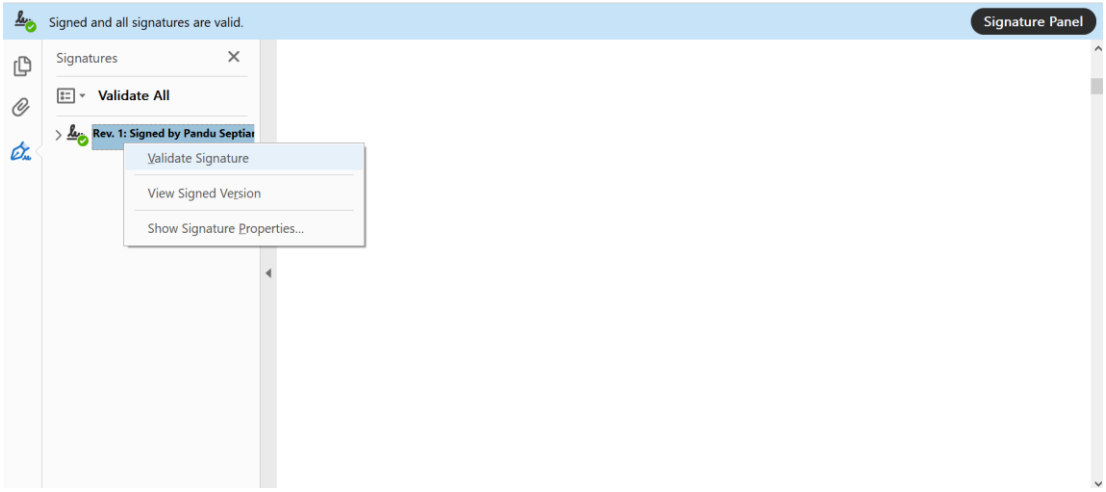
- Tanda tangan penerbit;
- Parameter kebijakan;
- Parameter penggunaan;
- Periode validitas;
- Informasi pencabutan atau pembekuan;
- Batas tanggung jawab penggunaan sertifikat

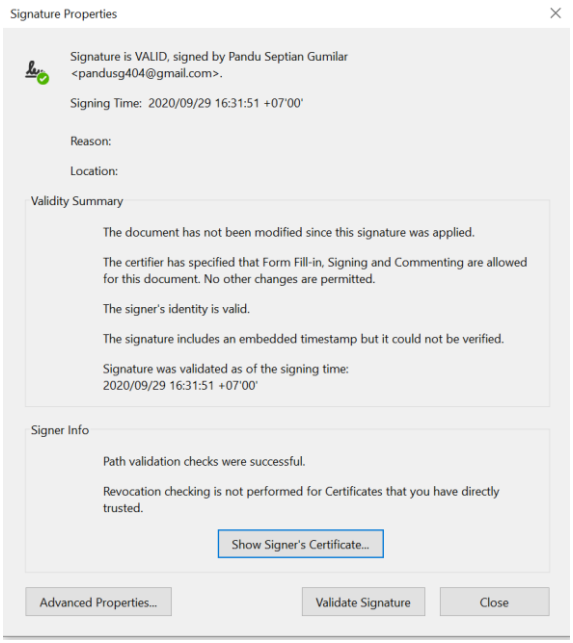
Verifikasi sertifikat menggunakan aplikasi Adobe Reader

A. Buka file dokumen menggunakan aplikasi Adobe Reader
B. Adobe Reader akan secara otomatis memeriksa validitas tanda tangan Ketika file dibuka. Tanda tangan akan dianggap valid jika kontennya tidak dirubah, serta sertifikat elektroniknya terpercaya (trusted) dan masih berlaku. Jika tanda tangan valid, akan muncul tampilan “Signed and all signatures are valid” seperti pada gambar

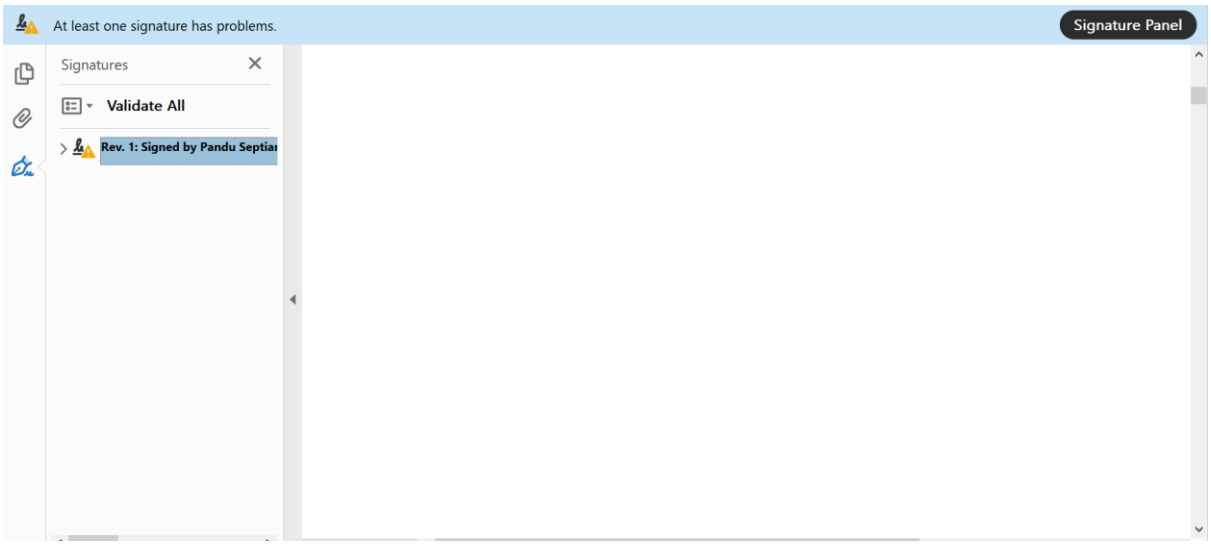


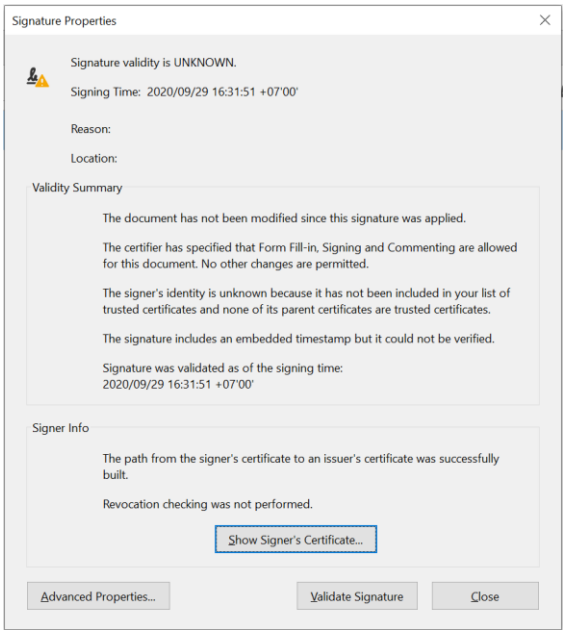
C. Untuk melihat detail tanda tangan, bisa dilakukan dengan mengklik Signature Panel, lalu klik kanan pada signature, kemudian pilih “Show Signature Properties”





D. Jika verifikasi dilakukan menggunakan Adobe Reader, ada kemungkinan bahwa sertifikat elektronik belum dikenali oleh Adobe Reader sehingga saat dilakukan verifikasi sebagaimana yang dijelaskan di atas, akan muncul keterangan Signature Validity is UNKNOWN seperti pada gambar di bawah.

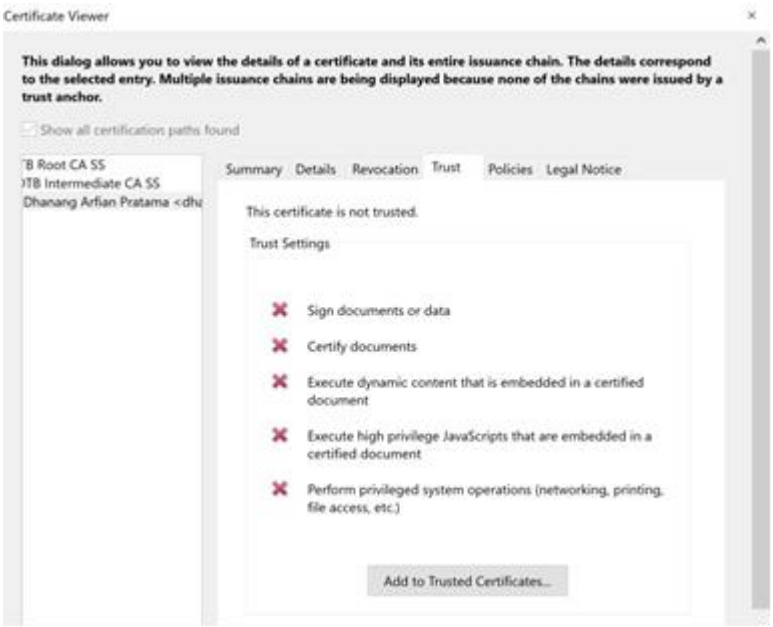




Ini dikarenakan identitas yang terdapat di sertifikat elektronik belum masuk ke daftar trusted sertifikat di komputer dimana Adobe Reader di-install. Alasan lainnya adalah sertifikat induk dari sertifikat elektronik belum dikenali sebagai trusted sertifikat .
Oleh karena itu, sertifikat harus ditambahkan secara manual ke komputer.

Hal ini bisa dilakukan dengan langkah-langkah berikut:

1. Pada Signature Properties ,klik “Show Signer’s Sertifikat” , pilih tab Trust , lalu klik Add to Trusted Sertifikats. Namun perlu dipastikan bahwa sertifikat induk tersebut memang sudah Anda percaya.



2. Setelah klik OK, lalu klik “Validate Signature” pada Signature Properties.
3. Selesai, tanda tangan telah tersetifikasi